	<b>UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA</b>			
	Documento <b>FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO</b>	Código <b>F-AC-DBL-007</b>	Fecha <b>10-04-2012</b>	Revisión <b>A</b>
Dependencia <b>DIVISIÓN DE BIBLIOTECA</b>	Aprobado <b>SUBDIRECTOR ACADEMICO</b>		Pág. <b>i(93)</b>	

## RESUMEN – TRABAJO DE GRADO

<b>AUTORES</b>	MARCELA TORCOROMA ÁLVAREZ ANGARITA LUZ MERY DURAN ALVERNIA		
<b>FACULTAD</b>	FACULTAD DE INGENIERIAS		
<b>PLAN DE ESTUDIOS</b>	ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS		
<b>DIRECTOR</b>	Mag. GENNY TORCOROMA NAVARRO CLARO		
<b>TÍTULO DE LA TESIS</b>	GUÍA DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN EN LUBRICENTRO AVENIDA OCAÑA, ESTABLECIDOS EN EL ESTÁNDAR ISO/IEC 27002:2013		
<b>RESUMEN</b> (70 palabras aproximadamente)			
<p style="text-align: center;">LA PRESENTE INVESTIGACION PROPONE EL DISEÑO DE UNA GUÍA DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN PARA EL LUBRICENTRO AVENIDA OCAÑA, DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013. PARA ESTO, SE HIZO NECESARIO REALIZAR EL DIAGNÓSTICO DE LA SITUACIÓN ACTUAL EN CUANTO A SEGURIDAD DE LA INFORMACIÓN Y ESTABLECER LOS POSIBLES RIESGOS A LOS QUE SE EXPONE LA EMPRESA, DEBIDO A LA FALTA DE POLÍTICAS, PROCEDIMIENTOS DOCUMENTADOS Y CONTROLES ESPECÍFICOS PARA LA ADECUADA PROTECCIÓN DE SUS ACTIVOS DE INFORMACIÓN.</p>			
<b>CARACTERÍSTICAS</b>			
PÁGINAS: 93	PLANOS:	ILUSTRACIONES:	CD-ROM: 1



VÍA ACOLSURE, SEDE EL ALGODONAL, OCAÑA N. DE S.  
Línea Gratuita Nacional 018000 121022 / PBX: 097-5690088  
[www.ufpso.edu.co](http://www.ufpso.edu.co)



GUÍA DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN EN LUBRICENTRO  
AVENIDA OCAÑA, ESTABLECIDOS EN EL ESTÁNDAR ISO/IEC 27002:2013

AUTORES:

LUZ MERY DURAN ALVERNIA

MARCELA TORCOROMA ALVAREZ ANGARITA

Trabajo de grado presentado para obtener el título de especialistas en Auditoria de Sistemas

Director

GENNY TORCOROMA NAVARRO CLARO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS

Ocaña, Colombia

Febrero, 2017

## Índice

<b>Introducción .....</b>	<b>12</b>
<b>Capítulo 1. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña, de acuerdo con el estándar internacional ISO/IEC 27002:2013.....</b>	<b>15</b>
1.1 Planteamiento del problema.....	15
1.2 Formulación del problema .....	16
1.3 Objetivos .....	16
1.3.1 Objetivo General.....	16
1.3.2 Objetivos Específicos.....	16
1.4 Justificación .....	17
1.5 Delimitaciones .....	18
1.5.1 Conceptual. ....	18
1.5.2 Espacial.....	18
1.5.3 Temporal.....	18
<b>Capítulo 2. Marco Referencial.....</b>	<b>19</b>
2.1 Marco Histórico .....	19
2.2 Marco conceptual.....	24
2.3 Marco contextual .....	27
2.4 Marco Teórico.....	28
2.5 Marco legal .....	31
<b>Capítulo 3. Diseño Metodológico .....</b>	<b>38</b>
3.1 Tipo de Investigación.....	38
3.2 Población.....	38
3.3 Muestra .....	38
3.4 Recolección de la Información .....	39

<b>Capítulo 4. Resultados .....</b>	<b>40</b>
4.1 Diagnóstico de la seguridad de la información en Lubricentro Avenida Ocaña. ....	40
4.2 Identificación de riesgos de seguridad de la información para Lubricentro Avenida Ocaña. .....	53
4.3 Guía de controles de gestión de seguridad de la información para Lubricentro Avenida Ocaña, de acuerdo con el estándar ISO/IEC 27002:2013. ....	67
<b>Conclusiones .....</b>	<b>80</b>
<b>Recomendaciones .....</b>	<b>82</b>
<b>Referencias.....</b>	<b>84</b>
<b>Apéndices.....</b>	<b>87</b>

## Lista de Tablas

Tabla 1. Dominio y objetivos de control ISO/IEC 27002:2013 .....	42
Tabla 2. Plan de Trabajo .....	45
Tabla 3. Identificación de activos .....	55
Tabla 4. Identificación de amenazas .....	56
Tabla 5. Matriz de riesgos informáticos para Lubricentro Avenida Ocaña. ....	58
Tabla 6. Establecimiento de riesgo 1 de seguridad de la información para Lubricentro Avenida Ocaña. ....	61
Tabla 7. Establecimiento de riesgo 2 de seguridad de la información para Lubricentro Avenida Ocaña. ....	62
Tabla 8. Establecimiento de riesgo 3 de seguridad de la información para Lubricentro Avenida Ocaña. ....	62
Tabla 9. Establecimiento de riesgo 4 de seguridad de la información para Lubricentro Avenida Ocaña. ....	63
Tabla 10. Establecimiento de riesgo 5 de seguridad de la información para Lubricentro Avenida Ocaña. ....	63
Tabla 11. Establecimiento de riesgo 6 de seguridad de la información para Lubricentro Avenida Ocaña. ....	64
Tabla 12. Establecimiento de riesgo 7 de seguridad de la información para Lubricentro Avenida Ocaña. ....	64
Tabla 13. Establecimiento de riesgo 8 de seguridad de la información para Lubricentro Avenida Ocaña. ....	65
Tabla 14. Establecimiento de riesgo 9 de seguridad de la información para Lubricentro Avenida Ocaña. ....	65
Tabla 15. Establecimiento de riesgo 10 de seguridad de la información para Lubricentro Avenida Ocaña. ....	66
Tabla 16. Establecimiento de riesgo 11 de seguridad de la información para Lubricentro Avenida Ocaña. ....	66
Tabla 17. Establecimiento de riesgo 12 de seguridad de la información para Lubricentro Avenida Ocaña. ....	67

Tabla 18. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 5 .....	68
Tabla 19. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 6 .....	69
Tabla 20. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 7 .....	70
Tabla 21. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 8 .....	71
Tabla 22. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 9 .....	72
Tabla 23. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 10 .....	73
Tabla 24. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 11 .....	74
Tabla 25. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 12 .....	75
Tabla 26. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 13 .....	76
Tabla 27. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 14 .....	77
Tabla 28. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 15 .....	77
Tabla 29. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 16 .....	78
Tabla 30. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 17 .....	78
Tabla 31. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 18 .....	79

**Lista de figuras**

Figura 1. Historia ISO/IEC 27001:2013.....	29
Figura 2. Estructura orgánica Lubricentro Avenida Ocaña. Fuente: Gerente Lubricentro Avenida Ocaña .....	41
Figura 3. Valoración del riesgo.....	57

## Lista de Apéndices

Apendice A. Instrumento para el diagnóstico inicial en materia de seguridad de la información en el Lubricentro Avenida Ocaña. ....	88
Apendice B. Solicitud documentación para la ejecución de la auditoría. ....	89
Apendice C. Lista de verificación controles de acceso a áreas seguras. ....	90
Apendice D. Lista de verificación controles para la protección física de los equipos de cómputo. ....	91
Apendice E. Entrevista evaluación mecanismos para el control de acceso a la información. ....	92
Apendice F. Lista de verificación controles para la protección física de los equipos de cómputo. ....	93
Apendice G. Entrevista evaluación controles organización de la seguridad de la información. ..	94
Apendice H. Entrevista verificación procedimientos para la gestión de activos. ....	95
Apendice I. Entrevista evaluación procedimientos para la gestión de los incidentes de seguridad. ....	96
Apendice J. Acta de entrega de la Guía de controles de seguridad de la información ISO/IEC 27002:2013 para Lubricentro Avenida. ....	97



**DEDICATORIA**

*A Dios, por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por disponer un camino lleno de personas maravillosas que han sido mi soporte y compañía durante mi vida .*

*Luz Mery Duran Alvernia*

*Dedico este nuevo logro a Dios quien me dio la fe, la salud, la fortaleza y la esperanza para culminar este proyecto.*

*A mi padre que aunque no esté en el mundo terrenal siento que siempre me acompaña.  
A mi mamá, mi hija María Isabella y a mi esposo Jhon, por su apoyo incondicional quienes de alguna manera contribuyeron a lograr esta meta que me propuse en la vida, permitiéndome crecer intelectualmente como persona y como ser humano*

*Marcela Alvarez Angarita*

## Introducción

Información se puede definir como “datos dotados de propósito”. En la actualidad, la información desempeña una función cada vez más importante en todos los aspectos de nuestra vida y se ha vuelto un componente indispensable para realizar negocios para casi todas las organizaciones y en un número cada vez mayor de empresas, la información es el negocio. Sería difícil encontrar un negocio que se haya mantenido al margen de la tecnología de la información y que no dependa de la información que procesa. Los sistemas de información han dominado la sociedad y los negocios, y la dependencia de estos sistemas y la información que manejan, es casi, indiscutiblemente absoluta (CONSULTORES, s.f.).

Esta dependencia de la tecnología, requiere implementar una serie de mecanismos que mantengan al margen de la información de la organización, las amenazas y los ataques potenciales que puedan afectarla, accesándola, modificándola o en el peor de los casos, eliminándola.

Contar con medidas de protección implica más que la simple implementación de controles; se necesita organizar la gestión de la seguridad de la información y que la misma tenga una visión sistémica, es decir, contemple todos los aspectos que directa o indirectamente pongan en riesgo los activos organizacionales y los datos necesarios para la marcha del negocio, así como la repercusión que su pérdida pueda traer para la empresa y para los demás stakeholders. Para cumplir con este cometido, el estándar internacional ISO/IEC 27002 de 2013, provee los lineamientos y las buenas prácticas en lo relacionado con la administración de la seguridad de la

información, estableciendo 14 dominios, 35 objetivos de control y 114 controles, todos éstos, útiles para la adecuada protección de la información de la organización.

El presente documento entrega los resultados de la evaluación realizada a Lubricentro Avenida Ocaña, en lo relacionado con la seguridad de la información y el diseño de una guía de controles bajo el estándar ISO/IEC 27002:2013, que una vez implementados, permita mejorar los niveles de seguridad en la empresa en mención.

La estructura del documento final del Proyecto, es la siguiente: en el primer capítulo, se hace mención del problema que dio origen a la presente propuesta, así como los objetivos planteados, la justificación y las delimitaciones del proyecto.

En el capítulo II, aparece el Marco Referencial, que pretende enmarcar el proyecto en los fundamentos teóricos, conceptuales, contextuales y legales, apuntando a la necesidad de establecer un sistema de gestión de la seguridad de la información para Lubricentro Avenida Ocaña.

En el capítulo III, se presenta el diseño metodológico necesario para la ejecución del proyecto.

En el capítulo IV, se muestran los resultados obtenidos producto de la aplicación de los instrumentos planificados; para esto, se realizó inicialmente una evaluación utilizada como diagnóstico de la seguridad de la información y de otros aspectos de seguridad física en

Lubricentro Avenida Ocaña, teniendo como marco normativo el estándar internacional ISO/IEC 27002:2013; para dar cumplimiento al segundo objetivo, se realizó una identificación de los riesgos potenciales de la empresa objeto de estudio, especificando las áreas o procesos más sensibles o de mayor vulnerabilidad; finalmente, se procedió a diseñar una guía de controles de seguridad de la información, de acuerdo con lo sugerido por el estándar ya mencionado.

Los capítulos V y VI, presentan las conclusiones y recomendaciones de la investigación.

# **Capítulo 1. Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña, de acuerdo con el estándar internacional ISO/IEC 27002:2013.**

## **1.1 Planteamiento del problema.**

La Seguridad de la Información permite a la organización asegurar la confidencialidad, integridad y disponibilidad tanto de sus activos informáticos como de los datos que utiliza para llevar a cabo su misión estratégica; dichas características, pueden, en un momento determinado no garantizarse, debido a los riesgos a los que estos activos están expuestos constantemente, por la inexistencia de controles que minimicen su impacto.

Lubricentro Avenida Ocaña, es una empresa dedicada a la comercialización y distribución de lubricantes, aditivos y productos de limpieza para vehículos automotores, además de la prestación de servicios de lavado para todo tipo de vehículo y parqueo las 24 horas. Atiende un número considerable de clientes al día, a los cuales busca satisfacer con la venta de sus productos o la prestación de sus servicios.

De acuerdo con un diagnóstico inicial (Ver Anexo A) realizado a la empresa en mención, se evidenció un nivel de riesgo considerable, debido a la carencia de controles de seguridad de la información, desde el punto de vista físico, como desde el aspecto relacionado con la seguridad lógica y de aplicaciones de software. De igual forma, a pesar de que existen algunas medidas para controlar ciertos activos, las mismas no son evaluadas, ni sometidas a verificación para

determinar su eficiencia y eficacia, generando entre otras situaciones, pérdidas constantes de información contable, redundancia de datos, específicamente de sus clientes, pérdida de activos y acceso no autorizado a información confidencial.

## **1.2 Formulación del problema**

¿Cuál será la estrategia que permita orientar la implementación de controles de seguridad de la información en Lubricentro Avenida Ocaña?

## **1.3 Objetivos**

### **1.3.1 Objetivo General.**

Diseñar una guía de controles de seguridad de la información en Lubricentro Avenida Ocaña, de acuerdo con el estándar internacional ISO/IEC 27002:2013.

### **1.3.2 Objetivos Específicos**

Realizar un diagnóstico del estado actual del Lubricentro Avenida Ocaña en cuanto a seguridad de la información, utilizando el estándar ISO/IEC 27002:2013.

Establecer los posibles riesgos para los activos de información en Lubricentro Avenida Ocaña.

Diseñar la guía de controles de gestión de seguridad de la información para Lubricentro Avenida Ocaña, de acuerdo como lo establece el estándar ISO/IEC 27002:2013.

#### **1.4 Justificación**

En la actualidad, con la significativa presencia de las tecnologías de la información y comunicación en las organizaciones y el gran volumen de información que se maneja al interior de las mismas, además de la preferencia cada vez más persistente de estar interconectado, las amenazas potenciales y el grado de exposición de los activos informáticos frente a éstas, son cada vez mayores, teniendo en cuenta, que la información sensible de una organización es blanco de ataque de terceros internos o externos que poseen cierto interés en la misma.

Por consiguiente, las organizaciones dentro de sus procesos de negocio, estrategias y actividades se han visto en la necesidad de incluir mecanismos de protección de forma sistemática y continua que les permita garantizar la seguridad de la información.

Por este motivo, se han desarrollado normas y estándares internacionales, diseñadas específicamente para orientar la adopción e implementación de buenas prácticas en lo relacionado con la gestión de la seguridad de la información de forma eficaz y eficiente a corto, mediano y largo plazo, con alto grado de flexibilidad y adaptabilidad a los requerimientos de la empresa.

De acuerdo con lo anterior, la presente propuesta pretende mediante el diseño de una guía de controles a partir del estándar ISO/IEC 27002: 2013, constituirse en una herramienta de gestión para Lubricentro Avenida Ocaña, que promueva las buenas prácticas en cuanto a seguridad de la información se refiere y que la implementación de los controles contemplados en dicho estándar, permitan garantizar la confidencialidad, integridad y disponibilidad de su información y de sus demás activos informáticos.

## 1.5 Delimitaciones

**1.5.1 Conceptual.** Los conceptos a manejar en este proyecto son los relacionados con la seguridad de la información, sistema de Gestión de Seguridad de la Información (SGSI), Riesgos, políticas de Seguridad de la Información y Controles, seguridad física, seguridad lógica y norma ISO/IEC 27002: 2013 estándar para la gestión de la seguridad de la información.

**1.5.2 Espacial.** El proyecto se desarrollará en Lubricentro Avenida Ocaña, en la ciudad de Ocaña, Norte de Santander, empresa que se dedica a la comercialización y distribución de lubricantes, aditivos y productos de limpieza para vehículos automotores, además de la prestación de servicios de lavado para todo tipo de vehículo y parqueo las 24 horas. Atiende un número considerable de clientes al día, a los cuales busca satisfacer con la venta de sus productos o la prestación de sus servicios.

**1.5.3 Temporal.** El tiempo determinado para la ejecución de la propuesta será de 12 semanas; se iniciará después de la aprobación del anteproyecto.



## Capítulo 2. Marco Referencial

### 2.1 Marco Histórico

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org. (El portal de ISO 27002 en Español, s.f.)

Las normas ISO/IEC 27001, ISO/IEC 27002 están enfocadas a todo tipo de organizaciones (por ej. empresas comerciales, agencias, gubernamentales, organizaciones sin ánimo de lucro), tamaños (pequeña, mediana o gran empresa), tipo o naturaleza.

En la realización de este documento se tomaron como referencias proyectos de investigación con temas afines y que se relacionan con los controles de seguridad de la información basados en el estándar ISO/IEC 27002:2013, realizados a nivel internacional, nacional y regional. Según (Molina Rincón, Rodriguez Alvarez, Sanchez Delgado, & Vergel Nuñez)

Esta guía tiene como propósito instruir en la implementación de controles, para proteger y salvaguardar tanto la información como los sistemas que la almacenan y administran.

Sustentando en un marco teórico basado en el estándar ISO/IEC 27002 código de buenas prácticas para la gestión de la seguridad de la información y los reglamentos internos de la institución.

El trabajo de investigación está compuesto por: el primer capítulo que contiene el problema, donde se especifica el título, el planteamiento del problema a tratar, los objetivos que se pretenden alcanzar con la investigación, la justificación e importancia, las limitaciones que se pueden presentar, así como los alcances para el desarrollo de la misma.

El segundo capítulo el cual contiene el marco teórico conformado por los antecedentes de la investigación, bases teóricas y legales con las cuales se fundamenta la investigación.

El tercer capítulo se establece la metodología para la realización de la investigación determinando el tipo de investigación que se va a realizar, la población y muestra a la cual se dirige la investigación, los instrumentos a utilizar para la recolección de la información (encuesta, entrevista y lista de chequeo) la forma como se recolectaran los datos y las técnicas para su análisis.

El cuarto Capítulo el cual contiene los resultados obtenidos de la investigación, análisis de controles existentes y una guía de buenas prácticas para la seguridad basada en la ISO/IEC 18

27002 código de buenas prácticas para la administración de la seguridad de la información y finalmente se incluye un capítulo de conclusiones y recomendaciones.

(Parra Alvernia, Contreras Navarro, Díaz Pacheco, & López Ovalle, 2014)\_en el presente documento de Políticas de Seguridad de la información para la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, busca fortalecer el compromiso con los procesos de gestión responsable de la información; que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad, teniendo como eje el cumplimiento de los objetivos misionales. El enfoque de esta investigación es cuantitativo y se fundamenta en un proceso deductivo, al plantear como hipótesis que las políticas de seguridad de la información contribuyen a dar un manejo adecuado de la información que se opera en la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar. Teniendo en cuenta lo anterior, este proyecto busca dar respuesta a la pregunta ¿Con el diseño de las políticas de seguridad de la información, permitirá a la Empresa Comunitaria de Acueducto de Rio de Oro, Cesar “EMCAR”, proteger y salvaguardar su información en caso de pérdida o daño?, la cual se quiere comprobar en esta investigación

Según (Iscala Tobito, Meléndez Buitrago, & Pabón Sánchez, 2014) hoy en día la rápida evolución del entorno competitivo y tecnológico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sus s (Doria Corcho, 2015)istemas. Por tal motivo surge el termino seguridad de la información, el cual hace referencia a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y

de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma. El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas. Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo. El propósito de este proyecto es proporcionar al área financiera de la Secretaria de Educación Departamental de Norte de Santander una visión general de los requisitos mínimos de seguridad que se le debe aplicar a sus procesos para salvaguardar la integridad de su información. A su vez se busca hacer una descripción de los controles que se deben tener en cuenta si se quiere cumplir con dicho objetivo, también pretende asignar lineamientos básicos tales como funciones y responsabilidades de todos los individuos que acceden al sistema ya que del comportamiento de estos se logran avances significativos en pro del cumplimiento de los indicadores de gestión.

(Doria Corcho, 2015) en el presente proyecto diseña un Sistema de Gestión de la Seguridad de la Información para la oficina de Sistemas y Telecomunicaciones de la Universidad de Córdoba que sirva como punto de partida para su implementación mediante un análisis de la situación actual de los dominios, objetivos de control y controles que sugiere la norma ISO 27001, la selección de una metodología de evaluación de riesgos informáticos, el establecimiento de una política de seguridad informática institucional que sea liderada por la alta gerencia, además de generar la documentación respectiva para los Planes de Continuidad de Negocio con

el fin de mantener y/o restaurar los servicios críticos y el análisis y selección de un modelo de Gobierno de Tecnología Informática que se ajuste a las necesidades institucionales.

(Pulgarín Gómez, 2014) En el presente proyecto, se analiza una empresa colombiana del sector agropecuario con más de 5000 empleados a nivel nacional. Se plantea a implementación de un sistema de gestión de seguridad de la información basado en los requerimientos de la norma ISO/IEC 27001:2013 y la planeación de la implementación de controles de la ISO/IEC 27002:2013. La empresa solo tiene un oficial de seguridad informática y no cuenta con una estrategia de seguridad de la información. Se realiza toda la propuesta de implementación para sustentar la necesidad de implementar un SGSI a corto plazo.

(López Camacho & López Obando, 2014) Actualmente el mercado tecnológico se encuentra en una fase de globalización y modernización de alta competitividad en productos y servicios, lo que ha traído consigo una avalancha de dispositivos móviles cada vez más potentes y con mayores capacidades de almacenamiento, tanto en el mercado de los smartphones como de las tablets. En este momento, el personal de las organizaciones ha integrado el uso de estos dispositivos a sus actividades laborales, generando cambios y adaptaciones en las empresas a nivel de informática, procesos y talento humano. Una organización, desde su nivel de gobierno hasta las áreas operativas, debe adoptar medidas de seguridad para los dispositivos móviles. BYOD (Bring your Own Device), en español “Traiga su propio dispositivo”, consiste en la incorporación de dispositivos móviles personales al ambiente de trabajo para acceder a los sistemas de información corporativo tales como: bases de datos, información comercial, correos electrónicos, archivos y aplicaciones propias de la organización. A nivel de seguridad de la

información existe un vacío conceptual en lo referente a los dispositivos móviles, puesto que el estándar ISO 27002 no considera de manera explícita la regulación del uso de BYOD. Por lo anterior, y tomando como base la familia de estándares ISO 27002, en el presente trabajo se plantea un marco de referencia para la regulación del uso de BYOD en las organizaciones. Posteriormente se define un modelo para determinar el nivel de madurez de la organización con respecto al modelo propuesto, permitiendo identificar debilidades, fortalezas, además de establecer los puntos 11 críticos para el mejoramiento continuo de los procesos de seguridad referentes al uso de BYOD en la organización.

## 2.2 Marco conceptual

Las organizaciones desean proteger un activo primordial llamado información, implementan un Sistema de Gestión de la Seguridad de la información, en adelante SGSI, que asegura la información utilizada en los diferentes procesos del negocio donde es necesario demostrar que se ejercen normas y controles que ofrecen calidad a estos procesos, en este caso a continuación se definen de manera clara y sencilla los términos relacionados:

**Seguridad de la información:** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

**Activo:** Cualquier cosa que tenga valor para la empresa.

**Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**Estándares de seguridad:** Son productos, procedimientos y métricas aprobadas, que definen en detalle como las políticas de seguridad serán implementadas para un ambiente en particular, teniendo en cuenta las fortalezas y debilidades de las características de seguridad disponibles. Deben estar reflejadas en un documento que describe la implantación de una guía para un componente específico de hardware, software o infraestructura.

**Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos.

**Vulnerabilidad:** Debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

**Disponibilidad:** Es que las personas o procesos autorizados accedan a los activos de información cuando así lo requieran.

**Causa:** Son los medios, circunstancias y agentes que generan los riesgos.

**Control:** Es toda acción que tiende a minimizar los riesgos, significa analizar el desempeño de las operaciones, evidenciando posibles desviaciones frente al resultado esperado para la adopción de medidas preventivas. Los controles proporcionan un modelo operacional de seguridad razonable en el logro de los objetivos.

**Factores de riesgo:** Manifestaciones o características medibles u observables de un proceso que indican la presencia de Riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

**Probabilidad:** Una medida (expresada como porcentaje o razón) para estimar la posibilidad de que ocurra un incidente o evento. Contando con registros, puede estimarse a partir de su frecuencia histórica mediante modelos estadísticos de mayor o menor complejidad.

**Sistema:** Conjunto de cosas o partes coordinadas, ordenadamente relacionadas entre sí, que contribuyen a un determinado objetivo.

**Administración de riesgos:** Proceso de identificación, control o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

**Proceso para la gestión del riesgo:** Aplicación sistemática de las políticas, procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo.

**Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.



**Monitoreo:** Comprobar, supervisar, observar críticamente o registrar el progreso de una actividad, acción en forma sistemática para identificar cambios.

**Criterio del riesgo:** Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

### 2.3 Marco contextual

El Almacén Lubricentro Avenida, fue fundado hace 5 años, por Javier Ortiz Navarro y algunos de sus familiares, como una empresa dedicada la comercialización y distribución de lubricantes, aditivos y productos de limpieza para vehículos automotores, ubicado en la Avenida Francisco Fernández de contreras como sitio estratégico; las marcas que distribuye son reconocidas a nivel nacional e internacional, lo que le ha otorgado a la empresa reconocimiento por la calidad de sus productos.

En el año 2014 tienen la oportunidad de ampliar su infraestructura tomando en alquiler el local contiguo y comienzan a ofrecer en este mismo el servicio de lavado para todo tipo de vehículo y servicio de parqueo las 24 horas.

La Administración espera en el mediano plazo diversificar el portafolio de productos y servicios y lograr mayor participación en el mercado regional y nacional

## **MISION**

Lubricentro Avenida es un establecimiento de comercio distribuidor y comercializador de lubricantes, filtros, aditivos, refrigerantes y demás fluidos de alta calidad para toda clase de vehículos, maquinaria y equipos. Nuestro compromiso es buscar la satisfacción de nuestros clientes y la excelencia en el servicio, facilitándoles y proporcionando los mejores productos del mercado en un solo sitio, así como la asesoría y el acompañamiento que requieran nuestros clientes y usuarios, como lo expresa nuestro lema " **Un mundo de lubricantes a su servicio. No vendemos aceites, asesoramos en lubricación**". Creemos en el mejoramiento continuo y confiamos en nuestro recurso humano como eje principal del negocio.

## **VISION**

Nuestra visión es lograr para el año 2019 ser los líderes y convertirnos en la primera opción en lubricantes y servicio automotriz en la ciudad de Ocaña, además brindar el abastecimiento eficiente y oportuno de fluidos lubricantes, filtros, aditivos, refrigerantes y demás productos para el óptimo desempeño de su vehículo o maquinaria ya sea de servicio público o particular, proporcionando las mejores marcas; al mejor precio, calidad, servicio y asesoría en lubricación que nuestros competidores.

### **2.4 Marco Teórico**

(Collazos Balaguer) define la ISO y sus principios de gestión como una federación mundial de organismos nacionales de normalización alrededor de 160 países, trabajan a nivel de Comités Técnicos, tienen al menos 19,000 estándares publicados desde 1947 (creación), 1951 (publicación). Trabaja en función a 8 principios de gestión: Orientación al cliente, Liderazgo,

Participación del personal, Enfoque de procesos, Enfoque de sistemas de gestión, Mejora Continua, Enfoque de mejora continua, Relación mutuamente beneficiosa con el proveedor.

## HISTORIA NORMAS ISO/IEC 27001: 2013 E ISO/IEC 27002:2014

Según (Parra Casallas) la NORMA ISO/IEC 27001:2013 La ISO 27001 es la que especifica los requisitos necesarios para establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información.



**Figura 1.** *Historia ISO/IEC 27001:2013.*

**Nota Fuente:** <http://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/>

Su origen fue:

- La BS 7799-1, publicada en 1995: serie de mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Incluía recomendaciones que no daban opción a ningún tipo de certificación ni establecía la forma de conseguirla.
- La BS 7799-2, en 1998 (segunda parte de la BS 7799-1): establecía los requisitos a cumplir para tener un Sistema de Gestión de Seguridad de la Información certificable.

Ambas partes fueron revisadas en el año 1999 y en el año 2000 la Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799-1 que dio lugar a la

llamada ISO 17799. En este momento la norma no experimentó grandes cambios. En el año 2001 fue revisada de acuerdo a la línea de las normas ISO.

- Nueva versión de la BS 7799 en el año 2002: incluyó la acreditación de empresas por una entidad certificadora en Reino Unido y en otros países.
- Estándar ISO 27001 en el año 2005: modificación de la ISO 17799.
- Estándar ISO 27002:2005 en el año 2007: surge de renombrar la ISO 17799
- Nueva versión de la ISO 27001:2007
- ISO 27001:2007/1M: 2009: Esta norma es conocida en Chile como NCh-ISO27001, en España como UNE-ISO/IEC 27001:2007, en Colombia como NTC-ISO-IEC 27001, en Venezuela como Fondo norma ISO/IEC 27001, en Argentina como IRAM-ISO IEC 27001, en México como NMX-I-041/02-NYCE y en Uruguay como UNIT-ISO/IEC 27001.
- Nueva versión de la ISO 27001 en el año 2013: trae cambios en la estructura, en la evaluación y tratamiento de los riesgos.
- Nueva versión de la ISO 27002 en el año 2014: Se actualiza de acuerdo con los cambios de la norma ISO 27001:2013

(ISO 27000) ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001

contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en [www.iso.org](http://www.iso.org).

## 2.5 Marco legal

En Colombia se maneja una serie de leyes, normas y decretos en relación con la seguridad de la Información; para la implementación de un Sistema de Gestión de seguridad de la Información se debe dar cumplimiento a todas estas; en lo que se refiere específicamente a Seguridad de la Información, estas son las leyes vigentes. Información tomada según (Camelo, 2010):

### **Derechos de Autor**

Decisión 351 de la C.A.N.

Ley 23 de 1982

Decreto 1360 de 1989

Ley 44 de 1993

Decreto 460 de 1995

Decreto 162 de 1996

Ley 545 de 1999

Ley 565 de 2000

Ley 603 de 2000

Ley 719 de 2001

### **Propiedad Industrial**

Decisión 486 de la C.A.N.

Decreto 2591 de 2000

Ley 463 de 1998

Ley 170 de 1994

Ley 178 de 1994

### **Propiedad Intelectual**

Decisión 345 de la C.A.N.

Decisión 391 de la C.A.N.

Decisión 523 de la C.A.N.

### **Comercio Electrónico y Firmas Digitales**

Ley 527 de 1999

Decreto 1747 de 2000

Resolución 26930 de 2000

### **ACTUALIZACIÓN AGOSTO 2013**

**LEY 603 DE 2000**

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.

La Ley faculta a la DIAN para realizar verificaciones y enfatiza en la obligación de declarar en los informes de gestión el cumplimiento de las normas que protegen el software. Solicitarán a las empresas las licencias que demuestren la legalidad de los programas, las facturas de compra, la contabilización del intangible, equipos y demás dispositivos en los que se encuentra instalado el software. (COLOMBIA, 2013)

#### **LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 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.

Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se haya recogido sobre ellas.

En el TITULO VI VIGILANCIA DE LOS DESTINATARIOS DE LA LEY, Artículo 17. Función De Vigilancia. La Superintendencia de Industria y Comercio ejercerá la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales que se regula en la presente ley. (UIAF, 2008)

### **LEY 1273 DEL 5 DE ENERO DE 2009**

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, y las siguientes disposiciones: DE LOS ATENTADOS CONTRA LA CONFIDENCIALIDAD Acceso abusivo a un sistema informático, Obstaculización ilegítima de sistema informático o red de telecomunicación, Interceptación de datos informáticos, Daño Informático, Uso de software malicioso, Violación de datos personales, Suplantación de sitios web para capturar datos personales.

LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y DE LOS SISTEMAS INFORMÁTICOS hurto por medios informáticos y semejantes, Transferencia no consentida de activos. (BOGOTÁ S. G., 2009)

### **LEY 1341 DEL 30 DE JULIO DE 2009**

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. Su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en



relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.

### **LEY ESTATUTARIA 1581 DE 2012**

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.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Aspectos claves de la normatividad:

1. Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.
2. Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

3. Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.
4. Crea una especial protección a los datos de menores de edad.
5. Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.
6. Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.
7. Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.
8. Crea el Registro Nacional de Bases de Datos.
9. Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

### **DECRETO 1377 DE JUNIO 2013**

Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Precisó que el tratamiento de datos personales se debe formalizar mediante contrato suscrito entre el responsable y el encargado de tal actividad; y determina que el primero responde

por los daños causados a los titulares de los datos personales por el inadecuado tratamiento, esto es una apuesta a una nueva globalización corporativa. (Bogotá, 2013)

## **Capítulo 3. Diseño Metodológico**

### **3.1 Tipo de Investigación**

El tipo de investigación utilizado en el presente proyecto fue el cuantitativo, dado que a través de ésta se pudo mantener el control sobre factores contextuales que pudieron interferir en la recopilación de los datos necesarios, con el fin de reducir los posibles errores.

El método que se utilizó fue el descriptivo, porque se pudo realizar la descripción, registro, análisis e interpretación de las condiciones existentes en la empresa, para poder interpretar la información obtenida más allá de la simple recolección de datos.

### **3.2 Población**

Para este proyecto, el universo lo conforman todos los empleados de Lubricentro Avenida Ocaña, para un total de 14 personas.

### **3.3 Muestra**

De acuerdo con las áreas específicas relacionadas con la gestión de información de la empresa, se tomará como muestra los empleados de los siguientes cargos: Gerencia, Contabilidad, Secretaría y Ventas de la empresa Lubricentro Avenida para un total de (10) empleados en esas áreas.

### **3.4 Recolección de la Información**

La técnica e instrumento de recolección a emplear para la obtención de la información relacionada con el diagnóstico inicial para la propuesta de la guía de controles de seguridad de la información, de acuerdo como lo establece el estándar internacional ISO/IEC 27002:2013, son la entrevista y el cuestionario respectivamente. Los demás instrumentos se configuraron en listas de verificación y formatos de observación (Ver Apéndices).

## Capítulo 4. Resultados

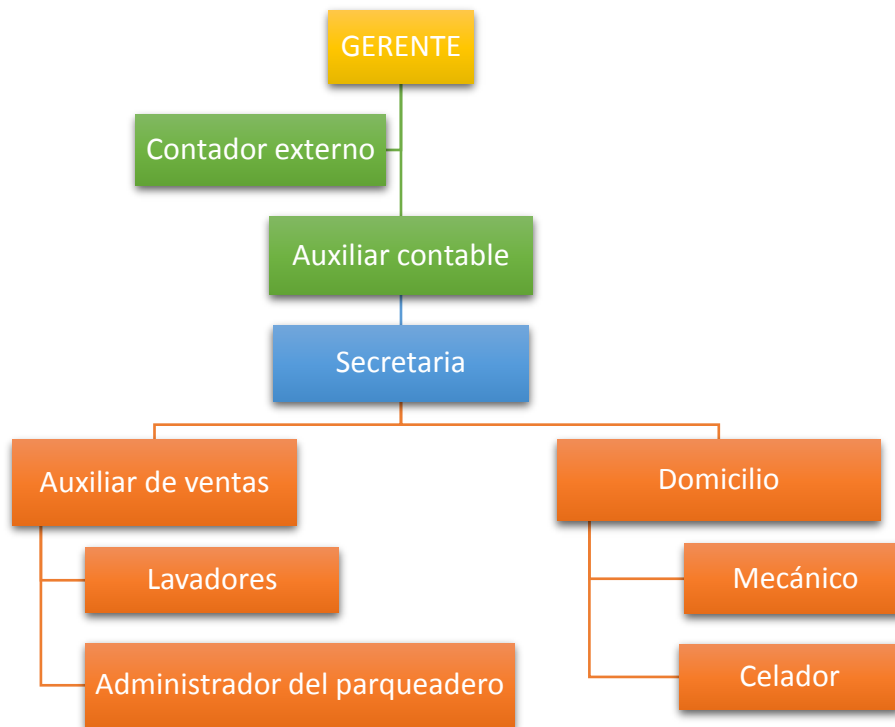
### 4.1 Diagnóstico de la seguridad de la información en Lubricentro Avenida Ocaña.

Con el fin de emitir un juicio objetivo en relación con el estado actual de la seguridad de la información en Lubricentro Avenida Ocaña, se hizo necesario definir las siguientes actividades:

**Caracterización de la Empresa.** Lubricentro Avenida Ocaña es un establecimiento de comercio distribuidor y comercializador de lubricantes, filtros, aditivos, refrigerantes y demás fluidos de alta calidad para toda clase de vehículos, maquinaria y equipos. Ofrece además asesoría y acompañamiento a sus clientes en lo que respecta a los suministros para su vehículo.

Lubricentro Avenida Ocaña, se encuentra ubicado en la Calle 7 # 30-23 Avenida Francisco Fernández de Contreras, en la ciudad de Ocaña, Norte de Santander. Además de los productos que ofrece, presta los servicios de lavado, engrase, mecánica rápida, parqueadero, venta de SOAT (seguro obligatorio).

La estructura orgánica de Lubricentro Avenida Ocaña, se muestra a continuación:



**Figura 2.** Estructura orgánica Lubricentro Avenida Ocaña.

**Nota Fuente:** Gerente Lubricentro Avenida Ocaña

En lo que respecta a la infraestructura tecnológica, Lubricentro Avenida Ocaña, posee ocho (8) equipos de cómputo utilizados para el procesamiento de la información contable, facturación y servicios de mantenimiento. Actualmente, se encuentra instalado una aplicación llamada VENTAS OSLI 2015, que genera los registros de las ventas, los cuales se constituyen en el suministro de datos para la administración contable de la empresa. Cabe resaltar que el paquete de contabilidad que se utiliza, es propiedad del contador, quien lo lleva instalado en su equipo portátil. Además, existe un formato en Microsoft Excel 2010 para registrar los mantenimientos que se realizan a cada uno de los vehículos a los que se ofrece los distintos servicios.

Los equipos de cómputo se administran de forma independiente, es decir, sólo comparten la conexión a Internet, pero no archivos u otros servicios.

**Definición de los objetivos de la auditoría.** El propósito del presente diagnóstico fue el de evaluar la existencia y eficiencia de controles de seguridad de la información en Lubricentro Avenida Ocaña, de acuerdo con los dominios contemplados en el estándar ISO/IEC 27002:2013.

**Alcances de la evaluación.** La evaluación cubrió los catorce dominios del estándar internacional ISO/IEC 27002:2013, haciendo una excepción en el *Dominio 14, Adquisición, desarrollo y mantenimiento de los sistemas de información*. Para este dominio, sólo fue posible evaluar el objetivo de control *Requisitos de seguridad de los sistemas de información*; los otros dos objetivos no se tuvieron en cuenta, ya que Lubricentro Avenida Ocaña, no lleva a cabo procesos de desarrollo de software.

Los dominios de la norma se relacionan a continuación:

**Tabla 1.**

***Dominio y objetivos de control ISO/IEC 27002:2013***

DOMINIO	OBJETIVOS DE CONTROL
<b>Dominio 5: Políticas de seguridad</b>	▪ Directrices de la Dirección en seguridad de la información
<b>Dominio 6: Aspectos organizativos de la seguridad de la información</b>	▪ Organización interna ▪ Dispositivos para movilidad y teletrabajo
<b>Dominio 7: Seguridad ligada a los recursos humanos</b>	▪ Antes de la contratación. ▪ Durante la contratación
<b>Gestión de activos</b>	▪ Cese o cambio de puesto de trabajo ▪ Responsabilidad sobre los activos



---

<b>Control de accesos</b>	<ul style="list-style-type: none"><li>▪ Clasificación de la información</li><li>▪ Manejo de los soportes de almacenamiento</li><li>▪ Requisitos de negocio para el control de accesos.</li><li>▪ Gestión de acceso de usuario</li><li>▪ Responsabilidades del usuario</li><li>▪ Control de acceso a sistemas y aplicaciones</li></ul>
<b>Cifrado</b>	<ul style="list-style-type: none"><li>▪ Controles criptográficos</li></ul>
<b>Seguridad física y ambiental</b>	<ul style="list-style-type: none"><li>▪ Áreas seguras</li><li>▪ Seguridad de los equipos</li><li>▪ Responsabilidades y procedimientos de operación.</li><li>▪ Protección contra código malicioso</li><li>▪ Copias de seguridad</li></ul>
<b>Seguridad en la operativa</b>	<ul style="list-style-type: none"><li>▪ Registro de actividad y supervisión</li><li>▪ Control del software en explotación</li><li>▪ Gestión de la vulnerabilidad técnica</li><li>▪ Consideraciones de las auditorías de los sistemas de información.</li></ul>
<b>Seguridad en las telecomunicaciones</b>	<ul style="list-style-type: none"><li>▪ Gestión de la seguridad en las redes.</li><li>▪ Intercambio de información con partes externas.</li></ul>
<b>Adquisición, desarrollo y mantenimiento de los sistemas de información.</b>	<ul style="list-style-type: none"><li>▪ Requisitos de seguridad de los sistemas de información</li></ul>
<b>Relaciones con suministradores</b>	<ul style="list-style-type: none"><li>▪ Seguridad de la información en las relaciones con suministradores.</li><li>▪ Gestión de la prestación del servicio por suministradores</li></ul>
<b>Gestión de incidentes en la seguridad de la información</b>	<ul style="list-style-type: none"><li>▪ Gestión de incidentes de seguridad de la información y mejoras</li></ul>
<b>Aspectos de seguridad de la información en la gestión de la continuidad del negocio.</b>	<ul style="list-style-type: none"><li>▪ Continuidad de la seguridad de la información</li><li>▪ Redundancias</li></ul>
<b>Cumplimiento</b>	<ul style="list-style-type: none"><li>▪ Cumplimiento de los requisitos legales y contractuales</li><li>▪ Revisiones de la seguridad de la información</li></ul>

---

**Nota.** La tabla muestra los dominios y objetivos de control ISO/IEC 27002:2013. **Nota Fuente.**

Autores del Proyecto

**Metodología de trabajo.** La evaluación realizada a Lubricentro Avenida Ocaña, tuvo en cuenta la ejecución de varias actividades como las que se describen a continuación:

- ***Estudio inicial del entorno.*** Para llevar a cabo esta actividad, fue necesario solicitar documentación a la empresa objeto de estudio, con el ánimo de identificar procesos, procedimientos, normatividad, directrices, entre otros, que tuvieran relación con la gestión de la seguridad de la información. La solicitud de la información se hizo mediante oficio dirigido a la gerencia de la empresa (Ver Anexo B). Tal solicitud no arrojó muy buenos resultados dado que Lubricentro Avenida Ocaña, carece de documentos formales para la estandarización de sus procesos, lo que dificultó las tareas de recolección de información, puesto que la misma tuvo que obtenerse por otras fuentes.

- ***Programación de las actividades.*** Con el objeto de formalizar las actividades para la realización de la auditoría, se diseñó un plan de trabajo, que incluyó los objetivos a alcanzar y las tareas específicas para cumplirlos. El formato del plan de trabajo, se detalla a continuación:

Tabla 2.

*Plan de Trabajo*

 <b>Universidad</b> Francisco de Paula Santander Ocaña - Colombia		
<b>PLAN DE TRABAJO</b>		<b>PT-01</b>
Empresa: <b>LUBRICENTRO AVENIDA OCAÑA</b>		Fecha de Inicio: __/__/__ Fecha de Finalización: __/__/__
Responsables Ejecución: <b>MARCELA TORCOROMA ÁLVAREZ ANGARITA - MTAA</b> <b>LUZ MERY DURÁN ALVERNIA - LMDA</b>		
<b>OBJETIVO GENERAL</b> Evaluar la existencia y eficiencia de controles de seguridad de la información en Lubricentro Avenida Ocaña, de acuerdo con los dominios contemplados en el estándar ISO/IEC 27002:2013		
<b>OBJETIVOS ESPECÍFICOS</b>		
1. Realizar una revisión de los controles de seguridad física, teniendo en cuenta el dominio 11 del estándar en mención.		
2. Evaluar la existencia y eficiencia de controles de seguridad lógica bajo los dominios 9, 10, 12 y 13.		
3. Evaluar la pertinencia de controles administrativos de la seguridad de la información de acuerdo con los dominios: 5, 6, 8, 15, 16, 17 y 18.		
<b>ALCANCES</b> La presente evaluación cubre todos los dominios del estándar ISO/IEC 27002:2013, en cuanto a requerimientos de seguridad de la información.		
<b>DESCRIPCIÓN DE TAREAS</b>		
ÍTEM	TAREA	REF. PT
1.1	Evaluación de los controles de acceso a las áreas seguras definidas por la organización.	<b>LV-01</b>
1.2	Verificación de controles para la protección física de los equipos de cómputo de Lubricentro Avenida Ocaña.	<b>LV-02</b>
2.1	Evaluación de los mecanismos existentes para el control de acceso a la información y a las aplicaciones utilizadas para la marcha del negocio, así como la existencia de controles criptográficos.	<b>EN-02</b>
2.2	Revisión de procedimientos y responsabilidades relacionados con la operatividad de los sistemas de información.	<b>LV-03</b>
3.1	Evaluación de controles relacionados con la organización de la seguridad de la información, así como la seguridad ligada al talento humano en Lubricentro Avenida Ocaña.	<b>EN-03</b>
3.2	Verificación de procedimientos implementados para la gestión de los activos de Lubricentro Avenida Ocaña.	<b>EN-04</b>
3.3	Evaluación de procedimientos para la gestión de los incidentes de seguridad y de la continuidad del negocio.	<b>EN-05</b>

**MARCAS UTILIZADAS EN EL PRESENTE DOCUMENTO****PT-01:** Programa de Trabajo.**LV 01-03:** Listas de Verificación No. 1, 2 y 3.**EN 01 -04:** Entrevistas No. 1, 2, 3 y 4.

**Nota.** La siguiente tabla contiene el plan de trabajo. Nota **Fuente** Autores del proyecto.

▪ **Diseño de herramientas.** El proceso de recolección de datos se llevó a cabo mediante entrevistas, listas de verificación, observación directa, entre otras, con el fin de poder obtener información confiable y útil para realizar el diagnóstico en cuanto a seguridad de la información se refiere en Lubricentro Avenida Ocaña (Ver Anexos C, D, E, F, G, H, I).

▪ **Ejecución de actividades.** Después de haber elaborado las herramientas de recolección, se dio inicio a la tarea de toma de datos, y a la formalización de las actividades planeadas. Es de anotar que gran parte de la información que se pretendía recoger no se obtuvo, debido a la carencia de procesos y procedimientos estandarizados que le dieran soporte a las actividades que se llevan a cabo en Lubricentro Avenida Ocaña.

▪ **Presentación de hallazgos.** Los resultados de la evaluación a la gestión de la seguridad de la información para Lubricentro Avenida Ocaña, se detallan a continuación, por cada uno de los dominios de los que trata la norma en mención.

**DOMINIO 5: Políticas de Seguridad de la Información.** En la actualidad, Lubricentro Avenida Ocaña, no cuenta con un documento de políticas de seguridad de la información, que direcciona y soporte los requerimientos de seguridad de sus activos informáticos. No hay documentación alguna que especifique los lineamientos en cuanto a la protección de la información sensible para la empresa.

**DOMINIO 6: Aspectos organizativos de la seguridad de la información.** Lubricentro Avenida Ocaña, carece de un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de su información más importante. Las labores de coordinación de la seguridad de la información no se encuentran definidas, puesto que ni siquiera en el organigrama de la empresa existe un área de sistemas que pueda asumir las tareas propias de la gestión de la seguridad informática y de la información. Así mismo, la empresa no cuenta con procedimientos que especifiquen cuándo y cuáles autoridades contactar, y cómo se debieran reportar los incidentes de seguridad de la información que se puedan presentar en un momento determinado.

**DOMINIO 7: Seguridad ligada a los Recursos Humanos.** La empresa Lubricentro Avenida Ocaña, no posee un área de Personal o Recursos Humanos dentro de su estructura organizacional y por lo tanto, no existen procedimientos para definir los roles y responsabilidades de la seguridad de la información que manejan los empleados y terceros y que se ajusten a las necesidades de protección de sus activos informáticos.

Esta situación pone de manifiesto que a la hora de realizar el reclutamiento y selección de personal, sobre todo, del que tiene que ver con el manejo de información confidencial, el gerente de Lubricentro hace la respectiva escogencia de sus nuevos empleados, ya sea por la revisión de su hoja de vida o porque éstos hayan sido recomendados por alguien de su entera confianza, sin hacer un estudio de sus antecedentes personales, profesionales y/o laborales.

Después de haber hecho una revisión de algunos de los contratos de trabajo, se pudo detectar, que en ninguna parte del documento aparece alguna cláusula de confidencialidad que indique la responsabilidad del empleado frente a la información que tendrá a su disposición, ni tampoco de las sanciones a que el incumplimiento de la misma diera lugar.

Cabe resaltar que los empleados del área administrativa manifiestan que son conscientes de la importancia de proteger la información que utilizan, a pesar de que hasta el momento no hayan recibido ningún entrenamiento al respecto.

**DOMINIO 8: *Gestión de Activos.*** Lubricentro Avenida Ocaña mantiene un inventario de los productos que vende, con el fin de controlar las entradas y salidas de los mismos, sin embargo, este inventario se lleva a cabo de forma manual y en muchos casos se han presentado inconsistencias o pérdidas de productos, sin que nadie en específico asuma responsabilidad alguna. De los demás activos de la empresa como muebles, enseres, equipos, dispositivos, software, licencias, documentos, entre otros, no hay registro alguno. La empresa en mención no posee procedimientos definidos que permitan administrar de forma adecuada y segura, la información de sus activos tangibles e intangibles.

**DOMINIO 9: *Control de accesos.*** En la actualidad, Lubricentro Avenida Ocaña no cuenta con una política de control de acceso a la información y a las aplicaciones que manejan datos confidenciales de las operaciones del negocio; es cierto que controlan el acceso a las aplicaciones mediante sistemas de logueo (usuario y contraseña), pero de acuerdo con la entrevista aplicada a los empleados del área administrativa, se pudo evidenciar que éstas claves de acceso, no se

actualizan periódicamente; que los privilegios no se establecen adecuadamente, porque los usuarios tienen acceso a servicios y aplicaciones sin ninguna restricción; que en la mayoría de los casos se comparten las claves de usuario, entre otras situaciones que pueden poner en riesgo la integridad, confidencialidad y disponibilidad de la información. Cabe anotar, que la persona que apoya la administración del sistema, acude ocasionalmente a la empresa cuando se produce una solicitud por parte de algún usuario.

**DOMINIO 10: *Cifrado*.** En cuanto a la gestión de la seguridad de la información, Lubricentro Avenida Ocaña, no cuenta con controles definidos y documentados para la asignación de privilegios de acceso a las aplicaciones.

**DOMINIO 11: *Seguridad física y ambiental*.** La evaluación de la seguridad física en las instalaciones de Lubricentro Avenida Ocaña, permitió concluir que en lo relacionado con el subdominio de áreas seguras, no cuenta con perímetros de seguridad bien definidos, para el área administrativa, ni la de atención al cliente. Cualquier persona que tenga interés alguno en la información en pantalla o en la contenida en documentos, puede tener acceso a ella sin mucha dificultad, puesto que no hay muchas restricciones, además de que algunas veces, estas áreas quedan desatendidas por un tiempo considerable.

En lo que respecta a las cámaras de vigilancia, cuenta con dos cámaras de vigilancia que están ubicadas en el área administrativa y en Atención al Cliente. Sin embargo, los registros de las mismas, no se revisan con frecuencia.

Por otra parte, analizando los aspectos del subdominio de seguridad de los equipos, Lubricentro Avenida Ocaña, tiene instalados dos extintores vigentes, uno ubicado en el área de mantenimiento (lavado, engrase,...) y otro, en el área administrativa; sin embargo no cuenta con detectores de humo, ni alarma contra incendios; no cuenta con una plana eléctrica como fuente alternativa de corriente, para darle continuidad a sus servicios, en especial a los relacionados con el manejo de la información; debido al número de equipos en el área administrativa, existe aire acondicionado para su refrigeración; el cableado de datos de los equipos de cómputo se encuentra en mal estado y en el suelo, situación que pone en riesgo la disponibilidad de la información; tampoco existen prohibiciones visibles sobre comer, beber o fumar en el área donde se encuentran los equipos.

**DOMINIO 12: Seguridad en la Operativa.** De acuerdo con la revisión de los equipos, se pudo constatar que aunque solo ocho (8) equipos tienen instalado un software antimalware, éste no se encuentra actualizado, hecho que representa una vulnerabilidad para una amenaza de virus o cualquier código malicioso que pueda afectar la integridad, disponibilidad y confidencialidad de su información sensible.

Para efectos de respaldos de datos, la secretaria que maneja la información contable de la empresa, manifiesta que realiza backup`s cada quince (15) días y lo hace en un disco duro externo; éste queda guardado en una gaveta de un archivador de madera, en donde además guardan los registros físicos de las diversas operaciones que se manejan. El resto de la información como registros de mantenimientos realizados, no se respaldan.



**DOMINIO 13: *Seguridad en las telecomunicaciones.*** No existe ningún tipo de restricción en cuanto a la seguridad de la información que es consultada, descargada o subida a Internet; la empresa no tiene protocolos para establecer los límites en cuanto a las aplicaciones que se utilizan como es el caso de las redes sociales; así mismo la descarga de juegos u otras aplicaciones específicas, se realiza sin ningún tipo de prohibición.

**DOMINIO 14: *Adquisición, desarrollo y mantenimiento de sistemas de información.*** Es de resaltar que por el objeto social de la empresa en cuestión, ésta no lleva a cabo procesos de desarrollo y mantenimiento de sistemas y por lo tanto, sólo se evaluó el dominio relacionado con los requisitos de seguridad de los sistemas de información. En lo relacionado con la adquisición de hardware y software, ésta se realiza mediante contratación directa con uno o dos proveedores de la ciudad. Este procedimiento de adquisición no obedece a ningún estudio previo y planificado de ampliación o mejoramiento de su infraestructura tecnológica, sino que se hace, de acuerdo con la necesidad presente.

**DOMINIO 15: *Relaciones con suministradores.*** Para establecer acuerdos con terceros, Lubricentro Avenida Ocaña, establece contratos para el suministro de sus productos y de otros servicios que ofrece; una vez puesto el producto en la empresa, se hace la respectiva verificación y se firma el recibido a satisfacción; no obstante, dentro del documento del contrato, no aparece estipulada una cláusula de confidencialidad con el proveedor, para establecer los límites en cuanto al uso de información que comparten.

**DOMINIO 16: *Gestión de incidentes en la seguridad de la información.*** A pesar de que en Lubricentro Avenida Ocaña no se han presentado situaciones de riesgo para la información, no cuenta con protocolos definidos, ni mucho menos documentados para realizar el respectivo reporte de los incidentes de seguridad que puedan poner en riesgo la estabilidad y/o continuidad de los servicios que ofrece la empresa y de la información que utiliza o produce para el cumplimiento de su misión.

**DOMINIO 17: *Aspectos de seguridad de la información en la gestión de la continuidad del negocio.*** En la actualidad, la empresa objeto de estudio, carece de un plan de continuidad del negocio y de plan de contingencias que especifique las actividades necesarias que deben llevarse a cabo para restablecer sus servicios, ante la presencia de un ataque a la información o a cualquier activo de la empresa.

Desafortunadamente, Lubricentro Avenida Ocaña desconoce los procedimientos para realizar la planificación y documentación de dichos planes de contingencias, además de las capacitaciones que los empleados deben recibir para hacer frente a este tipo de situaciones.

**DOMINIO 18: *Cumplimiento.*** Lubricentro Avenida Ocaña, carece de procedimientos formales para establecer los lineamientos de seguridad de su información y en conversaciones con el Gerente, éste justifica tal situación en el desconocimiento que sobre el tema posee. Así mismo, mediante solicitud de documentación se confirmó la inexistencia de estándares para la protección de sus activos, al igual que mecanismos de control para evitar la pérdida o modificación fraudulenta de su información.

## 4.2 Identificación de riesgos de seguridad de la información para Lubricentro Avenida

### Ocaña.

Desde hace varias décadas la información ha pasado de ser un producto del desarrollo de las actividades de las organizaciones a ser un insumo de alto valor, fundamental para el cumplimiento de los objetivos y subsistencia de las mismas. En muchas de estas organizaciones, y con el objeto de brindar eficiencia y agilizar la administración, los procesos incorporan la utilización de sistemas automatizados de procesamiento de información.

El auge en el rol que ha tomado la información, sin embargo, no exime a las organizaciones de una serie de peligros, que se han visto incrementados por las nuevas amenazas surgidas del uso de tecnologías de la información y las comunicaciones. De esta manera, toda organización se encuentra constantemente expuesta a una serie de riesgos mientras que resulta imposible establecer un entorno totalmente seguro.

En un seminario de Taller Riesgo vs. Seguridad de la Información de la (Universidad Nacional de Lujan ), la gestión de riesgos se presenta entonces como una actividad clave para el resguardo de los activos de información de una organización y en consecuencia protege la capacidad de cumplir sus principales objetivos. Es un proceso constante que permite a la administración balancear los costos operacionales y económicos causados por la interrupción de las actividades y la pérdida de activos, con los costos de las medidas de protección a aplicar sobre los sistemas de información y los datos que dan soporte al funcionamiento de la

organización, reduciendo los riesgos que presentan los activos de información a niveles aceptables para la misma. El proceso de gestión de riesgos involucra cuatro actividades cíclicas:

- La identificación de activos y los riesgos a los que están expuestos.
- El análisis de los riesgos identificados para cada activo.
- La selección e implantación de controles que reduzcan los riesgos.
- El seguimiento, medición y mejora de las medidas implementadas.

Para el caso particular de Lubricentro Avenida Ocaña, mediante distintos instrumentos de recolección de información, se identificaron los siguientes activos de información como etapa inicial del proceso de gestión de riesgos y se les dio una valoración con respecto a la magnitud del daño que sufriría el activo, en caso de materialización de alguna amenaza.

La escala de valoración de la magnitud del daño es la siguiente:

- **I - Insignificante:** No causa ningún tipo de impacto o daño a la organización.
- **B - Bajo:** El daño causado no perjudica a ningún componente de la organización.
- **M - Medio:** Provoca la desarticulación de un componente de la organización.
- **A - Alto:** En el corto plazo desarticula a la organización.

A continuación se presenta el listado de activos con su correspondiente valoración:

Tabla 3.

*Identificación de activos*

 <b>Universidad</b> Francisco de Paula Santander Ocaña - Colombia		VALORACIÓN MAGNITUD DEL DAÑO			
ACTIVOS DE INFORMACIÓN					
Ítem	DESCRIPCIÓN DEL ACTIVO	I	B	M	A
1.	Documentación de la empresa: contratos, facturación, libros de contabilidad.				X
2.	Información de contactos			X	
3.	Correos electrónicos				X
4.	Información contable				X
5.	Información de inventarios				X
6.	Respaldos de información contable				X
7.	Equipos de cómputo		X		
8.	Software de contabilidad		X		
9.	Impresoras	X			
10.	Dispositivos de almacenamiento (USB, discos duros,...)				X
11.	Personal administrativo y ejecutivo				X
12.	Inventarios (mercancías)			X	

**Nota.** Tabla que identifica los riesgos de Lubricentro Avenida Ocaña. **Nota Fuente:** Autoras del Proyecto.


Una vez identificados los activos, se realizó una lista de las amenazas más importantes por tener una alta repercusión en el riesgo que pueden representar para la empresa y se valoró la probabilidad de ocurrencia de la misma, con la siguiente escala:

- **I - Insignificante:** No existen condiciones que impliquen riesgo.
- **B - Baja:** Existen condiciones que hacen muy lejana la posibilidad del ataque
- **M - Mediana:** Existen condiciones que hacen poco probable un ataque en el corto plazo pero que no son suficientes para evitarlo en el largo plazo
- **A – Alta:** La realización del ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque.

La valoración de la probabilidad de ocurrencia de las amenazas se presenta en la siguiente tabla:

Tabla 4.

*Identificación de amenazas.*

 <b>Universidad</b> Francisco de Paula Santander Ocaña - Colombia		VALORACIÓN PROBABILIDAD DE OCURRENCIA DE LA AMENAZA			
IDENTIFICACIÓN DE AMENAZAS		I	B	M	A
Ítem	DESCRIPCIÓN DE LA AMENAZA				
1.	Ataques externos e internos				X
2.	Código malicioso				X
3.	Ingeniería social		X		
4.	Robo de mercancía			X	
5.	Robo de información				X
6.	Fraude			X	
7.	Fallas de corriente			X	
8.	Aplicaciones espía			X	
9.	Descarga e instalación no controlada de software			X	
10.	Phising		X		
11.	Fallas en los equipos			X	
12.	Incendios		X		
13.	Inundaciones		X		

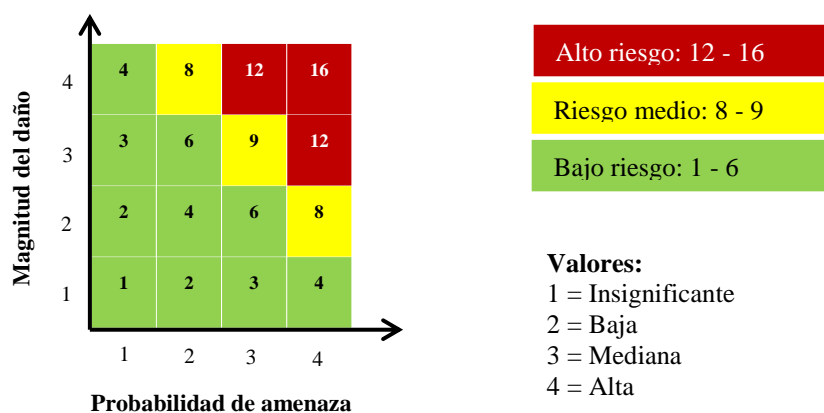
**Nota.** Tabla que identifica las amenazas de Lubricentro Avenida Ocaña. **Nota Fuente:** Autoras del Proyecto.

A partir de los datos anteriores, se utilizó una matriz que permitió mostrar el nivel de riesgo de la empresa en lo relacionado con los activos informáticos, para el caso en el que se materializara una amenaza o se produjera un ataque.

Para realizar la matriz y medir el riesgo se utilizó la siguiente fórmula, que ha sido muy utilizada para evaluar riesgos informáticos:

$$\text{Riesgo} = \text{Probabilidad de Amenaza} \times \text{Magnitud de Daño}$$

Cabe resaltar que se tuvieron en cuenta las variables anteriormente descritas en las tablas 3 y 4 (magnitud del daño sobre el activo y probabilidad de ocurrencia de la amenaza). Para la presentación del resultado (riesgo) se usó una gráfica de dos dimensiones, en la cual, el eje X, representó la **probabilidad de amenaza** y el eje Y, la **magnitud de daño sobre el activo**. La probabilidad de amenaza y magnitud del daño, pueden tomar valores entre **Insignificante** (1) y **Alta** (4), así:



**Figura 3.** Valoración del riesgo.

**Nota Fuente:** Autoras del Proyecto

La siguiente matriz muestra claramente el nivel de riesgo a nivel de seguridad informática y de información en el que se encuentra Lubricentro Avenida Ocaña:

**Tabla 5.**

*Matriz de riesgos informáticos para Lubricentro Avenida Ocaña.*

VALORACIÓN DE ACTIVOS		PROBABILIDAD DE OCURRENCIA DE LA AMENAZA												
ACTIVOS DE INFORMACIÓN	MAGNITUD DEL DAÑO	LISTADO DE AMENAZAS												
		Ataques externos e internos	Código malicioso	Ing. social	Robo de mercancía	Robo de inform.	Fraude	Fallas de corriente	Aplic. espía	Inst. no controlada de software	Phising	Fallas en los equipos	Incendios	Inundación
		4	4	2	3	4	3	3	3	3	2	3	2	2
Docum. (contratos, facturación, libros contables)	4	16	16	8	12	16	12	12	12	12	8	12	8	8
Información de contactos	3	12	12	6	9	12	9	9	9	9	6	9	6	6
Correos electrónicos	4	16	16	8	12	16	12	12	12	12	8	12	8	8
Información contable	4	16	16	8	12	16	12	12	12	12	8	12	8	8
Información de inventarios	4	16	16	8	12	16	12	12	12	12	8	12	8	8
Respaldos de información	4	16	16	8	12	16	12	12	12	12	8	12	8	8
Equipos de cómputo	2	8	8	4	6	8	6	6	6	6	4	6	4	4
Software de contabilidad	2	8	8	4	6	8	6	6	6	6	4	6	4	4
Impresoras	1	4	4	2	3	4	3	3	3	3	2	3	2	2
Dispositivos de almacenam. (USB, discos duros,...)	4	16	16	8	12	16	12	12	12	12	8	12	8	8
Personal admin. y ejecutivo	4	16	16	8	12	16	12	12	12	12	8	12	8	8



Inventarios (mercancías)	3	12	12	6	9	12	9	9	9	9	6	9	6	6
-----------------------------	---	----	----	---	---	----	---	---	---	---	---	---	---	---

**Nota Fuente:** Autores del Proyecto

La tabla anterior evidencia el alto riesgo en el que se encuentran algunos activos de la empresa, debido a las vulnerabilidades existentes y a la alta probabilidad de ocurrencia de algunas de las amenazas, situación que puede generar un impacto negativo en el cumplimiento de la misión organizacional.

La gran debilidad se centra en la ausencia de procedimientos formales para proteger la información; así como de normas y políticas institucionales que estén orientadas a la seguridad no solo de los activos institucionales, sino también de los datos personales tanto de empleados como de directivos.

La ausencia de controles estandarizados, pone en riesgo la confidencialidad, disponibilidad e integridad de la información de la que dispone Lubricentro Avenida Ocaña para el cumplimiento de su objeto social.

Finalmente como complemento de la evaluación anterior, se diseñó un cuadro en el que se pudieron relacionar tanto los activos, como las amenazas potenciales teniendo en cuenta los niveles de vulnerabilidad que éstos activos presentaban en el momento de la auditoría. A partir de estos datos, se establecieron los riesgos potenciales que pueden causar una parálisis parcial o total en el desarrollo de las actividades comerciales para Lubricentro Avenida Ocaña y se establecieron las recomendaciones pertinentes para la mitigación de dichos riesgos.

La información que se presenta a continuación está organizada de la siguiente manera:

- Ítem: Número para la secuencia
- Vulnerabilidad: Debilidad presente en el activo de información
- Amenaza: Elemento que puede atentar contra la seguridad de un activo
- Descripción del riesgo: Detalle de la situación de alarma para la empresa
- Acciones: Estrategias para mitigar o reducir el impacto de los riesgos

**Tabla 6.**

*Establecimiento de riesgo 1 de seguridad de la información para Lubricentro Avenida Ocaña.*

<b>VULNERABILIDAD</b>		
Falta de políticas de seguridad de la información.		
<b>AMENAZAS</b>	<b>DESCRIPCIÓN DEL RIESGO</b>	<b>ACCIONES</b>
<ul style="list-style-type: none"> <li>▪ Ataques externos</li> <li>▪ Ataques internos</li> <li>▪ Código malicioso</li> <li>▪ Ingeniería social</li> </ul>	<ul style="list-style-type: none"> <li>▪ Pérdida parcial o total de la información.</li> <li>▪ Modificación no autorizada de datos sensibles.</li> </ul> Pérdida de disponibilidad, integridad y confidencialidad de la información.	<ul style="list-style-type: none"> <li>▪ Diseño e implantación de procedimientos definidos y documentados para la protección de la información.</li> </ul> Capacitación en seguridad informática.

**Nota.** Tabla que establece el riesgo 1 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto.

**Tabla 7.**

*Establecimiento de riesgo 2 de seguridad de la información para Lubricentro Avenida Ocaña.*

---

**VULNERABILIDAD**

---

Inexistencia de un marco regulatorio para la organización de la seguridad de la información.

---

AMENAZAS	DESCRIPCIÓN DEL RIESGO	ACCIONES
<ul style="list-style-type: none"> <li>▪ Incidentes de seguridad</li> </ul>	<ul style="list-style-type: none"> <li>▪ Pérdida de información.</li> <li>▪ Suspensión parcial de las actividades comerciales.</li> <li>▪ Pérdida de imagen corporativa</li> </ul>	<ul style="list-style-type: none"> <li>▪ Incluir dentro del organigrama, un área para la gestión de la seguridad de la información.</li> <li>▪ Establecimiento de políticas de seguridad.</li> </ul>

---

**Nota.** Tabla que establece el riesgo 2 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto.

**Tabla 8.**

*Establecimiento de riesgo 3 de seguridad de la información para Lubricentro Avenida Ocaña.*

---

**VULNERABILIDAD**

---

Inexistencia de procedimientos para el proceso de reclutamiento y selección del personal

---

AMENAZAS	DESCRIPCIÓN DEL RIESGO	ACCIONES
<ul style="list-style-type: none"> <li>▪ Ataques internos</li> <li>▪ Ataques externos</li> </ul>	<ul style="list-style-type: none"> <li>▪ Pérdida de la confidencialidad e integridad de la información.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Establecimiento de políticas para definir la seguridad ligada a los recursos humanos, de acuerdo con el estándar ISO 27002:2013.</li> </ul>

---

**Nota.** Tabla que establece el riesgo 3 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto.

**Tabla 9.**

*Establecimiento de riesgo 4 de seguridad de la información para Lubricentro Avenida Ocaña.*

<b>VULNERABILIDAD</b>		
Falta de lineamientos para la administración de los activos.		
<b>AMENAZAS</b>	<b>DESCRIPCIÓN DEL RIESGO</b>	<b>ACCIONES</b>
<ul style="list-style-type: none"> <li>▪ Robo</li> <li>▪ Fraude</li> </ul>	<ul style="list-style-type: none"> <li>▪ Inconsistencia en los registros de inventarios.</li> <li>▪ Pérdida de activos</li> </ul>	<ul style="list-style-type: none"> <li>▪ Realizar un inventario de todos los activos de la empresa.</li> <li>▪ Establecer protocolos para la clasificación y etiquetado de activos.</li> <li>▪ Asignar un responsable para la gestión de activos</li> </ul>

**Nota.** Tabla que establece el riesgo 4 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto.

**Tabla 10.**

*Establecimiento de riesgo 5 de seguridad de la información para Lubricentro Avenida Ocaña.*

<b>VULNERABILIDAD</b>		
Las claves de acceso de los usuarios no se actualizan periódicamente.		
<b>AMENAZAS</b>	<b>DESCRIPCIÓN DEL RIESGO</b>	<b>ACCIONES</b>
<ul style="list-style-type: none"> <li>▪ Ataques internos</li> <li>▪ Ataques externos</li> </ul>	<ul style="list-style-type: none"> <li>▪ Pérdida de integridad, disponibilidad y confidencialidad de los datos.</li> <li>▪ Acciones fraudulentas para extracción o modificación de información.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Definición de procedimientos para establecer restricciones en el acceso a los datos.</li> </ul>

**Nota.** Tabla que establece el riesgo 5 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto.

**Tabla 11.**

*Establecimiento de riesgo 6 de seguridad de la información para Lubricentro Avenida Ocaña.*

<b>VULNERABILIDAD</b>		
La infraestructura tecnológica de la empresa no cuenta con los requerimientos técnicos necesarios (normatividad cableado, ups, sistemas alternativos de corriente).		
<b>AMENAZAS</b>	<b>DESCRIPCIÓN DEL RIESGO</b>	<b>ACCIONES</b>
<ul style="list-style-type: none"> <li>▪ Sobrecargas eléctricas</li> <li>▪ Fallas de corriente</li> </ul>	<ul style="list-style-type: none"> <li>▪ Daño en los equipos de cómputo.</li> <li>▪ Pérdida de información.</li> <li>▪ Retraso en la gestión contable y financiera.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Asignación presupuestal para el mejoramiento de la infraestructura tecnológica.</li> </ul>

**Nota.** Tabla que establece el riesgo 6 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto.

**Tabla 12.**

*Establecimiento de riesgo 7 de seguridad de la información para Lubricentro Avenida Ocaña.*

<b>VULNERABILIDAD</b>		
Inexistencia de perímetros de seguridad bien definidos.		
<b>AMENAZAS</b>	<b>DESCRIPCIÓN DEL RIESGO</b>	<b>ACCIONES</b>
<ul style="list-style-type: none"> <li>▪ Hurto físico y electrónico</li> </ul>	<ul style="list-style-type: none"> <li>▪ Pérdida de información.</li> <li>▪ Alteración de datos</li> <li>▪ Pérdida de activos</li> <li>▪ Acceso a información confidencial</li> </ul>	<ul style="list-style-type: none"> <li>▪ Establecer perímetros en las áreas que se consideren críticas por el tipo de información que se maneja.</li> <li>▪ Establecer una política de escritorio y pantalla limpias para equipos desatendidos.</li> <li>▪ Implementar mecanismos de cierre de sesión automática para evitar el acceso a datos sensibles.</li> </ul>

**Nota.** Tabla que establece el riesgo 7 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto

**Tabla 13.**

*Establecimiento de riesgo 8 de seguridad de la información para Lubricentro Avenida Ocaña.*

<b>VULNERABILIDAD</b>		
Las aplicaciones antimalware no se encuentran actualizadas.		
<b>AMENAZAS</b>	<b>DESCRIPCIÓN DEL RIESGO</b>	<b>ACCIONES</b>
<ul style="list-style-type: none"> <li>▪ Virus informático</li> <li>▪ Aplicaciones espía</li> </ul>	<ul style="list-style-type: none"> <li>▪ Daños en la información</li> <li>▪ Daños en los equipos</li> <li>▪ Pérdida de datos</li> </ul>	<ul style="list-style-type: none"> <li>▪ Adquisición de licencias de software antimalware.</li> <li>Definir lineamientos para evitar utilizar medios extraíbles sin la revisión previa adecuada.</li> </ul>

**Nota.** Tabla que establece el riesgo 8 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto

**Tabla 14.**

*Establecimiento de riesgo 9 de seguridad de la información para Lubricentro Avenida Ocaña.*

<b>VULNERABILIDAD</b>		
Los respaldos de datos se realizan cada quince días en un disco duro externo.		
<b>AMENAZAS</b>	<b>DESCRIPCIÓN DEL RIESGO</b>	<b>ACCIONES</b>
<ul style="list-style-type: none"> <li>▪ Problemas de corriente eléctrica.</li> <li>▪ Inundaciones.</li> <li>▪ Fallas en los equipos</li> <li>▪ Incendios</li> </ul>	<ul style="list-style-type: none"> <li>▪ Pérdida parcial o total de la información.</li> <li>▪ Sanciones por parte de entes reguladores (DIAN)</li> <li>▪ Pérdida de imagen corporativa</li> </ul>	<ul style="list-style-type: none"> <li>▪ Aumentar la frecuencia de realización de copias de respaldo.</li> <li>▪ Establecer procedimientos para realizar pruebas en la restauración de dichos datos.</li> <li>▪ Definir el almacenamiento de las copias de respaldo físicas, en un lugar externo a la empresa y que cuente con las medidas de seguridad física y lógica.</li> <li>▪ Contratar un servicio externo de salvaguarda de las copias de respaldo.</li> </ul>

**Nota.** Tabla que establece el riesgo 9 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto

**Tabla 15.**

*Establecimiento de riesgo 10 de seguridad de la información para Lubricentro Avenida Ocaña.*

<b>VULNERABILIDAD</b>		
Acceso ilimitado a redes sociales y a descarga e instalación de aplicaciones.		
<b>AMENAZAS</b>	<b>DESCRIPCIÓN DEL RIESGO</b>	<b>ACCIONES</b>
<ul style="list-style-type: none"> <li>▪ Código malicioso</li> <li>▪ Ataques externos</li> <li>▪ Phising</li> <li>▪ Fraudes</li> </ul>	<ul style="list-style-type: none"> <li>▪ Robo de identidad</li> <li>▪ Alteración no autorizada de datos</li> <li>▪ Daños en los equipos</li> </ul>	<ul style="list-style-type: none"> <li>▪ En el documento de políticas de seguridad, establecer procedimientos para el uso responsable de Internet.</li> </ul>

**Nota.** Tabla que establece el riesgo 10 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto

**Tabla 16.**

*Establecimiento de riesgo 11 de seguridad de la información para Lubricentro Avenida Ocaña.*

<b>VULNERABILIDAD</b>		
No existen acuerdos de confidencialidad con terceros (clientes, proveedores, etc.)		
<b>AMENAZAS</b>	<b>DESCRIPCIÓN DEL RIESGO</b>	<b>ACCIONES</b>
<ul style="list-style-type: none"> <li>▪ Fraudes</li> </ul>	<ul style="list-style-type: none"> <li>▪ Pérdida de confidencialidad de la información</li> </ul>	<ul style="list-style-type: none"> <li>▪ Definir una política de seguridad de la información para proveedores.</li> <li>▪ Establecer mecanismos de supervisión y revisión de los servicios prestados por terceros.</li> </ul>

**Nota.** Tabla que establece el riesgo 11 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto



**Tabla 17.**

*Establecimiento de riesgo 12 de seguridad de la información para Lubricentro Avenida Ocaña.*

<b>VULNERABILIDAD</b>		
No existen acuerdos de confidencialidad con terceros (clientes, proveedores, etc.)		
<b>AMENAZAS</b>	<b>DESCRIPCIÓN DEL RIESGO</b>	<b>ACCIONES</b>
<ul style="list-style-type: none"> <li>▪ No existe un protocolo para el reporte de eventos en la seguridad de la información.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Fallas eléctricas</li> <li>▪ Falla en los equipos</li> <li>▪ Fallas en el software</li> <li>▪ Ataques internos</li> <li>▪ Ataques externos</li> <li>▪ Incendios</li> </ul>	<ul style="list-style-type: none"> <li>▪ Suspensión parcial o total de las actividades comerciales.</li> <li>▪ Pérdidas humanas</li> <li>▪ Daños en los equipos</li> <li>▪ Robo de información</li> <li>▪ Pérdida de imagen corporativa</li> </ul>

**Nota.** Tabla que establece el riesgo 12 de seguridad de la información para Lubricentro Avenida Ocaña.

**Nota Fuente:** Autoras del Proyecto

#### **4.3 Guía de controles de gestión de seguridad de la información para Lubricentro Avenida Ocaña, de acuerdo con el estándar ISO/IEC 27002:2013.**

A continuación se presenta un cuadro con la especificación de los controles que deberían ser implementados para la adopción de un sistema de gestión de seguridad de la información, de acuerdo como lo establece la norma en mención.

Se recomienda a la Gerencia de Lubricentro Avenida Ocaña asumir un compromiso para el diseño e implementación de buenas prácticas en la seguridad de la información, a fin de que se genere un ambiente de seguridad y se establezcan lineamientos y procedimientos concretos para la reducción de los riesgos potenciales a los que se encuentra expuesta la empresa y de esta manera se pueda minimizar el impacto que los mismos pueden generar sobre sus activos o sobre la imagen corporativa de la misma.

La guía de controles que se presenta a continuación, consta de los siguientes ítems: Objetivo de control, Controles y Justificación.

**Tabla 18.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 5*

<b>GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013</b>
<p><b>A5. POLÍTICAS DE SEGURIDAD</b></p> <p><b>OBJETIVO DE CONTROL</b></p> <p>5.1 DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD DE LA INFORMACIÓN</p> <p><b>CONTROLES</b></p> <p>5.1.1 Conjunto de políticas para la seguridad de la información</p> <p>5.1.2 Revisión de las políticas para la seguridad de la información.</p> <p><b>JUSTIFICACIÓN</b></p> <p>Es necesario establecer una política de seguridad de la información que defina los lineamientos para el aseguramiento de sus activos.</p> <p>Se debe generar conciencia sobre los riesgos a los que están expuestos sus activos más valiosos, así como los controles necesarios para reducir el impacto de los mismos.</p> <p>La revisión de las políticas de seguridad de la información debería tener en cuenta los resultados de las revisiones por parte del nivel directivo de Lubricentro Avenida Ocaña.</p> <p>De igual forma, se sugiere diseñar, implementar y comunicar a los empleados de la empresa los lineamientos que deben estar contemplados en el documento de Políticas de Seguridad de la Información, para que se adopte una cultura de la protección de la información y de los demás activos de información de la empresa.</p>
<p><b>Nota.</b> Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 5.</p> <p><b>Nota Fuente.</b> Autores del proyecto</p>

**Tabla 19.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 6*

---

<b>GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013</b>
<b>A6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN</b>
<b>OBJETIVO DE CONTROL</b>
<b>6.1 ORGANIZACIÓN INTERNA</b>
<b>CONTROLES</b>
6.1.1 Asignación de responsabilidades para la segur. de la información
6.1.2 Segregación de tareas
6.1.3 Contacto con las autoridades
6.1.4 Contacto con grupos de interés especial
<b>JUSTIFICACIÓN</b>
La Gerencia de la empresa mediante su política de seguridad de la información debe establecer el compromiso, organización y asignación de responsabilidades para su cumplimiento, de igual forma velar por mantener protegida su información mediante la revisión del sistema de gestión de seguridad de la información.
Definir un marco regulatorio que garantice el cumplimiento de los controles de seguridad contemplados en la política de seguridad de la información. Igualmente, se deben definir claramente las responsabilidades para la protección de los activos individuales y llevar a cabo los procesos de seguridad específicos, definiendo y documentando claramente los niveles de autorización.
<b>Nota.</b> Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 6.
<b>Nota Fuente.</b> Autores del proyecto

---

**Tabla 20.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 7*

---

**GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO  
CON EL ESTÁNDAR ISO/IEC 27002:2013**

---

**A7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**

**OBJETIVO DE CONTROL**

7.1 Antes de la contratación

7.2 Durante la contratación

7.3 Cese o cambio de puesto de trabajo

**CONTROLES**

7.1.1 Investigación de antecedentes

7.1.2 Términos y condiciones de contratación

7.2.1 Responsabilidades de gestión.

7.2.2 Concienciación, educación y capacitación en seguridad. de la información

7.2.3 Proceso disciplinario

7.3.1 Cese o cambio de puesto de trabajo

**JUSTIFICACIÓN**

Se recomienda establecer un acuerdo de confidencialidad para cada uno de los empleados de Lubricentro Avenida Ocaña en el momento de su contratación o cuando haya algún cambio de puesto de trabajo, que contemple los requerimientos para proteger la información, utilizando términos legalmente ejecutables y especificando entre otros aspectos, el tipo de información que debe protegerse, la duración esperada del acuerdo, las responsabilidades para usar información confidencial, así como para evitar su divulgación, condiciones específicas de terminación del contrato laboral y las sanciones impuestas para los casos de incumplimiento de dicho acuerdo.

De igual forma, es necesario capacitar al personal permanentemente en temas de seguridad de la información según sea pertinente para sus funciones laborales.

---

**Nota.** Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 7.

**Nota Fuente.** Autores del proyecto

**Tabla 21.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 8*

---

**GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO  
CON EL ESTÁNDAR ISO/IEC 27002:2013**

---

**A8. GESTIÓN DE ACTIVOS****OBJETIVO DE CONTROL**

- 8.1 Responsabilidad sobre los activos
- 8.2 Clasificación de la información.
- 8.3 Manejo de los soportes de almacenamiento

**CONTROLES**

- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 8.1.3 Uso aceptable de los activos.
- 8.1.4 Devolución de activos.
- 8.2.1 Directrices de clasificación
- 8.2.2 Etiquetado y manipulado de la información
- 8.2.3 Manipulación de activos
- 8.3.1 Gestión de soportes extraíbles.
- 8.3.2 Eliminación de soportes
- 8.3.3 Soportes físicos en tránsito.

**JUSTIFICACIÓN**

Lubricentro Avenida Ocala, en el proceso de implementación y mantenimiento del sistema de gestión de seguridad de la información debe realizar un inventario de todos sus activos de información, e identificar y documentar los propietarios de estos, realizar un inventario de los más importantes, y también garantizar el uso adecuado de los mismos a través de reglas documentadas e implementadas.

De igual manera, se recomienda establecer una clasificación específica para la empresa, que indique los niveles de protección de acuerdo con la importancia de los mismos y el valor comercial que representan para la Institución, así como documentar e implementar reglas para el uso aceptable y seguro de los activos de información.

---

**Nota.** Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 8.

**Nota Fuente.** Autores del proyecto

**Tabla 22.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 9*

---

**GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO  
CON EL ESTÁNDAR ISO/IEC 27002:2013**

---

**A9. CONTROL DE ACCESOS****OBJETIVO DE CONTROL**

- 9.1 Requisitos de negocio para el control de accesos
- 9.2 Gestión de acceso de usuario
- 9.3 Responsabilidades del usuario
- 9.4 Control de acceso a sistemas y aplicaciones

**CONTROLES**

- 9.1.1 Política de control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2.1 Gestión de altas/bajas en el registro de usuarios
- 9.2.2 Gestión de los derechos de acceso asignados a usuarios
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales
- 9.2.4 Gestión de información confidencial de autenticación de usuarios.
- 9.2.5 Revisión de los derechos de acceso de los usuarios
- 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3.1 Uso de información confidencial para la autenticación.
- 9.4.1 Restricción del acceso a la información
- 9.4.2 Procedimientos seguros de inicio de sesión.
- 9.4.3 Gestión de contraseñas de usuario.
- 9.4.4 Uso de herramientas de administración de sistemas.
- 9.4.5 Control de acceso al código fuente de los programas.

**JUSTIFICACIÓN**

Se hace necesario establecer un procedimiento formal para la gestión de los derechos de acceso de los usuarios de los sistemas de información y de las aplicaciones, donde se entregue un documento a cada usuario indicando la información relacionada con el acceso (usuario y contraseña) y los requerimientos de protección de la información que tendrá bajo su responsabilidad.

---

**Nota.** Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 9.

**Nota Fuente.** Autores del proyecto

**Tabla 23.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 10*

---

**GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO  
CON EL ESTÁNDAR ISO/IEC 27002:2013**

---

**A10. CIFRADO****OBJETIVO DE CONTROL**

10.1 Controles criptográficos

**CONTROLES**

10.1.1 Política de uso de los controles criptográficos.

10.1.2 Gestión de claves.

**JUSTIFICACIÓN**

La empresa debe establecer controles criptográficos para los sistemas de información que se utilizan, con el objetivo de garantizar la confidencialidad e integridad de la información.

Se deben establecer protocolos y documentar los procedimientos para la gestión de los derechos y niveles de acceso a los sistemas de información.

---

**Nota.** Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 10.

**Nota Fuente.** Autores del proyecto

**Tabla 24.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 11*

---

<b>GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013</b>
<b>A11. SEGURIDAD FÍSICA Y AMBIENTAL</b>
<b>OBJETIVO DE CONTROL</b>
11.1 Áreas seguras
11.2 Seguridad de los equipos
<b>CONTROLES</b>
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada
11.1.3 Seguridad de oficinas, despachos y recursos
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2.1 Emplazamiento y protección de equipos
11.2.2 Instalaciones de suministro
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
<b>JUSTIFICACIÓN</b>
La empresa debe diseñar e implementar un Plan de Continuidad del Negocio y un documento de Políticas de Seguridad, que contemple los riesgos de seguridad física. Para esto, se sugiere:
Instalar alarmas contra incendios, detectores de humo y salidas de emergencia, para minimizar el impacto que puede provocar la presencia de una catástrofe ambiental.
Construir o adecuar un espacio fuera de las instalaciones de la IPS, con las medidas de seguridad física necesarias para almacenar las copias de respaldo, o en su defecto, contratar los servicios de un DataCenter.
Es necesario establecer controles que permitan reducir la ocurrencia de eventos que puedan generar la pérdida parcial o total de los datos, daño, robo o interrupción de las actividades comerciales de la empresa.
Así mismo, se recomienda establecer protocolos documentados para el retiro de los equipos fuera de las instalaciones, y para la reutilización o retirada segura de los mismos.
<b>Nota.</b> Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 11.
<b>Nota Fuente.</b> Autores del proyecto

---



**Tabla 25.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 12*

<b>GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013</b>
<b>A12. SEGURIDAD EN LA OPERATIVA</b>
<b>OBJETIVO DE CONTROL</b>
12.1 Responsabilidades y procedimientos de operación
12.2 Protección contra código malicioso
12.3 Copias de seguridad
12.4 Registro de actividad y supervisión
12.5 Control del software en explotación
12.6 Gestión de la vulnerabilidad técnica
12.7 consideraciones de las auditorías de los sistemas de información.
<b>CONTROLES</b>
12.1.1 Documentación de procedimientos de operación
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades
12.1.4 Separación de entornos de desarrollo, prueba y producción
12.2.1 Controles contra el código malicioso
12.3.1 Copias de seguridad de la información
12.4.1 Registro y gestión de eventos de actividad
12.4.2 Protección de los registros de información
12.4.3 Registros de actividad del administrador y operador del sistema
12.4.4 Sincronización de relojes.
12.5.1 Instalación del software en sistemas en producción
12.6.1 Gestión de las vulnerabilidades técnicas
12.6.2 Restricciones en la instalación de software
12.7.1 Controles de auditoría de los sistemas de información
<b>JUSTIFICACIÓN</b>
Este objetivo de control no aplica para Lubricentro Avenida Ocaña, ya que no tiene dentro de su objeto social, la producción y mantenimiento de software y/o aplicaciones.
Es importante establecer controles de seguridad que permitan la prevención, detección y corrección de la acción de códigos maliciosos así como también procedimientos de sensibilización a usuarios. Diseñar e implementar una política de respaldo que contenga los procedimientos para la realización de backup's y su debida restauración; así mismo, que contemple las acciones para definir el nivel necesario de respaldo de la información y la frecuencia de dicho procedimiento, de acuerdo con sus requerimientos comerciales. Se recomienda establecer controles de seguridad definidos, documentados, implementados, socializados y evaluados, que permitan la detección oportuna de actividades de procesamiento de información no autorizada y herramientas para investigaciones futuras de incidentes de seguridad de la información.
Es importante establecer controles de seguridad para garantizar la protección y correcta operación de los sistemas Y aplicaciones. De igual forma, se debe restringir la posibilidad de descarga e instalación de programas. Es necesario establecer controles de seguridad para garantizar la reducción de los riesgos derivados de las vulnerabilidades técnicas o de cualquier otro incidente voluntario o involuntario que pueda generar una suspensión de las actividades comerciales de la empresa.
Se debe mantener un registro de auditoría de todos los procedimientos realizados en las distintas aplicaciones instaladas.
<b>Nota.</b> Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 12.
<b>Nota Fuente.</b> Autores del proyecto

**Tabla 26.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 13*

---

<b>GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013</b>
<b>A13. SEGURIDAD EN LAS TELECOMUNICACIONES</b>
<b>OBJETIVO DE CONTROL</b>
13.1 Gestión de la seguridad en las redes
13.2 Intercambio de información con partes externas
<b>CONTROLES</b>
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red
13.1.3 Segregación de redes.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto
<b>JUSTIFICACIÓN</b>
Este objetivo de control no aplica puesto que Lubricentro Avenida Ocaña no tiene implementada ninguna red de datos. Hasta el momento, el procesamiento de la información se hace de manera independiente, en cada equipo de trabajo.
<b>Nota.</b> Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 13.
<b>Nota Fuente.</b> Autores del proyecto

---

**Tabla 27.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 14*

---

<b>GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013</b>
<b>A14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORM.</b>
<b>OBJETIVO DE CONTROL</b>
14.1 Requisitos de seguridad de los sistema de información
<b>CONTROLES</b>
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas
14.1.3 Protección de las transacciones por redes telemáticas
<b>JUSTIFICACIÓN</b>
Se recomienda que para los contratos de adquisición de software, se consideren los siguientes puntos:
Contratos de licencias, propiedad de códigos, derechos de propiedad intelectual; certificación de la calidad y exactitud del trabajo llevado a cabo; contratos de depósito en custodia en el evento de la falla de una tercera persona; requerimientos contractuales para la funcionalidad de calidad y seguridad del código; prueba antes de la instalación para detectar códigos maliciosos.

---

**Nota.** Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 14.

**Nota Fuente.** Autores del proyecto

**Tabla 28.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 15*

---

<b>GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013</b>
<b>A15. RELACIONES CON SUMINISTRADORES</b>
<b>OBJETIVO DE CONTROL</b>
15.1 Seguridad de la información en las relaciones con suministradores
15.2 Gestión de la prestación del servicio por suministradores
<b>CONTROLES</b>
15.1.1 Política de seguridad de la información para suministradores
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros
<b>JUSTIFICACIÓN</b>
Establecer formalmente protocolos para la prestación de servicios ofrecidos por terceros, que contemple entre otras cosas, el tratamiento del riesgo al proporcionar información confidencial, controles para garantizar el cumplimiento de los acuerdos y procedimientos para la gestión del cambio en dichos servicios.

---

**Nota.** Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 15.

**Nota Fuente.** Autores del proyecto

**Tabla 29.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 16*

---

**GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO  
CON EL ESTÁNDAR ISO/IEC 27002:2013**

---

**A16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**

**OBJETIVO DE CONTROL**

16.1 Gestión de incidentes de seguridad de la información y mejoras

**CONTROLES**

16.1.1 Responsabilidades y procedimientos.  
 16.1.2 Notificación de los eventos de seguridad de la información.  
 16.1.3 Notificación de puntos débiles de la seguridad.  
 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.  
 16.1.5 Respuesta a los incidentes de seguridad  
 16.1.6 Aprendizaje de los incidentes de seguridad de la información.  
 16.1.7 Recopilación de evidencias.

**JUSTIFICACIÓN**

Se recomienda establecer un procedimiento formal para el reporte de eventos de seguridad, así como el establecimiento de canales seguros para el reporte de los mismos.

Además, procedimientos para dar respuesta oportuna a dichos incidentes, asignando responsables.

Se recomienda entrenar a los usuarios de los sistemas de información y de aquellos que tengan activos de información a su cargo, sobre las diversas actividades de identificación y reporte de eventos de seguridad.

---

**Nota.** Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 16.

**Nota Fuente.** Autores del proyecto

**Tabla 30.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 17*

---

**GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO  
CON EL ESTÁNDAR ISO/IEC 27002:2013**

---

**A17. ASPECTOS DE SEGURIDAD DE LA INF. EN LA GESTIÓN DE LA CONTIN. NEGOCIO.**

**OBJETIVO DE CONTROL**

17.1 Continuidad de la seguridad de la información  
 17.2 Redundancias

**CONTROLES**

17.1.1 Planificación de la continuidad de la seguridad de la información.  
 17.1.2 Implantación de la continuidad de la seguridad de la información.  
 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.  
 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

**JUSTIFICACIÓN**

Se recomienda implementar un proceso de gestión de la continuidad del negocio, para minimizar el impacto en caso de pérdida parcial o total de sus funciones de operación, provocada por eventos no intencionados como desastres naturales, accidentes, fallas en los equipos o cualquier otro incidente cometido de forma deliberada.

---

---

Para llevar a cabo este cometido, se requiere entre otras cosas, la realización permanente de análisis y evaluación de riesgos, que permitan identificar amenazas y vulnerabilidades en los elementos de información y calcular el impacto que la materialización de las mismas pueda generar para el desarrollo de sus actividades comerciales.

---

**Nota.** Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 17.

**Nota Fuente.** Autores del proyecto

### **Tabla 31.**

*Guía de controles de seguridad de la información para Lubricentro Avenida Ocaña. Dominio 18*

---

#### **GUÍA DE CONTROLES DE SEGURIDAD PARA LUBRICENTRO AVENIDA OCAÑA DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27002:2013**

---

#### **A18. CUMPLIMIENTO**

##### **OBJETIVO DE CONTROL**

- 18.1 Cumplimiento de los requisitos legales y contractuales
- 18.2 Revisiones de la seguridad de la información

##### **CONTROLES**

- 18.1.1 Identificación de la legislación aplicable
- 18.1.2 Derechos de propiedad intelectual (DPI)
- 18.1.3 Protección de los registros de la organización
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.
- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento de las políticas y normas de seguridad.
- 18.2.3 Comprobación del cumplimiento.

##### **JUSTIFICACIÓN**

Se sugiere definir, documentar y actualizar todos los requerimientos legales, reguladores y contractuales y el enfoque de la empresa para satisfacer esos requerimientos.

De igual forma se recomienda, que para efecto de revisión y publicación de procedimientos relacionados con sistemas de información, arquitecturas de hardware y software, se cuente con la asesoría de un experto, para que el resultado de dicha evaluación pueda ser lo más objetivo posible.

---

**Nota.** Tabla que contiene la guía de controles de seguridad para Lubricentro Avenida Ocaña del Dominio 18.

**Nota Fuente.** Autores del proyecto

## Conclusiones

La presente investigación relacionada con el diseño de una guía de controles de seguridad de la información para Lubricentro Avenida Ocaña, de acuerdo con el Estándar ISO/IEC 27002:2013, permitió concluir lo siguiente:

La elaboración del diagnóstico se constituyó en una herramienta valiosa para determinar la situación actual de la empresa objeto de estudio, en lo relacionado con la gestión de la seguridad de su información. Para ello fue necesario, recurrir a distintos instrumentos que facilitaran la recolección de la información, dado que la empresa carece de documentación y procedimientos formales para establecer mecanismos de protección de sus activos.

La situación relacionada con la gestión de la seguridad de la información en Lubricentro Avenida Ocaña, no debe verse como un hecho aislado, sino como un problema que requiere atención prioritaria.

Por otra parte, para establecer los riesgos potenciales a los que se expone la empresa, se hizo uso de los datos arrojados por los instrumentos de recolección y se identificaron las vulnerabilidades, las amenazas, los riesgos y las distintas acciones que se pueden implantar para superar dichos problemas.

Finalmente, el trabajo concluyó con el diseño de un cuadro que contiene los criterios de seguridad que deben ser aplicados por cada uno de los dominios y objetivos de control de los que habla el estándar ISO/IEC 27002:2013, para la adopción de buenas prácticas en seguridad de la información.

## Recomendaciones

Para garantizar un adecuado Sistema de Gestión de la Seguridad de la Información, es necesario que la Gerencia de Lubricentro Avenida Ocaña, adquiera el compromiso de diseñar, implementar y evaluar de forma periódica las políticas y procedimientos formales para garantizar que la información que utiliza o que produce, se encuentra debidamente protegida y de esta manera, contribuya con el logro de su misión y visión organizacional.

A partir del diagnóstico obtenido, producto de la aplicación de herramientas de recolección de datos, en lo referente a la gestión de la seguridad de la información, de acuerdo con el estándar internacional ISO/IEC 27002:2013, se establecen las siguientes recomendaciones:

Establecer una política de seguridad de la información que defina los lineamientos específicos para la adecuada protección de la información y de los demás activos de la empresa. Así mismo, establecer procedimientos claros, definidos y documentados que faciliten la implementación de dichas políticas.

Definir un marco regulatorio que garantice el cumplimiento de los controles de seguridad contemplados en la política de seguridad de la información. Igualmente, se deben definir claramente las responsabilidades para la protección de los activos individuales y llevar a cabo los procesos de seguridad específicos, definiendo y documentando claramente los niveles de autorización.



Implementar el proceso de gestión de la continuidad del negocio para minimizar el impacto sobre la empresa y la recuperación de la pérdida parcial o total de los activos de información o de los servicios ofrecidos por la misma.

Implementar una política de respaldos de información que contenga los procedimientos definidos para la realización de backup's y su debida restauración; así mismo, que contemple las acciones para definir el nivel necesario de respaldo de la información y la frecuencia de dicho procedimiento, de acuerdo con sus requerimientos comerciales.

Establecer formalmente protocolos para la prestación de servicios ofrecidos por terceros, que contemple entre otras cosas, el tratamiento del riesgo al proporcionar información confidencial.

Establecer un procedimiento formal para el reporte de eventos de seguridad, así como el establecimiento de canales seguros para el reporte de los mismos.

Finalmente, capacitar de forma permanente a cada uno de los empleados de la empresa en buenas prácticas de seguridad de la información, de tal forma que se genere una cultura de seguridad, que redunde en beneficios para la empresa y la satisfacción de sus clientes.

## Referencias

- Bogotá, S. G. (5 de ENERO de 2009). *DIARIO OFICIAL*. Obtenido de <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>
- Bogotá, S. G. (27 de 06 de 2013). *RÉGIMEN LEGAL DE BOGOTÁ*. Obtenido de <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646>
- Camelo, L. (2010). *Seguridad de la Información en Colombia*. Obtenido de <http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html>
- Collazos Balaguer, M. (s.f.). Obtenido de [File:///C:/Users/Ufso/Downloads/Presentacion\\_Manuel\\_Collazos\\_-\\_1.Pdf](File:///C:/Users/Ufso/Downloads/Presentacion_Manuel_Collazos_-_1.Pdf)
- Colombia, D. D. (31 de DICIEMBRE de 2013). *DOCUMENTOS DIAN*. Obtenido de [http://www.dian.gov.co/descargas/EscritosComunicados/2013/260\\_Comunicado\\_de\\_prensa\\_31122013.pdf](http://www.dian.gov.co/descargas/EscritosComunicados/2013/260_Comunicado_de_prensa_31122013.pdf)
- Consultores, B. (S.F.). *Bsc Consultores*. Obtenido de <http://www.bsconsultores.cl/>
- Doria Corcho, A. F. (2015). *Diseño De Un Sistema De Gestión De Seguridad De La Información Mediante La Aplicación De La Norma Internacional Iso/Iec 27001:2013 En La Oficina De Sistemas De Información Y Telecomunicaciones De La Universidad De Córdoba, Montería*.
- El portal de ISO 27002 en Español. (s.f.). *El portal de ISO 27002 en Español*. Obtenido de [http://www.iso27000.es/download/doc\\_iso27000\\_all.pdf](http://www.iso27000.es/download/doc_iso27000_all.pdf)

Iscala Tobito, N. A., Meléndez Buitrago, S. M., & Pabón Sánchez, M. Y. (2014). *Diseño De Un Protocolo De Seguridad De La Informacion Del Area Financiera De La Secretaria De Educación Departamental De Norte De Santander*. Ocaña.

ISO 27000. (s.f.). Obtenido de [http://www.iso27000.es/download/doc\\_iso27000\\_all.pdf](http://www.iso27000.es/download/doc_iso27000_all.pdf)

López Camacho, R. A., & López Obando, R. (2014). *Diseño de un Marco de Referencia para regular el uso BYOD en organizaciones bajo el estandar ISO 27002*. Santiago de Cali.

Molina Rincón, E. L., Rodriguez Alvarez, O. H., Sanchez Delgado, Y., & Vergel Nuñez, J. A. (2014). *Guia para la seguridad basada en la norma ISO/IEC 27002, para la dependencia División de Sistemas de la Universidad Francisco de Paula Santander Ocaña*. Ocaña.

Parra Alvernia, H., Contreras Navarro, J., Díaz Pacheco, D. Y., & López Ovalle, E. J. (2014). *DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR "EMCAR"*. Ocaña.

Parra Casallas, J. (s.f.). Obtenido de <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43114/6/jparracasaTFM0715memoria.pdf>

Pulgarín Gómez, R. (2014). *Elaboración De Un Plan De Implementación De La Iso/Iec 27001:2013, Master interuniversitario de seguridad de las tecnologías de la información de las comunicaciones (UOC-UAB-URV)*. España.


UIAF. (31 de DICIEMBRE de 2008). *unidad de inteligencia financiera y económica*. Obtenido de <https://www.uiaf.gov.co/?idcategoria=20630>

Universidad Nacional de Lujan . (s.f.). *Material adicional del Seminario Taller Riesgo vs. Seguridad de la Información*. Obtenido de

[http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material\\_taller\\_gestion\\_de\\_riesgo.pdf](http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf)

# Apéndices

**Apéndice A.** Instrumento para el diagnóstico inicial en materia de seguridad de la información en el Lubricentro Avenida Ocaña.

 <b>Universidad</b> Francisco de Paula Santander Ocaña - Colombia	
<b>ENTREVISTA INICIAL</b>	
<b>PT. EN-01</b>	
Entrevistado: Gerente Lubricentro Avenida	
Objetivo: Identificar las medidas de protección de la información en Lubricentro Avenida.	
ÍTEM	PREGUNTA
1.	¿Cuál es la misión o el propósito fundamental de Lubricentro Avenida?
2.	¿Cuántas personas laboran en la empresa?
3.	¿Cuál considera que es la información más importante para la empresa?
4.	¿Quién es el encargado de administrar dicha información?
5.	¿Quiénes tienen acceso a esa información?
6.	¿Existen medidas que eviten el acceso no autorizado a dicha información?
7.	¿Existen limitaciones desde el punto de vista físico para evitar el acceso a las áreas restringidas de la empresa?
8.	¿La empresa tiene implementado algún sistema de información para administrar los datos producto de sus actividades?
9.	Si la pregunta anterior es afirmativa, ¿existe algún mecanismo para controlar el acceso al mismo?
10.	¿Se realiza copias de respaldo de la información que genera el sistema?
11.	¿Cada cuánto realizan estas copias?
12.	¿Dónde quedan almacenadas estas copias?
13.	¿Los activos de la empresa están debidamente inventariados?
14.	En cuanto a la contratación de los empleados, ¿se tiene estipulado cuáles son sus funciones y el nivel de responsabilidad frente a la información que manejan?
15.	¿Existen procedimientos documentados que establezcan las acciones inmediatas, en caso de que se presente algún siniestro y que pueda afectar la operatividad de la empresa?

**ENTREVISTADO**

Gerente Lubricentro Avenida Ocaña

**AUDITORA**

Marcela T. Álvarez Angarita

**Apéndice B.** Solicitud documentación para la ejecución de la auditoría.

Ocaña, Julio 21 de 2016

Señor

**JAVIER ORTIZ NAVARRO**

Gerente Lubricentro Avenida Ocaña

L. C.

Cordial saludo.

Respetuosamente nos dirigimos a usted con el objeto de solicitar algunos documentos necesarios para llevar a cabo la auditoría informática, acordada con usted, hace unas semanas.

Los documentos son los siguientes:

- Historia de Lubricentro Avenida Ocaña
- Filosofía institucional (misión, visión, objetivos, ...)
- Manual de funciones y procedimientos
- Plan de contingencias
- Información de la red de datos (si existe)
- Manual de usuario de las aplicaciones instaladas
- Manual de políticas de seguridad de la información
- Inventarios de hardware y software y otros activos.
- Procedimientos de copias de respaldo.
- Plan de mantenimiento de equipos
- Plan de capacitaciones

Agradecemos su atención y estamos informándole de nuevos requerimientos.

De usted,

**MARCELA T. ÁLVAREZ ANGARITA**  
Estudiante Esp. Auditoría de Sistemas

**LUZ MERY DURÁN ALVERNIA**  
Estudiante Esp. Auditoría de Sistemas

**Apéndice C.** Lista de verificación controles de acceso a áreas seguras.


 <b>Universidad</b> Francisco de Paula Santander Ocaña - Colombia					
<b>LISTA DE VERIFICACIÓN</b>					<b>PT. LV-01</b>
<b>Empresa:</b> LUBRICENTRO AVENIDA OCAÑA				Fecha de Elaboración: __/__/__ Fecha de Ejecución: __/__/__	
<b>Objetivo:</b> Evaluar los controles de acceso a las áreas seguras definidas por la organización.					
No.	ACTIVIDAD	SI	NO	OBSERVACIONES	AUDITOR
1.	Perímetro de seguridad en áreas sensibles				<b>M.T.A.A.</b>
2.	Área de recepción o servicio al cliente				
3.	Personal encargado servicio al cliente				
4.	Cámara de vigilancia área servicio al cliente				
5.	Cámara de vigilancia área administrativa				
6.	Cámara de vigilancia área de mantenimiento				
7.	Control para el acceso al área administrativa				
8.	Control de acceso al área de caja				
<b>MARCAS UTILIZADAS EN EL PRESENTE DOCUMENTO</b> <b>LV-01:</b> Lista de Verificación 1 <b>M.T.A.A.:</b> Marcela Torcoroma Álvarez Angarita – Responsable Auditoría					



**Apéndice D.** Lista de verificación controles para la protección física de los equipos de cómputo.

 <b>Universidad</b> Francisco de Paula Santander Ocaña - Colombia					
<b>LISTA DE VERIFICACIÓN</b>					<b>PT. LV-02</b>
<b>Empresa: LUBRICENTRO AVENIDA OCAÑA</b>				Fecha de Elaboración: __/__/__ Fecha de Ejecución: __/__/__	
<b>Objetivo:</b> Verificar los controles existentes para la protección física de los equipos de cómputo de Lubricentro Avenida Ocaña.					
No.	ACTIVIDAD	SI	NO	OBSERVACIONES	AUDITOR
1.	Ubicación adecuada para la protección de los equipos de cómputo.				<b>M.T.A.A.</b>
2.	Aire acondicionado para la refrigeración de los equipos de cómputo.				
3.	Conexiones eléctricas				
4.	Conexiones de datos				
5.	Dispositivo de suministro de energía ininterrumpido (UPS)				
6.	Fuente alternativa de corriente (planta eléctrica u otro dispositivo)				
7.	Salidas de emergencia				
8.	Protección del cableado eléctrico				
9.	Protección del cableado de datos				
10.	Aislamiento de fuentes electromagnéticas				
11.	Mantenimiento de equipos				
12.	Controles para la protección de los equipos fuera del puesto de trabajo				
13.	Controles para la baja de los equipos de cómputo				
14.	Alarmas contra incendios				
15.	Extintores				
16.	Detectores de humo				
17.	Prohibiciones formales sobre fumar y/o consumir alimentos en las áreas sensibles				
<b>MARCAS UTILIZADAS EN EL PRESENTE DOCUMENTO</b> <b>LV-02:</b> Lista de Verificación 2 <b>M.T.A.A.:</b> Marcela Torcoroma Álvarez Angarita – Responsable Auditoría					


**Apéndice E.** Entrevista evaluación mecanismos para el control de acceso a la información.

 <b>Universidad</b> Francisco de Paula Santander Ocaña - Colombia		
<b>ENTREVISTA</b>		<b>PT. EN-02</b>
<b>Empresa: LUBRICENTRO AVENIDA OCAÑA</b> <b>Entrevistado: Secretaria</b>		Fecha de Elaboración: __/__/__ Fecha de Ejecución: __/__/__
<b>Objetivo:</b> Evaluar los mecanismos existentes para el control de acceso a la información y a las aplicaciones utilizadas para la marcha del negocio, así como la existencia de controles criptográficos.		
No.	PREGUNTA / RESPUESTA	AUDITOR
1.	¿De qué manera restringe el acceso de los usuarios al equipo y a las aplicaciones?	<b>L.M.D.A.</b>
R.		
2.	¿Quién otorga los permisos de acceso a las aplicaciones?	
R.		
3.	¿Los permisos otorgados a los usuarios, son documentados adecuadamente?	
R.		
4.	¿Los derechos de acceso de los usuarios, son revisados periódicamente?	
R.		
5.	¿Cada cuánto se cambia las claves de acceso a las aplicaciones?	
R.		
6.	¿Quién realiza estas modificaciones?	
R.		
7.	¿Se ha capacitado a los usuarios en buenas prácticas de seguridad en lo que respecta al uso de claves secretas?	
R.		
8.	¿Qué tipo de restricciones existe para la descarga e instalación de aplicaciones desde Internet?	
R.		
9.	¿Qué aplicaciones se encuentran instaladas para evitar la infección por virus?	
R.		
10.	¿Se realizan copias de respaldo de la información? ¿Cada cuánto? ¿Qué tipo de información?	
R.		
<b>MARCAS UTILIZADAS EN EL PRESENTE DOCUMENTO</b> <b>EN-02:</b> Entrevista 2 <b>L.M.D.A.:</b> Luz Mery Durán Alvernia – Responsable Auditoría		

**Apéndice F.** Lista de verificación controles para la protección física de los equipos de cómputo.

 <b>Universidad</b> Francisco de Paula Santander Ocaña - Colombia					
<b>LISTA DE VERIFICACIÓN</b>					<b>PT. LV-03</b>
<b>Empresa: LUBRICENTRO AVENIDA OCAÑA</b>				Fecha de Elaboración: __/__/__ Fecha de Ejecución: __/__/__	
<b>Objetivo:</b> Revisar los procedimientos y responsabilidades relacionados con la operatividad de los sistemas de información.					
No.	ACTIVIDAD	SI	NO	OBSERVACIONES	AUDITOR
1.	Documentación procedimientos de operación de las aplicaciones				<b>M.T.A.A.</b>
2.	Controles contra código malicioso				
3.	Copias de seguridad				
4.	Restricciones en la descarga de software				
5.	Restricciones en la instalación de software				
6.	Restricciones en el acceso a redes sociales				
7.	Gestión de las fallas técnicas en aplicaciones				
<b>MARCAS UTILIZADAS EN EL PRESENTE DOCUMENTO</b> <b>LV-03:</b> Lista de Verificación 3 <b>M.T.A.A.:</b> Marcela Torcoroma Álvarez Angarita – Responsable Auditoría					


**Apéndice G.** Entrevista evaluación controles organización de la seguridad de la información.

 <b>Universidad</b> Francisco de Paula Santander Ocaña - Colombia		
<b>ENTREVISTA</b>		<b>PT. EN-03</b>
<b>Empresa: LUBRICENTRO AVENIDA OCAÑA</b> <b>Entrevistado: Gerente</b>		Fecha de Elaboración: __/__/__ Fecha de Ejecución: __/__/__
Objetivo: Evaluar los controles relacionados con la organización de la seguridad de la información, así como la seguridad ligada al talento humano en Lubricentro Avenida Ocaña.		
No.	PREGUNTA / RESPUESTA	AUDITOR
1.	¿Cómo se lleva a cabo el proceso de reclutamiento del personal que requiere para su empresa?	<b>L.M.D.A.</b>
R.		
2.	¿Se hace revisión de los antecedentes del aspirante al cargo?	
R.		
3.	¿Los candidatos seleccionados reciben el respectivo entrenamiento para ocupar el cargo vacante?	
R.		
4.	¿Se establecen acuerdos de confidencialidad de la información para establecer las restricciones en cuanto al uso de los datos y a las implicaciones legales que acarrea el incumplimiento de las mismas?	
R.		
5.	¿Se firman cláusulas de confidencialidad y protección de los datos con terceros?	
R.		
6.	¿Los empleados han recibido capacitación en las medidas de seguridad que deben tenerse en cuenta para la correcta manipulación de la información que utilizan para el desarrollo de las actividades propias de su cargo?	
R.		
7.	¿Formalmente existe algún procedimiento disciplinario para aquellos empleados que incumplan con los requerimientos de seguridad, como fraude, divulgación, eliminación de información, entre otros?	
R.		
8.	¿Existe algún protocolo para eliminar la información del usuario en el sistema, cuando éste ha sido removido de su puesto de trabajo?	
R.		
<b>MARCAS UTILIZADAS EN EL PRESENTE DOCUMENTO</b> EN-03: Entrevista 3 L.M.D.A.: Luz Mery Durán Alvernia – Responsable Auditoría		

**Apéndice H.** Entrevista verificación procedimientos para la gestión de activos.

 <b>Universidad</b> Francisco de Paula Santander Ocaña - Colombia		
<b>ENTREVISTA</b>		<b>PT. EN-04</b>
<b>Empresa: LUBRICENTRO AVENIDA OCAÑA</b> <b>Entrevistado: Gerente</b>		Fecha de Elaboración: __/__/__ Fecha de Ejecución: __/__/__
Objetivo: Verificar los procedimientos implementados para la gestión de los activos de Lubricentro Avenida Ocaña.		
<b>No.</b>	<b>PREGUNTA / RESPUESTA</b>	<b>AUDITOR</b>
1.	¿De qué manera se encuentran identificados los activos más importantes de la empresa?	<b>L.M.D.A.</b>
R.		
2.	¿Existe algún método específico para el manejo de los inventarios de la empresa?	
R.		
3.	¿Existe un responsable de los inventarios de la empresa? ¿Qué actividades le competen?	
R.		
4.	¿Existe algún procedimiento formal para gestionar la seguridad de los activos de la empresa, específicamente de la información necesaria para la marcha de la empresa?	
R.		
5.	¿Existen reglas para el uso aceptable de la información y de los activos de la empresa por parte de los empleados que los requieran en un momento determinado?	
R.		
6.	¿Existen reglas para asegurar la información cuando se establecen intercambios con terceros (contratistas, proveedores, clientes)?	
R.		
<b>MARCAS UTILIZADAS EN EL PRESENTE DOCUMENTO</b> <b>EN-04:</b> Entrevista 4 <b>L.M.D.A.:</b> Luz Mery Durán Alvernia – Responsable Auditoría		

**Apéndice I.** Entrevista evaluación procedimientos para la gestión de los incidentes de seguridad.

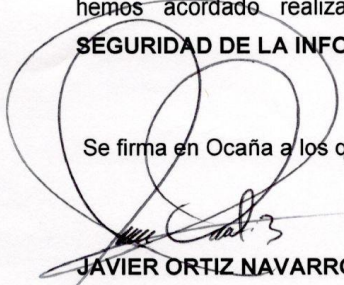
 <b>Universidad</b> Francisco de Paula Santander Ocaña - Colombia		
<b>ENTREVISTA</b>		<b>PT. EN-05</b>
<b>Empresa: LUBRICENTRO AVENIDA OCAÑA</b> <b>Entrevistado: Gerente</b>		Fecha de Elaboración: __/__/__ Fecha de Ejecución: __/__/__
Objetivo: Evaluar la existencia de procedimientos para la gestión de los incidentes de seguridad y de la continuidad del negocio.		
No.	PREGUNTA / RESPUESTA	AUDITOR
1.	¿Qué importancia tiene para usted asegurar la información que es utilizada para el desarrollo de sus actividades comerciales?	<b>L.M.D.A.</b>
R.		
2.	¿Desde la gerencia se ha hecho alguna identificación de las amenazas que puedan poner en riesgo la continuidad de los procesos comerciales (fallas en el equipo, errores humanos, robo, fuego, desastres naturales, etc.) y el impacto de dicha situación?	
R.		
3.	¿La empresa cuenta con algún procedimiento para el reporte de eventos en la seguridad de la información o en cualquier otro activo?	
R.		
4.	¿Los empleados de la empresa están capacitados para identificar y reportar incidentes que puedan afectar la información o cualquier otro activo?	
R.		
5.	¿Tienen ustedes como empresa la información de contactos especiales para realizar el respectivo reporte de algún evento que pueda interrumpir el servicio de procesamiento de información (energía eléctrica, comunicaciones, bomberos, etc.)?	
R.		
6.	¿Se han presentado situaciones o fallas en el sistema que hayan hecho suspender las actividades de gestión de la información (contable, de servicios, de ventas, etc.)?	
R.		
7.	¿Cómo se ha solucionado este tipo de incidentes?	
R.		
8.	¿Están preparados para enfrentar un incidente que pueda suspender temporalmente los servicios que ofrece la empresa?	
R.		
<b>MARCAS UTILIZADAS EN EL PRESENTE DOCUMENTO</b> <b>EN-05:</b> Entrevista 5 <b>L.M.D.A.:</b> Luz Mery Durán Alvernia – Responsable Auditoría		

**Apéndice J.** Acta de entrega de la Guía de controles de seguridad de la información ISO/IEC 27002:2013 para Lubricentro Avenida.

### ACTA DE ENTREGA

Entre los suscritos a saber **LUZ MERY DURAN ALVERNIA**, mayor de edad, con domicilio en el Municipio de Ocaña, Norte de Santander, identificado con cédula de ciudadanía 37.331.710 expedida en Ocaña y **MARCELA TORCOROMA ALVAREZ ANGARITA**, mayor de edad, con domicilio en el Municipio de Ocaña, Norte de Santander, identificado con cédula de ciudadanía 37.371.201 expedida en Convención obrando en calidad de **ESTUDIANTES DE ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE LA UFPSO** y **JAVIER ORTIZ NAVARRO**, mayor de edad, con domicilio en Ocaña, Norte de Santander, identificado con la cedula de ciudadanía 88.282.592 expedida en Ocaña, en condición de **REPRESENTANTE LEGAL LUBRICENTRO AVENIDA** con el NIT 88.282.592-8 hemos acordado realizar la entrega de la **GUÍA DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27002:2013**

Se firma en Ocaña a los quince (5) días del mes de Diciembre de 2016.



**JAVIER ORTIZ NAVARRO**

**REPRESENTANTE LEGAL LUBRICENTRO AVENIDA OCAÑA**



**LUZ MERY DURAN ALVERNIA**

**EST. ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS**



**MARCELA TORCOROMA ALVAREZ ANGARITA**

**EST. ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS**