VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSTGRADOS

MAESTRÍA EN GERENCIA DE SISTEMAS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN GERENCIA DE SISTEMAS

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA EL CONTROL FÍSICO Y DIGITAL DE DOCUMENTOS APLICADO A LA EMPRESA LOCKERS S.A."

AUTORES: LEMA VINLASACA, ROBERTO CARLOS

DONOSO GALLO, DIEGO FERNANDO

DIRECTOR: ING. GÓMEZ TORRES, ESTEVAN RICARDO MSC

SANGOLQUÍ

2018

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación ***"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA EL CONTROL FÍSICO Y DIGITAL DE DOCUMENTOS APLICADO A LA EMPRESA LOCKERS S.A."*** fue realizado por los señores ***Lema Vinlasaca, Roberto Carlos y Donoso Gallo, Diego Fernando***, el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustenten públicamente.

Sangolquí, 27 de febrero del 2018

Firma:

Ing. Estevan Ricardo Gómez Torres, Msc, PhD(c)
C.C: 170772430-6

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORÍA DE RESPONSABILIDAD

Nosotros, ***Lema Vinlasaca, Roberto Carlos,*** con cédula de ciudadanía nº 171936701-1 y ***Donoso Gallo, Diego Fernando***, con cédula de ciudadanía nº 171764734-9 declaramos que el contenido, ideas y criterios del trabajo de titulación: "***IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA EL CONTROL FÍSICO Y DIGITAL DE DOCUMENTOS APLICADO A LA EMPRESA LOCKERS S.A.***" es de nuestra autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciado las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 27 de febrero del 2018

Roberto Carlos Lema Vinlasaca
C.C. 171936701-1

Diego Fernando Donoso Gallo
C.C 1717647334-9

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN

Nosotros, ***Lema Vinlasaca, Roberto Carlos***, con C.C. nº 171936701-1 y ***Donoso Gallo, Diego Fernando***, con C.C nº 171764734-9, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación ***"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA EL CONTROL FÍSICO Y DIGITAL DE DOCUMENTOS APLICADO A LA EMPRESA LOCKERS S.A"*** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 27 de febrero del 2018

Roberto Carlos Lema Vinlasaca

C.C. 171936701-1

Diego Fernando Donoso Gallo

C.C 1717647334-9

DEDICATORIA

A mis padres, por el ejemplo de lucha, perseverancia, respeto y humildad, porque han estado junto a mi compartiendo logros y fracasos, por las arduas luchas durante mi formación académica, éste logro es para ustedes.

Roberto Lema

DEDICATORIA

A mi esposa, pilar fundamental para la obtención de mi título de Magíster, a mi madre quien fue mi apoyo desde mi corta edad y a mis hijos quienes son mi inspiración para lograr alcanzar la cima del éxito profesional y personal.

Diego Donoso

AGRADECIMIENTO

A Dios, quien ha estado presente en cada etapa de mi vida siendo fuente de sabiduría y fortaleza; a mis padres por su apoyo incondicional, sus consejos y palabras de aliento que han sido fuente inspiración para demostrarme que todo es posible con esfuerzo y perseverancia.

A mis amigos quienes me han brindado su apoyo incondicional durante la etapa académica y han formado parte del desarrollo de este proyecto.

Roberto Lema

AGRADECIMIENTO

A la Universidad de las Fuerzas Armadas ESPE por haberme brindado la oportunidad actualizar mis conocimientos profesionales

Diego Donoso

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente documento establece una metodología para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) aplicando los requisitos y procedimientos establecidos por la norma ISO/IEC 27001:2013 para empresas cuyo principal proceso de negocio sea el control físico y digital de documentos. El proyecto inicia con la justificación e importancia del desarrollo del proyecto, el planteamiento y formulación del problema, la definición de las hipótesis y objetivos del proyecto. En el segundo capítulo establece la conceptualización de las normas y marcos de referencia a ser utilizadas durante el desarrollo del proyecto, su alcance y aplicación para la gestión de seguridad de la información. En el tercer capítulo se realiza el estudio, análisis y selección del marco de referencia para la planificación y ejecución de la gestión de riesgo en la seguridad de información. Posteriormente, en el cuarto capítulo se desarrolla una propuesta metodológica para la definición, planeación, diseño e implementación de un sistema de gestión de seguridad de la información para empresas de control físico y digital de documentos. Finalmente, en el quinto capítulo se implementa un Sistema de Gestión de Seguridad de la Información sobre la empresa Lockers S.A acorde a la metodología descrita en el Capítulo 4 para concluir con la emisión de conclusiones y recomendaciones del proyecto.

Palabras clave:

- **SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN**
- **GESTIÓN DE RIESGO**
- **ISO 27001**
- **ISO 27002**
- **ISO 27003**
- **ISO 27005.**

ABSTRACT

This document establishes a methodology for the Information Security Management System (ISMS) implementation applying the requirements and procedures established by ISO / IEC 27001: 2013 for organizations whose main business process is physical and digital management of documents. The project begins with the justification and importance of the development of the project, the approach and formulation of the problem, the definition of the hypotheses and objectives of the project. In the second chapter describes the terms and definitions that will be used during the progress of the project, as well as the description of the norms and reference frames, their scope and application for the management of information security. In the third chapter, the evaluation, analysis and selection of the reference framework for the planning and execution of risk management in information security is carried out. Subsequently, the fourth chapter establishes the methodology for the definition, planning, design and implementation of an information security management system for organization of physical and digital control of documents. Finally, in the fifth chapter an Information Security Management System is implemented on the company Lockers S.A according to the methodology described in Chapter 4 to conclude with the issuance of conclusions and recommendations of the project.

Keywords:

- **INFORMATION SECURITY MANAGEMENT SYSTEM**
- **RISK MANAGEMENT**
- **ISO 27001**
- **ISO 27002**
- **ISO 27003**
- **ISO 27005**

CAPÍTULO 1
GENERALIDADES

En el presente capítulo se plantea el problema que será objeto de estudio durante el desarrollo del proyecto, se formula hipótesis y se define los objetivos.

1.1 Introducción

Uno de los activos más críticos e importantes para cualquier organización es la información generada en su operación; por tal razón se ha de garantizar la disponibilidad, confidencialidad e integridad. Para ello, existen normas que permiten gestionar, regular y mitigar los riesgos asociados a las tecnologías de la información, que amenazan con la disponibilidad, confidencialidad e integridad de la información. Ésta es la norma ISO/IEC 27001:2013.

El presente proyecto de titulación, establece una metodología para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) aplicando los requisitos y procedimientos establecidos por la norma ISO/IEC 27001:2013 para empresas cuyo principal proceso de negocio es el control físico y digital de documentos. La implementación del SGSI será sobre la empresa Lockers S.A tomada como caso de estudio.

1.2 Justificación e importancia

Toda organización o persona natural se encuentra constantemente amenazada por varias situaciones que ponen en riesgo la integridad de la información. Estas amenazas conllevan riesgos no solo provenientes del exterior de las empresas sino desde su interior.

El activo más valioso de toda organización o empresa es la información generada durante su operación, que sirve de insumo para la toma de decisiones estratégicas, por ello debe ser protegida y resguardada de las amenazas existentes en el entorno, garantizando su integridad, disponibilidad y seguridad.

Es imprescindible contar con un sistema de Gestión de Seguridad de la Información que permita mitigar el impacto de los riesgos y crear una cultura organizacional de seguridad en la manipulación de la información.

El comportamiento de las empresas ante la problemática descrita es mayormente reactivo, es decir, actúan luego de que el incidente de seguridad ha ocurrido, por lo tanto, es importante actuar en forma proactiva en la manipulación de la información, tomando como base estándares de seguridad como la norma ISO/IEC 27001:2013.

Un Sistema de Gestión de Seguridad de la Información (SGSI), permite que la empresa conozca cuáles son los riesgos a los que se están expuestos los activos de información y permite realizar su tratamiento mediante instructivos bien definidos, documentados, disponibles, conocidos por todos y que constantemente deben ser expuestos a mejoras continuas. (ISO/IEC 27001:2013, 2014)

1.3 Planteamiento del problema

Lockers S.A. es una empresa dedicada desde hace más de 15 años a prestar servicios de Control Físico y Digital de todo tipo de documentos en el Ecuador. La empresa almacena información sensible de sus clientes en formato físico y digital, su custodia, operación y almacenamiento no están siendo gestionados con políticas basadas en normas de tratamiento de información, exponiendo así su integridad, seguridad y disponibilidad.

1.4 Formulación del problema

¿Cuáles son los eventos que afectan la operación sin la aplicación de normas y estándares que gestionen adecuadamente la seguridad de la información de la empresa Lockers S.A.?

¿Cómo mitigar los riesgos identificados que provienen de amenazas y vulnerabilidades que atentan contra la confidencialidad, disponibilidad e integridad de los activos de información?

1.5 Hipótesis

1.5.1 Hipótesis 1

Si Lockers S.A. contaría con normativas de seguridad en sus procesos de operaciones; minimizaría el riesgo de que los activos de información sean vulnerados, saboteados o destruidos.

1.5.2 Hipótesis 2

Si se contaría con un sistema de gestión de la seguridad de información; se podría identificar y tratar los riesgos de los activos de información que impactan negativamente en la operación de la empresa.

1.6 Objetivos

1.6.1 General

Implementar un sistema de gestión de seguridad de información basado en la norma ISO 27001:2013 para el control físico y digital de documentos, en la empresa Lockers S.A.

1.6.2 Específicos

- Establecer el alcance del Sistema de Gestión de Seguridad de la Información para el control físico y digital de documentos.
- Identificar, valorar y clasificar los activos de información asociados al proceso de control físico y digital de documentos.
- Realizar un estudio comparativo de marcos referenciales para la gestión de riesgos, entre ISO/IEC 27005:2011, MAGERIT v3 y CRAMM.
- Gestionar los riesgos asociados al proceso de control físico y digital de documentos, utilizando el marco de referencia seleccionado en el estudio comparativo.

- Evaluar y definir los controles de seguridad de la información apropiados para cada activo de información sugeridos por la norma ISO/IEC 27002:2012.

- Generar políticas, procedimientos y documentación necesaria para operación y mantenimiento del Sistema de Gestión de Seguridad de la Información.

- Evaluar la eficacia de los controles implementados en un período de 5 meses a partir de la fecha de implementación como caso de estudio.

CAPÍTULO 2
MARCO TEÓRICO

En el presente capítulo se realiza una conceptualización de las principales definiciones que se harán uso durante el desarrollo del proyecto, así como la descripción de las normas y marcos de referencia referenciados, su alcance y aplicación para la gestión de seguridad de la información.

2.1 Seguridad de la información

La información es generada a partir de un conjunto de datos que son recopilados en el transcurso del tiempo, ya sea de forma física o digital; dentro de una empresa u organización; la información se ha convertido en uno de los activos más valiosos y sensibles al dar valor en la toma de decisiones y a la anticipación de un plan estratégico al contener datos sobre las tendencias de mercado, estados financieros, proyecciones de crecimiento, talento humano, etc. (Susanto, Nabil, & Chee, 2011)

La seguridad de la información es la protección de la información contra amenazas presentes en el entorno a fin de minimizar los posibles daños causados sobre los activos, por lo que es necesario la implementación de un estándar que regule la gestión de la seguridad de la información para minimizar daños, ampliar las oportunidades del negocio, maximizar el retorno de las inversiones y asegurar la continuidad del negocio. Existen varios estándares como PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA, ITIL and COBIT. Sin embargo, algunos de estos estándares no se adaptan a todos los tipos de organizaciones por diversas razones.

2.2 Propiedades de la seguridad de la información

La gestión de la seguridad de la información se basa en tres pilares:

- Confidencialidad: La información no es expuesta a personas, entidades o procesos no autorizados.

- Integridad: La información debe ser clara y completa y solo podrá ser modificada por personas, entidades o sistemas autorizadas para ello. La falta de integridad de la información puede exponer a la organización a riesgos en la toma de decisiones.

- Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad los clientes.

La información y los sistemas asociados constituyen el activo más importante para una organización; asegurar la confidencialidad, integridad y disponibilidad de la información permite mantener la competitividad, rentabilidad, e imagen necesarios para alcanzar los objetivos empresariales y asegurar beneficios económicos. [1]

2.3 Términos y definiciones

Los términos y definiciones se encuentran en el ANEXO 1.

2.4 Familia ISO 27000

La familia ISO/IEC 27000 es un conjunto de normas que ayuda a las organizaciones a mantener seguros sus activos de información, determina la importancia y los lineamientos de implementar un sistema de gestión de la seguridad de la información para minimizar daños, ampliar las oportunidades del negocio, maximizar el retorno de las inversiones y asegurar la continuidad del negocio. (ISO, 2017)

Para el desarrollo del proyecto se hará énfasis en las normas ISO 27001, ISO 27002 e ISO 27005, necesarias para la dirección e implementación del SGSI.

2.4.1 ISO/IEC 27001

Esta norma proporciona los requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la

[1] http://www.iso27000.es/download/doc_sgsi_all.pdf

Seguridad de la Información dentro del contexto y necesidades de la organización (INEN-ISO/IEC 27001:2011, 2011).

2.4.2 ISO/IEC 27002

“Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización (…) Puede servir como guía práctica para el desarrollo de normas de la seguridad de una organización y para las prácticas eficaces de gestión de la seguridad” (ISO/IEC 27002:2013, 2013)

2.4.3 ISO/IEC 27005

Esta norma proporciona directrices para la gestión del riesgo de la seguridad de la información en una organización, dando soporte particular a los requisitos de un sistema de gestión de seguridad de la información de acuerdo con la ISO/IEC 27001. (ISO/IEC 27005:2011, 2011)

2.5 Sistema de Gestión de Seguridad de la Información

Salvaguardar los activos se convierte en una de las tareas más importantes para la organización, es así que un modelo de gestión de seguridad deberá contemplar políticas, procedimientos, planes e implementación de controles de seguridad basados en la evaluación y tratamiento de riesgos.

El Sistema de Gestión de la Seguridad de la Información ayuda a establecer las políticas y procedimientos en relación a los objetivos de negocio de la organización, asegura que los riesgos sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información.

La norma ISO/IEC 27001, especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información dentro del contexto, necesidades, objetivos, requisitos de seguridad, procesos, estructura y tamaño de la organización.

Para el desarrollo de este proyecto se utilizará la versión 2013 de la norma.

2.5.1 ISO/IEC 27001:2013

Esta norma, especifica los requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información dentro del contexto y necesidades de la organización. Además, incluye los requisitos para la apreciación y tratamiento de los riesgos de la información. (ISO/IEC 27001:2013, 2014)

La norma ha sido desarrollada en base al Anexo SL de la Parte 1 de las Directivas ISO/IEC “Suplemento Consolidado de las Directivas ISO/IEC”, donde se establece un formato y un conjunto de lineamientos a seguir para el desarrollo documental de un sistema de gestión sin importar su enfoque empresarial, alineando bajo una misma estructura todos los documentos relacionados con los sistemas de gestión y evitando así problemas de integración con otros marcos de referencia como ISO 9001, ISO 20000, ISO 14000, etc.

El Anexo SL proporciona una nueva estructura, denominada de Alto Nivel, para los sistemas de gestión ISO:

Tabla 1
Estructura SL de Alto Nivel

Cláusula 1	Objeto y campo de aplicación
Cláusula 2	Referencias normativas
Cláusula 3	Términos y Definiciones
Cláusula 4	Contexto de la organización
Cláusula 5	Liderazgo
Cláusula 6	Planificación
Cláusula 7	Soporte
Cláusula 8	Operación
Cláusula 9	Evaluación del desempeño
Cláusula 10	Mejora

Fuente: *(ISO/IEC 27001:2013, 2014)*.

Las cláusulas 1 al 3 determinan las generalidades de la norma en cuanto a los resultados esperados del sistema de gestión, normas de referencia o publicaciones relevantes relacionadas a esta norma y detalles de términos y definiciones aplicables a la norma[2].

Las cláusulas 4 a 10 son requisitos indispensables a ser cumplidos para una correcta implementación de un Sistema de Gestión de Seguridad de la Información; cláusulas que se hace una breve descripción a continuación[3]:

Cláusula 4: Contexto de la organización

- Comprensión de la organización y de su contexto
- Comprensión de las necesidades y expectativas de las partes interesadas.
- Determinación del alcance del SGSI.
- Sistema de gestión de seguridad de la información.

Cláusula 5: Liderazgo

- Liderazgo y compromiso de la alta dirección.
- Definición de políticas de seguridad de la información.
- Determinación de roles, responsabilidades y autoridades en la organización.

Cláusula 6: Planificación

- Establecer acciones para tratar los riesgos y oportunidades.
- Establecer objetivos de seguridad de la información y planificación para su consecución.

Cláusula 7: Soporte

- Determinación de recursos.
- Determinar la competencia de las personas.
- Concienciación de las personas de las políticas de seguridad de la información.
- Comunicación del SGSI.

[2] Para más detalles de las clausulas 1, 2 y 3, referirse a la documentación de la norma ISO/IEC 27001:2013.
[3] Para más detalles de las clausulas 4 a 10, referirse a la documentación de la norma ISO/IEC 27001:2013.

- Información documentada requerida por la norma.

Cláusula 8: Operación

- Planificación y control operacional necesarios para cumplir los requisitos de seguridad de la información.
- Apreciación de los riesgos de seguridad de información.
- Tratamiento de los riesgos de seguridad de información.

Cláusula 9: Evaluación del desempeño

- Evaluación del desempeño y eficacia del SGSI.
- Ejecución de auditorías internas.
- Revisión del SGSI por la alta dirección.

Cláusula 10: Mejora

- Hacer frente a las no conformidades y ejecutar acciones correctivas.
- Establecer estrategias de mejora continua.

La certificación en ésta norma requiere del cumplimiento de las cláusulas 4 al 10.

2.6 Gestión de Riesgo

La gestión de riesgo es el requisito fundamental para el desarrollo e implementación de un SGSI, ya que en esta etapa es donde se construye el modelo de seguridad en el cual se representan todos los activos y sus dependencias jerárquicas, también todo aquello que pudiera ocurrir sobre ellos y que tuviera un impacto en la organización.

2.6.1 Definiciones

El riesgo se define como una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado, de acuerdo a una probabilidad. La gestión del riesgo permite identificar los activos informáticos, las vulnerabilidades y amenazas a los que se encuentran expuestos, su probabilidad de ocurrencia e impacto; así como las acciones preventivas, correctivas y reductivas que deben tomarse para tratarlos con la finalidad de reducirlos a un nivel aceptable.

2.6.2 Análisis y evaluación del riesgo

El análisis del riesgo permite determinar el valor de los activos de información, identificar las amenazas y vulnerabilidades, controles existentes y sus efectos en el riesgo identificado, determinar las consecuencias potenciales, priorizar los riesgos derivados y clasificarlos frente a criterios de evaluación.

2.6.3 Marcos de referencia para el análisis de riesgos

MAGERIT.- Es de carácter público elaborada por el Consejo Superior de Administración Electrónica (CSAE) y publicada por el ministerio de administración pública de España (MAP) encargado de la preparación, elaboración, desarrollo y aplicación de la política informática del gobierno español. (MAGERIT v.3, 2012)

*ISO/IEC 27005***.-** Descrita en el acápite 2.4.3

CRAMM.- Es una herramienta cualitativa de análisis y gestión de riesgos desarrollada en 1978 por la Agencia Central de Informática y Telecomunicaciones (CCTA) del gobierno de Reino Unido. Consta de herramientas de evaluación de riesgo compatibles con la norma 27001 que se enfocan en la evaluación de impacto empresarial, identificación y evaluación de amenazas y vulnerabilidades.

2.6.4 Tratamiento del riesgo

El proceso de gestión del riesgo deberá establecer un contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. De manera general existen las siguientes opciones para el tratamiento del riesgo:

Asumir el Riesgo.- Cuando se determina que el nivel de exposición al riego es adecuado y por lo tanto se acepta.

Mitigar el Riesgo.- Cuando el riesgo se puede gestionar en caso de materialización, la entidad se encuentra en la capacidad de asumirlo, implementar controles adicionales como parte del fortalecimiento de los actuales o como resultado de haberlo compartido o transferido.

Transferir el Riesgo.- Pasarlo a otra responsabilidad, que en caso de ocurrencia responderá por los daños causados, generalmente los seguros contra eventos imprevistos.

Evitar el Riesgo.- Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

CAPÍTULO 3
ANÁLISIS DE LOS MARCOS DE REFERENCIA Y NORMATIVAS PARA LA GESTIÓN DE RIESGO

En el presente capítulo se realiza el estudio, análisis y selección del marco de referencia para la planificación y ejecución de la gestión de riesgo en la seguridad de información. Se detalla las características más relevantes de cada marco y normativa relacionada para posteriormente valorarlas y seleccionar la que cumpla con las características requeridas para la consecución del proyecto.

3.1 Selección del marco de referencia y normativas para la gestión de riesgo.

Existen varias guías informales, aproximaciones metodológicas y herramientas de soporte para llevar a cabo el análisis y evaluación del riesgo, cuyo objetivo general es saber cuán seguros o inseguros son los sistemas de información y establecer un tratamiento para los riesgos identificados. Cada una de las guías o métodos toman distintos matices en cuanto a la complejidad del problema al que se enfrentan; es decir, dependiendo del enfoque que presentan deben considerar varios elementos y variables, que de no ser tratados con rigurosidad pueden afectar la credibilidad de los resultados obtenidos y requeridos por la naturaleza de la organización.

Para el desarrollo de este proyecto, se han considerado diferentes herramientas, metodologías y estándares de referencia; entre éstas: MAGERIT, CRAMM e ISO/IEC 27005 en sus versiones actuales. Tras una breve descripción de cada uno de ellas, se realizará una selección en base a las características más relevantes que aporten a la ejecución del proyecto planteado.

3.1.1 MAGERIT v3.0

Es una metodología de análisis y gestión de riesgos de TIC de carácter público (Administración Pública) elaborada por el Ministerio de Administración Pública de España (MAP) encargado de la preparación, elaboración, desarrollo y aplicación de la política informática del gobierno español. La metodología establece principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información a fin de garantizar que las

organizaciones que siguen estos principios estén en capacidad de equilibrar riesgos y oportunidades derivados del uso de las TI.

Objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos indirectos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Fases de la metodología (González, 2012)

- Identificar activos: activos relevantes, su interrelación y valoración.
- Identificar amenazas.
- Determinar las salvaguardas que hay dispuestas y cuan eficaces son frente al riesgo.
- Estimar el impacto: daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo: impacto ponderado con la tasa de ocurrencia de la amenaza.

3.1.2 CRAMM v5.0

Es una herramienta cualitativa de análisis y gestión de riesgos desarrollada en 1978 por la Agencia Central de Informática y Telecomunicaciones (CCTA) del gobierno de Reino Unido. Consta de herramientas de evaluación de riesgo compatibles con la norma 27001 que se enfocan en la evaluación de impacto empresarial, identificación y evaluación de amenazas y vulnerabilidades.

CRAMM puede ser aplicado en distintos tipos de organizaciones para justificar inversiones en TI relacionadas con la identificación y tratamiento de los riesgos asociados a los sistemas de información y redes, demostrando la necesidad de una acción a nivel directivo, en base a resultados cuantificables.

Características principales:

- Dispone de un software que evalúa los riesgos y propone medidas para mejorar la seguridad de la información.
- Determina la creación de documentación de seguridad y planes de contingencia.
- Emplea reuniones, entrevistas y cuestionarios a las partes involucradas para la recolección de datos.
- Presenta 31 amenazas genéricas y 3000 contramedidas.

Fases de la metodología (Yazar, 2002)

- Establecimiento de objetivos de seguridad.
  - Definir el alcance del estudio.
  - Definir el valor de la información, entrevistando a los usuarios sobre los impactos potenciales para el negocio que podrían producirse por la indisponibilidad, destrucción, divulgación o modificación.
  - Identificar y evaluar los activos físicos que forman parte del sistema.
  - Identificar y evaluar los activos de software que forman parte del sistema.
- Análisis de riesgos.
  - Identificar y valorar el tipo de nivel de las amenazas que pueden afectar al sistema.
  - Valorar las vulnerabilidades de los sistemas ante las amenazas identificadas.
  - Combinar las valoraciones de amenazas y vulnerabilidades para calcular la medida de los riesgos.
- Identificación y selección de salvaguardas

3.1.3 ISO /IEC 27005:2011

Esta norma forma parte la familia ISO 27000 y se enfoca en la gestión de riesgos de seguridad de la información. La norma suministra las directrices para la gestión de riesgos de seguridad, en base de los requisitos para el diseño e implementación de un sistema de gestión de seguridad de la información (SGSI) definido en la norma ISO 27001. Se encuentra diseñada para facilitar la implementación satisfactoria de la seguridad de la información con enfoque de gestión de riesgo.

Características principales:

- Presenta un conjunto de directrices para realizar correctamente un análisis de riesgos.
- Apoya la tarea del análisis y la gestión de riesgos en el marco de un SGSI.
- Se aplica a todos los tipos de organizaciones (por ejemplo, empresas comerciales, entidades de gobierno, organizaciones sin fines de lucro).
- Tiene un enfoque sistemático para la gestión del riesgo.
- Aborda los riesgos de manera eficaz y oportuna, donde y cuando sea necesario.
- Es parte de todas las actividades de gestión de seguridad de la información tanto para su aplicación como para la operación continua de un SGSI.

Fases para su aplicación: (ISO/IEC 27005:2011, 2011)

- Alcance
- Normativas de referencia
- Términos y definiciones
- Estructura
- Antecedentes
- Visión del progreso de gestión de riesgos de seguridad de la información
- Establecimiento del contexto
- Evaluación de riesgos
- Tratamiento de riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitorización y revisión del riesgo, todas esta establecidas bajo unas cláusulas del estándar internacional.

3.2 Análisis Comparativo

El análisis comparativo de cada una de las metodologías, guías y herramientas seleccionadas para el estudio, se realiza mediante una ponderación de las características fundamentales descritas en el punto anterior.

Se han considerado las siguientes características:

- (C1) Permite identificar las necesidades de la organización sobre los requisitos de seguridad de información.
- (C2) Ayuda a crear los SGSI eficaz.
- (C3) Aborda los riesgos de manera eficaz y oportuna, donde y cuando sea necesario.
- (C4) Es parte de integridad de todas las actividades de gestión de seguridad de la información tanto para su aplicación como para su operación continua de un SGSI.
- (C5) Soporta herramientas informáticas para la gestión de riesgos.
- (C6) Es metódica por lo que se hace fácil su comprensión. Los activos se identifican.
- (C7) Recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria.
- (C8) Toma en cuenta un análisis de vulnerabilidades.
- (C9) La recomendación de los controles está incluída dentro del análisis de riesgos, sino en la gestión y evaluación.
- (C10) La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos.
- (C11) Puede ser aplicada en cualquier tipo de organización sin restricción.

3.2.1 Ponderación de las características seleccionadas.

Determinadas las características más relevantes, se asigna un valor porcentual acorde al requerimiento del proyecto, cuya sumatoria deberá ser igual a 100.

Tabla 2
Ponderación de las características seleccionadas.

CARACTERÍSTICAS	VALOR PORCENTUAL
C1	10%
C2	5%
C3	10%
C4	10%
C5	5%
C6	5%

CARACTERÍSTICAS	VALOR PORCENTUAL
C7	5%
C8	10%
C9	5%
C10	5%
C11	30%
TOTAL	100%

La selección de la herramienta de gestión de riesgo se realizará en base a la multiplicación del valor del nivel de aceptación de cada herramienta por la ponderación de cada característica establecida.

La valoración del nivel de aceptación es la siguiente:

- Ninguna aceptación 1
- Poca aceptación 5
- Gran aceptación 10

3.2.2 Selección de la herramienta.

De acuerdo al análisis realizado, se evalúa cada herramienta en base a las características requeridas para la ejecución del proyecto. Según el resultado obtenido en la Tabla 3, se determina que la herramienta más adecuada para realizar la gestión de riesgos en este proyecto es la norma ISO/IEC 27005:2011.

Tabla 3
Comparación de metodologías de Gestión de Riesgo.

CARACTERÍSTICA	PONDERACIÓN	MAGERIT		CRAMM		ISO 27005	
		ACEPTACIÓN	VALOR	ACEPTACIÓN	VALOR	ACEPTACIÓN	VALOR
C1	10%	7	0,7	8	0,8	9	0,9
C2	5%	8	0,4	8	0,4	10	0,5
C3	10%	7	0,7	7	0,7	10	1
C4	10%	7	0,7	7	0,7	9	0,9
C5	5%	10	0,5	0	0	10	0,5
C6	5%	9	0,45	10	0,5	5	0,25
C7	5%	7	0,35	5	0,25	5	0,25
C8	10%	2	0,2	10	1	10	1
C9	5%	3	0,15	3	0,15	3	0,15
C10	5%	3	0,15	3	0,15	3	0,15
C11	30%	8	2,4	7	2,1	10	3
TOTAL	**100%**	**71**	**6,7**	**68**	**6,75**	**84**	**8,6**

CAPÍTULO 4
DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En el presente capítulo se establece una metodología para la definición, planeación, diseño e implementación de un sistema de gestión de seguridad de la información para empresas de control físico y digital de documentos basado en la norma ISO/IEC 27001:2013. La metodología plantea el entendimiento de la empresa y su situación actual, la selección de los procesos críticos de operación, el diagnóstico de seguridad de la información, identificación de activos y las principales vulnerabilidades y amenazas asociadas, aplica una metodología de gestión de riesgos basado en la norma ISO/IEC 27005:2012 para el tratamiento de riesgos y genera un marco documental del sistema de gestión de seguridad de la información requerido por la norma.

4.1 Metodología de implementación

Por la naturaleza del proyecto, la implementación del SGSI requiere el cumplimiento de las clausulas 4 al 10 planteadas por la norma ISO/IEC 27001:2013; la estructura de la norma no define un orden en específico y deja a criterio de cada empresa la forma en que se cumpla los requisitos. De este modo, se establece las siguientes fases para la implementación del SGSI:

Tabla 4
Fases de implementación del SGSI

FASE 1	Contextualización de la organización.
FASE 2	Definición del Alcance y los Objetivos del SGSI
FASE 3	Identificación de activos.
FASE 4	Gestión de Riesgos.
FASE 5	Definición de políticas, normas y procedimientos.
FASE 6	Auditoría de Cumplimiento del SGSI.

A continuación, se describe la metodología propuesta por los autores que tiene las siguientes características: contextualización de la organización, definición del alcance y

los objetivos del SGSI, identificación de los activos, gestión del riesgo, definición de políticas de seguridad de la información y auditoría del cumplimiento.

4.1.1 Contextualización de la organización

Se realiza la contextualización de la empresa, identificando la misión, visión, objetivos, partes interesadas y responsables de cada una de las unidades de la organización relacionadas con al sistema de gestión de seguridad de la información.

Roles y responsabilidades

Para establecer el Sistema de Gestión de Seguridad de la Información se define la siguiente estructura organizacional:

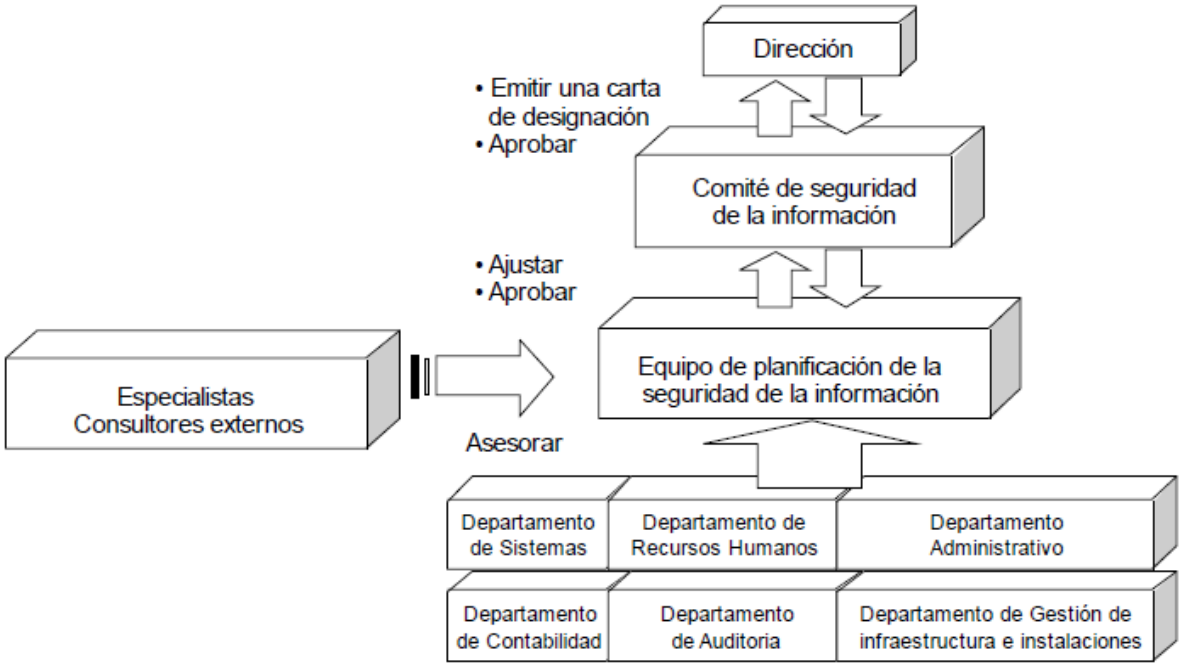

Figura 1 Estructura Organizacional para establecer el SGSI

Fuente: (INEN-ISO/IEC 27003:2012, 2012)

Los roles y responsabilidades en la estructura organizacional incluyen a personas que posean un profundo conocimiento de la organización y del entorno en el cual opera. Por ello se establecen los siguientes roles:

Tabla 5
Roles y responsabilidades para el SGSI

ROLES / POSICIONES	RESPONSABILIDADES
Alta Dirección	Toma de decisiones estratégicas. Incluye al Director General de Operaciones, Director Ejecutivo, Director de Seguridad y Director Financiero.
Gerentes de línea	Responsabilidad superior de las funciones organizacionales.
Director de seguridad de la Información	Responsabilidad y dirección total de la seguridad de la información asegurando el manejo correcto de los activos de información.
Miembro del comité de seguridad de la información	Manejo de los activos de información y el rol de liderazgo para el SGSI en la organización.
Equipo de planificación de la Seguridad de la Información	Durante la implementación del SGSI, el equipo trabaja con los departamentos y resuelve los conflictos hasta que el SGSI sea establecido.
Parte interesada	Personas u organizaciones que tienen interés directo sobre la organización, tales como: el directorio, accionistas, filiales, clientes o propietarios.
Administrador de Sistemas	Administrador responsable de un sistema de TI
Gerente de TI	Gestión de los recursos de TI.
Seguridad física	Persona responsable de la seguridad física. Acceso a instalaciones.
Gestión de Riesgos	Persona/s responsable del marco referencial de gestión del riego, incluyendo evaluación, tratamiento, y monitoreo.

Fuente: (INEN-ISO/IEC 27003:2012, 2012)

La estructura organizacional actual deberá se redefinida y acoplada a los roles y responsabilidades necesarios para la implementación y operación del SGSI.

4.1.2 Definición del Alcance y los Objetivos del SGSI

Se determina los límites y la aplicabilidad del sistema de gestión de seguridad de la información considerando cuestiones externas e internas (normativas legales), necesidades y expectativas de las partes interesadas dentro de la organización; se establecen de esta manera los objetivos de seguridad de la información.

4.1.3 Identificación de activos

El levantamiento de activos debe tener como referencia la información contenida en la caracterización de los procesos como: entradas, salidas, requerimientos, metodologías, procedimientos, hardware, software, bases de datos que permitan identificar la información y los activos asociados a ellas.

La identificación de activos busca determinar qué información es utilizada o generada durante la ejecución de los procesos de negocio y sus medios, sean físicos o digitales.

4.1.3.1 Inventario de activos

La valoración de activos requiere que la organización identifique primero sus activos de información, las responsabilidades y su criticidad para la organización.

Clases de Activos

La norma 27005:2011 diferencia dos clases de activos:

Activos primarios:

- Actividades y procesos del negocio: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización, procesos necesarios para que la organización cumpla con requisitos contractuales, legales o reglamentarios.
- Información: comprende información vital para la ejecución del negocio de la organización, información estratégica de toma de decisiones, información de alto costo operativo y adquisitivo.

Activos de soporte:

Estos activos tienen vulnerabilidades que pueden ser explotados por amenazas cuya meta es degradar los activos primarios.

Tabla 6
Tipos de activos de información

ACTIVO	DESCRIPCIÓN
Hardware	Consta de elementos físicos que dan soporte a los procesos. Entre estos constan: equipos de procesamiento de datos, equipos móviles, equipos fijos, periféricos de procesamiento, equipos de almacenamiento.
Software	Programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos.
Red	Dispositivos de telecomunicaciones utilizados para interconectar equipos de un sistema de información.
Base de datos	Información relacionada y almacenada en medios electrónicos.
Información Electrónica	Información contenida en medios electrónicos.
Información física	Información contenida en medios físicos.
Medio de almacenamiento	Medio de información que puede ser conectada a un computador o una red de computadores para el almacenamiento de datos.
Persona	Todos los grupos o personas involucradas en el sistema de información: personas a cargo de la toma de decisiones, usuarios, personal de operación/mantenimiento, desarrolladores.
Servicio	Servicio interno de la organización cuya operación requiera del uso de componentes de hardware, software e infraestructura de telecomunicaciones.
Sitio	Instalaciones de procesamiento o almacenamiento de información.

Fuente: (ISO/IEC 27005:2011, 2011)

Responsabilidades

Los activos de información identificados deben estar asociados al personal o áreas de la organización quienes ejerzan control y gestión sobre los mismos. Para ello, se definen los siguientes roles:

Propietario: Área, unidad organizacional o proceso donde la información es utilizada de maneras constante.

Responsable: Personas pertenecientes al área, unidad o proceso propietario de un grupo de activos de información, encargada de gestionar la implementación de los controles de seguridad sobre los activos.

Documentación

El inventario de los activos de información debe establecer y describir los elementos que permitan identificarlos de manera única con un grado adecuado de detalle. El documento debe contener:

Tabla 7
Inventario de Activos de Información

IDENTIFICADOR	DETALLE
ID	Identificador numérico secuencial
Nombre	Nombre del activo de información
Proceso	Nombre del proceso al que pertenece el activo de información
Descripción	Descripción del activo de información
Tipo	Tipología a la cual pertenece el activo.
Responsabilidades	Identifica los roles de Propietario, Responsable
Valoración	Valoración del activo de información en: confidencialidad, integridad y disponibilidad.
Clasificación	Confidencial, de uso interno, de uso público.
Ubicación	Lugar físico o electrónico donde reside el activo

4.1.3.2 Valoración de activos

La valoración de los activos determina el grado de impacto que presentan los activos identificados para la organización. La base propuesta para dar valor a los activos es la valoración cualitativa tomando en cuenta el costo en el que incurriría la pérdida de confidencialidad, integridad y disponibilidad como resultado de un incidente.

Perdida de confidencialidad: La información es conocida por personas no autorizadas, que en consecuencia representa impacto en la organización en:

- Pérdida de confianza del cliente.

- Pérdidas financieras.
- Pérdida de proveedores.
- Pérdida de activos.
- Pérdida de ventajas competitivas.

Pérdida de Integridad: La información que no es íntegra, genera errores en el procesamiento de la información y afecta a la toma de decisiones estratégicas. El impacto que presenta es:

- Contravenciones de leyes/reglamentos.
- Alteración en la operación de terceras partes.
- Alteración en la operación interna.
- Incumplimiento de contrato.

Pérdida de Disponibilidad: La información no está disponible para los procesos requirentes, clientes y dueños del activo. El impacto que presenta para la organización es:

- Interrupción de servicios de clientes.
- Pérdidas financieras
- Alteración a la operación de los clientes.
- Contravenciones de legales.
- Procesos judiciales.
- Perdida de liderazgo tecnológico.

Tras establecer los criterios de valoración considerados para el tipo de organización seleccionada, se define una escala que mide el nivel de impacto del activo a la organización, como consta en la Tabla 8.

Tabla 8

Métricas de Impacto

NIVEL	IMPACTO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
5	Crítico	La pérdida de la confidencialidad afecta totalmente al cumplimiento del proceso de negocio.	La pérdida de la integridad afecta totalmente al cumplimiento del proceso de negocio.	La pérdida de la disponibilidad afecta totalmente al cumplimiento del proceso de negocio.
4	Alto	La pérdida de la confidencialidad afecta parcial o totalmente al cumplimiento del proceso de negocio.	La pérdida de la integridad afecta parcial o totalmente al cumplimiento del proceso de negocio.	La pérdida de la disponibilidad afecta parcial o totalmente al cumplimiento del proceso de negocio.
3	Medio	La pérdida de la confidencialidad afecta de forma parcial al cumplimiento del proceso de negocio.	La pérdida de la integridad afecta de forma parcial al cumplimiento del proceso de negocio.	La pérdida de la disponibilidad afecta de forma parcial al cumplimiento del proceso de negocio.
2	Bajo	La pérdida de la confidencialidad, tendría bajo impacto o efecto sobre el proceso de negocio	La pérdida de la integridad, tendría bajo impacto o efecto sobre el proceso de negocio	La pérdida de la disponibilidad, tendría bajo impacto o efecto sobre el proceso de negocio
1	Insignificante	La pérdida de la confidencialidad no afecta al cumplimiento del proceso de negocio.	La pérdida de la integridad no afecta al cumplimiento del proceso de negocio.	La pérdida de la disponibilidad no afecta al cumplimiento del proceso de negocio.

Realizada la valoración del activo en cuanto a la confidencialidad, integridad y disponibilidad, se obtiene una valoración final tomando el nivel más alto de los tres definidos.

4.1.3.3 Clasificación de activos

La clasificación de activos se realiza en base al grado de confidencialidad, integridad y disponibilidad de la información contenida en ellos; acorde a la clasificación se determina los niveles de protección o manejo especial. De este modo, se clasifica la información de acuerdo con la escala que se presenta en la Tabla 9.

Tabla 9
Clasificación de activos

NIVEL	DESCRIPCIÓN
Confidencial	Información de interés solo para quienes va dirigida y cuya divulgación no autorizada puede ocasionar perjuicios al personal o a la organización.
Uso Interno	Información dirigida a los miembros de la organización.
Pública	Información que puede ser publicada sin restricciones a cualquier persona dentro o fuera de la organización sin que conlleve un impacto negativo.

4.1.4 Gestión del riesgo

Se establece una metodología de gestión del riesgo de los activos de información, basado en la norma ISO/IEC 27005:2011, cuyo objetivo es determinar criterios básicos para la gestión del riesgo, definir el alcance y los límites, identificar las amenazas y vulnerabilidades de los activos de información, fiar los lineamientos para evaluar la probabilidad, controles y obtención del riesgo residual y presentar el nivel de aceptación del riesgo.

En la Figura 2 se presenta el flujo de gestión del riesgo de seguridad de información recomendado por la norma ISO/ICE 27005:2011. El proceso de gestión del riesgo puede ser iterativo para las actividades de valoración y tratamiento del riesgo; este enfoque iterativo permite la reducción del tiempo y esfuerzo requerido para identificar los controles, garantizando que los riesgos se valoren de manera correcta.

4.1.4.1 Establecimiento del contexto, alcance y objetivo.

Se establecen los criterios básicos necesarios para la gestión del riesgo, se define el alcance, el objetivo y una adecuada organización que opere la gestión del riesgo de la seguridad de la información. Los lineamientos a seguir constan en la norma ISO/IEC 27005:2012, a la cual se hará referencia para el establecimiento del contexto y alcance.

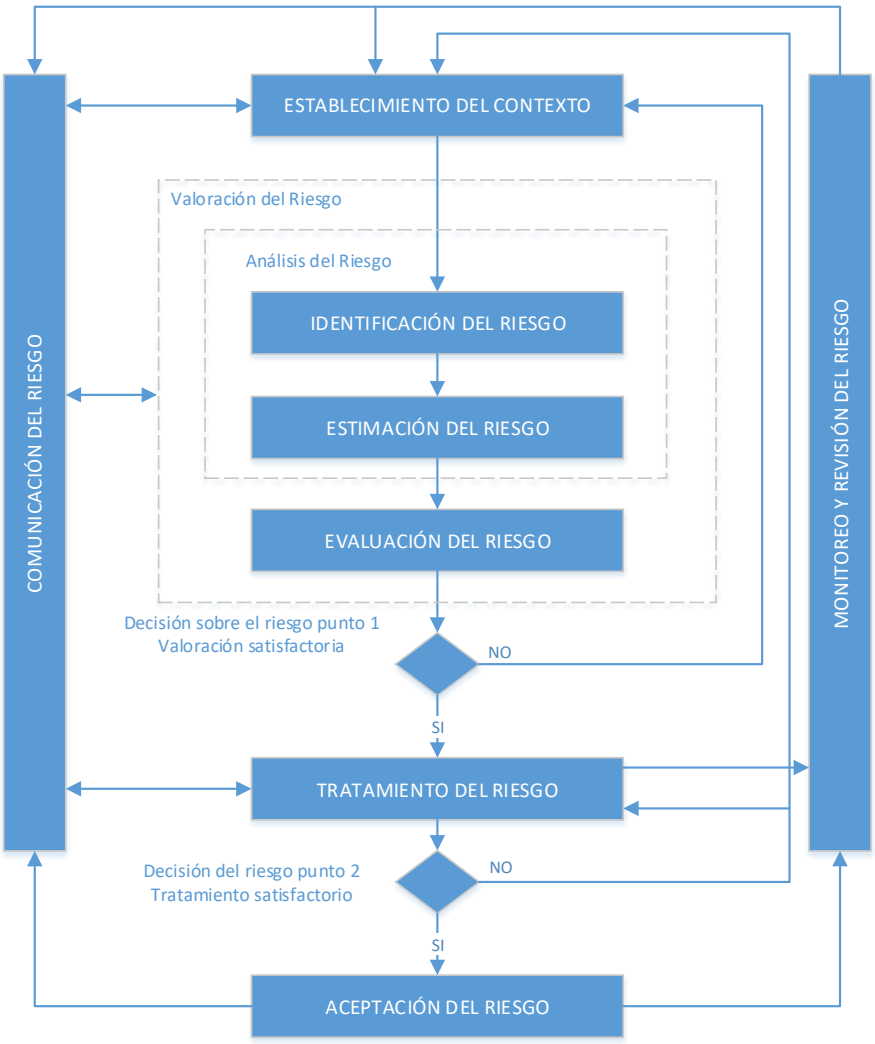

Figura 2: Proceso de gestión del riesgo de la seguridad de la información

Fuente: (ISO/IEC 27005:2011, 2011)

4.1.4.2 Valoración del riesgo

Según la (ISO/IEC 27005:2011, 2011) la valoración del riesgo identifica las amenazas y vulnerabilidades que existen o podrían existir, identifica los controles existentes y sus efectos, determina las consecuencias potenciales y finalmente prioriza los riesgos derivados.

En este contexto, para la valoración del riesgo se toma como referencia las siguientes etapas:

a) Análisis del riesgo

El análisis del riesgo contempla las siguientes actividades[4]:

i) Identificación del riesgo
   - Identificación de activos
   - Identificación de amenazas (amenazas obtenidas de los propietarios de los activos, incidentes u otras fuentes incluidas amenazas externas.)
   - Identificación de controles existentes. (controles existentes y su eficacia)
   - Identificación de vulnerabilidades (vulnerabilidades que pueden ser explotadas por las amenazas y causar daños a los activos)
   - Identificación de consecuencias. (perdida de la eficacia, condiciones adversas, perdida del negocio, reputación, etc.)

ii) Estimación del riesgo

La estimación del riesgo se realiza de forma cualitativa, para esto, se platea la escala presentada en la Tabla 10 que describe la magnitud de las consecuencias potenciales y la probabilidad de ocurrencia. Las escalas establecidas pueden ser adaptadas para satisfacer las necesidades de cada organización.

Tabla 10
Escala de probabilidad de ocurrencia del riesgo

Nivel	Probabilidad	Descripción
5	Muy Alta	El riesgo ha ocurrido o podría ocurrir varias veces al mes
4	Alta	El riesgo ha ocurrido o podría ocurrir varias veces al año
3	Media	El riesgo ha ocurrido o podría ocurrir alguna vez en un año
2	Baja	El riesgo ha ocurrido o podría ocurrir alguna vez dentro de 2 años
1	Muy Baja	El riesgo ha ocurrido o podría ocurrir alguna vez en un periodo de más de 2 años

[4] Las guías de implementación de las actividades de análisis, están descritas en la sección 8.2 de la norma ISO/IEC 27005:2011

b) Evaluación del riesgo

La evaluación del riesgo se realiza en base a la probabilidad de ocurrencia del riesgo multiplicada por el nivel de impacto que presenta el activo. El resultado es el valor que corresponde al **riesgo inherente** o bruto:

$$V_R = V_P * V_I$$

Donde,

V_R = Valor de Riesgo Inherente
V_P = Valoración de Probabilidad
V_I = Valoración del Impacto

Los valores obtenidos están comprendidos entre 1 y 25, corresponden a la zonificación del riesgo y servirán para la definición del tratamiento del riesgo.

4.1.4.3 Tratamiento de riesgo

Identificados y valorados los riesgos, se establece y desarrolla un plan de tratamiento a los riesgos asociados a los activos de información. Para establecer el plan de tratamiento, se zonifica el riesgo por su valor inherente; las zonas se han determinado conforme a las opciones de tratamiento propuestas por la norma ISO 27005:2011[5] y se muestran en la Tabla 11.

Tabla 11
Zonificación del Riesgo

Zona Aceptable	**Aceptar el Riesgo:** Riesgos para los cuales se determina que el nivel de exposición es adecuado y por lo tanto se acepta.
Zona Tolerable	**Transferir el Riesgo:** Riesgos que se puede permitir gestionar, que en caso de materialización la entidad correspondiente se encuentra en la capacidad de asumirlo.
Zona Moderada	**Reducir el Riesgo:** Riesgos para los cuales se requiere fortalecer los controles existentes y/o agregar nuevos controles.
Zona Inaceptable	**Evitar el Riesgo:** Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

Fuente: (ISO/IEC 27005:2011, 2011)

[5] Anexo B. Apartado 9.

Las zonas se han definido en cuatro escalas, de acuerdo la Tabla 12:

- Zona Aceptable: 1 <= VR <= 4
- Zona Tolerable: 5 <= VR <= 10
- Zona Moderada: 11 <= VR <= 15
- Zona Inaceptable: 16 <= VR <= 25

Tabla 12
Mapa de calor

PROBABILIDAD						
	5	Tolerable	Tolerable	Moderado	Inaceptable	Inaceptable
	4	Aceptable	Tolerable	Moderado	Inaceptable	Inaceptable
	3	Aceptable	Tolerable	Tolerable	Moderado	Moderado
	2	Aceptable	Aceptable	Tolerable	Tolerable	Tolerable
	1	Aceptable	Aceptable	Aceptable	Aceptable	Tolerable
		1	2	3	4	5
				IMPACTO		

Identificación y selección de controles

Para los riesgos cuyos tratamientos sean evitar o reducir, se debe identificar los posibles controles que podrían mitigar los riesgos identificados en las zonas “Inaceptables” o “Moderadas” y reducir el nivel de riesgo a “Tolerable” o “Aceptable”.

La selección de controles, depende de las decisiones de carácter organizativo, basadas en los criterios de aceptación del riesgo, opciones de tratamiento del riesgo y de la legislación y reglamentación nacional e internacional aplicable. (ISO/IEC 27002:2013, 2013)

Los controles a ser implementados se describen en la norma ISO/IEC 27002:2013 cuya selección considera los siguientes aspectos[6]:

- Objetivos de la organización.
- Restricciones legales y regulatorias.

[6] Los criterios para cada aspecto están definidos en base al numeral 7 de la ISO/IEC 27005:2011

- Costo de implementación.
- Restricciones operacionales.
- Efectividad

De esta manera, en el proceso de selección de controles, se valoriza cada criterio de acuerdo a la Tabla 13, considerando que:

- Se asigna el valor máximo si el control cumple con el criterio y un valor de cero (0) si el control no cumple o cumple parcialmente con el criterio determinado.
- Los criterios son agrupados y para cada uno de ellos se establece un valor mínimo que deberá cumplir para ser aceptado.

La sumatoria de valores de los criterios establecidos, dará como resultado el valor total de aceptación del control a ser implementado, cuyo valor mínimo aceptable es 68.

Tabla 13
Valoración del control

ASPECTOS	CRITERIOS	VALOR	VALOR ACEPTABLE
Objetivos de la organización	El control apoya a los objetivos de la organización.	8	12
	El control cumple con las políticas o normativas organizacionales.	6	
	El control presenta una oportunidad de mejora a las políticas o normativas.	6	
Restricciones legales y Regulatorias	El control cumple con la legislación o regulación vigente	20	20
Restricciones operacionales	El control se integra con la infraestructura tecnológica existente	8	12
	El tiempo de implementación es acorde a la necesidad de la organización	6	
	Se cuenta con personal capacitado para la implantación del control	6	
Costo de implementación	El costo de implementación no supera al costo de materialización del riesgo	10	10
	El control no genera gastos adicionales a los considerados en el proceso de implementación	10	

ASPECTOS	CRITERIOS	VALOR	VALOR ACEPTABLE
Efectividad	El control reduce la probabilidad de ocurrencia del riesgo	6	14
	El control reduce el nivel de impacto del riesgo	6	
	El control mitiga más de un riesgo identificado	8	
	TOTAL	100	68

La selección y evaluación de los controles deben ser realizadas por el equipo responsable de la ejecución del proceso de gestión de riesgo, quienes priorizaran la implementación de controles acorde a los valores obtenidos en la selección de controles y el cumplimiento de las necesidades organizacionales.

La planificación y aceptación de los controles será puesta a consideración de los responsables de los activos de información involucrados quienes, de aceptar la implementación de los controles, establecerán las fechas de implementación acorde a sus criterios y necesidades.

4.1.4.4 Aceptación del riesgo

De acuerdo a las zonas de riesgo definidas en la Tabla 11, se acepta o asume los riesgos que estén dentro de la Zona de Aceptación, no obstante, está determinación no es obligatoria; dependerá de las necesidades del negocio y de la priorización que se dé a la mitigación de los riesgos; es así que la organización podrá optar por tratar los riesgos de la Zona Inaceptable con prioridad y bajar el riesgo residual hasta la Zona Tolerable para posteriormente reevaluar el riesgo y mitigarlo.

Quienes tomen la decisión de aceptar un riesgo que no cumpla con los criterios normales de aceptación expuestos, deberán comentar explícitamente los riesgos e incluir una justificación para la decisión tomada.

4.1.4.5 Comunicación de los riesgos de la seguridad de la información

Los riesgos identificados, así como el plan de tratamiento establecido, deben ser puestos en conocimiento de las partes interesadas, dado que se puede tener un impacto significativo en las decisiones que se deben tomar. Esto garantiza que los responsables de la implementación de la gestión del riesgo y las partes interesadas comprendan las

bases sobre la cuales toman las decisiones y por qué se requieren acciones particulares (ISO/IEC 27005:2011, 2011).

Los reportes a emitir son:

- El coordinador del equipo de riesgos deberá reportar periódicamente al Comité de Riesgos acerca de la gestión de riesgos de la organización en forma unificada y los avances de los planes de acción.
- El Presidente del Comité de Riesgos presentará al Directorio informes de la gestión de riesgos de la organización y en particular sobre:
    - Proceso de Gestión de Riesgos.
    - Matriz de Riesgos actualizada.
    - Probabilidad e impacto de ocurrencia de los riesgos más relevantes.
    - Recomendaciones y mejoras que el Comité considere pertinentes para mejorar la Gestión de Riesgos.
    - Planes de contingencia y continuidad del negocio ante la materialización de eventos críticos.
    - Informe de los riesgos críticos identificados y gestionados.

4.1.5 Definición de Políticas de Seguridad de la Información.

La efectividad de los controles seleccionados depende de la definición de las políticas, normas y procedimientos de seguridad que serán generados acorde al plan de tratamiento de riesgos apropiado a los intereses y necesidades de la organización.

La Política de Seguridad de la Información debe considerar lo siguiente[7]:

- Estrategia de negocio
- Alcance y definición de la seguridad de la información
- Objetivos de la seguridad de la información
- Asignación de responsabilidades
- Compromiso de la alta dirección
- Política general de seguridad de la información

[7] (ISO/IEC 27002:2013, 2013) Numeral 5. Políticas de seguridad de la información.

- Políticas específicas de seguridad de la información

Las políticas específicas permiten profundizar la implementación de controles, las mismas que deben incluir:

- Organización de seguridad de la información
- Gestión de activos de información
- Control de acceso
- Controles criptográficos
- Seguridad de las comunicaciones
- Seguridad del personal
- Seguridad en las operaciones
- Seguridad física y medioambiental
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Relación con terceras partes
- Gestión de incidentes de seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento (requisitos legales y contractuales)

Las políticas deben ser:

- Comunicadas a todo el personal de la organización y las partes interesadas de forma que sea entendible y accesible al lector al que va dirigida.
- Revisadas en intervalos planificados a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

4.1.6 Auditoría de Cumplimiento del SGSI

La implementación de un SGSI debe ser evaluado mediante auditorías internas e independientes para determinar el nivel de avance en la implementación de controles y planes de acción determinados en el plan de tratamiento de riesgos y su cumplimiento de los requerimientos de la norma ISO/IEC 27001.

La ejecución de la auditoria debe considerar[8] que:

[8] Las consideraciones son tomadas de la norma ISO/IEC 27003 Anexo C

- La auditoría evalúe la efectividad y eficiencia de los controles implementados.
- No debe ser realizada por aquellas personas que estuvieron involucradas en la planificación y diseño de los objetivos de seguridad, por lo tanto, las unidades de la organización o personas que se encuentren fuera del alcance del SGSI deberían ser seleccionados por la alta dirección como auditores.
- De no contar con el recurso suficiente y experimentado, la auditoría debe ser encarga a expertos externos.
- El auditor cuente con las siguientes competencias para realizar el proceso de auditoria:
    - Planificación y ejecución de la auditoria.
    - Reporte de resultados determinados en base a evidencia.
    - Propuesta de acciones preventivas y correctivas.
- Se debe definir la documentación de procedimiento, responsabilidades de los auditores y los procesos para la auditoria.

4.2 Documentación

Parte de la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001, es la generación de documentos, cuya inexistencia daría lugar a no conformidades. La norma establece los siguientes documentos obligatorios de acuerdo a lo estipulado en cada cláusula:

- Alcance y objetivos del SGSI
- Política de la seguridad de la información
- Políticas, procedimientos y normativas de soporte del SGSI
- Metodología de gestión de riesgo
- Declaración de aplicabilidad del SGSI
- Plan de tratamiento de riesgos

Estos documentos forman parte de los entregables del proyecto de implementación del SGSI y son indispensables al momento de optar por la certificación de la empresa.

CAPITULO 5
IMPLEMENTACIÓN DEL SGSI, CASO DE ESTUDIO LOCKERS S.A.

En el presente capítulo se describe la implementación del Sistema de Gestión de Seguridad de la Información de la empresa Lockers S.A. acorde a la metodología descrita en el Capítulo 4.

5.1 Contextualización de la empresa

Lockers S.A. es una compañía que, desde hace más de 15 años, presta servicios de Control Físico y Digital de todo tipo de documentos, con un fuerte compromiso a sus clientes para entregarles, a precio competitivo, la mejor solución tecnológica hecha a la medida basada en sus necesidades.

La empresa brinda productos y servicios, con el "Valor Agregado Lockers", ayuda a sus clientes a lograr una importante disminución de costos y la consiguiente mejora en los niveles de productividad.

5.1.1 Misión

Proveer un servicio de cobertura regional, utilizando la mejor tecnología, obteniendo los mejores niveles de satisfacción del cliente y alcanzando el liderazgo en el sector.

Sus productos y servicios deben generar una importante reducción de costos en las operaciones de los clientes.

5.1.2 Visión

Ser el mejor socio de negocios de sus clientes, proveyendo soluciones empresariales en administración de documentos.

5.1.3 Procesos de Negocio

La empresa Lockers S.A. cuenta con una certificación ISO 9001:2008 en Gestión de Calidad, con un enfoque a procesos que implica la definición y gestión sistemática de

los procesos y sus interacciones, a fin de alcanzar los resultados previstos de acuerdo con la política de la calidad y la dirección estratégica de la organización.

En la Figura 3 se presenta el mapa de procesos de Lockers S.A., como una visión general de aquellos procesos que contribuyen a la eficacia y eficiencia de la organización en el logro de sus resultados previstos:

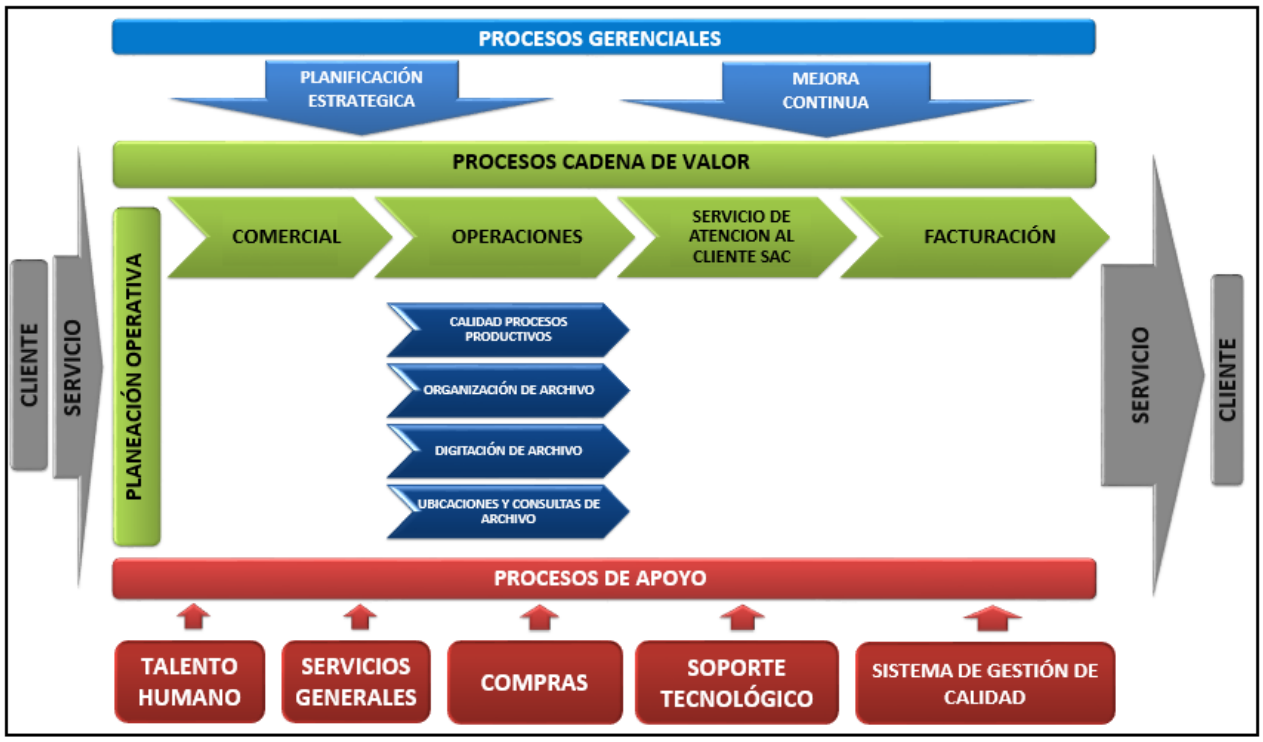

Figura 3 Mapa de procesos Lockers S.A

Fuente: (Lockers S.A. 2017)

El documento interno REG-PDA-SGC-ISO-MAPPRO-01 (Confidencial), especifica los procesos de la Figura 3 y su interacción. Se puede identificar el principal proceso operativo que crea valor y tiene impacto en el cliente final: “Custodia física y digital de documentos” sobre el que se enfocará la implementación del SGSI e involucra:

- Calidad de procesos productivos
- Organización del archivo
- Digitación del archivo
- Ubicaciones y consultas de archivo

5.1.4 Estructura organizacional

La empresa Lockers S.A presenta la estructura organizacional descrita en el Anexo 2, en la que se muestra los niveles jerárquicos de la institución. Como parte de la implementación del SGSI, se ha incorporado en la estructura organizacional al Comité de Seguridad de la Información y al Equipo de Planificación de Seguridad de la Información, conforme a la Figura 4.

5.1.5 Roles y responsabilidades

En la Tabla 14 se indican las personas asignadas para cada rol y responsabilidad en la implementación del SGSI de la empresa Lockers S.A.

Tabla 14
Descripción de personas asignadas

ROLES	PERSONAS ASIGNADAS
Alta Dirección	Ing. Erika Gallardo – Gerente General
Gerentes de línea	Ing. Giovanny Macancela – Gerente de TI Ing. José Toabanda – Gerente de Operación
Director de seguridad de la Información	Ing. Diego Donoso – Oficial de Seguridad de la Información.
Comité de seguridad de la información	Ing. Roberto Lema
Equipo de planificación de la Seguridad de la Información	Ing. Diego Donoso Ing. Roberto Lema
Parte interesada	Alta Dirección.
Administrador de Sistemas	Ing. Rubén Morales
Gestión de Riesgos	Ing. Roberto Lema Ing. Diego Donoso
Auditor	Ing. Roberto Lema Ing. Diego Donoso

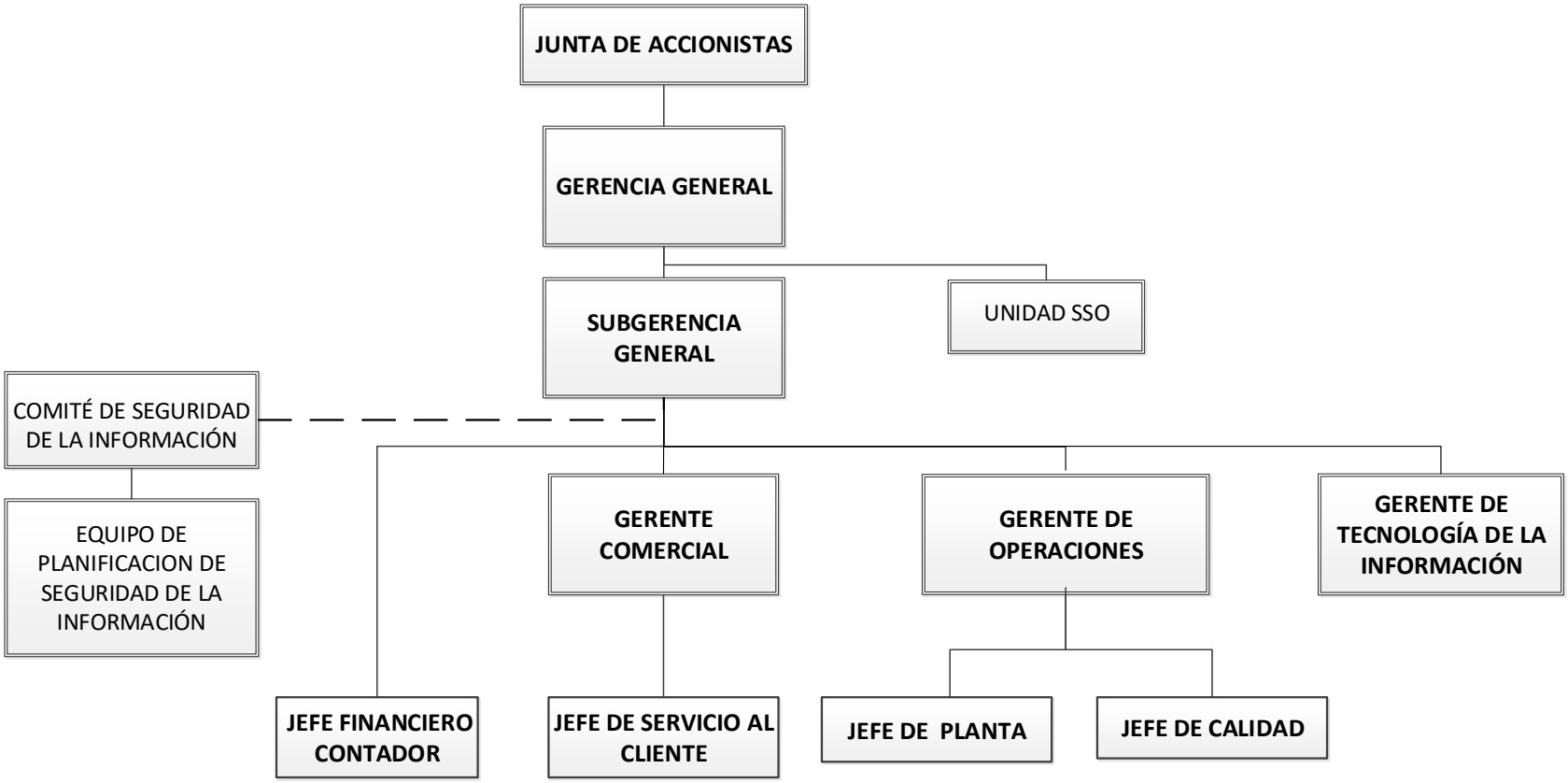

Figura 4 Estructura Organizacional Lockers S.A.
Fuente: (Lockers S.A. 2017)

5.2 Definición del Alcance y los Objetivos del SGSI

La empresa Lockers S.A. se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), con la finalidad de establecer un marco de confianza en el ejercicio de sus actividades como prestador de servicios de custodia física y digital de documentos; por lo que ha visto necesario definir su alcance considerando procesos y unidades organizativas relacionadas.

5.2.1 Alcance del SGSI

El Sistema de Gestión de Seguridad de la Información de Lockers S.A. se basa en un modelo por procesos que soportan el cumplimiento de la misión de la empresa. El alcance del SGSI comprende los sistemas de información que apoyan a las actividades relacionadas con el proceso de Custodia física y digital de documentos.

5.2.1.1 Procesos y Servicios

El proceso de Custodia física y digital de documentos es establecido como proceso principal y razón de ser de la empresa Lockers S.A. del que forman parte los procedimientos que se describen en la Tabla 15.

Tabla 15
Procesos críticos para la operación de Lockers S.A.

Proceso	Descripción
Procedimiento Gerencia de Operaciones	PRD-PCV-OPE-GOPS-03: (Confidencial) Está dirigido a la Gerencia de Operaciones como gestor directo, como también a los mandos medios como responsables de la vigilancia y supervisión de las estrategias operativas difundidas, que a su vez y conjuntamente se emiten los resultados mensuales de la gestión.
Procedimiento de Digitación, Digitalización, Indexación y Expurgo de Archivo	PRD-PCV-OPE-DIGI-04: (Confidencial) Garantiza la eficiencia y eficacia de producción de inventario de documentos digitados, digitalizados, indexados y expurgo; suministrados al sistema informático SADLE, satisfaciendo las necesidades de los clientes de acorde al MPA.
Procedimiento de Recepción y Organización de Archivo	PRD-PCV-OPE-ORG-06: (Confidencial) Garantiza la eficiencia y eficacia de producción de inventario de documentos digitados, digitalizados, indexados y expurgo; suministrados al sistema informático SADLE, satisfaciendo las necesidades de los clientes de acorde al MPA.

Fuente: (Lockers S.A. 2017)

5.2.1.2 Unidades Organizativas

Las unidades de negocio que conforman el alcance son:

- Gerencia General (*Alta Dirección*)
- Gerencia de Tecnologías de la Información (*Sistemas de Información*)
- Gerencia de Operaciones (*Implementación de Soluciones*)

5.2.1.3 Responsabilidades

a) El Comité de Seguridad de Información, es responsable de mantener y velar por el cumplimiento del presente documento.
b) La Alta Dirección de Lockers S.A es responsable de la decisión en el despliegue del SGSI a través de los procesos de la organización.
c) Todo el personal de Lockers S.A y los dueños de procesos involucrados en el SGSI son responsables por el cumplimiento de los requisitos del SGSI y políticas de seguridad dentro de su ámbito de acción y alcance.

5.2.1.4 Centro de actividades

Comprende las instalaciones físicas de Lockers S.A. ubicadas en Calderón - Vía a Marianas / Calle de los Fundadores, Lote Nº. 36 y Giovanni Calles, Quito – Ecuador.

5.2.1.5 Centro de procesamiento de Datos

La instalación de procesamiento y la infraestructura tecnológica que soporta los procesos del alcance, se encuentran dentro de las instalaciones físicas de la empresa.

5.2.1.6 Redes e Infraestructura de TI

El alcance cubre la infraestructura de comunicaciones con la que cuenta Lockers S.A. en sus instalaciones físicas para la prestación de servicios internos y externos.

5.2.2 Objetivos del SGSI

- OS1. Alinear la orientación estratégica de la seguridad de la información con la estrategia de negocio de Lockers S.A. salvaguardando los activos de información y los procesos de negocio.

- OS2. Afianzar la imagen de Lockers S.A como una empresa confiable que cumple con los requerimientos de seguridad de información mediante la implementación de controles de seguridad sobre los activos de información.
- OS3. Mejorar los procesos de custodia física y digital de documentos mediante la implementación de controles políticas y procedimientos de seguridad basados en la norma ISO/IEC 27001.
- OS4. Contribuir al logro de los objetivos del negocio gestionando los riesgos de seguridad de la información en los activos de información de la empresa.

El cumplimiento de los objetivos del SGSI se evalúa mediante métricas de seguridad de la información relacionadas con los procesos que hacen parte del alcance del SGSI, los activos de información y las partes interesadas en la organización. En la Tabla 16 se presenta las métricas relacionadas con cada uno de los objetivos del SGSI:

Tabla 16
Métricas de seguridad de la información por objetivos del SGSI

OBJETIVO	DESCRIPCIÓN	NO	MÉTRICA	TIPO
OS1	Métricas dirigidas a establecer el avance de la identificación y clasificación de los activos de información.	1	Número de procesos de negocio cuyos activos de información han sido identificados sobre el número total de procesos que hacen parte del SGSI	Porcentaje
		2	Numero de procesos de negocio cuyos activos de información han sido clasificados sobre el número total del procesos que hacen parte del alcance del SGSI	Porcentaje
OS2	Métricas dirigidas a establecer el avance de la implementación de controles de seguridad de la información y la concientización de seguridad de la	3	Número de sistemas de información que han sido asegurados mediante la implementación de controles sobre el número total de sistemas que hacen parte del alcance del SGSI.	Porcentaje

OBJETIVO	DESCRIPCIÓN	NO	MÉTRICA	TIPO
	información a las partes interesadas y al personal involucrado en los procesos de negocio.	4	Número de dueños de proceso sensibilizados en buenas prácticas de seguridad de la información sobre el número total de dueño de procesos que hacen parte del alcance del SGSI.	Porcentaje
		5	Número de empleados que han recibido entrenamiento en seguridad de la información sobre el número total de empleados que participan en los procesos de negocio.	Porcentaje
OS3	Métricas dirigidas a establecer el avance de la implementación de controles, políticas y procedimientos de seguridad de la información como mejora en los procesos de negocio.	6	Número de controles de seguridad implementados sobre el número total de controles de seguridad seleccionados.	Porcentaje
		7	Número de políticas de seguridad implementados sobre el número total de políticas de seguridad seleccionados.	Porcentaje
		8	Número de procedimientos de seguridad implementados sobre el número total de procedimientos de seguridad seleccionados.	Porcentaje
OS4	Métricas que permiten conocer el avance de la ejecución del análisis de riesgos sobre los activos de información.	9	Número de activos de información a los que se ha realizado el análisis de riesgos.	Número
		10	Número de activos de información que tiene riesgos con clasificación inaceptable	Número

5.3 Identificación de activos

En relación al Alcance del SGSI, se identifican y clasifican los activos de información relacionados al proceso de “Custodia física y digital de documentos”; que sirven de insumo para la Gestión de Riesgo.

5.3.1 Inventario de los activos

5.3.1.1 Activos Primarios

Como activos primarios se han considerado y catalogado los procesos que se describen en la Tabla 17.

Tabla 17
Activos Primarios

MACRO PROCESO	PROCESO	ID	PROPIETARIO	RESPONSABLE
Custodia física y digital de documentos	Procedimiento de Gerencia de Operaciones	AP1	Gerencia de Operaciones	Jefe de Calidad
	Procedimiento de Digitación, Digitalización, Indexación y Expurgo de Archivo	AP2	Gerencia de Operaciones	Jefe de Calidad
	Procedimiento de Recepción y Organización de Archivo	AP3	Gerencia de Operaciones	Jefe de Calidad

5.3.1.2 Activos de Soporte

Sobre los activos primarios se identifican y tipifican los activos de soporte con sus propietarios y responsables que agregan valor, según se describe en la Tabla 6.

Tabla 18
Activos de soporte para los activos primarios

ID ACTIVO	PROCESO	NOMBRE DEL ACTIVO	TIPO DE ACTIVO	PROPIETARIO	RESPONSABLE
AS1	AP1, AP2	Sistema Lockers y las bases de datos que provean su servicio.	Software	Gerencia de Operaciones	Técnico Desarrollador
AS2	AP1, AP2	Sistema Docuware y las bases de datos que provean su servicio.	Software	Gerencia de Operaciones	Técnico Desarrollador
AS3	AP1, AP3	Sistema GLPI y las bases de datos que provean su servicio.	Software	Gerencia de Operaciones	Técnico Help Desk

ID ACTIVO	PROCESO	NOMBRE DEL ACTIVO	TIPO DE ACTIVO	PROPIETARIO	RESPONSABLE
AS4	AP1	Directorio Activo	Software	Gerencia de TI	Técnico Help Desk
AS5	AP1, AP2, AP3	Correo electrónico	Software	Gerencia de TI	Técnico Help Desk
AS6	AP2, AP3	Servicio DHCP	Software	Gerencia de TI	Técnico Help Desk
AS7	AP2, AP3	Servicio Antivirus	Software	Gerencia de TI	Técnico Help Desk
AS8	AP2, AP3	Servicio Web Proxy	Redes	Gerencia de TI	Gerente TI
AS9	AP1	Servicio VPN	Redes	Gerencia de TI	Gerente TI
AS10	AP1, AP2, AP3	Servidor de archivos	Software	Gerencia de Operaciones - Administrativa Financiera	Gerente TI
AS11	AP1, AP2, AP3	Dispositivos de comunicaciones (Switches, routers, access points)	Redes	Gerencia de TI	Técnico Help Desk - Gerente TI
AS12	AP1, AP2, AP3	Firewall perimetral	Redes	Gerencia de TI	Gerente TI
AS13	AP2	Servicio de Conexiones de Escritorio Remoto	Software	Gerencia de Operaciones	Técnico Help Desk
AS14	AP3	Impresora de etiquetas	Hardware	Gerencia de Operaciones	Supervisor Digitación
AS15	AP1, AP2, AP3	Servidores de respaldos	Hardware	Gerencia de TI	Técnico Help Desk
AS16	AP2, AP3	Terminales de usuarios operativos conectados al dominio LOCKERS.COM	Hardware	Gerencia de Operaciones	Usuarios Gerencia Operaciones
AS17	AP1	Terminales de usuarios directivos	Hardware	Gerentes	Gerentes
AS18	AP1, AP2, AP3	Personal de la gerencia de TI	Personal	Gerencia de TI	Usuarios Gerencia TI
AS19	AP1, AP2, AP3	Personal de la gerencia de Operaciones	Personal	Gerencia de Operaciones	Gerente de Operaciones
AS20	AP3	Personal de Servicio al Cliente	Personal	Gerencia Comercial	Gerente de Operaciones
AS21	AP1, AP2, AP3	Servidores físicos	Hardware	Gerencia de TI	Gerente de TI

5.3.2 Valoración de los activos

Identificados los activos, se realiza su valoración cualitativa en base del promedio de criterios de cada supervisor de área, así como del gerente de operaciones.

En la Tabla 19 y Tabla 20 se utiliza los criterios establecidos en la Tabla 8, para determinar el nivel de impacto que puede tener la degradación de cada activo del proceso de control de documentación física y digital en Lockers S.A. El valor más alto obtenido se constituye como el valor del activo de la organización:

Tabla 19

Valoración de los activos primarios

ID ACTIVO	CONFIDENCIALIDAD		INTEGRIDAD		DISPONIBILIDAD		VALOR DEL ACTIVO
	IMPACTO	VALOR	IMPACTO	VALOR	IMPACTO	VALOR	
AP1	Crítico	5	Alto	4	Crítico	5	Crítico
AP2	Alto	4	Alto	4	Alto	4	Alto
AP3	Alto	4	Alto	4	Alto	4	Alto

Tabla 20

Valoración de los activos de soporte

ID ACTIVO	CONFIDENCIALIDAD		INTEGRIDAD		DISPONIBILIDAD		VALOR DEL ACTIVO
	IMPACTO	VALOR	IMPACTO	VALOR	IMPACTO	VALOR	
AS1	Crítico	5	Crítico	5	Crítico	5	Crítico
AS2	Alto	4	Medio	3	Medio	3	Alto
AS3	Bajo	2	Alto	4	Insignificante	1	Alto
AS4	Bajo	2	Insignificante	1	Medio	3	Medio
AS5	Alto	4	Medio	3	Medio	3	Alto
AS6	Insignificante	1	Insignificante	1	Medio	3	Medio
AS7	Insignificante	1	Insignificante	1	Insignificante	1	Insignificante
AS8	Alto	4	Medio	3	Medio	3	Alto

ID ACTIVO	CONFIDENCIALIDAD		INTEGRIDAD		DISPONIBILIDAD		VALOR DEL ACTIVO
	IMPACTO	VALOR	IMPACTO	VALOR	IMPACTO	VALOR	
AS9	Bajo	2	Bajo	2	Medio	3	Medio
AS10	Crítico	5	Alto	4	Crítico	5	Crítico
AS11	Medio	3	Medio	3	Medio	3	Medio
AS12	Alto	4	Alto	4	Medio	3	Alto
AS13	Alto	4	Medio	3	Alto	4	Alto
AS14	Insignificante	1	Insignificante	1	Medio	3	Medio
AS15	Medio	3	Medio	3	Medio	3	Medio
AS16	Alto	4	Alto	4	Alto	4	Alto
AS17	Alto	4	Alto	4	Alto	4	Alto
AS18	Crítico	5	Medio	3	Medio	3	Crítico
AS19	Crítico	5	Alto	4	Alto	4	Crítico
AS20	Alto	4	Medio	3	Alto	4	Alto
AS21	Alto	4	Alto	4	Crítico	5	Crítico

5.3.3 Clasificación de activos

Una vez obtenida la valoración de cada activo, en la Tabla 21 y Tabla 22, se clasifican los activos en base del grado de confidencialidad, integridad y disponibilidad descrito en la Tabla 9:

Tabla 21
Clasificación de los activos primarios

ID ACTIVO	CLASIFICACIÓN
AP1	Confidencial
AP2	Confidencial
AP3	Confidencial

Tabla 22
Clasificación de los activos de soporte

ID ACTIVO	CLASIFICACIÓN
AS1	Confidencial
AS2	Confidencial
AS3	Uso Interno
AS4	Uso Interno
AS5	Confidencial
AS6	Pública
AS7	Pública
AS8	Confidencial
AS9	Uso Interno
AS10	Confidencial
AS11	Uso Interno
AS12	Confidencial
AS13	Confidencial
AS14	Pública
AS15	Uso Interno
AS16	Confidencial
AS17	Confidencial
AS18	Confidencial
AS19	Confidencial
AS20	Confidencial
AS21	Confidencial

El inventario obtenido tanto para los activos primarios y de soporte se encuentra en el Anexo 4.

5.4 Gestión de Riesgos

El proceso de gestión de riesgos de seguridad de la información se realiza sobre los activos de información del proceso de Custodia de Archivos Físicos y Digitales identificados en la Tabla 18.

5.4.1 Contextualización, objetivo y alcance

En la Tabla 23, se detalla los escenarios de riesgo e identifican sus amenazas conforme el medio de operación de la empresa Lockers S.A. La mayoría de ellos se encuentran tipificados en la norma ISO/IEC 27005:2012:

Tabla 23
Escenarios de Riesgo

ESCENARIO	AMENAZA
Compromiso de las funciones	Abuso de derechos
	Acceso no autorizado
	Negación de acciones
	Error en el uso
	Escucha encubierta
	Espionaje remoto
	Manipulación de registros y sistemas de información
Acciones no autorizadas	Daño por tercera parte
	Elevación de privilegios
Falta de acciones gerenciales	Gestión ineficiente de Seguridad de la Información
	Chantaje
	Asalto a un empleado
	Fraude y hurto
	Ingreso de datos falsos y corruptos
	Observar información reservada
	Robo de información
	Uso inadecuado del computador
	Venta de información personal
Eventos naturales	Inundación
Fallas técnicas	Mal funcionamiento del equipo
Pérdida de los servicios esenciales	Pérdida de suministro de energía

5.4.1.1 Objetivo

Gestionar los riesgos de seguridad de la información asociados a los activos de información del proceso de Custodia de Archivos Físicos y Digitales de la empresa Lockers S.A.

5.4.1.2 Alcance

La gestión del riesgo de seguridad de la información se realiza en el proceso de Custodia de Archivos Físicos y Digitales de la empresa Lockers S.A.

5.4.2 Valoración del riesgo

5.4.2.1 Análisis del Riesgo

Una vez definidos los escenarios, se identifica las amenazas existentes, así como las vulnerabilidades que podrían ser explotadas para cada activo de información de la Tabla 18, con lo que se construye la Tabla 24.

Tabla 24
Identificación de amenazas y vulnerabilidades en activos

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
Sistema Lockers y las bases de datos que provean su servicio.	AS1	AS1R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS1R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS1R3	Daño por tercera parte	Una entidad externa ocasiona daños
		AS1R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS1R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS1R6	Error en el uso	Afectación no intencional sobre el servicio
		AS1R7	Escucha encubierta	Lectura de información no autorizada

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS1R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS1R9	Gestión ineficiente de Seguridad de la Información	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS1R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
Sistema Docuware y las bases de datos que provean su servicio.	AS2	AS2R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS2R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS2R3	Daño por tercera parte	Una entidad externa ocasiona daños
		AS2R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS2R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS2R6	Error en el uso	Afectación no intencional sobre el servicio
		AS2R7	Escucha encubierta	Lectura de información no autorizada
		AS2R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS2R9	Gestión ineficiente de Seguridad de la Información	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS2R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
Sistema GLPI y las bases de datos que provean su servicio.	AS3	AS3R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS3R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS3R3	Daño por tercera parte	Una entidad externa ocasiona daños

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS3R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS3R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS3R6	Error en el uso	Afectación no intencional sobre el servicio
		AS3R7	Escucha encubierta	Lectura de información no autorizada
		AS3R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS3R9	Gestión ineficiente de Seguridad de la Información	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS3R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
Directorio Activo	AS4	AS4R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS4R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS4R3	Daño por tercera parte	Una entidad externa ocasiona daños
		AS4R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS4R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS4R6	Error en el uso	Afectación no intencional sobre el servicio
		AS4R7	Escucha encubierta	Lectura de información no autorizada
		AS4R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS4R9	Gestión ineficiente de Seguridad de la Información	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS4R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
Correo electrónico	AS5	AS5R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS5R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS5R3	Daño por tercera parte	Una entidad externa ocasiona daños
		AS5R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS5R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS5R6	Error en el uso	Afectación no intencional sobre el servicio
		AS5R7	Escucha encubierta	Lectura de información no autorizada
		AS5R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS5R9	Gestión ineficiente de Seguridad de la Información	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS5R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
Servicio DHCP	AS6	AS6R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS6R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS6R3	Daño por tercera parte	Una entidad externa ocasiona daños
		AS6R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS6R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS6R6	Error en el uso	Afectación no intencional sobre el servicio

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS6R7	Escucha encubierta	Lectura de información no autorizada
		AS6R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS6R9	Gestión ineficiente de Seguridad de la Información	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS6R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
Servicio Antivirus	AS7	AS7R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS7R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS7R3	Daño por tercera parte	Una entidad externa ocasiona daños
		AS7R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS7R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS7R6	Error en el uso	Afectación no intencional sobre el servicio
		AS7R7	Escucha encubierta	Lectura de información no autorizada
		AS7R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS7R9	Gestión ineficiente de Seguridad de la Información	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS7R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
Servicio Web Proxy	AS8	AS8R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS8R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS8R3	Daño de externos	Una entidad externa ocasiona daños
		AS8R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS8R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS8R6	Error en el uso	Afectación no intencional sobre el servicio
		AS8R7	Escucha encubierta	Lectura de información no autorizada mediante técnicas de ataques informáticos como Sniffers
		AS8R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS8R9	Gestión ineficiente de seguridad por parte de TI	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS8R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
Servicio VPN	AS9	AS9R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS9R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS9R3	Daño por tercera parte	Una entidad externa ocasiona daños
		AS9R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS9R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS9R6	Error en el uso	Afectación no intencional sobre el servicio
		AS9R7	Escucha encubierta	Lectura de información no autorizada
		AS9R8	Espionaje remoto	Obtención encubierta de datos o información confidencial

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS9R9	Gestión ineficiente de Seguridad de la Información	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS9R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
Servidor de archivos	AS10	AS10R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS10R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS10R3	Daño de externos	Una entidad externa ocasiona daños
		AS10R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS10R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS10R6	Error en el uso	Afectación no intencional sobre el servicio
		AS10R7	Escucha encubierta	Lectura de información no autorizada mediante técnicas de ataques informáticos como Sniffers
		AS10R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS10R9	Gestión ineficiente de seguridad por parte de TI	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS10R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
		AS10R11	Robo de información	Robo de información
Dispositivos de comunicaciones	AS11	AS11R1	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS11R2	Error en el uso	Afectación no intencional sobre el servicio

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS11R3	Escucha encubierta	Lectura de información no autorizada mediante técnicas de ataques informáticos como Sniffers
		AS11R4	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
Firewall perimetral	AS12	AS12R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS12R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS12R3	Daño de externos	Una entidad externa ocasiona daños
		AS12R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS12R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS12R6	Error en el uso	Afectación no intencional sobre el servicio
		AS12R7	Escucha encubierta	Lectura de información no autorizada mediante técnicas de ataques informáticos como Sniffers
		AS12R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS12R9	Gestión ineficiente de seguridad por parte de TI	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS12R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
		AS12R11	Robo de información	Robo de información
Servicio de Conexiones de Escritorio Remoto	AS13	AS13R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS13R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS13R3	Daño de externos	Una entidad externa ocasiona daños
		AS13R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS13R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS13R6	Error en el uso	Afectación no intencional sobre el servicio
		AS13R7	Escucha encubierta	Lectura de información no autorizada mediante técnicas de ataques informáticos como Sniffers
		AS13R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS13R9	Gestión ineficiente de seguridad por parte de TI	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS13R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
		AS13R11	Robo de información	Robo de información
Impresora de etiquetas	AS14	AS14R1	Destrucción del equipo o los medios	Un usuario manipula incorrectamente el equipo y como consecuencia lo destruye
		AS14R2	Manipulación con software	Un usuario opera incorrectamente el software y compromete la disponibilidad del equipo
		AS14R3	Falla del equipo	El equipo se bloquea por corrupción de drivers
		AS14R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
Servidores de respaldos	AS15	AS15R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS15R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS15R3	Daño de externos	Una entidad externa ocasiona daños

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS15R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS15R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS15R6	Error en el uso	Afectación no intencional sobre el servicio
		AS15R7	Escucha encubierta	Lectura de información no autorizada mediante técnicas de ataques informáticos como Sniffers
		AS15R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS15R9	Gestión ineficiente de seguridad por parte de TI	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS15R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
		AS15R11	Robo de información	Robo de información
Terminales de usuarios operativos conectados al dominio LOCKERS.COM	AS16	AS16R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS16R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS16R3	Daño de externos	Una entidad externa ocasiona daños
		AS16R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS16R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS16R6	Error en el uso	Afectación no intencional sobre el servicio
		AS16R7	Escucha encubierta	Lectura de información no autorizada mediante técnicas de ataques informáticos como Sniffers
		AS16R8	Espionaje remoto	Obtención encubierta de datos o información confidencial

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS16R9	Gestión ineficiente de seguridad por parte de TI	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS16R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
		AS16R11	Robo de información	Robo de información
Terminales de usuarios directivos	AS17	AS17R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos
		AS17R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información
		AS17R3	Daño de externos	Una entidad externa ocasiona daños
		AS17R4	Negación de acciones	Persona no tiene acceso para ejecutar acciones operativas
		AS17R5	Elevación de privilegios	Una persona obtiene nuevos permisos no autorizados
		AS17R6	Error en el uso	Afectación no intencional sobre el servicio
		AS17R7	Escucha encubierta	Lectura de información no autorizada mediante técnicas de ataques informáticos como Sniffers
		AS17R8	Espionaje remoto	Obtención encubierta de datos o información confidencial
		AS17R9	Gestión ineficiente de seguridad por parte de TI	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información
		AS17R10	Manipulación de registros y sistemas de información	Pérdida de integridad de la información
		AS17R11	Robo de información	Robo de información
Personal de la gerencia de TI	AS18	AS18R1	Asalto a un empleado	Un usuario es asaltado y despojado de su computador y/o medio de almacenamiento

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS18R2	Chantaje	Un usuario sabotea sistemas o hace copias de información no autorizada para eliminarla de los activos y luego pedir rescate por la información
		AS18R3	Observar información reservada	Una persona observa lo que otro usuario está realizando con carácter de crítico y clasificado
		AS18R4	Uso inadecuado del computador	Un usuario no opera el equipo de cómputo de acuerdo a las especificaciones ni sugerencias del personal de tecnologías
		AS18R5	Fraude y hurto	Una persona roba información de la empresa previo a su separación de la misma
Personal de la gerencia de Operaciones	AS19	AS19R1	Asalto a un empleado	Un usuario es asaltado y despojado de su computador y/o medio de almacenamiento
		AS19R2	Chantaje	Un usuario sabotea sistemas o hace copias de información no autorizada para eliminarla de los activos y luego pedir rescate por la información
		AS19R3	Observar información reservada	Una persona observa lo que otro usuario está realizando con carácter de crítico y clasificado
		AS19R4	Uso inadecuado del computador	Un usuario no opera el equipo de cómputo de acuerdo a las especificaciones ni sugerencias del personal de tecnologías
		AS19R5	Fraude y hurto	Una persona roba información de la empresa previo a su separación de la misma

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS19R6	Ingreso de datos falsos o corruptos	Un usuario ingresa datos a los sistemas de la empresa con el fin de alterar los procesos ya sea por obtener puntajes altos en evaluaciones o por justificar trabajo que no ha realizado
		AS19R7	Venta de información personal	Competencia sucia
Personal de Servicio al Cliente	AS20	AS20R1	Chantaje	Un usuario sabotea sistemas o hace copias de información no autorizada para eliminarla de los activos y luego pedir rescate por la información
		AS20R2	Observar información reservada	Una persona observa lo que otro usuario está realizando con carácter de crítico y clasificado
		AS20R3	Uso inadecuado del computador	Un usuario no opera el equipo de cómputo de acuerdo a las especificaciones ni sugerencias del personal de tecnologías
		AS20R4	Fraude y hurto	Una persona roba información de la empresa previo a su separación de la misma
		AS20R5	Ingreso de datos falsos o corruptos	Un usuario ingresa datos a los sistemas de la empresa con el fin de alterar los procesos ya sea por obtener puntajes altos en evaluaciones o por justificar trabajo que no ha realizado
		AS20R6	Venta de información personal	Competencia sucia
Servidores físicos	AS21	AS21R1	Inundación	Lluvias torrenciales y prolongadas pueden causar inundación dentro del Data Center
		AS21R2	Falla en el sistema de suministro de agua o de aire acondicionado	Mal funcionamiento del equipo de los equipos de aire acondicionado

Activo	ID Activo	ID Riesgo	Amenaza	Vulnerabilidad
		AS21R3	Pérdida de suministro de energía	El sector no garantiza estabilidad ni continuidad de suministro eléctrico. Apagones y variaciones de voltaje en la red eléctrica desabastecen de energía
		AS21R4	Mal funcionamiento del equipo	Falla en el hardware provocado principalmente por tener equipos obsoletos

5.4.2.2 Evaluación del Riesgo

Una vez obtenidos los criterios de probabilidad e impacto, se realiza el cálculo del riesgo inherente aplicando el criterio $V_R = V_P * V_I$.

Los resultados obtenidos se presentan en la Tabla 25.

Tabla 25
Evaluación del Riesgo

ACTIVO	ID ACTIVO	ID RIESGO	CÁLCULO DEL RIESGO INHERENTE
Sistema Lockers y las bases de datos que provean su servicio.	AS1	AS1R1	8
		AS1R2	8
		AS1R3	5
		AS1R4	4
		AS1R5	4
		AS1R6	8
		AS1R7	3
		AS1R8	3
		AS1R9	12
		AS1R10	6
Sistema Docuware y las bases de datos que provean su servicio.	AS2	AS2R1	8
		AS2R2	4
		AS2R3	4
		AS2R4	3
		AS2R5	8
		AS2R6	9
		AS2R7	3

ACTIVO	ID ACTIVO	ID RIESGO	CÁLCULO DEL RIESGO INHERENTE
		AS2R8	4
		AS2R9	12
		AS2R10	2
Sistema GLPI y las bases de datos que provean su servicio.	AS3	AS3R1	8
		AS3R2	4
		AS3R3	4
		AS3R4	3
		AS3R5	8
		AS3R6	6
		AS3R7	3
		AS3R8	4
		AS3R9	12
		AS3R10	2
Directorio Activo	AS4	AS4R1	6
		AS4R2	3
		AS4R3	4
		AS4R4	3
		AS4R5	4
		AS4R6	8
		AS4R7	3
		AS4R8	3
		AS4R9	8
		AS4R10	3
Correo electrónico	AS5	AS5R1	4
		AS5R2	4
		AS5R3	4
		AS5R4	6
		AS5R5	4
		AS5R6	8
		AS5R7	3
		AS5R8	4
		AS5R9	8
		AS5R10	2
Servicio DHCP	AS6	AS6R1	2
		AS6R2	2
		AS6R3	2
		AS6R4	3

ACTIVO	ID ACTIVO	ID RIESGO	CÁLCULO DEL RIESGO INHERENTE
		AS6R5	2
		AS6R6	2
		AS6R7	2
		AS6R8	2
		AS6R9	4
		AS6R10	2
Servicio Antivirus	AS7	AS7R1	1
		AS7R2	1
		AS7R3	1
		AS7R4	2
		AS7R5	1
		AS7R6	2
		AS7R7	1
		AS7R8	1
		AS7R9	2
		AS7R10	1
Servicio Web Proxy	AS8	AS8R1	6
		AS8R2	3
		AS8R3	3
		AS8R4	6
		AS8R5	3
		AS8R6	3
		AS8R7	2
		AS8R8	2
		AS8R9	6
		AS8R10	2
Servicio VPN	AS9	AS9R1	3
		AS9R2	3
		AS9R3	2
		AS9R4	3
		AS9R5	2
		AS9R6	3
		AS9R7	2
		AS9R8	2
		AS9R9	6
		AS9R10	2
Servidor de archivos	AS10	AS10R1	12

ACTIVO	ID ACTIVO	ID RIESGO	CÁLCULO DEL RIESGO INHERENTE
		AS10R2	6
		AS10R3	5
		AS10R4	6
		AS10R5	6
		AS10R6	9
		AS10R7	4
		AS10R8	4
		AS10R9	12
		AS10R10	3
		AS10R11	15
Dispositivos de comunicaciones (Switches, routers, access points)	AS11	AS11R1	3
		AS11R2	6
		AS11R3	3
		AS11R4	2
Firewall perimetral	AS12	AS12R1	8
		AS12R2	3
		AS12R3	3
		AS12R4	9
		AS12R5	4
		AS12R6	6
		AS12R7	4
		AS12R8	4
		AS12R9	8
		AS12R10	2
		AS12R11	4
Servicio de Conexiones de Escritorio Remoto	AS13	AS13R1	8
		AS13R2	3
		AS13R3	3
		AS13R4	6
		AS13R5	3
		AS13R6	6
		AS13R7	3
		AS13R8	3
		AS13R9	8
		AS13R10	2
		AS13R11	3
Impresora de etiquetas	AS14	AS14R1	8

ACTIVO	ID ACTIVO	ID RIESGO	CÁLCULO DEL RIESGO INHERENTE
		AS14R2	6
		AS14R3	6
		AS14R4	3
Servidores de respaldos	AS15	AS15R1	3
		AS15R2	4
		AS15R3	4
		AS15R4	3
		AS15R5	4
		AS15R6	3
		AS15R7	4
		AS15R8	3
		AS15R9	6
		AS15R10	4
		AS15R11	5
Terminales de usuarios operativos conectados al dominio LOCKERS.COM	AS16	AS16R1	3
		AS16R2	6
		AS16R3	3
		AS16R4	6
		AS16R5	3
		AS16R6	9
		AS16R7	3
		AS16R8	3
		AS16R9	9
		AS16R10	2
		AS16R11	10
Terminales de usuarios directivos	AS17	AS17R1	12
		AS17R2	12
		AS17R3	12
		AS17R4	6
		AS17R5	2
		AS17R6	8
		AS17R7	12
		AS17R8	12
		AS17R9	12
		AS17R10	2
		AS17R11	16
Personal de la gerencia de TI	AS18	AS18R1	10

ACTIVO	ID ACTIVO	ID RIESGO	CÁLCULO DEL RIESGO INHERENTE
		AS18R2	10
		AS18R3	8
		AS18R4	4
		AS18R5	8
Personal de la gerencia de Operaciones	AS19	AS19R1	10
		AS19R2	15
		AS19R3	8
		AS19R4	8
		AS19R5	15
		AS19R6	12
		AS19R7	1
Personal de Servicio al Cliente	AS20	AS20R1	10
		AS20R2	8
		AS20R3	8
		AS20R4	15
		AS20R5	12
		AS20R6	1
Servidores físicos	AS21	AS21R1	10
		AS21R2	8
		AS21R3	16
		AS21R4	12

5.4.3 Tratamiento del riesgo

Identificado el riesgo inherente, se define el tratamiento para todos los riesgos resultantes según la Tabla 11 y se construye la Tabla 26.

Tabla 26
Determinación del tratamiento según zonificación

ID Riesgo	CALCULO DEL RIESGO INHERENTE	TRATAMIENTO
AS1R1	8	TRANSFERIR
AS1R2	8	TRANSFERIR
AS1R3	5	TRANSFERIR
AS1R4	4	ACEPTAR
AS1R5	4	ACEPTAR
AS1R6	8	TRANSFERIR

ID Riesgo	CALCULO DEL RIESGO INHERENTE	TRATAMIENTO
AS1R7	3	ACEPTAR
AS1R8	3	ACEPTAR
AS1R9	12	REDUCIR
AS1R10	6	TRANSFERIR
AS2R1	8	TRANSFERIR
AS2R2	4	ACEPTAR
AS2R3	4	ACEPTAR
AS2R4	3	ACEPTAR
AS2R5	8	TRANSFERIR
AS2R6	9	TRANSFERIR
AS2R7	3	ACEPTAR
AS2R8	4	ACEPTAR
AS2R9	12	REDUCIR
AS2R10	2	ACEPTAR
AS3R1	8	TRANSFERIR
AS3R2	4	ACEPTAR
AS3R3	4	ACEPTAR
AS3R4	3	ACEPTAR
AS3R5	8	TRANSFERIR
AS3R6	6	TRANSFERIR
AS3R7	3	ACEPTAR
AS3R8	4	ACEPTAR
AS3R9	12	REDUCIR
AS3R10	2	ACEPTAR
AS4R1	6	TRANSFERIR
AS4R2	3	ACEPTAR
AS4R3	4	ACEPTAR
AS4R4	3	ACEPTAR
AS4R5	4	ACEPTAR
AS4R6	8	TRANSFERIR
AS4R7	3	ACEPTAR
AS4R8	3	ACEPTAR
AS4R9	8	TRANSFERIR
AS4R10	3	ACEPTAR
AS5R1	4	ACEPTAR
AS5R2	4	ACEPTAR
AS5R3	4	ACEPTAR
AS5R4	6	TRANSFERIR
AS5R5	4	ACEPTAR
AS5R6	8	TRANSFERIR

ID Riesgo	CALCULO DEL RIESGO INHERENTE	TRATAMIENTO
AS5R7	3	ACEPTAR
AS5R8	4	ACEPTAR
AS5R9	8	TRANSFERIR
AS5R10	2	ACEPTAR
AS6R1	2	ACEPTAR
AS6R2	2	ACEPTAR
AS6R3	2	ACEPTAR
AS6R4	3	ACEPTAR
AS6R5	2	ACEPTAR
AS6R6	2	ACEPTAR
AS6R7	2	ACEPTAR
AS6R8	2	ACEPTAR
AS6R9	4	ACEPTAR
AS6R10	2	ACEPTAR
AS7R1	1	ACEPTAR
AS7R2	1	ACEPTAR
AS7R3	1	ACEPTAR
AS7R4	2	ACEPTAR
AS7R5	1	ACEPTAR
AS7R6	2	ACEPTAR
AS7R7	1	ACEPTAR
AS7R8	1	ACEPTAR
AS7R9	2	ACEPTAR
AS7R10	1	ACEPTAR
AS8R1	6	TRANSFERIR
AS8R2	3	ACEPTAR
AS8R3	3	ACEPTAR
AS8R4	6	TRANSFERIR
AS8R5	3	ACEPTAR
AS8R6	3	ACEPTAR
AS8R7	2	ACEPTAR
AS8R8	2	ACEPTAR
AS8R9	6	TRANSFERIR
AS8R10	2	ACEPTAR
AS9R1	3	ACEPTAR
AS9R2	3	ACEPTAR
AS9R3	2	ACEPTAR
AS9R4	3	ACEPTAR
AS9R5	2	ACEPTAR
AS9R6	3	ACEPTAR

ID Riesgo	CALCULO DEL RIESGO INHERENTE	TRATAMIENTO
AS9R7	2	ACEPTAR
AS9R8	2	ACEPTAR
AS9R9	6	TRANSFERIR
AS9R10	2	ACEPTAR
AS10R1	12	REDUCIR
AS10R2	6	TRANSFERIR
AS10R3	5	TRANSFERIR
AS10R4	6	TRANSFERIR
AS10R5	6	TRANSFERIR
AS10R6	9	TRANSFERIR
AS10R7	4	ACEPTAR
AS10R8	4	ACEPTAR
AS10R9	12	REDUCIR
AS10R10	3	ACEPTAR
AS10R11	15	REDUCIR
AS11R1	3	ACEPTAR
AS11R2	6	TRANSFERIR
AS11R3	3	ACEPTAR
AS11R4	2	ACEPTAR
AS12R1	8	TRANSFERIR
AS12R2	3	ACEPTAR
AS12R3	3	ACEPTAR
AS12R4	9	TRANSFERIR
AS12R5	4	ACEPTAR
AS12R6	6	TRANSFERIR
AS12R7	4	ACEPTAR
AS12R8	4	ACEPTAR
AS12R9	8	TRANSFERIR
AS12R10	2	ACEPTAR
AS12R11	4	ACEPTAR
AS13R1	8	TRANSFERIR
AS13R2	3	ACEPTAR
AS13R3	3	ACEPTAR
AS13R4	6	TRANSFERIR
AS13R5	3	ACEPTAR
AS13R6	6	TRANSFERIR
AS13R7	3	ACEPTAR
AS13R8	3	ACEPTAR
AS13R9	8	TRANSFERIR
AS13R10	2	ACEPTAR

ID Riesgo	CALCULO DEL RIESGO INHERENTE	TRATAMIENTO
AS13R11	3	ACEPTAR
AS14R1	8	TRANSFERIR
AS14R2	6	TRANSFERIR
AS14R3	6	TRANSFERIR
AS14R4	3	ACEPTAR
AS15R1	3	ACEPTAR
AS15R2	4	ACEPTAR
AS15R3	4	ACEPTAR
AS15R4	3	ACEPTAR
AS15R5	4	ACEPTAR
AS15R6	3	ACEPTAR
AS15R7	4	ACEPTAR
AS15R8	3	ACEPTAR
AS15R9	6	TRANSFERIR
AS15R10	4	ACEPTAR
AS15R11	5	TRANSFERIR
AS16R1	3	ACEPTAR
AS16R2	6	TRANSFERIR
AS16R3	3	ACEPTAR
AS16R4	6	TRANSFERIR
AS16R5	3	ACEPTAR
AS16R6	9	TRANSFERIR
AS16R7	3	ACEPTAR
AS16R8	3	ACEPTAR
AS16R9	9	TRANSFERIR
AS16R10	2	ACEPTAR
AS16R11	10	TRANSFERIR
AS17R1	12	REDUCIR
AS17R2	12	REDUCIR
AS17R3	12	REDUCIR
AS17R4	6	TRANSFERIR
AS17R5	2	ACEPTAR
AS17R6	8	TRANSFERIR
AS17R7	12	REDUCIR
AS17R8	12	REDUCIR
AS17R9	12	REDUCIR
AS17R10	2	ACEPTAR
AS17R11	16	EVITAR
AS18R1	10	TRANSFERIR
AS18R2	10	TRANSFERIR

ID Riesgo	CALCULO DEL RIESGO INHERENTE	TRATAMIENTO
AS18R3	8	TRANSFERIR
AS18R4	4	ACEPTAR
AS18R5	8	TRANSFERIR
AS19R1	10	TRANSFERIR
AS19R2	15	REDUCIR
AS19R3	8	TRANSFERIR
AS19R4	8	TRANSFERIR
AS19R5	15	REDUCIR
AS19R6	12	REDUCIR
AS19R7	1	ACEPTAR
AS20R1	10	TRANSFERIR
AS20R2	8	TRANSFERIR
AS20R3	8	TRANSFERIR
AS20R4	15	REDUCIR
AS20R5	12	REDUCIR
AS20R6	1	ACEPTAR
AS21R1	10	TRANSFERIR
AS21R2	8	TRANSFERIR
AS21R3	16	EVITAR
AS21R4	12	REDUCIR

Establecidas las estrategias de tratamiento para cada riesgo identificado, se define los planes de tratamiento para los riesgos en zonas moderada e inaceptable, donde el valor del riesgo inherente se encuentra entre 11 y 25, como se presenta en la Tabla 27.

Tabla 27

Riesgos a ser tratados

ID Riesgo	Cálculo del riesgo inherente
AS1R9	12
AS2R9	12
AS3R9	12
AS10R1	12
AS10R9	12
AS10R11	15
AS17R1	12
AS17R2	12
AS17R3	12

AS17R7	**12**
AS17R8	**12**
AS17R9	**12**
AS17R11	**16**
AS19R2	**15**
AS19R5	**15**
AS19R6	**12**
AS20R4	**15**
AS20R5	**12**
AS21R3	**16**
AS21R4	**12**

Las zonas de riesgo para la definición de los planes de tratamiento son establecidas por la alta dirección.

5.4.3.1 Selección de controles

Una vez obtenidos los riesgos en la zona inaceptable y moderada, se identifican los posibles controles a implementar basados en norma ISO/IEC 27002:2013 con el fin de mitigarlos, de acuerdo a la Tabla 28.

Tabla 28

Controles seleccionados

No.	Control Anexo A ISO 27001	Nombre del Plan	Descripción del Plan	Riesgos Gestionados
1	**5.1.1** **5.1.2** **6.1.5**	Definición de políticas de seguridad de información	Generar políticas que proporcionen orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio, leyes y normas pertinentes.	AS1R9 AS2R9 AS3R9 AS10R9 A17R9

No.	Control Anexo A ISO 27001	Nombre del Plan	Descripción del Plan	Riesgos Gestionados
2	**9.1.1** **9.1.2** **9.2.1** **9.2.2** **9.2.3** **9.2.4** **9.2.5** **9.2.6** **9.4.1**	Elaboración de Normativas de Control de Acceso	Revisión de permisos en el File Server, donde el ingreso al servidor esté plenamente autorizado por el propietario de la información.	AS10R1 AS17R1 AS17R2
3	**9.2.3** **9.2.5** **13.1.1**	Cifrado de Información	La información de los equipos portátiles que son más propensos a robo, permanecerá cifrada para evitar la pérdida de confidencialidad de la información.	AS17R7 AS17R8
4	**13.2.1** **13.2.2**	Elaboración de Normativa Capacitaciones de Seguridad	Capacitar al personal sobre la aplicación de buenas prácticas de seguridad de la información.	AS1R9 AS2R9 AS3R9 AS11R9 AS11R1 AS17R11 AS19R2 AS19R5 AS19R6 AS20R4 AS20R5 AS19R1 AS19R9
5	**6.2.1**	Elaboración de Normativa de Protección de la información dispositivos móviles	Aplicar políticas estrictas en el uso de dispositivos móviles que se conectan a la red mediante una VPN para encriptar la información, así como la restricción de la copia de información no autorizada. Restringir en el acceso a internet y correos personales.	AS17R1 AS17R2

No.	Control Anexo A ISO 27001	Nombre del Plan	Descripción del Plan	Riesgos Gestionados
6	**7.1.1** **7.1.2** **7.2.1** **7.2.2** **7.2.3** **7.3.1**	Elaboración de Normativa de Recursos Humanos	Investigar la reputación y honorabilidad de los empleados previa contratación a la empresa. Mantenerlos una capacitación permanente en seguridad de la información, responsabilidades y consecuencias en caso de no cumplir las políticas internas. Ante la desvinculación de un empleado de la empresa, se deberá salvaguardar los activos asignados a la persona.	A21R2 A21R5 A21R6
7	**17.2.1**	Elaboración de Normativa de Redundancia	Implementación de mecanismos y/o hardware redundante que garantice alta disponibilidad de los servicios de TI en el Data Center como UPS, fuentes de energía para servidores, balanceadores de carga de servidores web y otros.	AS21R3 AS21R4

5.4.3.2 Valoración de controles

Se realiza la valoración de los controles seleccionados según la Tabla 13 con el fin de determinar la factibilidad de implementación de cada control. Los resultados se presentan en la Tabla 29.

Tabla 29

Valoración de la selección de controles

Control ISO/IEC 27002	Objetivos de la organización				Restricciones legales y Regulatorias	Restricciones operacionales				Costo de implementación		Efectividad				
	C1	C2	C3	TOTAL	C4	C5	C6	C7	TOTAL	C8	C9	TOTAL	C10	C11	C12	TOTAL	TOTAL
5.1.1	8	0	6	14	20	8	0	0	8	10	10	20	6	0	8	14	76
5.1.2	8	0	6	14	20	8	0	0	8	10	10	20	6	0	8	14	76
6.1.1	8	0	6	14	20	8	0	0	8	10	10	20	6	0	8	14	76
6.1.5	8	0	6	14	20	8	0	0	8	10	10	20	6	0	8	14	76
9.1.1	8	0	6	14	20	8	0	6	14	10	10	20	6	0	8	14	82
9.1.2	0	0	0	0	20	8	0	6	14	10	10	20	6	0	8	14	68
9.2.1	8	0	6	14	20	8	6	6	20	10	10	20	6	0	8	14	88
9.2.2	0	0	6	6	20	8	0	0	8	10	10	20	6	0	8	14	68
9.2.3	0	0	6	6	20	8	0	6	14	10	10	20	6	0	8	14	74
9.2.4	8	6	6	20	20	8	6	6	20	10	10	20	6	0	8	14	94
9.2.5	0	0	6	6	20	8	0	6	14	10	10	20	6	0	8	14	74
9.2.6	8	6	6	20	20	8	6	6	20	10	10	20	6	0	8	14	94
9.4.1	8	6	6	20	20	8	0	6	14	10	10	20	0	0	8	8	82
13.1.1	8	6	6	20	20	8	0	6	14	10	10	20	6	0	0	6	80
13.2.1	8	6	6	20	20	8	0	6	14	0	10	10	6	0	0	6	70
13.2.2	8	6	6	20	20	8	0	6	14	0	10	10	6	0	0	6	70
6.2.1	8	6	6	20	20	8	0	0	8	10	10	20	6	0	0	6	74
7.1.1	8	6	6	20	20	8	0	6	14	0	10	10	6	0	0	6	70
7.2.1	8	6	6	20	20	8	0	6	14	0	10	10	6	0	0	6	70
7.2.2	8	6	6	20	20	8	0	6	14	0	10	10	6	0	0	6	70
7.2.3	8	6	6	20	20	8	0	6	14	0	10	10	6	0	0	6	70
7.3.1	8	6	6	20	20	8	0	6	14	0	10	10	6	0	0	6	70
17.2.1	8	6	6	20	20	8	0	6	14	0	0	0	6	0	0	6	60

5.4.4 Aceptación

Para la aceptación de la aplicación o exclusión de los controles basados ISO/IEC 27002:2013, se elabora un documento de Declaración de Aplicabilidad de dichos controles, el mismo que se encuentra aprobado por la alta dirección (Anexo 7).

Los resultados de los controles a aplicar se describen en la Tabla 33.

Tabla 33
Declaración de aplicabilidad

Ítem	Dominio, Objetivo y Control	Aplicabilidad (Si - No)	Descripción	Razón para la aplicación o exclusión
A.5	**A.5 Política de Seguridad de Información**		Políticas de seguridad de la información	
A.5.1	A.5.1 Gestión y Dirección para Seguridad de la Información		Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	
A.5.1.1	A.5.1.1 Documento de Política de Seguridad de la Información	SI	Definir políticas para la seguridad de la información, aprobadas por la dirección, publicadas y comunicadas a los empleados y partes externas pertinentes.	Producto de la documentación del Sistema de Gestión de Seguridad donde se considera la protección de la confidencialidad, integridad y disponibilidad de la información.
A.5.1.2	A.5.1.2 Revisión a la Política de Seguridad de la Información	SI	Las políticas para seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continuas.	Producto de la documentación del sistema donde se considera la protección de la confidencialidad, integridad y disponibilidad de la información.
A.6	**A.6 Organización de Seguridad de la Información**		Organización de la seguridad de la información	

Ítem	Dominio, Objetivo y Control	Aplicabilidad (Si - No)	Descripción	Razón para la aplicación o exclusión
A.6.1	A.6.1 Organización interna		Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.	
A.6.1.1	A.6.1.1 Roles y Responsabilidades de Seguridad de la Información	SI	Definir y asignar las responsabilidades de la seguridad de la información.	Producto de la documentación del sistema donde se considera la protección de la confidencialidad, integridad y disponibilidad de la información.
A.6.1.2	A.6.1.2 Segregación de Funciones	NO	Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	El control no mitiga directamente riesgos de seguridad de seguridad de la información.
A.6.1.3	A.6.1.3 Contacto con las Autoridades	NO	Mantener contactos apropiados con las autoridades pertinentes.	El control no mitiga directamente riesgos de seguridad de seguridad de la información.
A.6.1.4	A.6.1.4 Contacto con Grupos de Interés	NO	Mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	El control no mitiga directamente riesgos de seguridad de seguridad de la información.
A.6.1.5	A.6.1.5 Seguridad de la información en Gestión de Proyectos	SI	Tratar la seguridad de la información en la gestión de proyectos, independientemente del tipo de proyecto.	Aunque el control no mitiga directamente riesgos de seguridad de seguridad de la información, este control apoya el cumplimiento de las políticas y normativas del SGSI.
A.6.2	A.6.2 Dispositivos móviles y teletrabajo		Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	

Ítem	Dominio, Objetivo y Control	Aplicabilidad (Si - No)	Descripción	Razón para la aplicación o exclusión
A.6.2.1	A.6.2.1 Política de dispositivos móviles	SI	Adoptar una política y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.6.2.2	A.6.2.2 Teletrabajo	NO	Implementar una política y medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	La organización no implementa el teletrabajo para sus funcionarios.
A.7	**A.7 Seguridad de Recursos Humanos**		Seguridad de los recursos humanos	
A.7.1	A.7.1 Previo a la contratación		Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	
A.7.1.1	A.7.1.1 Selección	SI	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.7.1.2	A.7.1.2 Términos y Condiciones del Empleo	SI	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.

Ítem	Dominio, Objetivo y Control	Aplicabilidad (Si - No)	Descripción	Razón para la aplicación o exclusión
A.7.2	A.7.2 Durante la contratación		Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	
A.7.2.1	A.7.2.1 Responsabilidades de la Dirección	SI	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.7.2.2	A.7.2.2 Concientización, educación y entrenamiento en Seguridad de la Información	SI	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.7.2.3	A.7.2.3 Proceso Disciplinario	SI	Contar con un proceso formal y comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.7.3	A.7.3 Terminación o cambio de trabajo		Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.	

Ítem	Dominio, Objetivo y Control	Aplicabilidad (Si - No)	Descripción	Razón para la aplicación o exclusión
A.7.3.1	A.7.3.1 Responsabilidades de Terminación	SI	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.9	**A.9 Control de Acceso**		Control de acceso	
A.9.1	A.9.1 Requerimientos del negocio para el control de acceso		Limitar el acceso a información y a instalaciones de procesamiento de información.	
A.9.1.1	A.9.1.1 Política de Control de Acceso	SI	Establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.9.1.2	A.9.1.2 Acceso a redes y servicios de red	SI	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Aunque el control no mitiga directamente riesgos de seguridad de seguridad de la información, este control apoya el cumplimiento de los lineamientos de red establecidos.
A.9.2	A.9.2 Administración de acceso de usuarios		Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.	
A.9.2.1	A.9.2.1 Registro y cancelación de usuarios	SI	Implementar un proceso formal de registro y de cancelación del registro, para posibilitar la asignación de los derechos de acceso.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.

Ítem	Dominio, Objetivo y Control	Aplicabilidad (Si - No)	Descripción	Razón para la aplicación o exclusión
A.9.2.2	A.9.2.2 Asignación de acceso a usuarios	SI	Implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.9.2.3	A.9.2.3 Gestión de derechos de acceso privilegiados	SI	Restringir y controlar la asignación y uso de derechos de acceso privilegiado.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.9.2.4	A.9.2.4 Gestión de información de autenticación de usuarios	SI	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.9.2.5	A.9.2.5 Revisión de los derechos de acceso de los usuarios	SI	Los dueños de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.9.2.6	A.9.2.6 Remoción o ajuste de derechos de acceso	SI	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.9.3	A.9.3 Responsabilidades de los usuarios		Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.	

Ítem	Dominio, Objetivo y Control	Aplicabilidad (Si - No)	Descripción	Razón para la aplicación o exclusión
A.9.3.1	A.9.3.1 Uso de la información de autenticación	NO	Exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	El control no mitiga directamente riesgos de seguridad de la información.
A.9.4	A.9.4 Control de acceso a sistemas y aplicaciones		Prevenir el uso no autorizado de sistemas y de aplicaciones.	
A.9.4.1	A.9.4.1 Restricción de acceso a la información	SI	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.9.4.2	A.9.4.2 Procedimientos de autenticación segura	NO	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.	El control no mitiga directamente riesgos de seguridad de seguridad de la información.
A.9.4.3	A.9.4.3 Sistema de administración de contraseñas	NO	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	El control no mitiga directamente riesgos de seguridad de seguridad de la información.
A.9.4.4	A.9.4.4 Uso de utilidades	NO	Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	El riesgo asociado a este control lo gestiona el controlar la instalación de aplicaciones
A.9.4.5	A.9.4.5 Control de acceso al código fuente de programas	NO	Se debe restringir el acceso a códigos fuente de programas.	El control no mitiga directamente riesgos de seguridad de seguridad de la información.
A.13	**A.13 Seguridad en las Comunicaciones**		Seguridad de las comunicaciones	

Ítem	Dominio, Objetivo y Control	Aplicabilidad (Si - No)	Descripción	Razón para la aplicación o exclusión
A.13.1	A.13.1 Gestión de seguridad en la red		Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	
A.13.1.1	A.13.1.1 Controles de Red	SI	Gestionar las redes y controlar para proteger la información en sistemas y aplicaciones.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.13.1.2	A.13.1.2 Seguridad de los servicios de red	NO	Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.13.1.3	A.13.1.3 Segmentación de redes	NO	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.13.2	A.13.2 Intercambio de información		Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	
A.13.2.1	A.13.2.1 Políticas y procedimientos de intercambio de información	SI	Contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.

Ítem	Dominio, Objetivo y Control	Aplicabilidad (Si - No)	Descripción	Razón para la aplicación o exclusión
A.13.2.2	A.13.2.2 Acuerdos de intercambio de información	SI	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	Debido a la cantidad de información que comparte la empresa con sus clientes y proveedores se deben seguir procedimientos y políticas al respecto de transferencia de información teniendo en cuenta la clasificación de esta.
A.13.2.3	A.13.2.3 Mensajería Electrónica	SI	Proteger apropiadamente la información incluida en los mensajes electrónicos.	Aunque el control no mitiga directamente riesgos de seguridad de seguridad de la información, este control apoya las consideraciones para el manejo adecuado de activos de información y la aplicación de los controles de red.
A.13.2.4	A.13.2.4 Acuerdos de confidencialidad o no divulgación	SI	Identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	En el análisis de riesgos realizado se identificó la necesidad del control para mitigar riesgos potenciales de seguridad de la información.
A.17.2	A.17.2 Redundancia		Asegurarse de la disponibilidad de instalaciones de procesamiento de información.	
A.17.2.1	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	NO	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Los costos de implementación de sistemas redundantes para el Data Center ubicado en la oficina matriz que garanticen alta disponibilidad de servicios superan a las pérdidas ocurridas por indisponibilidad en el año.

5.4.5 Comunicación de los riesgos de la seguridad de la información

Una vez que realizada la gestión de riesgos, los resultados son puestos en conocimiento de la Alta Dirección en los documentos que se detallan en la Tabla 30.

Tabla 30
Comunicación del riesgo

No.	DOCUMENTO	ANEXO
1	Identificación de los activos	ANEXO 5
2	Identificación de los riesgos	ANEXO 8
3	Definición de planes de tratamiento de riesgos	ANEXO 10
4	Declaración de Aplicabilidad	ANEXO11

5.5 Definición de la Política de Seguridad de la Información

Lockers S.A. considera la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la organización, en este contexto, se establece una política de seguridad que asegura que la información sea protegida de una manera adecuada.

La administración de la seguridad de la información en Lockers S.A. está basada en la versión 2013 de la Norma ISO/IEC 27001 y su operación es responsabilidad de todo el personal, quienes deben ejecutar sus actividades con estricta sujeción a los lineamientos y normativas vigentes en Lockers S.A., para prevenir o responder a eventos de seguridad de la Información.

Las políticas incluídas en este documento se constituyen como parte fundamental del Sistema de Gestión de Seguridad de la Información de Lockers S.A. y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La política se encuentra en el ANEXO 12.

5.5.1 Objetivo

Establecer los lineamientos orientados a garantizar y preservar la información organizacional en base a los principios de seguridad de la información (Confidencialidad, Integridad y Disponibilidad) en concordancia con los requerimientos del negocio.

5.5.2 Alcance

El presente documento y las políticas definidas en él, aplican para todo el ámbito de Lockers S.A., su cumplimiento es mandatorio para todo el personal y terceras partes que hagan uso de los activos de información de la empresa en el desarrollo de sus actividades o funciones.

5.5.3 Responsabilidades

a. Área Responsable y con autoridad para implementar, actualizar y vigilar el cumplimiento de estas políticas: Comité de Seguridad de la Información.
b. Área responsable de normalización de este documento: Comité de Seguridad de la Información.
c. Áreas responsables de conocer y aplicar estas políticas: Todas las áreas de Lockers S.A.

5.5.4 Referencias

a. ISO/IEC 27001:2013. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.
b. ISO/IEC 27002:2013. Código de Práctica para Controles de Seguridad de la Información.
c. PRD-PCV-OPE-GOPS-03. Procedimiento Gerencia de Operaciones
d. PRD-PCV-OPE-DIGI-04. Procedimiento de Digitación, Digitalización, Indexación y Expurgo de Archivo
e. REGL-PDA-THU-INT-TRAB-01. Reglamento Interno de Trabajo de Lockers S.A.

5.5.5 Objetivos de la seguridad de la información

Los objetivos de la seguridad de la información se encuentran orientados a contribuir, minimizar y controlar los riesgos de la empresa, por lo que Lockers S.A. definirá objetivos consistentes y medibles que deberán ser revisados anualmente con el fin de velar por su alineación con la estrategia de la empresa.

5.5.6 Enunciado de la política de seguridad de la información

Lockers S.A. se compromete a velar por el cumplimiento de la presente política aplicable a sus procesos de negocio, salvaguardando la confidencialidad, integridad y disponibilidad de la información.

5.5.7 Política general de seguridad de la información

La Política General de Seguridad de la Información de Lockers S.A. se encuentra soportada por políticas, normas y procedimientos específicos definidos bajo estándares que garantizan la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, alineados a los objetivos y actividades de la empresa.

5.5.8 Compromiso de la dirección

La Gerencia General de Lockers S.A. promueve las Políticas de Seguridad de la Información reafirmando su compromiso a través de:

a. El cumplimiento de la normatividad vigente y requisitos aplicables a seguridad de la información.
b. La promoción activa de una cultura de seguridad.
c. El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
d. La mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) aplicando mejores prácticas para proteger la confidencialidad, integridad y disponibilidad de la información.

5.5.9 Políticas específicas de seguridad de la información

5.5.9.1 Organización de la seguridad de la información

5.5.9.1.1 Estructura organizacional de seguridad de la información

Lockers S.A. establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

5.5.9.1.2 Uso de dispositivos móviles

Lockers S.A. proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) y personales que hagan uso de servicios de la empresa. Así mismo, velará porque los funcionarios hagan uso responsable de los servicios y equipos proporcionados por la entidad.

5.5.9.1.3 Uso de conexiones remotas

Lockers S.A. establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la empresa; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

5.5.9.2 Seguridad del personal

5.5.9.2.1 Vinculación de funcionarios

Lockers S.A. garantizará que la vinculación de nuevos colaboradores se realice siguiendo un proceso formal de selección, orientado a las funciones y roles que deben desempeñar los empleados en sus cargos.

5.5.9.2.2 Desvinculación, licencias, vacaciones o cambio de labores de los funcionarios y personal provisto por terceros

Lockers S.A. asegurará que sus colaboradores y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

5.5.9.3 Gestión de activos de información

5.5.9.3.1 Responsabilidad por los activos

Lockers S.A. como propietaria de la información física, los sistemas, los servicios y los equipos de trabajo, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

5.5.9.3.2 Clasificación y manejo de la información

Toda la información de Lockers S.A. debe ser identificada, clasificada y documentada de acuerdo con los lineamientos de clasificación de la información establecidos por la Alta Dirección a través del representante para el SGSI.

5.5.9.3.3 Uso de periféricos y medios de almacenamiento

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de Lockers S.A. será reglamentado por las Gerencias o Jefaturas responsables de administrar la plataforma, considerando las labores que realizan los empleados.

5.5.9.4 Control de acceso

5.5.9.4.1 Acceso a redes y recursos de red

La Gerencia de TI, responsable de administrar la plataforma tecnológica, las redes de datos y los recursos de red de la organización, debe protegerlos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

5.5.9.4.2 Administración de acceso de usuarios

Lockers S.A. establecerá privilegios para el control de acceso lógico de cada usuario interno y externo o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la organización.

5.5.9.4.3 Responsabilidades de acceso de los usuarios

Los usuarios de los recursos tecnológicos y los sistemas de información de Lockers S.A. realizarán un uso adecuado y responsable de los recursos y sistemas, salvaguardando la información a la cual se les ha permitido el acceso.

5.5.9.5 Criptografía

5.5.9.5.1 Controles criptográficos

Lockers S.A. asegurará que la información sea cifrada de acuerdo con lo definido en los lineamientos establecidos para el manejo de activos de información.

5.5.9.6 Cumplimiento

5.5.9.6.1 Privacidad y protección de datos personales

Lockers S.A. asegurará la protección y privacidad de los datos personales que almacene, procese y transmita de sus clientes, empleados y proveedores, acorde con la legislación, reglamentación y regulación aplicable para Lockers S.A.

5.5.10 Revisión y actualización

Las políticas de seguridad de la información deberán revisarse al menos una vez al año o cuando ocurrieran cambios significativos en la organización que pudieran comprometer su aplicabilidad y eficacia.

5.5.11 Incumplimiento y excepciones

El incumplimiento de las presentes políticas se considerará una falta que será observada y considerada para proceder conforme a lo previsto en el Reglamento de

Gestión del Talento Humano de Lockers S.A. y de ser el caso la aplicación de las penas previstas en las leyes aplicables.

5.6 Auditoría de cumplimiento del SGSI.

Considerando que los autores del diseño e implementación del SGSI no pueden realizar la auditoria de cumplimiento del SGSI, se ha definido la realización de un caso de estudio en el cual se evalúe la eficacia de los controles implementados a los riesgos clasificados como inaceptables y moderados para la organización.

5.6.1 Caso de estudio

La evaluación se realiza mediante la aplicación de la metodología de gestión del riesgo planteada en el capítulo 4, con el nuevo cálculo del riesgo luego de 5 meses de la fecha de implementación.

Para valorar la probabilidad de ocurrencia del riesgo con fines del caso de estudio para la empresa Lockers S.A., se determina una escala proporcional al período de tiempo definido en la Tabla 10 y se presenta en la Tabla 31.

Tabla 31
Escala proporcional de probabilidad de ocurrencia del riesgo luego de implementado el SGSI

NIVEL	PROBABILIDAD	DESCRIPCIÓN
5	Muy Alta	El riesgo ha ocurrido o podría ocurrir varias veces dentro de 1 semana
4	Alta	El riesgo ha ocurrido o podría ocurrir alguna vez dentro de 3 meses
3	Media	El riesgo ha ocurrido o podría ocurrir alguna vez dentro de 3 meses
2	Baja	El riesgo ha ocurrido o podría ocurrir alguna vez dentro de 5 meses
1	Muy Baja	El riesgo ha ocurrido o podría ocurrir alguna vez en un periodo de más de 5 meses

Una vez que se implementados los controles de seguridad y habiendose generado las políticas para su cumplimiento, se realiza por segunda vez la gestión de riesgos, que permite valorar nuevamente la probabilidad e impacto de los riesgos. Los resultados fueron se presentan en la Tabla 32.

5.6.1.1 Resultados

Tabla 32
Valoración del riesgo luego de implementados los controles de seguridad

ID RIESGO	AMENAZA	VULNERABILIDAD	PROB	NIVEL DE PROB.	IMPACTO	NIVEL DE IMPACTO	CÁLCULO DEL RIESGO
AS1R9	Gestión ineficiente de Seguridad de la Información	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información	1	Posible	4	Mayor	4
AS2R9	Gestión ineficiente de Seguridad de la Información	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información	1	Posible	4	Mayor	4
AS3R9	Gestión ineficiente de Seguridad de la Información	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información	1	Posible	4	Mayor	4

ID RIESGO	AMENAZA	VULNERABILIDAD	PROB	NIVEL DE PROB.	IMPACTO	NIVEL DE IMPACTO	CÁLCULO DEL RIESGO
AS10R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos	1	Probable	3	Moderado	3
AS10R11	Robo de información	Robo de información	1	Posible	4	Catastrófico	4
AS10R9	Gestión ineficiente de seguridad por parte de TI	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información	1	Posible	4	Mayor	4
AS17R1	Abuso de los derechos	Un usuario con los niveles de autorización elevados, haga mal uso de los derechos	1	Posible	4	Mayor	4
AS17R11	Robo de información	Robo de información	1	Rara vez	4	Mayor	4
AS17R2	Acceso no autorizado	Violación a la confidencialidad e integridad de la información	1	Posible	4	Mayor	4
AS17R3	Daño de externos	Una entidad externa ocasiona daños	1	Posible	4	Mayor	4

ID RIESGO	AMENAZA	VULNERABILIDAD	PROB	NIVEL DE PROB.	IMPACTO	NIVEL DE IMPACTO	CÁLCULO DEL RIESGO
AS17R7	Escucha encubierta	Lectura de información no autorizada mediante técnicas de ataques informáticos como Sniffers	1	Posible	4	Mayor	4
AS17R8	Espionaje remoto	Obtención encubierta de datos o información confidencial	1	Posible	4	Mayor	4
AS17R9	Gestión ineficiente de seguridad por parte de TI	Aplicación inadecuada de medidas preventivas y reactivas que permiten proteger la información	1	Posible	4	Mayor	4
AS19R2	Chantaje	Un usuario sabotea sistemas o hace copias de información no autorizada para eliminarla de los activos y luego pedir rescate por la información	1	Posible	5	Catastrófico	5
AS19R5	Fraude y hurto	Una persona roba información de la empresa previo a su separación de la misma	1	Posible	5	Catastrófico	5

ID RIESGO	AMENAZA	VULNERABILIDAD	PROB	NIVEL DE PROB.	IMPACTO	NIVEL DE IMPACTO	CÁLCULO DEL RIESGO
AS19R6	Ingreso de datos falsos o corruptos	Un usuario ingresa datos a los sistemas de la empresa con el fin de alterar los procesos ya sea por obtener puntajes altos en evaluaciones o por justificar trabajo que no ha realizado	1	Posible	4	Mayor	4
AS20R4	Fraude y hurto	Una persona roba información de la empresa previo a su separación de la misma	1	Posible	5	Catastrófico	5
AS20R5	Ingreso de datos falsos o corruptos	Un usuario ingresa datos a los sistemas de la empresa con el fin de alterar los procesos ya sea por obtener puntajes altos en evaluaciones o por justificar trabajo que no ha realizado	1	Posible	4	Mayor	4
AS21R3	Pérdida de suministro de energía	El sector no garantiza estabilidad ni continuidad de suministrso eléctrico. Apagones y variaciones de voltaje en la red eléctrica desabastecen de energía	1	Rara vez	4	Mayor	4

ID RIESGO	AMENAZA	VULNERABILIDAD	PROB	NIVEL DE PROB.	IMPACTO	NIVEL DE IMPACTO	CÁLCULO DEL RIESGO
AS21R4	Mal funcionamiento del equipo	Falla en el hardware provocado principalmente por tener equipos obsoletos	1	Posible	4	Mayor	4

5.6.2 Evaluación de resultados

Luego se determinó el estado del riesgo una vez implementados los controles, siendo Controlado si esta baja a una zona inferior indicada en la Tabla 11.

Tabla 33
Estado del riesgo luego de la implementación del SGSI

ID RIESGO	RIESGO INHERENTE 1	RIESGO INHERENTE 2	ESTADO
AS10R1	12	3	CONTROLADO
AS10R11	15	4	CONTROLADO
AS10R9	12	4	CONTROLADO
AS17R1	12	4	CONTROLADO
AS17R11	16	4	CONTROLADO
AS17R2	12	4	CONTROLADO
AS17R3	12	4	CONTROLADO
AS17R7	12	4	CONTROLADO
AS17R8	12	4	CONTROLADO
AS17R9	12	4	CONTROLADO
AS19R2	15	5	CONTROLADO
AS19R5	15	5	CONTROLADO
AS19R6	12	4	CONTROLADO
AS1R9	12	4	CONTROLADO

ID RIESGO	RIESGO INHERENTE 1	RIESGO INHERENTE 2	ESTADO
AS20R4	15	5	CONTROLADO
AS20R5	12	4	CONTROLADO
AS21R3	16	4	CONTROLADO
AS21R4	12	4	CONTROLADO
AS2R9	12	4	CONTROLADO
AS3R9	12	4	CONTROLADO

Se evidencia que los controles aplicados a los riesgos, son eficaces ya que el riesgo residual se encuentra en una zona aceptable definida por la empresa.

5.7 Documentación

Como resultado de la implementación del SGSI, se desarrolla la siguiente documentación.

- Definición de Roles y Responsabilidades – ANEXO 3
- Compromiso de la Alta Dirección – ANEXO 4
- Inventario de Activos Primarios – ANEXO 5
- Inventario de Activos de Soporte – ANEXO 5
- Alcance y Objetivos del SGSI – ANEXO 6
- Metodología de Gestión de Riesgos - ANEXO 7
- Gestión de Riesgos – ANEXO 8
- Valoración de controles – ANEXO 9
- Plan de Tratamiento – ANEXO 10
- Declaración de Aplicabilidad – ANEXO 11
- Política de Seguridad de la Información – ANEXO 12
- Auditoría de Cumplimiento - ANEXO 13

CAPÍTULO 6
CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- La metodología propuesta de Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de control físico y digital de documentos fue aplicada a la empresa Lockers S.A. dando los resultados esperados.
- Las políticas, normativas y procedimientos generados fueron aplicados satisfactoriamente dentro de la organización y puestas en conocimiento del personal interno de la alta dirección desarrollando una cultura organizacional de seguridad de la información.
- El Sistema de Gestión de Seguridad de la Información implementado ayudó a identificar los riesgos de seguridad que vulneran la integridad, confidencialidad y disponibilidad de la información generada en el proceso de custodia de archivo físico y digital de la empresa Lockers S.A., registrados en el Anexo 8.
- En el caso de estudio realizado sobre el cumplimiento del SGSI, se pudo evidenciar que los controles implementados para los riesgos inaceptables, moderados y tolerables fueron mitigados dentro del periodo establecido dando resultados favorables para la organización.

6.2 RECOMENDACIONES

- Realizar la auditoria de cumplimiento del SGSI para la mejora continua del sistema, dentro del tiempo establecido en la Política de Seguridad de la Información de la empresa.
- Realizar el proceso de certificación de la empresa en la ISO 27001:2013 para posicionar a la empresa como líder en la custodia de archivos físicos y digital.
- Realizar revisiones periódicas de las políticas, procedimientos y normas implementadas conforme los cambios estratégicos de la empresa en futuro.

- Designar un Oficial de Seguridad encargado de velar el cumplimiento de los objetivos de seguridad de la información establecidos.
- La documentación obtenida como parte de la implementación del SGSI en la empresa Lockers S.A. puede ser utilizada como base para la certificación de la empresa en gestión de seguridad de la información ISO 27001:2013.

BIBLIOGRAFÍA

Alfantookh, A. (2009). An Approach for the Assessment of The Application of ISO 27001 Essential Information Security Controls. *Computer Sciences*.

BSI GROUP. (2015). *Documento técnico Introducción al Anexo SL.*

Fernández Barcell, M. (2003). *ESTUDIO DE UNA ESTRATEGIA PARA LA IMPLANTACIÓN DE LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.* Cádiz, España: Universidad de Cádiz.

González, J. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.* Madrid, España.

Hernández, R. (2003). *Metodología de la Investigación.* Mexico D.F: McGraw - Hill.

Huerta, A. (2012). *Introducción al análisis de riesgos – Metodologías (I)*. Retrieved from https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

Hurdado, L., & Toro, G. (2001). *Paradigmas y Métodos de Investigación.*

INEN-ISO/IEC 27001:2011. (2011). *Tecnolog[ia de la Informnación - Técnicas de Seguridad - Sistema de Gestión de la Seguridad de la Información (SGSI) - Requisitos.* Quito, Ecuador.

INEN-ISO/IEC 27003:2012. (2012). *Guía de implementación del Sistema de Gestión de Seguridad de la Información.*

ISO. (2017, 10 30). Retrieved from ISO/IEC 27000 family - Information security management systems: https://www.iso.org/isoiec-27001-information-security.html

ISO 27001: El método MAGERIT. ISOTools Excellence. (2015). Retrieved from http://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

ISO/IEC 27001:2013. (2014). *Tecnología de la información - Técnicasde seguridad - Sistema de Gestion de Seguridad de la Información (SGSI) - Requisitos.*

ISO/IEC 27002:2013. (2013). *Tecnología de la Información - Técnicas de la Seguridad - Código de Práctica para la Géstion de la Seguridad de la Infromación.*

ISO/IEC 27005:2011. (2011). *Information technology - Security techniques - Information security rik management.*

MAGERIT v.3. (2012). Retrieved Febrero 25, 2017, from https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WfwNzWjWzDc

Marquis, H. (2008). *10 Steps to Do It Yourself CRAMM.* Retrieved from http://www.itsmsolutions.com/newsletters/DITYvol4iss50.pdf

Potter, C., & Beard, A. (2010). *Information Security Breaches Survey 2010.* London: Price Water House Coopers.Earl‟s Court.

Radovanovic, D., Radojević, T., Lucic, D., & Šarac, M. (2010). IT audit in accordance with Cobit standard. Belgrade: Singidunum University.

SANS Institute. (2002). *A Qualitative Risk Analysis and Management Tool – CRAMM*. Retrieved from https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83

Superintendencia Nacional de Salud. (2017). *Guía Metodológica de Análisis de Riesgos de Seguridad y Privacidad de la Información Superintendencia Nacional de Salud.* Bogotá, Colombia.

Susanto, H., Almunawar Nabil, M., Syam, W., Chee Tuan, Y., & Hajj Bakry, S. (2011). I-SolFramework View on ISO 27001. Information Security Management System: Refinement Integrated Solution‟s Six Domains. *Asian Transaction on Computer Journal*.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). nformation Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level. *International Journal of Engineering and Technology (IJET)*.

Susanto, H., Nabil, M., & Chee, Y. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Engineering and Computer Science*.

Tola, D. (2015). *Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001.* Guayaquil, Ecuador: Escuela Superior Politécnica del Litoral.

Trejo, G. D. (2013, Agosto 30). *ISO-27001:2013 ¿Qué hay de nuevo?* Retrieved Noviembre 1, 2017, from http://www.magazcitum.com.mx/?p=2397#.WfvFkWjWzs0

Yazar, Z. (2002). *A qualitative risk analysis and management tool – CRAMM.* SANS Institute.

ANEXOS

ANEXO 1

TÉRMINOS Y DEFINICIONES

ANEXO 2

ESTRUCTURA ORGANIZACIONAL LOCKERS S.A.

ANEXO 3

ACTAS DE REUNIÓN

ANEXO 4

COMPROMISOS DE LA ALTA DIRECCIÓN

ANEXO 5

INVENTARIO DE ACTIVOS

ANEXO 6

ALCANCE Y OBJETIVOS DEL SGSI

ANEXO 7

METODOLOGÍA DE GESTIÓN DE RIESGOS

ANEXO 8

MATRIZ DE RIESGOS

ANEXO 9

VALORACIÓN DE CONTROLES

ANEXO 9

PLAN DE TRATAMIENTO

ANEXO 10

DECLARACIÓN DE APLICABILIDAD

ANEXO 11

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ANEXO 12

AUDITORÍA DE CUMPLIMIENTO