DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA ENTIDAD FINANCIERA DE SEGUNDO PISO

TRABAJO DE GRADO

CARLOS ALBERTO GUZMAN SILVA
COD. 1412010642

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2015

DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA ENTIDAD FINANCIERA DE SEGUNDO PISO

TRABAJO DE GRADO

CARLOS ALBERTO GUZMAN SILVA
COD. 1412010642

Asesor
Giovanny Andrés Piedrahita Solorzano
Coordinador Investigación y Posgrados DIST-FICB

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2015

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Ciudad, Fecha

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCION

Hoy en día, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, la cual, sólo tiene sentido cuando está disponible y es utilizada de forma adecuada, integra, oportuna, responsable y segura, lo que implica, que es necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razon por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio. Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones. Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, contantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada.

En la medida que las organizaciones tenga una visión general de los riesgos que pueden afectar la seguridad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la integridad, disponibilidad y confidencialidad tanto de la información del negocio como los datos de carácter personal de sus empleados y usuarios. Es indispensable que las organizaciones realicen una adecuada identificación,

clasificación, valoración, gestión y tratamiento de los riegos que pueden afectar su seguridad, con el propósito de implementar salvaguardas efectivas que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

Las entidades del sector financiero, están en la obligación de garantizar la debida seguridad, protección y privacidad de la información financiera y personal de los usuarios que residen en sus bases de datos, lo que implica, que deben contar con los más altos estándares y niveles de seguridad con el propósito de asegurar la debida recolección, almacenamiento, tratamiento y uso de esta información. Una de las preocupaciones permanentes de este tipo de entidades financieras, es la de poder garantizar la seguridad de las operaciones que realizan sus clientes, lo cual, cada día es más complejo de conseguir debido a la evolución de las tecnologías y la apertura de nuevos canales de transacciones que generan retos significativos con el propósito de prevenir los fraudes en general.

Debido a los múltiples riesgos y amenazas que hoy en día atentan contra la seguridad de la información y la protección y privacidad de los datos, es fundamental que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un sistemas de gestión de seguridad de la información basado en los riesgos y a su vez, alineado con los objetivos estratégicos y necesidades tanto del negocio como de sus partes interesadas.

El presente trabajo de grado busca diseñar un Sistema de Gestión de Seguridad de la Informacion para una entidad financiera de segundo piso, tendiendo en cuenta para esto el marco de referencia de la norma ISO 27001:2013 [1] que proporciona un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de Gestión de Seguridad de la Informacion en cualquier tipo de organización, lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo.

El diseño del Sistema de Gestión de Seguridad de la Información se realizará para una empresa real, pero por motivos de confidencialidad de su información para efectos del presente trabajo se utilizará el nombre de **IGM S.A**.

1. RESUMEN EJECUTIVO

1.1. DESCRIPCIÓN GENERAL

IGM S.A es un Banco de Segundo Piso, también conocidos como bancos de desarrollo o bancos de fomento, cuyos recursos de crédito son desembolsados a los usuarios de los créditos a través de otras instituciones financieras.

IGM S.A, es una sociedad anónima, de economía mixta del orden nacional, constituida con la participación exclusiva de entidades públicas, con personería jurídica, autonomía administrativa y capital independiente, organizada como un establecimiento de crédito, vinculada al Ministerio de Hacienda y Crédito Público y sometida a vigilancia por la Superintendencia Financiera de Colombia.

La entidad por ser de carácter público y financiero, este vigilada y controlada por la Superintendencia Financiera de Colombia y otros entes de control, por lo tanto, debe cumplir la normatividad vigente relacionada con seguridad de la información impartida por estos organismos aplicable a entidades del estado y financieras.

La Entidad cuenta con la infraestructura tecnológica adecuada y tiene implementado una serie de mecanismos de seguridad, tanto físicos como lógicos, con el propósito de poder proteger la confidencialidad, integridad y disponibilidad de la información del negocio y la privacidad de los datos de los clientes que residen en sus bases de datos. A pesar de contar con estos recursos tecnológicos y tener implementadas medidas de seguridad, la Entidad no cuenta con los mecanismos adecuados y expeditos que le permitan conocer el estado real de su seguridad en cuanto a personas, procesos y tecnología, ni el nivel de efectividad de las medidas de seguridad que tiene implementadas, lo que dificulta o impide identificar y por ende gestionar de manera efectiva los riesgos asociados a la seguridad de sus activos de información y las amenazas que puedan llegar con comprometer la integridad, disponibilidad y confidencialidad de su información.

1.1.1. ESTADO DE LA SEGURIAD DE LA INFORMACION EN IGM S.A

A principios del 2012, la Jefatura de Control Interno de la entidad realizó una auditoría al proceso de Gestión de Tecnología[1], con el fin de evaluar el estado de

[1] Auditoría interna realizadas por la Jefatura de Control Interno de la Entidad.

la seguridad de la infraestructura tecnológica y con ello poder identificar su nivel de exposición ante posibles ataque externo, para lo cual, realizó pruebas de vulnerabilidades de tipo no intrusivas a una serie de servicios de TI. Resultado de esta prueba, la auditoria encontró que el nivel de exposición de la plataforma tecnológica de la entidad ante ataques informáticos era alto y recomendó entre otras aspectos, la implementación de una serie de medidas y controles de seguridad con el objetivo de cerrar las brechas encontradas y la necesidad de que la entidad cuente con un modelo de seguridad de la información.

Con el propósito, de solventar cada una de los hallazgos encontrados y atender las recomendaciones y acciones de mejora establecidas en esta auditoría, la entidad contrato en el segundo semestre de 2012 a una empresa especializada en temas de seguridad de la información y continuidad del negocio, quien desarrollo en términos generales las siguientes actividades:

- Diagnóstico físico y de infraestructura.
- Gestión de vulnerabilidades.
- Revisión de las políticas de seguridad.

Como resultado de esta consultoría, la entidad desarrollo un plan de mitigación de vulnerabilidades para disminuir el nivel de exposición de sus recursos tecnológicos y estableció un plan anual de pruebas de vulnerabilidades, con el propósito de poder identificar de manera proactiva las debilidades de su infraestructura tecnológica y con esto establecer e implementar las medidas y controles orientadas a mejorar su nivel de seguridad.

Adicional a las labores realizadas por esta consultaría, la Dirección de Tecnología durante el año 2013 adelantado una serie de capacitación para sensibilizar a los funcionarios de la Entidad en temas de seguridad de la información.

A finales del año 2013, la Jefatura de Control Interno realizo la respetiva auditoria anual, la cual evidencio entre otros aspectos, la ausencia de un modelo de Gobierno de Seguridad en la entidad, la poca concienciación y apropiación por parte de los funcionarios en temas de seguridad y la ausencia de una metodológica de gestión de riesgos de seguridad. Como resultado de esta auditoría, la Jefatura de Control Interno recomendó la necesidad de contar con un Gobierno de Seguridad adecuado dentro de la organización para poder alinear la Seguridad de la información con las estrategias y objetivos del negocio, para lo

cual, sugirió la implementación de un Sistema de Gestión de Seguridad de la Información. Con el propósito de atender esta recomendación, desde enero del 2014, la Vicepresidencia de Crédito y Riesgos asumió la responsabilidad de definir el modelo de Seguridad de la Información a implementar en la entidad.

La Entidad cuenta con la Dirección de Tecnología que tiene por objetivo proveer y administrar los recursos tecnológicos, la cual es considerada como una de las áreas fundamentes para garantizar la integridad, confidencialidad y disponibilidad de la información de la entidad. La Dirección de Tecnología desarrolla actividades propias de seguridad informática, pero en muchos casos también funciones relacionadas con seguridad de la información, lo cual genera un riesgo debido a la falta de segregación de funciones asociadas con seguridad de la información.

1.1.2. IDENTIFICACION DEL PROBLEMA

A pesar de las acciones que se han realizado con el objetivo de fortalecer la Seguridad de la Información en la entidad, situaciones como, la falta de un adecuado modelo de Gobierno de Seguridad de la Información, la no existencia y de un sistema de información que apoye la gestión de riesgos de seguridad y la poca concienciación, apropiación y conocimiento en temas de seguridad por parte de los funcionarios de la entidad, debido, tal vez a una sensación de seguridad que hace pensar que nada va a pasar o que en algunos casos no le dan la importancia a la seguridad de la información por su intangibilidad, generan la poca efectividad de las acciones que en materia de seguridad de la información se realicen en la entidad. Esta situación, también implica que los funcionarios no conciben la diferencia entre seguridad informática y seguridad de la información.

La entidad no cuenta con sistema de información adecuado y robusto para la gestión de riesgos de seguridad, lo que dificulta establecer y visualizar el estado global y transversal de su seguridad, en cuanto a personas, procesos y tecnología, e implica entre otros aspectos, que no existe la participación activa de toda la organización con relación a la definición de procedimientos adecuados y a la planeación e identificación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos[2].

[2] http://www.iso27000.es/sgsi.html

La Entidad requiere asegurar sus activos de información con el propósito de proteger su exactitud y totalidad con el fin de que los mismos solo sean accesibles por aquellas personas que estén debidamente autorizadas. La entidad no cuenta con una metodología para la identificación y clasificación de sus activos de información y para la valoración y tratamiento de riesgos de seguridad de la información, lo que implica, que no cuenta con una visión global del estado de su seguridad.

La Dirección de Tecnología realiza algunas funciones propias de seguridad de la información, lo cual va en contravía con las mejores prácticas definidas en modelos y estándares de seguridad. Por lo tanto, es indispensable segregar las funciones de seguridad de la información y seguridad informática con el propósito de evitar que coexistan funciones que requieren diferentes niveles de seguridad.

1.1.3. DIAGNOSTICO SITUACION PROBLEMA

Con base en el análisis del estado de la seguridad de la entidad y la identificación de situaciones que de alguna forma afectan su seguridad, la siguiente figura ilustrar la identificación de la situación problema:

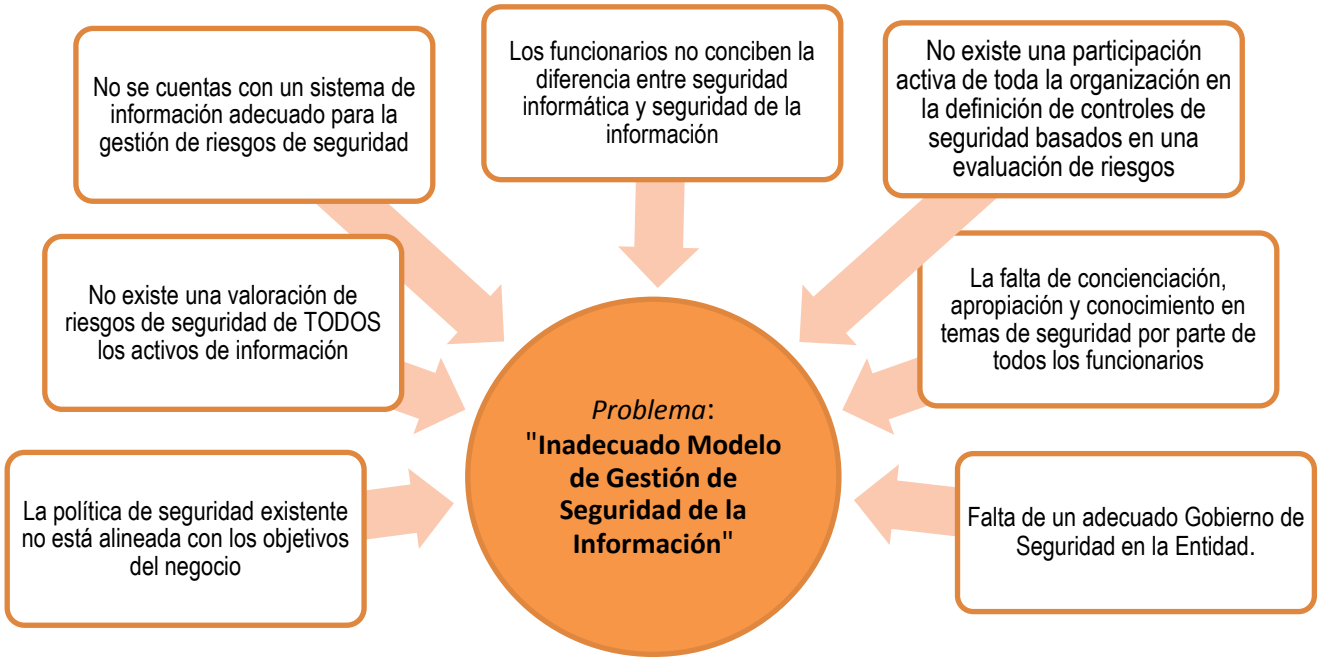


Figura 1. Identificación Situación Problema
Fuente: El Autor

A continuación se describen los diferentes factores que se presentan en la entidad y que están asociados a cada una de las situaciones que generan el problema:

Tabla 1. Factores asociados a las situaciones del problema

Situación	Factores
Falta de un Gobierno de Seguridad en la Entidad	• No existe una directriz a nivel gerencial sobre seguridad de la información. • No existe una participación activa de la alta directiva
No existe una cultura de seguridad de la información en la Entidad.	• Falta de concienciación, apropiación y conocimiento en temas de seguridad por parte de todos los funcionarios de la Entidad. • No existe una cultura de mejora continua de seguridad de la información. • Falta de interés por parte de los funcionarios en temas de seguridad. • No existe una participación actividad de toda la organización con relación a la definición de procedimientos adecuados y a la planeación e identificación de controles de seguridad basados en una evaluación de riesgos • Los funcionarios no distinguen la diferencia entre seguridad informática y seguridad de la información.
No existe Sistema de Información adecuado para la gestión de riesgos de seguridad.	• La entidad no cuenta con un sistema de información adecuado para la gestión de riesgos de seguridad. • No existe una valoración de riesgos de seguridad de TODOS los activos de información. • La entidad no cuenta con una visión global del estado de su seguridad, y por lo tanto no puede determinar con exactitud la efectividad de las medidas que sobre seguridad implemente. • Dificultad para el control y clasificación de los activos de información. • Inadecuada identificación de riesgos y controles de seguridad.
La política de seguridad existente no está alineada con los objetivos del negocio	• La política de seguridad existente no está alineada con las estrategias y objetivos del negocio. • Las políticas de seguridad son definidas por la Dirección de Tecnología. • Se requiere segregar las funciones de seguridad informática y seguridad de la información.

Con base en las anteriores situaciones, se puede determinar que el problema corresponde a un "**Inadecuado Modelo de Gestión de Seguridad de la Información**" en la Entidad.

1.1.4. INDICADORES DEL PROBLEMA

Los siguientes son los indicadores que se establecieron con el objetivo de poder identificar el estado actual de la situación problema:

Tabla 2. Indicadores del problema

Indicador	Objetivo del indicador
Nivel de compromiso de funciones y responsabilidades de seguridad	Establecer el nivel de compromiso de los funcionarios de la entidad en adoptar las funciones y responsabilidades que se establezcan en el manual de políticas de seguridad de la información.
Cubrimiento planes de tratamiento de riesgos de seguridad	Determinar el nivel o grado de cubrimiento de los planes de tratamiento de riesgos de seguridad de la información en la entidad.
Eficacia tratamiento de riesgos	Determina el grado de eficacia de la gestión de tratamiento de riesgos de la entidad.
Concienciación en seguridad de la información	Determinar el grado de cumplimiento de los planes de concienciación, sensibilización y capacitación en temas de seguridad.

De acuerdo a encuestas y estudios globales realizados sobre temas de seguridad de la información, a continuación se rescatan algunos resultados de dichos estudios con el objetivo de identificar el nivel de medición de estos indicadores en las diferentes organizaciones que fueron encuestadas:

Nivel de compromiso de funciones y responsabilidades de seguridad

De acuerdo a la "*XV Encuesta Global de Seguridad de la Información" realizado por Ernst & Young*" [2] en el año 2013, el 21% de los encuestados a nivel global han atribuido la responsabilidad de la seguridad de la información al CEO, CFO o COO logrando con esto que dicha responsabilidad sea un tema de la alta dirección, pero solo el 5% señala que la función de seguridad de la información le reporta al director de riesgos. De acuerdo al estudio, esta decisión se vuelve crítica al momento de querer gestionar las amenazas que puedan llegar comprometer la seguridad y dificulta la medición del desempeño y efectividad de las medidas implementadas. La encuesta, indica que generalmente las áreas de TI no cuentan con un panorama de riesgos formal o un mecanismo para evaluarlos, lo que de alguna forma explica porque el 52% de los encuestados a nivel global no cuentan con un programa adecuado y proactivo para la gestión de amenazas.

También se indica en la encuesta que el 63% de las organizaciones a nivel global depositan la responsabilidad de la seguridad de la información en la función de TI, lo que puede impedir que haya una evaluación, medición y alineación eficaz con las prioridades del negocio.

Cubrimiento planes de tratamiento de riesgos de seguridad

En la XV Encuesta Global de Seguridad de la Información realizado por Ernst & Young"[3] en el año 2013, se estableció que el 52% de los encuestados a nivel global no cuentan con un programa adecuado y proactivo para la identificación y gestión de amenazas. En un estudio realizado por la Asociación Colombiana de Ingenieros de Sistemas ACIS, denominado "Tendencias 2014 Encuesta Nacional de Seguridad Informática" [3], se evidenció que el 50.29% de las empresas encuestados no realizan análisis de riesgos.

Concienciación en seguridad de la información

De acuerdo a la encuesta "XV Encuesta Global de Seguridad de la Información, realizado por Ernst & Young en el 2013, entre otros resultados se estableció que el 40% de la organización invierten en programas de concientización y el 60% han implementado programas de concientización para empleados.

1.1.5. PLANTEAMIENTO DEL PROBLEMA

Debido a los múltiples riesgos y amenazas que se generan por el cambio constante y dinámico que enmarca la evolución de las tecnología de la información, es necesario que las organizaciones cuenten con una estrategia seguridad basado en los riesgos y a su vez alineada con las necesidades del negocio, con el objetivo de contar con un modelo de la Seguridad de la Información que apoye y apalanque los objetivos estratégicos de la organización.

Un Sistema de Gestión de la Seguridad de la Información, es una herramienta de gran utilidad para la gestión de la seguridad en las organizaciones, permite establecer políticas, procedimientos y controles en relación a los objetivos de negocio de la organización. Brinda una visión general del estado de los sistemas de información y permite conocer la efectividad de las medidas de seguridad que se implementen, lo cual, es fundamental para apoyar la toma de decisiones por parte de la alta directiva con relaciones a las estrategias a seguir.

[3] XV Encuesta Global de Seguridad de la Información de Ernst & Young, Pág. 13

La existencia de un sistema de seguridad de la información en las organizaciones genera sentido de pertenencia y apropiación en temas de seguridad en las personas, de tal forma, que se logra la participación activa de toda la organización en la planeación, definición, identificación e implementación de medidas orientadas a salvaguardar la seguridad de la información de la organización.

La implementación de un Sistema de Gestión de Seguridad de la Información, requiere que inicialmente se realicé un proceso ineludible de clasificar los activos de información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la organización, con el propósito de identificar los riesgos de seguridad asociados con la información y de esta forma realizar un análisis para definir y establecer los mecanismos más convenientes para protegerla.

Con base en el diagnóstico de la situación problema, la empresa IGM S.A. requiere implementar un Sistema de Gestión de Seguridad de la Información con el objetivo de fortalecer integralmente en la entidad, los pilares fundamentales de la seguridad correspondiente a la Integridad, Confidencialidad y Disponibilidad de la información y garantizar con esto la debida protección de la información del negocio y la privacidad de la información de sus partes interesadas.

IGM S.A, requiere diseñar, implementar y mantener un Sistema de Gestión de Seguridad de la Información mediante un conjunto coherente de procesos para la gestión eficaz de acceso a la información. Se requiere como conocer el estado actual de sus activos de información, clasificarlos, priorizarlos y determinar su valor en caso de pérdida de información, lo que implica que es necesario que se conozcan los posibles riesgos que afectan la seguridad de la información y se establecen los mecanismos para minimizar el impacto en caso de presentarse la materialización de una vulnerabilidad.

IGM S.A, requiere establecer un Gobierno de Seguridad alineado la cultura organizacional y con las necesidades y objetivos del negocio, compuesto por una estructura organizacional con roles y responsabilidades y un conjunto coherente de políticas, procesos y procedimientos, con el objetivo de forjar, promover y extender una cultura de seguridad en todos los niveles de la organización.

De acuerdo a lo anterior, se puede establecer que el problema está relacionado con un inadecuado modelo de seguridad de la información, lo que significa que es necesario diseñar un Sistema de Gestión de Seguridad de la Información para la

entidad, basado en un estándar de seguridad reconocido a nivel mundial, con el propósito de garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo.

1.1.6. FORMULACION DEL PROBLEMA

¿Un Sistema de Gestión de Seguridad de la Información le proveerá a IGM S.A los elementos, mecanismo y lineamientos adecuados para mejorar la seguridad de la información de la entidad y la gestión y tratamiento de los riesgos asociados al uso de la información?

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información para la empresa IGM S.A., tomando como referencia la norma NTC-ISO-IEC 27001:2013.

1.2.2. OBJETIVO ESPECIFICOS

OE1. Analizar la situación actual de la entidad, con relación a la Gestión de Seguridad de la Información.

OE2. Determinar el Nivel de Madurez en el que se encuentra la entidad para su modelo de seguridad de la información.

OE3. Establecer el nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la ISO 27001:2013 y definir los planes de acción orientados a cerrar las brechas de seguridad encontradas.

OE4. Establecer la estructura organizacional, roles y responsabilidades en cuanto a la Seguridad de la Información.

OE5. Analizar las necesidades y requerimientos de las partes interesas de la entidad con relación al Sistema de Gestión de Seguridad de la Información.

OE6. Definir la política, alcance y objetivos del Sistema de Gestión de Seguridad de la información.

OE7. Definir la metodología para la identificación y clasificación de activos de información y para la valoración y tratamiento de riesgos de Seguridad de la Información.

OE8. Clasificar los activos de información del proceso de Gestión de Tecnología de la entidad, valorar sus riesgos de seguridad y definir los planes de tratamiento de los riegos encontrados, de acuerdo a la metodología definida.

OE9. Definir las políticas de la Seguridad de la Información de la entidad tomando como base la norma ISO 27001:2013.

OE10. Definir un mecanismo para la gestión de incidentes de seguridad.

1.3. ALCANCE Y LIMITACIONES

1.3.1. ALCANCE

El alcance del proyecto abarca el diseño un Sistema de Gestión de Seguridad de la información para la empresa IGM S.A., el cual está orientado a cubrir la primera fase de la implementación de un Sistema de Gestión de Seguridad de la Información, que corresponde a la etapa de planeación.

El alcance del proyecto abarca solo el Proceso de Gestión de Tecnología, para la sede principal de la Entidad, por lo tanto, el proceso de clasificación de activos de información y valoración de riesgos solo se realizará para este proceso.

Para el desarrollo del proyecto se utilizará como guía principal la norma NTC-ISO-IEC 27001 versión 2013, que corresponde a un estándar referente a nivel mundial que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información[4].

1.3.2. LIMITACIONES

El proyecto consistirá solo en el análisis y diseño del Sistema de Gestión de Seguridad de la Información para la empresa IGM S.A, basado en la norma NTC-ISO-IEC 27001:2013, pero no abarca las fases de implementación, revisión y mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.

[4] Wikipedia, ISO/IEC 27001, http://es.wikipedia.org/wiki/ISO/IEC_27001

1.4. RESULTADOS ESPERADOS DEL TRABAJO

1.4.1. ENTREGABLES DEL TRABAJO

A continuación se listan los diferentes entregables del presente trabajo de grado:

- La política, alcance y objetivos del Sistema de Gestión de Seguridad de la información.
- La estructura organizacional, roles y responsabilidades en cuanto a la Seguridad de la Información.
- Análisis de las necesidades y requerimientos de las partes interesas de la entidad con relación al Sistema de Gestión de Seguridad de la Información.
- Metodología para la identificación y clasificación de los activos de información y para el análisis y valoración de riesgos de Seguridad de la Información.
- Inventario de los activos de información resultado de aplicar la metodología de identificación, clasificación y valoración de los activos de información, para el proceso de Gestión de Tecnología.
- Informe de evaluación de riesgos, correspondiente al resultado de aplicar la metodología de análisis y valoración de riesgos de seguridad de la información al proceso de Gestión de Tecnología.
- Plan de tratamiento de riesgos, el cual contendrá las acciones para la gestión de los riesgos de seguridad identificados en el proceso de Gestión de Tecnología.
- Diagnóstico del nivel de cumplimiento de la entidad con relación a los objetivos de control y controles establecidos en el Anexo A de la norma ISO 27001:2013, y los planes de acción orientados de cerrar la brechas encontradas.
- Manual de políticas de seguridad de la Información.
- Procedimiento para la gestión de incidentes de seguridad.

1.4.2. IMPACTO DEL PROYECTO

Con este proyecto se pretende establecer diseñar un adecuado y sostenible modelo de seguridad de la información basado en la norma ISO/IEC 27001:2013, con el propósito de que la seguridad de la información soportada en un Gobierno de Seguridad, apoye y apalanque los objetivos estratégicos de la entidad.

Los objetivos planteados en este proyecto, están orientados a poder diseñar un adecuado Sistema de Gestión de Seguridad de la Información para la entidad, con el propósito de poder generar los siguientes beneficios:

Garantizar su Misión y Alcanzar su visión. El diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013, proveerá los mecanismo adecuados para poder garantizar la protección y aseguramiento de su información, lo cual es fundamental para la debida y segura gestión administrativa, financiera, operativa y técnica de la entidad necesaria para poder garantizar su Misión y alcanzar su Visión.

Mejorar la Imagen de la entidad. Un Sistema de Gestión de Seguridad de la Información le provee a la entidad una metodología para la gestión de riesgos de seguridad de la información, lo cual mejora su imagen antes sus partes interesadas ya que genera confianza debido a que demuestra que la entidad identifica, clasifica, valora y trata de manera adecuada sus riesgos de seguridad.

Disminuir costos. Un Sistema de Gestión de Seguridad de la Información puede generar un impacto positivo en las finanzas de la entidad, ya que en la medida de que los colaboradores tengan una conciencia clara de cuál es la información que se debe proteger y gestionen adecuadamente sus riesgos, se puede evitar inversiones innecesarias en seguridad y tecnología.

Cumplimiento normativo. Sistema de Gestión de Seguridad de la Información permite determinar el estado real de la seguridad de la información de la entidad, conocer las posibles amenazas que la puedan afectar y establecer las acciones efectivas para mitigarlas, lo cual, indique una adecuada gestión de riesgos que garantizar la debida protección de su información y la privacidad de los datos personales de sus clientes, lo cual, ayuda al cumplimiento de la normatividad vigente relacionada con seguridad de la información.

2. JUSTIFICACION

El diseño de un Sistema de Gestión de Seguridad de la Información basado en un modelo de buenas prácticas de seguridad conocido a nivel mundial, como es la norma ISO/IEC 27001:2013, proveerá las condiciones de gobernabilidad, oportunidad y viabilidad necesarias para que la seguridad de la información apoye y extienda los objetivo estratégicos del negocio, mediante la protección y aseguramiento de su información que es fundamental para garantizar la debida gestión financiera, administrativa y operativa de la entidad, y con ello asegurar el cumplimiento de su Misión.

Un Sistema de Gestión de Seguridad de la Información, demuestra el compromiso de la organización hacia la Seguridad de la Información y provee los elementos requeridos para gestionar de manera eficiente los riesgos que puedan atentar con la seguridad de su información, lo cual genera confianza en sus partes interesadas que es fundamental para el crecimiento y la sostenibilidad de la entidad.

Establecer un Sistema de Gestión de Seguridad de la Información, significa que la entidad se caracteriza en relación a la seguridad de la información por tener un modelo de seguridad donde se tiene una estrategia eficaz y es proactiva en la ejecución del plan, que según encuesta global de Seguridad de la Información 2014, realizada por PWC[5], ubicaría a la entidad en el 50% de la organizaciones a nivel mundial que son pioneras en adoptar este tipo de modelos de seguridad.

Un Sistema de Gestión de Seguridad de la Información, le permitirá a la entidad poder contar con un Gobierno de Seguridad alineado a las necesidades y objetivos estratégicos del negocio, compuesto por una estructura organizacional con roles y responsabilidades y un conjunto coherente de políticas, procesos y procedimientos, con el objetivo de forjar, promover y extender una cultura de seguridad en todos los niveles de la organización y de esta forma gestionar de manera adecuada la seguridad de su información.

Un Sistema de Gestión de Seguridad de la Información le permitirá a la Entidad fortalecer integralmente en cada uno de sus colaboradores, los pilares fundamentales de la seguridad correspondiente a la integridad, confidencialidad y

[5] PWC, Resultados de la Encuesta Global de Seguridad de la Información, Pag, 4

disponibilidad de la información, lo cual, ayuda a forjar, fomentar y extender en toda la organización una cultura apropiada de seguridad de la información.

El diseño de un Sistema de Gestión de Seguridad de la Información basado en un estándar de seguridad reconocido a nivel mundial, como es la norma ISO 27001, permitirá estructurar las bases necesarias que permiten forjar un adecuado modelo de seguridad en la entidad basado en mejores practica para la implementación de este tipo de sistemas y sobre todo, permitirá garantizar su mejora continua y su debida permanecía y evolución en el tiempo.

Un Sistema de Gestión de Seguridad de la Información, le permitirá a la entidad gestionar de manera efectiva los riesgos asociados a la seguridad de la información mediante la identificando de amenazas que puedan llegar con comprometer la integridad, disponibilidad y confidencialidad de sus activos de información y con esto poder establecer los mecanismos para minimizar el impacto en caso de presentarse la materialización de una vulnerabilidad.

La implementación de un adecuado Modelo de Seguridad de la Información demuestra el compromiso de la organización hacia la Seguridad de la Información y le proporciona a la entidad las herramientas y elementos necesarios para alcanzar de manera efectiva los siguientes objetivos de seguridad:

- Fomentar la cultura de Seguridad de la Información en todos los niveles de la organización, lo cual facilita la tarea de proteger sus activos de información.
- Generar sentido de pertenencia y apropiación en temas de seguridad en cada uno de los funcionarios de la entidad, logrando con ello la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de la información de la organización.
- Generar mayor conciencia en los funcionarios de la Entidad con relación a los riesgos que pueden afectar la seguridad de la información evitando fugas de información por ataques externos.
- Promover a que los funcionarios adopten, interioricen y acaten la política, procedimientos y las prácticas de seguridad definidas en la entidad, y a su vez comprendan las implicaciones, peligros y riesgos de sus acciones.

- Promover que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados por la organización, así como, que los problemas de seguridad se comuniquen de manera proactiva y oportuna.
- Promover la cultura de mejora continua del sistema de gestión de seguridad de la información, contribuyendo a su mejor administración, desempeño, eficacia y cumplimiento.
- Promover una buena cultura de seguridad al interior de la organización y una conciencia clara de cuál es la información que se debe proteger, evita con esto, inversiones innecesarias en seguridad y tecnología.

Un modelo de Seguridad de la Información, le ayudará a la entidad a medir, cuantificar y mejorar el nivel de cumplimiento de los indicadores que se establecieron para determinar el estado actual de la situación problema. A continuación, se describir con un modelo o Sistema de Seguridad de la Información apoya y apalanca a la entidad en la debida gestión y cumplimiento de dichos indicadores:

Tabla 3. SGSI y cumplimiento de los indicadores

Indicador	Como apoya un modelo de Seguridad de la Información
Nivel de compromiso de los funcionarios en adoptar funciones y responsabilidades de seguridad	• Establece un Gobierno de Seguridad compuesto por una estructura organizacional con roles y responsabilidades de seguridad. • Define funciones y responsabilidades de seguridad asociados a roles y cargos de la entidad. • Define políticas y procedimiento de seguridad. • Promueve la divulgación y sensibilización de las políticas de seguridad con el propósito de garantizar su desempeño, eficacia y cumplimiento. • Promueve que los funcionarios adopten, interioricen y acaten la política, procedimientos y prácticas de seguridad definidas en la entidad y comprendan las implicaciones, peligros y riesgos de sus acciones.
Grado de cubrimiento de los planes de tratamiento de riesgos de seguridad	• Genera sentido de pertenencia y apropiación en temas de seguridad en cada uno de los funcionarios de la entidad, logrando con ello la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de la información de la organización. • Permite disponer de una metodología para la gestión de riesgos, con el objetivo identificar, clasificar y valorar los riesgos que puedan atentar contra la confidencialidad, integridad y disponibilidad de la información. • Permite clasificar los activos de información en términos de su valor,

	requerimientos legales, sensibilidad y criticidad para la Entidad. • Permite determinar la efectividad de los controles existentes orientados a proteger la seguridad de la información. • Permite establecer planes de tratamiento a los riesgos identificados.
Eficacia tratamiento de riesgos	• Permite medir la eficacia de los controles, medidas y actividades establecidas para el cumplimiento de los planes de tratamiento de los riesgos identificados. • Permite reaccionar de manera oportuna y ágil ante incidentes de seguridad gracias a un esquema claro de roles y responsabilidades, minimizando así los impactos de la materialización de una vulnerabilidad. • Permite establecer un modelo o mecanismo para la gestión y monitoreo de los incidentes de seguridad. • Permite contar con los mecanismos para la mejora continua de la seguridad de la información, mediante la supervisión, revisión y eficacia de los procesos implantados. • Promueve que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización, así como, que los problemas de seguridad se comuniquen de manera proactiva y oportuna.
Concienciación en seguridad de la información	• Fomenta la cultura de seguridad de la información a todo nivel dentro de la organización, mediante campañas y/o capacitaciones en temas de seguridad. • Provee herramientas para fomentar en los funcionarios una mayor concienciación con relación a la importancia de la seguridad, evitando fugas de información. • Define un lenguaje común dentro de la Entidad para referirse a la protección de la información. • Enseña a los funcionarios sobre mejores prácticas y buenos hábitos en materia de seguridad. • Una buena cultura de seguridad al interior de la organización y una conciencia clara de cuál es la información que se debe proteger, evita inversiones innecesarias en seguridad y tecnología.

De acuerdo a lo anterior, el establecimiento de un Sistema de Gestión de Seguridad de la Información provee las condiciones de gobernabilidad, oportunidad y viabilidad necesarias para lograr a cabalidad el objetivo deseable de la situación positiva a la que pretende llegar, la cual está relacionada con forjar un '**Adecuado Modelo de Gestión de Seguridad de la Información'.**

3. MARCO DE REFERENCIA

3.1. MARCO TEORICO

Debido a la evolución permanente de las tecnologías de la información y las comunicaciones que demandan un mayor esfuerzo para garantizar la seguridad, a las constantes amenazas que hoy en día atentan contra la seguridad de la información que cada vez son más especializadas, complejas y avanzadas, y a la normatividad vigente que regula y exige una mayor protección y privacidad de los datos sensibles, personales, comerciales y financieros de las personas, la organizaciones deben contar con un modelo o Sistema de Gestión de Seguridad de la Información basado en estándares de seguridad reconocidos a nivel mundial, con el propósito de poder establecer y mantener un gobierno de seguridad alineado a las necesidades y objetivos estratégicos del negocio, compuesto por una estructura organizacional con roles y responsabilidades y un conjunto coherente de políticas, procesos y procedimientos, que le permiten gestionar de manera adecuada los riesgos que puedan atentar contra la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y no repudio de la seguridad de la información.

Para lograr una adecuada gestión de la información es indispensable que las organizaciones establezcan una metodología estructurada, clara y rigurosa para la valoración y tratamiento de los riesgos de seguridad, con el objetivo de (i) conocer el estado real de la seguridad de los activos de información a través de los cuales se gestiona la información del negocio, (ii) identificar y valorar las amenazas que puedan comprometer la seguridad de la información y (iii) determinar los mecanismos y medidas de seguridad a implementar para minimizar el impacto en caso de las posibles pérdidas de confiabilidad, integridad y disponibilidad de la información.

Para efectos de tener claro los diferentes conceptos que se enuncian en este marco teórico, en el capítulo “3.2. MARCO CONCEPTUAL (GLOSARIO DE TERMINOS)” se encuentran el glosario de los términos con sus respectivas definiciones, los cuales son utilizados a lo largo del presente trabajo de grado.

3.1.1. SEGURIDAD DE LA INFORMACION

La Seguridad de la Información, de acuerdo a la norma ISO 27000:2014[6], se define como la preservación de la confidencialidad, integridad y disponibilidad de la información.

De acuerdo a la Asociación Española para la Calidad [4], la Seguridad de la Información tiene como propósito la protección de la información y de los sistemas de la información contra las amenazas y eventos que atenten con el acceso, uso, divulgación, interrupción y destrucción de forma no autorizada[7].

La información representa uno de los activos más valioso de las organizaciones, lo que implica que es indispensable asegurar su protección contra amenazas y eventos que puedan llegar comprometer su confidencialidad, integridad y disponibilidad. La información puede existir en diferentes medios tanto físicos como electrónicos, pero independientemente del medio, es necesario que las organizaciones garanticen y aseguren la debida protección de la información durante su recolección, almacenamiento, tratamiento y uso.

La seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de la información mediante el establecimiento de un conjunto coherente de procesos, normas y herramientas para la gestión eficaz de acceso a la información, y la implementación de mecanismos y medidas de seguridad tanto físicas como lógicas, orientadas a la prevención y detección de amenazas internas y externas que puedan atentar contra la seguridad de la organización y la continuidad del negocio.

La seguridad de la información en una organización, es un proceso de mejora continua que demanda la participación activa de toda la organización y busca preservar, entre otros, los siguientes principios de la información:

- La **confidencialidad,** asegurando que solo las personas debidamente autorizadas tengan acceso a la información.
- La **disponibilidad**, asegurando que la información esté totalmente disponible para las personas debidamente autorizadas cuando ellos la requieran.

[6] ISO/IEC 27000:2014, Tercera Edición, Pág. 4
[7] http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

- La **integridad**, asegurando que la información no sea modificada sin la debida autorización.
- La **autenticidad,** con el propósito de garantizar la identidad de la persona que genera la información. La autenticidad de la información, es la capacidad de asegurar que el emisor de la información es quien dice ser y no un tercero que esté intentando suplantarlo.
- El **no repudio,** con el propósito de conocer exactamente quienes son los actores que participan en una transacción o una comunicación y no puedan negarlo en ningún momento. El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje[8].
- La **trazabilidad,** con el objetivo de poder monitorear o rastrear cualquier operación que se realiza sobre la información desde su mismo origen.

La seguridad de la información dentro de las organizaciones, depende del nivel de protección y seguridad de sus activos de información, por lo tanto es fundamental la implementación de medidas y controles de seguridad adecuados, y el permanente monitoreo, revisión y mejora de los mismos de manera proactiva con el objetivo de garantizar su efectividad.

3.1.2. GESTION DE SEGURIDAD DE LA INFORMACION

La gestión de la seguridad de la información es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados por todos los miembros de 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[9].

La gestión de la seguridad de la información requiere la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de la información, así como el debido control de acceso a los recursos y activos de información.

La gestión de la seguridad de la información, implica que las organizaciones clasifican sus activos de información en términos de su valor, requerimientos

[8] Wikipedia, Seguridad de la información
[9] http://www.iso27000.es/sgsi.html

legales, sensibilidad y criticidad, con el propósito de identificar los riesgos que pueden afectar su seguridad y determinar las medidas de prevención, detección, retardo y reacción que se requieran implementar para controlar el acceder no autorizado a las instalaciones, recursos, sistemas e información de la organización, o cualquier amenaza proveniente del entorno, la naturaleza y las acciones del hombre que pueda llegar a comprometer el normal funcionamiento y operación del negocio.

3.1.3. SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Con el objetivo de garantizar que las organizaciones realizan una correcta gestión de la seguridad de la información, es necesario contar con un proceso sistemático, documento, conocido y adoptado por toda la organización, basado en un enfoque de gestión de riesgos. Este proceso, es el que constituye un Sistema de Gestión de Seguridad de la Información.

De acuerdo a la norma NTC-ISO-IEC 27001:2013[10], un sistema de gestión de seguridad de la información tiene por finalidad preservar la confidencialidad, integridad y disponibilidad de la información, a través de la aplicación de un proceso de gestión del riesgo.

Un Sistema de Gestión de Seguridad de la Información, le permite a la organizaciones gestionar de manera efectiva los riesgos asociados a la seguridad sobre sus activos de información mediante la identificación de las amenazas que puedan llegar con comprometer la seguridad sus activos de información, lo cual, genera confianza en sus partes interesadas debido a que demuestra que los riesgos de la organización son debidamente gestionados.

Un Sistema de Gestión de Seguridad de la Información permite el establecimiento de un gobierno de seguridad, soportado en una estructura organizacional, responsabilidades, políticas, procedimientos, procesos y recursos, para gestionar de manera adecuada la seguridad de la información. Proporciona una herramienta que le ayuda a las organizaciones a establecer políticas, procedimientos, medidas y controles de seguridad alineados a los objetivos de negocio, y provee los elementos adecuados para la debida gestión de los riesgos con propósito de poder mantener el riesgo por debajo del nivel definido por la organización.

[10] NTC-ISO-IEC 27001:2013, Capitulo Introducción

Un Sistema de Gestión de la Seguridad de la Información le permite a las organizaciones tener una visión general del estado de protección y vulnerabilidad de sus activos de información y de la efectividad de las medidas de seguridad que se implementen, insumos que son fundamentales para apoyar la toma de decisiones por parte de la alta directiva con relaciones a las estrategias a seguir.

La implementación de un Sistema de Gestión de Seguridad de la Información, le provee a las organizaciones un proceso de mejora continua que asegura la debida y continua gestión de los riesgos de seguridad y permite la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de los activos de información de la organización.

3.1.4. NORMAS ISO/IEC 27000

La familia de las normas ISO/IEC 27000, son un marco de referencia de seguridad a nivel mundial desarrollado por la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización. Estas normas especifican los requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

En Colombia, el Instituto Colombiano de Norma Técnicas y Certificaciones, ICONTEC, es el organismo encargado de normalizar este tipo de normas.

Las siguientes son algunas de las normas que componen la familia ISO/IEC 27000, las cuales serán el marco teórico que se tendrá en cuenta para efectos del presente trabajo:

- **ISO/IEC 27000**. Esta norma proporciona una visión general de los sistemas de gestión de seguridad de la información y contiene los términos y definiciones que se utilizan en las diferentes normas de la 27000.
- **ISO/IEC 27001**. La última versión de esta norma fue publicada a finales del 2013, y corresponde a la principal norma de la serie 27000 debido a que contiene los diferentes requisitos para establecer, implementar, mantener y

mejorar continuamente un Sistema de Gestión de Seguridad de la Información en las organizaciones independiente de su tipo, tamaño o naturaleza. Esta norma también incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adoptadas a las necesidades de la organización[11].

La versión 2013 de la norma ISO 27001, alineo su estructura conforme a los lineamientos definidos en el Anexo SL[12] de las directivas ISO/IEC, con el objetivo de mantener la compatibilidad entre las normas ISO de sistemas de gestión que se han ajustado a este anexo. Este enfoque de la estructura de la nueva ISO27001:2013 basado en el Anexo SL, le ayuda a las organizaciones que deseen integrar sus diferentes sistemas de gestión, como el de Calidad, Ambiental, Seguridad de la Información, etc., en un único sistema integrado de gestión, debido a que las normas ISO que se han ajustado al Anexo SL, manejan aspectos comunes como, la misma estructura de alto nivel e idénticos títulos de numerales, textos y términos.

Los dominios de la norma ISO/IEC 27001:2013 corresponde a los diferentes capítulos que establecen los requerimientos que las organizaciones deben cumplir para el establecimiento de un Sistema de Gestión de Seguridad de la Información, los cuales se resumen a continuación:

Tabla 4. Dominios de la norma ISO/IEC 27001:2013

0. INTRODUCCION
1. OBJETO Y CAMPO DE APLICACIÓN
2. REFERENCIAS NORMATIVAS
3. TÉRMINOS Y DEFINICIONES
4. CONTEXTO DE LA ORGANIZACIÓN
5. LIDERAZGO
6. PLANIFICACIÓN
7. SOPORTE
8. OPERACIÓN
9. EVALUACIÓN DE DESEMPEÑO
10. MEJORA

[11] NTC-ISO-IEC 27001:2013, Pág. 1

[12] Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

El Anexo A de la norma ISO 27001, contiene los diferentes objetivos de control y controles que las organizaciones deberían tener en cuenta para la planeación e implementación de su Sistema de Gestión de Seguridad de la Información, los cuales se describen con más detalle en la norma ISO 27002.

- **ISO/IEC 27002**. Guía de buenas prácticas en seguridad de la información que describe de forma detallada las acciones que se deben tener en cuenta para el establecimiento e implementación de los objetivos de control y controles descritos de una forma general en el Anexo A de la norma ISO 27001.
- **ISO/IEC 27003.** Guía que contiene aspectos necesarios para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información de acuerdo a los requerimientos establecidos en la norma ISO/IEC 27001, donde se describe el proceso desde la planeación hasta la puesta en marcha de planes de implementación.
- **ISO/IEC 27004.** Guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un Sistema de Gestión de Seguridad de la Información y de los objetivos de control y controles implementados de acuerdo al Anexo A de la norma ISO 27001[13].
- **ISO/IEC 27005.** Esta norma establece los lineamientos para la gestión de riesgos de seguridad de la información y está diseñada para ayudar a las organizaciones en la implementación de un Sistema de Gestión de Seguridad de la Información basada es un enfoque de gestión de riesgos. Entre otros aspectos, establecer lo requerimiento que se deben tener en cuenta para el proceso de valoración de riesgos, relacionados con la identificación, análisis, evaluación y tratamiento de los riesgos en la seguridad de la información.
- **ISO/IEC 27006.** Establece los requisitos relacionados en la norma ISO 27001 que deben cumplir las organizaciones para la acreditación de entidades de auditoría y certificación de Sistemas de Gestión de Seguridad de la Información.
- **ISO/IEC 27035.** Proporciona una guía sobre la gestión de incidentes de seguridad en la información

[13] http://www.iso27000.es/iso27000.html

3.1.5. CICLO DE MEJORA CONTINÚA VS NORMA ISO/IEC 27001:2013

El ciclo de mejora continua, también conocido como ciclo PDCA (del inglés **plan-do-check-act)** o PHVA (**planificar-hacer-verificar-actuar**) o Ciclo de Deming por ser Edwards Deming su creador, es uno de los sistemas más usados para la implementación de un sistema de mejora continua, el cual establece los siguientes cuatro pasos o fases esenciales que de forma sistemática las organizaciones deben llevar a cabo para lograr la mejora continua de sus sistemas de gestión:

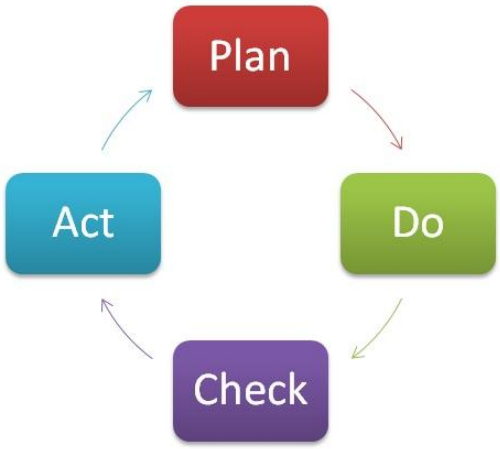


Figura 2. Ciclo de mejora continua (Ciclo Deming)
Fuente: http://www.pdcahome.com/5202/ciclo-pdca/

- **Fase Planificar (Plan):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- **Pase Hacer (Do):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Verificar (Check):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- **Fase Actuar (Act):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

En la versión 2013 de la norma ISO/IEC 27001, no aparece la sección de "Enfoque basado en procesos" que existía en la versión 2005, lo cual brinda una

mayor flexibilidad en el momento de seleccionar o definir un modelo para la mejora continua del Sistema de Gestión de Seguridad de la Información. Aunque en la versión 2013, no se determina el modelo PHVA como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:

Figura 3. Ciclo de mejora continua alineado a la norma ISO 27001:2013
Fuente: Elaborada con base en la información publicada en la página web http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

El siguiente cuadro muestra la relación entre las fases del ciclo de mejora continua 'PHVA' (planear, hacer, verificar y actuar) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Tabla 5. Fases PHVA vs Estructura ISO 27001:2013

Fase PHVA	Capitulo ISO 27001:2013
PLANEAR	4. Contexto de la Organización 5. Liderazgos 6. Planificación 7. Soporte
HACER	8. Operación
VERIFICAR	9. Evaluación de desempeño
ACTUAR	10. Mejora

- **Fase PLANEAR en la norma ISO 27001:2013**

  En el **capítulo 4** - **Contexto de la organización**[14] de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del SGSI.

  En el **capítulo 5 - Liderazgo**[15], se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización, aseguren la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.

  En el **capítulo 6 - Planeación**[16], se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

  En el **capítulo 7 - Soporte**[17] se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua Sistema de Gestión de Seguridad de la Información.

- **Fase HACER en la norma ISO 27001:2013.** En el **capítulo 8 - Operación**[18] de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

- **Fase VERIFICAR en la norma ISO 27001:2013.** En el **capítulo 9 - Evaluación del desempeño**[19]**,** se define los requerimientos para evaluar

[14] NTC-ISO-IEC 27001:2013, Pág. 1-2
[15] Ibídem, Pág. 2-3
[16] Ibídem, Pág. 4-6
[17] Ibídem, Pág. 6
[18] Ibídem, Pág. 8-9
[19] Ibídem, Pág. 9-11

periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

- **Fase ACTUAR en la norma ISO 27001:2013.** En el **capítulo 10 - Mejora**[20], se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

3.2. MARCO CONCEPTUAL (GLOSARIO DE TERMINOS)

Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

Amenaza: Es la causa potencial de un daño a un activo de información.

Anexo SL: Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

Causa: Razón por la cual el riesgo sucede.

Ciclo de Deming: Modelo mejora continua para la implementación de un sistema de mejora continua.

Colaborador: Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.

Confidencialidad: Propiedad que determina que la información no esté disponible a personas no autorizados

[20] NTC-ISO-IEC 27001:2013, Pág. 11-12

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Disponibilidad: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.

Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

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

Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.

Responsables del Activo: Personas responsables del activo de información.

Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

PSE: Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.

SARC: Siglas del Sistema de Administración de Riesgo Crediticio.

SARL: Siglas del Sistema de Administración de Riesgo de Liquidez.

SARLAFT: Siglas del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo.

SARO: Siglas del Sistema de Administración de Riesgos Operativos.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

4. METODOLOGIA

En el presente capitulo, se describe los métodos utilizados para alcanzar la solución al problema planteado que corresponde a un **Inadecuado Modelo de Gestión de Seguridad de la Información** de IGM S.A, teniendo en cuenta para esto, los objetivos y el alcance que se plantearon en el presente trabajo de investigación.

La metodología planteada pretende dar cumplimiento a los objetivos específicos que se definieron con el propósito de poder alcanzar el objetivo general de proyecto, para lo cual, esta metodología tendrá en cuenta el marco de referencia de la norma ISO/IEC 27001:2013 que especifica, entre otros aspectos, los requerimientos y actividades que se deben desarrollar para el diseño de un Sistema de Gestión de Seguridad de la Información.

4.1. TIPO DE INVESTIGACION

Tiendo en cuenta la características del proyecto, se empleará en el desarrollo del mismo el método investigación de tipo factible, que de acuerdo al "*Manual de Tesis de Grado y Especialización y Maestría y Tesis Doctorales*" [5] de la Universidad Pedagógica Experimental Libertador, consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos[21]. Con base en la anterior definición, el presente trabajo corresponde al análisis y desarrollo de una propuesta para el diseño de un Sistema de Gestión de Seguridad de la Información para entidad IGM S.A, de acuerdo al alcance definido, las necesidades de la entidad y tomando para base para ello el modelo de referencia de seguridad de la norma ISO/IEC 27001:2013.

También, durante el desarrollo del proyecto se utilizara el método de investigación de campo, que permite el análisis sistemático del problema en la realidad, con el fin de describirlo, interpretarlo, entender su naturaleza y explicar sus causas y

[21] Manual de Tesis de Grado y Especialización y Maestría y Tesis Doctorales de la Universidad Pedagógica Libertador, Pág.13.

efectos[22]. En este tipo de investigación, la información de interés es recogida de forma directa de la fuente, mediante encuestas, cuestionario, entrevista o reuniones.

4.2. LINEA DE INVESTIGACION

Tomando como referencia la norma ISO/IEC 27001:2013, se puede determinar que la línea de investigación del presente trabajo esta relacionados con los siguientes temas: Tecnología de la información, Seguridad de la Información, Gestión de la Seguridad, Gestión de Riesgos y Sistema de Gestión de Seguridad de la Información.

4.3. INSTRUMENTOS DE RECOLECCION DE INFORMACION

Para el desarrollo del presente trabajo de grado, se utilizaron los siguientes mecanismos e instrumentos para la recolección de información:

- Cuestionario.
- Observaciones.
- Entrevistas con funcionarios y sobre todo con el personal de la Dirección de Tecnología de la Entidad.
- Documentación existente en el sistema de gestión calidad de la entidad.
- Evaluación con base en la experiencia del autor.

También, se usó de diferentes fuentes de información, tales como tesis, libros, textos, revistas, normas, etc., existentes tanto en medios físicos, electrónicos y publicados en Internet.

4.4. FASES METODOLOGICAS

Teniendo en cuenta los requerimientos establecidos en la norma ISO/IEC 27001:2013 para el diseño del Sistema de Gestión de Seguridad de la Información, se establecieron las siguientes fases para el desarrollo del proyecto:

[22] Manual de Tesis de Grado y Especialización y Maestría y Tesis Doctorales de la Universidad Pedagógica Libertador, Pág.11

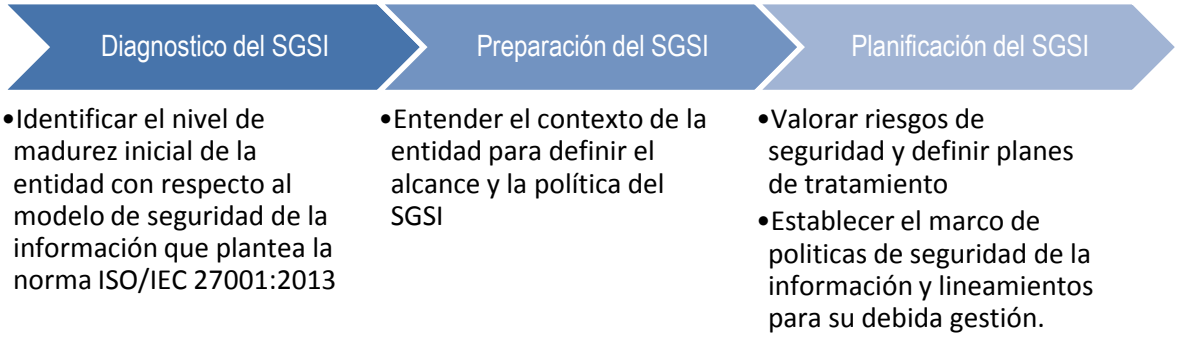


Figura 4. Fases para la diseño del SGSI
Fuente: El autor

Para llevar a cabo las fases propuestas para el diseño del Sistema de Gestión de Seguridad de la Entidad, las siguientes son las actividades a realizar:

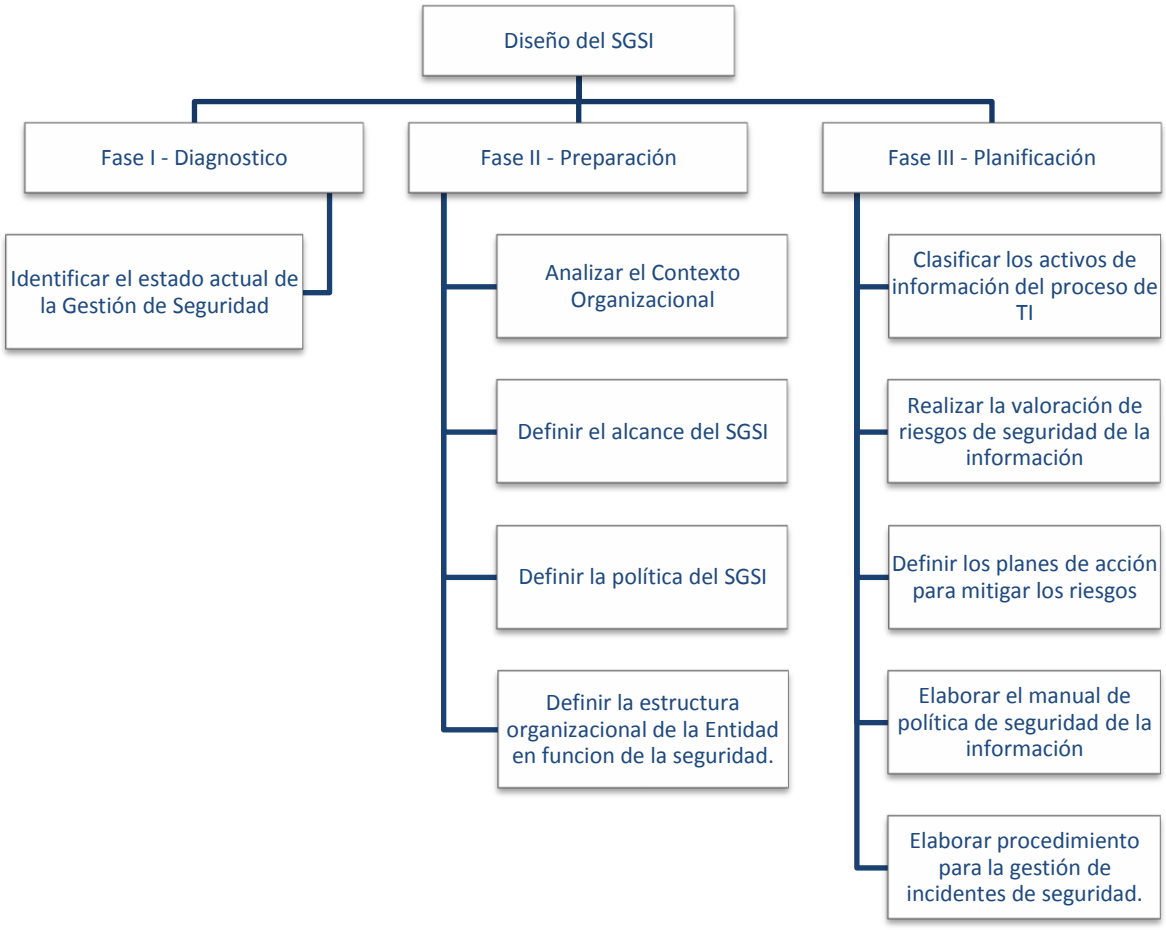


Figura 5. Fases para el diseño del SGSI de la Entidad
Fuente: El autor

Fase I - Diagnostico.

Corresponde a las actividades para identificar el nivel de madurez inicial de la Entidad con respecto al modelo de seguridad de la información que plantea la norma ISO/IEC 27001:2013.

Para la recolección de la información, en esta fase se utilizarán mecanismo como:

- Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento de le entidad con relación a los dominios de la norma ISO/IEC 27001:2013.
- Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.
- Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

Fase II - Preparación

Corresponde a las actividades que se desarrollaran para establecer el Sistema de Gestión de Seguridad de la Información, las cuales corresponde a:

- Analizar el contexto organización, que de acuerdo a los requerimientos establecidos en el “Capítulo 4.1 – Conocimiento de la organización y de su contexto”[23] de la norma ISO/IEC 27001:2013, corresponde a determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Sistema de Gestión de Seguridad de la Información.
- Definir el alcance del SGSI, en el cual se establece los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información[24].
- Definir la política del Sistema de Gestión de Seguridad de la Información.
- Definir la estructura organizacional de la Entidad que contendrá los roles y responsabilidad pertinentes a la seguridad de la información.

Fase III – Planificación.

[23] NTC-ISO-IEC 27001:2013, Pág. 1
[24] Ibídem, Pág. 2

Esta fase contempla las actividades relacionadas con:

- Identificar los activos de información del proceso de gestión de tecnología y clasificarlos de acuerdo a su criticidad y protección.
- Realizar la valoración de riesgos de seguridad de la información de acuerdo al alcance del SGSI.
- Definir los planes de acción que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos. Para la seleccionar de los controles, se tomará como base los objetivos de control y los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013.
- Elaborar la declaración de aplicabilidad, que corresponde a un documento que contiene los objetivos de control y controles seleccionados del anexo A de la norma ISO/IEC 27001:2013, su nivel de cumplimiento y los motivos para su elección o exclusión.
- Elaborar el manual de política de seguridad de la información, que corresponde a un documento que contiene las políticas y los lineamientos que se implementaran en la Entidad con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información.
- Elaborar el procedimiento para la gestión de incidentes de seguridad, que corresponde a un documento que contiene el proceso para el reporte, atención y respuesta a incidencias de seguridad.

El desarrollo de las fases que se plantearon en esta metodología para el diseño del Sistema de Gestión de Seguridad de la información de la entidad, se encuentran descritas y desarrolladas en el próximo capítulo.

5. DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Este capítulo corresponde al desarrollo de las diferentes fases que se definieron para el diseño del Sistema de Gestión de Seguridad de la Información de la empresa IGM S.A, las cuales contemplan una serie de actividad cuya ejecución permiten alcanzar los objetivos específicos que establecidos para el logro del objetivo general del presente trabajo de grado.

A lo largo de este capítulo, se relaciona los diferentes elementos, insumos, datos recolectados, valoraciones y cálculos realizados para el desarrollo de cada una de las actividades de las fases de la metodología definida para el diseño del Sistema de Gestión de Seguridad de la Información de la Entidad.

Los siguientes son algunos de estos elementos:

- La información o datos que se obtuvieron a través de las diferentes técnicas de recolección de información y que utilizaron con insumo para llevar a cabo los respectivos análisis y diagnósticos.
- El resultado de cada uno de los análisis realizados.
- El resultado del proceso de valoración de riesgos.
- Los capítulos de la norma ISO/IEC 27001:2013 que contienen los requerimientos de seguridad que se deben cumplir.
- Los objetivos de control y controles relacionados en el Anexo A de la norma ISO/IEC 27001:2013.

5.1. FASE I. DIAGNOSTICO

En este capítulo se presentan los diagnósticos que se realizaron con el objetivo de poder tener un conocimiento inicial de la situación que presenta la entidad frente al establecimiento de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013.

5.1.1. DIAGNOSTICO ESTADO ACTUAL DE LA SEGURIDAD

El capítulo **1.1.3. DIAGNOSTICO SITUACION PROBLEMA** del presente documento, presenta un análisis detallado de las diferentes situaciones que afectan la seguridad de la entidad que permitieron establecer que el problema está asociado a un “*Inadecuado Modelo de Gestión de Seguridad de la Información*”.

En términos general, las siguientes fueron las situaciones identificadas:

- Falta de un adecuado Gobierno de Seguridad en la Entidad.
- La falta de concienciación, apropiación y conocimiento en temas de seguridad por parte de todos los funcionarios
- No existe una participación activa de toda la organización en la definición de controles de seguridad basados en una evaluación de riesgos
- Los funcionarios no conciben la diferencia entre seguridad informática y seguridad de la información
- No se cuentas con un sistema de información adecuado para la gestión de riesgos de seguridad.
- No existe una valoración de riesgos de seguridad.
- La política de seguridad no está alineada con los objetivos del negocio.

5.1.2. IDENTIFICACION ESTRATIFICACION DE LA ENTIDAD

La identificación del nivel de estratificación de la entidad permite identificar de forma general, el nivel de complejidad que le puede significar a la entidad la implementación de su Sistema de Gestión de Seguridad de la Información. Para lo cual, se tomó como referencia el método planteado en el documento "*ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES*" del modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0 [6], el cual define tres tipos de estratos de entidades: bajo, medio y alto[25], y cuyo valor se obtiene al realizar una evaluación de los siguientes aspectos: el valor del presupuesto de funcionamiento, la infraestructura asociada al número total de computadores, los servicios ofrecidos en línea y el tamaño y capacidad del área de sistemas[26].

Para establecer el nivel de estratificación de la entidad se utilizó el formato relacionado en el Anexo A del presente trabajo de grado, el cual, se muestra a continuación con las respuestas que fueron seleccionadas de acuerdo a la información suministrada por la entidad y el respectivo el puntaje asignado a cada una de ellas, puntajes que fueron sumados para así obtener el valor de estratificación de la entidad:

[25] Anexo 3: Estratificación de Entidades - Modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0, Pág. 8.
[26] Ibídem.

Tabla 6. Valoración estratificación de la entidad

PARAMETROS DE EVALUACION	OPCIONES DE RESPUESTA	PUNTOS	OBSERVACION
Presupuesto	Menos de 3,000 millones de pesos	**3**	Para el 2014: $146.362.311.000. Fuente: área de Contabilidad.
	Entre 3.000 millones y 50.000 millones de pesos		
	Más de 50.000 millones de pesos		
Número total de computadores	Menos de 100 computadores	**3**	Dato suministrado por la dirección de tecnología.
	Entre 100 y 500 computadores		
	Más de 500 computadores		
Número de Servidores	Menos de 4 Servidores	**3**	Dato suministrado por la dirección de tecnología
	Entre 4 y 20 Servidores		
	Más de 20 Servidores		
Número Empleados de Tecnología	Menos de 6 empleados	**2**	Dato suministrado por la dirección de tecnología
	Entre 6 y 50 empleados		
	Más de 50 empleados		
Existencia y función del área de sistemas (tecnología).	No hay área de sistemas o tecnología como tal	**3**	Dato suministrado por la dirección de tecnología
	Área de tecnología enfocada en la operación del día a día, que cumple labores en su mayoría REACTIVAS		
	Punto anterior más área de sistemas que planea y desarrolla proyectos nuevos o de actualización, administra su presupuesto y desarrolla labores proactivas a través de comités y participación en decisiones corporativas		
Existencia y objeto de la WAN.	WAN pública (p.ej. Internet) sólo para usar correo y navegar. Incluye servidores de correo y Web en hosting.	**3**	Dato suministrado por la dirección de tecnología
	WAN pública (p.ej. Internet) con servicios ofrecidos al ciudadano. Puede o no haber desarrollos sofisticados de transaccionalidad.		
	Lo anterior más la existencia de una WAN privada (no incluye VPN a través de Internet)		
Transaccionalidad en la WEB.	Solo ofrece servicios de consulta (páginas WEB estáticas y correo electrónico)	**3**	Dato suministrado por la dirección de tecnología. Aplicación web para el pago de créditos por PSE
	Transaccionalidad local. Generación de servicios y seguimiento de trámites, solo con base en datos y aplicativos propios.		
	Lo anterior más interacción con aplicativos, datos y servicios de otras entidades y/o terceros		
Desarrollo de Software.	No desarrolla software. Incluye aquellas entidades que tienen en hosting una página WEB básica e informativa y un servidor de correo.	**2**	Dato suministrado por la dirección de tecnología.
	Sí desarrolla software pero solo para aplicativos internos. Hay que aclarar que este desarrollo puede ser interno o en outsourcing (realizado por terceros).		
	Sí desarrolla software para aplicativos externos. Sí publica información transaccional.		
	TOTAL PUNTOS	**22**	

El puntaje total de la estratificación se determina por la suma de los puntajes independientes obtenidos de cada una de las respuestas, que para el caso de la entidad es igual a **22 puntos.**

El nivel de estratificación de la entidad, de acuerdo al puntaje obtenido, se determina con base en los rangos de valores relacionados en la siguiente tabla:

Tabla 7. Rangos de Estratificación de Entidades[27]

RANGO DE PUNTOS	ESTRATO
Menor a 10 puntos	BAJO
Entre 11 y 22 puntos	**MEDIO**
Mayor a 22 puntos	ALTO

De acuerdo al puntaje obtenido por la entidad, **22 puntos**, el nivel de estratificación de la misma se encuentra clasificado en un nivel **MEDIO**, lo que inicialmente implicaría un esfuerzo considerable para la implementación de su Sistema de Gestión de Seguridad de la Información.

Con base en la información suministrada por la Entidad para determinar su nivel de estratificación, se realizaron los siguientes análisis:

- El presupuesto de la entidad para el año 2014 fue aproximadamente de $146.362.311.000, lo que supondría que la entidad pude asegurar la disponibilidad de los recursos necesarios para el Sistema de Gestión de Seguridad de la Información de acuerdo a lo establecido en el numeral c) del capítulo 5.1 ´Liderazgo y Compromiso' de la norma ISO/IEC 27001:2013[28].
- El número de computadores y servidores que posee la entidad, implica un mayor esfuerzo para garantizar la seguridad de estos activos de información, por lo tanto, es esencial que se incluyan en el proceso de valoración de riesgos para determinar su nivel de protección y las medidas de seguridad a implementar para salvaguardarlos. Lo anterior es indispensable para cumplir los requerimientos establecidos en los controles '**6.1.2 Valoración de riesgos**

[27] Anexo 3: Estratificación de Entidades - Modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0, Pág. 12.
[28] Norma ISO/IEC 27001:2013, Pág. 2

de la seguridad de la información'[29] y '**6.1.3 Tratamiento de riesgos de la seguridad de la información'**[30] de la norma ISO/IEC 27001:2013.

- El número de empleados de la aérea de tecnología, refleja el tamaño de la entidad y los recursos que implica atender los requerimientos de los usuarios y la prestación de los servicios de tecnología. A pesar de que el área de tecnológica cuenta con estos recursos humanos, los mismos pueden no ser suficientes para la implementación de las medidas y controles que se establezcan productos de los diagnósticos y valoración de riesgos de seguridad que se realicen. Por lo tanto, este un factor que puede implicar un mayor esfuerzo para la implementación de su Sistema de Gestión de Seguridad de la Información.
- El área de tecnología de la entidad, además de administrar y proveer los recursos tecnológicos, planea y desarrolla proyecto, factor fundamente en caso de requerir la implementación planes de acción y/o medidas de seguridad que impliquen el establecimiento de un proyecto para su ejecución.

5.1.3. NIVEL DE CUMPLIMIENTO ANEXO A - ISO 27001:2013

Por medio de este análisis, se estableció el nivel de cumplimiento de la entidad con relación a los objetivos de control y controles definidos en el Anexo A de la norma ISO/IEC 27001:2013, cuyo resultado permitió definir una serie de acciones orientas a poder cerrar las brechas encontradas que deben ser implementadas por la entidad en la fase de operación del SGSI con el objetivo de asegurar la integridad, confidencialidad y disponibilidad de su información.

Para realizar este diagnóstico se utilizó una lista de chequeo basada en un conjunto de preguntas con opción de respuesta 'SI' o 'NO', que fue respondida por funcionarios de las áreas de la entidad de acuerdo al objetivo de control que se estaba evaluando. Las áreas que participaron en esta evaluación fueron, la Vicepresidencia de Riesgos, Dirección de Tecnología, Gestión Humana y Jefatura de Recursos Físicos, ya que los controles de la norma ISO/IEC 27001:2013 están orientados a proteger la seguridad de las personas, de la infraestructura física y lógica, de los recursos tecnológicos y por ende de la información.

[29] Norma ISO/IEC 27001:2013, Pág. 4
[30] Ibídem, Pág. 5

El formato utilizado para realizar este diagnóstico corresponde al ANEXO B del presente documento, el cual, contiene las preguntas que se plantearon para evaluar cada uno de los controles y las respectivas respuestas dadas por los usuarios. Con base en la información recopilada, los siguientes son los resultados del análisis realizado:

De acuerdo a la siguiente gráfica, el nivel de cumplimiento de la entidad con relación a los controles del Anexo A de la norma ISO 27001:2013, es de **46.09%**:

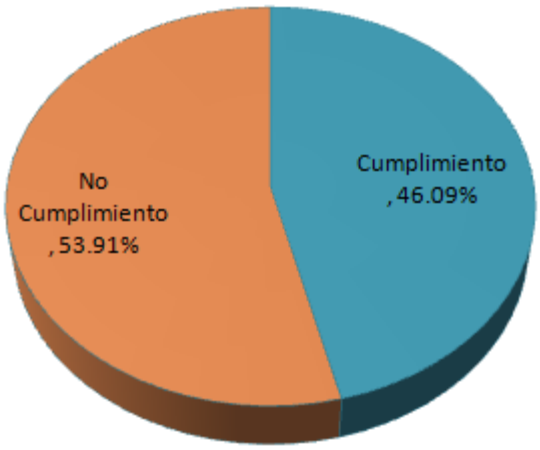


Figura 6. Nivel de cumplimiento controles Anexo A ISO 27001:2013
Fuente: El autor

Lo anterior significa que la implementación del Sistema de Gestión de Seguridad de la información de acuerdo al nivel de cumplimiento de los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013, le implicará a la entidad un refuerzo considerable debido a la ausencia de controles o al bajo grado de cumplimiento de muchos de ellos. Algunos de estos controles requieran la adquisición, adecuación o mejora de mecanismos y herramientas tecnológicas con el propositivo de poder garantizar su debida efectividad, lo que implica, que en algunos de estos casos la entidad deberá adelantar procesos de contratación para la adquisición de soluciones tecnológicas cuyos costos pueden ser elevados y su implementación puede demandar un tiempo considerable.

El nivel de cumplimiento de los controles del Anexo A de la ISO 27001:2013 indica, el grado de madures de la entidad frente a la gestión de la seguridad de la información, el nivel de protección de sus activos de información, el nivel de cumplimiento de la normatividad vigente relacionada con seguridad de la información y el nivel de riesgos de la entidad a partir de los controles

implementados de acuerdo al cumplimiento riguroso de los requerimientos establecidos en la norma.

El modelo de seguridad de la información para la estrategia de gobierno en línea, SISTEMA SANSI [7], determina que el nivel de riesgo de las entidades a partir del nivel de cumplimiento de los controles se clasifica en Alto, Medio y Bajo[31]. Con base en esta clasificación se definió la siguiente tabla de medición:

Tabla 8. Nivel de riesgos vs nivel cumplimiento controles

Porcentaje cumplimiento controles	**Nivel de riesgo e implicaciones**	
Alto	Bajo	Los controles de seguridad que se tienen implementados demuestran un grado alto de madures de la entidad hacia la seguridad de la información y un nivel apropiado de protección de sus activos de información. Esta situación representa un riesgo bajo para la entidad.
Medio	Medio	La entidad cuenta con controles implementados, algunos de ellos no documentos o no adecuados, que requieren su revisión en un medio plazo para mejorar su efectividad y su cumplimiento. Esta situación representa un Riesgo Medio para la entidad debido a la presencia de debilidades en algunos de sus controles que pueden ser aprovechadas por amenazas internas o externas para atentar contra la seguridad de la información. También es necesario revisar el nivel cumplimiento de la normatividad vigente relacionada con seguridad de la información.
Bajo	Alto	La ausencia de controles o el bajo grado de cumplimiento de los mismos, representa un riesgo ALTO para la entidad debido al inadecuado nivel de protección de sus activos de información y/o al incumplimiento de la normatividad vigente relacionado con seguridad de la información. Para este caso, es necesario que se implementen con carácter urgente las medidas de seguridad en un corto plazo con el objetivo de cerrar las brechas encontradas.

De acuerdo al nivel de cumplimento frente al Anexo A de la norma ISO/IEC 27001:2013, la entidad se encuentra en un grado MEDIO de implementación (**46.09%**) de los requerimientos establecidos en los objetivos de control y controles

[31] Modelo de Seguridad de la Información, SISTEMA SANSI - SGSI – Modelo de Seguridad de la información para la estrategia de gobierno en línea, Pág., 47.

de este anexo y en un nivel de riesgo MEDIO con relación al nivel de protección y efectividad de los controles implementados.

El siguiente es el resultado de la evaluación de cada uno de los objetivos de control del Anexo A de la norma ISO/IEC 27001:2013:

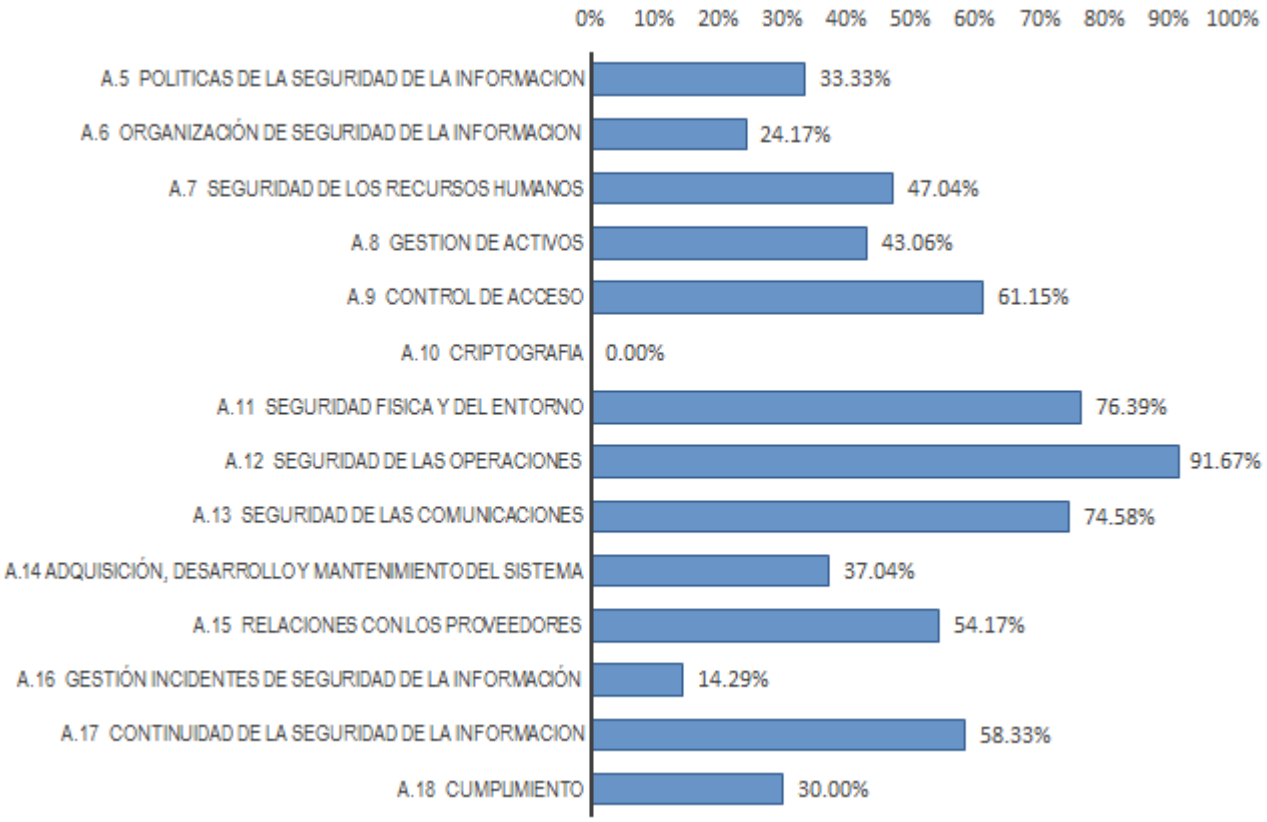


Figura 7. Nivel Cumplimiento Objetivos de Control Anexo A ISO 27001:2013
Fuente: Autor

OBJETIVOS DE CONTROL CON NIVEL DE CUMPLIMIENTO 'BAJO'

Los siguientes son los objetivos de control del Anexo A de la norma ISO/IEC 27001:2013 cuyo cumplimiento por parte de la entidad se encuentran en un nivel BAJO (menor o igual al 33%), lo que representa un riesgo ALTO para la entidad debido a la ausencia o inadecuada implementación de los controles que generan un nivel de bajo protección de sus activos de información y/o en algunos casos, el incumplimiento de la normatividad vigente relacionado con seguridad de la información.

Tabla 9. Objetivos de control con nivel BAJO de cumplimiento

OBJETIVO DE CONTROL	% CUMPLIMIENTO
A.10 CRIPTOGRAFIA	0%
A.16 GESTIÓN INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	14%
A.6 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACION	24%
A.18 CUMPLIMIENTO	30%
A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION	33%

- **A.10 Criptográfica (0%)**

  Tiene por objetivo asegurar el uso apropiado y eficaz de mecanismo criptográficos para proteger la confidencialidad, autenticidad e integridad de la información[32]. La entidad no cuenta con mecanismos de cifrado para proteger la información en tránsito y/o reposo, lo cual representa un riesgo de nivel ALTO debido que no se garantizar la confidencialidad, integridad, autenticidad y no repudio de la información sensible de la entidad que se intercambia entre las áreas o con terceros. Esta situación, además de poner en riesgo la información sensible de la entidad, puede implicarle sanciones legales por incumplimiento normativo que exige la debida protección de la información.

  Por lo tanto, es necesario que la entidad implemente cuanto antes los debidos mecanismos de cifrado con el objetivo de asegurar la confidencialidad, autenticidad e integridad de la información, tales como: cifrado de correos, portal de intercambio seguro y cifrado del almacenamiento de dispositivos movibles y portátiles.

- **A.16 Gestión de Incidentes de seguridad de la información (14%)**

  La entidad no cuenta con un proceso de gestión de incidentes de seguridad de la información, por lo tanto, es necesario establecer el respectivo proceso con el objetivo de asegurar un enfoque coherente y eficaz para la debida gestión de los incidentes de seguridad y con esto proveer a la entidad de un mecanismo para el reporte, evaluación y respuesta a los incidentes de seguridad de la información.

- **A.6 Organización de la seguridad de la información (24%)**

[32] Norma ISO/IEC 27001:2013, Pág. 17

La entidad no tiene definidos todos los roles y responsabilidades de la seguridad de la información, la cual es una de las responsabilidades que debe garantizar la Alta Dirección y que es esencial para forjar un adecuado Sistema de Gestión de Seguridad de la Información.

También se encontró que los encargados de la seguridad de la información no mantienen un contacto con grupos de interés especializados en seguridad de la información, lo cual, es esencial para conocer las tendencias del mercado y las nuevas amenazas que surgen y que atentan contra la seguridad de la información, por lo tanto, es indispensables que la entidad comience a participar en eventos, foros, asociaciones y otros organizamos relacionados con seguridad de la información.

- **A.18 Cumplimiento (30%)**

  Dentro de este objetivo de control, está el control A.18.1.5 Reglamentación de controles criptográficos, que indica que la entidad debe establecer controles criptográficos, en cumplimiento de todos los acuerdos, legislaciones y reglamentación pertinentes[33]. Debido a que la entidad no cuenta con mecanismo de cifrado no cumple con este control. Por lo tanto, se requiere que la implementación cuanto antes de los debidos mecanismos de cifrado con el objetivo de asegurar la confidencialidad, autenticidad e integridad de la información.

  También se encontró que los controles relacionados con el objetivo A.18.2 Revisiones de seguridad de la información no están implementados en la entidad, los cuales son indispensables para asegurar la adecuada implementación del sistema de gestión de seguridad de la información de acuerdo a las políticas y procedimientos organizaciones[34].

- **A.5 Políticas de seguridad de la información (33%)**

  Actualmente, las políticas relacionadas con seguridad de la información están definidas en el Manual de Políticas de Seguridad Informática del proceso de tecnología. Esta manual no está aprobado ni es revisado por la Alta Dirección lo que dificulta su cumplimento por parte de los empleados y terceros que proveen servicios de la entidad. Por lo tanto, es necesario el establecimiento

[33] Norma ISO/IEC 27001:2013, Pág. 24
[34] Ibídem

de unas políticas de seguridad aprobadas por la Alta Dirección para garantizar su debida implementación, actualización y cumplimiento.

OBJETIVOS DE CONTROL CON NIVEL DE CUMPLIMIENTO 'MEDIO'

Los siguientes son los objetivos de control del Anexo A de la norma ISO/IEC 27001:2013 cuyo cumplimiento por parte de la entidad se encuentran en un nivel MEDIO (mayor a 33% y menor 70%), lo que implica un riesgo MEDIO para la seguridad de la información de la entidad, debido a que algunos de los controles no están debidamente implementados, documentados o formalizados, o presentan debilidades que pueden ser aprovechadas por amenazas internas o externas para atentar contra la seguridad de la información de la Entidad.

Tabla 10. Objetivos de control con nivel MEDIO de cumplimiento

OBJETIVO DE CONTROL	% CUMPLIMIENTO
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA	37%
A.8 GESTION DE ACTIVOS	43%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	47%
A.15 RELACIONES CON LOS PROVEEDORES	54%
A.17 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	58%
A.9 CONTROL DE ACCESO	61%

- **A.14 Adquisición, desarrollo y mantenimiento del sistema (37%)**

  El nivel de cumplimiento de control se debe a las siguientes situaciones:

  - La entidad no incluye los requisitos relacionados con seguridad de la información en las especificaciones y requerimientos para el diseño y desarrollo sistemas de información, tal cual, como lo especifica el control A.14.1.1 del Anexo A de la norma ISO/IEC 27001:2013[35].
  - No siempre se realizan las verificaciones técnicas a las aplicaciones críticas del negocio cuando se realizan cambios en la plataforma de procesamiento de la entidad, situación que no garantiza la norma operación, disponibilidad y seguridad de los servicios de TI una vez realizado los cambios.
  - La entidad no cuenta con un procedimiento adecuado de control de versionamiento del software, lo que genera en algunos casos que se

[35] Norma ISO/IEC 27001:2013, Pág. 21

presenten incidentes o problemas cuando se realizando cambios de las aplicaciones en el ambiente de producción.

- No existe un proceso controlar para el manejo de datos en los ambientes de producción, lo que genera un riesgo alto debido a que no se garantiza la debida protección y privacidad de los datos sensibles de la entidad.
- Durante el desarrollo de las aplicaciones no se incluyen pruebas de seguridad, lo que puede generar debilidades o vulnerabilidad en los ambientes productivos que pueden ser aprovechas por amenazas para atentar contra la disponibilidad, integridad y confidencialidad de los activos de información de la entidad.

Por lo tanto, es indispensable implementar controles adecuados y efectivos, o fortalecer los existentes, con el objetivo de asegurar que la seguridad de la información sea parte del ciclo de vida del desarrollo de aplicaciones de la entidad y con ello garantizar que los cambios que se realizan en producción no afecten la seguridad de la información.

- **A.8 Gestión de activos (43%)**

  La entidad no tiene identificados todos los activos de información a través de los cuales se gestiona la información del negocio, lo cual, representa un riesgo en la medida que no tiene conocimiento del estado general de la criticidad y protección de sus activos de información. Lo anterior implica, que es necesario realiza una identificación y clasificaciones de los activos de la entidad con el objetivo de determinar su nivel de relevancia de acuerdo su necesidad, prioridad y nivel de protección.

  La entidad no tiene establecidos los lineamientos para el uso aceptable de los activos de información asociados con la información e instalaciones de procesamiento de información, lo que genera que los usuarios desconozcan sus responsabilidades y consecuencia de sus acciones.

- **A.7 Seguridad de los recursos humanos (47%)**

  No se cuenta con un mecanismo que permite garantizar que los empleados y terceras partes que brindan servicios para la entidad, estén debidamente informados sobre las funciones y las responsabilidades respecto a la seguridad de la información antes de que se les autorice el acceso a la información o a los sistemas de información, por lo tanto, es fundamental que para los nuevos

empleados se les instruya sobre sus responsabilidades y consecuencias de sus acciones entorno a la seguridad de la información.

La entidad no cuenta con un plan anual de capacitación y formación en seguridad de la información para sus empleados, lo que genera en algunos casos la poca efectividad de los controles implementados.

- **A.15 Relaciones con los proveedores (54%)**

  No existe una política de seguridad que defina los lineamientos de seguridad para la relación con los proveedores con el propósito de evitar accesos no autorizados a la información de la Entidad.

  Por otra parte, no todos los contratos que se suscriben con terceros tienen acuerdo de confidencialidad de la información, lo que representa un riesgo en la medida que dichos terceros tengan acceso información confidencial y/o sensible de la Entidad.

- **A.17 Continuidad de la seguridad de la información (58%)**

  Dentro del plan de continuidad del negocio de la entidad no se tiene contemplados los requisitos para garantizar la seguridad de la información en situaciones adversar que pueden comprometer la disponibilidad de los servicios de TI. El plan de continuidad, está orientado a asegurar las condiciones operativas y técnicas que permitan garantizar la continuidad de los servicios críticos de la entidad. Por lo tanto, es necesario establecer, documentar, implementar y mantener los procesos, procedimientos y controles necesarios para asegurar el nivel de continuidad requerido con el objetivo de garantizar la seguridad de la información en situaciones adversas.

- **A.9 Control de acceso (61%)**

  El nivel de cumplimiento de este control se debe a los siguientes aspectos:

  - La identificación del equipo no hace forma parte del esquema de autenticación de los usuarios al directorio activo de la entidad, solo se contempla los datos de autenticación (usuario y contraseña) para verificar la validez de usuario.
  - La entidad no cuenta con un procedimiento para la asignación, control y restricción de derechos de acceso y privilegios sobre sus recursos tecnológicos y aplicaciones.

- No se cuenta con un procedimiento para la gestión de contraseñas en los sistemas base de la entidad.
- No se audita los derechos de acceso de manera regular.
- Los usuarios administradores y propietarios de los activos de información no revisan los derechos de acceso de los usuarios de manera regular.

Las anteriores situaciones representan un riesgo para la entidad debido a la ausencia o falencia de algunas medidas de seguridad de control de acceso, que puede generar la posibilidad de la materialización de amenazas relacionadas con abuso de privilegios, accesos no autorizados o uso indebido de la información, y con ello afectar seriamente la seguridad de la información, la continuidad del negocio y la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad de los activos de información involucrados en el proceso de Gestión de Identidad y Control de Acceso a los recursos tecnológicos de la entidad.

OBJETIVOS DE CONTROL CON NIVEL DE CUMPLIMIENTO 'ALTO'

Los siguientes son los objetivos de control del Anexo A de la norma ISO/IEC 27001:2013 cuyo cumplimiento por parte de la entidad se encuentran en un nivel ALTO (mayor al 70%), lo que representa un riesgo BAJO debido a los controles implementados garantizan la debida protección de sus activos de información.

Tabla 11. Objetivos de control con nivel ALTO de cumplimiento

OBJETIVO DE CONTROL	% CUMPLIMIENTO
A.13 SEGURIDAD DE LAS COMUNICACIONES	75%
A.11 SEGURIDAD FISICA Y DEL ENTORNO	76%
A.12 SEGURIDAD DE LAS OPERACIONES	92%

- **A.13 Seguridad de las comunicaciones (75%)**

  Este objetivo de control de encuentra en un nivel de cumplimiento ALTO debido a que las redes de la entidad son debidamente administradas y aseguradas. Con el objetivo de subir su nivel de cumplimiento y con esto cumplir a cabalidad los requerimientos establecidos en este objetivo de control de la norma, la entidad debe:

- Garantizar la debida separación de los servicios de información, usuarios y sistemas de información en la red, de acuerdo al control A.13.1.3 del Anexo A de la ISO/IEC 27001:2013[36].
- Garantizar la debida protección de la información incluida en la mensajería electrónica, de acuerdo al control A.13.2.3 del Anexo A de la norma ISO/IEC 27001:2013[37].
- Establecer y revisar periódicamente que los requerimientos que se establecen para los acuerdos de confidencialidad reflejen las necesidades de la entidad para la protección de la información, de acuerdo al control A.13.2.4 del Anexo A de la ISO/IEC 27001:2013[38].

- **A.11 Seguridad Física y del Entorno (76%)**

  Con el objetivo de subir el nivel de cumplimiento de este objetivo de control la Entidad debe:

  - Establecer los procedimientos para trabajo en áreas seguras de acuerdo al control A.11.1.5 del Anexo A de la ISO/IEC 27001:2013[39].
  - Identificar los riesgos asociados a trabajar fuera de las instalaciones, con el objetivo de dar cumplimiento al control A.11.2.6 'Seguridad de Equipos y activos fuera de las instalaciones' del Anexo A de la ISO/IEC 27001:2013[40].
  - Con el objetivo de dar total cumplimiento al control A.11.2.6 'Seguridad de equipos y activos fuera de las instalaciones' del Anexo A de la ISO/IEC 27001:2013[41], la entidad debe: (i) establecer un mecanismo de seguridad y autenticación que permita validar que la estación de trabajo que se conecta a la red interna de la entidad es una estación de trabajo segura y valida, y (ii) implementar un mecanismo de monitoreo de las estaciones que se conectan a la red.
  - Implementar una política de escritorio limpio con el objetivo de proteger la confidencialidad de la información.

[36]NORMA ISO/IEC 27001:2013, pág. 20
[37]Ibídem
[38]Ibídem
[39]Ibídem, pág. 16
[40]Ibídem, pág. 18
[41]Ibídem

- **A.12 Seguridad de las operaciones (92%)**

  Con el objetivo de subir el nivel de cumplimento de este objetivo de control la entidad debe:

  - Garantizar que el oficial de seguridad participa en los comités de cambios.
  - Separar los ambiente de desarrollo, pruebas y producción para reducir los riesgos de acceso y no autorizados, de acuerdo al control A.12.1.4 ‘Separación de los ambientes de desarrollo, pruebas y operación’ del Anexo A de la ISO/IEC 27001:2013[42].
  - Implementar un mecanismo para el monitoreo de los LOGs de eventos de seguridad y las actividades que realizan los administradores sobre la plataforma de procesamiento.

5.2. FASE II. PREPARACION

Esta fase corresponde a las actividades que se desarrollaron con el propósito de establecer el Sistema de Gestión de Seguridad de la Información en la Entidad.

5.2.1. CONTEXTO DE LA ORGANIZACION

La norma ISO/IEC 27001:2013 reitera la importación de conocer y comprender los factores externos e internos de la organización, que pueden afectar o ser afectados de manera positiva o negativa por el establecimiento del Sistema de Gestión de Seguridad de la Información.

Para tal efecto, la norma ISO/IEC 27001:2013 incluye el capítulo “4. CONTEXTO DE LA ORGANIZACIÓN”, donde se establece que la entidad debe determinar las situaciones y factores externos e internos que la rodean y que son pertinentes para establecer al Sistema de Gestión de Seguridad de la Información.

5.2.1.1. CONOCIMIENTO DE LA ORGANIZACIÓN

NATURALEZA DE LA ENTIDAD.

IGM S.A, es una sociedad anónima, de economía mixta del orden nacional, constituida con la participación exclusiva de entidades públicas, con personería

[42] Norma ISO/IEC 27001:2013, pág. 19

jurídica, autonomía administrativa y capital independiente, organizada como un establecimiento de crédito y vinculada al Ministerio de Hacienda y Crédito Público.

IGM S.A, es un banco de segundo piso, cuyos recursos de crédito son desembolsados a los usuarios del sistema de crédito a través de intermediario financieros[43] y está sometida a la vigilancia de la Superintendencia Financiera de Colombia.

MISION DE LA ENTIDAD

Apoyamos el desarrollo sostenible del País, generando bienestar en las regiones[44].

VISION DE LA ENTIDAD

Ser la Banca del Desarrollo para la infraestructura sostenible del País[45].

ACTIVIDADES QUE DESARROLLA LA ENTIDAD

IGM S.A promociona el desarrollo regional y urbano por medio de la financiación y la asesoría en cuanto a diseño, ejecución y administración de proyectos en infraestructura, mediante el otorgamiento de créditos. Estos recursos son desembolsados a través de intermediarios financieros mediante el sistema de redescuento para los diferentes sectores de la economía[46].

La entidad obtiene sus recursos del público mediante la emisión de Certificados de Depósito a Término 'CDTs', inscritos ante la Superintendencia Financiera de Colombia, en el Registro Nacional de Valores y Emisores. Celebra contratos de crédito interno y recibe depósitos de las entidades públicas sobre los cuales reconoce rendimientos o contraprestaciones especiales.

IGM S.A está calificada como Emisor AAA (Triple A) en el largo plazo y F1+ en el corto plazo por la Agencia Calificadora de Riesgos Fitch Ratings Colombia S.A., calificación que la Financiera ha mantenido por once (11) años consecutivos[47].

Brinda servicio de asistencia técnica en la estructuración de proyectos.

---

[43] Son los que pueden realizar operaciones de redescuento con la Entidad
[44] Fuente: Pagina web de la entidad
[45] Ibídem
[46] Ibídem
[47] Ibídem

ESTRUCTURA ORGANIZACIONAL

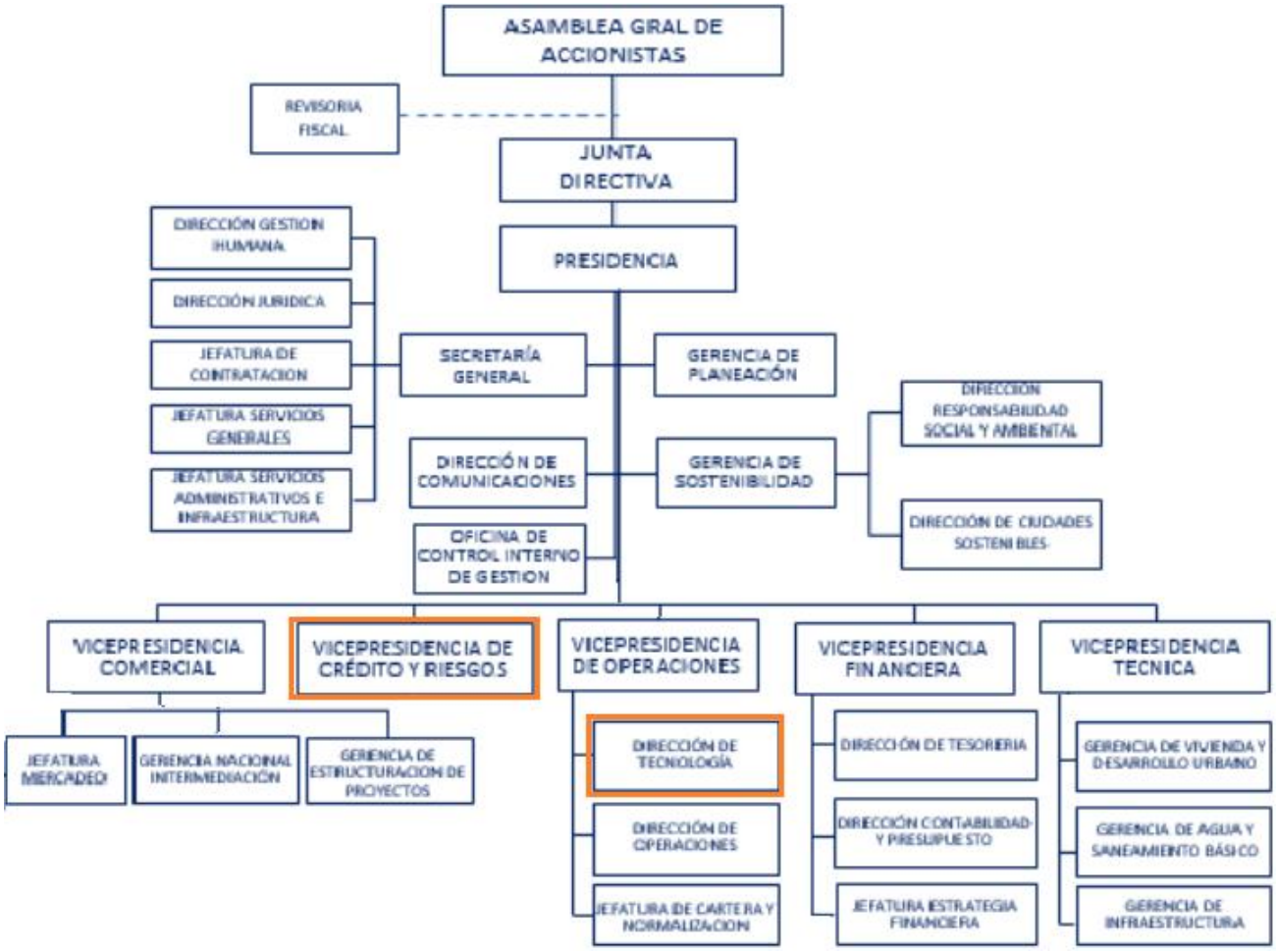


Figura 8. Organigrama de la Entidad
Fuente: La Entidad

En este organigrama existen dos áreas que desempeñan las funciones de seguridad de la información en la Entidad, la Vicepresidencia de Crédito y Riesgos que desde el mes de enero del año 2014 asumió las funciones de Seguridad de la Información y la Dirección de Tecnología de la Vicepresidencia de Operaciones que desempeña las funciones de Seguridad Informática.

MAPA DE PROCESOS

El siguiente es el mapa de mapa de procesos de la entidad, en la cual se resalta el proceso estratégico de Gestión de Riesgos y el proceso de apoyo de Gestión de Tecnología:

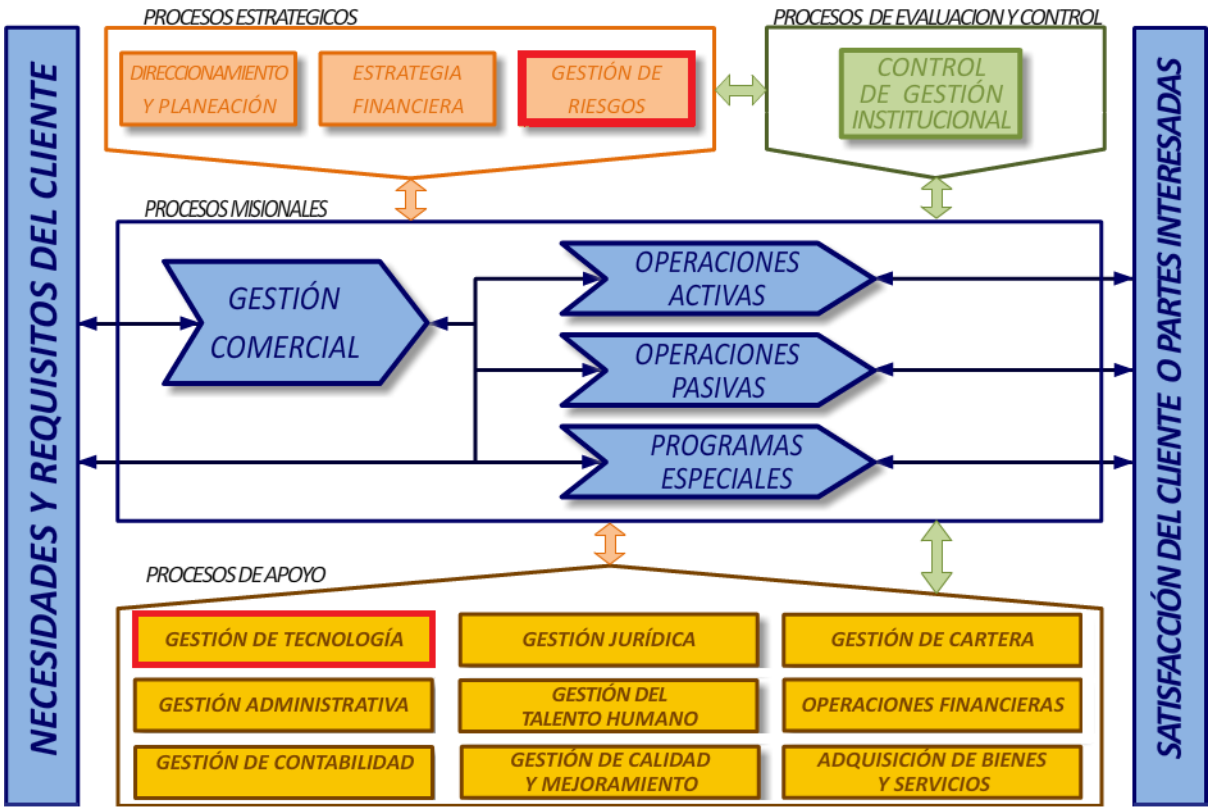


Figura 9. Mapa de proceso de la Entidad
Fuente: La Entidad

- **PROCESO DE GESTION DE RIESGOS.** El proceso de Gestión de Riesgos, es uno de los procesos estratégicos de la entidad y tiene por objetivo establecer, implementar y mantener el Sistema de Administración de Riesgos de la entidad, acorde con las políticas establecidas por la Junta Directiva, ajustadas a la normatividad vigente[48]. Su alcance, inicia con la identificación de los riegos y termina con la implementación y administración de los sistemas de riesgos, tales como SARC[49], SARO[50], SARL[51] y SARLAFT[52]. Lo anterior implica, la definición de políticas, mapas de riesgos, procedimientos, metodología y valoración de riesgos. El proceso de Gestión de Riesgos, es en la entidad una de la parte más interesadas en forjar un adecuado Modelo de Gestión de Seguridad de la Información, debido a que tiene a su cargo la responsabilidad

[48] Caracterización Proceso de Gestión de Riesgos, Sistema de Gestión IGM S.A
[49] Sistema de Administración de Riesgo Crediticio
[50] Sistema de Administración de Riesgos Operativos
[51] Sistema de Administración de Riesgo de Liquidez
[52] Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo

de la gestión de riesgos de la entidad, seguridad de la información y el plan de Continuidad del Negocio de la entidad.

- **PROCESO DE GESTION DE TECNOLOGIA.** Tiene por objetivo administrar y proveer los recursos tecnológicos de la entidad garantizando su confidencialidad, disponibilidad, integridad y oportunidad. Su alcance inicia desde la concepción del plan estratégico de tecnología, su ejecución y la adecuada prestación de los servicios de tecnología de la información y termina con el monitoreo y evaluación. Tiene entre otras, la responsabilidad de la Gestión de Infraestructura y Plataforma de Procesamiento, Gestión de Aplicaciones, Gestión de Proveedores de TI, Gestión de Incidentes y Requerimiento, Gestión de Mesa de Ayuda, Gestión de Cambios de TI y Seguridad Informática.

  El Proceso de Gestión de Tecnología es considerado como uno de los procesos fundamentes para garantizar la integridad, confidencialidad y disponibilidad de la información de la entidad, ya que administra y soporta los recursos tecnológicos del negocios a través de los cuales se gestiona, intercambia y almacena la información de los procesos estratégicos, misionales y de apoyo de la entidad, por lo tanto, es necesario asegurar sus activos de información con el objetivo de poder forjar un adecuado Seguridad de Gestión de Seguridad la Información y garantizar su mejora continua.

AREAS CRÍTICAS DE LA ENTIDAD

Las siguientes son las áreas críticas de la entidad, donde están establecidos las mayores medidas y controles de seguridad con el objetivo de proteger y garantizar la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y no repudio de la información que en ellas se maneja:

- **ALTA DIRECCION.** Corresponden al área donde están ubicadas las oficinas de los altos directivos de la entidad, tales como Presidencia, Secretaria General, Asesores y la respectiva sala de junta. Debido a la información sensible y confidencial que se maneja en esta área que es fundamental para la toma de decisiones y definición de planes estratégicos, su acceso es restringido con el objetivo de evitar amenazas relacionadas con el robo, sustracción, pérdida y divulgación no autorizada de la información.

- **MESA DE DINERO.** La entidad por medio de la Mesa de Dinero obtiene recursos del público a través de emisión de títulos valores que están inscritos ante la Superintendencia Financiera de Colombia, en el Registro Nacional de Valores y Emisores. Estos recursos, son uno de los más importantes y representativos dentro del fondeo de la entidad. Por la naturaleza del negocio de la entidad, la información que se maneja en la Mesa de Dinero es de carácter confidencial y privilegiado, ya que con ella los funcionarios que analizan el mercado de valores y determinan las condiciones oportunas para realizar negociaciones de interbancarios. Las condiciones de acceso a esta área, están dadas en el Reglamento AMV del Autorregulador del Mercado de Valores de Colombia [8], en el cual, entre otras normas, se establece los lineamientos y restricciones para el ingreso de elementos, dispositivos, equipos informáticos y de las personas a las Mesas de Dinero de las entidades financieras afiliadas a la AMV.[53]

- **OPERACIONES FINANCIERAS Y DE TESORERIA.** Encargada de las operaciones financieras y de tesorería, y de la administración de ingresos y pagos de la entidad. Debe velar por garantizar la seguridad en el manejo de los títulos valores y los sistemas transaccionales por medio de los cuales se realiza los pagos de las obligaciones de la entidad de acuerdo a los periodos y compromisos establecidos. Así mismo, debe verificar el cumplimiento de las operaciones de compra y venta de divisas requeridas por la entidad. Para el desarrollo de estas actividades, las terminales de los funcionarios de esta área tienen conexión a los siguientes sistemas o portales de información:

  - **Terminas empresariales**, de otras entidades bancarias, a través de las cuales se realiza las transacciones electrónicas de los pagos de las obligaciones contraídas con terceros.
  - **Portal web del Sistema de Registro de Deceval**, sistema para el manejo de los títulos desmaterializados que le permite a la entidad el pre-ingreso, confirmación y conocimiento de la información relacionada con las operaciones sobre valores en el mercado mostrador. También permite consultar el estado de las operaciones registradas, así como información global para fines estadísticos[54].

[53] Reglamento AMV, *artículos 46.3 y 46.4*
[54] DECEVAL, REGLAMENTO DEL SISTEMA DE REGISTRO DE DECEVAL

- **Sistema de Depósito Central de Valores del Banco de la República,** permite el depósito, custodia y administración de títulos valores desmaterializados, que tiene por objetivo primordial eliminar el riesgo que representa el manejo de títulos físicos, facilitar las transacciones en el mercado secundario y realizar de forma segura, ágil y oportuna el cobro de capital o de rendimientos financieros[55].
- **Sistema SEBRA**, permite el acceso seguro a los servicios electrónicos para realizar las transacciones y las comunicaciones entre el Banco de la República y la entidad, de una manera ágil, eficiente y segura[56].

Debido a las operaciones y transacciones electrónicas que realiza el área de Operaciones Financieras y de Tesorería, esta área cuenta con las medidas de seguridad físicas y lógicas orientadas a evitar el acceso por parte de personas no autorizadas, con el propósito de evitar la modificación, manipulación, divulgación no autorizada, pérdida y robo de la información, y el uso inadecuado de los sistemas para fraudes.

- **JEFATURA DE CARTERA.** Entre sus funciones principales esta, coordinar y controlar las actividades de normalización de cartera y la recuperación de cartera, velar por la adecuada administración de las garantías que soportan las operaciones de cartera de la entidad y reportar a las centrales de riesgos las obligaciones que superen los plazos en mora establecidos en la normatividad vigente. Esta jefatura está catalogada como área crítica debido a que debe garantizar la reserva bancaria de la información que se maneja dentro de esta, la total integridad de las garantías que soportan las operaciones de cartera y la confidencialidad y protección de los datos personas de los titulares.

- **AREA ADMINISTRACION DE PLATAFORMA.** Tiene por función principal garantizar la disponibilidad, continuidad, confiabilidad y seguridad de la infraestructura tecnológica y de telecomunicaciones que soportan los sistemas de información y recursos tecnológicos necesarios para la operación del negocio. Así mismo, su responsabilidad es garantizar la seguridad informática en la entidad e implementar las medidas y controles tecnológicos orientados a

[55] http://www.banrep.gov.co/es/contenidos/page/qui-nes-pueden-acceder-dcv
[56] http://www.banrep.gov.co/es/sebra-objetivo

evitar, prevenir o mitigar las amenazas informáticas que puede atentar contra la disponibilidad, integridad y confidencialidad de la información de la entidad.

- **CENTRO DE CÓMPUTO.** En el centro de cómputo están ubicados los servidores, sistemas de almacenamiento, sistemas de respaldo, equipos de seguridad y equipos de telecomunicaciones necesarios para soportar los servicios tecnológicos y sistemas de información requeridos para la operación del negocio y para el procesamiento, tratamiento, aseguramiento y respaldo de la información. El centro de cómputo cuenta con las medias y mecanismos de seguridad físicas y lógicas con el objetivo de prevenir accesos no autorizado a esta instalación y por ende a los equipos ubicados dentro de la misma.
- **AREA DE RECEPCION DE CORRESPONDENCIA.** Encarga de la recepción de correspondencia y documentos tanto internos como externos, y de la radicación e inclusión de los mismos en el sistema de gestión documental de la entidad, para su respectiva clasificación, asignación, distribución y entrega digital o en medio físico a los usuarios destinarios de la información. Debido que esta área está expuesta al público para la recepción de documentación, paquetes y otros elementos, y al volumen y tipo de información que maneja de carácter confidencial, público o de uso interno, en zona cuenta con las medidas de seguridad orientas a evitar accesos no autorizados.

5.2.1.2. NORMATIVIDAD DE SEGURIDAD APLICABLE A LA ENTIDAD

La entidad por ser de carácter público y financiero, está vigilada y controlada por la Superintendencia Financiera de Colombia y otros organismos y entes de control, lo que significa que debe garantizar el cumplimiento de la normatividad vigente relacionada con seguridad de la información que es aplicable a entidades del estado y financieras, como por ejemplo:

- **Circular 052 de 2007** [9], por medio de la cual la Superintendencia Financiera de Colombia “establece los requerimientos mínimos se seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios”[57], y entre otros establece que las entidades vigiladas

[57] Superintendencia Financiera de Colombia, Circular externa 052 de 2007.

deben gestionar la seguridad de la información para lo cual pueden tomar como el estándar de las normas ISO 27001[58].

- **Circular 038 de 2009** [10], por medio de la cual la Superintendencia Financiera de Colombia determina que las entidades vigiladas deben contar con sistemas que garanticen que la información cumpla con los criterios de seguridad relacionados con la confidencialidad, integridad y disponibilidad[59].
- **Ley estatutaria 1266 de 2008 "Habeas Data"** [11], que regula el manejo de la información de las personas recopiladas y almacenadas en bases de datos de terceros, en especial la información de carácter financiero, crediticio, comercial, de servicios y la proveniente de terceros países .
- **Ley 1581 de 2012**[60] [12] que fue regulada en el **Derecho 1377 de 2013**[61] [13], que definen el marco jurídico orientado a garantizar que la debida, recolección, almacenamiento, tratamiento, uso y distribución de los datos personales de los titulares por parte de terceros.
- **Reglamento AMV** del Autorregulador del Mercado de Valores de Colombia, que definir los lineamientos de seguridad para las Mesas de Dinero de las entidades afiliados a la AMV.
- **Modelo de seguridad y privacidad de la información** [14]**,** por medio del cual el Ministerio de Tecnologías de la Información y las Comunicaciones establece los lineamientos que deben seguir las entidades del estado para la implementación de la gestión de seguridad y privacidad de la información con el objetivo de dar cumplimiento a la Estrategia de Gobierno en Línea.

5.2.1.3. PARTES INTERESAS DE LA ENTIDAD

Los grupos de interés o partes interesadas de la entidad corresponden a las personas naturales o jurídicas con la cuales la entidad interactúa en el ejercicio de sus funciones, que pueden afectar o ser afectadas de manera positiva o negativa por la Seguridad de la información de la entidad y en algunos casos, pueden manifestar un interés directo, explícito y comprometido con los objetivos y propósitos del Sistema de Gestión de Seguridad de la Información.

---

[58] Ibídem, numeral 3.1.2

[59] Superintendencia Financiera de Colombia, Circular externa 038 de 2009, numeral 7.5.4.1.

[60] Ley estatutaria 1581 del 17 de octubre de 2012 "Por el cual se dictan disposiciones generales para la protección de los datos personales".

[61] Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Las siguientes son las partes interesadas de la entidad en función a la seguridad de información:

Tabla 12. Partes de interés externas en función del SGSI

Grupos de interés	Descripción
Accionistas	Pueden ser: la Nación, entidades públicas de orden nacional, departamentos, personas naturales o jurídicas, nacionales o extranjeras y organismos internacionales
Inversionista	Corresponde al grupo de individuos que adquieren CDT u otros títulos valores ofrecidos por la entidad y las personas que adquieren acciones de la entidad.
Gobierno	Corresponde a los organismos con competencia para establecer un marco normativo de funcionamiento de la entidad.
Superintendencia Financiera de Colombia	La Superintendencia Financiera de Colombia, es un organismo técnico que tiene por objetivo supervisar el sistema financiero colombiano con el fin de preservar su estabilidad, seguridad y confianza, así como, promover, organizar y desarrollar el mercado de valores colombiano y la protección de los inversionistas, ahorradores y asegurados.
Intermediarios Financieros	Entidades a través de las cuales la entidad realiza operaciones de crédito por redescuento.
Comunidad	Corresponde a los individuos y grupos externos que se ven impactados por las actividades que desarrollar la entidad.
Beneficiarios	Son las personales naturales o jurídicas que ejecutan los proyectos con recursos otorgados por la entidad.
Entes de control externo	Corresponde a los entres de vigilancia y control de supervisan las actividades de la entidad
Bancos Multilaterales y de Desarrollo	Son los aliados empresariales, instituciones y organismos con los que la entidad participa en proyectos de inversión.
Proveedores	Individuos que prestan sus servicios a la entidad.
Ex empleados	Funcionaros retirados que siguen teniendo productos de la entidad y cuyos datos personales son tratados por la entidad.

Tabla 13. Partes de interés internas en función del SGSI

Grupos de interés	Descripción
Alta Directiva	Debe demostrar liderazgo y compromiso con la Seguridad de la Información, asegurando que los objetivos que se establecen son compatibles con la planeación estratégica de la organización.
Comité de Riesgo	Apoyar a la Junta directiva y a la Presidencia de la Entidad, en la definición, seguimiento, control e implementación de las políticas y procedimientos de la gestión de riesgos, de la seguridad de la información y del plan de continuidad del negocio.
Vicepresidencia de Crédito y Riesgos	Responsable de establecer, implementar y mantener el Sistema de Administración de Riesgos de la Entidad, Sistema de Seguridad de la Información y el Plan de Continuidad.
Oficial de Seguridad	Responsable de la implementación y operación del Sistema de Gestión de Seguridad de la Información
Dirección de Tecnología	Responsable entre otros aspectos, de la Seguridad Informática y Continuidad Tecnológica de la Entidad.
Jefatura de Recursos Físicos	Responsable de la Seguridad Física de la Entidad.
Gestión humana	Responsable de la seguridad antes, durante y después de la vinculación de los funcionarios Responsable de la capacitaciones
Dirección Jurídica	Garantizar el cumplimiento de la normatividad vigente relacionada con seguridad de la información.
Colaboradores	Responsables de velar por la seguridad sus activos de información, cumplir a cabalidad con las normas de seguridad establecidas en la Entidad. También, tienen la responsabilidad del tratamiento de los datos personales de los titulares vinculados de alguna forma con la Entidad.

La siguiente es la relación del grado de interés, motivación y gobernabilidad de los actores o partes interesadas de acuerdo a su función, responsabilidad y capacidad influir de manera positiva o negativa en el Sistema de Gestión de Seguridad de la Información:

Tabla 14. Actores relevantes en función a la seguridad de la información

Actores Relevantes	Función con relación a la seguridad de la información	Interés	Motivación	Gobernabilidad
Alta Dirección	Debe demostrar liderazgo y compromiso con la Seguridad de la Información , asegurando que los objetivos que se establecen son compatibles con la planeación estratégica de la organización	Alta	Alta	Alta
Comité de Riesgos	Asegurar la implementación, operación y mejora continua del sistema de gestión de seguridad de la información	Alta	Alta	Alta
Vicepresidencia de Crédito y Riesgos	Establecer, implementar y mantener el Sistema de Seguridad de la Información	Alto	Alta	Alta
Oficial de Seguridad	Establecer, implementar y velar por el cumplimiento de las políticas, normas y lineamientos de seguridad que se establezcan en la organización.	Alto	Alta	Meda
Dirección de Tecnología	Garantizar la disponibilidad de los sistemas de información. Garantizar la integridad, disponibilidad y confidencialidad de infraestructura de TI y por ende de la información almacenada en ella	Alto	Alta	Media
Jefatura de Recursos Físicos	Responsable de la seguridad física	Alto	Alta	Media
Colaboradores Proveedores	Velar por la seguridad de sus activos de información. Acatar las políticas de seguridad y velar porque sus funcionarios las cumplan. Velar por la integridad, disponibilidad y confidencialidad de la información sensible de la organización. Determinar el nivel de autorización a sus información	Medio	Medio	Baja
Entes de Control Superintendencia Financiera de Colombia	Asegurar cumplimiento de normatividad	Alto	Medio	Medio
Gobierno	Procurar porque las entidades del estado implementen sistema de gestión que las permitan fortalecer su seguridad	Alto	Alta	Alto
Intermediarios Financieros Bancos Multilaterales y de Desarrollo	Interesados en que la entidad les brindad las garantías de protección de las operaciones que realizan con la entidad y de la información que intercambian	Alto	Bajo	Baja
Ex empleados	Interesados en que la entidad le garantice la protección de sus datos financieros y la privacidad de sus datos personales	Alto	Bajo	Baja

5.2.2. ALCANCE DEL SGSI

El alcance permite determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información de la entidad[62].

El alcance del Sistema de Gestión de Seguridad de la Información de la entidad está incluido dentro del documento que se referencia en el ANEXO C del presente trabajo, y corresponde al siguiente:

Alcance del SGSI

El alcance del Sistema de Gestión de la Seguridad de la información de IGM S.A, abarca solo para el proceso de Gestión de Tecnología de la Entidad, que involucra la gestión de la infraestructura y plataforma de procesamiento, gestión de aplicaciones, gestión de proveedores de TI, gestión de Incidentes y requerimiento y gestión de cambios de TI.

El Sistema de Gestión de la Seguridad de la información aplica solo para la sede principal de la entidad, ubicada en la ciudad de Bogotá, limitando los procesos y actividades que se desarrollan en esta sede.

5.2.3. POLITICA DEL SGSI

La política del Sistema de Gestión de Seguridad de la información corresponde a la declaración general que representa la posición de la Alta Directiva de la entidad con relación a la seguridad de la información.

La norma ISO/IEC 27001:2013 en su numeral 5.2 Política, indica que la Alta Dirección de la entidad debe establecer una política de seguridad de la información adecuado al propósito de la organización, que incluya los objetivo de seguridad de la información, los requerimientos normativos vigentes relacionados con seguridad de la información y el compromiso de la mejora continua[63].

La siguiente es la política general del Sistema de Gestión de Seguridad que se definió:

[62] Norma ISO/IEC 27001:2013, Pág. 2
[63] Norma ISO/IEC 27001:2013, Pág. 3

POLITICA DEL SGSI

IGM S.A*, enfocada en promover el progreso sostenible de las regiones, en cumplimiento de nuestra misión, visión y objetivo estratégico, y para satisfacer las necesidades de nuestros clientes, colaboradores, comunidad y demás partes interesadas, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:*

- *Cumplir con los requerimientos legales y reglamentarios aplicables a la entidad y al Sistema de Gestión de Seguridad de la Información.*
- *Entregar resultados de excelencia, con sentido de pertenencia, actitud proactiva y comunicación continua y oportuna.*
- *Gestionar los riesgos de la entidad a través de la aplicación de estándares y controles orientados a preservar la seguridad de nuestra información.*
- *Mantener buenas prácticas de seguridad de la información que garantizan la Disponibilidad, Integridad y Confidencialidad de la información, proporcionando confianza en nuestras partes interesadas*
- *Implementar el sistema de gestión de seguridad de la información.*
- *Fortalecer la cultura de seguridad de la información en los colaboradores de la Entidad.*
- *Garantizar la continuidad de los servicios y la seguridad de la información.*

Aplicabilidad de la Política del SGSI.

Esta política aplica a toda la entidad, sus colaboradores, proveedores, terceros y demás partes interesadas.

5.2.4. OBJETIVO DEL SGSI

Los siguientes son los objetivos de Sistema de Gestión de Seguridad de la Información que se definieron, los cuales están incluidos en el ANEXO C del presente trabajo de grado

:

OBJETIVOS DEL SGSI

- *Incrementar el nivel de satisfacción de los clientes internos y externos de IGM S.A.*
- *Optimizar el nivel de eficacia de los controles de la Entidad.*
- *Incrementar el nivel de competencias del talento humano.*
- *Garantizar el acceso a la información de IGM S.A de acuerdo con los niveles de la organización y criterios de seguridad que establezca la Entidad, la normatividad aplicable y/o las partes interesadas.*
- *Mantener la integridad de la información de la entidad, teniendo en cuenta los requisitos de seguridad aplicables y los resultados de la valoración y el tratamiento de los riesgos identificados.*
- *Asegurar que la información de IGM S.A esté disponible para los usuarios o procesos autorizados en el momento en que así lo requieran.*

5.2.5. ESTRUCTURA ORGANIZACIONAL DE LA SEGURIDAD

De acuerdo al numeral '5.3 Roles, Responsabilidades y autorizadas en la organización' de la norma ISO/IEC 27001:2013, la alta directiva debe asegurar que se asignen las responsabilidad y autoridades para los roles pertinentes a la seguridad de la información[64]. Con base en este requerimiento de la norma, como primero medida se identificaron las áreas dentro de la entidad cuyas funciones están relacionadas con la seguridad de la información, para lo cual se tuvo en cuenta los siguientes aspectos:

- Responsable de la seguridad de la información
- Responsable de la seguridad informática
- Responsable de la seguridad física
- Responsable de la seguridad de los recursos humanos, antes, durante y después del contrato.
- Responsable del cumplimiento de la normatividad vigente
- Responsables y encargado del tratamiento de los datos personales de los titulares.

[64] Norma ISO/IEC 27001:2013, Pag, 3

De acuerdo a lo anterior, se identifico el siguiente organigrama que permite identificar las dependencias de la entidad cuyas funciones son pertinentes a la seguridad de la información:

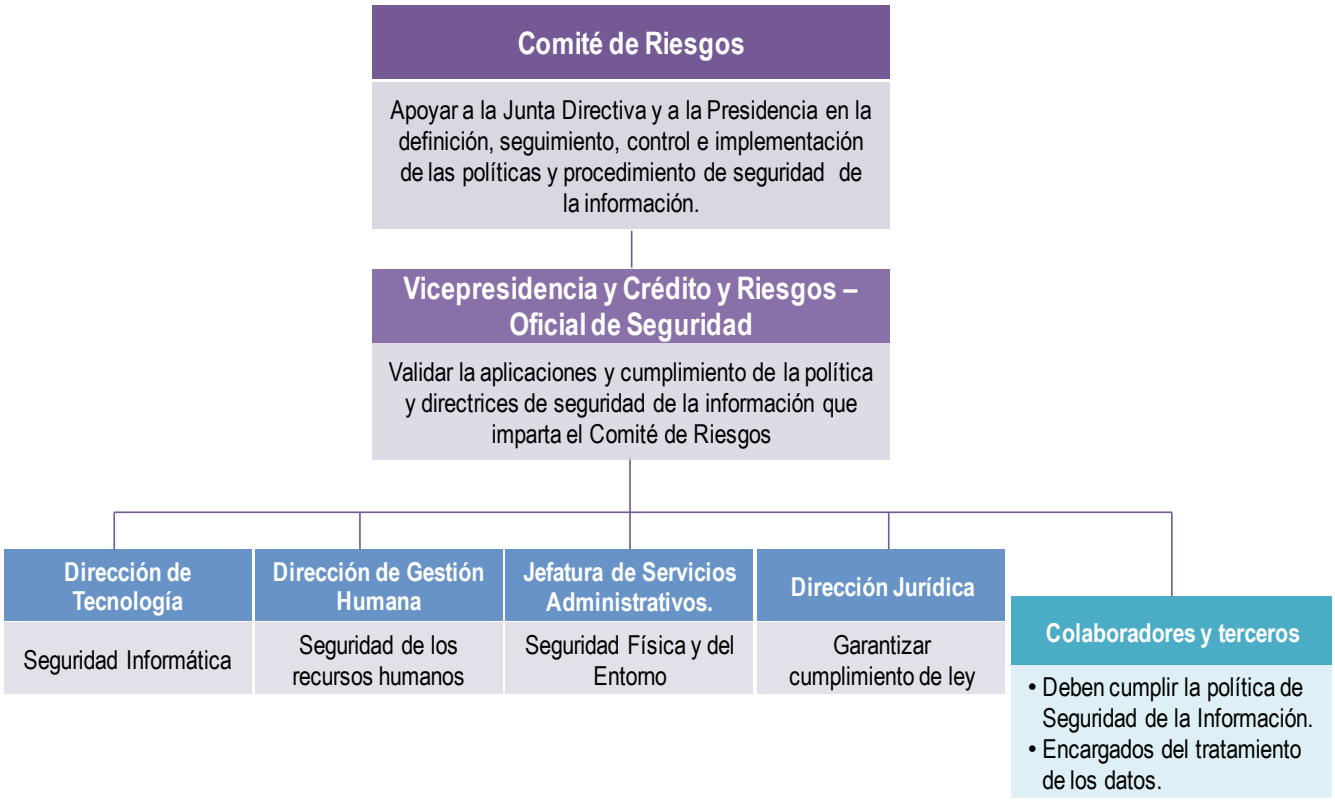


Figura 10. Organización de la seguridad de la información
Fuente: El autor

Una vez identificadas las áreas que cumplen funciones de seguridad de la información, se procedió a establecer las siguientes responsabilidades de la seguridad de la información para los roles pertinentes:

ALTA DIRECCIÓN

- Aprobar la Política de Seguridad de la Información que debe ser publica y divulga a todos los colaboradores de la entidad.
- Revisar la Política de Seguridad de la Información en intervalos planificados o cuando se produzcan cambios significativos en la normatividad aplicable.
- Definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

- Promover activamente una cultura de seguridad de la información en la entidad.

COMITÉ DE RIESGOS

- Establecer los mecanismos adecuados para la gestión y administración de riesgos, seguridad de la información, continuidad del negocio, velar por la capacitación del personal de la entidad en lo referente a estos temas.
- Informar a la Junta Directiva sobre aspectos relacionados con la gestión de riesgos, seguridad de la información y continuidad de negocio.
- Diseñar y aprobar la estrategia de gestión de riesgos, seguridad de la información y continuidad de negocio de la Entidad y liderar su ejecución.
- Asegurar la existencia de metodologías, políticas y sistemas para riesgos, seguridad de la información y continuidad de negocio.
- Asegurar la implementación en la entidad, de la normatividad o requerimientos que sobre los temas de riesgos, seguridad de la información y continuidad del negocio que impartan o solicite el ente regulador o los entes de control.

OFICIAL DE SEGURIDAD

- Diseñar y coordinar la implementación de las políticas, normas y procedimientos de seguridad de la información, con la participación activa de las dependencias de la Entidad.
- Identificar los riesgos que afectan a los recursos de información frente a las amenazas más importantes y gestionar la actualización del mapa de riesgos.
- Definir los controles asociados al Sistema de Seguridad de la Información y evaluarlos periódicamente
- Hacer la evaluación del desempeño del SGSI.
- Establecer un programa periódico de revisión de vulnerabilidades y coordinar los respectivos planes de mitigación.
- Desarrollar de forma periódica, charlas de capacitación y concientización en temas de Seguridad de Información para el personal de la institución.
- Atender auditorías internas y externas de aspectos asociados a la Seguridad de Información y facilitar la información sobre los controles implementados.
- Reportar al Comité de Riesgos los incidentes de seguridad de la información, los resultados de las auditorias, la revisión y supervisión del SGSI.

- Asesorar en forma permanente y cercana a las distintas áreas de la Institución en temas referentes a seguridad.

DIRECCIÓN DE TECNOLOGÍA – SEGURIDAD INFORMATICA

- Asegurar el cumplimiento de las políticas y requerimientos de seguridad establecidos para la adquisición, diseño, desarrollo, operación, administración y mantenimiento de los sistemas operativos, bases de datos, recursos, plataforma tecnológica y servicios de telecomunicaciones de la entidad.
- Asegurar el cumplimiento de las políticas y requerimientos de seguridad establecidos para la adquisición, diseño, desarrollo, operación, administración y mantenimiento de los Sistemas de Información de la entidad.
- Asignar las funciones, roles y responsabilidades de Seguridad, a sus funcionarios para la operación y administración de la plataforma tecnológica de la entidad. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.
- Implementar los controles y medidas de seguridad

DIRECCION JURIDICA

- Conocer e interpretar la normatividad vigente relacionada con seguridad de la información bajo el contexto de la entidad.
- Hacer cumplir en la entidad la normatividad vigente
- Actualizar la normatividad vigente en el sistema de gestión de la entidad.

JEFATURA DE RECURSOS FISICOS

- Implementar las medidas de seguridad física adecuadas con el objetivo de proteger a la entidad antes situaciones generadas por eventos naturales, alteraciones del entorno, acciones humanes y accesos no autorizadas, que pueden comprometer la seguridad de la información de la entidad y la continuidad del negocio.
- Implementar las medidas de seguridad física con el objetivo de control el acceso a las instalaciones de la entidad de acuerdo a nivel de criticidad.

COLABORADORES Y PARTES INTERESADAS

- Cumplir en su totalidad las Políticas de Seguridad de la Información.

- Mantener la Confidencial, Integridad y Disponibilidad de la información a la cual tienen acceso para la ejecución de sus actividades.
- Los colaboradores dueños de proceso deben definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos en función a la Seguridad de la Información.
- Los colaboradores propietarios de los riesgos deben apoyar en la identificación, valoración y gestión de los riesgos de Seguridad.
- Garantizar el debido tratamiento de los datos personales de los titulares.

5.3. FASE III. PLANIFICACION

En esta fase se llevaron a cabo las actividades pertinentes con el propósito de poder asegurar que el diseño del Sistema de Gestión de Seguridad de la Información alcance los objetivos propuestos, que corresponden la determinación de los riesgos y las acciones para mitigarlos y a la definición los lineamientos y límites en torno a la seguridad de la información que deben cumplir los colaboradores y tercero.

Las actividades relacionadas con la clasificación de los activos de información y su valoración de riesgos, se desarrollaron de acuerdo a los siguientes aspectos:

- **Alcance identificación de activos.** La identificación de los activos de información se realizo de acuerdo al alcance del SGSI, el cual solo contempla el proceso de tecnología, por lo tanto, únicamente se identificaron los activos de información que son administrados y utilizados por la Dirección de Tecnología de la entidad, los cuales fueron el insumo para el proceso de valoración de riesgos de los activos de información.
- **Metodología para la clasificación de activos y valoración de sus riesgos**. Para el desarrollo de las actividades relacionas con la identificación y clasificaciones de los activos de información del proceso de gestión de tecnología y la respectiva valoración de los riesgos, se utilizo la metodología de riesgos relacionada en el Anexo D del presente trabajo de grado.
- **Confidencialidad de la información**. Para efectos del presente trabajo no se relaciona el nombre de las aplicaciones sino su propósito, por requerimiento de de confidencialidad de la información por parte de la entidad.

5.3.1. CLASIFICACION DE ACTIVOS DE TECNOLOGIA

NOTA: El detalle de los activos del proceso de tecnología de la entidad se encuentra en el Anexo E del presente trabajo, el cual además de esta información contiene los parámetros, la formulación y los cálculos que se utilizaron para determinar el nivel de criticidad de los activos de información.

Como primera actividad de esta etapa se identificaron los activos de información del proceso de tecnología, de acuerdo a la metodología del Anexo D del presente documento, la cual establece la siguiente clasificación de tipos de activos:

Tabla 15. Tipos de activos de información

Tipo de activo	Descripción
Servicios	Contempla servicios prestados por el sistema
Datos / información	Ficheros, copias de respaldo, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad.
Software	Programas, aplicativos, desarrollos, software base, sistema de información
Equipos informáticos	Hardware. Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización
Personal	Personas relacionadas con los sistemas de información.
Redes de comunicaciones	Servicios de comunicaciones contratados a terceros; medios de transporte que llevan datos de un sitio a otro
Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente
Equipamiento auxiliar	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones

A continuación se relaciona el inventario de los activos de información que se pudieron identificar en el proceso de tecnología:

Tabla 16. Inventario de activos de información de tecnología

No	Nombre del Activo	Descripción del Activo	Tipo de activo	Contenedor
A1	Centro Principal de Procesamiento	Centro Principal de procesamiento donde reside la infraestructura para soporta la operación del negocio	Instalaciones	Data Center del proveedor
A2	Centro Alterno de Procesamiento	Centro Alterno de procesamiento que contiene la infraestructura para la continuidad del negocio	Instalaciones	Data Center del proveedor
A3	Cuartos de comunicaciones	Instalación física donde residen los rack de comunicaciones	Instalaciones	Cuartos de rack
A4	Area administración de plataforma	Instalación física donde están ubicados los administradores de plataforma	Instalaciones	Area administración de plataforma
A5	Red LAN	Red LAN corporativa de la entidad	Redes de comunicaciones	Red LAN
A6	Red WAN	Red WAN de la entidad	Redes de comunicaciones	RED WAN
A7	Red WIFI corporativa	Red Wifi utilizada por los equipos móviles para acceder a los recursos de la red corporativa de la entidad	Redes de comunicaciones	Red LAN
A8	Red WIFI invitados	Red Wifi para invitados	Redes de comunicaciones	Red LAN
A9	Servidores de administración	Servidores que soportan los servicios bases de administración	Equipos informáticos	Data Center del proveedor
A10	Servidores de bases de datos de producción	Servidores de producción que soportan los motores e instancias de bases de datos	Equipos informáticos	Data Center del proveedor
A11	Servidores de aplicaciones de producción	Servidores de producción que soportan las aplicaciones y sistemas de información	Equipos informáticos	Data Center del proveedor
A12	Plataforma de Correo	Servidores que soportan la plataforma y servicio de correo corporativo	Equipos informáticos	Data Center del proveedor
A13	Servidores de Pruebas	Servidores que soportan los ambientes de prueba de la entidad	Equipos informáticos	Data Center del proveedor
A14	Servidores de Desarrollo	Servidores que soportan los ambientes de desarrollo de la entidad	Equipos informáticos	Data Center del proveedor
A15	SAN	Unidades de almacenamiento donde reside la información de la entidad	Equipos informáticos	Data Center del proveedor
A16	Solución de Backup	Solución de Backup para el respaldo de información del negocio	Equipos informáticos	Data Center del proveedor
A17	Dispositivos de red	Equipos y dispositivos de red activos (switch, router)	Equipos informáticos	Cuartos de rack
A18	Computadores Administradores	Computadores que utilizan los administradores de plataforma	Equipos informáticos	Area administración de plataforma
A19	Computadores de escritorio usuarios	Computadores de escritorio asignados a los colaboradores de la entidad	Equipos informáticos	Computadores
A20	Portátiles	Computadores portátiles de la entidad	Equipos informáticos	Portátiles
A21	Impresoras	Impresoras de la entidad ubicada en diferentes áreas	Equipos informáticos	Impresoras
A22	Equipos de	Equipos informáticos destinados a	Equipos	Equipos de seguridad

	seguridad perimetral	proteger la seguridad perimetral de la entidad	informáticos	perimetral
A23	Aplicación Mesa de Ayuda	Aplicación utilizada por la mesa de ayuda para la gestión de requerimientos e incidentes	Software	Servidores de administración
A24	Sistema Monitoreo de servicios	Aplicaciones utiliza para monitorear el rendimiento y disponibilidad de los servicios de TI	Software	Servidores de administración
A25	Sistema de Control de Acceso	Sistema para controlar el acceso a las áreas de la entidad	Software	Servidores de administración
A26	Herramienta de Virtualización	Herramienta utilizada para la virtualización de servidores	Software	Servidores de administración
A27	Sistema Gestor Base de Datos	Sistema de gestión y administración de las bases de datos de la entidad	Software	Servidores de bases de datos
A28	Antivirus	Software de administración de seguridad para el control de virus	Software	Servidores de administración
A29	Sistema administración de la SAN	Sistema para administrar la SAN	Software	Servidores de administración
A30	Sistema de control de versiones	Sistema de administración para el control de versionamiento de software	Software	Servidores de administración
A31	Sistema de Grabación de llamadas	Sistema para la grabación de las llamadas	Software	Servidores de administración
A32	ERP	Sistema integrado de gestión de la entidad	Software	Servidores de aplicaciones
A33	Aplicativos CORE del negocio	Corresponde a los aplicativos que soportan el CORE del negocio	Software	Servidores de aplicaciones
A34	Aplicativo de nomina	Aplicativo para la gestión de recursos humanos	Software	Servidores de aplicaciones
A35	Sistema de Gestión Documental	Sistema de Gestión documental de la entidad	Software	Servidores de aplicaciones
A36	Sistema de Gestión de Calidad	Aplicativo para el Sistema de Gestión de Calidad	Software	Servidores de aplicaciones
A37	Aplicativo WEB transaccional	Aplicativo web para la consulta y pago de las obligaciones de cartera de los ex empleados	Software	Servidores de aplicaciones
A38	Página WEB	Página Web de la Entidad	Software	Servidores de aplicaciones
A39	Intranet	Página Web de la Entidad	Software	Servidores de aplicaciones
A40	Aplicativos seguimiento proyectos	Página Web de la Entidad	Software	Servidores de aplicaciones
A41	CRM	Aplicativo para gestión relación con clientes	Software	Servidores de aplicaciones
A42	Terminales empresariales	Aplicativo para el pago de las obligaciones con terceros	Software	Otros bancos
A43	Directorio activo	Servicio establecido donde están los objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red	Servicios	Servidores de administración

A44	Correo Electrónico	Correo electrónico corporativo de la entidad	Servicios	Plataforma de Correo
A45	Bases de datos	Bases de datos que almacenan la información de la entidad	Servicios	Servidores de bases de datos
A46	FileServer	Almacenamiento de los documentos electrónicos que manejan las áreas de la entidad	Servicios	Servidores de administración
A47	Video Conferencia	Corresponde al servicio de videoconferencia de la entidad	Servicios	Servidores de administración
A48	Gestión de privilegios	Corresponde al mecanismo para la administración y asignación de privilegios de acceso a los recursos tecnológicos y aplicaciones.	Servicios	Directorio activo
A49	Identidad del Usuario	Información que identifica a un funcionario (nombre, cedula, datos biométricos como la huella, código del usuario, etc)	Datos / Información	Directorio activo
A50	Datos de autenticación	Usuario y Contraseña que utiliza los usuarios para ingresar a los recursos tecnológicos y aplicaciones.	Datos / Información	Directorio activo
A51	Usuarios genéricos	Usuario genéricos que utilizan las aplicaciones para conectarse a las bases de datos	Datos / Información	Bases de datos
A52	Log de evento de seguridad	Log que contiene los registros de los eventos de seguridad y de los eventos de administración sobre las aplicaciones	Datos / Información	Log de eventos
A53	Registro de incidentes de seguridad	Registro de incidentes de seguridad reportados por la herramienta de mesa de ayuda	Datos / Información	Bases de datos
A54	Manuales técnicos de administración	Corresponde a los documentos, manuales y procedimientos relacionadas con la administración de la plataforma	Datos / Información	File Server
A55	Bitácora de control de acceso al centro de computo	Registro de acceso al centro de computo	Datos / Información	Carpetas
A56	Plan estratégico de tecnología	Documento que contiene el plan estratégico de tecnología	Datos / Información	File Server
A57	Documentos del proceso	Corresponde a los documentos del proceso que están publicados en el sistemas de gestión de calidad	Datos / Información	Bases de datos

Una vez identificados los activos de información se procedió a valorar su grado de importación y criticidad para la organización, para lo cual, se valoro la afectación o perdida que le puede generar a la entidad en cuanto aspectos financieros, legales y de imagen, en caso dado que al materializarse una amenaza afecte su disponibilidad, integridad o confidencialidad. Para tal efecto, se utilizaron los siguientes criterios para realizar la respectiva valoración:

Tabla 17. Tabla para valoración activos de información

Aspecto	Criterio de valoración	Criterio de valoración	Valor a asignar
Financiero	Pérdidas económicas para la empresa (porcentaje calculado sobre la utilidad operacional)	Menor o igual a 0.25%	1
		Mayor a 0.25% y menor o igual a 5%	2
		Mayor a 5% y menor o igual a 20%	3
		Mayor a 20% y menor o igual a 50%	4
		Mayor al 50%	5
Legal	Incumplimiento de normatividad y legislación	No tiene repercusión frente a normatividad y contratos.	1
		Genera llamados de atención por parte de los entes de control.	2
		Genera posibles sanciones menores por parte de los entes de control y/o reclamos por parte de terceros.	3
		Genera sanciones económicas por parte de los entres de control y/o demandas por parte de terceros.	4
		Genera sanciones mayores por parte de entes de control, cancelación de contratos, suspensión de licencias, cierre de líneas de negocios.	5
Imagen	Afectación de la imagen de la empresa	Conocido solo de manera interna de la empresa pero no de interés publico	1
		Atención de algunas partes interesadas a nivel local que potencialmente puede afectar a la empresa	2
		Media atención de las partes interesadas a nivel local y regional.	3
		Alta Atención de las partes interesadas a nivel local, regional y nacional.	4
		Conocimiento general a nivel nacional e internacional.	5

Para determinar la criticidad del activo se formularon las siguientes preguntas

:

Tabla 18. Preguntas para determinar la criticidad del activo

Criterio	Factor Afectado	Pregunta
Disponibilidad	Financiero	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control o demandas de terceros?
	Imagen	¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la entidad?
Integridad	Financiero	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la entidad?
Confidencialidad	Financiero	¿Su divulgación no autorizada puede relevar información sensible de la empresa requerida para la toma de decisiones estratégicas y financieras?
	Legal	¿Su divulgación no autorizada puede afectar el cumplimiento de regulaciones impartidas por entes de control o puede generar demandas de terceros?
	Imagen	¿Su divulgación no autorizada puede afectar la imagen de la entidad?

Por último, para determinar el nivel de criticidad del activo se valoro se utilizo los criterios de valoración de la siguiente tabla:

Tabla 19. Nivel de criticidad de los activo de información

Criterio de Evaluación	Valor criticidad activo	Nivel criticidad
La gestión del activo compromete en un alto grado la integridad y/o confidencialidad y/o disponibilidad de la información de la empresa.	>= 4	**Alto**
La gestión del activo compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información.	> 2 y < 4	**Medio**
La gestión del activo compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información de la empresa.	> 0 y <= 2	**Bajo**
La gestión del activo no compromete la integridad, confidencialidad y disponibilidad de la información de la empresa	Igual a 0	No aplica

De acuerdo a la metodología planteada que está relacionado en el Anexo D del presente trabajo, la siguiente es la valoración del nivel de criticidad de los activos del área de tecnológica que se identificaron:

Tabla 20. Valoración nivel criticidad activos información de tecnología

No.	Nombre del Activo	Valoración nivel de criticidad del activo													Nivel de criticidad
		Confidencialidad			Integridad			Disponibilidad							
		Financiero	Legal	Imagen	Financiero	Legal	Imagen	Financiero	Legal	Imagen	Confidencialidad	Integridad	Disponibilidad	Valor Total	
A1	Centro Principal de Procesamiento	5	4	3	5	4	3	5	4	4	5	5	5	5	Alto
A2	Centro Alterno de Procesamiento	5	4	3	5	4	3	5	4	3	5	5	5	5	Alto
A3	Cuartos de comunicaciones	3	3	1	3	3	1	3	3	1	3	3	3	3	Medio
A4	Area administración de plataforma	4	4	3	4	4	3	4	4	3	4	4	4	4	Alto
A5	Red LAN	4	4	3	4	4	3	2	1	1	4	4	2	4	Alto
A6	Red WAN	4	4	3	4	4	3	2	1	1	4	4	2	4	Alto
A7	Red WIFI corporativa	4	4	3	4	4	3	3	3	2	4	4	3	4	Alto
A8	Red WIFI invitados	3	2	1	3	2	1	3	3	1	3	3	3	3	Medio
A9	Servidores de administración	4	3	2	4	3	2	4	3	2	4	4	4	4	Alto
A10	Servidores de bases de datos de producción	4	3	2	4	2	2	4	2	2	4	4	4	4	Alto
A11	Servidores de aplicaciones de producción	4	3	2	4	2	2	4	2	2	4	4	4	4	Alto
A12	Plataforma de Correo	3	3	3	3	3	3	3	3	3	3	3	3	3	Medio
A13	Servidores de Pruebas	1	1	0	0	0	0	0	0	0	1	0	0	1	Bajo
A14	Servidores de Desarrollo	1	1	0	0	0	0	0	0	0	1	0	0	1	Bajo
A15	SAN	4	4	3	4	4	3	4	4	3	4	4	4	4	Alto
A16	Solución de Backup	3	3	2	3	3	2	3	2	2	3	3	3	3	Medio
A17	Dispositivos de red	4	4	3	4	4	3	3	3	2	4	4	3	4	Alto
A18	Computadores Administradores	4	4	3	5	4	3	5	4	3	4	5	5	5	Alto
A19	Computadores de escritorio usuarios	3	3	1	3	3	1	1	1	1	3	3	1	3	Medio
A20	Portátiles	3	3	1	3	3	1	1	1	1	3	3	1	3	Medio
A21	Impresoras	1	1	0	1	1	0	1	1	0	1	1	1	1	Bajo
A22	Equipos de seguridad perimetral	4	4	3	4	4	3	3	3	2	4	4	3	4	Alto
A23	Aplicación Mesa de Ayuda	0	1	0	1	1	0	0	1	0	1	1	1	1	Bajo
A24	Sistema Monitoreo de servicios	0	2	0	0	2	0	0	2	0	2	2	2	2	Bajo
A25	Sistema de Control de Acceso	1	3	0	1	3	0	0	1	0	3	3	1	3	Medio
A26	Herramienta de Virtualización	4	4	3	4	4	3	4	4	3	4	4	4	4	Alto
A27	Sistema Gestor Base de Datos	4	4	3	4	4	3	3	2	2	4	4	3	4	Alto
A28	Antivirus	0	2	0	0	2	0	2	2	2	2	2	2	2	Bajo
A29	Sistema administración de la SAN	4	4	3	4	4	3	4	4	3	4	4	4	4	Alto
A30	Sistema de control de versiones	0	2	0	0	2	0	0	0	0	2	2	0	2	Bajo
A31	Sistema de Grabación de llamadas	3	3	1	3	3	1	3	3	1	3	3	3	3	Medio

A32	ERP	3	3	1	3	3	1	2	1	0	3	3	2	3	Medio
A33	Aplicativos CORE del negocio	4	3	1	4	3	1	2	1	0	4	4	2	4	Alto
A34	Aplicativo de nomina	3	3	1	3	3	1	2	1	0	3	3	2	3	Medio
A35	Sistema de Gestión Documental	2	2	1	2	2	1	1	1	0	2	2	1	2	Bajo
A36	Sistema de Gestión de Calidad	1	1	1	1	1	1	1	1	0	1	1	1	1	Bajo
A37	Aplicativo WEB transaccional	0	3	2	0	3	2	0	0	1	3	3	1	3	Medio
A38	Página WEB	1	3	3	1	3	3	1	1	2	3	3	2	3	Medio
A39	Intranet	0	1	1	0	1	1	0	0	0	1	1	0	1	Bajo
A40	Aplicativos seguimiento proyectos	0	2	2	0	2	2	0	2	2	2	2	2	2	Bajo
A41	CRM	0	3	1	0	2	1	0	0	0	3	2	0	3	Medio
A42	Terminales empresariales	0	3	0	0	3	1	0	0	0	3	3	0	3	Medio
A43	Directorio activo	4	4	0	4	4	0	0	0	0	4	4	0	4	Alto
A44	Correo Electrónico	3	3	2	3	3	2	0	0	2	3	3	2	3	Medio
A45	Bases de datos	4	4	2	4	4	2	0	0	2	4	4	2	4	Alto
A46	FileServer	4	4	2	4	4	2	0	0	2	4	4	2	4	Alto
A47	Video Conferencia	0	1	1	0	1	1	0	0	1	1	1	1	1	Bajo
A48	Gestión de privilegios	4	4	0	4	4	0	0	0	0	4	4	0	4	Alto
A49	Identidad del Usuario	2	4	1	2	4	1	0	0	2	4	4	2	4	Alto
A50	Datos de autenticación	4	4	1	3	4	1	0	0	2	4	4	2	4	Alto
A51	Usuarios genéricos	4	4	1	3	4	1	0	0	2	4	4	2	4	Alto
A52	Log de evento de seguridad	3	4	0	3	4	0	0	0	0	4	4	0	4	Alto
A53	Registro de incidentes de seguridad	3	4	0	3	4	0	0	0	0	4	4	0	4	Alto
A54	Manuales técnicos de administración	1	1	0	1	1	0	0	0	0	1	1	0	1	Bajo
A55	Bitácora de control de acceso al centro de computo	1	1	0	1	1	0	0	0	0	1	1	0	1	Bajo
A56	Plan estratégico de tecnología	2	2	0	1	2	2	0	0	0	2	2	0	2	Bajo
A57	Documentos del proceso	1	1	0	1	1	0	0	0	0	1	1	0	1	Bajo

Para el análisis de riesgos de los activos información y teniendo en cuenta las recomendaciones del capítulo '**3.9 Determinar los activos para la valoración de riesgos**' de la metodología relacionada en el Anexo D del presente trabajo, se opto por seleccionar los activos de información con nivel de criticidad Alto y Medio, y agruparlos en la medida de lo posible por contener. Aquellos contenedores que incluyeran más de un activo de información se utilizaron para la valoración de riesgos en vez de hacerlo sobre el activo.

De acuerdo a lo anterior, los siguientes fueron los contenedores y/o activos de información que se seleccionaron para el proceso de valoración de riesgos:

Tabla 21. Activos seleccionados para valoración de riesgos

Activo de Información	Nivel de criticidad	Contener y/o activo seleccionado para valoración de riesgos
A4. Area administración de plataforma	Alto	Area administración de plataforma
A18. Computadores Administradores	Alto	
A53. Registro de incidentes de seguridad	Alto	Bases de datos
A51. Usuarios genéricos	Alto	
A19. Computadores de escritorio usuarios	Medio	Computadores
A17. Dispositivos de red	Alto	Cuartos de rack
A3. Cuartos de comunicaciones	Medio	
A2. Centro Alterno de Procesamiento	Alto	Data Center del proveedor
A1. Centro Principal de Procesamiento	Alto	
A15. SAN	Alto	
A9. Servidores de administración	Alto	
A11. Servidores de aplicaciones de producción	Alto	
A10. Servidores de bases de datos de producción	Alto	
A12. Plataforma de Correo	Medio	
A16. Solución de Backup	Medio	
A50. Datos de autenticación	Alto	Directorio activo
A48. Gestión de privilegios	Alto	
A49. Identidad del Usuario	Alto	
A22. Equipos de seguridad perimetral	Alto	Equipos de seguridad perimetral
A52. Log de evento de seguridad	Alto	Log de eventos
A42. Terminales empresariales	Medio	Otros bancos
A44. Correo Electrónico	Medio	Plataforma de Correo
A20. Portátiles	Medio	Portátiles
A5. Red LAN	Alto	Red LAN
A7. Red WIFI corporativa	Alto	
A8. Red WIFI invitados	Medio	
A6. Red WAN	Alto	RED WAN
A43. Directorio activo	Alto	Servidores de administración
A46. FileServer	Alto	
A26. Herramienta de Virtualización	Alto	
A29. Sistema administración de la SAN	Alto	
A25. Sistema de Control de Acceso	Medio	
A31. Sistema de Grabación de llamadas	Medio	
A33. Aplicativos CORE del negocio	Alto	Servidores de aplicaciones
A34. Aplicativo de nomina	Medio	
A37. Aplicativo WEB transaccional	Medio	
A41. CRM	Medio	
A32. ERP	Medio	
A38. Página WEB	Medio	
A45. Bases de datos	Alto	Servidores de bases de datos
A27. Sistema Gestor Base de Datos	Alto	

5.3.2. VALORACION RIESGOS ACTIVOS DE TECNOLOGIA

Se procedió a realizar la valoración de los riesgos a los cuales están expuestos los activos de información que se identificaron para el proceso de tecnología, para lo cual, se desarrollo las siguientes actividades:

- Identificación de riesgo
- Análisis del riesgo inherente
- Elaboración matriz de riesgo inherente
- Valoración de controles existentes para mitigar el riesgo inherente
- Determinación de riesgos residual
- Elaboración matriz de riesgo residual

NOTA: El detalle de los riesgos del proceso de tecnología se encuentra en el Anexo E del presente trabajo, el cual además de esta información contiene los parámetros, la formulación y los cálculos se utilizaron para determinar el riesgo inherente y el residual.

5.3.2.1. IDENTIFICACION DE AMENZAS

Se identificaron las amenazas a las que estos están expuestos los activos de información de la dirección de tecnología que fueron seleccionados para la valoración de riesgos, para lo cual, se planearon las siguientes preguntas:

- ¿Cuál es la probabilidad de ocurrencia de la amenaza?
- ¿Cuál sería el impacto en caso de que ocurriera?
- ¿Cuáles de los criterios de seguridad afectaría, si la confidencialidad, la integridad o la disponibilidad?

Para facilitar esta labor de identificación, se elaboro la siguiente lista que contiene una serie de riesgos de seguridad que en términos generales pueden afectar a cualquier tipo de organización y los principios de seguridad que se ven afectos, relacionados con la confidencialidad, disponibilidad e integridad de la información:

Tabla 22. Lista de riesgos y principios de seguridad afectados

RIESGOS	Principios afectadas		
	C	I	D
Abuso de privilegios de acceso	X	X	
Acceso no autorizado	X	X	
Auditorias débiles			
Cambio de privilegios sin autorización	X	X	X
Denegación de Servicio			X
Divulgación o robo de información de autenticación	X		
Divulgación no autorizada de información del negocio	X		
Ejecución de ingeniería social	X		
Errores del administrador	X	X	X
Instalación de software no autorizado		X	X
Interceptación no autorizada de información en tránsito	X		
Manipulación de la configuración	X		
Modificación sin autorización		X	
Pérdida o robo de información	X		X
Suplantación de identidad de usuarios	X	X	
Uso inadecuado de sistemas para generar fraudes	X	X	
Uso inadecuado de sistemas que generan interrupción			X

Con base en esta información se identificaron las siguientes amenazas a las cuales están expuestos los activos de información de la Dirección de Tecnología seleccionados para el proceso de valoración de riesgos:

Tabla 23. Amenazas que pueden afectar los activos de tecnología

Amenazas	Activos de tecnología que pueden ser afectado	
Acceso no autorizado	• Area administración de plataforma • Bases de datos • Cuartos de Rack • Data Center del proveedor • Directorio Activo • Equipos de seguridad perimetral	• Servidores de Administración • Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo
Ataques externos / internos (hacking no ético)	• Bases de datos • Equipos de seguridad perimetral • Servidores de Administración • Plataforma de Correo	• Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Data Center del proveedor
Cambio de privilegios sin	• Bases de Datos	• Servidores de bases de datos de producción

autorización	• Directorio Activo • Servidores de Administración	• Servidores de aplicaciones de producción • Plataforma de Correo
Desastres naturales	• Data Center del proveedor	
Divulgación de información de autenticación	• Bases de Datos • Directorio Activo	• Servidores de Administración
Error del administrador	• Bases de datos • Data Center del proveedor • Directorio Activo • Red LAN • Red WAN	• Servidores de Administración • Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo • Equipos de seguridad perimetral
Instalación de software no autorizado	• Directorio Activo • Computadores	• Portátiles
Interceptación no autorizada de información en tránsito	• Red LAN • Red WAN	• Servicio de Correo
Interrupción en los servicios	• Bases de datos • Data Center del proveedor • Directorio Activo	• Red LAN • Red WAN • Servidores de Producción
Modificación sin autorización	• Bases de datos • Directorio Activo • Servidores de Administración	• Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo
Robo de equipos	• Area administración de plataforma • Cuartos de Rack	• Data Center del proveedor
Robo de información	• Bases de datos • Directorio Activo • Servidores de Administración	• Servidores de bases de datos de producción • Plataforma de Correo
Suplantación de identidad de usuarios	• Directorio Activo	• Servicio de Correo
Uso inadecuado de sistemas para generar fraudes	• Bases de datos • Directorio Activo • Servidores de Administración	• Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo
Uso inadecuado de sistemas que generan interrupción	• Bases de datos • Data Center del proveedor • Directorio Activo • Red LAN • Red WAN	• Servidores de Administración • Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo
Abuso de privilegios	• Data Center del proveedor • Directorio Activo • Servidores de Administración	• Servidores de bases de datos de producción • Servidores de aplicaciones de producción • Plataforma de Correo

Las siguientes son vulnerabilidades asociadas a las diferentes amenazas identificadas y que están relacionados con las características de los activos de la dirección de tecnología o de sus contenedores:

Tabla 24. Vulnerabilidad asociados a las amenazas de los activos

AMENAZA	ACTIVOS	VULNERABILIDADES
Acceso no autorizado	Area administración de plataforma Bases de datos Cuartos de Rack Data Center del proveedor Directorio Activo Equipos de seguridad perimetral Servidores de Administración Servidores de bases de datos de producción Servidores de aplicaciones de producción Plataforma de Correo	• Inadecuada Administración de Seguridad • Ausencia o Inadecuada plataforma de Seguridad Perimetral • Inadecuada Administración o Asignación de roles y permisos • Ausencia de una configuración segura de la red • Contraseñas no seguras • Configuración incorrecta de las cuentas de usuario • Falta de seguridad de los puertos de red • Políticas no aplicada o no existencia de seguridad
Ataques externos / internos (hacking no ético)	Bases de datos Equipos de seguridad perimetral Servidores de Administración Servidores de bases de datos de producción Servidores de aplicaciones de producción Plataforma de Correo Data Center del proveedor	• Inadecuada Administración de Seguridad • Ausencia o Inadecuada plataforma de Seguridad Perimetral • Ausencia de una configuración segura de la red • Falla de seguridad en los componentes de red
Cambio de privilegios sin autorización	Bases de Datos Directorio Activo Servidores de Administración Servidores de bases de datos de producción Servidores de aplicaciones de producción Plataforma de Correo	• Contraseñas no seguras • Inadecuada Administración o Asignación de roles y permisos • Inadecuada Administración de Seguridad • Políticas no aplicada o no existencia de seguridad
Desastres naturales (Terremotos, Incendios, Inundaciones, etc.)	Data Center del proveedor	• Ausencia de un sistema de continuidad de negocio • Ubicación física de los equipos • Ubicación física del centro de cómputo • Políticas no aplicada o no existencia de seguridad física
Divulgación de información de autenticación	Bases de Datos Directorio Activo Servidores de Administración	• Inadecuada Administración de Seguridad • Contraseñas no seguras • Políticas no aplicada o no existencia de seguridad • Inadecuada Administración o Asignación de roles y permisos • Inadecuado mecanismo de cifrado
Error del administrador	Bases de datos Data Center del proveedor Directorio Activo Red LAN	• Ausencia de capacitación permanente • Ausencia o inadecuado procedimiento de control de cambios • Desmotivación del personal

	Red WAN Servidores de Administración Servidores de bases de datos de producción Servidores de aplicaciones de producción Plataforma de Correo Equipos de seguridad perimetral	
Instalación de software no autorizado	Directorio Activo Computadores Portátiles	• Políticas no aplicada o no existencia de seguridad • Inadecuada Administración o Asignación de roles y permisos
Interceptación no autorizada de información en tránsito	Red LAN Red WAN Correo	• Políticas no aplicada o no existencia de seguridad • Inadecuado mecanismo de cifrado
Interrupción en los servicios	Bases de datos Data Center del proveedor Directorio Activo Red LAN Red WAN Servidores de Producción	• Inadecuada Configuración y Capacidad de los ambientes • Ausencia o inadecuado procedimiento de control de cambios • Falta de mantenimiento de equipos
Modificación sin autorización	Bases de datos Directorio Activo Servidores de Administración Servidores de bases de datos de producción Servidores de aplicaciones de producción Plataforma de Correo	• Políticas no aplicada o no existencia de seguridad • Inadecuada Administración o Asignación de roles y permisos • Inadecuado mecanismo de cifrado
Robo de equipos	Area administración de plataforma Cuartos de Rack Data Center del proveedor	• Políticas no aplicada o no existencia de seguridad • Ausencia o inadecuado plataforma de vigilancia física • Inadecuado inventario de activos físicos • Ubicación física de los equipos
Robo de información	Bases de datos Directorio Activo Servidores de Administración Servidores de bases de datos de producción Plataforma de Correo	• Inadecuada Administración de Seguridad • Ausencia o Inadecuada plataforma de Seguridad Perimetral • Políticas no aplicada o no existencia de seguridad • Inadecuada Administración o Asignación de roles y permisos • Inadecuado mecanismo de cifrado • Inexistencia de Logs de eventos de seguridad
Suplantación de identidad de usuarios	Directorio Activo Servicio de Correo	• Contraseñas no seguras • Cuentas de usuario sin auditar • Ausencia o inadecuado plataforma de vigilancia física • Inadecuado mecanismo de cifrado
Uso inadecuado de sistemas para generar fraudes	Bases de datos Directorio Activo Servidores de Administración Servidores de bases de datos de producción	• Inadecuada Administración de Seguridad • Cuentas de usuario sin auditar • Inexistencia de Logs de eventos de seguridad • Inadecuada Administración o Asignación de roles y permisos

	Servidores de aplicaciones de producción Plataforma de Correo	• Políticas no aplicada o no existencia de seguridad
Uso inadecuado de sistemas que generan interrupción	Bases de datos Data Center del proveedor Directorio Activo Red LAN Red WAN Servidores de Administración Servidores de bases de datos de producción Servidores de aplicaciones de producción Plataforma de Correo	• Inadecuada Administración de Seguridad • Cuentas de usuario sin auditar • Inexistencia de Logs de eventos de seguridad • Inadecuada Administración o Asignación de roles y permisos • Políticas no aplicada o no existencia de seguridad
Abuso de privilegios	Data Center del proveedor Directorio Activo Servidores de Administración Servidores de bases de datos de producción Servidores de aplicaciones de producción Plataforma de Correo	• Cuentas de usuario sin auditar • Contraseñas no seguras • Inexistencia de Logs de eventos de seguridad • Inadecuada Administración o Asignación de roles y permisos • Políticas no aplicada o no existencia de seguridad

5.3.2.2. ANALISIS DEL RIESGO INGERENTE

Por medio del análisis de riesgos se estableció la probabilidad de ocurrencia de los riesgos y el impacto de los mismos, con el fin de obtener el nivel de riesgo inherente, el cual, nos permitió establecer el nivel de riesgo propio de la actividad sin tener en cuenta las medidas y controles de seguridad que actualmente existen en la entidad para mitigar o minimizar los riesgos.

Para determinar la probabilidad de ocurrencia de una amenaza sobre cada uno de los activos, se utilizo los siguientes criterios de valoración:

Tabla 25. Valoración probabilidad de ocurrencia

Probabilidad de ocurrencia en un (1) años	Valor Cualitativo	Valor Asignado
Una vez cada año	Raro	1
Una vez cada seis (6) meses	Baja (Improbable)	2
Una vez cada tres (3) meses	Media (Posible)	3
Una vez cada mes	Alta (Probable)	4
Más de una vez al mes	Muy Alta	5

Para determinar el impacto que pueden tener las pérdidas de confidencialidad, integridad y disponibilidad sobre los activos de información se utilizo los siguientes criterios de valoración:

Tabla 26. Valoración del impacto

Impacto	Impacto cuantitativo (Porcentaje sobre utilidad operacional)	Impacto Cualitativo (Uno o más factores)	Valor
Insignificante	Genera pérdidas financieras pequeñas no significativas. (Perdida Menor o igual a 0.25%)	• No afecta la seguridad de la información de la entidad. • No afecta la imagen de la entidad ante las partes interesadas. • Genera reprocesos insignificantes. • La información se puede recuperar rápidamente con la misma calidad.	1
Menor	Genera pérdidas financieras menores no significativas. (Perdida Mayor a 0.25% y menor o igual a 5%)	• No afecta la seguridad de la información de la entidad. • Afecta en menor grado la imagen de la entidad ante las partes interesadas. • Genera reprocesos menores. • La información se puede recuperar en un tiempo moderado con la misma calidad.	2
Moderado	Genera pérdidas financieras moderadas. (Mayor a 5% y menor o igual a 20%)	• Afecta en menor grado la seguridad de la información de la entidad. • Afecta medianamente la imagen de la entidad ante las partes interesadas. • Genera reprocesos moderados. • La información se puede recuperar pero no con la misma calidad	3
Mayor	Genera pérdidas financieras mayores. (Perdida mayor o igual a 20% y menor a 50%)	• Afecta en mayor grado la seguridad de la información de la entidad. • Afecta altamente la imagen de la entidad ante las partes interesadas. • Genera reprocesos mayores. • Es difícil recuperar la información	4
Catastrófico	Genera pérdidas financieras críticas. (Perdidas Mayores a 50%)	• Afectar seriamente la seguridad de la información de la entidad. • Afecta gravemente la imagen de la empresa ante las partes interesadas • Puede generar pérdida masiva de clientes. • Genera alto nivel de reprocesos. • Es difícil y costoso recuperar la información. • Afecta la continuidad del negocio	5

El nivel de **riesgo inherente** es igual a el **valor de la probabilidad x valor del impacto.**

Para clasificar el riesgo ya se inherente o residual dependiente de su nivel de riesgo, se utilizo los siguientes criterios de valoración que determinan el tipo de riesgo:

Tabla 27. Valoración de los riesgos

Tipo de riesgo	Valor Nivel Riesgo	Acción requerida
Riesgo Extremo	Nivel Riesgo mayor o igual a 15 puntos	Requiere acciones inmediatas que permitan reducir y compartir el riesgo, transferirlo o incluso evitarlo
Riesgo Alto	Nivel Riesgo mayor o igual a 10 y menor a 15 puntos	Requieren atención urgente e implementar medidas para reducir el nivel del riesgo
Riesgo Medio	Nivel Riesgo mayor o igual a 5 y menor a 10 puntos	Requiere de medidas prontas y adecuadas que permitan disminuir el riesgo a nivel bajo o inusual
Riesgo Bajo	Nivel Riesgo mayor o igual a 3 y menor a 5 puntos	El riesgo se mitiga con actividades propias y por medio de algunas medidas preventivas para reducir el riesgo
Riesgo Inusual	Nivel Riesgo Menor a 3 puntos	Se puede aceptar el riesgo sin necesidad de tomar otras medidas de control diferentes a las existentes.

El siguiente es el resultado del proceso de valoración del riesgo inherente de las amenazas asociados a los activos de información de la Dirección de Tecnología:

Tabla 28. Valoración de riesgos inherente Dirección de Tecnología

RIESGOS	VALORACION IMPACTO			Probabilidad	ESTIMACION DE RIESGO			Nivel de Riesgo
	D	I	C		D	I	C	
R1. Acceso no autorizado		Mayor	Catastrófico	Alta		Riesgo Extremo	Riesgo Extremo	Riesgo Extremo
R2. Ataques externos / internos (hacking no ético)	Mayor		Mayor	Alta	Riesgo Extremo		Riesgo Extremo	Riesgo Extremo
R3. Cambio de privilegios sin autorización	Moderado	Moderado	Moderado	Alta	Riesgo Alto	Riesgo Alto	Riesgo Alto	Riesgo Alto
R4. Desastres naturales (Terremotos, Incendios, Inundaciones, etc.)	Mayor			Raro	Riesgo Bajo			Riesgo Bajo
R5. Divulgación de información de autenticación			Moderado	Media			Riesgo Medio	Riesgo Medio
R6. Error del administrador	Moderado			Alta	Riesgo Alto			Riesgo Alto
R7. Instalación de software no autorizado		Menor		Media		Riesgo Medio		Riesgo Medio
R8. Interceptación no autorizada de información en tránsito		Mayor	Mayor	Alta		Riesgo Extremo	Riesgo Extremo	Riesgo Extremo
R9. Interrupción en los servicios	Moderado			Media	Riesgo Medio			Riesgo Medio
R10. Modificación sin autorización		Moderado		Media		Riesgo Medio		Riesgo Medio
R11. Robo de equipos	Moderado			Media	Riesgo Medio			Riesgo Medio
R12. Robo de información	Mayor		Mayor	Media	Riesgo Alto		Riesgo Alto	Riesgo Alto
R13. Suplantación de identidad de usuarios			Moderado	Baja			Riesgo Medio	Riesgo Medio
R14. Uso inadecuado de sistemas para generar fraudes			Mayor	Baja			Riesgo Medio	Riesgo Medio
R15. Uso inadecuado de sistemas que generan interrupción	Mayor			Baja	Riesgo Medio			Riesgo Medio
R16. Abuso de privilegios		Mayor	Mayor	Alta		Riesgo Extremo	Riesgo Extremo	Riesgo Extremo

D: Disponibilidad, I: Integridad, C: Confidencialidad

Tabla 29. Riesgos inherentes de Tecnología por tipo de riesgo

RIESGO	ACTIVOS	Probabilidad	Impacto	Nivel de Riesgo Probabilidad x impacto	
R1. Acceso no autorizado	Area administración de plataforma Bases de datos Cuartos de Rack Data Center del proveedor Directorio Activo Equipos de seguridad perimetral Servidores de Administración, bases de datos y aplicaciones de producción Plataforma de Correo	4. Alta	5. Catastrófico	20	Riesgo Extremo
R2. Ataques externos / internos (hacking no ético)	Bases de datos Equipos de seguridad perimetral Servidores de Administración, bases de datos y aplicaciones de producción Plataforma de Correo Data Center del proveedor	4. Alta	4. Mayor	16	Riesgo Extremo
R8. Interceptación no autorizada de información en tránsito	Red LAN y Red WAN Correo	4. Alta	4. Mayor	16	Riesgo Extremo
R16. Abuso de privilegios	Data Center del proveedor Directorio Activo Servidores de Administración, bases de datos y aplicaciones de producción Plataforma de Correo	4. Alta	4. Mayor	16	Riesgo Extremo
R3. Cambio de privilegios sin autorización	Bases de Datos Directorio Activo Servidores de Administración, bases de datos y aplicaciones de producción Plataforma de Correo	4. Alta	3. Moderado	12	Riesgo Alto
R6. Error del administrador	Bases de datos Data Center del proveedor Directorio Activo Red LAN y Red WAN Servidores de Administración, bases de datos y aplicaciones de producción Plataforma de Correo Equipos de seguridad perimetral	4. Alta	0. No afecta	12	Riesgo Alto
R12. Robo de información	Bases de datos Directorio Activo Servidores de Administración Servidores de bases de datos de producción Plataforma de Correo	3. Media	4. Mayor	12	Riesgo Alto
R5. Divulgación de información de autenticación	Bases de Datos Directorio Activo Servidores de Administración	3. Media	3. Moderado	9	Riesgo Medio
R9. Interrupción en los servicios	Bases de datos Data Center del proveedor Directorio Activo Red LAN y Red WAN Servidores de Administración, bases de datos y aplicaciones de producción	3. Media	0. No afecta	9	Riesgo Medio
R10. Modificación sin	Bases de datos	3. Media	0. No afecta	9	Riesgo

autorización	Directorio Activo Servidores de Administración, bases de datos y aplicaciones de producción Plataforma de Correo				Medio
R11. Robo de equipos	Area administración de plataforma Cuartos de Rack Data Center del proveedor	3. Media	0. No afecta	9	Riesgo Medio
R14. Uso inadecuado de sistemas para generar fraudes	Bases de datos Directorio Activo Servidores de Administración, bases de datos y aplicaciones de producción Plataforma de Correo	2. Baja	4. Mayor	8	Riesgo Medio
R15. Uso inadecuado de sistemas que generan interrupción	Bases de datos Data Center del proveedor Directorio Activo Red LAN y Red WAN Servidores de Administración, bases de datos y aplicaciones de producción Plataforma de Correo	2. Baja	0. No afecta	8	Riesgo Medio
R7. Instalación de software no autorizado	Directorio Activo Computadores Portátiles	3. Media	0. No afecta	6	Riesgo Medio
R13. Suplantación de identidad de usuarios	Directorio Activo Servicio de Correo	2. Baja	3. Moderado	6	Riesgo Medio
R4. Desastres naturales	Data Center del proveedor	1. Raro	0. No afecta	4	Riesgo Bajo

La siguiente es la distribución del riesgo inherente asociado a los activos de información de la Dirección de Tecnología que fueron seleccionados para el proceso de valoración de riesgos:

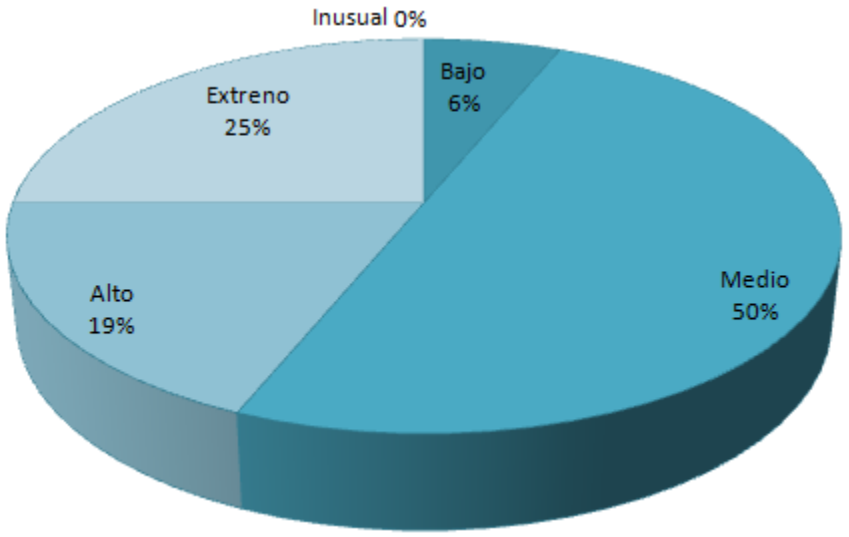


Figura 11. Distribución del riesgo inherente activos Dirección de Tecnología
Fuente: El autor

5.3.2.3. MAPA DE CALOR

El mapa de calor permite representar de forma gráfica un plano conformado por zonas donde se ubicación los riesgos de acuerdo a su probabilidad y su impacto. Cada zona dentro del mapa de calor corresponde a un tipo de riesgo, el cual indica las acciones que se deben realizar para el tratamiento del riesgo.

El siguiente es el mapa de calor que tuvo en cuenta para determinar la ubicación de los riesgos inherentes que fueron identificados:

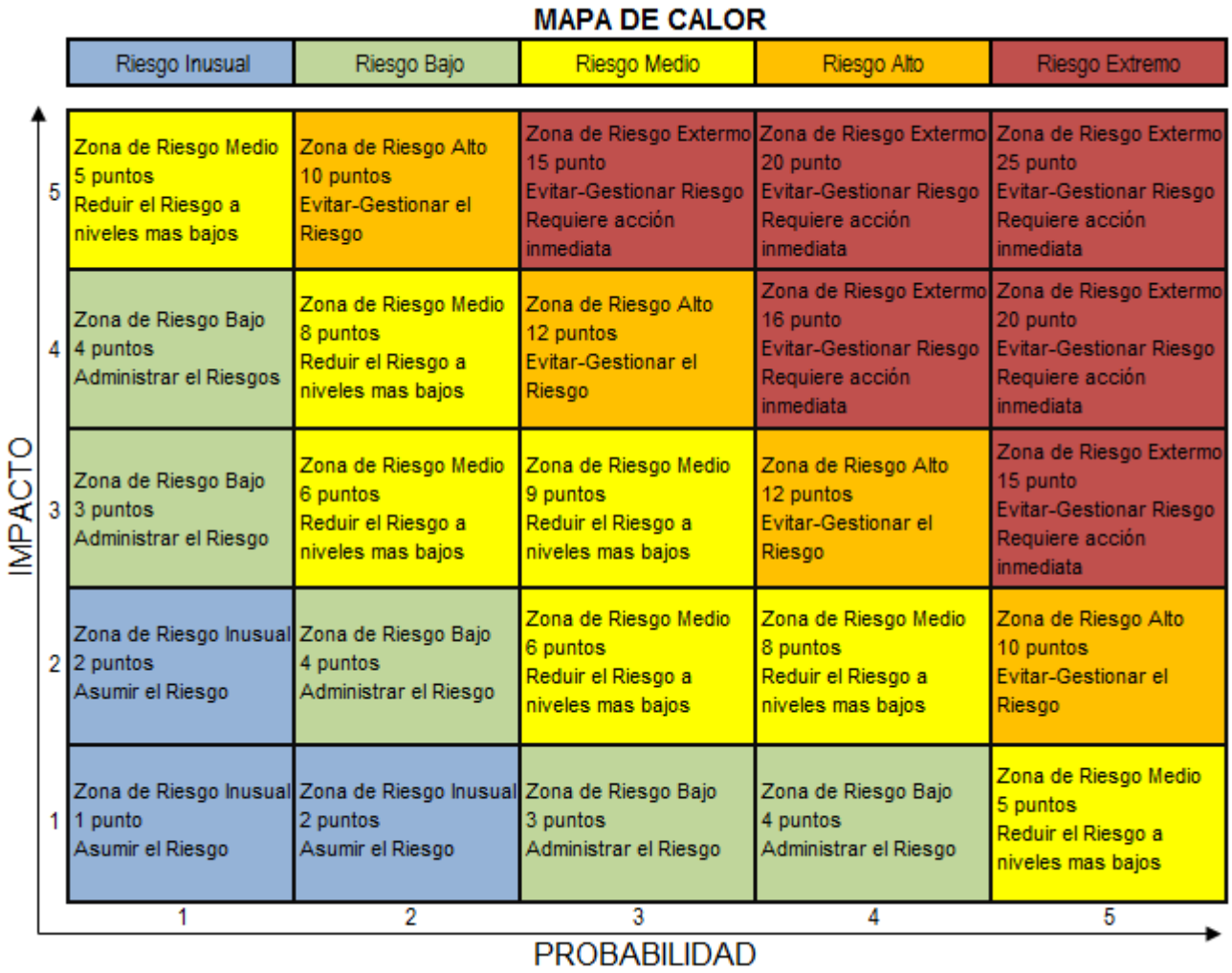


Figura 12. Mapa de Calor
Fuente: La entidad

Se utilizo una matriz de 5x5 para el mapa de calor, debido a que las metodologías de riesgos de la entidad utilizan este tipo de matrices para la valoración de los diferentes tipos de riesgos.

5.3.2.4. MAPA DE RIESGO INHERENTE

Los siguientes son los mapas de riesgo inherente del proceso de tecnología:

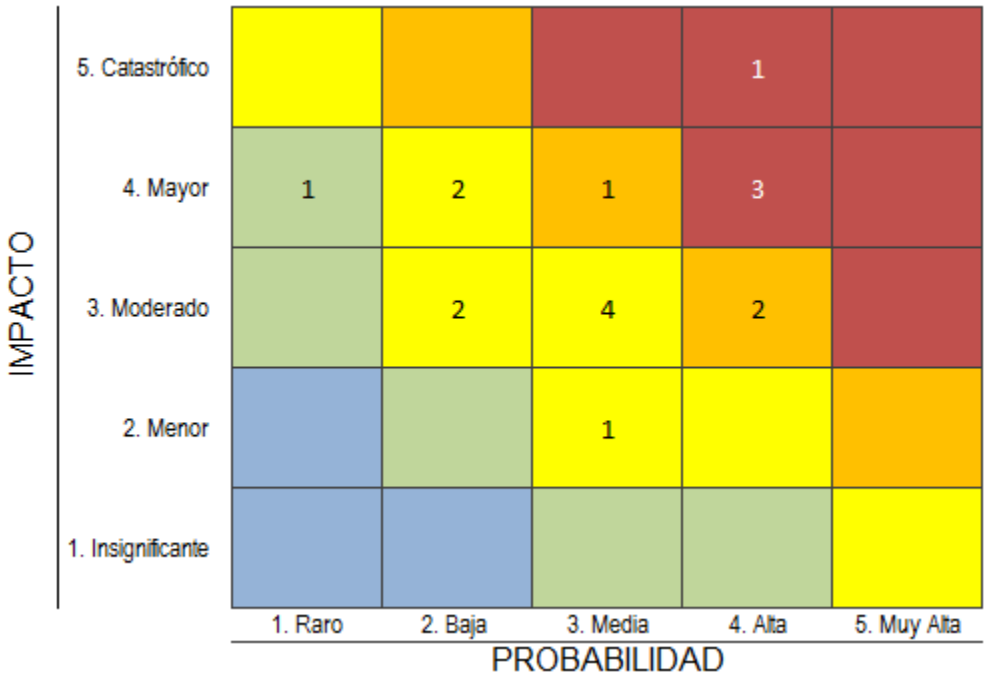


Figura 13. Mapa Riesgo inherentes detallado proceso de tecnología

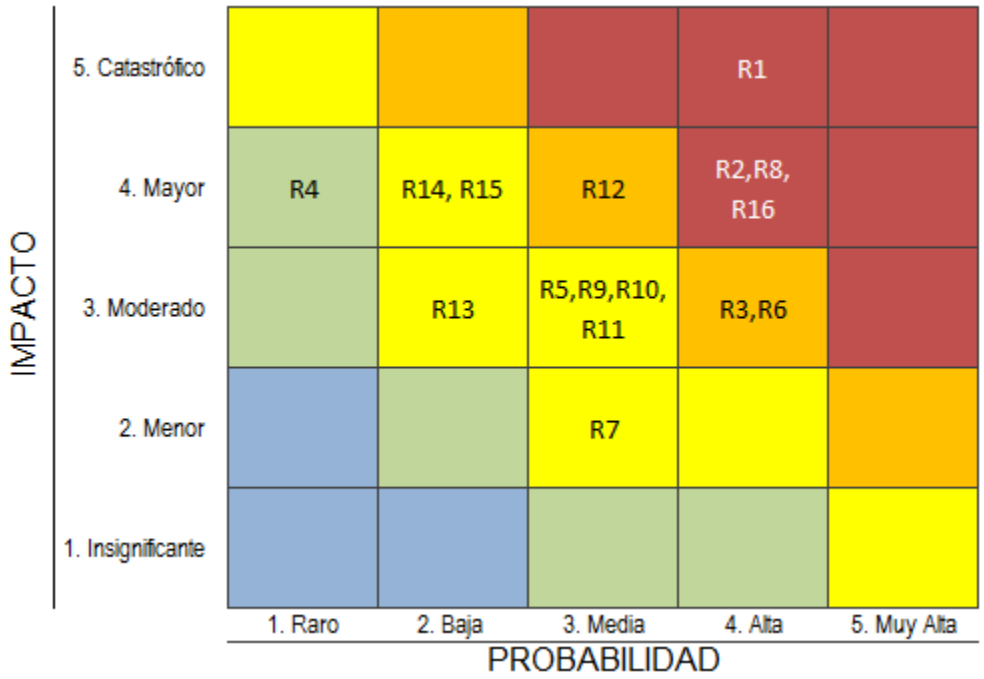


Figura 14. Mapa Riesgo inherentes detallado proceso de tecnología

5.3.2.5. VALORACION DE CONTROLES

Una vez generada la matriz de riesgo inherente se procedió a valorar la efectividad de los controles existentes, con el objetivo determinar el nivel de desplazamiento que estos pueden genera sobre el mapa de calor de riesgo, lo cual determina, el mapa de calor del riesgo residual.

Para determinar la efectividad del control se utilizo como guía la metodología de riesgos propuesta por el Departamento Administrativo de la Función Pública en su guía para la administración del riesgo [15], la cual propone valorador los siguientes aspectos, características o cualidades del control, a los cuales se les asigna un peso sobre un total de 100 puntos[65]:

Tabla 30. Criterios para evaluar la efectividad del control

Aspectos a evaluar	Opciones de respuesta	Peso
Afecta impacto o probabilidad. Permite establecer el movimiento que genera sobre la matriz, si sobre el eje X (probabilidad) o sobre el eje Y (impacto)	Impacto	
	Probabilidad	
Categoría del control	Control Preventivo	20
	Control Detectivo	15
	Control Correctivo	5
Herramientas para ejercer el control	SI	15
	NO	0
Están definidos los responsables de la ejecución del control y del seguimiento	SI	15
	NO	0
La frecuencia de la ejecución del control y seguimiento es adecuada.	SI	20
	NO	0
El tiempo que lleva el control ha demostrado ser efectivo	SI	20
	NO	0
Está documentado los pasos para el manejo del control	SI	10
	NO	0

La pregunta relacionada con ‘Afecta impacto o probabilidad’, permite establecer el movimiento que genera la efectividad del control sobre el mapa de calor, si sobre el eje X (probabilidad) o sobre el eje Y (impacto).

Con base en los anteriores criterios, el siguiente es el resultado de la valoración de la efectividad de los controles existentes:

[65] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, Pág., 34

Tabla 31. Valoración de controles

RIESGO \ AMENAZA	DESCRIPCION DEL CONTROL	ASPECTOS A EVALUAR DEL CONTROL							
		Tipo de control (afecta impacto o probabilidad)	Categoria	Existe una herramienta para ejercer el control	Están definidos los responsables de la ejecución del control y del seguimiento	La frecuencia de la ejecución del control y seguimiento es adecuada.	El tiempo que lleva el control ha demostrado ser efectivo	Está documentado los pasos para el manejo del control	TOTAL PUNTAJE
R1. Acceso no autorizado	Se cuenta con un sistema de control de acceso biométrico para ingresar a las áreas seguras y cámaras de vigilancia	Probabilidad	Preventivo	SI	NO	SI	SI	NO	75
			20	15	0	20	20	0	
	Existe un plataforma de seguridad perimetral en alta disponibilidad	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
	El acceso de los usuarios al los recursos tecnológicos se controla por el directorio activo	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	Probabilidad	Preventivo	SI	NO	NO	NO	NO	35
			20	15	0	0	0	0	
	Se cuenta con un esquema de privilegios sobre el fileserver	Probabilidad	Preventivo	SI	NO	NO	NO	NO	35
			20	15	0	0	0	0	
R2. Ataques externos / internos (hacking no ético)	Existe un plataforma de seguridad perimetral en alta disponibilidad	Probabilidad	Preventivo	SI	SI	SI	SI	NO	90
			20	15	15	20	20	0	
R3. Cambio de privilegios sin autorización	Se cuenta con un procedimiento formal de control de cambios	Probabilidad	Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	
R4. Desastres naturales (Terremotos, Incendios, Inundaciones, etc.)	Centro principal de procesamiento TIER III y Centro alterno de procesamiento TIER II	Impacto	Correctivo	SI	SI	NO	NO	SI	45
			5	15	15	0	0	10	
	Simulacros de evacuación	Impacto	Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	
R5. Divulgación de información de autenticación	Se tiene implementada la política de contraseña segura	Probabilidad	Preventivo	SI	NO	SI	SI	NO	75
			20	15	0	20	20	0	
R6. Error del administrador	Se cuenta con un procedimiento formal de control de cambios	Probabilidad	Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	
R7. Instalación de software no autorizado	Se tiene implementada la política para restringir la instalación de software por parte de los usuarios	Probabilidad	Preventivo	SI	NO	SI	SI	NO	75
			20	15	0	20	20	0	
R8. Interceptación no autorizada de información en tránsito	Los canales de comunicaciones con las regionales utilizan protocolos de encripción para la transmisión de datos.	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
R9. Interrupción en los servicios	Se cuenta con una plataforma en alta disponibilidad	Impacto	Correctivo	SI	SI	NO	SI	NO	55
			5	15	15	0	20	0	
	Se cuenta con un procedimiento formal de	Probabilidad	Preventivo	SI	SI	NO	NO	SI	60

	control de cambios		20	15	15	0	0	10	
	Centro principal de procesamiento TIER III y Centro alterno de procesamiento TIER II	Impacto	Correctivo	SI	SI	NO	NO	SI	45
			5	15	15	0	0	10	
R10. Modificación sin autorización	El acceso de los usuarios al los recursos tecnológicos se controla a través del directorio activo	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	Probabilidad	Preventivo	SI	NO	NO	NO	NO	35
			20	15	0	0	0	0	
	Se cuenta con un esquema de privilegios sobre el fileserver	Probabilidad	Preventivo	SI	NO	SI	NO	NO	55
			20	15	0	20	0	0	
R11. Robo de equipos	Se cuenta con un sistema de control de acceso biométrico para ingresar a las áreas seguras y cámaras de vigilancia	Probabilidad	Preventivo	SI	SI	SI	SI	SI	100
			20	15	15	20	20	10	
	Existe guardias de seguridad que revisan a los equipos que entran y salen de la entidad	Probabilidad	Preventivo	SI	SI	SI	NO	SI	80
			20	15	15	20	0	10	
	Existen pólizas contra robo de equipos	Impacto	Correctivo	SI	SI	SI	SI	SI	85
			5	15	15	20	20	10	
R12. Robo de información	Existe un plataforma de seguridad perimetral en alta disponibilidad	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
	Existe un esquema de premisos implementado en el FileServer y en las aplicaciones	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
R13. Suplantación de identidad de usuarios	Se cuenta con un sistema de control de acceso biométrico para ingresar a las áreas seguras y cámaras de vigilancia	Probabilidad	Preventivo	SI	SI	SI	SI	SI	100
			20	15	15	20	20	10	
R14. Uso inadecuado de sistemas para generar fraudes	Los aplicativos críticos de la entidad tienen un esquema de autenticación integrado con el dominio y basado en roles y permisos	Probabilidad	Preventivo	SI	NO	SI	NO	NO	55
			20	15	0	20	0	0	
R15. Uso inadecuado de sistemas que generan interrupción	Se cuenta con una plataforma en alta disponibilidad	Impacto	Correctivo	SI	SI	NO	SI	NO	55
			5	15	15	0	20	0	
	Centro principal de procesamiento TIER III y Centro alterno de procesamiento TIER II	Impacto	Correctivo	SI	SI	NO	NO	SI	45
			5	15	15	0	0	10	
R16. Abuso de privilegios	El acceso al los recursos tecnológicos se controla a través del directorio activo	Probabilidad	Preventivo	SI	SI	NO	NO	NO	50
			20	15	15	0	0	0	
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	Probabilidad	Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	
	Se cuenta con un esquema de privilegios sobre el fileserver	Impacto	Correctivo	SI	SI	NO	NO	NO	35
			5	15	15	0	0	0	

5.3.2.6. DETERMINAR DESPLAZAMIENTO MAPA DE CALOR

Después de evaluar los aspectos, características o cualidades del control, se procedió a determinar el nivel de desplazamiento que puede llegar a generar el control dentro de la matriz de riesgo de acuerdo a su efectividad.

Para determinar el nivel de desplazamiento, se utilizo los siguientes criterios de valoración[66]:

Tabla 32. Valores de desplazamiento que genera el control

Valores de calificación del control	Dependiendo si el control afecta Probabilidad o Impacto	
	Niveles a disminuir en la probabilidad	Niveles a disminuir en el impacto
Entre 0 y 50 puntos	0	0
Entre 51 y 75 puntos	1	1
Entre 76 y 100 puntos	2	2

El nivel de desplazamiento que genera la efectividad del control, permite determinar el riesgo residual y por consiguiente las acciones de tratamiento de riesgos a que hubiese lugar.

La siguiente fue la valoración que se realiza para determinar el nivel de desplazamiento en el mapa de riesgos de los controles identificados:

[66] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, Pág., 35

Tabla 33. Determinación nivel de desplazamiento

RIESGO \ AMENAZA	DESCRIPCION DEL CONTROL	TOTAL PUNTAJE	DESPLAZAMIENTO MAPA DE RIESGOS										
			Inherente			Disminución				Residual			
			Probabilidad	Impacto	Nivel riesgo	Probabilidad	Total Controles	Impacto	Total Controles	Probabilidad	Impacto	Nivel Riesgo
R1. Acceso no autorizado	Se cuenta con un sistema de control de acceso biométrico para ingresar a las áreas seguras y cámaras de vigilancia	75	4	5	Riesgo Extremo	1	3	0	0	1	5	Riesgo Medio
	Existe un plataforma de seguridad perimetral en alta disponibilidad	70				1		0				
	El acceso de los usuarios al los recursos tecnológicos se controla por el directorio activo	70				1		0				
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	35				0		0				
	Se cuenta con un esquema de privilegios sobre el fileserver	35				0		0				
R2. Ataques externos / internos (hacking no ético)	Existe un plataforma de seguridad perimetral en alta disponibilidad	90	4	4	Riesgo Extremo	2	2	0	0	2	4	Riesgo Medio
R3. Cambio de privilegios sin autorización	Se cuenta con un procedimiento formal de control de cambios	60	4	3	Riesgo Alto	1	1	0	0	3	3	Riesgo Medio
R4. Desastres naturales (Terremotos, Incendios, Inundaciones, etc.)	Centro principal de procesamiento con nivel de TIER III y Centro alterno de procesamiento con nivel de TIER II	45	1	4	Riesgo Bajo	0	0	0	1	1	3	Riesgo Bajo
	Simulacros de evacuación	60				0		1				
R5. Divulgación de información de autenticación	Se tiene implementada la política de contraseña segura	75	3	3	Riesgo Medio	1	1	0	0	2	3	Riesgo Medio
R6. Error del administrador	Se cuenta con un procedimiento formal de control de cambios	60	4	3	Riesgo Alto	1	1	0	0	3	3	Riesgo Medio
R7. Instalación de software no autorizado	Se tiene implementada la política para restringir la instalación de software por parte de los usuarios	75	3	2	Riesgo Medio	1	1	0	0	2	2	Riesgo Bajo
R8. Interceptación no autorizada de información en tránsito	Los canales de comunicaciones con las regionales utilizan protocolos de encripción para la transmisión de datos.	70	4	4	Riesgo Extremo	1	1	0	0	3	4	Riesgo Alto
R9. Interrupción en los servicios	Se cuenta con una plataforma en alta disponibilidad	55	3	3	Riesgo Medio	0	1	1	1	2	2	Riesgo Bajo
	Se cuenta con un procedimiento formal de control de	60				1		0				

	cambios													
	Centro principal de procesamiento con nivel de TIER III y Centro alterno de procesamiento con nivel de TIER II	45				0		0						
R10. Modificación sin autorización	El acceso de los usuarios al los recursos tecnológicos se controla a través del directorio activo	70	3	3	Riesgo Medio	1	2	0	0	1	3	Riesgo Bajo		
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	35				0		0						
	Se cuenta con un esquema de privilegios sobre el fileserver	55				1		0						
R11. Robo de equipos	Se cuenta con un sistema de control de acceso biométrico para ingresar a las áreas seguras y cámaras de vigilancia	100	3	3	Riesgo Medio	2	4	0	2	1	1	Riesgo Inusual		
	Existe guardias de seguridad que revisan a los equipos que entran y salen de la entidad	80				2		0						
	Existen pólizas contra robo de equipos	85				0		2						
R12. Robo de información	Existe un plataforma de seguridad perimetral en alta disponibilidad	70	3	4	Riesgo Alto	1	2	0	0	1	4	Riesgo Bajo		
	Existe un esquema de premisos implementado en el FileServer y en las aplicaciones	70				1		0						
R13. Suplantación de identidad de usuarios	Se cuenta con un sistema de control de acceso biométrico para ingresar a las áreas seguras y cámaras de vigilancia	100	2	3	Riesgo Medio	2	2	0	0	1	3	Riesgo Bajo		
R14. Uso inadecuado de sistemas para generar fraudes	Los aplicativos críticos de la entidad tienen un esquema de autenticación integrado con el dominio y basado en roles y permisos	55	2	4	Riesgo Medio	1	1	0	0	1	4	Riesgo Bajo		
R15. Uso inadecuado de sistemas que generan interrupción	Se cuenta con una plataforma en alta disponibilidad	55	2	4	Riesgo Medio	0	0	1	1	2	3	Riesgo Medio		
	Centro principal de procesamiento con nivel de TIER III y Centro alterno de procesamiento con nivel de TIER II	45				0		0						
R16. Abuso de privilegios	El acceso al los recursos tecnológicos se controla a través del directorio activo	50	4	4	Riesgo Extremo	0	1	0	0	3	4	Riesgo Alto		
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	60				1		0						
	Se cuenta con un esquema de privilegios sobre el fileserver	35				0		0						

5.3.2.7. DETERMINACION RIESGO RESIDUAL

Una vez determinado el nivel de desplazamiento que genero el control por disminución de la probabilidad o del impacto, se procedió a elaborar la matriz de riesgos residual, para lo cual, se ubico el riesgos residual dentro del mapa de riesgos teniendo en cuenta el nuevo valor de su probabilidad y de su impacto.

El desplazamiento que se genero dentro de la matriz de riesgos determino la opción de tratamiento para el riesgo.

La siguiente es la distribución de riesgo residual asociados a los activos de la dirección de tecnología:

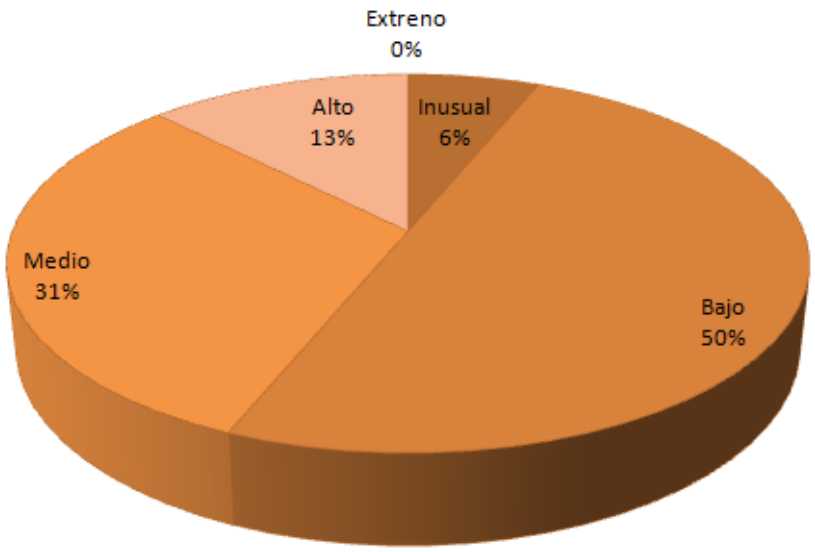


Figura 15. Distribución del riesgo residual activos Dirección de Tecnología
Fuente: El autor

5.3.2.8. MAPA DE RIESGO RESIDUAL

Los siguientes son los mapas de riesgo residual una vez valorada la efectividad de los controles identificados:

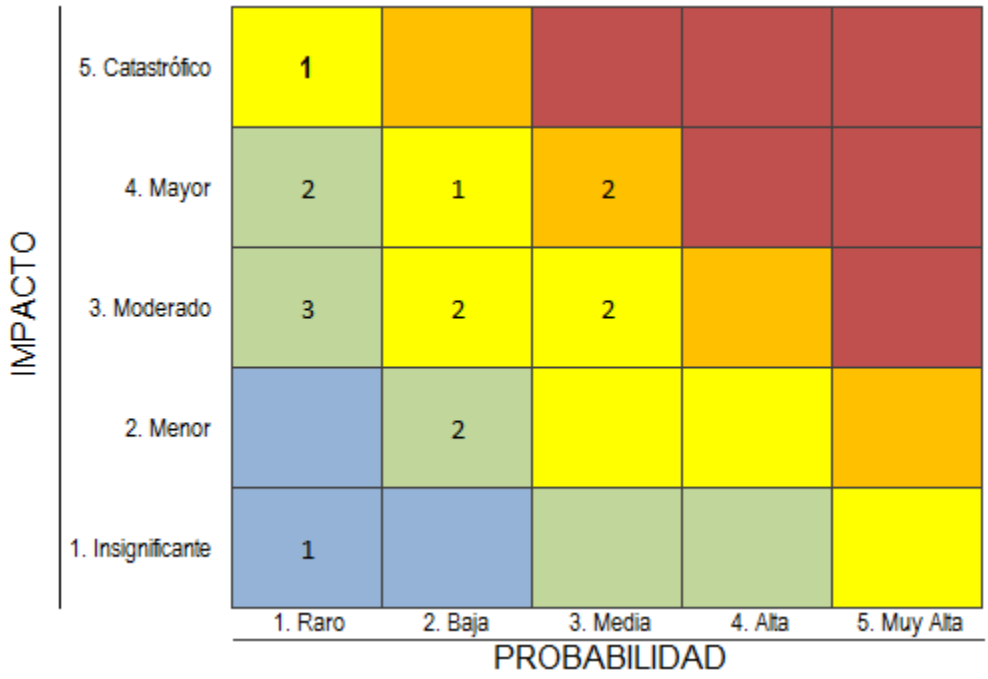


Figura 16. Mapa Riesgo residual general proceso de tecnología

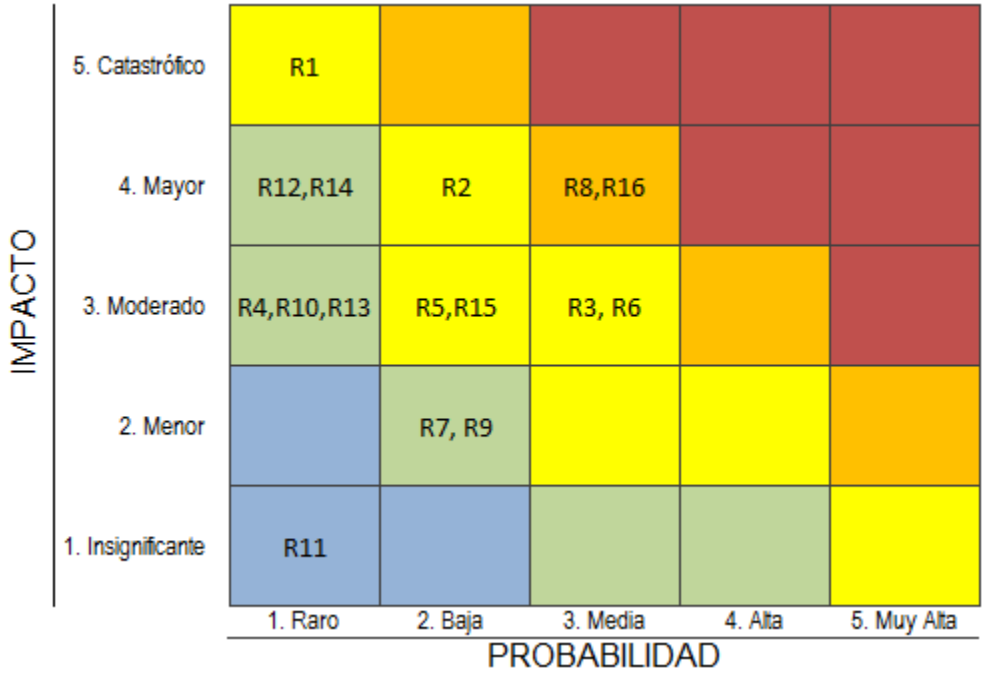


Figura 17. Mapa Riesgo residual detallado proceso de tecnología

5.3.2.9. COMPARATIVA MAPAS DE CALOR

Los siguientes son los comparativos entre el mapa de riesgo inherente y el riesgo residual:

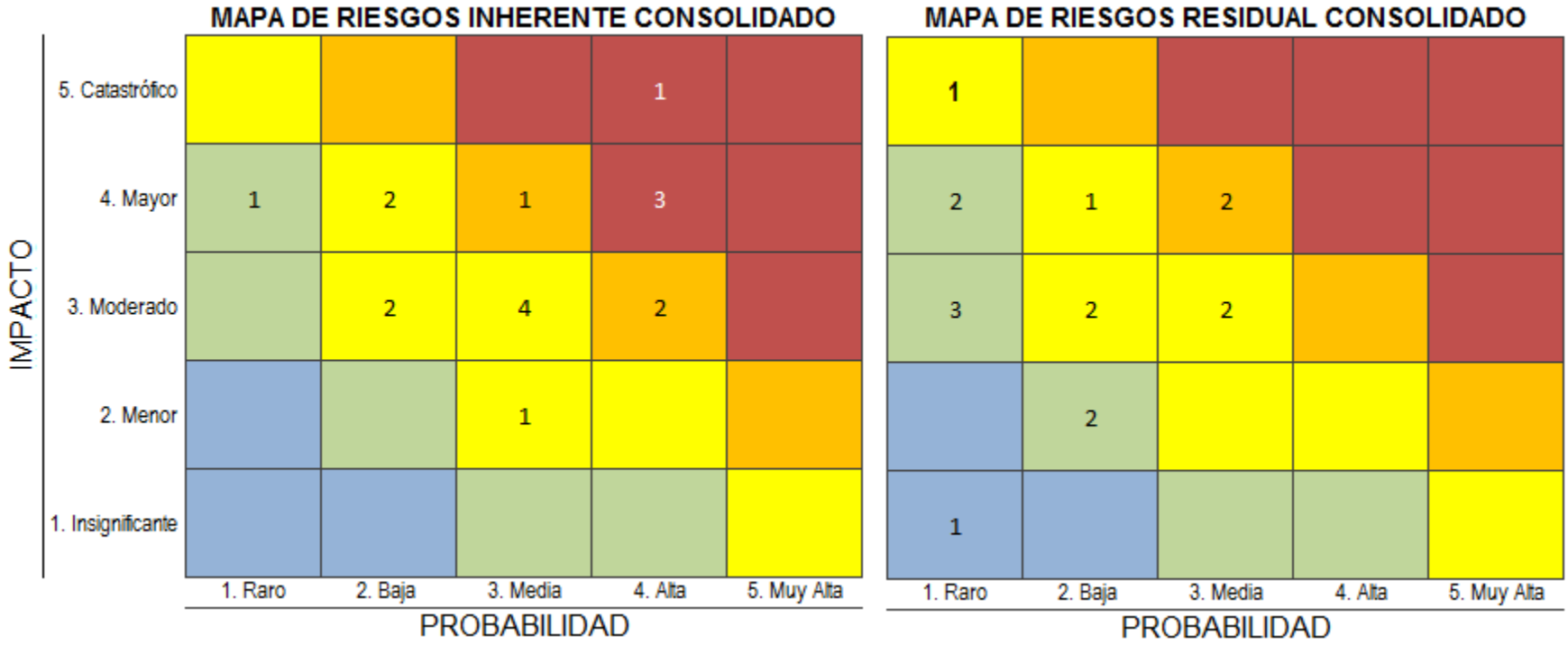


Figura 18. Comparativo Mapas de Calor Consolidadas

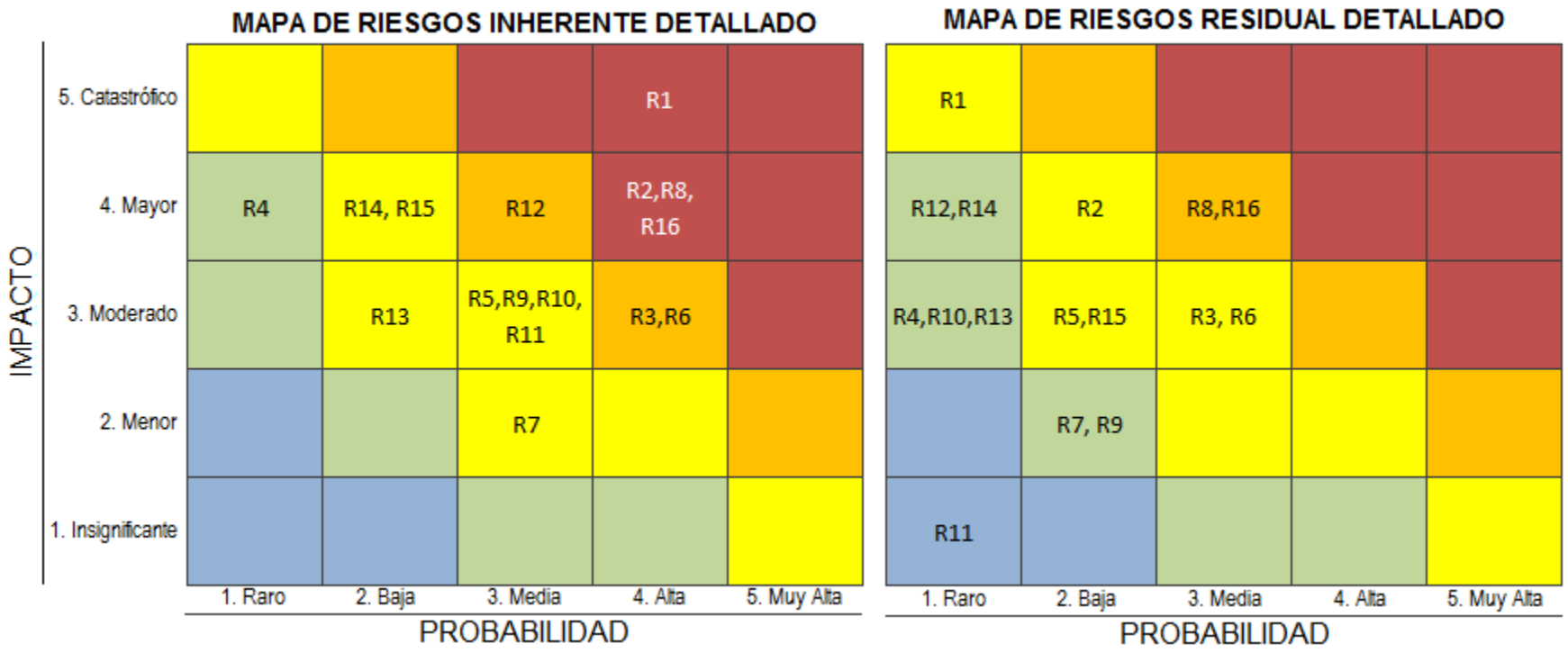


Figura 19. Comparativo Mapas de Calor Detalladas

5.3.3. PLANES DE TRATAMIENTO DE RIESGO

Con el objetivo de gestionar el riesgo residual se establecieron los planes de tratamiento orientados a preservar las características de confidencialidad, integridad y disponibilidad de los activos de información de tecnología seleccionados para la respectiva valoración de riesgos. Para determinar la opción para el tratamiento del riesgo, se utilizo como base el siguiente mapa de calor que especifica para cada una de las posiciones de la matriz de 5x5 la acción a seguir:

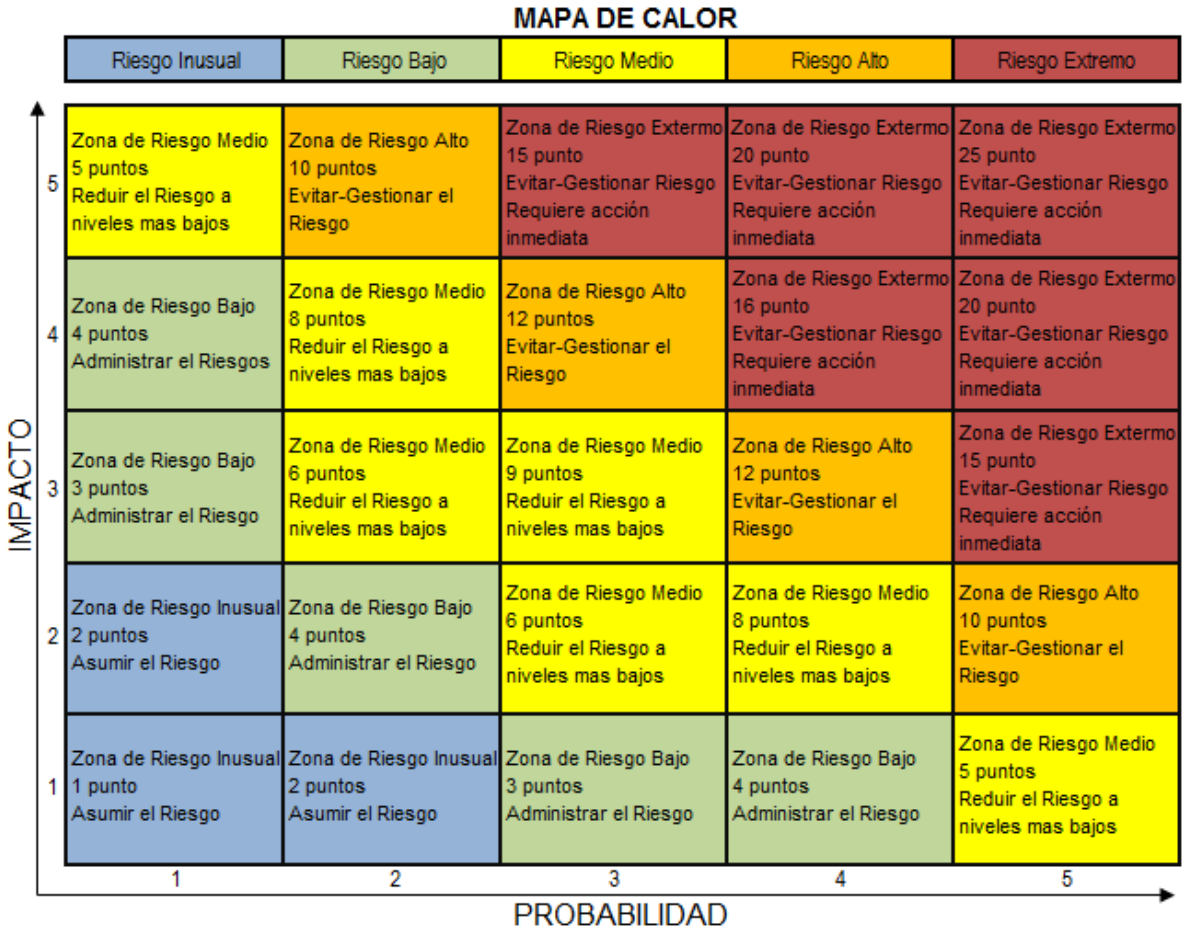


Figura 20. Mapa de calor opción tratamiento de riesgo
Fuente: La entidad

Dependiendo del desplazamiento o no que generaron los controles valorados, se definieron planes de tratamiento relacionadas para evitar, disminuir o mitigar el riesgo residual de acuerdo a los siguientes criterios:

Tabla 34. Criterios para tratamiento de riesgos

Opción	Acción de seguir
Evitar	Establecer las medidas orientadas a prevenir su materialización.
Reducir	Establecer medidas encaminadas a disminuir tanto la probabilidad mediante medidas de prevención, como el impacto mediante medidas de protección.
Transferir	Si es posible, reducir su efecto a través del traspaso del riesgo a otras organizaciones (ej. Seguros, tercerización de servicios).
Asumir	Si al mitigar el riesgo este queda como un riesgo residual, se puede aceptar el riesgo sin necesidad de tomar otras medidas de control.

Las siguientes son las opciones que se establecieron para el tratamiento de los riesgos residuales de acuerdo a su a posición en la matriz de 5x5:

Tabla 35. Opciones tratamiento riesgo residual del proceso de tecnología

Riesgos	Riesgo	Opción de tratamiento
R1. Acceso no autorizado	Riesgo Medio	Disminuir el riesgo
R2. Ataques externos / internos (hacking no ético)	Riesgo Medio	Disminuir el riesgo
R3. Cambio de privilegios sin autorización	Riesgo Medio	Disminuir el riesgo
R4. Desastres naturales	Riesgo Bajo	Reducir el riesgo
R5. Divulgación de información de autenticación	Riesgo Medio	Disminuir el riesgo
R6. Error del administrador	Riesgo Medio	Disminuir el riesgo
R7. Instalación de software no autorizado	Riesgo Bajo	Reducir el riesgo
R8. Interceptación no autorizada de información en tránsito	Riesgo Alto	Prevenir el riesgo.
R9. Interrupción en los servicios	Riesgo Bajo	Reducir el riesgo
R10. Modificación sin autorización	Riesgo Bajo	Reducir el riesgo
R11. Robo de equipos	Riesgo Inusual	Aceptar el riesgo
R12. Robo de información	Riesgo Bajo	Reducir el riesgo
R13. Suplantación de identidad de usuarios	Riesgo Bajo	Reducir el riesgo
R14. Uso inadecuado de sistemas para generar fraudes	Riesgo Bajo	Reducir el riesgo
R15. Uso inadecuado de sistemas que generan interrupción	Riesgo Medio	Disminuir el riesgo
R16. Abuso de privilegios	Riesgo Alto	Prevenir el riesgo.

Los siguientes son los planes de tratamiento que se definieron para evitar, disminuir o mitigar los riesgos residuales del proceso de tecnología:

Tabla 36. Plan de tratamiento de riesgos residuales proceso de Tecnología

Riesgos	Activos afectados	Riesgo Residual	Plan de Tratamiento	Afecta			Descripción plan de acción	Responsable
				D	I	C		
R1. Acceso no autorizado	Area administración de plataforma, Bases de datos, Cuartos de Rack Data Center del proveedor, Directorio Activo, Equipos de seguridad perimetral, Servidores de Administración, Servidores de bases de datos de producción, Servidores de aplicaciones de producción, Plataforma de Correo	**Riesgo Medio**	Disminuir el riesgo		I	C	Realizar periódicamente pruebas de Hacking Ético para establecer el nivel de protección de la infraestructura de TI, sobre todo, los servicios publicados hacia la web	Oficial de Seguridad
							Adquirir una solución para el monitoreo de Logs y correlación de eventos	Dirección de Tecnología
							Monitorear periódica los Logs de eventos de seguridad y las bitácoras de entrada a las áreas de la entidad.	Oficial de Seguridad
							Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Oficial de Seguridad
							Realizar permanentemente campañas de seguridad	Oficial de Seguridad
R2. Ataques externos / internos (hacking no ético)	Bases de datos, Equipos de seguridad perimetral, Servidores de producción (Administración, bases de datos, aplicaciones), Plataforma de Correo, Data Center	**Riesgo Medio**	Disminuir el riesgo	D	I	C	Realizar periódicamente prueba de Hacking Ético con el objetivo de establecer el nivel de protección de la infraestructura de TI, sobre todo, los servicios de la entidad publicados hacia la web	Oficial de Seguridad
R3. Cambio de privilegios sin autorización	Bases de Datos, Directorio Activo, Servidores de producción (Administración, bases de datos, aplicaciones), Plataforma de Correo	**Riesgo Medio**	Disminuir el riesgo	D	I		Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Oficial de Seguridad
							Garantizar que este implementada la política de contraseña segura	Oficial de Seguridad Dirección de Tecnología
R4. Desastres naturales	Data Center del proveedor	**Riesgo Bajo**	Reducir el riesgo	D			Garantizar la debida ejecución de las pruebas de continuidad	Coordinador plan de continuidad
R5. Divulgación de información de autenticación	Bases de Datos, Directorio Activo Servidores de Administración	**Riesgo Medio**	Disminuir el riesgo			C	Garantizar que este implementada las políticas de contraseña segura y bloqueo automático de pantallas.	Dirección de seguridad
							Realizar permanentemente campañas de seguridad	Oficina de Informática
R6. Error del administrador	Bases de datos, Data Center, Directorio Activo, Red LAN, Red WAN, Servidores de producción (Administración, bases de datos, aplicaciones), Plataforma de Correo, Equipos de seguridad perimetral	**Riesgo Medio**	Disminuir el riesgo	D	I	C	Monitorear periódica los Logs de eventos de seguridad.	Oficina de Informática
							Garantizar la debida capacitación del personal de TI	Dirección de Tecnología
							Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios	Dirección de Tecnología

Riesgos	Activos afectados	Riesgo Residual	Plan de Tratamiento	Afecta			Descripción plan de acción	Responsable
				D	I	C		
R7. Instalación de software no autorizado	Directorio Activo, Computadores, Portátiles	**Riesgo Bajo**	Reducir el riesgo		I		Garantizar que la política que restringe instalación de software por parte de las usuarios está debidamente implementada	Oficial de Seguridad Dirección de Tecnología
R8. Interceptación no autorizada de información en tránsito	Red LAN, Red WAN, Correo	**Riesgo Alto**	Evitar el riesgos Atención inmediata		I	C	Implementar un portal de intercambio seguro que garantice la integridad, confidencialidad, autenticidad y no repudio de la información que se intercambió con terceros	Dirección de Tecnología
							Implementar mecanismos que garanticen el cifrado de la información que se intercambia con terceros a través del correo electrónico	Dirección de Tecnología
R9. Interrupción en los servicios	Bases de datos, Data Center del proveedor, Directorio Activo, Red LAN, Red WAN, Servidores de Producción	**Riesgo Bajo**	Reducir el riesgo	D			Monitorear periódica los Logs de eventos de seguridad.	Dirección de Tecnología
							Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios	Dirección de Tecnología
							Garantizar que todos los contratos con los proveedores de TI tengan Acuerdos de niveles de servicio	Dirección de Tecnología
							Garantizar la debida ejecución de las pruebas de contingencia de TI	Coordinador plan de continuidad
R10. Modificación sin autorización	Bases de datos, Directorio Activo, Servidores de Administración, Servidores de bases de datos de producción, Servidores de aplicaciones de producción, Plataforma de Correo	**Riesgo Bajo**	Medidas preventivas para reducir el riesgo		I		Monitorear periódica los Logs de eventos de seguridad.	Oficial de Seguridad
							Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios	Dirección de Tecnología
							Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema	Oficial de Seguridad
R11. Robo de equipos	Área administración de plataforma, Cuartos de Rack, Data Center	**Riesgo Inusual**	Aceptar el riesgo			C		
R12. Robo de información	Bases de datos, Directorio Activo, Servidores de Administración, Servidores de bases de datos de producción, Plataforma de Correo	**Riesgo Bajo**	Medidas preventivas para reducir el riesgo			C	Monitorear periódica los Logs de eventos de seguridad.	Oficial de Seguridad
							Revisar periódicamente el estado de los usuarios, roles y permisos los sistemas.	Oficial de Seguridad
							Implementar mecanismo de cifrado de disco duro de los dispositivos móviles y portátiles de la entidad	Dirección de Tecnología
							Garantizar la implementación del bloqueo de dispositivos externos en los computadores de la entidad	Dirección de Tecnología
							Clasificar la información de la entidad, de acuerdo a si es pública, privada o confidencial	Oficial de Seguridad Dueños de proceso

Riesgos	Activos afectados	Riesgo Residual	Plan de Tratamiento	Afecta			Descripción plan de acción	Responsable
				D	I	C		
R13. Suplantación de identidad de usuarios	Directorio Activo, Servicio de Correo	**Riesgo Bajo**	Medidas preventivas para reducir el riesgo		I	C	Monitorear periódica los Logs de eventos de seguridad.	Oficial de Seguridad
							Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Oficial de Seguridad
							Revisar periódicamente la efectividad de la solución de anti spam	Oficial de Seguridad Dirección de Tecnología
							Garantizar que este implementada las políticas de contraseña segura y bloqueo automático de pantallas.	Oficial de Seguridad Dirección de Tecnología
							Realizar permanentemente campañas de seguridad	Oficial de Seguridad
R14. Uso inadecuado de sistemas para generar fraudes	Bases de datos, Directorio Activo, Servidores de Administración, Servidores de bases de datos de producción, Servidores de aplicaciones de producción, Plataforma de Correo	**Riesgo Bajo**	Medidas preventivas para reducir el riesgo		I	C	Monitorear periódica los Logs de eventos de seguridad.	Oficial de Seguridad
							Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Dirección de Tecnología
							Garantizar la debida segregación de funciones	Oficial de Seguridad Dirección de Tecnología
R15. Uso inadecuado de sistemas que generan interrupción	Bases de datos, Data Center del proveedor, Directorio Activo, Red LAN, Red WAN, Servidores de Administración, Servidores de bases de datos de producción, Servidores de aplicaciones de producción, Plataforma de Correo	**Riesgo Medio**	Medidas prontas y adecuadas para disminuir el riesgo	D			Monitorear de manera periódica los Logs de eventos de seguridad.	Oficial de Seguridad
							Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Dirección de Tecnología
R16. Abuso de privilegios	Data Center del proveedor, Directorio Activo, Servidores de Administración, Servidores de bases de datos de producción, Servidores de aplicaciones de producción, Plataforma de Correo	**Riesgo Alto**	Atención inmediata	D	I	C	Monitorear de manera periódica los Logs de eventos de seguridad y las actividades que realizan los administradores	Oficial de Seguridad
							Revisar periódicamente el estado de los usuarios, roles y permisos en el sistema de control de acceso, directorio activo, bases de datos y aplicaciones	Oficial de Seguridad
							Eliminar (si es posible) o bloquear las cuentas de súper administradores. En caso de bloqueo la contraseña de la misma deberá ser administrado por el oficial de seguridad	Oficial de Seguridad Dirección de Tecnología
							Garantizar que todo cambio que se realizan en producción es aprobado por el comité de cambios	Dirección de Tecnología

5.3.4. POLITICAS DE SEGURIDAD DE LA INFORMACION

Se elaboro el manual de Políticas de Seguridad de la información, que corresponde al documento que contiene las políticas, normas y lineamientos que regirán la seguridad de la información en la entidad y las responsabilidades y obligaciones de todos los colaboradores y terceros que tengan acceso a la información de la entidad.

El debido cumplimiento de las políticas de seguridad de la información por parte todos los colaboradores y de terceros que tienen relación alguna con la entidad, permite minimizar al máximo los riesgos asociados con la seguridad de la información, pero para alcanzar este propósito, es necesario que la política del sistema de gestión de seguridad de la información sea impulsada por la alta directiva de la entidad.

En el presente trabajo se definido la política del Sistema de Gestión de Seguridad de la información y política que lo soportan (ver Anexo C), las cuales demuestran que existe un compromiso expreso por para de la Alta Directiva con relación a la seguridad de la información. Adicional, a estas políticas es necesario contar con políticas relacionadas de seguridad involucren aspectos administrativos, físicos y tecnológicos orientadas a proteger los activos de información a través de los cuales se gestiona la información del negocio

Es fundamental divulgar en la entidad de forma adecuada el propósito de las políticas de seguridad de la información antes de su aplicación, con el objetivo de que los colaboradores y terceros comprendan como estas políticas ayudan a proteger la confidencialidad, integridad y disponibilidad de la información del negocio. Esta labor es esencial, para que los usuarios no vean en estas políticas como una serie de restricciones que les complicaran sus labores diarias, sino por el contrato, lo que se busca con una adecuada socialización es conseguir que los usuarios entiendan los riesgos a los cuales está expuesta la entidad y las necesidades de tener unas normas para evitarlos.

El manual de Políticas de Seguridad de la Información desarrollado se basa en los objetivos de control y controles definidos en el Anexo A de la Norma ISO/IEC 27001:2013, y para efecto del presente trabajo se documentaron las siguientes políticas de seguridad:

ANEXO A NORMA ISO 27001:2013	A.5.	Política General de Seguridad de la Información
	A.6.	Organización de Seguridad de la Información
	A.7.	Seguridad de los Recursos Humanos
	A.8.	Gestión de Activos
	A.9.	Control de Acceso
	A.10.	Criptografía
	A.11.	Seguridad Física y del Entorno
	A.12.	Seguridad de las Operaciones
	A.13.	Seguridad de las Comunicaciones
	A.14.	Adquisición, Desarrollo y Mantenimiento de Sistemas
	A.15.	Relaciones con los Proveedores
	A.16.	Gestión de Incidentes de Seguridad de la Información
	A.17.	Seguridad de la Información en la Continuidad del Negocio
	A.18.	Cumplimiento de Requisitos Legales y Contractuales

Las Políticas de Seguridad de la Información definidas en este manual, son de obligatorio cumplimiento por todos los colaboradores y terceros que laboran o presten sus servicios a la entidad.

La documentación de cada una de estas políticas, se presenta en el Anexo F de presente de trabajo de grado.

5.3.5. INCIDENTES DE SEGURIDAD

El objetivo principal de la Gestión de Incidentes de Seguridad de la información es proveer un mecanismo estructurado y planificado que permita gestionar de manera adecuada los incidentes de seguridad que puede afectar la disponibilidad, integridad, confidencialidad de la información de la entidad.

La Gestión de Incidentes de seguridad de la información debe garantizar que:

- Los eventos de seguridad de la información se detectan y tratan con eficiencia, con el propósito de identificar si los mismos se clasifican como incidentes de seguridad de la información.
- Los incidentes de seguridad de la información se gestionan de forma eficiente y adecuada.

- Se implementan las medidas de seguridad adecuadas con el objetivo de mitigar los incidentes presentados.
- La entidad aprende de las lecciones que dejan los incidentes de seguridad, con el fin de mejorar las medidas y mecanismos orientados a proteger la seguridad de la información.
- Se disponen de mecanismo que permitan cuantificar y monitorear los incidentes de seguridad de la información.

Para una adecuado gestión de incidentes se seguridad, es necesarios que todos los colaboradores y terceros que laboren o tengan relación con la entidad, identifiquen o detecten un evento de seguridad de la información que pueden afectar la Disponibilidad, Integridad y Confidencialidad de los activos de información a través de los cuales se gestiona la información de la entidad, y los reportar de manera oportuna a la áreas encargadas de analizar y determinar las medidas para contener los incidentes de seguridad.

Así mismo, le entidad debe contar con el equipo de Respuesta a Incidentes de Seguridad de la información, quien tendrá la responsabilidad de analizarlos y trataros.

5.3.5.1. FASES GESTION DE INCIDENTES DE SEGURIDAD

De acuerdo a la guía de Gestión de Incidentes de seguridad de la información del MINTIC [16], las siguientes son las actividades involucradas en el ciclo de vida de la gestión de incidentes de seguridad:

Figura 21. Ciclo de vida gestión incidentes de seguridad de la información
Fuente: http://www.mintic.gov.co/gestionti/615/articles-5482_Gestion_Incidentes.pdf

Tabla 37. Actividades Ciclo Gestión de Incidentes

Actividad	Objetivo
Preparación	Se obtienen los recursos para garantizar las fases del ciclo de vida de la gestión de incidentes de seguridad. También se determina como se van a clasificar los incidentes de seguridad y los tiempos para su atención.
Detección	Corresponde a la detección de un evento de seguridad de la información, ya sea por parte de los usuarios o del área de tecnología o del oficial de seguridad. Una vez identificado el evento, se reporta.
Análisis	Evaluación de los eventos se seguridad de la información con el propósito de determinar si se clasifica como incidente de seguridad.
Contención	Corresponde a establecer los mecanismos para evitar que el incidente siga generando daños.
Erradicación	Busca eliminar la causa del incidente y todo rastro de daños.
Recuperación	Consiste en restaurar los servicios afectados usando procedimientos de recuperación.
Actividades post incidente	Corresponde al reporte apropiado y oportuno del incidente, la generación de las lecciones aprendidas y el registro en la base de conocimiento, que son insumos para alimentar los indicadores de gestión del Sistema de Gestión de Seguridad de la Información.

5.3.5.2. CATEGORIZACION INCIDENTES DE SEGURIDAD

Los incidentes de seguridad de la información pueden ser generados por acciones humanas deliberadas o accidentales y también por medios técnicos o físicos, por lo tanto, para la clasificación de los incidentes de seguridad de la información se considerará las amenazas como factores de categorización[67].

[67] Guía Técnica Colombiana, GTS-ISO/IEC 27035:2012, Pág. 64.

Para establecer la clasificación de los incidentes de seguridad de la información de la entidad, se utilizó como marco de referencia la categorización que plantea la GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-817) [17], del Centro Criptológico Nacional de España.

Tabla 38. Categorización Incidentes de Seguridad de la Información[68]

Clase de Incidente	Incidente	Descripción
Abuso de privilegios y usos inadecuados	Abuso de privilegios o cambios de privilegios sin autorización	Acciones de intentar y/o conseguir cambiar, elevar, asignar o denegar sin la debida autorización privilegios a recursos, aplicaciones o información más allá de los que un usuario o administrador ya posee legítimamente y que de acuerdo a sus funciones y responsabilidades no deberían tener.
	Infracciones de derechos de autor o piratería	Copia o uso indebido o no autorizado de material publicado, patentado o en general protegido por derechos de propiedad intelectual.
	Violación de la Políticas Seguridad de la información.	Incidentes de seguridad generados por el incumplimiento o violación de las políticas de Seguridad de la Información establecidos en la Entidad
	Incumplimiento normativo y de ley	Incumplimiento normativo vigente en seguridad aplicable a la Entidad impartido por la jurisprudencia o por entes de control.
Acceso no autorizado	Acceso no Autorizado	Todo tipo de ingreso y operación no autorizada a los sistemas y/o a la información, sea o no exitoso. Son parte de esta categoría: • Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos. • Intentos recurrentes y no recurrentes de acceso no autorizado. • Abuso y/o Mal uso de los servicios informáticos internos o externos que requieren autenticación.
	Modificación no Autorizada	Incidentes de seguridad relacionados con la modificación, alteración o borrado de la información de manera no autorizada o los intentos recurrentes que se detecten asociados a este tipo de incidentes
	Fuga o perdida de información	Incidentes relacionados con la Fuga, robo o pérdida o copia de información confidencial o sensible de la entidad, generados por agentes internos o externos de manera deliberada.
	Robo o pérdida de equipo	Robo o pérdida de equipamiento, portátiles, cintas de copias de seguridad, equipamiento de redes, etc, que contengan información confidencial de la entidad
Código Malicioso	Detección o ataque de virus, software malicioso y/o actividad no confiable.	Se refiere a la introducción de códigos maliciosos en la infraestructura tecnológica de la Entidad. Ejemplos: Virus informáticos, Troyanos, spam, Gusanos informáticos

[68] GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-817), Pág. 9

	Propagación de contenido indeseable	La pérdida de seguridad de la información es causada por la propagación de contenido indeseable a través de redes de información, tales como: contenido ilegal, contenido que provoca pánico, contenido malicioso, contenido abusivo, etc.
Ataques	Denegación del servicio -	Incidentes que generan la interrupción prolongada en un servicio de tecnología o que un sistema, servicio o red deje de operar a su capacidad prevista.
	Modificación de sitios web (Defacement)	Vulnerabilidades explotadas con éxito en los servidores web o en las aplicaciones que estos alojan, que permiten a un atacante modificar contenidos y páginas web.
	Ingeniería social, fraude o phishing	Corresponden a la interceptación, espionaje, chuzadas de teléfonos, ingeniería social o phishing, con el objetivo de obtener información sin autorización y/o por engaño.
Pruebas y reconocimientos	Escaneos, pruebas o intentos de obtener información, redes o servidores sin autorización.	Agrupa los eventos que buscan obtener información de la infraestructura tecnológica de la Entidad a través de sniffers (software utilizado para capturar información que viaja por la red) o detección de Vulnerabilidades.
	Alarmas de sistemas de monitorización	En esta categoría se consideran aquellos eventos de seguridad (cortafuegos, sistemas de detección de intrusos, filtrado web, etc.) que puedan ser significativos pero que no permitan clasificar al incidente en alguna de las categorías establecidas.
Mal uso de los recursos tecnológicos	Mal uso de los recursos tecnológicos	Incluye los eventos que atentan contra los recursos tecnológicos por el mal uso y comprenden: - Mal uso y/o Abuso de servicios informáticos internos o externos - Violación de las normas de acceso a Internet - Mal uso y/o Abuso del correo electrónico de la Entidad - Modificación, instalación o eliminación no autorizada de software
Otro Incidente		No clasificados en ninguna de las categorías de incidentes anteriores

5.3.5.3. PROCEDIMIENTO REPORTE Y ATENCION DE INCIDENTES

El procedimiento para el reporte y atención de incidentes de seguridad de información, corresponde al Anexo G de presente de trabajo de grado.

6. RESULTADOS Y DISCUSIONES

Los resultados obtenidos de este proyecto se derivan del desarrollo de tres fases que fueron definidas para dar cumplimiento a los objetivos específicos que se establecieron con el propósito de poder alcanzar el objetivo general de proyecto.

Las fases que se plantearon para llevar a cabo el proyecto son:

- **Fase I - Diagnostico**. Actividades desarrolladas con el propósito de poder identificar el nivel de madurez inicial de la Entidad con respecto al establecimiento del Sistema de Gestión Seguridad de la información.
- **Fase II – Preparación.** Actividades que de acuerdo a la norma ISO/IEC 27001:2013, se deben desarrollar para establecer el Sistema de Gestión de Seguridad de la Información.
- **Fase III – Planificación**. Corresponde a la valoración de los riesgos de seguridad y la definición del marco normativo de políticas y lineamientos en torno a la seguridad de la información que se deberán establecer en la entidad.

Para el desarrollo de estas actividades se utilizaron diferentes métodos o instrumentos de recolección de información, como, entrevistas, cuestionarios, formularios en Excel, evaluación con base en la experiencia del autor, documentos físicos y electrónicos, documentos publicaciones en la WEB, entre otros.

Esto métodos fueron aplicados y posteriormente analizados, cuyos resultados se exponen a continuación de acuerdo a las fases de proyecto:

6.1. RESULTADOS FASE I – DIAGNOSTICO

Esta fase se planteo y desarrollo con el propósito de poder alcanzar los siguientes objetivos específicos del proyecto:

OE1. Analizar la situación actual de la entidad, con relación a la Gestión de Seguridad de la Información.
OE2. Determinar el Nivel de Madurez en el que se encuentra la entidad para su modelo de seguridad de la información.
OE3. Establecer el nivel de cumplimiento de la entidad frente a los controles establecidos en el Anexo A de la ISO 27001:2013 y definir los planes de acción orientados a cerrar las brechas de seguridad encontradas.

Los resultados de los diagnósticos que se realizaron en esta fase permitieron determinar:

- El estado actual de la seguridad de la entidad que se encuentra desarrollado en el capitulo **5.1.1 DIAGNOSTICO ESTADO ACTUAL DE LA SEGURIDAD** del presente trabajo, que permite alcanzar el objetivo especifico OE1.
- La estratificación de la entidad que se encuentra desarrollada en el capitulo **5.1.2. IDENTIFICACION ESTRATIFICACION DE LA ENTIDAD** del presente trabajo, que permite alcanzar el objetivo especifico OE2.
- El nivel de cumplimiento de la entidad con relación a los controles establecidos en el Anexo A de la norma ISO 27001:2013 que se encuentra desarrollado en el capitulo **5.1.3. NIVEL DE CUMPLIMIENTO ANEXO A - ISO 27001:2013** del presente documento, que permite alcanzar el objetivo especifico OE3.

OE1. Análisis de la situación actual de la entidad con relación a la Gestión de Seguridad de la Información.

La situación actual de la entidad con relación a la gestión de seguridad de la información, se determino de acuerdo al diagnostico realizado en el capitulo **1.1.3. DIAGNOSTICO SITUACION PROBLEMA** del presente documento, dónde se presenta un análisis detallado de las diferentes situaciones que afectan la seguridad de la entidad que permitieron establecer que el problema está asociado a un "*Inadecuado Modelo de Gestión de Seguridad de la Información*".

Para realizar este diagnostico se utilizo los siguientes métodos de recolección y evaluación de información:

- Evaluación con base en la experiencia del autor, debido a que labora en la entidad y conoce ha detalle el estado de la misma en torno a la seguridad de la información.
- Consulta de los documentos que contienen los resultados de las diferentes auditorías realizadas al proceso de tecnología, donde se evidenciaron una serie de debilidades asociados a la seguridad de la información. La información tomada de estos documentos para realizar el análisis no fue anexada al presente trabajo de grado, debido a que corresponden a información de carácter interno y de tipo confidencial de la entidad.

En términos general, las siguientes fueron las situaciones identificadas producto del diagnostico de la situación problema de la entidad:

- Falta de un adecuado Gobierno de Seguridad en la Entidad.
- La falta de concienciación, apropiación y conocimiento en temas de seguridad por parte de todos los funcionarios
- No existe una participación activa de toda la organización en la definición de controles de seguridad basados en una evaluación de riesgos
- Los funcionarios no conciben la diferencia entre seguridad informática y seguridad de la información
- No se cuentas con un sistema de información adecuado para la gestión de riesgos de seguridad.
- No existe una valoración adecuado de riesgos de seguridad.
- La política de seguridad no está alineada con los objetivos del negocio.

De acuerdo al análisis del diagnostico realizado, se determino que la situación de la entidad con relación a la gestión de seguridad de la información, corresponde a un "*Inadecuado Modelo de Gestión de Seguridad de la Información"*.

Este diagnostico permitido determinar la situación actual de la entidad con relación a la gestión de seguridad, lo cual permite alcanzar el objetivo específico OE1.

OE2. Determinación del Nivel de Madurez en el que se encuentra la entidad para su modelo de seguridad de la información.

Para determinar el nivel de madurez de la entidad frente a un modelo de seguridad de la información, se tomó como referencia el método para determinar el nivel de estratificación de las entidades que plantea el modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0[69], el cual, permite determinar la complejidad que le puede significar a la entidad la implementación de su Sistema de Gestión de Seguridad de la Información.

Para determinar el nivel de estratificación de la entidad se utilizó el formato relacionado en el Anexo A del presente trabajo de grado, el cual fue enviado a la Dirección de Tecnología para su respectivo diligenciamiento, debido a que la mayoría de las preguntas de este formato están orientadas a evaluar aspectos

[69] Anexo 3: Estratificación de Entidades - Modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0, Pág. 8.

relacionados con, la infraestructura asociada al número total de computadores, los servicios ofrecidos en línea por la entidad y el tamaño y capacidad del área de sistemas. Para la respuesta a la primera pregunta del formulario, que está relacionado con el presupuesto de funcionamiento de la entidad, se acudió al área de contabilidad de la entidad.

Durante este proceso de recolección de información no se presento ningún inconveniente debido a la colaboración oportuna de las áreas consultadas.

Los siguientes son los resultados obtenidos y los análisis que se realizaron de acuerdo a la información suministrada por la entidad para poder determinar su nivel de estratificación:

- Con base en la sumatoria del puntaje asignado para cada uno de las respuestas seleccionados, el puntaje total obtenido por la entidad fue de **22 puntos,** lo que significa que la entidad se encuentra clasificada en un nivel **MEDIO SUPERIOR** de estratificación, lo cual, significaría inicialmente un esfuerzo considerable por parte de la entidad para el establecimiento y implementación de su Sistema de Gestión de Seguridad de la Información.
- El presupuesto de la entidad para el año 2014 fue aproximadamente de $146.362.311.000, lo que supondría que la entidad pude asegurar la disponibilidad de los recursos necesarios para el Sistema de Gestión de Seguridad de la Información de acuerdo a lo establecido en el numeral c) del capítulo 5.1 ´Liderazgo y Compromiso' de la norma ISO/IEC 27001:2013[70].
- El número de computadores y servidores que posee la entidad, implica un mayor esfuerzo para garantizar la seguridad de estos activos de información, por lo tanto, es esencial valorar los riesgos de estos activos de información con el objetivo de determinar su nivel de protección y por consiguiente establecer las medidas de seguridad para salvaguardarlos.
- El número de empleados de la aérea de tecnología, refleja el tamaño de la entidad y los recursos que implica atender los requerimientos de los usuarios y la prestación de los servicios de tecnología, los cuales, pueden no ser suficientes en el momento que se requieran implementar las medidas y controles que se establezcan productos de los diagnósticos y valoración de riesgos de seguridad que se realicen. Este es un factor que puede implicar un

[70] Norma ISO/IEC 27001:2013, Pág. 2

mayor esfuerzo para la implementación del Sistema de Gestión de Seguridad de la Información en la entidad.

- El área de tecnología de la entidad, además de administrar y proveer los recursos tecnológicos, planea y desarrolla proyectos, factor fundamente en caso de requerir la implementación planes de acción y/o medidas de seguridad que impliquen el establecimiento de un proyecto para su ejecución.

Este diagnostico permitido determinar el Nivel de Madurez en el que se encuentra la entidad frente a un modelo de seguridad de la información, lo cual permite alcanzar el objetivo específico OE2.

OE3. Establecer el nivel de cumplimiento de la entidad frente al Anexo A de la ISO 27001:2013 y definir los planes de acción para cerrar brechas.

Para realizar este diagnóstico se utilizó una lista de chequeo (ver Anexo B) basada en un conjunto de preguntas con opción de respuesta 'SI' o 'NO', que fueron respondidas por funcionarios de las áreas de la entidad de acuerdo al objetivo de control que se estaba evaluando.

Las preguntas de esta lista de chequeo que se relaciona en el Anexo B del presente trabajo de grado, se diseñaron teniendo en cuenta los requerimientos que establece el Anexo A de la norma ISO/IEC 27001:2013 para el cumplimiento de cada uno los 113 controles que están agrupados 14 dominios de control.

La siguiente tabla contiene el valor que se asigno a cada respuesta dependiendo de la opción seleccionada:

Respuesta	Valor
SI	1
NO	0

Para determinar el nivel del cumplimiento del control se pondero el valor asignado a las respuestas asociadas a él, resultado que se pondero con el valor obtenido por los otros controles agrupados al determinado objetivo de control, para así poder determinar el nivel de cumplimiento de los dominios de control y por ende el de la entidad.

Para realizar este diagnostico se conto con la colaboración de la Vicepresidencia de Riesgos, la Dirección de Gestión Humana, la Jefatura de Recursos Físicos y la Dirección de Tecnología y Dirección Jurídica, ya que los controles del Anexo A de la norma ISO/IEC 27001:2013 prácticamente están orientados a proteger la seguridad de las personas, de la infraestructura física y lógica, de los recursos tecnológicos y por ende de la información, y garantizar el cumplimiento de la normatividad vigente relacionado con seguridad de la información.

El diligenciamiento del Anexo B del presente trabajo que corresponde a una hoja de Excel, fue dispendioso debido a la cantidad de controles que propone el Anexo A de la norma ISO/IEC 27001:2013 y a la disponibilidad de tiempo por parte de algunos funcionarios asignados para responder cada las preguntas que se establecieron para medir el nivel de cumplimiento de dichos controles.

Con base en las respuestas dadas por los usuarios, el siguiente es el resultado del nivel de cumplimiento de la entidad de los dominios y objetivos de control que establece el Anexo A de la norma ISO/IEC 27001:2013:

Tabla 39. Cumplimiento Dominios y Objetivos de Control ISO 27001

OBJETIVO DE CONTROL	SI
A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION	33.33%
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información	33%
A.6 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACION	24.17%
A.6.1 Organización Interna	48.33%
A.6.2 Dispositivos móviles y teletrabajo	0.00%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	47.04%
A.7.1 Antes de asumir el empleo	100.00%
A.7.2 Durante la ejecución del empleo	41.11%
A.7.3 Terminación y cambio de empleo	0.00%
A.8 GESTION DE ACTIVOS	43.06%
A.8.1 Responsabilidad por los activos	62.50%
A.8.2 Clasificación de la información	66.67%
A.8.3 Manejo de Medios	0.00%
A.9 CONTROL DE ACCESO	61.15%
A.9.1 Requisitos de negocio para control de acceso.	69.05%
A.9.2 Gestión de acceso de usuarios	38.89%
A.9.3 Responsabilidad de los usuarios	50.00%

A.9.4 Control de acceso a sistemas y aplicaciones	86.67%
A.10 CRIPTOGRAFIA	0.00%
A.10.1 Controles Criptográficos	0.00%
A.11 SEGURIDAD FISICA Y DEL ENTORNO	76.39%
A.11.1 Áreas seguras	66.67%
A.11.2 Equipos	86.11%
A.12 SEGURIDAD DE LAS OPERACIONES	91.67%
A.12.1 Procedimientos Operacionales y responsabilidades	62.50%
A.12.2 Protección contra códigos maliciosos	100.00%
A.12.3 Copias de respaldo	100.00%
A.12.4 Registro y seguimiento	79.17%
A.12.5 Control de software operacional	100.00%
A.12.6 Gestión de la vulnerabilidad técnica	100.00%
A.12.7 Consideraciones sobre auditorias de sistemas de información	100.00%
A.13 SEGURIDAD DE LAS COMUNICACIONES	74.58%
A.13.1 Gestión de la seguridad de las redes	66.67%
A.13.2 Transferencia de información	82.50%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA	37.04%
A.14.1 Requisitos de seguridad de los sistemas de información	66.67%
A.14.2 Seguridad en los procesos de desarrollo y de soporte	44.44%
A.14.3 Datos de prueba	0.00%
A.15 RELACIONES CON LOS PROVEEDORES	54.17%
A.15.1 Seguridad de la información en las relaciones con los proveedores	33.33%
A.15.2 Gestión de la prestación de servicios de proveedores	75.00%
A.16 GESTIÓN INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	14.29%
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información	14.29%
A.17 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	58.33%
A.17.1 Continuidad de seguridad de la información	16.67%
A.17.2 Redundancias	100.00%
A.18 CUMPLIMIENTO	30.00%
A.18.1 Cumplimiento de requisitos legales y contractuales	60.00%
A.18.2 Revisiones de seguridad de la información	0.00%

Con base en esta información, la siguiente es la distribución del nivel de cumplimiento de la entidad con relación de los 14 dominios de control que plantea el Anexo A de ISO 27001:2013:

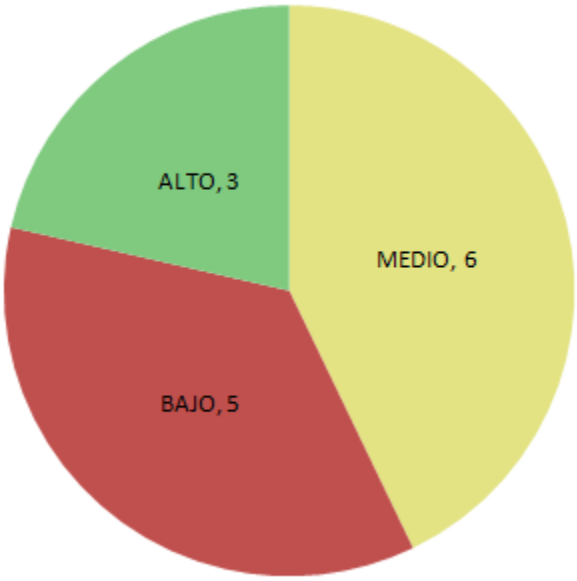


Figura 22. Nivel cumplimiento dominios de control Anexo A ISO 27001:2013
Fuente: El autor

- **Nivel Bajo** (menor o igual al 33%): corresponden a 5 dominios de control cuyo complimiento por parte de la entidad es menor al 33%, lo cual representa un riesgo ALTO para la entidad, debido a la ausencia o inadecuada implementación de los controles que generan un nivel de bajo protección de sus activos de información y/o en algunos casos, el incumplimiento de la normatividad vigente relacionado con seguridad de la información.
- **Nivel Medio** (mayor a 33% y menor 70%), corresponden a 6 dominios de control cuyo cumplimiento por parte de la entidad implica un riesgo MEDIO, debido a que algunos de los controles no están debidamente implementados, documentados o formalizados, o presentan algún tipo de debilidad que pueden ser aprovechadas por amenazas internas o externas para atentar contra la seguridad de la información de la Entidad.
- **Nivel Alto** (mayor al 70%), corresponde a 3 dominios de control que se encuentran en un nivel de implementación ALTO, lo que representa un riesgo BAJO para la entidad debido a que los controles implementados son efectivos y por lo tanto garantizan la debida protección de sus activos de información.

El siguiente es el nivel de cumplimiento de la entidad con relación al Anexo A de la norma ISO/IEC 27001:2013:

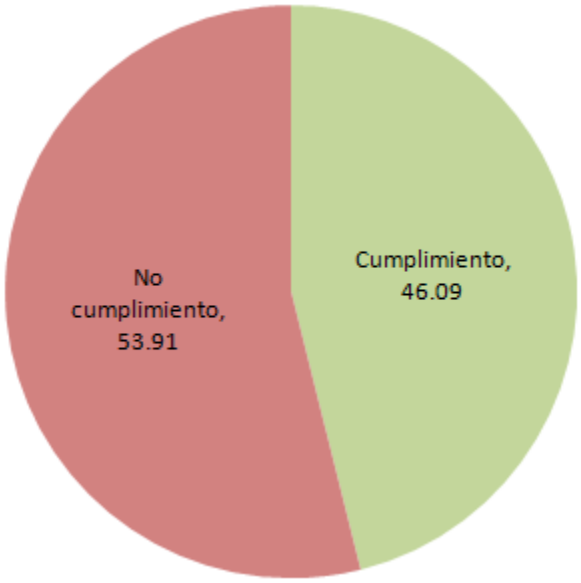


Figura 23. Nivel cumplimiento entidad frente al Anexo A ISO 27001

Con base en los resultados obtenidos producto de la valoración de las respuestas dadas por los usuarios, se pudo establecer que el nivel de cumplimiento de la entidad con relación al Anexo A de la norma ISO/IEC 27001:2013, es del **46.09%**, que equivale a un grado **MEDIO** de implementación de los controles, lo cual implicará un esfuerzo considerable en la fase de implementación del SGSI debido a la ausencia de controles o al bajo grado de cumplimiento de algunos de ellos.

El análisis realizado en el capitulo '5.1.3. NIVEL DE CUMPLIMIENTO ANEXO A - ISO 27001:2013' del presente trabajo de grado, permitió definir una serie de planes de acción orientados a cerrar las brechas encontradas con el objetivo de subir el nivel de cumplimiento de los controles. Estos planes de acción se muestran a continuación de forma ordenada, de menor a mayor nivel de cumplimiento de los respectivos objetivos de control:

Tabla 40. Planes de acción niveles cumplimiento controles Anexo A ISO 27001:2013

OBJETIVO DE CONTROL	% CUMPLE	CAUSA	PLAN DE ACCION	
A.10 CRIPTOGRAFIA	0%	No existen mecanismos para cifrar la información que se intercambio al interior de la entidad o con terceros.	PA1	Implementar cuanto antes los debidos mecanismos de cifrado con el objetivo de asegurar la confidencialidad, autenticidad e integridad de la información, tales como: cifrado de correos, portal de intercambio seguro y cifrado del almacenamiento de dispositivos movibles.
A.16 GESTIÓN INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	14%	La entidad no cuenta con un proceso para de gestión de incidentes de seguridad de la información.	PA2	Establecer cuenta antes el proceso de gestión de incidentes de seguridad para contar un enfoque coherente y eficaz para la debida gestión de los incidentes de seguridad y proveer a la entidad de un mecanismo para el reporte, evaluación y respuesta a los incidentes de seguridad de la información
		Los encargados de la seguridad de la información no mantienen un contacto con grupos de interés especializados en seguridad de la información	PA3	Los encargado de la seguridad de la información deben participar en eventos, foros, asociaciones y otros organizamos relacionados con seguridad de la información, para conocer las tendencias del mercado y las nuevas amenazas que surgen y que atentan contra la seguridad de la información
A.6 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACION	24%	La entidad no tiene definidos todos los roles y responsabilidades de la seguridad de la información.	PA4	Este es un entregable del proyecto. Se requiere que el respectivo documento sea aprobado por la Alta Dirección.
A.18 CUMPLIMIENTO	30%	No cumple el control A.18.1.5 Reglamentación de controles criptográficos		Implementar mecanismo de cifrado. (Asociado al PA1)
A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION	33%	Las políticas relacionadas con seguridad de la información están definidas en el Manual de Políticas de Seguridad Informática del proceso de tecnología, manual no está aprobado ni es revisado por la Alta Dirección	PA5	Elaborar unas políticas de seguridad aprobadas por la Alta Dirección para garantizar su debida implementación, actualización y cumplimiento.

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA	37%	No se incluyen los requisitos relacionados con seguridad de la información en las ciclo de vida de desarrollo. (control A.14.1.1 del Anexo A de la norma ISO/IEC 27001:2013)	PA6	Es indispensable implementar controles adecuados y efectivos, o fortalecer los existentes, con el objetivo de asegurar que la seguridad de la información sea parte del ciclo de vida del desarrollo de aplicaciones de la entidad y con ello garantizar que los cambios que se realizan en producción no afecten la seguridad de la información, para lo cual, se debe crear un documento que contengan las mejorar practicas para el desarrollo de software seguro.
		No siempre se realizan las verificaciones técnicas a las aplicaciones críticas del negocio cuando se realizan cambios en producción, situación que no garantiza la normal operación, disponibilidad y seguridad de los servicios de TI una vez realizado los cambios.		
		No existe con un procedimiento adecuado de control de versionamiento del software		
		Durante el desarrollo de las aplicaciones no se incluyen pruebas de seguridad		
A.8 GESTION DE ACTIVOS	43%	La entidad no tiene identificados todos los activos de información a través de los cuales se gestiona la información del negocio	PA7	En el proyecto se identifico los activos de información de acuerdo al alcance de SGSI.
		La entidad no tiene establecidos los lineamientos para el uso aceptable de los activos de información asociados con la información e instalaciones de procesamiento de información		Se requiere definir la respectiva política (Asociada al PA5)
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	47%	No se cuenta con un mecanismo que permite garantizar que los colaboradores o terceras, estén debidamente informados sobre las funciones y las responsabilidades respecto a la seguridad de la información	PA8	La Vicepresidencia de Riesgo debe capacitar a los colaboradores de la entidad para que conozcan las Políticas de Seguridad de la Información y las adopten en sus actividades diarias.
		La entidad no cuenta con un plan anual de capacitación y formación en seguridad de la información para sus empleados, lo que genera en algunos casos la poca efectividad de los		El área de gestiona humana realizar un plan de capacitación en temas de seguridad de la información. (Asociado al PA8)

		controles implementados.		
A.17 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	58%	Dentro del plan de continuidad del negocio de la entidad no se tiene contemplados los requisitos para garantizar la seguridad de la información	PA9	Documentar, implementar y mantener los procedimientos y controles necesarios para asegurar el nivel de continuidad requerido con el objetivo de garantizar la seguridad de la información en situaciones adversas.
A.9 CONTROL DE ACCESO	61%	La identificación del equipo no hace parte del esquema de autenticación de los usuarios al directorio activo.	PA10	La Dirección de Tecnológica deberá verificar la viabilidad de implementar este control
		La entidad no cuenta con un procedimiento formal para la asignación, control y restricción de derechos de acceso y privilegios sobre sus recursos tecnológicos y aplicaciones.	PA11	La Dirección de Tecnología deberá crear el respectivo procedimiento
		No se cuenta con un procedimiento para la gestión de contraseñas en los sistemas base de la entidad.	PA12	La Dirección de Tecnología deberá crear el respectivo procedimiento
A.13 SEGURIDAD DE LAS COMUNICACIONES	75%	No se cuenta con mecanismo adecuados para proteger la información confidencial que se envía por correo electrónico (control A.13.2.3 Anexo A de la norma ISO/IEC 27001:2013)		Garantizar la debida protección y cifrado de la información incluida en la mensajería electrónica (Asociado al PA1)
A.11 SEGURIDAD FISICA Y DEL ENTORNO	76%	No se cuenta con los procedimientos para trabajo en áreas seguras (control A.11.1.5 del Anexo A de la ISO/IEC 27001:2013)	PA13	Establecer el respectivo procedimiento
		No se cuenta con un mecanismo efectivo de seguridad que permita validar que los equipos que se conecta a la red interna de la entidad sea una estación de trabajo segura y valida	PA14	Implementar una solución de NAC (Control de acceso de la Red)
		No se cuenta con una política de escritorio limpio		Se requiere definir y establecer la respectiva política (Asociado al PA5)

El resultado del diagnostico indico que el nivel de cumplimiento o desarrollo de la entidad frente al Anexo A de la norma ISO/IEC 27001:2013 es del **46.09%**, debió a que no cuenta con algunos controles, o los existentes no son adecuados o no están documentos y que por la tanto requieren su revisión en un medio plazo para mejorar su efectividad y su cumplimiento. Esta situación representa un riesgo Medio para la entidad debido a la ausencia de controles o la presencia de algunos con debilidades, la cual, puede ser aprovechado por amenazas internas o externas para atentar contra la seguridad de la información de la entidad.

Los planes de acción que se definieron para cerrar las brechas encontradas están sujetos a la viabilidad de su implementación por parte de la entidad, debido a que algunos de ellos requieren la adquisición de herramientas y/o soluciones tecnológicas que implica que la entidad deba adelantar procesos de contratación para su adquisición. Algunas de las soluciones tecnológicas que se requieren, pueden llegar a tener un costo elevado y/o su implementación puede demandar un tiempo considerable. Dentro de estas soluciones se destacan:

- Portal de intercambio seguro para garantizar el cifrado de la información que se intercambio con tercero. (Plan de acción PA1)
- Mecanismos para cifrar la información confidencial de la entidad que se envía por correo electrónico. (Plan de acción PA1)
- Solución NAC para garantizar el debido control de acceso de los equipos y dispositivos que se conectan a la red de la entidad (Plan de acción PA14)

Este diagnostico y los planes de acción que se establecieron, que hacen parte de los entregables del proyecto, permitieron dar alcanzar el objetivo específico OE3.

6.2. RESULTADOS FASE II – PREPARACION

Esta fase se planteo y desarrollo con el propósito de poder alcanzar los siguientes objetivos específicos del proyecto:

OE4. Establecer la estructura organizacional, roles y responsabilidades en cuanto a la Seguridad de la Información.
OE5. Analizar las necesidades y requerimientos de las partes interesas de la entidad con relación al Sistema de Gestión de Seguridad de la Información.
OE6. Definir la política, alcance y objetivos del Sistema de Gestión de Seguridad de la información.

OE4. Establecer la estructura organizacional, roles y responsabilidades en cuanto a la Seguridad de la Información.

Para establecer la estructura organizacional, roles y responsabilidades pertinentes a la seguridad de la información, como primera medida se identificaron las áreas dentro de la entidad cuyas funciones están relacionadas con la seguridad de la información, para lo cual se tuvo en cuenta los siguientes aspectos:

- Responsables de la seguridad de la información y seguridad informática
- Responsable de la seguridad física
- Responsable de la seguridad de los recursos humanos, antes, durante y después del contrato.
- Responsable del cumplimiento de la normatividad vigente
- Responsables y encargado del tratamiento de los datos personales.

Para el análisis de esta información se utilizaron los siguientes instrumentos de recolección de información:

- El organigrama de la entidad.
- La caracterización de los procesos documentada en el sistema de gestión de calidad de la entidad.
- Las funciones específicas de los colaboradores de la Vicepresidencia de Riesgos que fueron proporcionas por la Dirección de Gestión Humana.
- Las funciones del Comité de Riesgos que estan documentadas en el proceso de riesgo.

El organigrama de la entidad es el único que se incluye en el presente trabajo debido a que esta publicado en la página web de la entidad. Los otros documentos no se relacionan ya que corresponde a documentos de uso interno de la entidad.

Para determinar los roles y responsabilidades en torno a la seguridad de la información, también se consulto la Ley 1581 del 2012[71], que establece que las entidades deben definir los responsables y encargados del tratamiento de los datos personales de los titulares.

Durante el proceso de recolección de la información no se presento inconvenientes debido al acceso que tenía el autor sobre estos documentos, por el

[71] Ley Estatutaria 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”

contrario, la revisión y análisis de la información demando más tiempo del presupuestado debido a que los documento publicados en el Sistema de Gestión de la entidad no se podían exportar, copiar o descargar a otros formatos por política de seguridad de la entidad. Resultado de la revisión y análisis de la documentación recolectada, se evidencio, que las funciones del oficial de seguridad no estaban debidamente formalizadas y las funciones de comité de riegos no incluían las relacionadas con seguridad de la información.

Con base en el análisis realizado, se esquematizo un organigrama de la seguridad de la información que está representado en el Figura 11 del presente documento, el cual, contiene el comité y las áreas más representativas en torno a la seguridad de la información dentro de la entidad.

El entregable de esta actividad que corresponde al Anexo D y las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información que se definieron en el Manual de Políticas de Seguridad de la Información (ver Anexo F), permiten dar alcance al objetivo específico OE4.

OE5. Analizar las necesidades y requerimientos de las partes interesas de la entidad con relación al Sistema de Gestión de Seguridad de la Información.

Para el análisis de las partes interesadas de la organización se tomo como base el documento de Codigo de Buen Gobierno de la entidad[72], donde están descritos los grupos de interés externos que corresponden a las personas naturales o jurídicas con la cuales la entidad interactúa en el ejercicio de sus funciones. Para determinar los grupos de interés internos de la entidad, se tomo como base la organización de la seguridad que se definió en el Manual de Políticas de Seguridad de la Información (ver Anexo F) del presente trabajo.

Para estos grupos de interés se evaluó el grado de interés, motivación y gobernabilidad en función de su responsabilidad y capacidad de influir de manera positiva o negativa en la seguridad de la información de la entidad.

Resultado de esta evaluación se estableció de que en términos generales, existe un alto **grado de interés** de la mayoría de las partes interesas hacia la seguridad de la información de la entidad:

[72] Codigo de Buen Gobierno que esta publicado en el página web de la entidad,

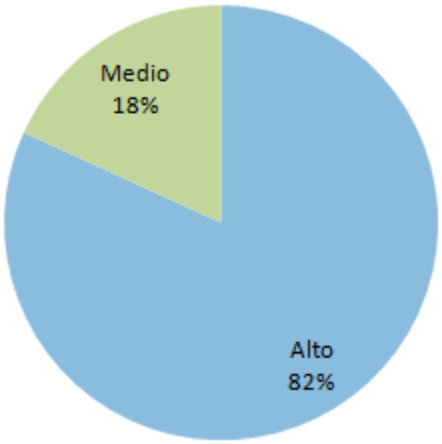


Figura 24. Grado de Interés Partes Interesadas
Fuente: El Autor

Las partes interesadas que tienen un interés medio (18%) en la seguridad de la información corresponden a los colaboradores y terceros que prestan sus servicios a la entidad, debido a que ven la seguridad de la información como un conjunto de restricciones que las complican su normal trabajo.

Las partes interesadas que tiene un interés alto (82%) corresponden aquellos que están interesadas de forma directa o indirecta en que la entidad tenga un adecuado sistema de gestión de seguridad para así proteger la información del negocio y de sus clientes. En este grupo estas las siguientes partes interesadas:

- El Gobierno, entes de control y la Superintendencia Financiera de Colombia, interesados en que la entidad cumpla con la normatividad relaciona con la protección, privacidad y seguridad de la información.
- La Alta Directiva de la entidad al establecer la política del SGSI demuestra liderazgo y compromiso con la Seguridad de la Información.
- El Comité de Riesgos, la Vicepresidencia de Riesgos y el oficial de seguridad interesados en implementar un adecuado SGSI.
- Las áreas como tecnología y recursos físicos, interesadas en implementar medidas y controles que garantice la seguridad de la información de la entidad.
- Los ex empleados interesados en que la entidad les garantice la protección de sus datos financieros y la privacidad de sus datos personales.
- Los intermediarios, bancos multilaterales e inversionistas, interesadas en que la entidad les brinde las garantías de protección de las operaciones que realizan con ella y de la información que intercambian.

El **grado motivación** hacia la seguridad de la información de la entidad por las partes interesas se ve reflejado en la siguiente grafica:

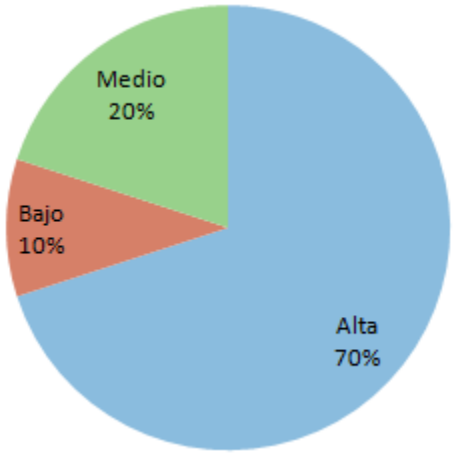


Figura 25. Grado de motivación partes interesadas
Fuente: El autor

El 70% de las partes interesadas tienen un grado alto de motivación hacia la seguridad de la información, lo cual se ve reflejado en la responsabilidad que tienen en garantizar la seguridad de la entidad. En este grupo están: Alta Dirección, Comité de Riesgos, Vicepresidencia de Crédito y Riesgos, Oficial de Seguridad, Dirección de Tecnología, Jefatura de Recursos Físicos y el Gobierno.

Por último, el **grado de gobernabilidad** está relacionado con al nivel de decisión de la parte interesada hacia la seguridad de la información de la entidad:

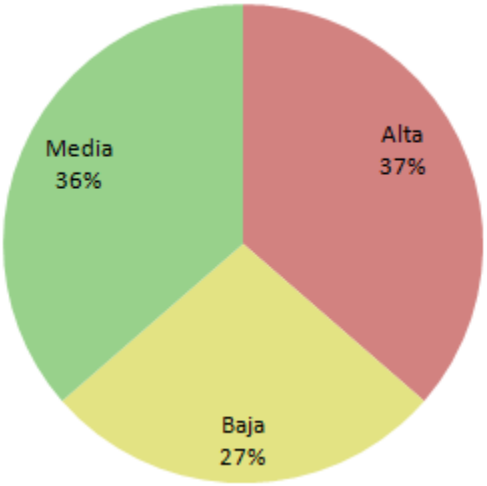


Figura 26. Grado de gobernabilidad partes interesadas
Fuente: El autor

El 37% de las partes interesadas tiene un alto grado de gobernabilidad sobre la seguridad de la información y corresponde a las partes que deciden las directrices de la seguridad a nivel estratégico o son los responsables de asegurar la implementación, operación y mejora continua del SGSI, en este grupo están: Alta Dirección, Comité de Riesgos, Vicepresidencia de Riesgos y Oficial de Seguridad.

El 36% de las partes interesadas tienen un grado medio de gobernabilidad sobre la seguridad de la información, en el cual, entres otros se encuentran las áreas que deben implementar y aseguras las medidas lógicos y físicas de seguridad, por ejemplo: Dirección de Tecnología y Jefatura de Recursos Físicos.

El 27% de las partes interesadas tienen un grado bajo de gobernabilidad sobre la seguridad de la información y corresponden a las partes que no tiene poder de decisión sobre la seguridad de la información de la entidad y no implementan medidas de seguridad, como son, colaboradores, proveedores, intermediarios financieros, bancos multilaterales y de desarrollo, y ex empleados.

El análisis realizado de las necesidades y requerimientos de las partes interesas de la entidad en función a la seguridad de la Información la entidad, permite el logro del objetivo específico OE5 que se planteo para el proyecto.

OE6. Definir la política, alcance y objetivos del Sistema de Gestión de Seguridad de la información.

La política, alcance y objetivos del Sistema de Gestión de Seguridad de la Información están definidos en el Anexo C que hace parte de los entregables del presente trabajo de grado.

Para la definición del alcance del Sistema de Gestión de Seguridad de la Información se tuvo en cuenta dos aspectos, el primero que corresponde a los requerimientos que establece la norma ISO\IEC 27001:2013 en su numeral '4.3 Determinación del Alcance del Sistema de Gestión de Seguridad de la Información'[73], y el segundo que corresponde al alcance que se defino en el presente trabajo de grado en el capitulo 1.3.1. ALCANCE.

[73] Norma ISO/IEC 27001:2013, Pág. 2

Para la definición de los objetivo del Sistema de Gestión de Seguridad de la Información se tuvo en cuenta el numeral '6.2 Objetivos de seguridad de la información y planes para lograrlos'[74] de la norma ISO\IEC 27001:2013.

La Política del Sistema de Gestión de Seguridad de la Información se definió teniendo en cuenta los requerimientos establecidos en el numeral '5.2 Política'[75] de la norma ISO\IEC 27001:2013 y los objetivo definidos de seguridad de la información que están definidos en Anexo C del presente trabajo.

Por lo tanto, las actividades desarrolladas para definir la política, alcance y objetivos del Sistema de Gestión de Seguridad de la información, permiten del alcance el objetivo específico OE6 definido en el presente proyecto de grado.

6.3. RESULTADOS FASE III – PLANIFICACION

Esta fase se planteo y desarrollo con el propósito de poder alcanzar los siguientes objetivos específicos del proyecto:

OE7. Definir la metodología para la identificación y clasificación de activos de información y para la valoración y tratamiento de riesgos de Seguridad de la Información.

OE8. Clasificar los activos de información del proceso de Gestión de Tecnología de la entidad, valorar sus riesgos de seguridad y definir los planes de tratamiento de los riegos encontrados, de acuerdo a la metodología definida.

OE9. Definir las políticas de la Seguridad de la Información de la entidad tomando como base la norma ISO 27001:2013.

OE10. Definir un mecanismo para la gestión de incidentes de seguridad.

OE7. Definir la metodología para la identificación y clasificación de activos de información y para la valoración y tratamiento de riesgos de Seguridad.

La metodología para la identificación y clasificación de activos de información y para la valoración y tratamiento de riesgos de Seguridad de la Información está definida en el Anexo D del presente trabajo de grado. Esta metodología establece los elementos y lineamientos para la valoración y el tratamiento de los Riesgos de Seguridad de la Información de la Entidad, para lo cual, se tuvo en cuenta los

[74] Norma ISO/IEC 27001:2013, Pág. 6
[75] Norma ISO/IEC 27001:2013, Pág. 3

requerimientos establecidos en los numerales '6.1.2 Valoración de riesgos de la seguridad de la información'[76] y '6.1.3 Tratamiento de riesgos de la seguridad de la información'[77] de la norma ISO\IEC 27001:2013.

Aunque la norma ISO/IEC 27001:2013, plantea un enfoque más amplio para la valoración de los riesgos, ya que no limita la identificación de los riesgos a partir de la identificación de los activos, amenazas y vulnerabilidades, el autor considera que para valorar riesgos de tecnología, si es necesario realizar el proceso ineludible y desgastados de clasificar los activos de información con el propósito de poder determinar su criticidad y nivel de protección, y así poder identificar los riesgos de seguridad asociados y de esta forma realizar un análisis para determinar los mecanismos más convenientes para protegerlos. Por lo tanto, en la metodología que se desarrollo se incluye la identificación y clasificación de los activos de información como elemento necesario para la valoración de los riesgos de tecnología.

La metodología desarrollada incluye los siguientes aspectos:

Tabla 41. Estructura metodología valoración de activos y riesgos

IDENTIFICAR Y VALORAR ACTIVOS DE INFORMACION	• Identificar los activos de información • Determinar el tipo de activo • Identificar los dueños de los riesgos • Identificar el responsable del activo • Identificar el contenedor del activo • Valorar los activos • Determinar el valor de criticidad del activo • Establecer el nivel de criticidad del activo • Determinar los activos para la valoración de riegos
IDENTIFICAR Y VALORAR ACTIVOS DE INFORMACION VALORACION DE RIESGOS	• Identificar de amenazas y vulnerabilidades • Analizar el riesgo inherente • Mapa de calor • Elaborar Matriz de Riesgo Inherente • Evaluar controles existentes para mitigar los riesgos • Determinar Riesgo Residual • Elaborar Matriz de Riesgo Residual • Establecer opciones y/o planes de tratamiento de riesgos

Por lo tanto, el documento relacionado con el Anexo D que hace parte de los entregables del proyecto, permite dar alcance al objetivo específico OE7.

[76] Norma ISO/IEC 27001:2013, Pág. 4
[77] Norma ISO/IEC 27001:2013, Pág. 5

OE8. Clasificar los activos de información del proceso de Gestión de Tecnología, valorar sus riesgos y definir los planes de tratamiento.

Las actividades relacionadas con la clasificación de los activos de información y la valoración de riesgos, se desarrollaron de acuerdo a los siguientes aspectos:

- La identificación de los activos de información se realizo de acuerdo al alcance que se definió para el Sistema de Gestión de Seguridad de la Información de la entidad, el cual solo contempla el proceso de tecnología para la sede principal de la entidad ubicada en la ciudad de Bogotá.
- Para el desarrollo de las actividades relacionas con la identificación y clasificaciones de los activos de información del proceso de tecnología y la respectiva valoración y tratamiento de los riesgos, se utilizo la metodología de riesgos que está relacionada en el Anexo D del presente trabajo de grado.
- Por requerimiento de confidencialidad de la empresa, para el presente trabajo en algunos casos no se relaciono el nombre específico de las aplicaciones, servidores y servicios de TI, sino se utilizo su finalidad para tal efecto.

Para la identificación y clasificación de los activos de información, se utilizo la hoja de Excel del Anexo E del presente trabajo, la cual además de contener el inventario y calificación de los activos de información del proceso de tecnología, también contiene los parámetros, las formulaciones y los cálculos que se utilizaron para determinar el nivel de criticidad de los activos.

Este proceso fue muy dispendioso debido a los siguientes factores:

- El área de tecnología no contaba con un inventario actualizado de sus activos de información, lo que significo que se tuvieran que realizar varias reuniones con los funcionarios de tecnología para recopilar esta información.
- Lo disponibilidad de tiempo por parte de los funcionarios del área de tecnología debido a sus múltiples actividades y compromisos, que genero que este proceso se demorara más tiempo del presupuestado.

Para clasificar los activos de información se utilizo el tipo de clasificación que se encuentra en la ‘Tabla 15. Tipos de activos de información’ del presente trabajo. Como resultado de este proceso se identificaron 57 de activos de información que fueron clasificados de acuerdo al tipo de activo, de la siguiente forma:

Tabla 42. Número de activos identificados por tipo de activo

Tipo de activo	No
Datos / Información	9
Equipos informáticos	14
Instalaciones	4
Redes de comunicaciones	4
Servicios	6
Software	20
Total	**57**

La siguiente es la distribución de los activos de información por tipo de activo:

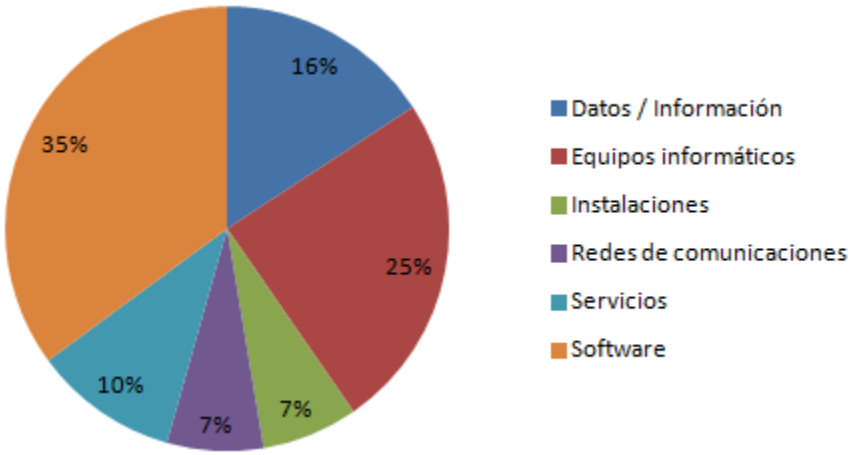


Figura 27. Clasificación activos de información de tecnología
Fuente: El autor

Los numero mostrados en este grafica, no representa el total de activos de la Dirección de Tecnología, debido a que por razones de confidencialidad de la entidad, para efectos del presente trabajo de grado algunos de los activos identificados no fueron incluidos o algunos con características similares fueron relacionados como un solo activo, pero esta última gráfica si muestra una tendencia de distribución por tipo de activos muy aproximación a la realidad.

- Los activos tipo de Software representan el 35% de los activos de información del proceso de tecnología, los cuales incluyen, el software base de administración y de monitoreo y los sistemas de información de la entidad.
- El grupo de Datos/Información que corresponde al 16% de los activos, incluye los activos relaciona con la identidad de los usuarios, los logs de eventos de errores, disponibilidad y seguridad, los documentos y manuales del proceso.

- En el grupo de Servicios que corresponde al 10% de los activos de información, están los servicios de directorio activo, correo, base de datos, fileserver, videoconferencia y gestión de privilegios.
- El grupo de Equipos Informáticos que equivale al 25% de los activos incluye, servidores de administración, bases de datos y aplicaciones de producción, pruebas y desarrollo, plataforma de correo, sistema de almacenamiento, computadores, equipos de seguridad perimetral, etc.
- El grupo de instalaciones que equivale al 7% de los activos incluye, centros de cómputo, cuartos de rack y área de administración de plataforma.
- El grupo de redes, que equivale al 7% corresponde a la red WAN y LAN

Una vez identificados los activos de información se procedió a valorar su grado de importación y criticidad para la organización, para lo cual, se valoro la afectación o perdida que le puede generar a la entidad en cuanto a aspectos financieros, legales y de imagen, en caso de verse afectada su seguridad.

Resultado de esta valoración, la siguiente es la clasificación de los activos de acuerdo a su grado de importancia y criticidad:

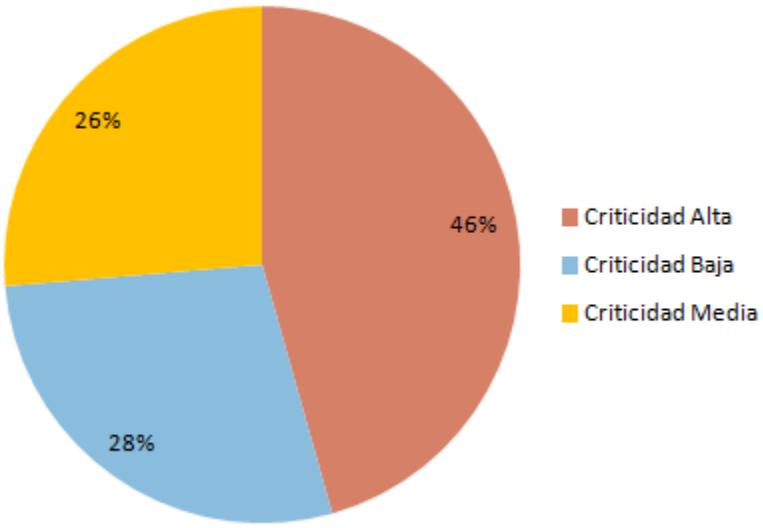


Figura 28. Clasificación activos de tecnología por criticidad
Fuente: El Autor

- El 46% de los activos de información de tecnología están clasificados como de criticidad Alta, los cuales corresponde a los activos cuya seguridad al ser vulnerada pueden poner en riesgo la información confidencial de la entidad, afectar la operación normal de las áreas críticas o la continuidad del negocio. En este grupo están activos como: centros de computo, equipos de seguridad

perimetral, red LAN y WAN, servidores de administración, bases de datos y aplicaciones de producción, bases de datos, unidades de almacenamiento, aplicativos CORE del negocio, directorio activo, datos de autenticación de los usuarios, riesgos de eventos de seguridad, entre otros.

- Los activos de criticidad Media que equivalen al 26% de los activos, corresponden a aquellos activos que soportan aplicaciones o servicios de producción que en caso de contingencia no se requieren para soportar los proceso críticos, aunque la seguridad de estos activos al ser vulnerada, puede poner en riesgo la información confidencial de la entidad. Dentro de estos activos estas: aplicaciones web, servicio de correo, solución de Backup, terminales empresariales, computadores de escritorio y portátiles de los usuarios, red WIFI de invitados, sistema de control de acceso, entre otros.
- Los activos de criticidad Baja que corresponde al 28% de los activos que, y son aquellos servicios de TI que no se requieren para soportar la contingencia de los procesos críticos pero cuya seguridad al ser vulnerada puede afectar en un grado bajo la confidencial del negocio. En este grupos están: aplicativo de mesa de ayuda, aplicativos no transacciones, intranet, video conferencia, impresoras, servidores de pruebas y desarrollo, entre otros.

Después de hacer clasificado los activos de información por su criticidad, se seleccionaron aquellos activos para el respectivo análisis de riesgos, para lo cual se tuvo en cuenta las recomendaciones dadas en la metodología de riesgos del Anexo D del presente trabajo, en el capítulo '3.9. Determinar los activos para la valoración de riegos'[78]. Por lo tanto, se opto por seleccionar los activos de información con nivel de criticidad Alto y Medio y agruparlos en la medida de lo posible por contenedor. Aquellos contenedores que incluyeran más de un activo de información se utilizaron para la valoración de riesgos en vez de hacerlo sobre los respectivos activos de manera individual, ya que de acuerdo a la metodología, si se protegen los contenedores también se protegen sus activos de información.

De acuerdo a lo anterior, se seleccionan 41 de los 57 activos de información identificados, los cuales están relacionados en la 'Tabla 21. Activos seleccionados para valoración de riesgos' del presente trabajo.

[78] Anexo D, Capitulo '3.9 Determinar los activos para la valoración de riesgos', Pág. 14

Una vez seleccionados los activos de información para la valorar los riesgos, se procedió a identificar las amenazas asociadas a estos, para lo cual y con el objetivo de facilitar esta labor, se utilizo la lista de riesgos relacionada en 'Tabla 22. Lista de riesgos y principios de seguridad afectados' del presente trabajo, la contiene los riesgos que pueden afectar a cualquier tipo de organización y los principios de seguridad de la información que se afectan, relacionados con la confidencialidad, integridad y disponibilidad. Esta lista fue compartida a los funcionarios de la Dirección de Tecnología, quienes a partir de ella identificaron las amenazas a las cuales están expuestos los activos de información seleccionados.

La siguiente grafica, muestra las amenazas identificadas y el número de los activos de información seleccionados que pueden ser afectados por estas:

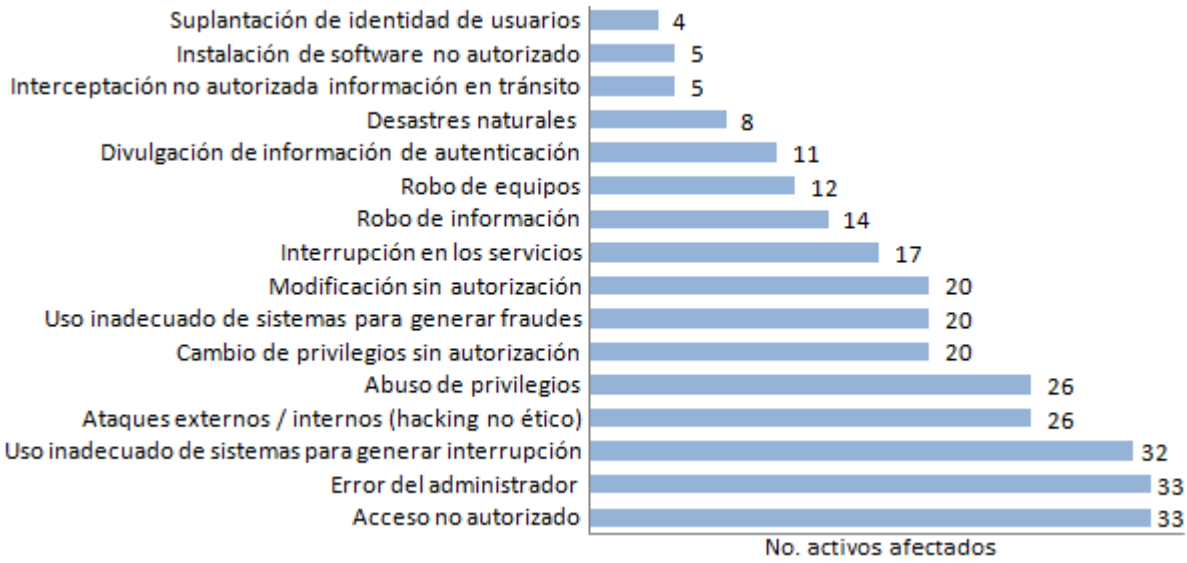


Figura 29. Cantidad de activos afectos por las amenazas
Fuente: El autor

La grafica anterior muestra una visión inicial de las amenazas internas o externas que pueden afectar la seguridad de la información de la entidad. En la misma, se puede observa que amenazas como acceso no autorizado y los errores del administrador, pueden poner en riesgos cada una de ellas, 33 de los 41 activos seleccionados, lo que equivale al 80% del total de estos activos. El inadecuado uso de sistema para generar interrupciones, que es otra amenaza, puede afectar 32 activos que equivalen al 78% del total de los seleccionados. Amenazas como abuso de privilegios y ataques externos o internos, pueden poder en riesgos de manera individual 26 activos que significan el 63% de los activos seleccionados.

Pasó seguido, con el área de tecnología se procedió a identificar las posibles vulnerabilidades de los activos de información que pueden ser aprovechas por las amenazas identificadas, para lo cual, se estableció como regla que no se debería tener en cuenta los controles o medidas de seguridad existentes que protegen la infraestructura tecnológica de la entidad. Esta labor no fue nada sencilla, debido a que los administradores de las plataformas fueron muy reservados en indicar las debilidades de ciertos componentes tecnológicos, lo cual, es entendible en la medida que esta información puede poner en riesgos la seguridad de la entidad.

Resultado de esta labor se identificaron las siguientes vulnerabilidades y el número de amenazas que pueden explotarlas:

Figura 30. Vulnerabilidades y No. de Amenazas que pueden explotarlas
Fuente: El autor

Una de las vulnerabilidades que puede ser aprovecha por 12 de las amenazas identificadas, corresponde a la ausencia, no aplicación o aplicación no adecuada de las políticas de seguridad de la información, por lo tanto, es esencial que las políticas definidas en el Manual de Políticas de Seguridad de la información (ver Anexo F) del presenta trabajo, sean aprobadas, publicadas e implementadas.

La inadecuada administración de roles y permisos que puede ser aprovechada por 9 de las amenazas identificadas, es una de las debilidades que generalmente se presente porque las organizaciones no cuentan con un esquema centralizado para la gestión de la identidad de los usuarios y el manejo de los roles y permisos que se les deben otorgar sobre los recursos tecnológicos y sistemas de información.

También aparecen debilidades como, contraseñas no seguro, cuentas de usuario sin auditar y la inexistencia de logs de eventos de seguridad, que ponen en riesgos la confidencialidad, autentificad y trazabilidad de la identidad de los usuarios y la privacidad de los datos de autenticación (usuarios y contraseñas) que ellos utilizan parar acceder a los recursos tecnológicos de la entidad.

La siguiente gráfica corresponde al número de vulnerabilidades que puede ser explotada por cada una de las amenazas identificadas:

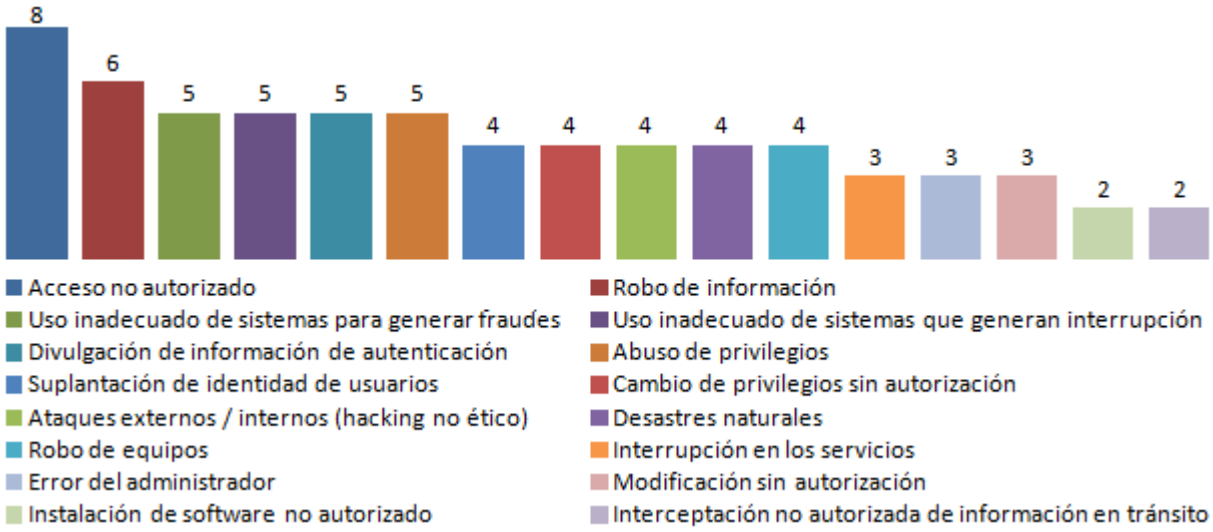


Figura 31. Número de vulnerabilidades que puede exportar una amenaza
Fuente: El autor

La anterior muestra un panorama inicial del nivel de exposición que pueden llegar a tener los activos de información del proceso de tecnología frente a las amenazas identificadas, el cual, no contempla la valoración de la probabilidad de ocurrencia e

impacto de los riesgos, que es fundamental para establecer el estado real de exposición de los activos de información.

Una vez identificadas las amenazas y vulnerabilidades se estableció al nivel de riesgo inherente, el cual, corresponde al nivel riesgo propio de acuerdo a la naturaleza y propósito de los activos de información sin tener en cuenta las medidas y controles de seguridad que existen para protegerlos.

Con el fin de facilitar el proceso de valoración y tratamiento de los riesgos, así como la elaboración de los respectivos mapas de riesgo inherente y residual, se codificaron los riesgos identificados de la siguiente forma:

Tabla 43. Codificación de riesgos del proceso de tecnología

R1	Acceso no autorizado
R2	Ataques externos / internos (hacking no ético)
R3	Cambio de privilegios sin autorización
R4	Desastres naturales (Terremotos, Incendios, Inundaciones, etc.)
R5	Divulgación de información de autenticación
R6	Error del administrador
R7	Instalación de software no autorizado
R8	Interceptación no autorizada de información en tránsito
R9	Interrupción en los servicios
R10	Modificación sin autorización
R11	Robo de equipos
R12	Robo de información
R13	Suplantación de identidad de usuarios
R14	Uso inadecuado de sistemas para generar fraudes
R15	Uso inadecuado de sistemas que generan interrupción
R16	Abuso de privilegios

Para determinar el riesgo inherente se valoro la probabilidad de ocurrencia de los riesgos identificados así como el impacto de los mismos en caso de su materialización, para lo cual, se tuvo en cuenta los pasos planteados en el capitulo ‘5.3.2.2 Análisis Riesgo inherente’ de la metodología referenciada en el Anexo D del presente trabajo. La probabilidad de ocurrencia del riesgo se determino a partir de número de veces que este puede llegar a presentarse en un periodo de un año, y el impacto se determino teniendo la afectación que puede generar la perdida de la confidencialidad, integridad y disponibilidad del activo de información en caso de la materialización del riesgo. Para calcular el valor de la probabilidad y del impacto

de los riesgos identificados, así como el valor del riesgo inherente, se utilizaron los criterios de valoración establecidos en las tablas, 'Tabla 5. Valoración probabilidad de ocurrencia', 'Tabla 6. Valoración del impacto' y 'Tabla 7. Valoración de los riesgos'[79], de la metodología de riesgos del Anexo D del presente trabajo. Con el objetivo de facilitar estos cálculos, se utilizo la hoja de Excel relacionada en el Anexo E del presente trabajo de grado, la cual, fue diligenciada conjuntamente con los coordinadores de las diferentes áreas de la Dirección de Tecnología, como son, plataforma, desarrollo, mesa de ayuda, entre otras.

Resultado de valorar la probabilidad de ocurrencia y el impacto de las amenazas identificadas, se obtuvo el valor del riesgo inherente de acuerdo a los datos y valores relacionados en las 'Tabla 28. Valoración de riesgos inherente Dirección de Tecnología' y 'Tabla 29. Riesgos inherentes de Tecnología por tipo de riesgo' del presente trabajo de grado.

La siguiente es la distribución del riesgo inherente del proceso de gestión de tecnología:

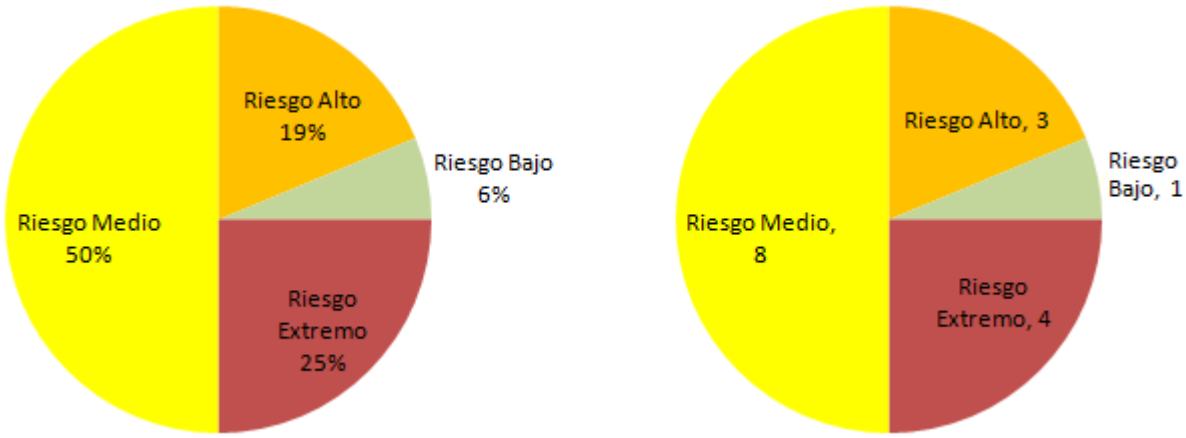
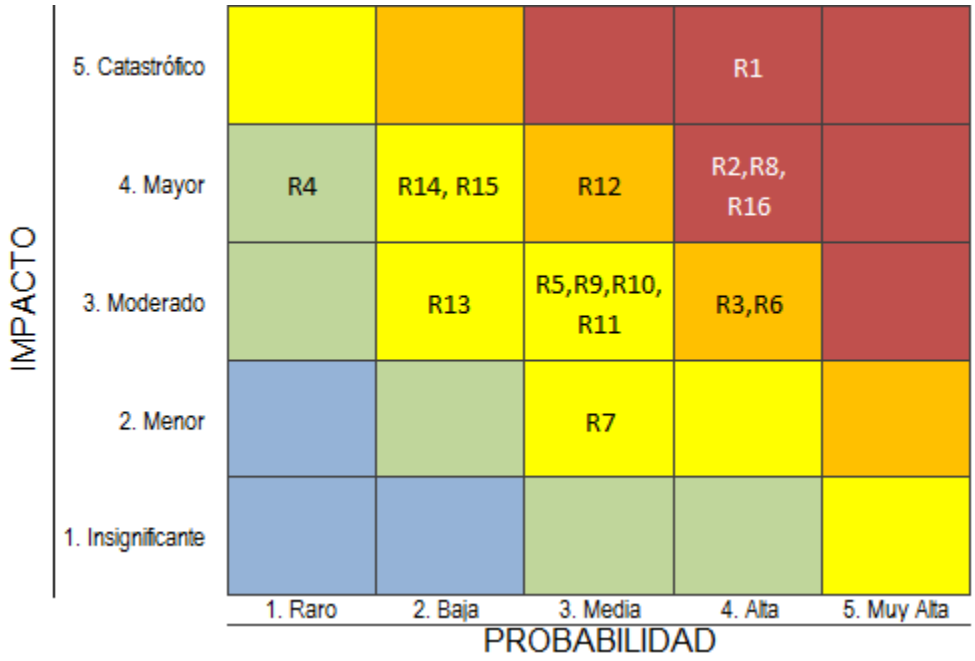


Figura 32. Distribución Riesgos Inherente proceso de tecnología
Fuente: El Autor

Para establecer el mapa de riesgos inherente se utilizo como referencia el mapa de calor que aparece en el capítulo '5.3.2.3 MAPA DE CALOR' del presente trabajo, el cual, corresponde a una representación gráfica de una matriz de 5x5, donde se ubicación los riesgos de acuerdo al valor de la probabilidad (eje x) y al valor del impacto (eje y). Cada zona dentro del mapa de calor corresponde a un

[79] Anexo D, Metodología de valoración de riesgos de seguridad de la información, Pág. 16, 17 y 18

tipo de riesgo e indica las acciones de tratamiento del riesgo a seguir. El siguiente es el mapa de riesgos inherente del proceso de tecnología:



Dentro de los riesgos clasificados como riesgo extremo, se encuentra el riesgo ‘R16. Abuso de privilegios’, el cual representa uno de los mayores riesgos que atentan contra la seguridad de las organizaciones de acuerdo a estudios realizados. La empresa Oracle en su informe ‘’DBA – Security Superhero: 2014 IOUG Enterprise Data Security Survey’, indica que el 54% de los encuestados ven el abuso de los privilegios de acceso como uno de los mayores riesgos para los datos de las empresas[80]. La empresa Raytheon Company, en su informe ‘Privileged User Abuse & The Insider Threat’ publicado en mayo de 2014, indica que las personas con acceso a los datos privilegiados, frecuentemente ponen en riesgos la información sensible de la organización[81]. El abuso de privilegios es un riesgo que por su naturaleza y los efectos que conlleva, genera la posibilidad de la materialización de otros riesgos, como son, el cambio de privilegios sin autorización, accesos no autorizados, perdida o robo de información y uso inadecuado de sistemas para generar fraudes o interrupción en los servicios.

El mapa de riesgo inherente del proceso de tecnología, permite identificar que el 50% de los riesgos se clasifican como riesgos medios, lo que implica la

[80] https://www.oracle.com/es/corporate/pressrelease/2-19189.html
[81] http://raytheon.mediaroom.com/index.php?s=43&item=2570

identificación de controles orientados a reducir el riesgo a niveles más bajos. El 25% de los riesgos están clasificados como extremos, lo que significa que los controles deben que permitan reducir y compartir el riesgo, transferirlo o incluso evitarlo. El 19% corresponde a riesgos altos, que requiere de controles adecuados que permitan disminuir el riesgo a nivel bajo o inusual.

Una vez generada la matriz de riesgo inherente se procedió a valorar la efectividad de los controles existentes para determinar el nivel de desplazamiento que estos pueden genera sobre el mapa de calor para los respectivos riesgos, para lo cual, se utilizo como instrumento de recolección de información el cuestionario que está relacionado en el 'Tabla 30. Criterios para evaluar la efectividad del control', del presente documento, la cual, contiene una serie de pregunta orientadas a valorar la efectividad del control. Este cuestionario que esta formulado en la hoja de Excel relacionada en el Anexo E del presente trabajo, fue diligenciado por los funcionarios del área de tecnología quienes determinaron los controles existentes y respondieron las preguntas para valorar su efectividad.

Con base en la información proporcionada por tecnología, se identificaron el número de riesgos que puede mitigar cada uno de los controles, lo cual, incialmente indicaría el nivel de efectividad del control. La siguiente grafica muestra esta situacion:

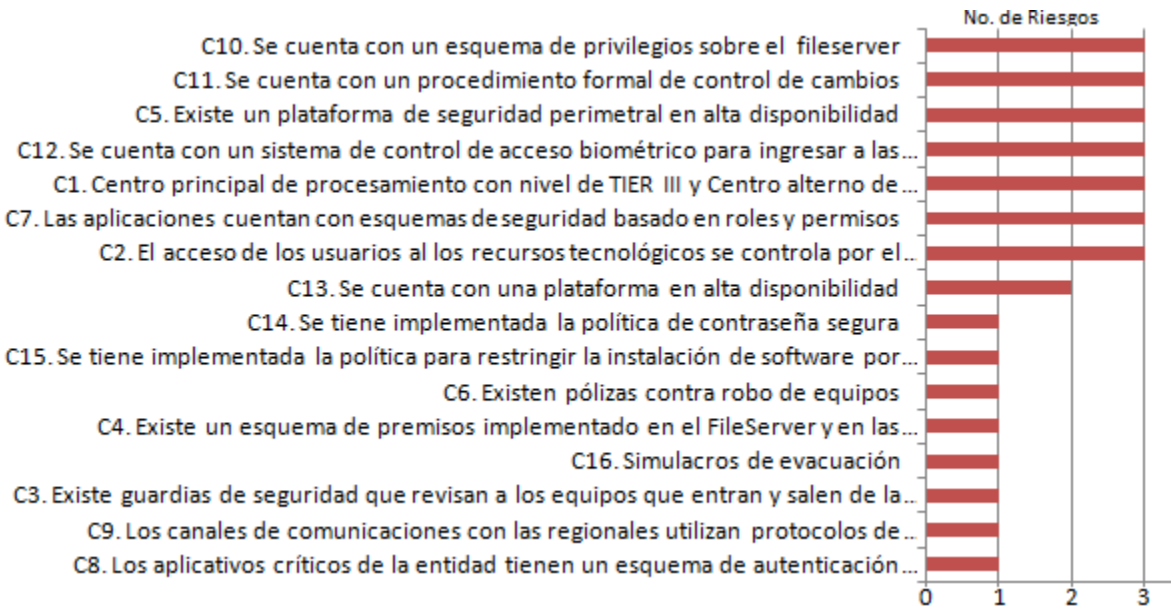


Figura 33. Numero de riesgos que mitiga los control identificados
Fuente: El Autor

La siguente es la relacion de las cantidad de controles que se indentificaron para cada uno de los riesgos evaluados:

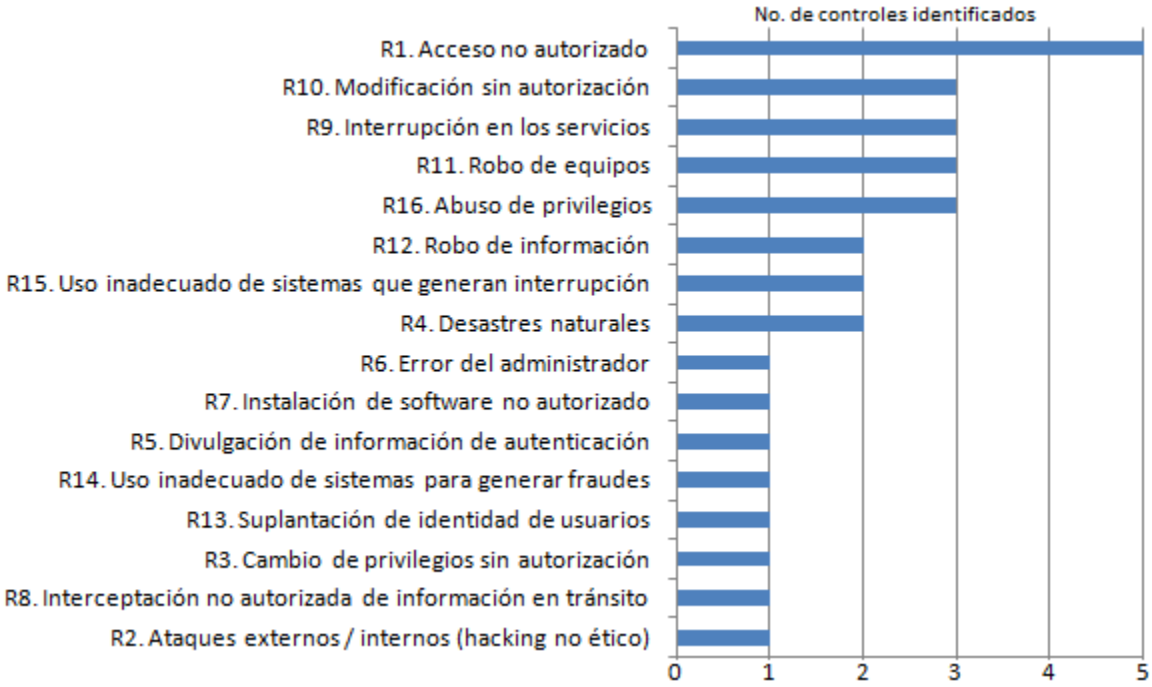


Figura 34. Cantidad de controles identificados por riesgo

En esta gráfica se puede observar que para cada riesgo por lo menos se identifico un control que puede generar el desplazamiento del riesgo a una zona menor en el mapa de calor, lo cual, es algo positivo ya que ayuda a mitigar el nivel de riesgo inherente del proceso de tecnología.

También se puede identificar que para los riesgos ‘R1 - Acceso no autorizado’ y ‘R16 - Abuso de privilegios’ que están en la zona extrema del mapa de calor, se identificaron por lo menos tres controles que ayudan de manera significativa a disminuir su nivel de riesgo inherente.

Con el objetivo de generar la matriz de riesgo residual del proceso de tecnología, se aplico en el mapa de calor la disminución que se genero en la probabilidad y/o impacto del riesgo al evaluar la efectividad de los respectivos controles. La información correspondiente a la valoración de los controles que se identificaron para mitigar los riesgos se encuentra en la Tabla 33. ‘Determinación Nivel de Desplazamiento’ del presente documento, la cual contiene los puntajes obtenidos por cada uno de los controles de acuerdo a su efectividad y el nivel de desplazamiento que genero en la probabilidad y/o en el impacto.

Las siguientes graficas muestras la disminución en el nivel de los riesgos que genero los respectivos controles identificados:

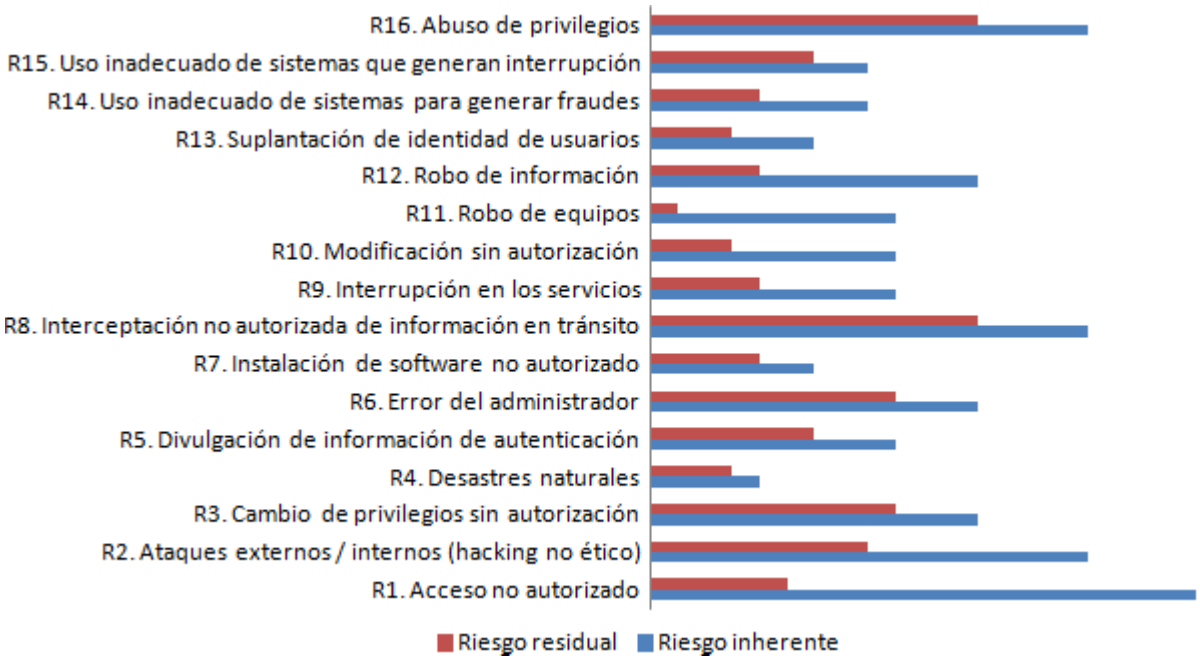


Figura 35. Disminución nivel de riesgo por efectividad del control (1)

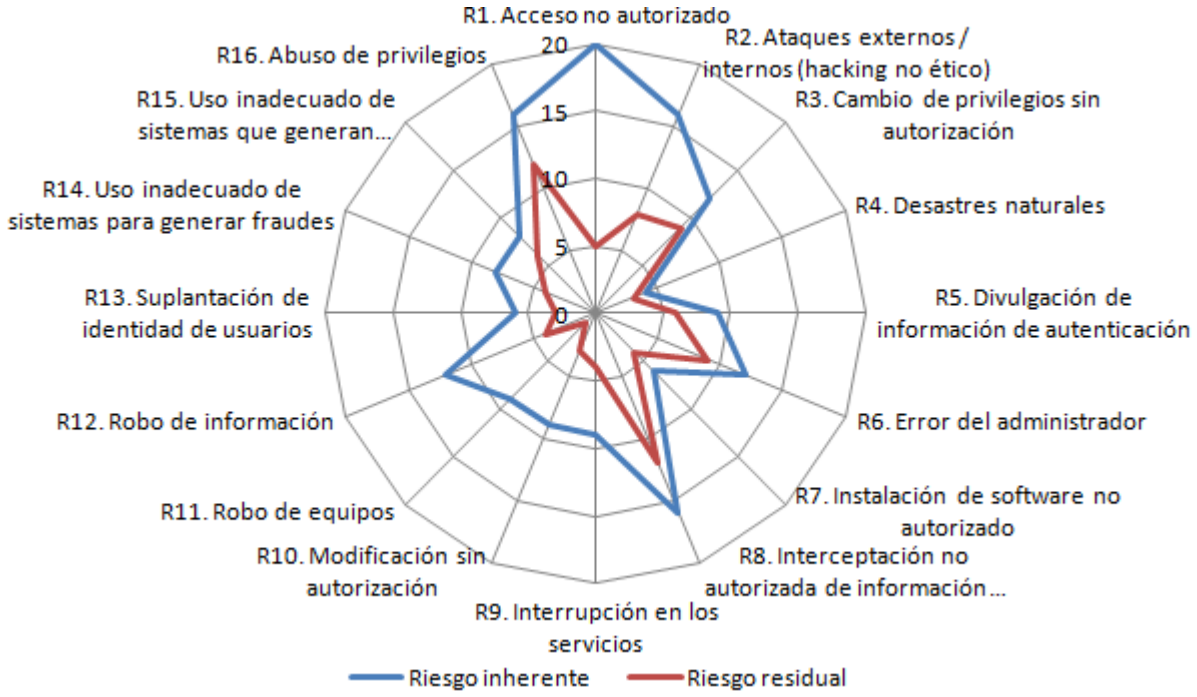


Figura 36. Disminución nivel de riesgo por efectividad del control (2)

De acuerdo a estas gráficas los controles identificados en términos generales fueron efectivos ya que permitieron reducir los respectivos riesgos a niveles más bajos, logrando con esto una disminución significativa en el nivel del riesgo inherente del proceso de tecnología.

La siguiente tabla muestra el porcentaje de disminución que género los controles identificados para mitigar cada uno de los riesgos:

Tabla 44. Disminución nivel riesgos por controles valorados

	Riesgo Inherente				Riesgo Residual				
RIESGO	Probabilidad	Impacto	PxI	Nivel Riesgo	Probabilidad	Impacto	PxI	Nivel riesgo	% Disminución
R1. Acceso no autorizado	4	5	**20**	Riesgo Extremo	1	5	**5**	Riesgo Medio	75.00%
R2. Ataques externos / internos (hacking no ético)	4	4	**16**	Riesgo Extremo	2	4	**8**	Riesgo Medio	50.00%
R3. Cambio de privilegios sin autorización	4	3	**12**	Riesgo Alto	3	3	**9**	Riesgo Medio	25.00%
R4. Desastres naturales	1	4	**4**	Riesgo Bajo	1	3	**3**	Riesgo Bajo	25.00%
R5. Divulgación de información de autenticación	3	3	**9**	Riesgo Medio	2	3	**6**	Riesgo Medio	33.33%
R6. Error del administrador	4	3	**12**	Riesgo Alto	3	3	**9**	Riesgo Medio	25.00%
R7. Instalación de software no autorizado	3	2	**6**	Riesgo Medio	2	2	**4**	Riesgo Bajo	33.33%
R8. Interceptación no autorizada de información en tránsito	4	4	**16**	Riesgo Extremo	3	4	**12**	Riesgo Alto	25.00%
R9. Interrupción en los servicios	3	3	**9**	Riesgo Medio	2	2	**4**	Riesgo Bajo	55.56%
R10. Modificación sin autorización	3	3	**9**	Riesgo Medio	1	3	**3**	Riesgo Bajo	66.67%
R11. Robo de equipos	3	3	**9**	Riesgo Medio	1	1	**1**	Riesgo Inusual	88.89%
R12. Robo de información	3	4	**12**	Riesgo Alto	1	4	**4**	Riesgo Bajo	66.67%
R13. Suplantación de identidad de usuarios	2	3	**6**	Riesgo Medio	1	3	**3**	Riesgo Bajo	50.00%
R14. Uso inadecuado de sistemas para generar fraudes	2	4	**8**	Riesgo Medio	1	4	**4**	Riesgo Bajo	50.00%
R15. Uso inadecuado de sistemas que generan interrupción	2	4	**8**	Riesgo Medio	2	3	**6**	Riesgo Medio	25.00%
R16. Abuso de privilegios	4	4	**16**	Riesgo Extremo	3	4	**12**	Riesgo Alto	25.00%
								Promedio disminución de controles	**44.97%**

De acuerdo a estos datos los controles valoradores generaron una disminución del **44.97%** en el nivel del riesgos del proceso de tecnología.

La siguiente grafica muestra el porcentaje de disminución en el nivel de riesgo que genero los respectivos controles valorados:

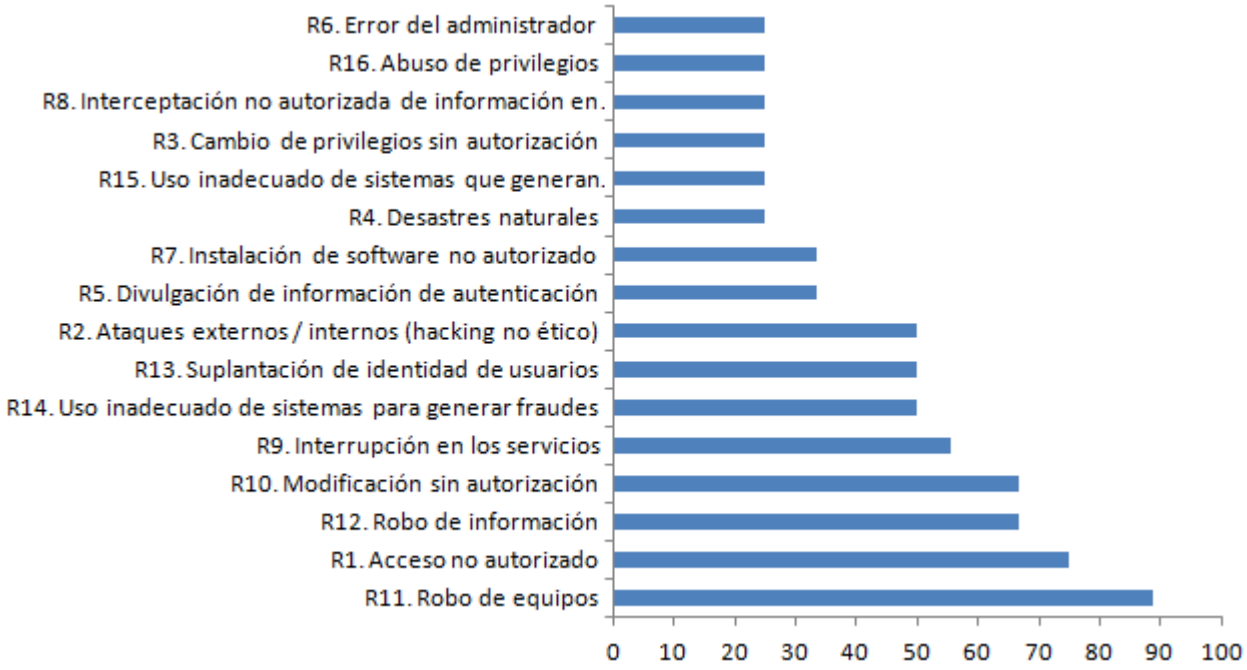


Figura 37. Disminución nivel riesgos por controles valorados

Las siguientes son las matrices de riesgos inherente y residual del proceso del proceso de tecnología, donde se puede observar el desplazamiento que género los controles identificados para cada uno de los riesgos:

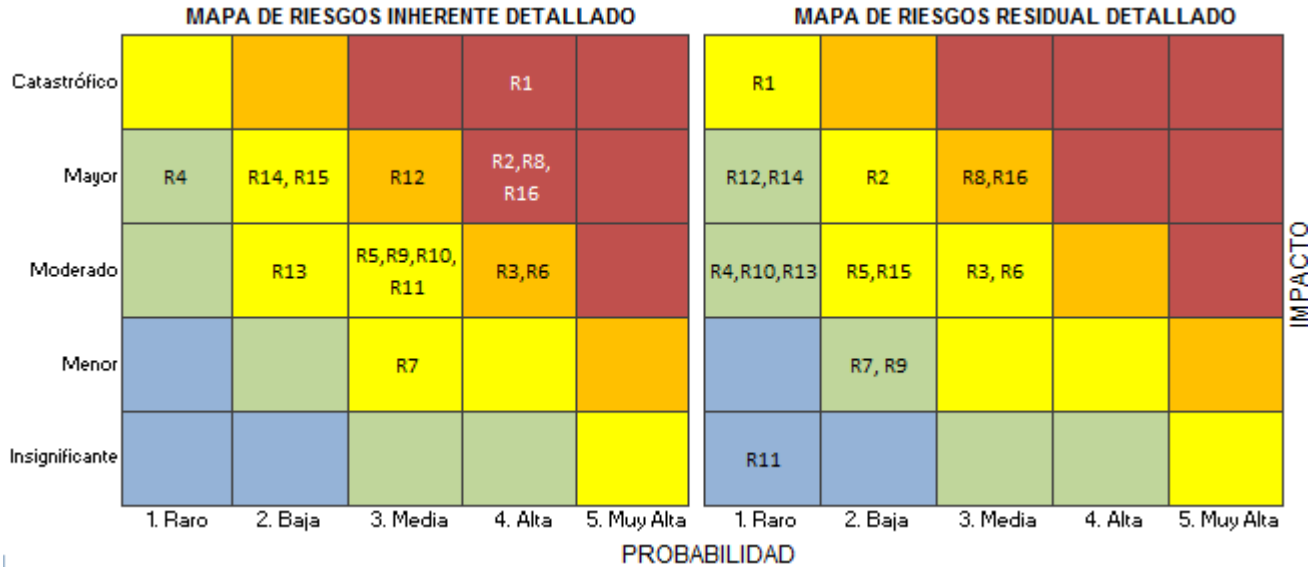


Figura 38. Comparativo matriz de riesgos proceso de tecnología

Los siguientes son algunos de los análisis que se pueden establecer de acuerdo a la disminución del nivel de los riesgos que se presenta en el mapa de riesgo residual del proceso de tecnología:

- La efectividad de los controles identificados permitió la disminución del nivel de los riesgos que estaban en la zona extrema, que correspondían a riesgos que requerían acciones inmediatas de tratamiento orientadas a reducir, compartir el riesgo, transferirlo o incluso evitarlo. Esta disminución permitió que todos los riesgos extremos se movieran a otras zonas del mapa de calor.
- Los controles identificados y valorados para el riesgo R1 - Acceso no autorizado, permitieron que este riesgo de moviera de la zona extrema a una de las zona de riesgo medio. Esta reducción fue una de las más efectivas en el mapa de calor, debido a que genero una disminución del 75% en el nivel de este riesgo. A pesar de la reducción del nivel de este riesgo, el mismo quedo es una zona de riesgo medio que requiere de medidas adecuadas que permitan seguir disminuyendo el riesgo a un nivel bajo o inusual.
- El Riesgos R2 - Ataques externos / internos (hacking no ético), paso de la zona extrema a la zona de riesgo medio, debido a una disminución en su nivel de riesgo del 50% generada por los controles identificados. Este riesgo requiere de acciones prontas y adecuadas para reducir el riesgo a niveles más bajos.
- Los Riesgo R8 - Interceptación no autorizada de información en tránsito y R16 - Abuso de privilegios, que estaban en la zona extrema, solo tuvieron una reducción del 25% generada por sus respectivas controles, quedando en la zona riesgo alto que requiere de una atención y medidas urgentes para reducir el nivel del riesgo.
- Los controles valorados para el riesgo R11 - Robo de equipos, generaron el mayor nivel desplazamiento en el mapa de calor, correspondiente a una disminución del nivel de riesgos del 89%, permitiendo que este riesgo pasara de la zona media a la zona más baja de riesgo inusual. Este riesgo se asume y no necesita tratamiento.
- El riesgo R12 - Robo de información pasó de la zona de riesgo alta a la zona de riesgo media, debido a que los controles valorados generaron una disminución del 66.67%. Este riesgo al quedar en una zona de riesgo medio

requiere de medidas adecuadas que permitan disminuir el riesgo a nivel bajo o inusual.

- Los Riesgos R3 - Cambio de privilegios sin autorización y R6 - Error del administrador, solo tuvieron una disminución del 25% de acuerdo a la valoración de los respectivos controles, lo cual, genero una disminución de un solo punto sobre el eje de la probabilidad (eje x). A pesar de que estos riesgos pasaron de la zona de riesgo alto a la de riesgo medio, requieren de acciones para seguir reduciendo el riesgo a niveles más bajos.
- Aunque los riesgos R5 - Divulgación de información de autenticación y R15 - Uso inadecuado de sistemas que generan interrupción, tuvieron una disminución del 25% en su nivel de riesgo, permanecieron en la zona media del mapa de calor. Estos riesgos requieren de medidas para seguir reduciendo el riesgo a niveles más bajos.
- A pesar de la disminución que los controles genero sobre el Riesgo R4 - Desastres naturales, este permaneció en la zona de riesgo bajo, donde se requieren de algunas medidas preventivas para reducir el riesgo.

Después de elaborar el mapa de riegos inherente del proceso de tecnología, se establecieron los planes de tratamiento orientados a mitigar los riesgos, con el objetivo de preservar las características de confidencialidad, integridad y disponibilidad de la información que se gestiona a través de los activos de tecnología seleccionados para el proceso de valoración de riesgos.

Para definir estos planes de tratamiento, se tuvo en cuenta el mapa de calor relacionado en el capítulo 4.3 ‘Mapa de Calor’ de la metodología de riesgos relacionada en el Anexo D del presente trabajo, el cual define para cada una de las zonas de mapa las acciones que se deben adelantar con el propósito de evitar, reducir, transferir o asumir el riesgo.

De acuerdo a las disminuciones generadas por los controles sobre cada uno de los riesgos valorados, la siguiente es la distribución del riesgo residual del proceso de tecnología, que permite establecer las acciones para el tratamiento de los riesgos valorados de acuerdo a como estos quedaron ubicados en los diferentes tipos de riesgos:

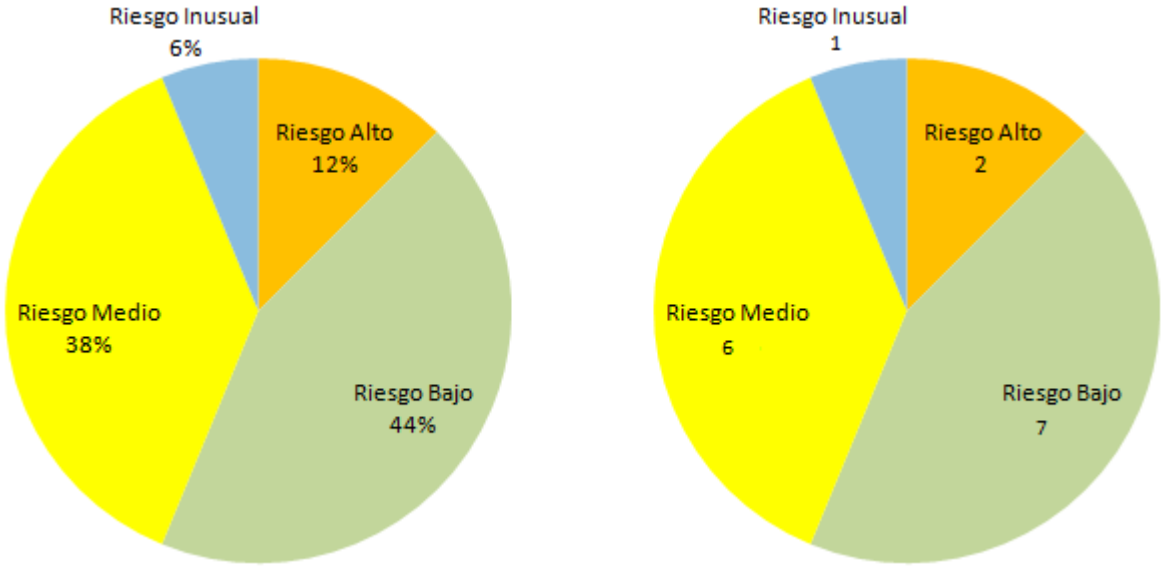


Figura 39. Distribución riesgo residual proceso de tecnología
Fuente: El autor

Estas graficas permiten establecer:

- Existe dos riesgos altos, que requieren atención urgente y la implementación medidas para reducir el nivel del riesgo, los cuales son: R16. Abuso de privilegios y R8. Interceptación no autorizada de información en tránsito.
- Existen seis riesgos (R1, R2, R5, R15, R3 y R6) en la zona media que requieren de medidas prontas y adecuadas que permitan disminuir el riesgo a nivel bajo o inusual.
- Existen siete riesgos en la zona baja (R12, R14, R4, R10, R13, R7, R9) donde el riesgo se mitiga con actividades propias y por medio de algunas medidas preventivas para reducir el riesgo.
- Existe un riesgo en la zona inusual (R11), que por esta en esta zona se puede aceptar el riesgo sin necesidad de tomar otras medidas de control diferentes a las existentes.

Las acciones que se definieron para el tratamiento de cada uno de los riesgos valorados se encuentran en la Tabla 35. Opciones tratamiento riesgo residual del proceso de tecnología', del presente trabajo de grado. A partir de esta información, se puede establecer la siguiente distribución que indica el número de amenazas de acuerdo a la opción de tratamiento que se debe realizar para mitigar el riesgo:

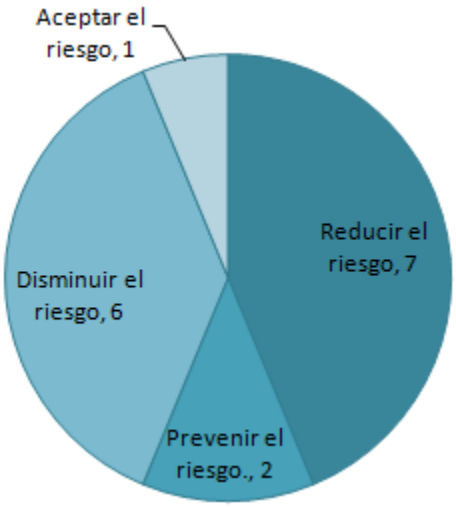


Figura 40. Distribución de amenazas por opción de tratamiento del riesgo
Fuente: El autor

Los planes de tratamiento que se definieron para mitigar los riesgos residuales del proceso de tecnología producto de valorar las amenazas que pueden afectar a los activos de información seleccionados, están relaciones en el capitulo '5.3.3. PLANES DE TRATAMIENTO DE RIESGO' del presente trabajo.

Algunos de estos planes de tratamiento, al igual que los que se definieron para cerrar las brechas encontradas producto del diagnostico del nivel de cumplimiento de la entidad con relación al Anexo A de la ISO 27001:2013, están sujetos a la viabilidad de su implementación por parte de la entidad, debido a que algunos de estos requieren la adquisición de soluciones tecnológicas que implican procesos de contratación, las cuales pueden llegar a tener un costo elevado y/o su implementación puede demandar un tiempo considerable. Dentro de estas soluciones definidas en estos los planes de tratamiento están:

- Solución para el monitoreo de Logs y correlación de evento, su costo aproximado puede estar al rededor de los $250.000.000 m/l.
- Implementar un portal de intercambio seguro que garantice la integridad, confidencialidad, autenticidad y no repudio de la información que se intercambió con terceros. Esta herramienta también se identifico dentro el plan de acción PA1 que se establecido para cerrar una de las brechas encontradas producto de la revisión realizada del nivel de cumplimiento de la entidad con relación al Anexo A de la ISO 27001:2013.

- Implementar mecanismos que garanticen el cifrado de la información que se intercambia con terceros a través del correo electrónico. Al igual que la anterior, también esta como parte del plan de acción PA1.
- Implementar mecanismo de cifrado de disco duro de los dispositivos móviles y portátiles de la entidad. También hace parte del plan de acción PA1.

Por lo tanto, y con el propósito de dar alcance al objetivo específico OE8 que se definido para el proyecto, se realizaron las siguientes actividades:

- Identificación y clasificación de los activos de información del proceso de Gestión de Tecnología de la entidad.
- Selección de los activos para la valoración de riesgos de seguridad de la información
- Análisis del riesgo inherente y elaboración de la respectiva matriz
- Evaluación de los controles existentes para mitigar los riesgos
- Determinación del nivel de riesgos residual y elaboración de la respectiva matriz
- Definición de planes de tratamiento

OE9. Definir las políticas de la Seguridad de la Información de la entidad tomando como base la norma ISO 27001:2013.

Para el desarrollo de las políticas de Seguridad de la Información, se tuvo en cuentas los dominios, objetivos de control y controles que están definidos en el Anexo A de la Norma ISO/IEC 27001:2013. También, para el desarrollo de las policitas se tomo como marco de referencia el formato e implementación de políticas de seguridad y privacidad de la información que propone MINTIC [18].

Para efecto del presente trabajo se documentaron las políticas de seguridad de la información relacionadas con los siguientes dominios de control del Anexo A de la norma ISO 27001:2013:

Dominio de control	Nombre de la Política de seguridad
A.5.	Política General de Seguridad de la Información
A.6.	Organización de Seguridad de la Información
A.7.	Seguridad de los Recursos Humanos

A.8.	Gestión de Activos
A.9.	Control de Acceso
A.10.	Criptografía
A.11.	Seguridad Física y del Entorno
A.12.	Seguridad de las Operaciones
A.13.	Seguridad de las Comunicaciones
A.14.	Adquisición, Desarrollo y Mantenimiento de Sistemas
A.15.	Relaciones con los Proveedores
A.16.	Gestión de Incidentes de Seguridad de la Información
A.17.	Seguridad de la Información en la Continuidad del Negocio
A.18.	Cumplimiento de Requisitos Legales y Contractuales

Las políticas, normas y lineamientos que regirán la seguridad de la información en la entidad y las responsabilidades y obligaciones de todos los colaboradores y terceros que tengan acceso a la información de la entidad, están documentadas ANEXO F - MANUAL POLITICAS DE SEGURIDAD DE LA INFORMACION, que hace parte de los entregables de este trabajo de grado.

Este manual de políticas debe ser aprobado por el comité de riesgos para su debida publicación, socialización y cumplimiento. Debido a que el presente trabajo de grado solo abarca el diseño de un sistema de gestión de seguridad de la información para la entidad, y no la implementación del mismo, la elaboración del manual de políticas de seguridad relacionado en el Anexo F, permite dar alcance al objetivo específico OE9 que se definió para el presente trabajo de grado.

OE10. Definir un mecanismo para la gestión de incidentes de seguridad.

Para alcanzar este objetivo específico del proyecto, se elaboro el procedimiento para el reporte y atención de incidentes de seguridad, el cual esta referencia en el ANEXO G - PROCEDMIENTO REPORTE Y ATENCION INCIDENTES DE SEGURIDAD que hace parte de los entregables de este proyecto.

Para determinar las actividades que se deberían contemplar este procedimiento, se tomo como referencia la guía de Gestión de Incidentes de seguridad de la información del MINTIC [16], la cual plantea las siguientes actividades involucradas en el ciclo de vida de la gestión de incidentes de seguridad:

Figura 41. Ciclo de vida gestión incidentes de seguridad de la información
Fuente: http://www.mintic.gov.co/gestionti/615/articles-5482_Gestion_Incidentes.pdf

La estructura de los capítulos que contiene este procedimiento, se tomo de acuerdo al estándar establecido en la entidad para este tipo de documento.

El procedimiento para el reporte y atención de incidentes de seguridad de la información, comienza con la identificación del evento de seguridad que pueda afectar la disponibilidad, integridad y confidencialidad de la información de la entidad, continua con el análisis del evento para determinar si se clasifica o no como una incidencia de seguridad para así determinar e implementar las medidas de Contención, Erradicación y Recuperación y finaliza con la aplicación de mejoras para prevenir la ocurrencia de nuevos incidentes.

El procedimiento de reporte y atención de incidentes de seguridad debe ser aprobado por el Vicepresidente de riesgos y el área de calidad, para su debida publicación y socialización. Debido a que el presente trabajo de grado solo abarca el diseño de un sistema de gestión de seguridad de la información para la entidad, y no la implementación del mismo, la elaboración de este procedimiento relacionado en el Anexo G de presente trabajo, permite dar alcance al objetivo específico OE10 que se definió para el presente trabajo de grado.

7. CONCLUCIONES

El diseño de un Sistema de Gestión de Seguridad de la Información basado en un modelo de mejoras practicas y lineamientos de seguridad, como es la norma ISO/IEC 27001:2013, es un herramientas de gran ayuda que permite identificar los diferentes aspectos que se deben tener en cuenta cuando las organizaciones deciden establecer un modelo de seguridad de la información, ya que si los organizaciones logran cumplir al pie de la letra lo establecido está en la norma ISO/IEC 27001:2013, podar llegar a forjar en el tiempo un adecuado y sostenible Sistema de Gestión de Seguridad de la Información, aunque dicha labor depende del tamaño y naturaleza de la entidad y de la cultura de la misma en torno a la seguridad de la información.

Esta labor debe comenzar con el compromiso demostrable de la alta directiva hacia la seguridad de la información, labor que no es nada fácil cuando no se tiene concebida la seguridad de la información dentro de los objetivos estratégicos de la organización. El apoyo de la alta directiva, es indispensable para poder concebir un modelo de Seguridad de la Información que realmente apoye y apalanque la misión y visión de la organización, el cual es fundamental que se tenga antes de comenzar a diseñar un Sistema de Gestión de Seguridad de la Información, ya que si este no se logra conseguir, es casi seguro que cualquier iniciativa de seguridad que se pretender adelantar, no alcancen los resultados esperados y si por el contrario, genere el rechazo o el poco apoyo o interés por parte de la organización.

Con este proyecto de grado se pretendió diseñar un Sistema de Seguridad de la Información para una entidad financiera de segundo piso, para lo cual se decidió utilizar como marco de referencia la norma ISO 27001:2013.

Resultado de tratar de aplicar los diferentes requerimientos de la norma ISO 27001:2013, se logro obtener una serie de diagnósticos que permitieron establecer el nivel de madures de la entidad frente a la gestión de la seguridad de la información.

A continuación de describen las conclusiones de estos diagnósticos:

- Debido a la complejidad de la infraestructura tecnología y a la capacidad del área de tecnología, la entidad se encuentra clasificada en un nivel MEDIO de estratificación, que implica un esfuerzo considerable para la implementación del Sistema de Gestión de Seguridad de la Información, lo cual, se ve reflejado en los diferentes planes de acción que se generaron a lo largo del proyecto que están orientado a dar cumplimiento a los requerimientos de la norma ISO/IEC 27001:2013.
- El nivel de cumplimiento de la entidad frente de los requerimientos del Anexo A de la norma ISO/IEC 27001:2013, es del 46%, lo que significa que la implementación del Sistema de Gestión de Seguridad de la información le implicará a la entidad un refuerzo considerable debido a la ausencia de controles o al bajo grado de cumplimiento de muchos de ellos.
- La falta de controles orientados a proteger la información que se intercambia con terceros, puede generar consecuencias graves para la entidad y afectar de manera negativa su imagen ante sus partes interesadas, por tal razón, es urgente que la entidad implementen mecanismos de cifrado con el objetivo de garantizar la integridad, confidencialidad y autenticidad de esta información.
- Es necesarios establecer cuenta antes el proceso de gestión de incidentes de seguridad para proveer en la entidad de un mecanismo para el reporte, evaluación y respuesta a los eventos e incidencias de seguridad de la información
- Es necesario el establecimiento de unas políticas de seguridad aprobadas por la Alta Dirección, para garantizar su debida implementación, actualización y cumplimiento.
- Se requiere implementar controles adecuados y efectivos, o fortalecer los existentes, con el objetivo de asegurar que la seguridad de la información sea parte del ciclo de vida del desarrollo de aplicaciones de la entidad y con ello garantizar que los cambios que se realizan en producción no afecten la operación ni la seguridad de la información de la entidad.
- Se requiere establecer un plan anual de capacitación, formación y sensibilización en seguridad de la información, con el objetivo de fortalecer la cultura de seguridad en los colaboradores y terceros que laboran para la entidad.

- Es necesario implementar un mecanismo que control de acceso de los dispositivos de la red de la entidad, con el objetivo de garantizar que solo puede acceder los dispositivos que autorizados.
- Se requiere implementar un mecanismo para el monitoreo de los LOGs de eventos de seguridad y las actividades que realizan los administradores sobre la plataforma de procesamiento.
- Es fundamental que el oficial de seguridad participa en los comités de cambios.
- La entidad no tiene establecidos los lineamientos para el uso aceptable de los activos de información asociados con la información e instalaciones de procesamiento de información, lo que genera que los usuarios desconozcan sus responsabilidades y consecuencia de sus acciones.

8. RECOMENDACIONES

La entidad requiere implementar una serie de controles con el objetivo de fortalecer su seguridad y poder dar cumplimiento a los requerimientos establecidos en la norma ISO 27001:2013, por eso es fundamental que lleven a cabo los diferentes planes de acciones que se definieron en el presente trabajo de grado.

Es necesario que la Dirección de Tecnología de la entidad revise su capacidad con el objetivo de garantizar la debida implementación de los controles y planes de acciones que se requieren llevar a cabo para cerrar las brechas encontradas producto de los diagnósticos realizados, ya que la mayoría de estos planes de acción requiere un componente tecnológico.

Es necesario que la entidad evalué la vialidad de algunos planes de acciones propuestos, debido a que su implementación demanda la adquisición de herramientas y/o soluciones tecnológicas que implica adelantar procesos de contratación para su adquisición. Algunas de las soluciones tecnológicas que se proponen, pueden llegar a tener un costo elevado y/o su implementación puede demandar un tiempo considerable.

Realizar campañas de seguridad de la información, con el propósito de poder generar un sentido de pertenencia y apropiación en temas de seguridad en cada uno de los funcionarios de la entidad, y concientizar sobre los riesgos que pueden afectar la seguridad de la información.

Por último, si no se consigue el compromiso demostrable de la Alta Directiva hacia la seguridad de la información, el autor considera que no es recomendable implementar en las organizaciones un Sistema de Gestión de Seguridad de la Información.

BIBLIOGRAFIA

[1] ICONTEC, NTC-ISO-IEC 27001, 2013.

[2] Ernst & Young, XV Encuesta Global de Seguridad de la Información de Ernst & Young, 2013. [En línea]. Available: http://www.ey.com. [Último acceso: 05 08 2015].

[3] ACIS, Tendencias 2014 Encuesta Nacional de Seguridad Informática, [En línea]. Available: http://acis.org.co/revistasistemas/index.php/component/k2/item/164-tendencias-2014-encuesta-nacional-de-seguridad-inform%C3%A1tica. [Último acceso: 10 06 2015].

[4] Asociación Española para la Calidad, [En línea]. Available: http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion. [Último acceso: 21 07 2015].

[5] Universidad Pedagógica Experimental Libertador, Manual de Tesis de Grado y Especialización y Maestría y Tesis Doctorales, 2002. [En línea]. Available: http://neutron.ing.ucv.ve/NormasUPEL2006.pdf. [Último acceso: 12 Agosto 2015].

[6] Gobierno en línea, ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES, [En línea]. Available: http://css.mintic.gov.co/ap/gel4/images/SeguridaddelaInformacion2_0_Anexo3_Estratificacion.pdf. [Último acceso: 12 Mayo 2015].

[7] Gobierno en Linea, MODELO DE SEGURIDAD DE LA INFORMACIÓN – SISTEMA SANSI - SGSI, 2008. [En línea]. Available: http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf. [Último acceso: 15 06 2015].

[8] Autorregulador del Mercado de Valores de Colombia AMV, Reglamento AMV, «www.amvcolombia.org.co,» 24 12 2009. [En línea]. Available: http://www.amvcolombia.org.co/attachments/data/20110214135739.pdf. [Último acceso: 10 05 2015].

[9] Superintendencia Financiera de Colombia, Circular Externa 052, 2007.

[10] Superintendencia Financiera de Colombia, Circular Externa 038, 2009.

[11] Congreso de la Republica, Ley Estatutaria 1266 de 2008, [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html.

[Último acceso: 10 Julio 2015].

[12] Congreso de Colombia, Ley Estatutaria 1581 de 2012, [En línea]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Último acceso: 10 Julio 2015].

[13] Presidente de la Republica, Decreto 1377 de 2013, [En línea]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646. [Último acceso: 10 Julio 2015].

[14] Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de seguridad y privacidad de la información, [En línea]. Available: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf. [Último acceso: 10 Julio 2015].

[15] Departamento Administrativo de la Función Pública (DAFP), Guía para la administración del riesgo, «portal.dafp.gov.co,» septiembre 2011. [En línea]. Available: http://portal.dafp.gov.co/portal/pls/portal/formularios.retrive_publicaciones?no=1592. [Último acceso: 10 2014].

[16] MINTIC, Guía: Gestión de Incidentes de Seguridad de la Información, «www.mintic.gov.co,» 2014. [En línea]. Available: http://www.mintic.gov.co/gestionti/615/articles-5482_Gestion_Incidentes.pdf. [Último acceso: 28 Agosto 2015].

[17] Centro Criptológico Nacional de España, GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-817), Agosto 2012. [En línea]. Available: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/817-Gestion_incidentes_seguridad/817-Gestion_incidentes_seguridad-ago12.pdf. [Último acceso: 4 Septiembre 2015].

[18] MINTIC, Formato e implementación de políticas de seguridad y privacidad de la información, [En línea]. Available: http://www.mintic.gov.co/gestionti/615/articles-5482_Implementacion_politicas.pdf. [Último acceso: 05 09 2015].

[19] Autorregulador del Mercado de Valores de Colombia AMV, Reglamento AMV, [En línea]. Available: http://www.amvcolombia.org.co/attachments/data/20110214135739.pdf. [Último acceso: 10 Julio 2015].

[20] Comisión Económica para América Latina y el Caribe, CEPAL, Metodología del marco lógico para la planificación, el seguimiento y la evaluación de proyectos y programas, «http://www.cepal.org/es,» [En línea]. Available: http://repositorio.cepal.org/bitstream/handle/11362/5607/S057518_es.pdf?sequence=1. [Último acceso: 4 Agosto 2014].

[21] Una metodología de evaluación de cadenas agro-alimenticias para la identificación de problemas y proyectos, Capitulo 5 - Identificar soluciones a los problemas, «http://www.fao.org,» [En línea]. Available: http://www.fao.org/wairdocs/x5405s/x5405s07.htm. [Último acceso: 10 Agosto 2014].

[22] ICONTEC, GUIA TECNICA COLOMBIA GTC-ISO/IEC 27035, 2012.

[23] iso27000.es, «ISO 27000.es,» [En línea]. Available: http://www.iso27000.es/sgsi.html. [Último acceso: 16 Junio 2015].

[24] DECEVAL, REGLAMENTO DEL SISTEMA DE REGISTRO DE DECEVAL, «www.deceval.com.co,» [En línea]. Available: https://www.deceval.com.co/portal/page/portal/Home/Marco_Legal/Reglamentos/Reglamento%20sist%20registro%2021%20de%20agosto%20de%202009.pdf. [Último acceso: 16 05 2015].

ANEXOS

ANEXO A. ENCUESTAS ESTRATIFICACION DE ENTIDADES

ANEXO B. EVALUACION CONTROLES ANEXO A ISO 27001-2013.

ANEXO C. ALCANCE POLITICAS Y OBJETIVO DEL SGSI

ANEXO D. METODOLOGIA DE GESTION DE RIESGOS

ANEXO E. CLASIFICACION ACTIVOS Y VALORACION DE RIESGOS

ANEXO F. MANUAL DE POLITICA SEGURIDAD DE LA INFORMACION

ANEXO G. PROCEDIMIENTO REPORTE Y ATENCION INCIDENTES DE SEGURIDAD