ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Sistemas de Información Gerencial

“Implementación de un marco de cumplimiento de la Norma ISO 27001:2013 para el proceso de Gestión de TI en una empresa familiar dedicada a la comercialización de productos para el hogar.”

TRABAJO DE TITULACIÓN

Previo a la obtención del grado de:

MAGÍSTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

ING. DIANA KARINA CÁRDENAS MARÍN

Guayaquil-Ecuador

AÑO: 2019

AGRADECIMIENTO

Agradezco en primer lugar a Dios por haberme puesto en el lugar y momento correctos para poder culminar mi maestría, a mis amados padres por su amor incondicional, a mis hermanos que me han apoyado siempre, a mi amado esposo que siempre ha estado conmigo apoyándome, que ha confiado en mis capacidades y por su paciencia y dedicación a nuestra familia y hacia el cuidado de nuestros pequeños Catalina y Mateo mientras yo me dedicaba a la elaboración de este trabajo de titulación, a mis amigas que han estado ahí cuando lo he necesitado y un agradecimiento especial a mi tutor el Ing. Lenin Freire por su guía a lo largo de toda la maestría.

DEDICATORIA

Dedico esta maestría a mis padres, hermanos y a mi amado esposo quienes desde un inicio me han apoyado y han creído en mí, quienes siempre han estado pendiente de la consecución de cada una de las metas que me he propuesto para aconsejarme y animarme a seguir.

Ing. Diana Karina Cárdenas Marín

TRIBUNAL DE SUSTENTACIÓN

PRESIDENTE DEL TRIBUNAL

Ph.D. CRISTINA L. ABAD R.

DIRECTOR DE TRABAJO DE TITULACIÓN

MSIG. LENIN E. FREIRE C.

MIEMBRO PRINCIPAL

MSIG. OMAR R. MALDONADO D.

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral."

ING. DIANA KARINA CÁRDENAS MARÍN

RESUMEN

La información es el activo más significativo de una empresa por lo que debe estar protegida bajo medidas de seguridad adecuadas para asegurar su confidencialidad, integridad y disponibilidad por lo que el concepto de seguridad de la información se torna prioritario. Más allá de la seguridad informática, la cual se enfoca en proteger los datos dentro de un sistema informático, se debe fomentar en la empresa una cultura de seguridad de la información cuyo ámbito es más amplio ya que la información en general puede generarse desde muchos contextos tanto internos como externos a la empresa.

La seguridad de los sistemas de la empresa, relacionada a las TICs, ha sufrido algunos ataques afectando, aunque no de forma grave, la confidencialidad de la información por lo cual el presente trabajo tiene como objetivo establecer y mantener un sistema de gestión que proporcione un enfoque estandarizado, documentado y continuo de los procesos, procedimientos y políticas de seguridad alineado a los requerimientos del negocio para elevar el nivel de madurez de la Seguridad de la Información.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

CIA: Confidencialidad, Integridad y Disponibilidad

CIS: Centro para la Seguridad en Internet (“Center for Internet Security”, en inglés)

CMM : Modelo de Madurez de Capacidades (“Capability Maturity Model” en inglés)

ERP: Planificación de Recursos Empresariales (“Enterprise Resource Planning” en inglés)

IEC: Comisión Electrotécnica Internacional

ISO: Organización Internacional de Normalización (“International Organization for Standardization”, en inglés)

KPI: Indicadores Claves de Desempeño (“Key Performance Indicators” en inglés)

KRI: Indicadores Claves de Riesgo (“Key Risk Indicators” en inglés)

OCDE: Organización para la Cooperación y el Desarrollo Económico

PEST: Político, Económico, Social y Tecnológico

PHVA: Planificar, Hacer, Revisar y Actuar

RFC: Solicitud de Cambio (“Request for Change” en inglés)

SGSI: Sistema de Gestión de la Seguridad de la Información

SLA: Acuerdo de Nivel de Servicio (“Service Level Agreement” en inglés)

SMART: Específico, Medible, Alcanzable, Orientado a resultados y A tiempo (“Specific, Measurable, Achievable, Result-oriented and Timely” en inglés)

TI: Tecnología de la Información

TIC Tecnologías de la Información y las Comunicaciones

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La implementación de un marco de referencia de la norma ISO/IEC 27001-2013 presenta diversos beneficios a una organización ya que existe una responsabilidad sobre los datos que ésta gestiona y primordialmente está que para el cumplimiento de los objetivos de negocio se debe asegurar la confidencialidad, integridad y disponibilidad de la información tanto de colaboradores como de personas externas relacionadas.

La norma ISO/IEC 27001-2013 permite realizar un análisis de la situación actual de la seguridad de la información de la empresa y además permite identificar y minimizar las amenazas y vulnerabilidades propias de los activos de información por medio de controles propuestos por la norma que ofrecen un lineamiento en relación a mejores prácticas de seguridad.

La evaluación de riesgos que se incluye en la norma ISO/IEC 27001-2013 es el análisis que señalará los controles a aplicar, las acciones y tratamientos a realizar y los objetivos a cumplir; por lo tanto es esencial para que el Sistema de Gestión de Seguridad de la Información sea realmente valioso para la empresa.

CAPÍTULO 1

GENERALIDADES DE LA EMPRESA

1.1 RESEÑA HISTÓRICA

En el año 1943, Comercializadora CC fue fundada por el Sr. Domingo Salame Hidrovo como una opción para poder comprar a crédito tanto artículos para el hogar como para uso personal ya que en aquella época dichos artículos solamente se vendían al contado. El primer local de la empresa se ubicó en un mezzanine de las calles Aguirre y Pedro Carbo, Guayaquil, Ecuador. El primer lema publicitario que utilizó Comercializadora CC fue “Solicítenos un crédito y compre a precios de contado”.

En el año 1967, por disposición del Sr. Domingo Salame Hidrovo, se construyó en Ecuador el primer edificio especialmente diseñado para almacenes por

departamentos; éste edificio se ubicó en la esquina de las calles Luque y Escobedo en la ciudad de Guayaquil.

En año 1978 comenzaron los planes de consolidación administrativa, expansión y modernización para lo cual se instalaron los sistemas de computación y se creó el área de Recursos Humanos. Para esa época Comercializadora CC ya contaba con dos locales, uno en Guayaquil y otro en Quito.

En el año 1997 se fundó en la ciudad de Nueva York, en el distrito de Queens la compañía americana Comercializadora CC The Gallery USA Inc. la cual brinda el servicio, a los ecuatorianos residentes en esa ciudad y alrededores en Estados Unidos, de escoger y pagar por electrodomésticos en el exterior y Comercializadora CC entrega en Ecuador dichos bienes.

En el año 2002 se publicó el sitio web www.creditoseconomicos.com para brindar un mejor servicio de compra a los ecuatorianos tanto en Ecuador como fuera del país. Ese mismo año fue lanzada al mercado la primera tarjeta de crédito para la compra de electrodomésticos llamada Credicard.

En el año 2004 un estudio realizado por la consultora Datanalisis determinó que Comercializadora CC era considerada por los ecuatorianos como su empresa favorita para la adquisición de electrodomésticos. [1]

1.2 MISIÓN

Mejorar la vida de nuestros clientes: acompañándolos en los momentos más trascendentales, brindado una experiencia de compra memorable a través de soluciones efectivas y siendo socialmente responsables. [1]

1.3 VALORES CORPORATIVOS

A continuación se presentan los valores corporativos de la empresa que la distinguen de otras del sector:

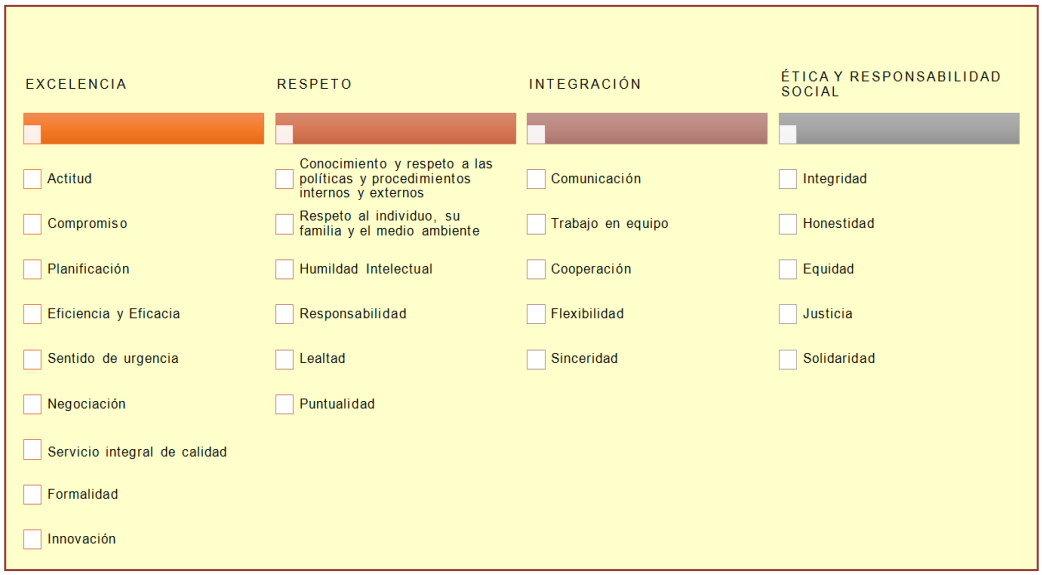

Figura 1.1: Valores Corporativos de Comercializadora CC

1.4 ACTIVIDADES

Comercializadora CC participa activamente en la comercialización de marcas propias e importadas de electrodomésticos para el hogar, además posee las siguientes líneas de negocio:

- **Dismayor**: Realiza la importación y comercialización de electrodomésticos para mayoristas.
- **Asistencia Facilita**: Comercializa la venta de seguros contras riesgos sobre los productos que comercializa a través de la página web y sus tiendas.
- **Multinova**: Se dedica a la comercialización de electrodomésticos del hogar a través de distribuidores independientes que reciben comisiones por ventas realizadas.
- **La Garantía**: es un servicio que consiste en cubrir los defectos de fábrica de los aparatos una vez que se concluya la garantía del fabricante al repararlos o reemplazarlos durante el periodo de contrato.

1.5 ORGANIGRAMA GENERAL

A continuación se presenta la estructura organizacional de la empresa en donde se detallan los diferentes departamentos y relaciones jerárquicas:

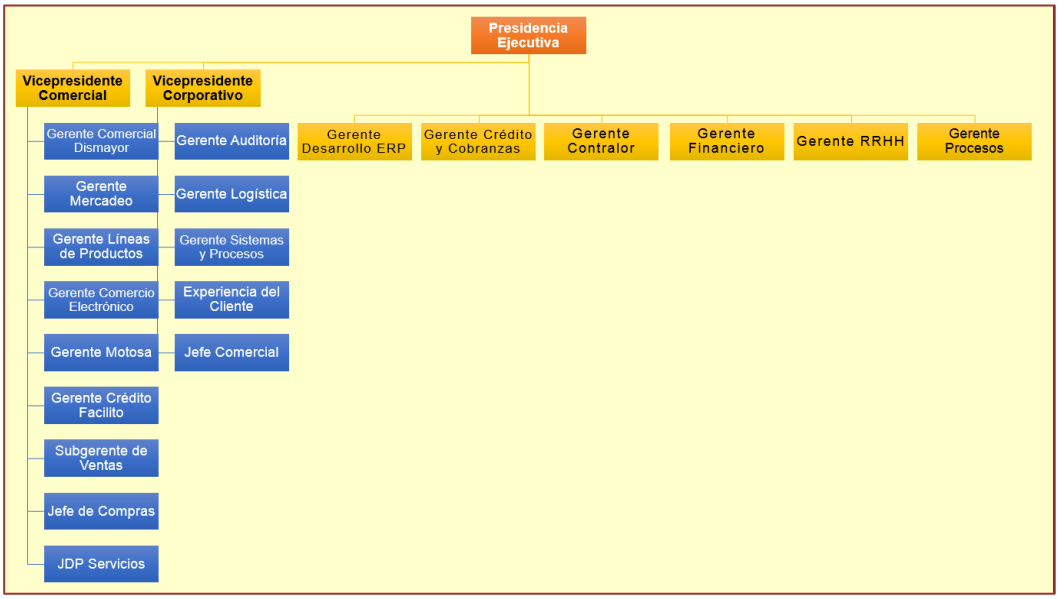

Figura 1.2: Organigrama General de la Empresa

1.6 DESCRIPCIÓN DEL PROBLEMA

Debido a la cultura de seguridad de la información elemental y a un esquema de seguridad lógica básica, la empresa ha sufrido ciertos incidentes relacionados a los servicios de TI como divulgación de información afectando la confidencialidad de la información, acceso a sitios no autorizados e infección por malware; que aunque no tuvieron un impacto mayor, generaron preocupación en la alta gerencia y con ello surgió el planteamiento de crear un Área de Seguridad de la Información que ayude a proteger los procesos de la empresa, en especial los que conforman la cadena de valor, de tal forma que no se vea afectada la continuidad del negocio.

1.7 SOLUCIÓN PROPUESTA

El Área de Seguridad de la Información diseñará e implementará un marco de cumplimiento de la Norma ISO 27001:2013 para la Gestión de TI sobre los procesos de la cadena de valor, para lo que se realizará una evaluación del análisis de brechas elaborado previamente por el área de Auditoría Interna de la empresa.

Paralelamente se evaluarán los controles de seguridad críticos que ofrece el framework CIS para la defensa cibernética que brindan formas específicas para detener los ataques contra la seguridad de la información.

Luego, se identificarán los principales riegos que afectan directamente los procesos de la cadena de valor para establecer la estrategia a aplicar a cada uno, se definirán actividades y sus responsables para así poder disminuir la probabilidad o el impacto; a éste esquema se le denomina tratamiento de riesgo con lo que se elaborará un plan que debe contar con la aprobación y compromiso de la dirección para poder implementar los controles planificados.

1.8 OBJETIVO GENERAL

Implementar un marco de cumplimiento de la Norma ISO 27001:2013 para la Gestión de TI sobre los procesos de la cadena de valor de una empresa comercializadora con la finalidad elevar el nivel de madurez de la Seguridad de la Información.

1.9 OBJETIVOS ESPECÍFICOS

- Establecer y mantener un sistema de gestión que proporcione un enfoque estandarizado, documentado y continuo de los procesos, procedimientos y políticas de seguridad alineado a los requerimientos del negocio.
- Implementar y mantener 5 de los 20 controles fundamentales que el framework CIS recomienda para asegurar un nivel de seguridad aceptable a lo largo de la empresa.
- Asegurar que los diferentes niveles de acceso a las aplicaciones, bases de datos, sistemas operativos; así como también los parámetros de configuración de seguridad estén apropiadamente implementados.
- Definir el mapa documental sobre el cual se diseñará e implementará el marco de cumplimiento de la Norma ISO 27001:2013 en la empresa.
- Elaborar el plan de trabajo para la implementación del Sistema de Gestión de la Seguridad de la Información adoptando como marco de referencia la Norma ISO 27001:2013.

CAPÍTULO 2

MARCO TEÓRICO

2.1 ESTRUCTURA DE ALTO NIVEL Y LAS NORMAS ISO

La Estructura de Alto Nivel es un modelo normalizado, establecido para preparar el sistema de redacción de las normas de gestión ISO. Se trata de un denominador común, establecido por parte del Comité ISO, para que todas las nuevas normas de gestión, respeten y compartan un objetivo común: la uniformización de las normas de gestión y con ella se puede:

- Sincronizar diferentes normas.

- Adoptar un lenguaje común, para facilitar que las organizaciones integren diferentes Sistemas de Gestión y puedan disfrutar de algunas ventajas añadidas, como puede ser, la eliminación de la duplicidad documental. [2]

La estructura de alto nivel procura llevar a cabo cierta coherencia o sincronización de todas las normas ISO con independencia del ámbito de cada norma. Además, implanta un conjunto de términos y definiciones comunes a todas ellas, para que a las organizaciones les sea mucho más fácil implementar de forma correcta los sistemas de gestión. [3]

La estructura de alto nivel define conceptos comunes a todas las normas ISO como pueden ser: el riesgo, la gestión documental, partes interesadas, contexto, entre otros. La uniformidad de todas las normas ISO no sólo es útil para las organizaciones que quieren implementar un sistema de calidad, sino también lo es para otros agentes que participan en el proceso.

La Estructura de Alto Nivel, consta de una estructura general común (Índice), con títulos de capítulos idénticos y con el mismo número de artículos que establece:

- Similar descripción introductoria para artículos.
- Similar título para requisitos idénticos.
- Terminología común y definiciones principales.

La finalidad de la normalización es promover la coincidencia entre las normas de sistemas de gestión para permitir su integración e implementación en las empresas.

También facilita el trabajo para los auditores. Esto se debe a que siempre deberán auditar un mismo conjunto de requisitos que serán comunes con independencia de la naturaleza de la norma en que se debe auditar.

Por otro lado, la Organización Internacional para la Estandarización (ISO) busca internamente con esta estructura, asegurar la calidad en la producción de normas, para que sean documentos coherentes que perduren en el tiempo, en toda clase de empresas, de todos los tamaños, en cualquier sector y en todos los entornos. La Estructura de Alto Nivel se encuentra seccionada de la siguiente manera:

0. Introducción
1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora

La expectativa de la ISO es asegurar que las normas que desarrolla ofrezcan una gran flexibilidad para su aplicación en las empresas y éstas mantengan la

capacidad para afinar los sistemas de gestión incluso de una forma superior a la norma propiamente dicha.

2.2 PRINCIPIOS DE GESTIÓN DE LA NORMA ISO

Los principios de gestión deberían utilizarse por la alta dirección con la determinación de encaminar una organización hacia la mejora en el desempeño.

De forma general se cree que los principios corresponden a buenas intenciones, que son deseables, pero difícil medir si efectivamente se aplican; ante esto, se revela que es totalmente realizable estimar de forma operativa si los principios se están usando en la empresa e incluso se puede medir y auditar el resultado de su aplicación.

La determinación de la aplicación de los principios se realiza por medio de la ejecución de acciones concretas que los soporten y/o de la evaluación del provecho logrado por la empresa durante sus operaciones. [4]

La gestión de la Norma ISO está basada en 8 principios que se detallan a continuación:

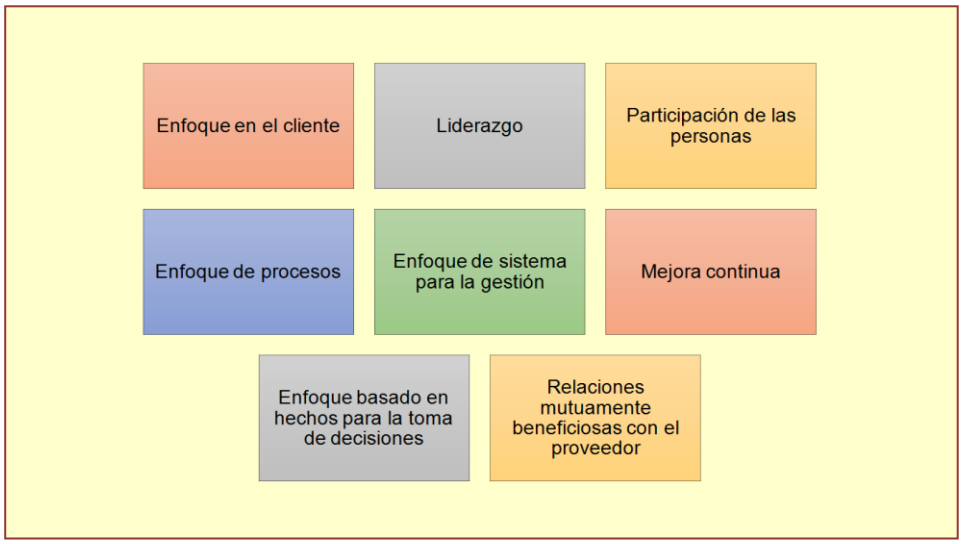

Figura 2.1: Principios de gestión de la Norma ISO

2.2.1 Enfoque en el cliente

Las organizaciones dependen de sus clientes y por lo tanto deberían comprender sus necesidades actuales y futuras, satisfacer sus requisitos y esforzarse en exceder las expectativas del cliente.

Implicaciones para el sistema de gestión

- Indagar y entender las exigencias y perspectivas del cliente.
- Garantizar que el propósito de la organización esté unido a las exigencias y perspectivas del cliente.
- Informar las exigencias y perspectivas del cliente a toda la empresa.
- Gestionar de forma sistemática las relaciones con el cliente.
- Garantizar el equilibrio entre la satisfacción del cliente y demás partes interesadas.

2.2.2 Liderazgo

Los líderes son aquellos capaces de movilizar a un conglomerado hacia la consecución de un fin común y establecer el curso de la organización. Éstos deberían establecer y conservar un ambiente interno en el cual la gente se involucre íntegramente en la consecución de los objetivos de la organización.

Implicaciones para el sistema de gestión

- Tomar en cuenta las exigencias de las partes interesadas como son los clientes, propietarios, empleados, proveedores y financistas.
- Construir una clara visión del futuro de la empresa.
- Fijar objetivos y metas retadores.
- Establecer y conservar los valores, la imparcialidad y la ética de trabajo a nivel de toda la organización.
- Instaurar la confianza y suprimir el miedo.
- Ofrecer a las personas las herramientas, la formación y la libertad para proceder responsablemente.
- Infundir, estimular y reconocer las aportaciones de las personas.

2.2.3 Participación de las personas

El recurso humano a cualquier nivel es el alma de una organización y el hecho de estar totalmente comprometido permite que sus competencias sean empleadas en beneficio de la organización.

Implicaciones para el sistema de gestión

- Las personas conocen su rol dentro de la organización y cuán importante es su contribución.
- Las personas reconocer los factores que impiden su desempeño.
- Las personas reconocen los problemas que son de su propiedad y se responsabilizan por su resolución.
- Las personas se proponen metas y objetivos personales y evalúan su cumplimiento.
- Las personas buscan de forma activa ocasiones para mejorar destrezas, habilidades y experiencia.
- Las personas comparten libremente conocimientos y experiencia.
- Las personas deliberan de forma abierta dilemas y asuntos varios.

2.2.4 Enfoque de procesos

Un resultado deseado se alcanza eficientemente cuando las actividades y los recursos relacionados se gestionan como un proceso.

Implicaciones para el sistema de gestión

- Definir de forma sistemática las tareas necesarias para alcanzar el resultado deseado.
- Establecer una responsabilidad clara y rendir cuentas acerca de la gestión de las tareas primordiales.
- Analizar y medir la amplitud de las tareas primordiales.

- Determinar las interrelaciones de las tareas primordiales entre las funciones de la organización.
- Enfocarse en factores como recursos y métodos que permitirán una mejora en las tareas clave de la organización.
- Evaluar los riesgos, las consecuencias y el impacto de las tareas en las partes interesadas.

2.2.5 Enfoque de sistema para la gestión

Para lograr la eficacia y eficiencia de la organización en la consecución de objetivos se debe identificar, entender y gestionar como un sistema todos los procesos interrelacionados.

Implicaciones para el sistema de gestión

- Disponer de un sistema para que la organización alcance sus objetivos de manera eficaz y eficiente.
- Entender la interdependencia de los procesos del sistema.
- Enfoque estructurados que permite enlazar e integrar los procesos.
- Proveer de un mejor entendimiento de las funciones y responsabilidades necesarias para la consecución de objetivos comunes.
- Entender la capacidad de la organización y establecer sus limitaciones en cuanto a recursos antes de la acción.
- Estudiar y definir la forma en que se debe realizar las tareas específicas dentro de un sistema.

- ➲ Buscar la mejora continua del sistema por medio de la medición y evaluación.

2.2.6 Mejora continua

La mejora continua en el desempeño de toda la organización es un objetivo fijo de la organización.

Implicaciones para el sistema de gestión

- ➲ Utilizar a lo largo de toda la organización un enfoque que sea consistente con la mejora continua en el desempeño de la organización.
- ➲ Brindar a las personas la formación necesaria en cuanto a métodos y herramientas para la mejora continua.
- ➲ Lograr que la mejora continua en productos, procesos y sistemas se convierta en un objetivo para cada persona de la organización.
- ➲ Fijar metas para guiar la mejora continua y adoptar medidas para realizar su seguimiento.

2.2.7 Enfoque basado en hechos para la toma de decisiones

Mediante el análisis de datos e información se pueden tomar decisiones eficaces.

Implicaciones para el sistema de gestión

- Garantizar que los datos y la información sean adecuados en cuanto a precisión y fiabilidad.
- Lograr que los datos sean alcanzables para las personas que lo requieran.
- Por medio de métodos válidos, realizar un análisis de los datos y de la información.
- Tomar decisiones y adoptar medidas en base al análisis de los eventos, la experiencia acumulada y la perspicacia.

2.2.8 Relaciones beneficiosas con el proveedor

En toda negociación lo que se busca son los mejores resultados para las partes involucradas, es decir, un acuerdo ganar-ganar. Es por esto que tanto empresas como proveedores se necesitan y mientras más beneficiosa es la relación más valor se crea.

Implicaciones para el sistema de gestión

- En las relaciones que se creen se debe equilibrar la ganancia teniendo las consideraciones a corto y largo plazo.
- Proveedores estratégicos deben ser identificados y seleccionados.
- Debe existir comunicación transparente y sincera.
- Participar de la información y proyectos futuros.
- De forma conjunta fijar tareas para la mejora y el desarrollo. [5]

2.3 DOMINIOS DE SEGURIDAD DE LA NORMA ISO 27001:2013

La implementación de un Sistema de Gestión de la Seguridad de la Información basada en la Norma ISO/IEC 27001-2013 se recomienda para que una organización logre llevar el control de toda la información generada.

La Norma ISO/IEC 27001-2013 presenta a todas las organizaciones una referencia para lograr la implementación, y ayuda a éstas últimas a controlar y evaluar la exposición ante posibles riesgos de la información mediante la aplicación de controles mitigantes.

El objetivo de la Norma ISO/IEC 27001-2013 es proteger la información de una empresa, brindando la certeza de que aún en situaciones de riesgo habrá continuidad en la prestación de servicios.

Los dominios de la Norma ISO/IEC 27001-2013 que son evaluados a continuación:

2.3.1 Dominio de la política de seguridad

Su objetivo es garantizar a la empresa el soporte y gestión necesarios para la seguridad de la información según todos los requisitos institucionales y normativos. Se debe establecer la política de seguridad según los objetivos fijados por la empresa y para ello se debe contar con el compromiso en lo relacionado a la seguridad de la información.

2.3.2 Dominio de la organización en cuanto a seguridad de la información

Su finalidad es instaurar un marco de referencia para definir el camino para la implantación y control de la seguridad de la información dentro de la empresa. La dirección de la empresa es la responsable de establecer la política de seguridad, además debe establecer los roles de los comités y nombrar al encargado mediante una resolución. El encargado debe coordinar y revisar el proceso.

2.3.3 Dominio de gestión de activos

Este dominio tiene el objetivo de llevar a cabo una protección adecuada en cuanto a los activos de la empresa. En todo momento los activos se encuentran inventariados y controlados por un responsable que también se encarga de manipularlos de forma correcta.

2.3.4 Dominio de seguridad de los recursos humanos

Su objetivo es fijar las medidas necesarias para controlar la seguridad de la información que ha sido manejada por los recursos humanos de la empresa.

2.3.5 Dominio en cuanto la seguridad física y del medio ambiente

Con este dominio se consigue proteger todas las instalaciones de la empresa y toda la información que maneja. Por esto, se establecen diferentes barreras de seguridad y controles de acceso.

2.3.6 Dominio gestión de las comunicaciones y operaciones

El objetivo se encuentra en determinar los procesos y responsabilidades de las operaciones que lleva a cabo la organización. Se debe asegurar que todos los procesos se encuentren relacionados con la información ejecutada de forma adecuada.

2.3.7 Dominio control de acceso

Se asegura el acceso autorizado a todos los sistemas de información de la empresa. Es necesario realizar diversas acciones como controles para evitar el acceso de usuarios no autorizados, controles de entrada, entre otros.

2.3.8 Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información

Este dominio se encuentra dirigido a aquellas empresas que desarrollen software internamente o que tenga un contrato con otra empresa que se encarga de desarrollarlo. Se tienen que establecer los requisitos en la etapa de implantación y desarrollo de software para que sea seguro.

2.3.9 Dominio de gestión de incidentes en la seguridad de la información

El objetivo es asegurar la continuidad operativa de la empresa. Se requiere aplicar controles que eviten o reduzcan todos los incidentes de las actividades desarrolladas por la empresa que puedan generar un impacto.

2.3.10 Dominio de la gestión de continuidad del negocio

Tiene como objetivo garantizar la continuidad de las operaciones de la organización para lo cual se aplican controles que eviten o minimicen los incidentes en las actividades desempeñadas por la empresa y que puedan originar un impacto.

2.3.11 Dominio de cumplimiento

Su propósito es garantizar que los requisitos legales en cuanto a seguridad y que están relacionados al diseño y gestión de los sistemas de información se cumplan. [6]

2.4 VENTAJAS DE LA NORMA ISO 27001

La aplicación de la Norma ISO/IEC 27001-2013 presenta, entre otras, las siguientes ventajas que se exponen a continuación:

Figura 2.2: Ventajas de la aplicación de la Norma ISO 27001

2.4.1 Mejora de la Seguridad

- Mejora general de la efectividad de la seguridad de la información.
- La norma cubre tantos aspectos tecnológicos de la seguridad como seguridad física, corporativa, entre otros.
- Revisión independiente del sistema de gestión de seguridad de la información.
- Mejor concienciación de la seguridad de la información.
- Mecanismos para evaluar la eficacia del sistema de gestión.

2.4.2 Buena gobernanza

- Concienciación y empoderamiento del personal en lo referente a la seguridad de la información.
- Disminución de riesgos de demandas legales en contra de la alta dirección en virtud de los principios de “Due diligence” y “buena fe”.
- Oportunidad de identificar los puntos débiles del SGSI y proporcionar correcciones.
- Aumento de la rendición de cuentas de la alta dirección en lo que referente a la seguridad de la información.

2.4.3 Conformidad

- Con otras normas ISO.
- Con la Organización para la Cooperación y el Desarrollo Económico.
- Con los estándares de la industria del sector.
- Con las leyes nacionales y regionales.

2.4.4 Reducción de Costos

- Los tomadores de decisiones frecuentemente preguntan para justificar la rentabilidad de los proyectos y exigen beneficios de retornos concretos y medibles y en base en esto, un nuevo concepto de evaluación financiera ha surgido para tratar lo relacionado al terreno de la seguridad de la información. El Retorno de la Inversión en Seguridad (ROSI) es un concepto derivado de Retorno de la Inversión (ROI). Se puede interpretar como la ganancia financiera

del proyecto de seguridad teniendo en cuenta su costo total en un periodo determinado de tiempo.

2.4.5 Marketing

- La diferenciación proporciona una ventaja competitiva para la organización.
- Satisfacción de las necesidades de los clientes y/u otras partes interesadas.
- Consolidación de la confianza de los clientes, proveedores y asociados de la organización. [7]

2.5 PRINCIPIOS BÁSICOS DE LA SEGURIDAD DE LA INFORMACIÓN

Cuando se habla de seguridad de la información, es importante conocer el término CIA (Confidencialidad, Integridad, Disponibilidad), que presenta los principios básicos de la seguridad de la información. [8]

Realizar una correcta gestión de la seguridad de la información establece como principio básico que sin los tres elementos mencionados nada seguro existe, con que solo falle uno de los componentes se encontrará ante un peligro para la seguridad de la información.

Se tiene que recordar que ningún sistema de seguridad es completamente seguro, siempre se debe tener claro que un sistema es mucho más vulnerable de lo que se piensa.

Es necesario tener en cuenta las causas de los riesgos y la posibilidad de que ocurran fallos. Una vez que se tiene esto claro, es posible tomar las medidas necesarias para conseguir un sistema menos vulnerable.

A continuación se aclaran cada uno de los puntos que forman la CIA:

2.5.1 Confidencialidad

La confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando una laptop con información sensible sobre una empresa es robada, cuando se divulga información confidencial a través del teléfono, entre otros. Todos estos casos pueden constituir una violación de la confidencialidad.

2.5.2 Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

La integridad también es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada, para salvaguardar la precisión y completitud de los recursos.

La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra datos importantes que son parte de la información.

La integridad garantiza que los datos permanezcan inalterados, excepto cuando sean modificados por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad.

2.5.3 Disponibilidad

Es la característica, cualidad o condición de la información para encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

La seguridad tiene como objetivo resguardar la confidencialidad, integridad y disponibilidad de la información, por lo tanto, se tiene que aplicar de forma efectiva en toda la cadena. [9]

2.6 ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

Las normas ISO/IEC 27000 son modelos de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y por la Comisión Electrotécnica Internacional (IEC).

La lista contiene las mejores prácticas recomendadas en cuanto a seguridad de la información para desarrollar, implementar, mantener y mejorar especificaciones de Sistemas de Gestión de la Seguridad de la Información (SGSI) e incluye:

ISO/IEC 27000 – comprende el vocabulario utilizado por las normas de la familia. Es semejante a un diccionario que explica los términos de todas las normas de la lista.

ISO/IEC 27001 – establece los requisitos para implementar un SGSI. Ésta norma es la única certificable de la familia y está conformada por una parte principal relacionada al ciclo de mejora continua y por un anexo en el que se precisan los lineamientos generales de los controles propuestos por el estándar.

ISO/IEC 27002 – es un compendio de buenas prácticas de la Seguridad de la Información que detalla los controles y sus respectivos objetivos. El estándar comprende 14 dominios, 35 objetivos de control y 114 controles.

ISO/IEC 27003 – es una guía en la implementación de un SGSI y se utiliza como soporte a la norma 27001 en donde se indican las directivas generales para la correcta implementación de un SGSI.

ISO/IEC 27004 – detalla recomendaciones para realizar mediciones de la gestión de la Seguridad de la Información. Detalla la configuración de métricas, objetivos de medición, frecuencia de medición, formas de medición y la consecución de objetivos.

ISO/IEC 27005 – detalla la forma de iniciar la gestión de los riesgos de seguridad de la información que puedan comprometer a una empresa. Una metodología de análisis y gestión de riesgos en concreto no se indica pero se proporcionan ejemplos.

ISO/IEC 27006 – comprende los requisitos que las organizaciones certificadoras requieren para obtener la acreditación.

ISO/IEC 27007 – corresponde a un manual para auditar SGSIs y todo lo relacionado al qué y cuándo auditar, la asignación adecuada de auditores, el plan de la auditoría y demás actividades clave. [10]

2.7 DEFINICIÓN DE SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI) corresponde a un planteamiento sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una empresa para que ésta logre conseguir sus objetivos de negocio.

Aunque de forma generalizada se piensa que la administración de información es un tema que le compete exclusivamente a empresas relacionadas de forma directa con datos, esto no es correcto ya que cada empresa posee información que le aporta valor indistintamente del origen o formato.

Por lo tanto, un SGSI es un conjunto de mejores prácticas que están orientadas a asegurar la seguridad, la integridad y la confidencialidad de ésta información. Al igual que ocurre con cualquier sistema, un SGSI se debe implementar estratégicamente para que se logren los propuestos.

Otros elementos que las organizaciones deben tener presente durante la implementación son:

- Obtener el apoyo y el compromiso de la alta dirección ya que debe presentarse como el patrocinador de la difusión, la gestión y el seguimiento del proceso.
- La definición del alcance es primordial ya que se deben establecer los objetivos que tendrá el SGSI y los beneficios que le proporciona a la empresa.

- La capacitación del capital humano de una empresa debe ser parte activa del proceso por lo que debe recibir la formación respectiva.
- El SGSI se centra en la administración de riesgos asociados a la gestión de la información propia de cada empresa con respectivas particularidades.
- Como en todo sistema de gestión debe existir el compromiso de adoptar la mejora continua para el SGSI que se implemente. [11]

2.8 ENFOQUE EN LOS PROCESOS

A continuación se detalla la estrategia de gestión de procesos que utiliza la Norma ISO/IEC 27001-2013:

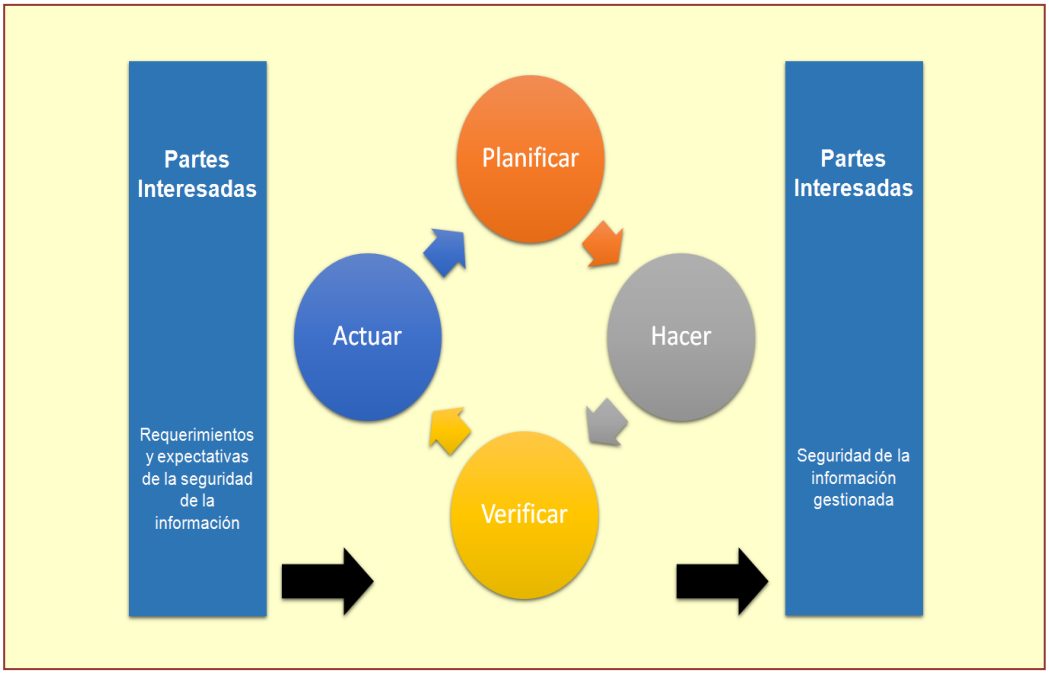

Figura 2.3: Enfoque en Procesos

El modelo de proceso PHVA (“Planificar – Hacer – Verificar – Actuar”) es aplicado en esta norma. En la Figura 2.3 se aprecia la forma en que un sistema de gestión toma como información de entrada los requisitos y expectativas de las partes interesadas a los cuales se aplican las acciones y procesos y como resultado se obtiene un SGSI que cumple con los requisitos y expectativas.

- **Planificar (establecer el sistema de gestión):**

  Aquí se detalla la base documental relacionada con la administración de riesgos y la mejora de la seguridad de la información y además se provee resultados alineados con los objetivos organizacionales.

- **Hacer (implementar y operar el sistema de gestión):**

  En esta etapa se realiza la implementación y operación de la política, los controles, los procesos y los procedimientos del sistema de gestión.

- **Verificar (monitorear y revisar el sistema de gestión):**

  Corresponde a la etapa de evaluación y si el caso lo amerita se realiza la medición del proceso en relación a la política.

- **Actuar (mantener y mejorar el sistema de gestión):**

  Implica las acciones correctivas y preventivas, en base de los resultados de la auditoria interna y revisión por la dirección.

La definición de procesos establece que corresponde a un grupo de tareas relacionadas entre sí ejecutadas para alcanzar un objetivo definido. Para que una empresa actúe de manera eficaz, debe implementar y gestionar numerosos

procesos interrelacionados e interactivos. De forma general, el elemento de salida de un proceso corresponde directamente el elemento de entrada del siguiente proceso. A La gestión ordenada de los procesos empresariales y la interacción de estos procesos se denomina “enfoque basado en procesos”.

CAPÍTULO 3

INICIO DEL SGSI

3.1. METODOLOGÍA DE IMPLEMENTACIÓN DEL SGSI

La metodología de implementación del SGSI está basada en los componentes del Ciclo PDCH (Plan - Do - Check - Act) el cual es un modelo de mejora continua. A continuación se detallan las actividades a realizar por cada etapa del ciclo:

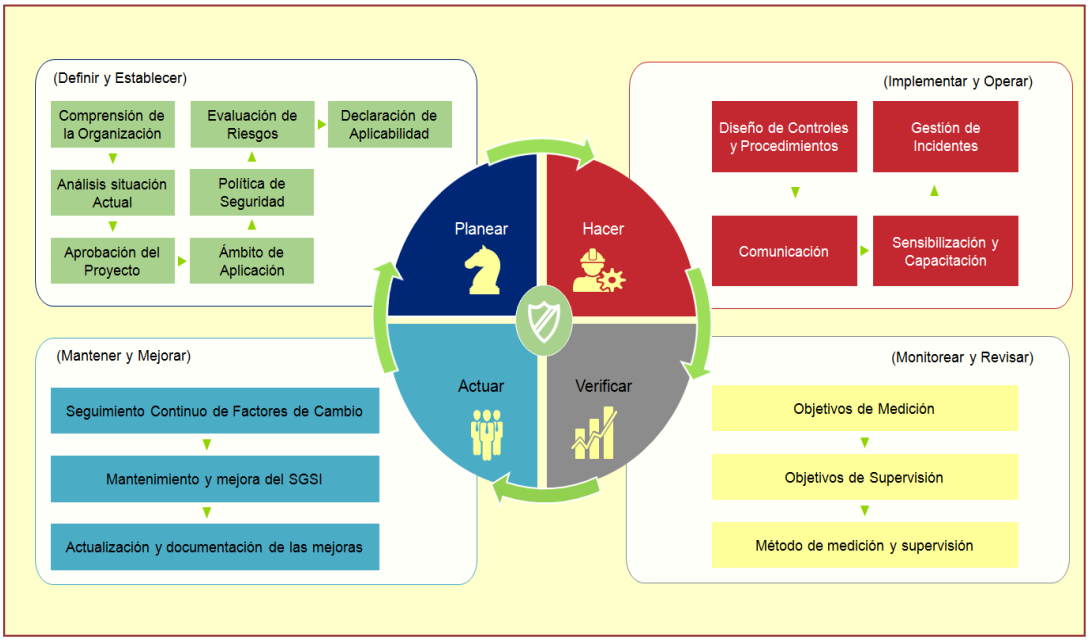

Figura 3.1: Metodología de Implementación del SGSI

3.2. COMPRENSIÓN DE LA ORGANIZACIÓN

Comercializadora CC busca una gestión de seguridad de la información que le posibilite disminuir el impacto y la ocurrencia de aquellos riesgos que puedan derivar en una pérdida en la confidencialidad, integridad y disponibilidad de sus activos críticos.

Es así que como paso inicial se identificarán y analizarán diversos componentes de la Organización; el resultado permitirá lo siguiente:

- Conocer la Organización y su entorno.
- Reunir la información necesaria para planificar la gestión de la seguridad de la información.
- Asegurar que los objetivos de la seguridad de la información están alineados con los objetivos de negocio de la Organización.

3.3. ALINEAMIENTO ESTRATÉGICO

Para realizar el alineamiento estratégico entre la gestión de la seguridad de la información y la organización se utilizará el Diagrama Causa-Efecto que permite realizar una representación de varios elementos, a continuación se detallan los pasos y consideraciones que se deben de seguir para realizar el análisis:

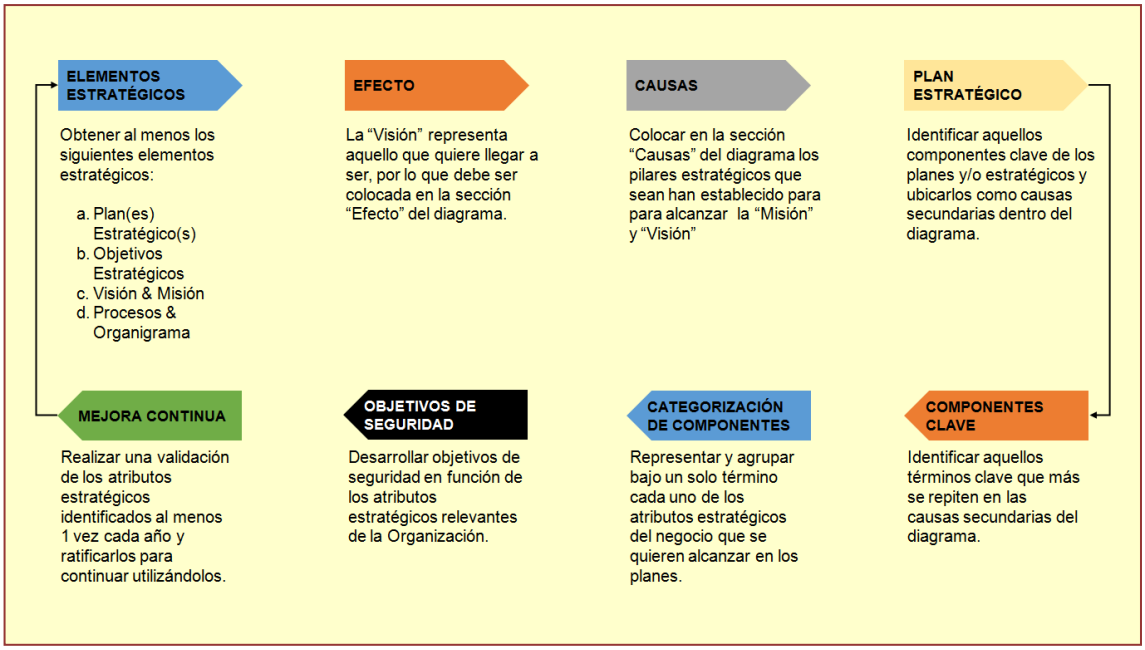

Figura 3.2: Alineamiento Estratégico

3.4. ATRIBUTOS ESTRATÉGICOS

Una vez aplicada la metodología de alineamiento estratégico se identificaron los componentes que requieren ser garantizados a través de la gestión de la seguridad de la información que son más relevantes para alcanzar la "Misión", "Visión" y "Objetivos" de la Organización, a continuación se muestran los resultados:

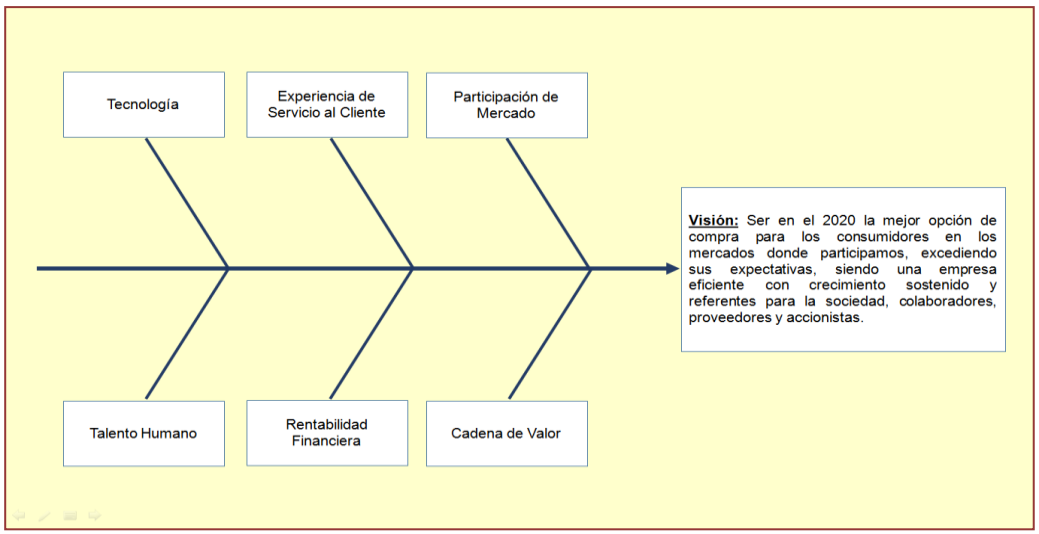

Figura 3.3: Atributos Estratégicos

3.5. ANÀLISIS DEL ENTORNO EXTERNO E INTERNO

Para identificar los factores que pueden afectar a la empresa en cuanto a su entorno externo se realizó un análisis PEST que se presenta a continuación:

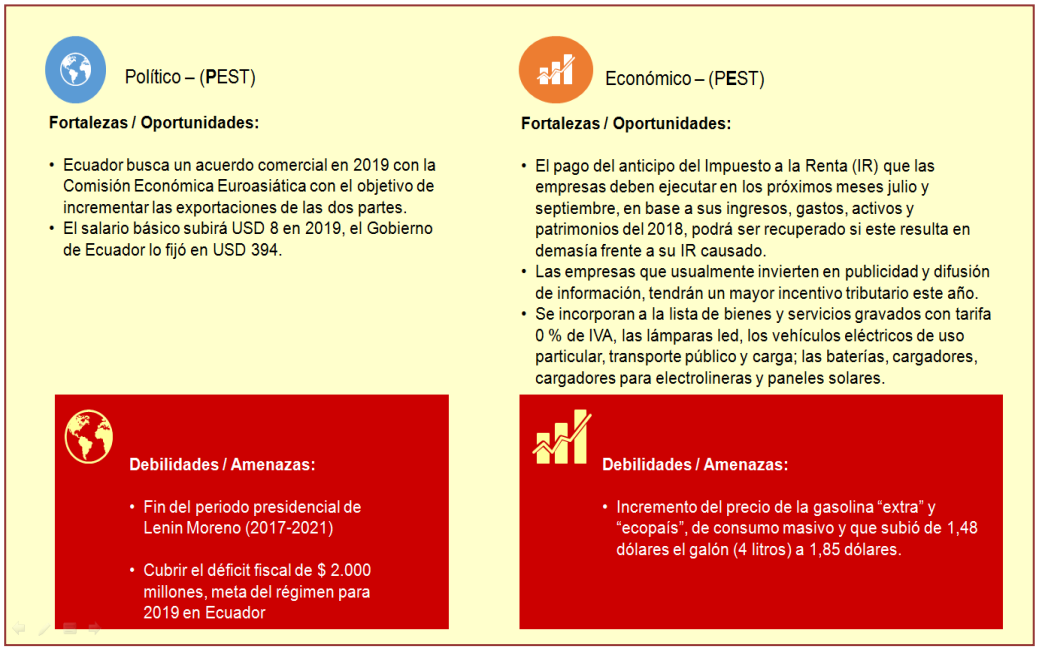

Figura 3.4: Análisis Político y Económico

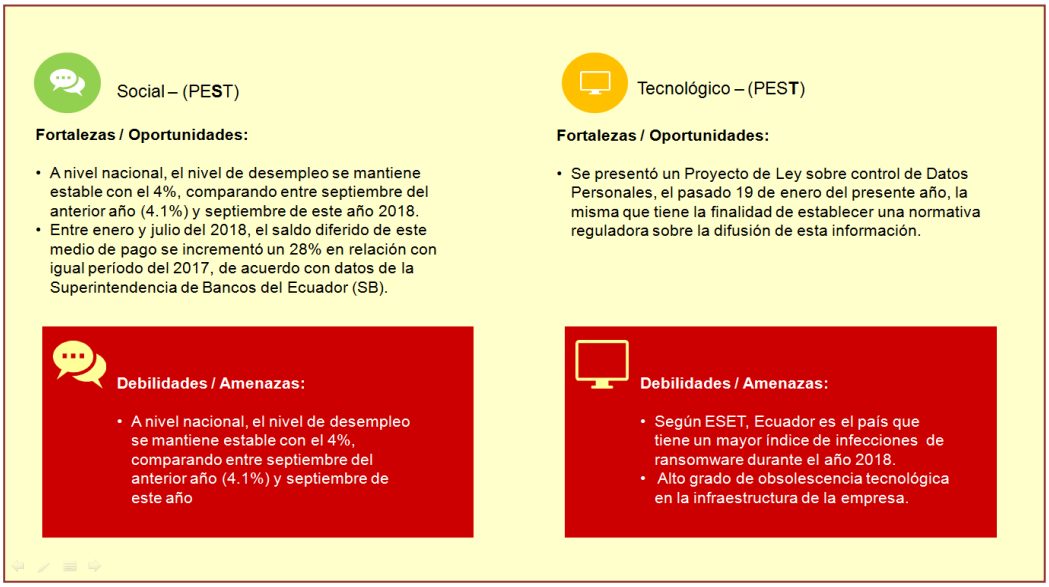

Figura 3.5: Análisis Social y Tecnológico

Para el análisis del entorno interno se consideró la estructura organizacional clasificando las áreas en cuanto a su nivel estratégico, de gobierno y operacional como se muestra a continuación:

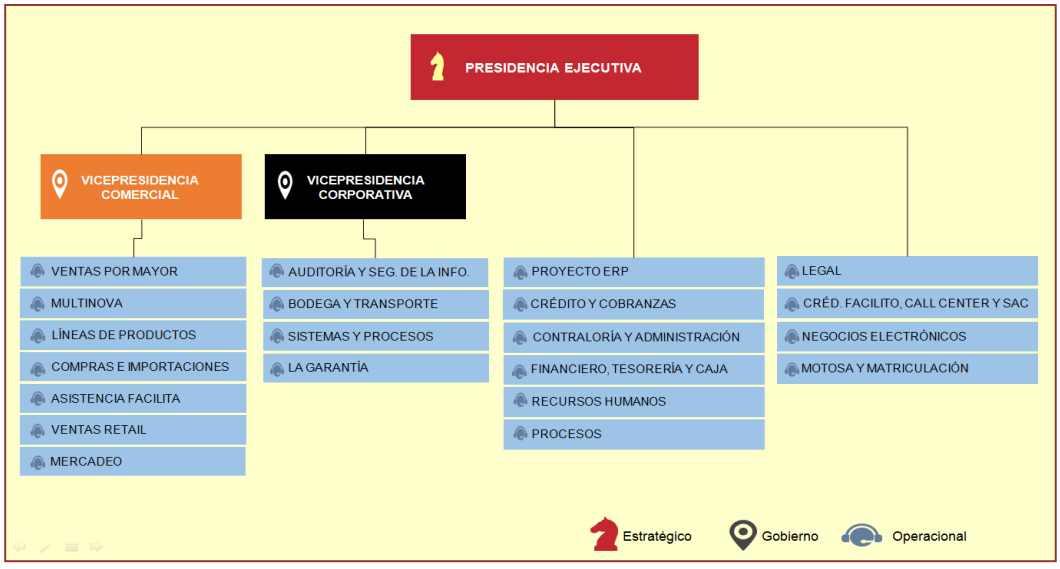

Figura 3.6: Estructura Organizacional Clasificado

3.6. PROCESOS

En la Figura 3.7 se presentan los macro procesos de la empresa, tanto los principales (Cadena de Valor) como los secundarios:

Figura 3.7: Macro procesos

3.7. DETERMINACIÓN Y ANÁLISIS DE PARTES INTERESADAS, REQUISITOS Y EXPECTATIVAS

Para el SGSI de Crédito Económicos, las partes interesadas pertinentes están constituidas por los proveedores, los clientes, los empleados y la alta gerencia. A continuación se exponen con detalles, las partes interesadas con las respectivas necesidades especificadas:

Proveedores

Requisitos

- Cooperación.
- Información.
- Comunicación.

- Sensibilizar y culturizar a nuestros proveedores para proteger toda la cadena de la información que maneja la empresa.

Expectativas

- Mantener cierto nivel de seguridad de la información en toda la empresa.
- Promover en la empresa la creación e integración de esquemas de atención de incidentes de seguridad.
- Asegurar la confidencialidad, integridad y disponibilidad de la información que se intercambia entre la empresa y los proveedores durante el cumplimiento de las obligaciones contractuales de estos últimos.
- Minimizar los riesgos por pérdida o uso indebido de la información cumpliendo con las políticas de la empresa.
- Mayor compromiso por parte de todos los proveedores garantizando el buen uso de la información de la empresa.

Clientes

Requisitos

- Monitorear la satisfacción del cliente.

Expectativas

- Mejorar en la organización la capacidad de satisfacer a sus clientes.
- Contar con información actualizada pertinente a los clientes.

Empleados

Requisitos

- Formalizar y socializar políticas, procedimientos y documentación del SGSI.
- Garantizar la seguridad de la información que se gestiona y almacena en los sistemas de información y/o equipos de la empresa.

- Prevenir fuga o pérdida de información.
- Asegurar la confidencialidad, la disponibilidad e integridad de datos.
- Fortalecer el acompañamiento frente la implementación del SGSI.
- Socializar consejos sobre seguridad de la información para la protección de los activos de información.

Expectativas

- Fortalecer permanentemente las políticas del SGSI y buenas prácticas en el uso de las TICs para beneficio de los usuarios.
- Lograr que los colaboradores adopten buenas prácticas que permitan garantizar la confidencialidad, seguridad y acceso a la información.
- Minimizar los riesgos por pérdida o uso indebido de la información cumpliendo con las políticas establecidas.

Alta gerencia

Requisitos

- Notificar a la empresa la relevancia de alcanzar los objetivos de seguridad de la información.
- Proveer con recursos para el desarrollo, implementación, operación, monitoreo, revisión, mantenimiento y mejora del SGSI.
- Decidir los criterios para aceptar el riesgo.

Expectativas

- Contar con políticas en donde se especifiquen las expectativas de seguridad en la empresa.
- Que los colaboradores tengan la motivación necesaria para cumplir con las políticas de seguridad de la empresa.

- ➲ Que los colaboradores cuenten con un alto nivel de conocimientos en seguridad dentro de su responsabilidad o rol.

3.8. DETERMINACIÓN DE OBJETIVOS

Una vez identificados los aspectos estratégicos del negocio se determinaron los objetivos estratégicos de la seguridad de la información que se muestran a continuación:

Tabla 1: Objetivos estratégicos de la Seguridad de la Información

ATRIBUTO ESTRATÉGICO	OBJETIVO
TECNOLOGÍA	MANTENER LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE PUEDAN AFECTAR EL CUMPLIMIENTO REGULATORIO POR DEBAJO DEL 3% SOBRE EL TOTAL DE INCIDENTES REGISTRADOS EN UN AÑO CALENDARIO.
TALENTO HUMANO	ASEGURAR QUE AL MENOS EL 90% DE COLABORADORES ESTÉ ADECUADAMENTE CAPACITADA EN LOS CONCEPTOS DE INTEGRIDAD, CONFIDENCIALIDAD Y PRIVACIDAD Y QUE SEAN CONSCIENTES DE SU ROL Y RESPONSABILIDAD SOBRE LA INFORMACIÓN DE LA EMPRESA.
EXPERIENCIA DE SERVICIO AL CLIENTE	ASEGURAR QUE LA INFORMACIÓN PROCESADA, TRANSMITIDA Y ALMACENADA PARA PRESTAR SERVICIOS DE FINANCIAMIENTO SEA UTILIZADA SALVAGUARDANDO SU CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD Y QUE DICHOS INCIDENTES NO SOBREPASEN EL 10% SOBRE EL TOTAL DE INCIDENTES REGISTRADOS EN UN AÑO CALENDARIO.

3.9. RECOPILACIÓN DE LA INFORMACIÓN

Para construir un conocimiento detallado del sistema de gestión existente y determinar el estado actual, se debe seleccionar el método de recolección de información. Las acciones utilizadas en este proyecto fueron las siguientes:

- Revisión de documentos con información de los controles de seguridad:
  - Procedimientos.
  - Informes de seguridad.
  - Procesos de gestión de la seguridad.
- Entrevistas individuales con responsables de seguridad de la información y personas que manejan las operaciones diarias relacionadas con controles de seguridad:
  - Oficial de Seguridad.
  - Jefe de Infraestructura.
  - Administrador de Centro de Cómputo.
  - Administrador de Base de Datos.
  - Jefe de Desarrollo.
  - Gerente de Sistemas.
  - Gerente de Recursos Humanos.
- Revisión de resultados de auditorías internas:
  - Informe de Auditoría de Tesorería.
  - Informe de Auditoría de Infraestructura Tecnológica.
  - Evaluación de Nivel de Madurez.

3.10. NIVEL DE MADUREZ

Al igual que cualquier otro sistema de gestión ISO, la Norma ISO/IEC 27001:2013 tiene una cláusula de mejora continua y esto se debe a que ningún proceso puede mantener altos niveles de rendimiento sin que se realicen ajustes continuamente para adaptarse a los cambios que se presentan y dado que la cláusula de la norma no profundiza en el tema pero sí es obligatorio, es necesario basarse en modelos de madurez. [12]

Un modelo de madurez es un marco sistemático con niveles estructurados que describe cómo los aspectos bien definidos de una organización pueden producir resultados confiables y sostenibles. Existen varios modelos pero el utilizado para evaluar el nivel de madurez de la seguridad de la información de la empresa es el CMM (Capability Maturity Model). [13]

El Modelo de Madurez de Capacidades es una metodología que describe una trayectoria evolutiva de cinco niveles de procesos cada vez más organizados y sistemáticamente más maduros.

En la Figura 3.8 se muestra gráficamente la interpretación de los niveles de madurez definido por el estándar ISO de modelos de madurez:

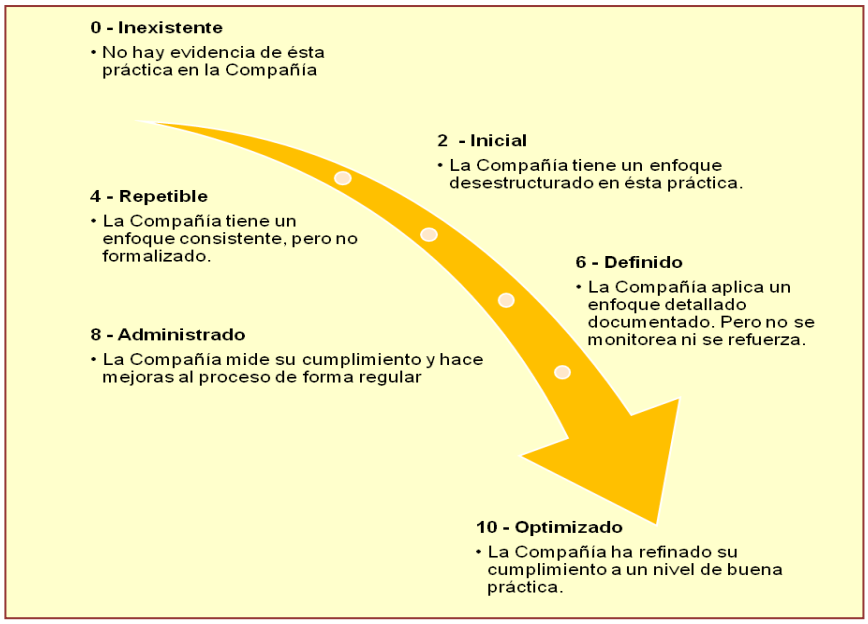

Figura 3.8: Nivel de Madurez

3.11. ANÁLISIS DE BRECHAS

El análisis de brechas es una técnica para conocer la situación actual de la seguridad de la información de la empresa frente a los controles de referencia detallados en la Norma ISO/IEC 27001 numerales 5 a 18 y de ésta manera determinar las acciones necesarias para pasar a un estado futuro deseado. A continuación se presenta la Tabla 2 con el nivel de cumplimiento alineado al Modelo de Madurez de Capacidades:

Tabla 2: Nivel de Cumplimiento

Nº	Dominio de la Norma	Inicial
5	A.5 Política de Seguridad de la Información	6
6	A.6 Organización de la Seguridad de la Información	6
7	A.7 Seguridad en Recursos Humanos	6
8	A.8 Gestión de Activos	4
9	A.9 Acceso Lógico / Control de Accesos	6
10	A.10 Criptografía	2
11	A.11 Seguridad Física y Ambiental	3
12	A.12 Seguridad en las operaciones	4
13	A.13 Seguridad de las Comunicaciones	3
14	A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	2
15	A.15 Relación con Proveedores	2
16	A.16 Gestión de Incidentes de Seguridad de la Información	4
17	A.17 Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio	3
18	A.18 Cumplimiento con Requerimientos Legales y Contractuales	1
Nivel de Cumplimiento		**4**

Figura 3.9: Evaluación de la Seguridad de la Información

En el Anexo “A” se encuentra el análisis de brecha detallado y en el Anexo “B” el análisis del Nivel de Madurez de la Seguridad de la Información.

3.12. RESULTADOS DE LA EVALUACIÒN

En base en el análisis de brechas y a la evaluación del nivel de madurez se concluye que la empresa tiene un enfoque desestructurado de las prácticas de seguridad de la información. A continuación se detallan los puntos críticos identificados en la evaluación:

- **Gestión de activos de Información**
  - No se encuentran identificados los activos de información manejados por área.
  - No se encuentra formalmente identificado los propietarios de activos de información.
  - No se ha definido formalmente la regla de uso aceptable de información en base a su criticidad.
  - No se evidenció una política o práctica clara en cuanto al retorno de activos informáticos.
  - Los activos de información no se encuentran clasificados y etiquetados según su nivel de confidencialidad.
  - Si bien es cierto existe una política de protección de medios extraíbles, el mismo presenta deficiencias que pueden anular dicho control.
  - No se elimina la información contenida dentro de los computadores previos a la chatarrización.
- **Seguridad en RRHH**
  - Comprobación de antecedentes únicamente se hace para posiciones de Jefatura y posiciones con manejo de dinero.
  - No se evidencia capacitaciones periódicas respecto a la Seguridad de la Información.
  - No se evidencia canales de reporte para incidentes de Seguridad de la Información.

- **Criptografía**
  - Ausencia de políticas y procedimientos de controles criptográficos.
  - No existe definición de qué información deberá ser cifrada.
- **Legales y contractuales**
  - Identificación de la legislación aplicable a las políticas de Seguridad de la Información.
  - Delimitación de derechos de propiedad intelectual.
  - Revisiones independientes de Seguridad de la Información.
- **Otros puntos identificados en la evaluación**
  - Políticas de Seguridad de Información desactualizadas.
  - Falta de revisión de segregación de funciones en los perfiles de usuarios.
  - No se involucra a Seguridad de la Información en el ciclo de vida de los proyectos de TI.
  - No se revisa periódicamente derechos de acceso de usuarios a Sistemas y recursos de TI.
  - Deficiencias en la gestión de contraseñas del core empresarial.
  - Ausencia de canales de comunicación para la gestión de incidentes de Seguridad de Información.

CAPÍTULO 4

PLANIFICACIÓN DE LA IMPLEMENTACIÓN DEL SGSI

4.1. INVENTARIO Y CLASIFICACIÓN DE ACTIVOS

El proceso que se desea asegurar es el de Gestión de TI en lo que concierne al apoyo principalmente de los procesos de la cadena de valor de la empresa. Para este efecto se han identificado los activos críticos de información los cuales se los ha categorizado en:

Software: aplicaciones, base de datos, Sistemas operativos, sistemas de información, sistemas de toma de decisiones, ERPs, software de equipos de redes, software de equipos de telecomunicaciones, etc.

Hardware: servidores, dispositivos, equipos de comunicación, equipos de redes etc.

Información Física: políticas, procedimientos, manuales, reglamentos y registros, en formato físico.

Información Digital: políticas, procedimientos, manuales, reglamentos y registros, en formato electrónico.

Personal: personal clave que desempeñe o acumule conocimientos especializados.

Instalación: la infraestructura -centro de cómputo y el acceso de las Instalación-Edificio Administrativo y almacenes.

Servicios: corresponde a servicios brindados a la empresa por terceros (proveedores entre otros). [15]

En el Anexo “C” se detalla el inventario de Activos de Información. A continuación se presenta la cantidad de activos de información identificados por tipo:

Tabla 3: Activos por Tipo

Tipo de Activo	Cantidad
(SW) Software	36
(ID) Información	13
(HW) Hardware	8
(PE) Personal	4
(IN) Instalaciones	2
(SR) Servicios	2
Total Activos	**65**

4.2. VALORACIÓN DE ACTIVOS

Una vez realizado el levantamiento del inventario de activos de información basado en la Norma ISO 27001-2013, se procede a realizar la clasificación y valoración con respecto a la confidencialidad, disponibilidad e integridad de acuerdo a los siguientes niveles:

Tabla 4: Valoración de Activos

Confidencialidad		Disponibilidad		Integridad		Importancia	
1	No Aplica	1	No Aplica	1	No Aplica	1	No Aplica
2	Pública	2	Muy Bajo	2	Muy Bajo	2	Muy Bajo
3	Uso Interno	3	Bajo	3	Bajo	3	Bajo
4	Uso Restringido	4	Medio	4	Medio	4	Medio
5	Confidencial	5	Alto	5	Alto	5	Alto
6	Secreto	6	Crítico	6	Crítico	6	Crítico

Tabla 5: Importancia de Activos

Valoración Cuantitativa	Valoración Cualitativa	Descripción
1	No Aplica	No aplica el criterio de importancia para el activo.
2	Muy Bajo	El activo no afecta procesos.
3	Bajo	El activo puede afectar una tarea aislada de la operación o del proceso. Las pérdidas o afectación serían menores y no incurrirían en sanciones pecuniarias.
4	Medio	El activo puede afectar de forma parcial una operación o un proceso. Las pérdidas o afectación pueden ser moderadas.
5	Alto	Uno o varios procesos pueden ser seriamente afectados. Las pérdidas o afectación causan sanciones.
6	Crítico	La organización se ve seriamente afectada y puede generar sanciones elevadas y afectar la credibilidad de la organización y sus procesos.

En el Anexo “D” se presenta el inventario de activos de información consolidado, con su respectiva categorización y valoración con respecto a la confidencialidad, disponibilidad e integridad.

4.3. IDENTIFICACIÓN DE AMENAZAS

Con la información recopilada se pudo identificar cualitativamente la probabilidad de ocurrencia de las amenazas y el impacto de las mismas por cada activo y tipo de activo; el detalle se encuentra en el Anexo “E”.

4.4. ANÁLISIS DE RIESGOS

Un estudio realizado en el año 2018 por la firma Deloitte a 50 empresas nacionales y multinacionales de diversas industrias reveló las siguientes situaciones:

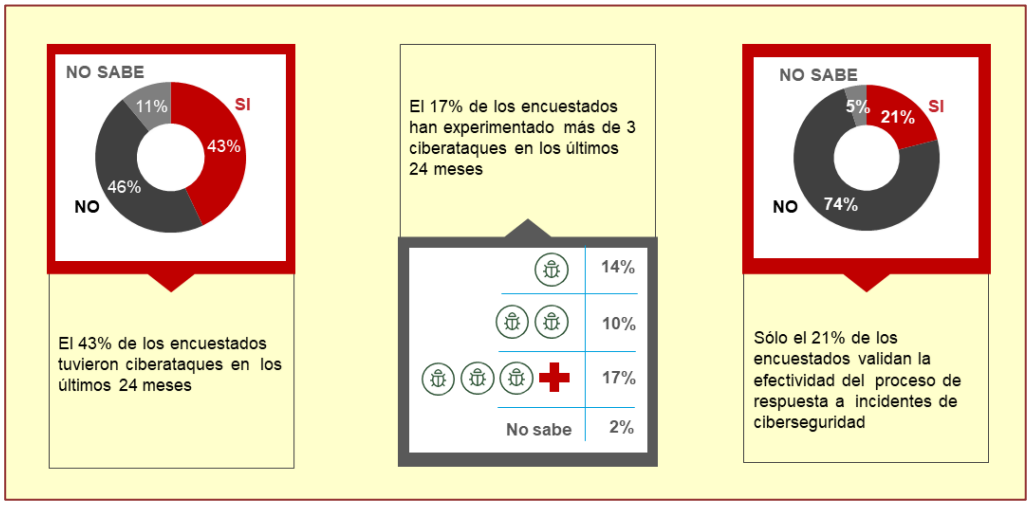

Figura 4.1: Estudio de Ataques

Según el estudio las principales deficiencias de control relacionadas con la seguridad de la información son las siguientes:

- Administración ineficiente de parámetros de seguridad.
- Fallas en el proceso de gestión de accesos y asignación de perfiles de usuarios.
- Fallas en el proceso de gestión de cambios a aplicaciones.
- Inadecuada configuración de log de auditoria.

Identificación de riesgos

La identificación del riesgo se realiza mediante el siguiente proceso:

1. Identificación de Amenazas o fuentes de Riesgo (Deliberadas, Accidentales, Entorno).
2. Identificación de las Vulnerabilidades.
3. Valoración de las Consecuencias.

Determinación del Riesgo

El riesgo se calcula multiplicando la valoración de la probabilidad por el nivel de impacto, es decir la estimación del riesgo se realiza con base en el resultado de estos dos valores.

4.4.1. Matriz de evaluación de riesgos

El análisis y diagnósticos de los riesgos dan como resultado la matriz de riesgos detallada en Anexo “F”, obtenidos con respecto a la probabilidad de ocurrencia; los criterios de valoración son los siguientes:

Tabla 6: Probabilidad de Ocurrencia

Valor Cualitativo	Valor Cuantitativo	Probabilidad
Casi seguro	5	Se espera que el evento ocurra en la mayoría de las circunstancias. Más de 1 vez al año.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias. Al menos 1 vez en el último año.
Posible	3	El evento podría ocurrir en algún momento. Al menos 1 vez en los últimos 2 años.
Improbable	2	El evento puede ocurrir en algún momento. Al menos 1 vez en los últimos 5 años.
Raro	1	El evento puede ocurrir solo en circunstancias excepcionales. No se ha presentado en los últimos 5 años.

Tabla 7: Impacto o Efecto

Valor Cualitativo	Valor Cuantitativo	Impacto
Catastrófico	5	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.
Mayor	4	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
Moderado	3	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
Menor	2	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
Insignificante	1	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.

En base a los criterios establecidos, la matriz para valoración de riesgos es la siguiente:

Tabla 8: Probabilidad e Impacto de Riesgo

Probabilidad	Impacto - Consecuencia				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Raro	Bajo	Bajo	Moderado	Alto	Alto
Improbable	Bajo	Bajo	Moderado	Alto	Extremo
Posible	Bajo	Moderado	Alto	Extremo	Extremo
Probable	Moderado	Alto	Alto	Extremo	Extremo
Casi Seguro	Alto	Alto	Extremo	Extremo	Extremo

4.4.2. Evaluación de riesgos

De acuerdo al análisis de las amenazas y vulnerabilidades se realizó la matriz de riesgos dando como resultados lo que se detalla a continuación:

Tabla 9: Resultados de Matriz de Riesgos

Tipo Activo	Tipo	Riesgo			
		Bajo	Moderado	Alto	Extremo
Hardware	I	16	8	40	16
	R	24	16	40	
Información	I		39	104	39
	R	52	13	117	
Instalaciones	I	2		6	6
	R	2	6	6	
Personal	I	4	12	8	4
	R	12	8	8	
Servicios	I	2	6	12	2
	R		10	12	
Software	I		36	216	144
	R	108	216	72	
Total Riesgos	I	24	101	386	211
	R	198	269	255	0

4.4.3. Tratamiento de riesgos

Una vez elaborado la matriz de riesgos en la cual se ha identificado y valorado los riesgos que afectan los objetivos de la Institución, se procederá a realizar la evaluación de los controles de la Norma ISO 27001-2013, que deberán ser implementados para el tratamiento de Riesgos.

Las acciones del tratamiento de riesgo por su naturaleza será Mitigar, Aceptar, transferir o eliminar, en la siguiente tabla se detalla la definición de las acciones del tratamiento de riesgos:

Tabla 10: Tratamiento de Riesgos

Acción	Definición
Reducir	Reducir/Minimizar/Eliminar la ocurrencia o afectación de un riesgo.
Aceptar	Aceptar la ejecución de un riesgo el mismo que el impacto en la institución no una mayor afectación.
Transferir	Compartir la responsabilidad del riesgo a terceros que contaran con los medios necesarios para tratar el riesgo.
Evitar	Acabar/eliminar la ocurrencia y ejecución de un riesgo, generalmente son las más costosas.

4.4.4. Asignación de controles

Los controles a implementarse para minimizar los riesgos, se detallan en el Anexo “G” los cuales se encuentran clasificados según el sub-proceso al que se relacionan.

4.5. DECLARACIÓN DE APLICABILIDAD

Este paso tiene como objetivo la definición de las acciones a realizar para mitigar los riesgos que han sido identificados y analizados. Para tal objeto se base en un documento que es un requisito del estándar ISO/IEC 27001:2013 que enlista los controles de seguridad establecidos en su Anexo A.

Para complementar los controles establecidos en el estándar ISO/IEC 27001:2013 se los ha combinado con los Controles CIS que son un conjunto completo de buenas prácticas de seguridad cibernética, desarrollado por expertos en TI para tratar con las amenazas y vulnerabilidades de seguridad más comunes. En la figura a continuación se ha realizado una agrupación de los controles CIS según su nivel de aplicabilidad:

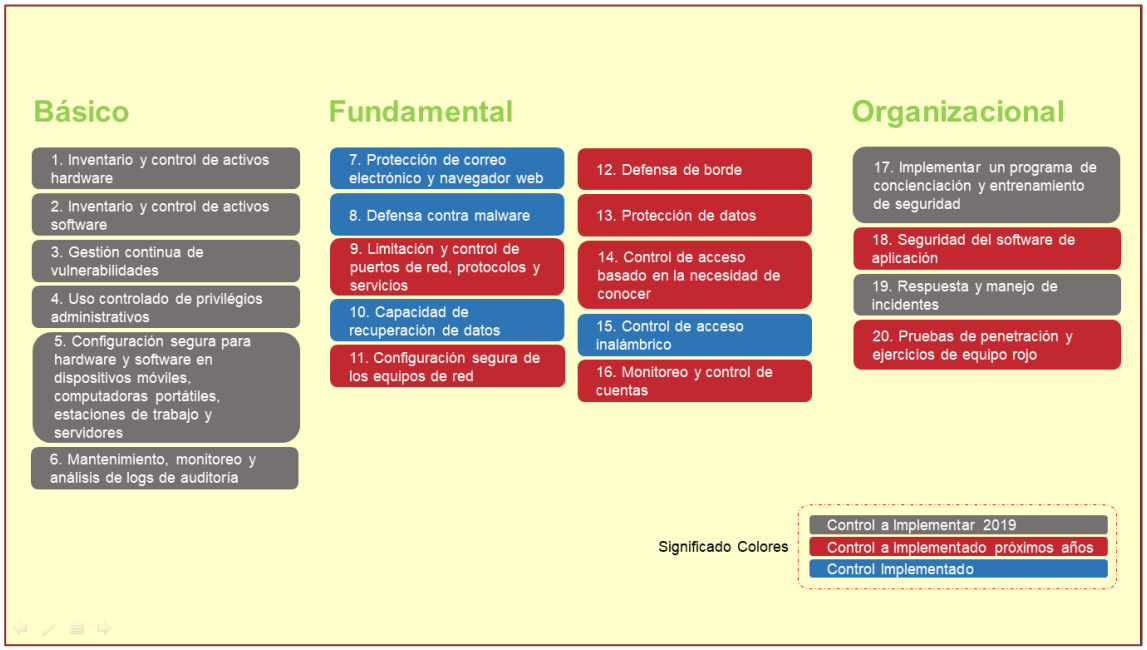

Figura 4.2: Controles CIS

En el Anexo “H” se detallan los controles del Anexo A de la Norma ISO/IEC 27001:2013 que se aplican a la empresa.

4.6. DEFINICIÓN DEL ALCANCE DEL SGSI

El alcance del SGSI se basa en el plan de trabajo presentado en la sección anterior el cual se ha diseñado para dar cumplimiento a los dominios del estándar ISO/IEC 27001:2013.

Para la determinación de los límites y la aplicabilidad del SGSI se ha establecido una diferenciación de los aspectos estratégicos correspondientes a la Seguridad de la Información y de los aspectos tácticos correspondientes a la Seguridad Informática tal como se presentan a continuación:

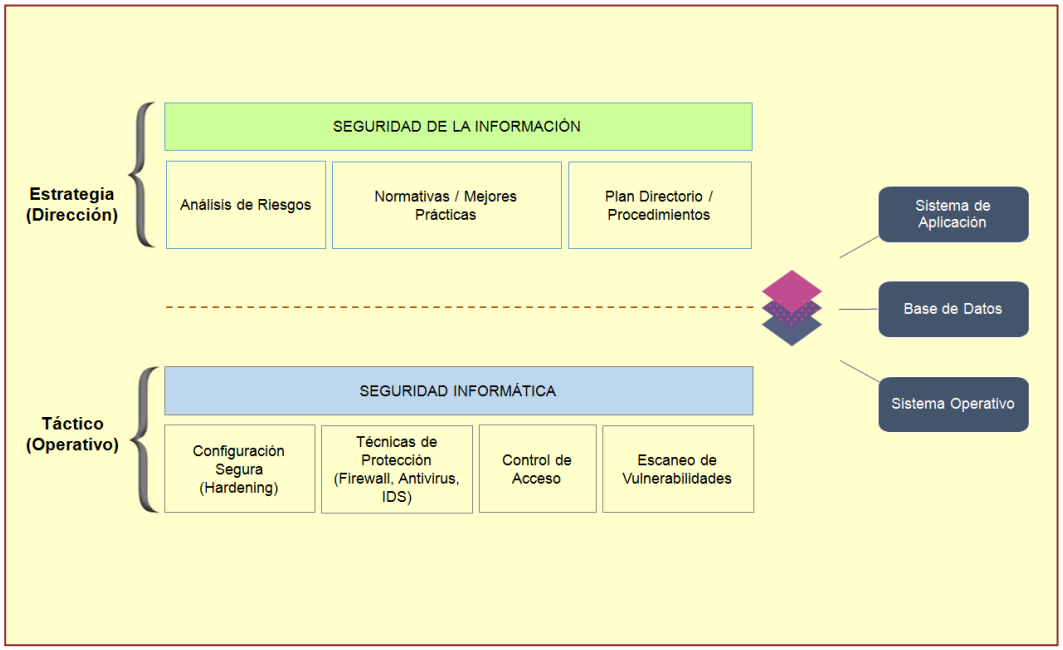

Figura 4.3: Límites del SGSI

Se ha realizado un análisis de las actividades que lleva a cabo tanto el Departamento de Sistemas como el Departamento de Seguridad de la Información para poder separarlas y establecer el alcance que tendrá el SGSI en la empresa. A continuación se presenta la Figura 4.4 que detalla el alcance actual de las mencionadas áreas y posteriormente la Figura 4.5 con el detalle del alcance propuesto:

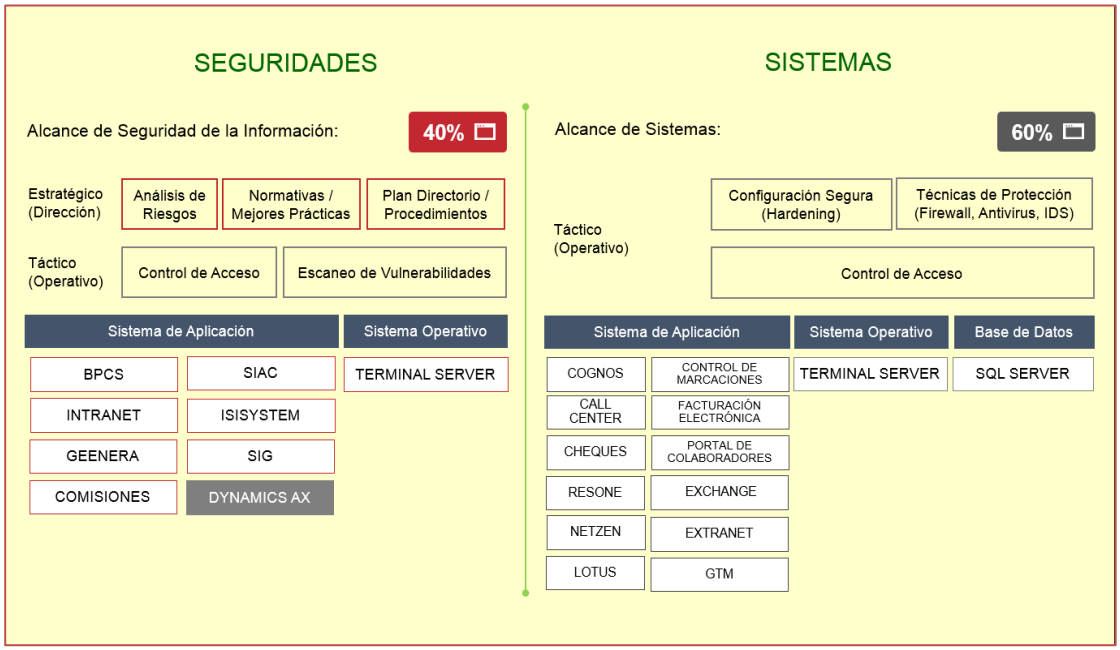

Figura 4.4: Alcance Actual

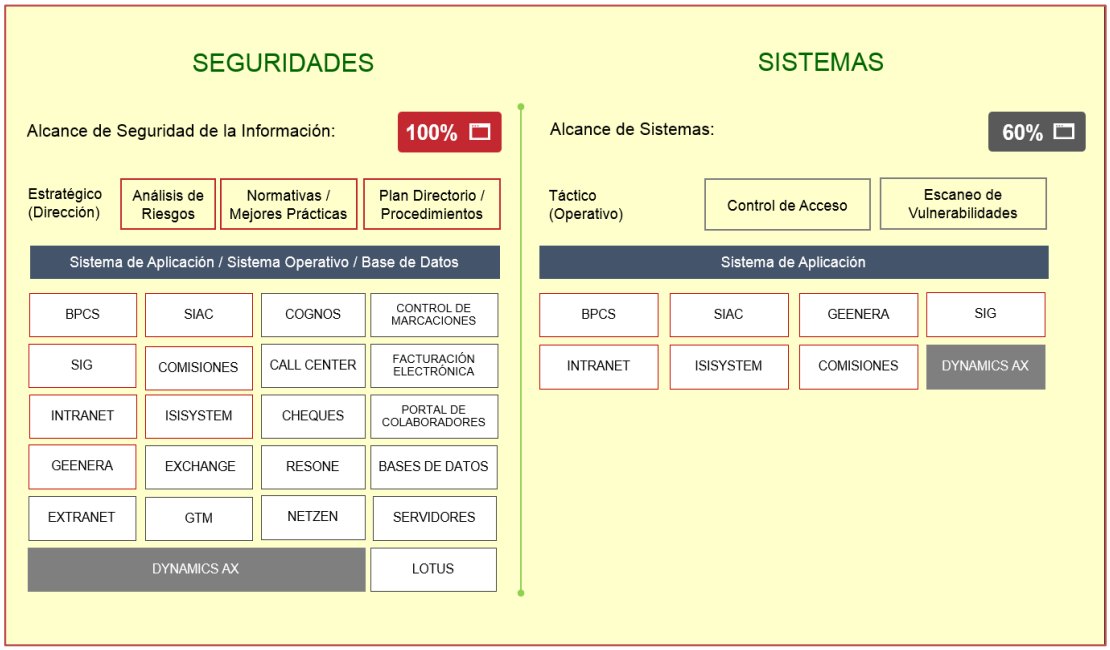

Figura 4.5: Alcance Propuesto

4.7. PLANIFICACIÓN DEL TRABAJO

El plan de trabajo que se ejecutará durante el año para el establecimiento del marco de referencia y cumplimiento de la Norma ISO 27001:2013 está estructurado por los componentes presentados a continuación:

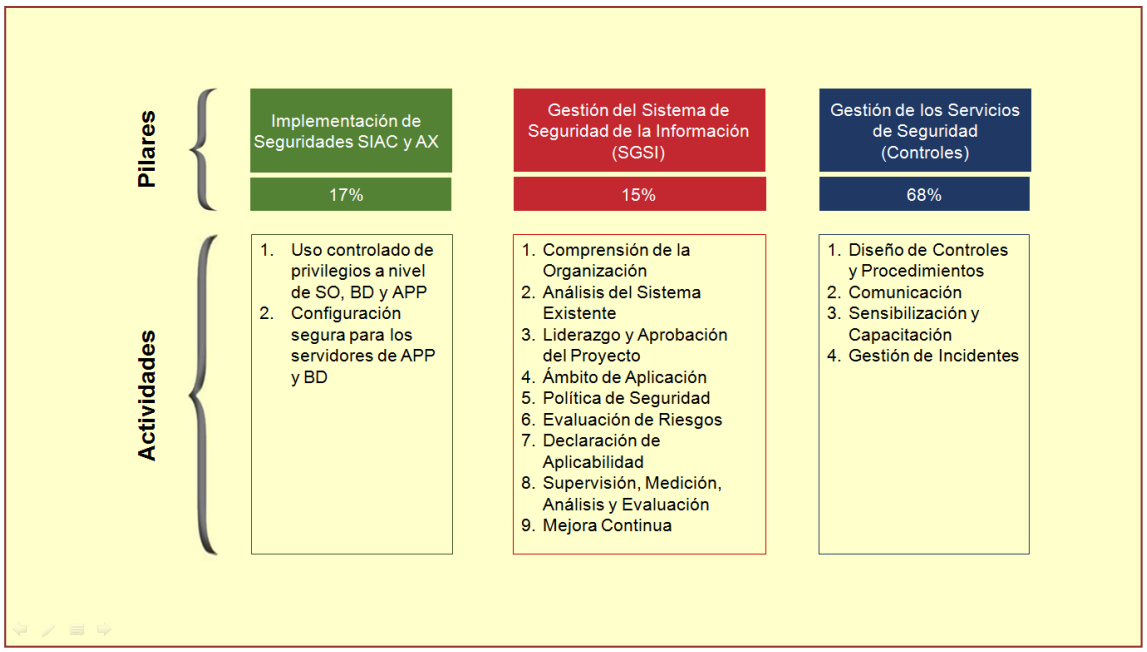

Figura 4.6: Componentes del Plan de Trabajo

En el siguiente diagrama de Gantt se presenta el cronograma general en el que se describen las diferentes tareas a realizar y su respectiva planificación:

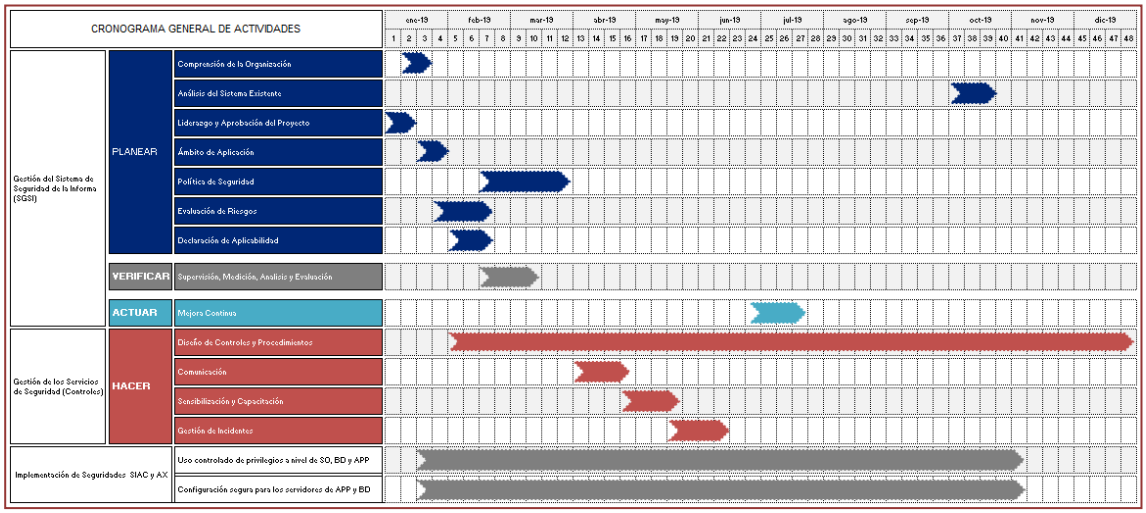

Figura 4.7: Tareas y Plazos del Plan de Trabajo

En cuanto a la carga laboral que requerirá la ejecución del cronograma presentado, a continuación se presenta el detalle de las actividades:

Pilares de Trabajo	Metodología	Componente		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Días x Componente	Días x Pilar de Trabajo	%
Gestión del Sistema de Seguridad de la Informa (SGSI)	Planear	Comprensión de la Organización		10	0	0	0	0	0	0	0	0	0	0	0	10	114	17%
		Análisis del Sistema Existente		0	0	0	0	0	0	0	0	0	16	0	0	16		
		Liderazgo y Aprobación del Proyecto		5	0	0	0	0	0	0	0	0	0	0	0	5		
		Ámbito de Aplicación		4	0	0	0	0	0	0	0	0	0	0	0	4		
		Política de Seguridad		2	7	3	0	0	0	0	0	0	0	0	0	12		
		Evaluación de Riesgos		12	7	3	0	0	0	0	0	0	0	0	0	22		
		Declaración de Aplicabilidad		0	0	2	0	0	0	0	0	0	0	0	0	2		
	Verificar	Supervisión, Medición, Análisis y Evaluación		0	1	1	1	9	5	1	1	1	1	1	1	23		
	Actuar	Mejora Continua		0	2	2	2	2	2	2	2	2	2	3	3	24		
Gestión de los Servicios de Seguridad (Controles)	Hacer	Diseño de Controles y Procedimientos	a. Inventario y control de activos HW y SW	0	5	5	5	6	4	7	5	6	5	5	9	62	468	68%
			b. Gestión continua de vulnerabilidades	0	3	3	3	5	5	8	7	4	3	3	9	53		
			c. Gestión de acceso administrativos y operativos	11	11	11	11	12	7	13	12	13	10	18	12	141		
			d. Establecer la configuración segura para HW y SW	0	3	3	3	5	5	8	7	4	3	4	9	54		
			e. Definir el mantenimiento, monitoreo y análisis de logs	0	3	3	3	4	5	8	7	3	3	4	7	50		
		Comunicación		0	0	8	2	4	2	5	2	2	2	2	3	32		
		Sensibilización y Capacitación		0	0	0	6	3	3	4	4	4	4	3	4	35		
		Gestión de Incidentes		3	3	3	8	3	3	3	3	3	3	3	3	41		
Implementación de Seguridades Proyectos SIAC y AX		Uso controlado de privilegios a nivel de SO, BD y APP		10	6	5	5	5	5	5	5	5	0	0	0	51	101	15%
		Configuración segura para los servidores de APP y BD		9	6	5	5	5	5	5	5	5	0	0	0	50		

Figura 4.8: Detalle de Actividades del Plan de Trabajo

4.8. DEFINICIÓN DE POLÍTICAS

Este paso es fundamental para proveer por parte de la dirección la orientación y apoyo a la seguridad de la información de acuerdo con los requerimientos del negocio y reglamentos aplicables.

En el Anexo “I” se detalla el mapa documental del SGSI que enlaza el macro-proceso de Gestión de Tecnologías de Información de la empresa a los dominios del estándar ISO/IEC 27001:2013.

Los entregables elaborados y mantenidos para la gestión de la seguridad de la información correspondiente a subprocesos de Nivel 3 se detallan en Anexo “J”.

CAPÍTULO 5

DESPLIEGUE DEL SGSI

5.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Toda persona con acceso a los activos de información de la empresa (empleados, contratistas, asesores, vendedores, socios comerciales o empleados temporales) es responsable por el manejo seguro y por la protección de los activos de la información del negocio.

Objetivo

Proteger la información de la empresa para asegurar su confidencialidad, integridad y disponibilidad.

Alcance

Esta política aplica a la empresa y todas sus unidades de negocio relacionadas, incluye cualquier entidad (clientes, proveedores) que acceden a los sistemas de información y usen los equipos (computadoras) del grupo.

Principios de la Política

Conformidad Legal, Estatutaria y Reglamentario:

Todos los empleados, contratistas, y terceros de la empresa deben cumplir con los requerimientos legales, estatutarios, y reglamentarios, tanto locales como internacionales, relacionados con la protección, distribución, o revelación de la información.

Comunicación Oportuna y Exacta:

Es requerido que todos los empleados, contratistas y terceros informen de violaciones, problemas, vulnerabilidades observadas o sospechadas, incidentes o amenazas contra la seguridad al responsable de la Seguridad de la Información o al Gerente de Auditoría Interna de manera oportuna. La información relacionada a violaciones y vulnerabilidades no debe ser distribuida a personas que no tengan “necesidad de informarse” para llevar a cabo sus responsabilidades laborales según Código de Conducta.

Cumplimiento y Conformidad:

Todas las compañías, divisiones, subsidiarias, socios comerciales, gerentes y personal de las unidades de negocio son responsables de hacer cumplir las políticas de seguridad de la información, estándares, y procedimientos. Aquellos que violen la seguridad de los sistemas o redes podrían estar sujetos a acción disciplinaria, incluyendo hasta el despido, y podrían incurrir en responsabilidad penal o civil según Reglamento Interno de Trabajo.

Actividades No Permitidas

Los recursos de la empresa no pueden ser usados para ninguna de las siguientes actividades:

- Recibir, ver, compartir o distribuir materiales que pudieran ser considerados ofensivos o que estuvieren prohibidos bajo la política de la Compañía.
- Para anuncios comerciales o personales.
- Para solicitar ventas o promover negocios externos; presión política o publicidad de actividades políticas; cualquier fin comercial aparte del negocio oficial de la empresa.
- Aparte del personal autorizado del departamento de Sistemas y de Seguridad de la Información, los usuarios tienen prohibido usar herramientas de prueba de seguridad, analizadores de paquete de la red, “sniffers”, o herramientas y tecnologías similares.

Prácticas de Seguridad de la Información

Los sistemas de comunicación de la empresa, incluyendo el Internet, correo electrónico, correo de voz, y sistemas de computación, son propiedad de la Compañía y deberían ser usados únicamente para fines del negocio.

La Política además establece disposiciones relacionadas a los siguientes aspectos:

- Uso Personal del Internet y Correo Electrónico.
- Renuncia a Privacidad.
- Protección de Contraseñas.
- Escritorio Limpio.
- Prevención de Virus.
- Acceso a Internet.

- Sitios de Internet Inapropiados:
  - Actividades Prohibidas en Internet.
  - Sitios Web Internos o de Usuario.

5.2 REDACCIÓN DE POLÍTICAS Y PROCEDIMIENTOS ESPECÍFICOS

Las políticas y procedimientos son una parte necesaria e indispensable para el éxito de los negocios y entre los beneficios de tenerlos dentro de una organización están:

- Orientan a los colaboradores sobre cómo hacer su trabajo.
- Agilidad en la toma de decisiones en todos los niveles jerárquicos.
- Los resultados de los procesos se incrementan.
- El personal de nuevo ingreso se capacita rápidamente.
- El desperdicio organizacional se ve reducido. [14]

El alcance del plan de trabajo fue ha diseñado para dar cumplimiento a los dominios del estándar ISO/IEC, los documentos que fueron elaborados para la gestión de la seguridad de la información los cuales se detallan en el Anexo “K” y los que aún están en proceso de elaboración se encuentran detallados en la tabla a continuación:

Tabla 11: Listado de Políticas En Elaboración

Nombre de la Política
Política de Clasificación de la Información
Política de Control de Acceso
Política de Copias de Seguridad de la Información
Política de Desarrollo Seguro
Política de Dispositivos Móviles y Teletrabajo
Política de Eliminación y Destrucción
Política de Intercambio de Información
Política de Pantalla y Escritorio Limpios
Política de Restricción de Acceso a la Información
Política de Seguridad para Proveedores
Política de Transferencia de Información
Política de Uso Aceptable de los Activos
Política de Uso de Controles Criptográficos

5.3 PLAN DE MONITOREO

En la Tabla 12 se presenta el Plan de Monitoreo elaborado para la monitorización y revisión continua de riesgos y de esta manera dar soporte al cumplimiento de los controles aplicables de la Norma ISO/IEC 27001:2013:

Tabla 12: Plan de Monitoreo

PLAN DE MONITOREO GENERAL PARA CUMPLIMIENTO						
Nº	ACTIVIDAD	IMPACTO	FREC.	INICIO PLAN	EVIDENCIA DE CONTROL	RESPONSABLE
1	Revisión de usuarios de aplicaciones	MEDIO				
1.1	SIAC y BPCS		Quincenal	MAR	- Matriz de revisión de usuarios SIAC creados_bloqueados_ eliminados. - Matriz de revisión de usuarios BPCS creados_bloqueados_ eliminados.	Analista de Seguridades
1.2	ISISYSTEM		Mensual	ABR	- Matriz de revisión de usuarios ISISYSTEM creados_bloqueados_ eliminados.	Analista de Seguridades
1.3	GEENERA		Mensual	MAR	- Matriz de revisión de usuarios GEENERA creados_bloqueados_ eliminados.	
1.4	COMISIONES		Mensual	ABR	- Matriz de revisión de usuarios COMISIONES creados_bloqueados_ eliminados.	

PLAN DE MONITOREO GENERAL PARA CUMPLIMIENTO						
Nº	ACTIVIDAD	IMPACTO	FREC.	INICIO PLAN	EVIDENCIA DE CONTROL	RESPONSABLE
1.5	INTRANET y SIG		Mensual	MAR	- Matriz de revisión usuarios INTRANET creados_bloqueados_ eliminados. - Matriz de revisión usuarios SIG creados_bloqueados_ eliminados.	Analista de Seguridades
2	Revisión de accesos de aplicaciones	MEDIO				
2.1	SIAC y BPCS		Trimestral	ABR	Correos enviados a los BPO indicando la validación de perfiles.	Analista de Seguridades
2.2	ISISYSTEM		Trimestral	ABR	Correos enviados a los BPO indicando la validación de perfiles.	Analista de Seguridades
2.3	GEENERA		Trimestral	ABR	Correos enviados a los BPO indicando la validación de perfiles.	Analista de Seguridades
2.4	COMISIONES		Trimestral	ABR	Correos enviados a los BPO indicando la validación de perfiles.	Analista de Seguridades
2.5	INTRANET y SIG		Trimestral	ABR	Correos enviados a los BPO indicando la validación de perfiles.	Analista de Seguridades

PLAN DE MONITOREO GENERAL PARA CUMPLIMIENTO						
Nº	ACTIVIDAD	IMPACTO	FREC.	INICIO PLAN	EVIDENCIA DE CONTROL	RESPONSABLE
3	Monitoreo de Infraestructura	MEDIO				
3.1	Puertos		Quincenal	MAR	Informe de revisión.	Analista de Redes
3.2	VPN (acceso remoto)		Quincenal	MAR	Matriz de los usuarios con acceso a VPN e informe de revisión.	Analista de Redes
3.3	Bases de Datos		Semestral	ABR	Informes de revisión.	Adm. de Base de Datos
3.4	Políticas locales en los servidores		Anual	ABR	Informes de revisión.	Analista de Seguridades
3.5	Usuarios creados en los servidores		Quincenal	ABR	Informes de revisión.	Analista de Seguridades
4	Revisión de procs. alineados al área de Sistemas	ALTO				

PLAN DE MONITOREO GENERAL PARA CUMPLIMIENTO						
Nº	ACTIVIDAD	IMPACTO	FREC.	INICIO PLAN	EVIDENCIA DE CONTROL	RESPONSABLE
4.1	Admón. Control de Cambios					
4.1.1	Una muestra de cambios de la bitácora de cambio es revisada en una base Trimestral y una evaluación para determinar si se siguió el procedimiento apropiado para cambios normales o de emergencia.		Trimestral	ABR	Forma de Revisión de cambio.	Gerente de Sistemas
4.2	Admón. de Respaldo y Restauración					

PLAN DE MONITOREO GENERAL PARA CUMPLIMIENTO						
Nº	ACTIVIDAD	IMPACTO	FREC.	INICIO PLAN	EVIDENCIA DE CONTROL	RESPONSABLE
4.2.1	Una muestra de aplicaciones es revisada sobre una base Trimestral según su conformidad con: evidencia de monitoreo de respaldo diario, plan de respaldo, etiquetas de medio, almacenamiento fuera de sitio, así como prueba exitosa de restauración de respaldo en los intervalos requeridos por el plan de respaldo y restauración.		Trimestral	ABR	- Reporte Periódico de Prueba de Respaldo. - Formulario de Revisión de Gestión de Respaldo.	Adm. de Centro de Cómputo

PLAN DE MONITOREO GENERAL PARA CUMPLIMIENTO						
Nº	ACTIVIDAD	IMPACTO	FREC.	INICIO PLAN	EVIDENCIA DE CONTROL	RESPONSABLE
4.2.2	Los archivos de acceso de sistema (bases de datos, equipo de comunicación y sistemas operativos) serán guardados por un período de treinta (30) días, luego de los cuáles serán archivados por un período de cinco (5) años.		Mensual	ABR	- Itinerario de Respaldo Mensual. - Reporte de acceso de respaldo generado luego de cada proceso de respaldo.	Adm. de Centro de Cómputo
4.3	Admón. de Incidentes	ALTO				

PLAN DE MONITOREO GENERAL PARA CUMPLIMIENTO						
Nº	ACTIVIDAD	IMPACTO	FREC.	INICIO PLAN	EVIDENCIA DE CONTROL	RESPONSABLE
4.3.1	Un ejemplo de incidentes es revisado bajo una base mensual para verificar si la fuente y el estado del incidente en el sistema y la persona asignada al incidente, apropiadamente reflejan la naturaleza del incidente, y que las acciones pertinentes son tomadas.		Mensual	ABR	-Reporte de incidentes provisto por el sistema de Mesa de Ayuda.	Líder de Seguridad de la Información
4.3.2	Un análisis de métricas de incidentes es desarrollado para determinar si otras acciones de mejora son necesarias.		Mensual	ABR	-Formulario de Revisión del Incidente.	Líder de Seguridad de la Información

PLAN DE MONITOREO GENERAL PARA CUMPLIMIENTO						
Nº	ACTIVIDAD	IMPACTO	FREC.	INICIO PLAN	EVIDENCIA DE CONTROL	RESPONSABLE
4.3.3	Se revisa en una base Trimestral, un ejemplo de incidentes para verificar todos los incidentes de seguridad que han sido apropiadamente identificados y las acciones correspondientes fueron tomadas.		Trimestral	ABR	Formulario de revisión firmado por el Gerente de Seguridad de la Información.	Líder de Seguridad de la Información
5	Difusión de Política de Seguridad	MEDIO				
5.1	Charlas de Inducción de la Política de Seguridad al personal que ingresa a la planta.		Semanal	MAY	Documento de aceptación de la política firmada.	Analista de Seguridades
5.2	Envío de comunicaciones al personal.		Mensual	MAR	Correos enviados a través de Comunicación Organizacional.	Analista de Seguridades

5.4 PLAN DE COMUNICACIÓN

Un programa de seguridad de la información no puede lograr sus objetivos sin el compromiso de todos los interesados; ya sea que esté involucrado un actor interno o externo (clientes, proveedores), la formación, la concientización y la comunicación son fundamentales para la exitosa implementación del SGSI. En la Tabla 13 se presenta el Plan de Comunicación con los diferentes tópicos a tratar en cada boletín de Seguridad enviado a todos los colaboradores de la empresa vía correo organizacional:

Tabla 13: Plan de Comunicación

PLAN DE COMUNICACIÓN				
Nº	Tópico	Herramienta	FECHA	Grupo de Enfoque
1	Phishing	Correo Electrónico	ABR	Todas las regiones
2	Uso adecuado de contraseñas	Correo Electrónico	ABR	Todas las regiones
3	Uso apropiado del correo organizacional	Correo Electrónico	MAY	Todas las regiones
4	Uso de la Mesa de Ayuda	Correo Electrónico	MAY	Todas las regiones
5	Redes Sociales	Correo Electrónico	JUN	Todas las regiones
6	Forma de Reportar Incidentes	Correo Electrónico	JUN	Todas las regiones

PLAN DE COMUNICACIÓN				
Nº	Tópico	Herramienta	FECHA	Grupo de Enfoque
7	Consejos de Seguridad de la Información	Correo Electrónico	JUL	Todas las regiones
8	Uso de Antivirus	Correo Electrónico	JUL	Todas las regiones
9	Consejos de Seguridad sobre equipos móviles	Correo Electrónico	AGO	Todas las regiones
10	Asignación de accesos a aplicaciones	Correo Electrónico	AGO	Todas las regiones
11	Escritorio y Pantalla Limpios	Correo Electrónico	SEP	Todas las regiones
12	Instalación de Software no autorizado	Correo Electrónico	SEP	Todas las regiones
13	Contraseñas Seguras	Correo Electrónico	OCT	Todas las regiones
14	Equipos desatendidos	Correo Electrónico	OCT	Todas las regiones
15	Uso apropiado de carpetas compartidas	Correo Electrónico	NOV	Todas las regiones
16	Uso de dispositivos personales en la empresa	Correo Electrónico	NOV	Todas las regiones
17	Uso adecuado de Internet	Correo Electrónico	DIC	Todas las regiones
18	Copias de Seguridad	Correo Electrónico	DIC	Todas las regiones

PLAN DE COMUNICACIÓN				
Nº	Tópico	Herramienta	FECHA	Grupo de Enfoque
19	Uso apropiado de los Sistemas de Información	Reunión Pública	INDUCCIÓN	Colaboradores Nuevos
20	Alertas de Vulnerabilidades Identificadas	Correo Electrónico	PUNTUAL	Todas las regiones

5.5 PROCEDIMIENTO DE ADMINISTRACIÓN DE INCIDENTES

Objetivo

El objetivo primario del proceso de administración de incidentes es restaurar los servicios de IT tan rápidamente como sea posible, asegurando así que los mejores niveles de servicio de calidad y disponibilidad pueden ser mantenidos. Los incidentes no administrados y resueltos de forma efectiva, puede impactar en de los estados financieros y es por esto que la gestión de incidentes busca minimizar el impacto en las operaciones del negocio de la empresa mediante la restauración de los servicios en los tiempos acordados.

Alcance

Abarca cualquier interrupción en los servicios de la organización o uno de sus componentes desde la ocurrencia, identificación y registro del incidente hasta su resolución y cierre. Este procedimiento cubre todos los servicios registrados por usuarios a través de un requerimiento o un incidente reportado (por teléfono, correo, intranet y alertas de herramientas de monitoreo). La participación activa

en este procedimiento es requerida por personal de Mesa de Ayuda, Infraestructura y Seguridad.

Este procedimiento se aplica a todos los empleados, terceras partes, contratistas o personal temporal que estén hacienda uso del ambiente computacional de la empresa.

Definición de Incidente

Todo evento que no es parte de la operación normal de un servicio, causando interrupción o degradación en la calidad del mismo. La interrupción en la operación de un componente del servicio.

Categorización del Incidente

Todos los incidentes reportados serán categorizados en cuatro grupos principales: crítico, alto, medio, bajo, dependiendo de la severidad del evento (impacto).

El personal de Mesa de Ayuda hará una valoración inicial y adjudicará al incidente a una de las categorías. Este es un paso importante ya que las acciones resultantes diferirán según la categorización. En la Tabla 9 se establecen las categorías por incidente:

Tabla 14: Categoría de Incidentes

Categoría	Definición	Áreas relacionadas
CRÍTICO	Incidentes que ocasionan el **mayor impacto** al negocio, las operaciones del negocio no pueden ser llevados a cabo de forma normal, y múltiples usuarios o usuarios críticos están impedidos de ejecutar aplicaciones de producción.	Relacionados con las operaciones críticas de Ventas y Procesos de Cierre Contable.
ALTO	Incidentes que tienen un impacto **significativo** en el negocio o en el servicio a los clientes.	Relacionados con las operaciones no críticas de los procesos de Ventas También se relacionan con las operaciones críticas de los procesos de finanzas.
MEDIANO	Incidentes que tienen un impacto **medio** en el negocio o en el servicio a los clientes.	Relacionados con las operaciones no críticas de los procesos de mercadeo y finanzas. Soportan las operaciones críticas de los procesos de apoyo para las demás áreas.
BAJO	Incidentes que tienen un impacto **mínimo** en el negocio o servicio a los clientes. Estos serán registrados con el propósito de establecer tendencias.	Relacionados con las operaciones no críticas de los procesos de apoyo.

Ciclo de Vida de los incidentes

En la Tabla 15 se establecen los estados por los cuales pasa un incidente desde el momento en que se presenta hasta que finalmente se resuelve:

Tabla 15: Ciclo de Vida de los Incidentes

Nombre	Descripción	Quiénes	Qué
Registrada	Llamada registrada por teléfono, correo o vía Intranet	Mesa de Ayuda	Registro de los incidentes y requerimientos de servicio.
Asignada	Llamada asignada a un especialista específico	Mesa de Ayuda, Grupo Resolutor	Asignación de los incidentes al personal respectivo y los SLAs definidos para el caso.
En Progreso	Llamada aceptada por un especialista	Mesa de Ayuda, Grupo Resolutor	Aceptación del incidente por parte de la persona asignada. Se documenta el incidente con las acciones que están siendo ejecutadas.
Escalada a Proveedor	Llamada escalada a un proveedor	Mesa de Ayuda, Grupo Resolutor	Documentar el incidente con los datos suministrados con el proveedor y en los casos que sea necesario crear una llamada de subcontrato con

Nombre	Descripción	Quiénes	Qué
			los datos del SLA del proveedor.
En Espera por Cambio	Llamada escalada a Cambio esperando aprobación	Mesa de Ayuda, Grupo Resolutor	Se genera el cambio que debe solucionar el incidente y se relaciona.
En Espera por Usuario	Llamada de servicio en espera por una respuesta o prueba del usuario que hizo el requerimiento	Mesa de Ayuda, Grupo Resolutor	Detener el tiempo para evitar el incumplimiento del SLA y establecer de canal de comunicación con el usuario para solucionar el caso.
Resuelta	Llamada resuelta	Mesa de Ayuda, Grupo Resolutor	Documentar la solución del incidente, notificar automáticamente al usuario la solución.
Cerrada	Llamada cerrada	Mesa de Ayuda	Se cierra el incidente. Para el caso de los incidentes resueltos en la primera llamada el caso se cierra inmediatamente.

Monitoreo de incidentes

Este proceso permite que se lleve un continuo control sobre los acuerdos de cumplimiento de servicios garantizando de esta manera que se cumplan los resultados esperados de la aplicación del procedimiento.

CAPÍTULO 6

MEDICIÓN DEL SGSI

6.1 INDICADORES CLAVE DE DESEMPEÑO

Los Indicadores Clave de Desempeño (KPI) se utilizan para evaluar si los procesos de una organización funcionan según las expectativas. Un principio extensamente aceptado mantiene que los KPI deben ser SMART:

- Específico (**S**pecific).
- Medible (**M**easurable).
- Alcanzable (**A**chievable).
- Orientado a resultados (**R**esult-oriented).
- A tiempo (**T**imely). [16]

Los siguientes indicadores, tomados de las bases de KPI para los procesos más importantes de la Gestión de servicios de TI, se adoptarán para continuamente monitorear el desempeño de las acciones implementadas para la mejora del nivel de seguridad en la empresa:

Tabla 16: Propuesta de KPIs

Gestión del Nivel de Servicio	Descripción
Servicios cubiertos por SLA	Número de servicios cubiertos por los SLA.
SLA bajo revisión	Número de servicios/ SLA revisados regularmente.
Cumplimiento de niveles de servicio	Número de servicios/ SLA que cumplen con los niveles de servicio acordados.
Gestión de la Capacidad	Descripción
Incidentes debidos a falta de capacidad	Número de incidentes ocurridos por la insuficiencia de capacidad de Servicios o de sus componentes.
Ajustes a la capacidad no planeados	Número de aumentos no planificados a la capacidad de Servicios o de componentes como producto de limitaciones de capacidad.
Gestión de la Disponibilidad	Descripción
Disponibilidad de servicio	Disponibilidad de servicios en relación a la disponibilidad acordada en los SLA.
Interrupciones de servicio	Número de interrupciones de servicio.
Duración de interrupciones de servicio	Duración media de interrupciones de servicio.
Gestión de la Continuidad del Servicios	Descripción
Procesos de negocio con acuerdos de continuidad	Porcentaje de procesos de negocio cubiertos por metas específicas de continuidad del servicio.
Duración de la implementación	Duración desde la identificación del riesgo relacionado a desastres hasta la implementación de un mecanismo de continuidad adecuado.
Gestión de la Seguridad	Descripción
Medidas preventivas implementadas	Número de medidas de seguridad preventivas implementadas como respuesta a amenazas de seguridad identificadas.
Duración de la implementación de medidas preventivas implementadas	Duración desde la identificación de una amenaza de seguridad hasta la implementación de una contramedida adecuada.

Incidentes graves de la seguridad	Número de incidentes de seguridad identificados, clasificados por categoría de gravedad.
Número de periodos de inactividad de servicio relacionados con la seguridad	Número de incidentes de seguridad que causan interrupciones de servicio o disponibilidad reducida.
Evaluación de Servicios	Descripción
Número de quejas de clientes	Número de quejas recibidas de los clientes internos o externos.
Número de Evaluaciones de Servicios	Número de Evaluaciones de Servicios realizadas durante el periodo.
Número de debilidades identificadas	Número de puntos débiles identificados durante la Evaluación de Servicio, para ser tratados mediante iniciativas de mejoras.
Evaluación de Procesos	Descripción
Número de Comparativas de Procesos, Evaluaciones de Madurez, y Auditorías	Número de Comparativas de Procesos formales, Evaluaciones de Madurez, y Auditorías realizadas durante el periodo del informe.
Número de Evaluaciones de Procesos	Número de Evaluaciones de Procesos formales realizadas.
Número de debilidades identificadas	Número de puntos débiles identificados durante la Evaluación de Procesos, para ser tratados mediante iniciativas de mejoras.
Definición de Iniciativas de Mejora Continua	Descripción
Número de Iniciativas de Mejora Continua	Número de Iniciativas de CSI, resultando de los puntos débiles identificados durante la Evaluación de Servicios y Procesos.
Número de Iniciativas de Mejora Continua completadas	Número de Iniciativas de CSI que fueron completadas durante el periodo del informe.
Gestión de Incidentes	Descripción
Número de incidentes repetidos	Número de incidentes repetidos (con métodos para su resolución ya conocidos).
Número de incidentes	Número de incidentes registrados, agrupados por categorías.
Tiempo de resolución de incidente	Tiempo medio para resolver un incidente, agrupados por categorías.
Resolución dentro del SLA	Porcentaje de incidentes resueltos durante el tiempo acordado en el SLA, agrupados por categorías.
Gestión de Cambios	Descripción
Número de cambios mayores	Número de cambios mayores.
Tiempo para autorización para cambios	Tiempo medio transcurrido desde la solicitud de una RFC (Solicitud de Cambio) a la Gestión de Cambios hasta la autorización para el cambio.
Tasa de aceptación de cambios	Número de RFC aceptadas vs rechazadas.
Número de cambios urgentes	Número de cambios urgentes evaluados.

6.2 INDICADORES CLAVE DE RIESGO

Un indicador clave de riesgo es una herramienta fundamental que se emplea para monitorear y mitigar los impactos de posibles amenazas. Los KRI, o indicadores de riesgo, son una métrica esencial para medir la posibilidad de un impacto futuro. [17]. A continuación se enlistan los KRIs a ser implementados en la empresa:

- Número de servidores sin aplicación de Hardening.
- Número de servidores sin parches aplicados.
- Número de estaciones de trabajo sin actualización de antivirus.
- Porcentaje de empleados que no han recibido capacitación sobre la Política de Seguridad de la Información.
- Porcentaje de aplicaciones que no tienen segregación de funciones.
- Porcentaje de servicios que no tienen SLAs establecidos.

6.3 EVALUACIÓN DE LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

Los mecanismos que se implementaron para cumplir con la Política de Seguridad de la Información se detallan a continuación:

- **Garantizar la disponibilidad de los recursos de la red y sus servicios:** Se implementó mecanismos para protección de mensajería electrónica para lo cual se fortaleció la infraestructura de seguridad y equipos de servidores, lo que permitirá minimizar los ataques informáticos.

- **Garantizar la integridad de la información, servicios, sistemas y demás recursos de red:** Para que la información y datos conserven su integridad, se implementó el uso de certificados de seguridad, credenciales digitales o firmas electrónicas.

  El Área de Seguridad de la Información será la encargado de realizar el análisis, control y monitoreo de seguridad de la Información, el mismo que se encuentra en fase inicial.

- **Garantizar la autenticidad de la información:** Se realizó la implementación de controles, mecanismos para control y protección de software en los sistemas operativos de producción; se encuentra en proceso la aplicación de Hardening en los servidores.

- **Garantizar la confidencialidad:** Para que la información sólo esté disponible para usuarios autorizados, se realizó la implementación de mecanismos de cifrado de documentos críticos para así evitar la alteración de la información sensible.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. El análisis de la situación inicial de la gestión de TI sobre los procesos de la cadena de valor de la empresa ha permitido conocer que el nivel de cumplimiento de seguridad de la información relacionado a los controles de la ISO 27001-2013 es de 4 y que el nivel de madurez actual es 2.
2. El levantamiento e identificación de los activos de información de la empresa permitió categorizar y valorar los activos para visualizar su importancia y criticidad dentro de los procesos que conforman la cadena de valor, dando como resultado 65 activos de los cuales 49 activos se encuentran bajo la gestión directa de la Gerencia de TI.
3. La elaboración de la matriz de riesgos presentó como resultado 211 riegos extremos, 386 altos, 101 moderados y 24 riegos bajos, que podrían incidir directamente sobre los servicios TICs, lo cual dificultaría o evitaría que la empresa logre alcanzar sus objetivos de negocio.

RECOMENDACIONES

1. Mantener actualizado, valorado y categorizado el inventario de activos de seguridad de la información con la finalidad de contar continuamente con la criticidad e importación de los activos relacionados a los procesos de la cadena de valor.
2. Periódicamente elaborar la matriz de evaluación de riesgos con la finalidad de mantener un control de la situación de la empresa relacionada a la seguridad de la información.
3. Implementar y monitorear los KPI y KRI propuestos para mantener informada a la alta gerencia y realizar un seguimiento del compromiso en lo que a seguridad de la información se refiere.

BIBLIOGRAFÍA

[1] Comercializadora CC. Quiénes Somos [Online]. Available: https://ofertas. comercializadoracc.com/quienes-somos.

[2] F. Navarro. (2016, Jul 15). Las Normas ISO y la Estructura de Alto Nivel [Online]. Available: https://revistadigital.inesem.es/gestion-integrada/las-normas-iso-la-estructura-alto-nivel/.

[3] Escuela Europea de Excelencia. (2018, Nov 20). Estructura de alto nivel [Online]. Available: https://www.nueva-iso-9001-2015.com/2018/11/que-supuso-la-implantacion-de-la-estructura-de-alto-nivel/.

[4] Academia. Fundamentos y principios de los Sistemas de Gestión ISO [Online]. Available: https://www.academia.edu/28807164/Fundamentos_y_principios_de_los_Sistemas_de_Gestión_ISO_Aplicación_de_los_Principios_de_Gestión_de_la_Calidad.

[5] Escuela Europea de Excelencia. (2017, Jul 27). Principios de la gestión de calidad [Online]. Available: https://www.nueva-iso-9001-2015.com/2017/07/principios-de-gestion-de-la-calidad/.

[6] ISOTools Excellence. (2017, Abr 20). Dominios ISO 27001:2013: Motivos para conocer mejor la nueva norma [Online]. Available: https://www.pmg-ssi.com/2014/03/iso-27001-los-dominios-de-la-informacion/.

[7] ISOTools Excellence. (2016, Jul 11). ISO 27001: ¿Qué beneficios nos aporta implantar esta norma? [Online]. Available: https://www.pmg-ssi.com/2016/07/iso-27001-beneficios-aporta-implantar-esta-norma/.

[8] ISOTools Excellence. (2017, Jul 6) ¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información? [Online]. Available: https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/.

[9] Wikipedia. (2019, Mar 14) Seguridad de la información [Online]. Available: https://es.wikipedia.org/wiki/Seguridad_de_la_información.

[10] Audisec. ISO 27000 y el conjunto de estándares de Seguridad de la Información [Online]. Available: https://www.audisec.es/en/iso-27000-estandares-de-seguridad-de-la-informacion/.

[11] ISOTools Excellence. (2016, Feb 16) Descubre qué es un SGSI y cuáles son sus elementos esenciales [Online]. Available: https://www.isotools.org/2016/02/16/descubre-que-es-un-sgsi-y-cuales-son-sus-elementos-esenciales/.

[12] 27001 Academy. Achieving continual improvement through the use of maturity models (CMM) [Online]. Available: https://advisera.com/27001academy/blog/2015/04/13/achieving-continual-improvement-through-the-use-of-maturity-models/.

[13] TechTarget. Capability Maturity Model (CMM) [Online]. Available: https://searchsoftwarequality.techtarget.com/definition/Capability-Maturity-Model.

[14] Grupo Albe Consultoría. Elaboración de Manuales de Políticas y Procedimientos [Online]. Available: http://www.grupoalbe.com/productos-de-consultoria/elaboracion-de-manuales-de-politicas-y-procedimientos/.

[15] Gobierno de España, Ministerio de Hacienda y Administraciones Públicas. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos.

[16] ITIL® Process Map & ITIL® Wiki. Métricas ITIL - KPIs ITIL [Online]. Available: https://wiki.es.it-processmaps.com/index.php/M%C3%A9tricas_ITIL_-_KPIs_ITIL.

[17] Riesgos Cero. Todo lo que debe saber sobre indicadores clave de riesgo (KRI) [Online]. Available: https://www.riesgoscero.com/todo-lo-que-debe-saber-sobre-indicadores-clave-de-riesgo-kri.

ANEXO A - ANÁLISIS DE BRECHAS				
Controles de la Norma			Puntaje Control	Nivel Individual
A.5	Políticas de seguridad de la información		3	Repetible
A.5.1	Directrices de gestión de la seguridad de la información Objetivo: Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normas pertinentes.		3	Repetible
A.5.1.1	Políticas para la seguridad de la información	Control: Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	3	Repetible
A.5.1.2	Revisión de las políticas para la seguridad de la información	Control: Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	2	Inicial
A.6	Organización de la seguridad de la información		4	Repetible
A.6.1	Organización interna Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		4	Repetible
A.6.1.1	Roles y responsabilidades en seguridad de la información	Control: Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.	3	Repetible
A.6.1.2	Segregación de tareas	Control: Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.	0	Inexistente
A.6.1.3	Contacto con las autoridades	Control: Deben mantenerse los contactos apropiados con las autoridades pertinentes.	8	Administrado

A.6.1.4	Contacto con grupos de interés especial	Control: Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializadas en seguridad.	8	Administrado
A.6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	2	Inicial
A.6.2 Los dispositivos móviles y el teletrabajo Objetivo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.			3	Repetible
A.6.2.1	Política de dispositivos móviles	Control: Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	3	Repetible
A.6.2.2	Teletrabajo	Control: Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.	3	Repetible
A.7 Seguridad relativa a los recursos humanos			2	Inicial
A.7.1 Antes del empleo Objetivo: Para asegurarse de que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.			3	Repetible
A.7.1.1	Investigación de antecedentes	Control: La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.	4	Repetible
A.7.1.2	Términos y condiciones del empleo	Control: Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.	2	Inicial
A.7.2 Durante el empleo			2	Inicial

Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.				
A.7.2.1	Responsabilidades de gestión	Control: La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	4	Repetible
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Control: Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	2	Inicial
A.7.2.3	Proceso disciplinario	Control: Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.	0	Inexistente
A.7.3 Finalización del empleo o cambio en el puesto de trabajo Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.			2	Inicial
A.7.3.1	Responsabilidades ante la finalización o cambio	Control: Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.	2	Inicial
A.8 Gestión de activos			0	Inexistente
A.8.1 Responsabilidad sobre los activos Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.			0	Inexistente
A.8.1.1	Inventario de activos	Control: Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.	0	Inexistente
A.8.1.2	Propiedad de los activos	Control: Todos los activos que figuran en el inventario deben tener un propietario.	0	Inexistente

A.8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.	0	Inexistente
A.8.1.4	Devolución de activos	Control: Todos los empleados y terceras partes deben devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	0	Inexistente
A.8.2 Clasificación de la información Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.			1	Inicial
A.8.2.1	Clasificación de la información	Control: La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.	1	Inicial
A.8.2.2	Etiquetado de la información	Control: Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	1	Inicial
A.8.2.3	Manipulado de la información	Control: Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	0	Inexistente
A.8.3 Manipulación de los soportes Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.			0	Inexistente
A.8.3.1	Gestión de soportes extraíbles	Control: Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	0	Inexistente
A.8.3.2	Eliminación de soportes	Control: Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.	0	Inexistente

A.8.3.3	Soportes físicos en tránsito	Control: Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.	0	Inexistente
A.9 Control de acceso			3	Repetible
A.9.1 Requisitos de negocio para el control de acceso Objetivo: Limitar el acceso a los recursos de tratamiento de información y a la información.			3	Repetible
A.9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	3	Repetible
A.9.1.2	Acceso a las redes y a los servicios de red	Control: Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.	2	Inicial
A.9.2 Gestión de acceso de usuario Objetivo: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.			3	Repetible
A.9.2.1	Registro y baja de usuario	Control: Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	4	Repetible
A.9.2.2	Provisión de acceso de usuario	Control: Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	3	Repetible
A.9.2.3	Gestión de privilegios de acceso	Control: La asignación y el uso de privilegios de acceso debe estar restringida y controlada.	2	Inicial
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	Control: La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.	2	Inicial
A.9.2.5	Revisión de los derechos de acceso de usuario	Control: Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	2	Inicial

A.9.2.6	Retirada o reasignación de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	4	Repetible
A.9.3 Responsabilidades del usuario Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.			3	Repetible
A.9.3.1	Uso de la información secreta de autenticación	Control: Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.	3	Repetible
A.9.4 Control de acceso a sistemas y aplicaciones Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.			1	Inicial
A.9.4.1	Restricción del acceso a la información	Control: Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.	1	Inicial
A.9.4.2	Procedimientos seguros de inicio de sesión	Control: Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.	1	Inicial
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.	2	Inicial
A.9.4.4	Uso de utilidades con privilegios del sistema	Control: Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	0	Inexistente
A.9.4.5	Control de acceso al código fuente de los programas	Control: Se debe restringir el acceso al código fuente de los programas.	1	Inicial
A.10 Criptografía			2	Inicial
A.10.1 Controles criptográficos Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y / o integridad de la información.			2	Inicial
A.10.1.1	Política de uso de los controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	2	Inicial

A.10.1.2	Gestión de claves	Control: Se debe desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	2	Inicial
A.11 Seguridad física y del entorno			4	Repetible
A.11.1 Áreas seguras Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.			5	Definido
A.11.1.1	Perímetro de seguridad física	Control: Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.	2	Inicial
A.11.1.2	Controles físicos de entrada	Control: Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	6	Definido
A.11.1.3	Seguridad de oficinas, despachos y recursos	Control: Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.	6	Definido
A.11.1.4	Protección contra las amenazas externas y ambientales	Control: Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	6	Definido
A.11.1.5	El trabajo en áreas seguras	Control: Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.	6	Definido
A.11.1.6	Áreas de carga y descarga	Control: Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.	6	Definido
A.11.2 Seguridad de los equipos Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.			2	Inicial
A.11.2.1	Emplazamiento y protección de equipos	Control: Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.	2	Inicial

A.11.2.2	Instalaciones de suministro	Control: Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	0	Inexistente
A.11.2.3	Seguridad del cableado	Control: El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.	6	Definido
A.11.2.4	Mantenimiento de los equipos	Control: Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	2	Inicial
A.11.2.5	Retirada de materiales propiedad de la empresa	Control: Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.	2	Inicial
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	Control: Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.	2	Inicial
A.11.2.7	Reutilización o eliminación segura de equipos	Control: Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.	0	Inexistente
A.11.2.8	Equipo de usuario desatendido	Control: Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.	2	Inicial
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Control: Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.	2	Inicial
A.12 Seguridad de las operaciones			4	Repetible
A.12.1 Procedimientos y responsabilidades operacionales Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.			6	Definido
A.12.1.1	Documentación de procedimientos de los operación	Control: Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.	6	Definido

A.12.1.2	Gestión de cambios	Control: Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deben ser controlados.	2	Inicial
A.12.1.3	Gestión de capacidades	Control: Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	8	Administrado
A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	Control: Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	6	Definido
A.12.2 Protección contra el software malicioso (malware) Objetivo: Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware.			4	Repetible
A.12.2.1	Controles contra el código malicioso	Control: Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.	4	Repetible
A.12.3 Copias de seguridad Objetivo: Evitar la pérdida de datos.			4	Repetible
A.12.3.1	Copias de seguridad de la información	Control: Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.	4	Repetible
A.12.4 Registros y supervisión Objetivo: Registrar eventos y generar evidencias.			2	Inicial
A.12.4.1	Registro de eventos	Control: Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	2	Inicial
A.12.4.2	Protección de la información de registro	Control: Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	2	Inicial

A.12.4.3	Registros de administración y operación	Control: Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	0	Inexistente
A.12.4.4	Sincronización del reloj	Control: Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo.	4	Repetible
A.12.5 Control del software en explotación Objetivo: Asegurar la integridad del software en explotación.			2	Inicial
A.12.5.1	Instalación del software en explotación	Control: Se deben implementar procedimientos para controlar la instalación del software en explotación.	2	Inicial
A.12.6 Gestión de la vulnerabilidad técnica Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.			3	Repetible
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	6	Definido
A.12.6.2	Restricción en la instalación de software	Control: Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	0	Inexistente
A.12.7 Consideraciones sobre la auditoria de sistemas de información Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.			4	Repetible
A.12.7.1	Controles de auditoría de sistemas de información	Control: Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	4	Repetible
A.13 Seguridad de las comunicaciones			4	Repetible
A.13.1 Gestión de la seguridad de redes Objetivo: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.			5	Definido
A.13.1.1	Controles de red	Control: Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	6	Definido

A.13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	2	Inicial
A.13.1.3	Segregación en redes	Control: Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.	6	Definido
A.13.2 Intercambio de información Objetivo: Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.			3	Repetible
A.13.2.1	Políticas y procedimientos de intercambio de información	Control: Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	2	Inicial
A.13.2.2	Acuerdos de intercambio de información	Control: Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.	2	Inicial
A.13.2.3	Mensajería electrónica	Control: La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	2	Inicial
A.13.2.4	Acuerdos de confidencialidad o no revelación	Control: Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.	4	Repetible
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información			3	Repetible
A.14.1 Requisitos de seguridad en sistemas de información Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.			4	Repetible
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Control: Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	2	Inicial

A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Control: La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.	6	Definido
A.14.1.3	Protección de las transacciones de servicios de aplicaciones	Control: La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.	4	Repetible
A.14.2 Seguridad en el desarrollo y en los procesos de soporte Objetivo: Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.			2	Inicial
A.14.2.1	Política de desarrollo seguro	Control: Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	2	Inicial
A.14.2.2	Procedimiento de control de cambios en sistemas	Control: La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.	6	Definido
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Control: Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.	2	Inicial
A.14.2.4	Restricciones a los cambios en los paquetes de software	Control: Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	2	Inicial
A.14.2.5	Principios de ingeniería de sistemas seguros	Control: Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.	2	Inicial
A.14.2.6	Entorno de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	2	Inicial

A.14.2.7	Externalización del desarrollo de software	Control: El desarrollo de software externalizado debe ser supervisado y controlado por la organización.	2	Inicial
A.14.2.8	Pruebas funcionales de seguridad de sistemas	Control: Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	2	Inicial
A.14.2.9	Pruebas de aceptación de sistemas	Control: Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	2	Inicial
A.14.3 Datos de prueba Objetivo: Asegurar la protección de los datos de prueba.			2	Inicial
A.14.3.1	Protección de los datos de prueba	Control: Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.	2	Inicial
A.15 Relación con proveedores			2	Inicial
A.15.1 Seguridad en las relaciones con proveedores Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			1	Inicial
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Control: Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.	2	Inicial
A.15.1.2	Requisitos de seguridad en contratos con terceros	Control: Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura IT.	0	Inexistente
A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Control: Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.	0	Inexistente
A.15.2 Gestión de la provisión de servicios del proveedor Objetivo: Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.			3	Repetible
A.15.2.1	Control y revisión de la provisión de servicios del proveedor	Control: Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor.	2	Inicial

A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Control: Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.	4	Repetible
A.16 Gestión de incidentes de seguridad de la información			4	Repetible
A.16.1 Gestión de incidentes de seguridad de la información y mejoras Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.			4	Repetible
A.16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	2	Inicial
A.16.1.2	Notificación de los eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	4	Repetible
A.16.1.3	Notificación de puntos débiles de la seguridad	Control: Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.	2	Inicial
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Control: Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	4	Repetible
A.16.1.5	Respuesta a incidentes de seguridad de la información	Control: Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	6	Definido
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Control: El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.	6	Definido

A.16.1.7	Recopilación de evidencias	Control: La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia.	6	Definido
A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio			3	Repetible
A.17.1 Continuidad de la seguridad de la información Objetivo: La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de continuidad de negocio de la organización.			3	Repetible
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	4	Repetible
A.17.1.2	Implementar la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	2	Inicial
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	2	Inicial
A.17.2 Redundancias. Objetivo: Asegurar la disponibilidad de los recursos de tratamiento de la información.			2	Inicial
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Control Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	2	Inicial
A.18 Cumplimiento			1	Inicial
A.18.1 Cumplimiento de los requisitos legales y contractuales Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.			1	Inicial

A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.	0	Inexistente
A.18.1.2	Derechos de propiedad intelectual (DPI)	Control: Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	2	Inicial
A.18.1.3	Protección de los registros de la organización	Control: Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.	2	Inicial
A.18.1.4	Protección y privacidad de la información de carácter personal	Control: Deber garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.	0	Inexistente
A.18.1.5	Regulación de los controles criptográficos	Control: Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	2	Inicial
A.18.2 Revisiones de la seguridad de la información Objetivo: Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.			1	Inicial
A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de seguridad de la información y su implantación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.	2	Inicial

A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Control: Los directivos deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.	2	Inicial
A.18.2.3	Comprobación del cumplimiento técnico	Control: Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.	0	Inexistente

ANEXO B - ANÁLISIS DEL NIVEL DE MADUREZ DE LA SEGURIDAD DE LA INFORMACIÓN		
Requisitos de la Norma	Puntaje Requisitos	Nivel Individual
4. CONTEXTO DE LA ORGANIZACIÓN	2	Inicial
4.1 Comprensión de la organización y su contexto	2	Inicial
La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad la información.	2	Inicial
NOTA: La determinación de estas cuestiones se refiere a establecer el contexto externo e interno de la organización considerado en el apartado 5.3 de la Norma ISO 31000:2009. [5]	2	Inicial
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	1	Inicial
La organización debe determinar:	1	Inicial
a) las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información; y	1	Inicial
b) los requisitos de estas partes interesadas que son relevantes para la seguridad de la información.	1	Inicial
NOTA: Los requisitos de las partes interesadas pueden incluir los requisitos legales y regulatorios, así como obligaciones contractuales.	1	Inicial
4.3 Determinación del alcance del sistema de gestión de seguridad de la información	1	Inicial
La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance.	1	Inicial
Cuando se determina este alcance, la organización debe considerar:	1	Inicial
a) las cuestiones externas e internas referidas en el apartado 4,1;	1	Inicial
b) los requisitos referidos en el apartado 4.2;	1	Inicial
c) las interfaces y dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones.	1	Inicial
El alcance debe estar disponible como información documentada.	1	Inicial
4.4 Sistema de gestión de seguridad de la información	2	Inicial
La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información, de acuerdo con los requisitos de esta Norma Internacional.	2	Inicial

5. LIDERAZGO	2	Inicial
5.1 Liderazgo y compromiso	2	Inicial
La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información:	2	Inicial
a) asegurando que la política y los objetivos de seguridad de la información se establecen y son compatibles con la dirección estratégica de la organización;	2	Inicial
b) asegurando la integración de los requisitos del sistema de gestión de seguridad de la información con los procesos de la organización;	2	Inicial
c) asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles;	3	Repetible
d) comunicando la importancia de una gestión de seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de seguridad de la información;	2	Inicial
e) asegurando que el sistema de gestión de seguridad de la información consigue los resultados previstos;	2	Inicial
f) dirigiendo y apoyando a las personas para contribuir a la eficacia del sistema de gestión de seguridad de la información;	3	Repetible
g) promoviendo la mejora continua; y	2	Inicial
h) apoyando otros roles pertinentes de la gestión, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.	3	Repetible
5.2 Política	2	Inicial
La alta dirección debe establecer una política de seguridad de la información que:	2	Inicial
a) sea adecuada al propósito de la organización;	3	Repetible
b) incluya objetivos de seguridad de la información (ver 6.2) o proporcione un marco de referencia para establecimiento de los objetivos de seguridad de la información;	2	Inicial
c) incluya el compromiso de cumplir con los requisitos aplicables a la seguridad de la información; e	3	Repetible
d) incluya un compromiso de mejora continua del sistema de gestión de seguridad de la información.	2	Inicial
La política de seguridad de la información debe:	3	Repetible
e) estar disponible como información documentada;	2	Inicial
f) ser comunicada dentro de la organización; y	2	Inicial
g) estar disponible para las partes interesadas, según sea apropiado.	3	Repetible
5.3 Roles organizacionales, responsabilidades y autoridad	2	Inicial

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la información seguridad se asignen y comuniquen dentro de la organización.	2	Inicial
La alta dirección debe asignar la responsabilidad y autoridad para:	3	Repetible
a) asegurarse que el sistema de gestión de seguridad de la información es conforme con los requisitos de esta Norma Internacional; e	2	Inicial
b) informar a la alta dirección sobre el comportamiento del sistema de gestión de seguridad de la información.	2	Inicial
NOTA: La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el comportamiento del sistema de gestión de la seguridad de la información dentro de la organización.	2	Inicial
6. PLANEACIÓN	3	Repetible
6.1 Acciones para tratar los riesgos y oportunidades	3	Repetible
6.1.1 Consideraciones generales	2	Inicial
Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar las cuestiones a las que se hace referencia en el apartado 4.1 y los requisitos incluidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario tratar con el fin de:	2	Inicial
a) asegurar que el sistema de gestión de seguridad de la información pueda conseguir sus resultados previstos;	2	Inicial
b) prevenir o reducir efectos indeseados; y	3	Repetible
c) lograr la mejora continua.	1	Inicial
La organización debe planificar:	1	Inicial
d) las acciones para hacer frente a estos riesgos y oportunidades; y	1	Inicial
e) la manera de: 1. integrar e implementar las acciones en los procesos del sistema de gestión de seguridad de la información; y 2. evaluar la eficacia de estas acciones.	2	Inicial
6.1.2 Evaluación de riesgos de seguridad de la información	4	Repetible
La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de información que:	4	Repetible
a) establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo: 1. los criterios de aceptación del riesgo; y 2. los criterios para realizar las evaluaciones de riesgos de seguridad de la información;	3	Repetible

b) asegure que las evaluaciones de riesgos de seguridad de la información repetidas produzcan resultados consistentes, válidos y comparables;	3	Repetible
c) identifique los riesgos de seguridad de la información: 1. aplicando el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información; y 2. identificando a los propietarios de los riesgos;	3	Repetible
d) analice los riesgos de seguridad de la información: 1. evaluando las posibles consecuencias que resultarían si los riesgos identificados en el punto 6.1.2 c) 1) llegasen a materializarse; 2. evaluando de forma realista la probabilidad de ocurrencia de los riesgos identificados en 6.1.2 c) 1); y 3. determinando los niveles de riesgo;	4	Repetible
e) evalúe los riesgos de seguridad de la información: 1. comparando los resultados del análisis de riesgos con los criterios de riesgos establecidos en el punto 6.1.2 a); y 2. priorizando el tratamiento de los riesgos analizados.	4	Repetible
La organización debe conservar información documentada sobre el proceso de evaluación de riesgos de seguridad de la información.	4	Repetible
6.1.3 Tratamiento de riesgos de seguridad de la información	3	Repetible
La organización debe definir y efectuar un proceso de tratamiento de riesgos de seguridad de la información para:	4	Repetible
a) seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de información teniendo en cuenta los resultados de la apreciación de riesgos;	2	Inicial
b) determinar todos los controles que sean necesarios para implementar la(s) opción(es) de tratamiento de los riesgos de seguridad de información;	3	Repetible
NOTA: Las organizaciones pueden diseñar controles según sea necesario, o identificarlos a partir de cualquier fuente.	2	Inicial
c) comparar los controles determinados en el punto 6.1.3 b) con los del Anexo A y comprobar que no se han omitido los controles necesarios;	2	Inicial
NOTA1: El Anexo A contiene una amplia lista de objetivos de control y controles. Se indica a los usuarios de esta Norma Internacional que se dirijan al Anexo A para asegurarse que no se pasen por alto los controles necesarios.	2	Inicial

NOTA2: Los objetivos de control se incluyen implícitamente en los controles seleccionados. Los objetivos de control y los controles enumerados en el Anexo A no son exhaustivos, por lo que pueden ser necesarios objetivos de control y controles adicionales.	2	Inicial
d) elaborar una "Declaración de aplicabilidad" que contenga los controles necesarios (véase los puntos 6.1.3 b) y c)) y la justificación de las inclusiones, estén implementados o no, y la justificación de las exclusiones de controles del Anexo A;	2	Inicial
e) formular un plan de tratamiento de riesgos de seguridad de la información; y	4	Repetible
f) obtener la aprobación del plan de tratamiento de riesgos de la seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información por parte de los propietarios de los riesgos.	4	Repetible
La organización debe conservar información documentada sobre el proceso de tratamiento de los riesgos de seguridad de información.	4	Repetible
NOTA: El proceso de evaluación y tratamiento de riesgos de seguridad de información recogidos en esta Norma Internacional se alinean con los principios y directrices genéricas definidos en la Norma ISO 31000. [5]	4	Repetible
6.2 Objetivos de seguridad de la información y planificación para su consecución	2	Inicial
La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.	2	Inicial
Los objetivos de seguridad de la información deben:	2	Inicial
a) ser coherentes con la política de seguridad de la información;	2	Inicial
b) ser medibles (si es posible);	2	Inicial
c) tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la evaluación y del tratamiento de los riesgos;	1	Inicial
d) ser comunicados; y	1	Inicial
e) ser actualizados, según sea apropiado.	1	Inicial
La organización debe conservar información documentada sobre los objetivos de seguridad de la información.	1	Inicial
Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar:	2	Inicial
f) lo que se va a hacer;	2	Inicial
g) qué recursos se requerirán;	2	Inicial

h) quién será responsable;	2	Inicial
i) cuándo se finalizará; y	2	Inicial
j) cómo se evaluarán los resultados.	2	Inicial
7. SOPORTE	3	Repetible
7.1 Recursos	4	Repetible
La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.	4	Repetible
7.2 Competencia	3	Repetible
La organización debe:	3	Repetible
a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en seguridad de la información; y	3	Repetible
b) asegurarse de que estas personas son competentes, basándose en la educación, formación o experiencias adecuadas;	3	Repetible
c) cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo; y	3	Repetible
d) conservar la información documentada apropiada, como evidencia de la competencia.	3	Repetible
NOTA: Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.	3	Repetible
7.3 Concienciación	2	Inicial
Las personas que trabajan bajo el control de la organización deben ser conscientes de:	2	Inicial
a) la política de seguridad de la información;	2	Inicial
b) su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de una mejora del desempeño en seguridad de la información; y	2	Inicial
c) las consecuencias de no cumplir con los requisitos del sistema de gestión de seguridad de la información.	2	Inicial
7.4 Comunicación	1	Inicial
La organización debe determinar la necesidad de las comunicaciones internas y externas pertinentes al sistema de gestión de seguridad de la información, que incluyan:	1	Inicial
a) qué comunicar;	1	Inicial
b) cuándo comunicar;	1	Inicial
c) a quién comunicar;	1	Inicial

d) quién debe comunicar;	1	Inicial
e) los procesos por los que debe efectuarse la comunicación.	1	Inicial
7.5 Información Documentada	4	Repetible
7.5.1 Consideraciones generales	4	Repetible
El sistema de gestión de seguridad de la información de la organización debe incluir:	4	Repetible
a) la información documentada requerida por esta Norma Internacional;	3	Repetible
b) la información documentada que la organización determinó como necesaria para la eficacia del sistema de gestión de seguridad de la información.	4	Repetible
NOTA: El alcance de la información documentada para un sistema de gestión de seguridad de la información puede ser diferente de una organización a otra, debido a: 1. el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios; 2. la complejidad de los procesos y sus interacciones; y 3. la competencia de las personas.	4	Repetible
7.5.2 Creación y actualización	4	Repetible
Cuando se crea y actualiza la información documentada, la organización debe asegurarse, en la manera que corresponda, de lo siguiente:	4	Repetible
a) la identificación y descripción (por ejemplo, título, fecha, autor, o número de referencia);	3	Repetible
b) formato (por ejemplo, idiomas, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);	3	Repetible
c) revisión y aprobación con respecto a la idoneidad y adecuación.	4	Repetible
7.5.3 Control de la información documentada	4	Repetible
La información documentada requerida por el sistema de gestión de seguridad de la información y por esta Norma internacional se debe controlar para asegurarse de que:	4	Repetible
a) esté disponible y preparada para su uso, dónde y cuándo se necesite;	4	Repetible
b) esté protegida adecuadamente (por ejemplo, contra la pérdida de confidencialidad, uso inadecuado, o pérdida de la integridad).	3	Repetible
Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:	4	Repetible
c) distribución, acceso, recuperación y uso;	3	Repetible
d) almacenamiento y preservación, incluida la preservación de la legibilidad;	3	Repetible
e) control de cambios (por ejemplo, control de versión);	3	Repetible

f) retención y disposición.	3	Repetible
La información documentada de origen externo, que la organización determina que es necesaria para la planificación y operación del sistema de gestión de seguridad de la información se debe identificar y controlar, según sea adecuado.	4	Repetible
NOTA: El acceso implica una decisión concerniente al permiso para solamente consultar la información documentada, o el permiso y la autoridad para consultar y modificar la información documentada, etc.	4	Repetible
8. OPERACIÓN	3	Repetible
8.1 Planificación y control operacional	4	Repetible
La organización debe planificar, ejecutar y controlar los procesos necesarios para cumplir los requisitos de seguridad de información y para implementar las acciones determinadas en el apartado 6.1. La organización debe implementar también planes para alcanzar los objetivos de seguridad de la información determinada en el apartado 6.2. En la medida necesaria la organización debe mantener información documentada, para tener la confianza de que los procesos se han llevado a cabo según lo planificado. La organización debe controlar los cambios planificados y examinar las consecuencias de los cambios no previstos, llevando a cabo acciones para mitigar los efectos adversos, cuando sea necesario. La organización debe asegurarse de que los procesos contratados externamente estén controlados.	4	Repetible
8.2 Evaluación de riesgos de seguridad de la información	4	Repetible
La organización debe llevar a cabo evaluaciones de riesgos de seguridad de la información a intervalos planificados, y cuando se propongan o se produzcan modificaciones importantes, teniendo en cuenta los criterios establecidos en el punto 6.1.2 a). La organización debe conservar información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.	4	Repetible
8.3 Tratamiento de riesgos de seguridad de la información	2	Inicial
La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información. La organización debe conservar información documentada de los resultados del tratamiento de los riesgos de seguridad de la información.	2	Inicial
9. EVALUACIÓN DEL DESEMPEÑO	0	Inexistente
9.1 Seguimiento, medición, análisis y evaluación	0	Inexistente
La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información.	0	Inexistente
La organización debe determinar:	0	Inexistente

a) a qué es necesario hacer seguimiento y qué es necesario medir, incluyendo procesos y controles de seguridad de la información;	0	Inexistente
b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos;	0	Inexistente
NOTA: Los métodos seleccionados deben producir resultados comparables y reproducibles para ser considerados válidos.	0	Inexistente
c) cuándo se debe llevar a cabo el seguimiento y la medición;	0	Inexistente
d) quién debe hacer el seguimiento y la medición;	0	Inexistente
e) cuándo se deben analizar y evaluar los resultados del seguimiento y la medición;	0	Inexistente
f) quién debe analizar y evaluar esos resultados.	0	Inexistente
La organización debe conservar la información documentada adecuada como evidencia de los resultados.	0	Inexistente
9.2 Auditoría Interna	0	Inexistente
La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información sobre si el sistema de gestión de seguridad de la información:	0	Inexistente
a) cumple con: 1. los requisitos propios de la organización para su sistema de gestión de seguridad de la información; y 2. los requisitos de esta norma internacional;	0	Inexistente
b) está implementado y mantenido de manera eficaz.	0	Inexistente
La organización debe:	0	Inexistente
c) planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, métodos, responsabilidades, requisitos de planificación y elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de auditorías previas;	0	Inexistente
d) para cada auditoría, definir sus criterios y su alcance;	0	Inexistente
e) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad e imparcialidad del proceso de auditoría;	0	Inexistente
f) asegurarse de que se informe a la dirección pertinente los resultados de las auditorías; y	0	Inexistente
g) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.	0	Inexistente
9.3 Revisión de la Dirección	0	Inexistente

La alta dirección debe revisar el sistema de gestión de seguridad de información de la organización a intervalos planificados para asegurarse de su conveniencia, adecuación y eficacia continuas.	0	Inexistente
La revisión por la dirección debe incluir consideraciones sobre:	0	Inexistente
a) el estado de las acciones desde anteriores revisiones realizadas por la dirección;	0	Inexistente
b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de seguridad de la información;	0	Inexistente
c) la información sobre el comportamiento de la seguridad de la información, incluidas las tendencias relativas a: 1. no conformidades y acciones correctivas; 2. seguimiento y resultados de las mediciones; 3. resultados de las auditorías; y 4. el cumplimiento de los objetivos de seguridad de la información.	0	Inexistente
d) los comentarios provenientes de las partes interesadas;	0	Inexistente
e) los resultados de la evaluación del riesgo y el estado del plan de tratamiento de riesgos; y	0	Inexistente
f) las oportunidades de mejora continua.	0	Inexistente
Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de seguridad de la información. La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.	0	Inexistente
10. MEJORA	0	Inexistente
10.1 No conformidades y acciones correctivas	0	Inexistente
Cuando se produce una no conformidad, la organización debe:	0	Inexistente
a) reaccionar a la no conformidad, y según sea el caso: 1. tomar medidas para controlarla y corregirla; y 2. hacer frente a las consecuencias;	0	Inexistente
b) evaluar la necesidad de acciones para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir o producirse en otros lugares, al: 1. revisar la no conformidad; 2. Determinar las causas de la no conformidad; y 3. determinar si existen incumplimientos similares o podrían producirse.	0	Inexistente
c) implementar medidas oportunas;	0	Inexistente

d) revisar la eficacia de las medidas correctivas adoptadas; y	0	Inexistente
e) si es necesario, hacer cambios al sistema de gestión de seguridad de la información.	0	Inexistente
Las acciones correctivas deben ser adecuadas a los efectos de las no conformidades encontradas.	0	Inexistente
La organización debe conservar información documentada como evidencia de:	0	Inexistente
f) la naturaleza de las no conformidades y de cualquier acción tomada posteriormente, y	0	Inexistente
g) los resultados de cualquier acción correctiva.	0	Inexistente
10.2 Mejora continua	0	Inexistente
La organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información.	0	Inexistente

ANEXO C - INVENTARIO DE ACTIVOS DE INFORMACIÓN						
Nº	Nombre del Activo	Descripción	Propietario	Custodio	Tipo	Ubicación
1	Sistema BPCS	Concentra y procesa todas las transacciones que afectan los estados financieros de la empresa.	Gerencia de Crédito y Cobranza	Gerencia de Sistemas	Software	Digital
2	Base de Datos Sistema BPCS	Es la base de datos del Sistema BPCS.	Gerencia de Crédito y Cobranza	Gerencia de Sistemas	Software	Digital
3	Sistema Operativo Sistema BPCS	Es el sistema operativo del servidor en el que funciona el Sistema BPCS.	Gerencia de Crédito y Cobranza	Gerencia de Sistemas	Software	Digital
4	Sistema Cognos	Recopila información de las diferentes bases de datos transaccionales, las procesa y entregar indicadores gerenciales.	Subgerencia de Ventas	Gerencia de Sistemas	Software	Digital
5	Base de Datos Sistema Cognos	Es la base de datos del Sistema Cognos.	Subgerencia de Ventas	Gerencia de Sistemas	Software	Digital
6	Sistema Operativo Sistema Cognos	Es el sistema operativo del servidor en el que funciona el Sistema Cognos.	Subgerencia de Ventas	Gerencia de Sistemas	Software	Digital
7	Sistema Aheeva	Su función es gestionar las llamadas a través del Call Center para la venta y atención a los clientes de la empresa.	Gerencia Crédito Facilito	Gerencia de Sistemas	Software	Digital
8	Base de Datos Sistema Aheeva	Es la base de datos del Sistema Aheeva.	Gerencia Crédito Facilito	Gerencia de Sistemas	Software	Digital

ANEXO C - INVENTARIO DE ACTIVOS DE INFORMACIÓN						
Nº	Nombre del Activo	Descripción	Propietario	Custodio	Tipo	Ubicación
9	Sistema Operativo Sistema Aheeva	Es el sistema operativo del servidor en el que funciona el Sistema Aheeva.	Gerencia Crédito Facilito	Gerencia de Sistemas	Software	Digital
10	Sistema Facturación Digital	Su función es enviar el archivo XML con los requerimientos para emitir comprobantes electrónicos del SRI.	Gerencia Financiera	Gerencia de Sistemas	Software	Digital
11	Sistema Operativo Sistema Facturación Digital	Es el sistema operativo del servidor en el que funciona el Sistema Facturación Digital.	Gerencia Financiera	Gerencia de Sistemas	Software	Digital
12	Sistema SIAC	Concentrar y procesa las transacciones relacionadas con las operaciones de crédito, cobranza, ventas, servicio al cliente, inventario, órdenes de trabajo, asistencias y gestión de productos.	Gerencia de Crédito y Cobranza	Gerencia de Sistemas	Software	Digital
13	Base de Datos del Sistema SIAC	Base de Datos del Sistema SIAC.	Gerencia de Crédito y Cobranza	Gerencia de Sistemas	Software	Digital
14	Sistema Operativo Base de Datos del Sistema SIAC	Es el sistema operativo del servidor en el que funciona la base de datos del Sistema SIAC.	Gerencia de Crédito y Cobranza	Gerencia de Sistemas	Software	Digital
15	Sistema Operativo Sistema SIAC	Es el sistema operativo del servidor en el que funciona el Sistema SIAC.	Gerencia de Crédito y Cobranza	Gerencia de Sistemas	Software	Digital

ANEXO C - INVENTARIO DE ACTIVOS DE INFORMACIÓN						
Nº	Nombre del Activo	Descripción	Propietario	Custodio	Tipo	Ubicación
16	Sistema SIG	Su función es recopilar información de las diferentes bases de datos transaccionales, procesarlas y entregar indicadores gerenciales.	Subgerencia de Ventas	Gerencia de Sistemas	Software	Digital
17	Base de Datos Sistema SIG	Es la base de datos del Sistema SIG.	Subgerencia de Ventas	Gerencia de Sistemas	Software	Digital
18	Sistema Operativo Sistema SIG	Es el sistema operativo del servidor en el que funciona el Sistema SIG.	Subgerencia de Ventas	Gerencia de Sistemas	Software	Digital
19	Sistema GTM	Su función es gestionar y procesar la documentación para la matriculación de motos.	Gerencia de Crédito y Cobranza	Gerencia de Sistemas	Software	Digital
20	Base de Datos Sistema GTM	Es la base de datos del Sistema GTM.	Gerencia de Crédito y Cobranza	Gerencia de Sistemas	Software	Digital
21	Sistema Operativo Sistema GTM	Es el sistema operativo del servidor en el que funciona el Sistema GTM.	Gerencia de Crédito y Cobranza	Gerencia de Sistemas	Software	Digital
22	Sistema Intranet General	Su función es presentar información de interés para los empleados, tales como Eventos, Comunicación, Noticias, Anuncios, Políticas Internas entre otra información corporativa.	Gerencia de Sistemas	Gerencia de Sistemas	Software	Digital

ANEXO C - INVENTARIO DE ACTIVOS DE INFORMACIÓN						
Nº	Nombre del Activo	Descripción	Propietario	Custodio	Tipo	Ubicación
23	Base de Datos Sistema Intranet General	Es la base de datos del Sistema Intranet General.	Gerencia de Sistemas	Gerencia de Sistemas	Software	Digital
24	Sistema Operativo Sistema Intranet General	Es el sistema operativo del servidor en el que funciona el Sistema Intranet General.	Gerencia de Sistemas	Gerencia de Sistemas	Software	Digital
25	Sistema Código de Barra	Su función es imprimir etiquetas codificadas que son utilizadas para inventariar los productos en bodega.	Gerencia Logística	Gerencia de Sistemas	Software	Digital
26	Sistema Operativo Sistema Código de Barra	Es el sistema operativo del servidor en el que funciona el Sistema Código de Barra.	Gerencia Logística	Gerencia de Sistemas	Software	Digital
27	Sistema Comisiones	Su función es evaluar el cumplimiento de controles de inventario, ventas, publicidad, crédito, caja, gestión de problemas y cobranzas para calcular la bonificación que recibirán los jefes de almacén.	Subgerencia de Ventas	Gerencia de Sistemas	Software	Digital
28	Base de Datos Sistema Comisiones	Es la base de datos del Sistema Comisiones.	Subgerencia de Ventas	Gerencia de Sistemas	Software	Digital
29	Sistema Operativo Sistema Comisiones	Es el sistema operativo del servidor en el que funciona el Sistema Comisiones.	Subgerencia de Ventas	Gerencia de Sistemas	Software	Digital

ANEXO C - INVENTARIO DE ACTIVOS DE INFORMACIÓN						
Nº	Nombre del Activo	Descripción	Propietario	Custodio	Tipo	Ubicación
30	Correo Electrónico	Envío y recepción de correos electrónicos internos y externos.	Gerencia de Sistemas	Gerencia de Sistemas	Software	Digital
31	Sistema operativo Correo electrónico	Es el sistema operativo del servidor en el que funciona el correo electrónico.	Gerencia de Sistemas	Gerencia de Sistemas	Software	Digital
32	Centro de Cómputo	Instalación física de propiedad de la empresa en donde operan los sistemas de la empresa.	Gerencia de Sistemas	Jefatura de Infraestructura	Instalación	Física
33	Instructivos de los programas de la empresa (Políticas y/o procedimientos internos)	Documentos de uso interno de las Áreas de la empresa involucradas en el alcance.	Gerente de Procesos	Jefatura de Procesos	Información	Digital
34	Responsable de Seguridad de la Información	Persona contratada por la empresa para la administración, operación y mejora del Sistema de Gestión de Seguridad de la Información SGSI.	Gerencia de Auditoría y Seguridad de la Información	Gerencia de Auditoría y Seguridad de la Información	Personal	Física
35	Responsable de Seguridad del Área de TI	Persona encargada de seguridad en el Área de Tecnología de la Información que ejecuta controles de seguridad de la información.	Jefatura de Infraestructura	Jefatura de Infraestructura	Personal	Física

ANEXO C - INVENTARIO DE ACTIVOS DE INFORMACIÓN						
Nº	Nombre del Activo	Descripción	Propietario	Custodio	Tipo	Ubicación
36	Coordinadores y Analistas de las Áreas involucradas en el alcance del SGSI	Personas responsables de la ejecución de tareas en cada uno de los subprocesos que componen el alcance del SGSI.	Vicepresidencia Comercial y Corporativa	Vicepresidencia Comercial y Corporativa	Personal	Física
37	Aprobadores de operaciones de crédito	Personas que apruebas operaciones de crédito.	Gerencia de Crédito y Cobranza	Gerencia de Crédito y Cobranza	Personal	Física
38	Oficinas JTM	Ubicación física donde opera el proceso del alcance del SGSI.	Vicepresidencia Comercial y Corporativa	Vicepresidencia Comercial y Corporativa	Instalación	Física
39	Documentos del SGSI	Conjunto de informes, procedimientos y registros que permiten una administración adecuada del SGSI.	Gerencia de Auditoría y Seguridad de la Información	Gerencia de Auditoría y Seguridad de la Información	Información	Digital
40	Red interna	Equipos que permiten la comunicación en la red interna de la empresa.	Gerencia de Sistemas	Jefatura de Infraestructura	Hardware	Física
41	Equipos de comunicación de acceso	Corresponden a los routers en cada área de la empresa.	Gerencia de Sistemas	Jefatura de Infraestructura	Hardware	Física
42	Equipos de comunicación core	Corresponden a los routers core de la red interna.	Gerencia de Sistemas	Jefatura de Infraestructura	Hardware	Física

ANEXO C - INVENTARIO DE ACTIVOS DE INFORMACIÓN						
Nº	Nombre del Activo	Descripción	Propietario	Custodio	Tipo	Ubicación
43	Firewall	Firewall de alta disponibilidad.	Gerencia de Sistemas	Jefatura de Infraestructura	Hardware	Física
44	Sistema de control de acceso a la red	Software que controla todos los accesos a la red interna de la empresa.	Gerencia de Sistemas	Jefatura de Infraestructura	Software	Digital
45	Chasis Blade Center	Equipo que contiene servidores Blade proporcionándoles comunicación y fuentes de alimentación de energía.	Gerencia de Sistemas	Jefatura de Infraestructura	Hardware	Física
46	Servidor Blade	En el servidor se encuentran alojados de manera virtual ciertos sistemas de la empresa.	Gerencia de Sistemas	Jefatura de Infraestructura	Hardware	Física
47	Sistema Operativo Servidor Blade	Software de virtualización que permite ejecutar varios sistemas operativos (máquinas virtuales) sobre la misma máquina física (servidor blade).	Gerencia de Sistemas	Jefatura de Infraestructura	Software	Digital
48	Equipo storage	Equipo de Almacenamiento que contiene los datos de los servidores virtuales de la empresa.	Gerencia de Sistemas	Jefatura de Infraestructura	Hardware	Física

ANEXO C - INVENTARIO DE ACTIVOS DE INFORMACIÓN						
Nº	Nombre del Activo	Descripción	Propietario	Custodio	Tipo	Ubicación
49	Directorio Activo	Herramienta que permite administrar el acceso de los usuarios a la red interna de la empresa.	Gerencia de Sistemas	Jefatura de Infraestructura	Software	Digital
50	Sistema operativo del Directorio Activo	Es el sistema operativo del servidor en el que funciona el directorio activo.	Gerencia de Sistemas	Jefatura de Infraestructura	Software	Digital
51	Medios de respaldos	Discos externos utilizados para almacenar copias de respaldos de información de las distintas aplicaciones de la empresa.	Gerencia de Sistemas	Jefatura de Infraestructura	Hardware	Física
52	Ticket de Servicio al Cliente	Ticket levantado en la Mesa de Servicios para dar seguimiento a problemas.	Gerencia Crédito Facilito	Jefatura de Servicio al Cliente	Información	Digital
53	Mesa de Servicio	Conjunto de recursos tecnológicos y humanos que prestan servicios de manera integral.	Gerencia de Sistemas	Gerencia de Sistemas	Software	Digital

ANEXO C - INVENTARIO DE ACTIVOS DE INFORMACIÓN						
Nº	Nombre del Activo	Descripción	Propietario	Custodio	Tipo	Ubicación
54	Buró de Crédito	Consulta de información crediticia de clientes con otras entidades comerciales y financieras.	Gerencia de Sistemas	Gerencia de Sistemas	Servicios	Digital
55	Registro Civil	Consulta de información personal y domiciliaria del cliente.	Gerencia de Sistemas	Gerencia de Sistemas	Servicios	Digital
56	Actas de entrega de comprobantes	Control de documentos entregados para el proceso de dación.	Gerencia de Crédito y Cobranza	Auxiliar de Cobranzas	Información	Digital
57	Confirmaciones bancarias	Aplicación de pagos de clientes realizados mediante transferencias o depósitos bancarios.	Gerencia de Crédito y Cobranza	Auxiliar de Cobranzas	Información	Digital
58	Hoja de negociación	Diferentes tipos de negociaciones para deudas vencidas de acuerdo a las validaciones que exige el sistema.	Gerencia de Crédito y Cobranza	Auxiliar de Cobranzas	Información	Digital
59	Reporte de Cartera	Reporte con detalles de clientes vencidos con varias columnas de información.	Gerencia de Crédito y Cobranza	Auxiliar de Cobranzas	Información	Digital
60	Informe de Cobranzas	Reporte de valores sean en efectivo o por documentos.	Gerencia de Crédito y Cobranza	Auxiliar de Cobranzas	Información	Digital
61	Análisis de Productividad	Consulta diaria de las gestiones telefónicas realizadas de todos los gestores telefónicos.	Gerencia de Crédito y Cobranza	Supervisor del CAAC	Información	Digital

ANEXO C - INVENTARIO DE ACTIVOS DE INFORMACIÓN						
Nº	Nombre del Activo	Descripción	Propietario	Custodio	Tipo	Ubicación
62	Listado de anticipos	Sirve para revisar el dinero que dejó el cliente para negociación.	Gerencia de Crédito y Cobranza	Auxiliar de Cobranzas	Información	Digital
63	Reporte La Garantía	Archivo con detalle de órdenes de trabajo apertura das en Taller La Garantía.	Jefatura Comercial La Garantía	Jefatura Comercial La Garantía	Información	Digital
64	Reporte de concreción de cotizaciones	Reporte semanal con los indicadores de cotizaciones.	Subgerencia de Ventas	Subgerencia de Ventas	Información	Digital
65	Disposición de Bodegas de Agencias	Disposición física de mercadería en agencias.	Gerencia de Mercadeo	Jefatura de Mercadeo	Información	Digital

ANEXO D - VALORACIÓN DE CRITICIDAD DE LOS ACTIVOS DE INFORMACIÓN							
Nº	NOMBRE DEL ACTIVO	TIPO	Confidencialidad	Disponibilidad	Integridad	Valor	Importancia
1	Sistema BPCS	Software	4	6	6	5	Alto
2	Base de Datos Sistema BPCS	Software	4	6	6	5	Alto
3	Sistema Operativo Sistema BPCS	Software	4	6	6	5	Alto
4	Sistema Cognos	Software	4	5	6	5	Alto
5	Base de Datos Sistema Cognos	Software	4	5	6	5	Alto
6	Sistema Operativo Sistema Cognos	Software	4	5	6	5	Alto
7	Sistema Aheeva	Software	4	5	5	5	Alto
8	Base de Datos Sistema Aheeva	Software	4	5	5	5	Alto
9	Sistema Operativo Sistema Aheeva	Software	4	5	5	5	Alto
10	Sistema Facturación Electrónica	Software	4	5	5	5	Alto
11	Sistema Operativo Sistema Facturación Electrónica	Software	4	5	5	5	Alto
12	Sistema SIAC	Software	4	6	6	5	Alto
13	Base de Datos del Sistema SIAC	Software	4	6	6	5	Alto
14	Sistema Operativo Base de Datos del Sistema SIAC	Software	4	6	6	5	Alto
15	Sistema Operativo Sistema SIAC	Software	4	6	6	5	Alto
16	Sistema SIG	Software	4	4	4	4	Medio
17	Base de Datos Sistema SIG	Software	4	4	4	4	Medio
18	Sistema Operativo Sistema SIG	Software	4	4	4	4	Medio
19	Sistema GTM	Software	4	4	4	4	Medio
20	Base de Datos Sistema GTM	Software	4	4	4	4	Medio
21	Sistema Operativo Sistema GTM	Software	4	4	4	4	Medio
22	Sistema Intranet General	Software	3	4	3	3	Bajo

ANEXO D - VALORACIÓN DE CRITICIDAD DE LOS ACTIVOS DE INFORMACIÓN							
Nº	NOMBRE DEL ACTIVO	TIPO	Confidencialidad	Disponibilidad	Integridad	Valor	Importancia
23	Base de Datos Sistema Intranet General	Software	3	4	3	3	Bajo
24	Sistema Operativo Sistema Intranet General	Software	3	4	3	3	Bajo
25	Sistema Código de Barra	Software	4	4	5	4	Medio
26	Sistema Operativo Sistema Código de Barra	Software	4	4	5	4	Medio
27	Sistema Comisiones	Software	4	5	5	5	Alto
28	Base de Datos Sistema Comisiones	Software	4	5	5	5	Alto
29	Sistema Operativo Sistema Comisiones	Software	4	5	5	5	Alto
30	Correo Electrónico	Software	3	6	6	5	Alto
31	Sistema operativo Correo electrónico	Software	4	6	6	5	Alto
32	Centro de Cómputo	Instalaciones	4	6	6	5	Alto
33	Instructivos de los programas de la empresa (Políticas y/o procedimientos internos)	Información	3	3	4	3	Bajo
34	Responsable de Seguridad de la Información	Personal	1	6	1	3	Bajo
35	Responsable de Seguridad del Área de TI	Personal	1	6	1	3	Bajo
36	Coordinadores y Analistas de las Áreas involucradas en el alcance del SGSI	Personal	1	6	1	3	Bajo
37	Aprobadores de operaciones de crédito	Personal	1	6	1	3	Bajo
38	Oficinas JTM	Instalaciones	3	6	6	5	Alto
39	Documentos del SGSI	Información	3	3	4	3	Bajo
40	Red interna	Hardware	4	6	6	5	Alto
41	Equipos de comunicación de acceso	Hardware	4	6	6	5	Alto
42	Equipos de comunicación core	Hardware	4	6	6	5	Alto
43	Firewall	Hardware	4	6	6	5	Alto
44	Sistema de control de acceso a la red	Software	4	6	6	5	Alto

ANEXO D - VALORACIÓN DE CRITICIDAD DE LOS ACTIVOS DE INFORMACIÓN							
Nº	NOMBRE DEL ACTIVO	TIPO	Confidencialidad	Disponibilidad	Integridad	Valor	Importancia
45	Chasis BladeCenter	Hardware	4	6	6	5	Alto
46	Servidor Blade	Hardware	4	6	6	5	Alto
47	Sistema Operativo Servidor Blade	Software	4	6	6	5	Alto
48	Equipo Storage	Hardware	4	6	6	5	Alto
49	Directorio Activo	Software	4	5	5	5	Alto
50	Sistema operativo del Directorio Activo	Software	4	5	5	5	Alto
51	Medios de respaldos	Hardware	4	6	6	5	Alto
52	Ticket de Servicio al Cliente	Información	4	4	4	4	Medio
53	Mesa de Servicio	Software	3	5	4	4	Medio
54	Buró de Crédito	Servicios	4	5	5	5	Alto
55	Registro Civil	Servicios	4	5	5	5	Alto
56	Actas de entrega de comprobantes	Información	4	5	5	5	Alto
57	Confirmaciones bancarias	Información	4	5	5	5	Alto
58	Hoja de negociación	Información	5	5	5	5	Alto
59	Reporte de Cartera	Información	4	5	5	5	Alto
60	Informe de Cobranzas	Información	4	5	5	5	Alto
61	Análisis de Productividad	Información	4	5	5	5	Alto
62	Listado de anticipos	Información	4	5	5	5	Alto
63	Reporte La Garantía	Información	4	5	5	5	Alto
64	Reporte de concreción de cotizaciones	Información	4	5	5	5	Alto
65	Layout de Bodegas de Agencias	Información	4	5	5	5	Alto

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
HW	Accidentales (A)	Fallas técnicas – Hardware	Falta de instalaciones, equipos o procesos de respaldo.
HW	Accidentales (A)	Fallas técnicas – Hardware	Falta de mantenimiento de equipos e instalaciones.
HW	Accidentales (A)	Fallas técnicas – Hardware	Falta de políticas y procedimientos de control de cambios.
HW	Accidentales (A)	Fallas técnicas – Hardware	Falta de procedimientos de monitoreo de hardware.
HW	Accidentales (A)	Fallas técnicas – Hardware	Falta de procedimientos de planeación de la capacidad del hardware.
HW	Accidentales (A)	Fallas técnicas – Hardware	No está definido un plan de continuidad o de recuperación de información o de activos de información.
HW	Deliberadas (D)	Acceso no autorizado a datos	Falta de un procedimiento de registro y autorización de salida de equipos.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
HW, IN	Deliberadas (D)	Sabotaje	Falta de seguridad física.
HW, IN	Entorno (E)	Fluctuaciones de potencia eléctrica	No está definido un plan de continuidad o de recuperación de información o de activos de información.
HW, IN	Entorno (E)	Fluctuaciones de potencia eléctrica	No existen sistemas de regulación.
ID, HW	Deliberadas (D)	Acceso remoto no autorizado a la red	Falta de políticas respecto al acceso a la red .
ID, HW, IN	Deliberadas (D)	Sniffing	Falta de seguridad física de los dispositivos de comunicaciones, cableado.
ID, HW, SR	Deliberadas (D)	Sniffing	Comunicaciones sin cifrado.
ID, HW, SR	Deliberadas (D)	Sniffing	Falta de segmentación lógica o física de la red.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
IF, HW, IN, SR	Deliberadas (D)	Destrucción de la información	Falta de medidas de protección física.
IF, ID, HW, IN	Entorno (E)	Inundación	Localización en áreas susceptibles a inundación.
IF, ID, PE	Deliberadas (D)	Divulgación de la información	Desconocimiento de procesos disciplinarios / regulatorios.
IF, ID, PE	Deliberadas (D)	Divulgación de la información	Entrenamiento insuficiente en seguridad.
IF, ID, PE	Deliberadas (D)	Divulgación de la información	Falta de conciencia en seguridad de la información.
IF, ID, PE	Deliberadas (D)	Divulgación de la información	Falta de incentivos al personal y oportunidades de crecimiento.
IF, ID, PE, SR	Deliberadas (D)	Manipulación de la información	Desconocimiento de procesos disciplinarios / regulatorios.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
IF, ID, PE, SR	Deliberadas (D)	Violación (conciente o no intencional) de las políticas de seguridad por parte de los empleados	No existencia de una política general de seguridad de la información.
IN	Accidentales (A)	Fallas técnicas – Hardware	Falta de protección ambiental.
PE	Accidentales (A)	Falla en la elección del personal	Falta de especificaciones con respecto a la selección de personal.
PE	Deliberadas (D)	Extorsión / Corrupción	Desconocimiento de procesos disciplinarios / regulatorios.
PE	Deliberadas (D)	Pérdida o ausencia de personal clave	Falta de acuerdos definidos para reemplazo de empleados.
PE, SR	Deliberadas (D)	Ingeniería Social	Desconocimiento de procesos disciplinarios / regulatorios.
PE, SR	Deliberadas (D)	Ingeniería Social	Falta de lineamientos que establezcan que no se debe suministrar información a terceros hasta no verificar la identidad y autoridad del solicitante.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SR	Accidentales (A)	Demoras o no restauración de los servicios ante una emergencia	Falta de garantías de la disponibilidad del servicio por parte del proveedor.
SR	Accidentales (A)	Destrucción de instalaciones, datos y equipos	Falta de garantías de la disponibilidad del servicio por parte del proveedor.
SR	Accidentales (A)	Deterioro de la calidad de servicios prestados por terceros	Falta de pruebas de los planes de respuesta ante incidentes.
SR	Deliberadas (D)	Negación de servicio	Falta de garantías de la disponibilidad del servicio por parte del proveedor.
SR	Deliberadas (D)	Sabotaje	Falta de garantías de la disponibilidad del servicio por parte del proveedor.
SW	Deliberadas (D)	Uso de software pirata	Falta de una política de uso de software licenciado.
SW, HW, SR	Accidentales (A)	Deterioro de la calidad de servicios prestados por terceros	No existe un monitoreo de los niveles de desempeño y servicios (SLA) de los proveedores.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, HW, SR	Accidentales (A)	Falla en servicios de comunicación	Administración inadecuada de la seguridad de la red.
SW, HW, SR	Accidentales (A)	Falla en servicios de comunicación	Falta de planeación en capacidad o cambios no autorizados en la red.
SW, HW, SR	Accidentales (A)	Falla en servicios de comunicación	No existe un proveedor alterno de canales de comunicación.
SW, ID	Accidentales (A)	Fallas técnicas – Software base	Falta de procedimientos de actualización de software base.
SW, ID	Deliberadas (D)	Acceso no autorizado a datos	Configuración o mantenimiento de seguridad de sistemas incorrectos (aplicativos, sistemas operativos, bases de datos).
SW, ID	Deliberadas (D)	Cambios no autorizados a datos	Falta de políticas y procedimientos de control de cambios.
SW, ID	Deliberadas (D)	Cambios no autorizados a datos	Supervisión inadecuada de los programadores.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, ID	Deliberadas (D)	Errores de software / programación	Especificaciones incompletas o confusas.
SW, ID	Deliberadas (D)	Errores de software / programación	Procedimientos inadecuados en el Ciclo de Desarrollo del software.
SW, ID	Deliberadas (D)	Intrusión a aplicaciones y web	Estándares inadecuados de desarrollo de software.
SW, ID	Deliberadas (D)	Intrusión a aplicaciones y web	Explotación de debilidades de seguridad del sistema operativo por no tener la última versión / actualización.
SW, ID	Deliberadas (D)	Robo y Fraude	Configuración o mantenimiento de seguridad de sistemas incorrectos (aplicativos, sistemas operativos, bases de datos).
SW, ID	Deliberadas (D)	Robo y Fraude	Falta de políticas y procedimientos de control de cambios.
SW, ID	Deliberadas (D)	Sabotaje	Configuración o mantenimiento de seguridad de sistemas incorrectos (aplicativos, sistemas operativos, bases de datos).

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, ID	Deliberadas (D)	Sabotaje	Falta de políticas y procedimientos de control de cambios.
SW, ID	Deliberadas (D)	Uso de software pirata	Control inapropiado de distribución de software (copias no restringidas).
SW, ID	Entorno (E)	Fluctuaciones de potencia eléctrica	Indisponibilidad de backups de información digital o sistemas de backup.
SW, ID	Entorno (E)	Incendio	Indisponibilidad de backups de información digital o sistemas de backup.
SW, ID	Entorno (E)	Inundación	Indisponibilidad de backups de información digital o sistemas de backup.
SW, ID	Entorno (E)	Temperatura / humedad extremas	Indisponibilidad de backups de información digital o sistemas de backup.
SW, ID, HW	Accidentales (A)	Falla en suministro eléctrico	Indisponibilidad de backups de información digital o sistemas de backup.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, ID, HW	Accidentales (A)	Respuesta no inmediata en la resolución de incidentes	Falta de pruebas de los planes de respuesta ante incidentes.
SW, ID, HW	Deliberadas (D)	Acceso remoto no autorizado a la red	Falta de logs de auditoría.
SW, ID, HW	Deliberadas (D)	Código malicioso	Falta de políticas en el uso de medios removibles de almacenamiento.
SW, ID, HW	Deliberadas (D)	Errores de software / programación	Falta de políticas y procedimientos de control de cambios en configuraciones.
SW, ID, HW	Deliberadas (D)	Errores de usuarios y operadores	Falta de políticas y procedimientos de control de cambios en configuraciones.
SW, ID, HW	Deliberadas (D)	Robo y Fraude	Falta de logs de auditoría.
SW, ID, HW	Deliberadas (D)	Sabotaje	Falta de un procedimiento de administración de privilegios de acceso.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, ID, HW, IN	Accidentales (A)	Destrucción de instalaciones, datos y equipos	Configuración o mantenimiento de seguridad de sistemas incorrectos (aplicativos, sistemas operativos, bases de datos).
SW, ID, HW, IN	Accidentales (A)	Falla en suministro eléctrico	No está definido un plan de continuidad o de recuperación de información o de activos de información.
SW, ID, HW, IN	Accidentales (A)	Falla en suministro eléctrico	No existen sistemas UPS.
SW, ID, HW, IN	Deliberadas (D)	Acceso no autorizado a datos	Falta de seguridad física de los dispositivos de comunicaciones, cableado y servidores.
SW, ID, HW, SR	Deliberadas (D)	Acceso no autorizado a datos	Falta de logs de auditoría.
SW, ID, HW, SR	Deliberadas (D)	Acceso remoto no autorizado a la red	Falta de esquema de firewall / software de detección de intrusos.
SW, ID, HW, SR	Deliberadas (D)	Errores de usuarios y operadores	Falta de documentación de procedimientos (uso y operación).

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, ID, HW, SR	Deliberadas (D)	ID spoofing	Falta de mecanismos de identificación / autenticación confiables (emisor o receptor).
SW, ID, HW, SR	Deliberadas (D)	ID spoofing	Passwords no protegidos (lógica o físicamente).
SW, ID, HW, SR	Deliberadas (D)	Negación de servicio	Administración y monitoreo inadecuado de seguridad de la red.
SW, ID, IN	Entorno (E)	Tormenta	Localización en áreas susceptibles a tormentas.
SW, ID, IN, SR	Entorno (E)	Tormenta	Indisponibilidad de backups de información digital o sistemas de backup.
SW, ID, PE, SR	Deliberadas (D)	Acceso no autorizado a datos	Desconocimiento de procesos disciplinarios / regulatorios.
SW, ID, PE, SR	Deliberadas (D)	Ingeniería Social	Entrenamiento o concienciación insuficiente en seguridad o falta de conocimiento y entrenamiento oportuno.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, ID, PE, SR	Deliberadas (D)	Robo y Fraude	Inadecuada segregación de funciones del personal.
SW, ID, SR	Accidentales (A)	Demoras o no restauración de los servicios ante una emergencia	Falta de pruebas de restauración de backups en ambiente de producción.
SW, ID, SR	Accidentales (A)	Repudio	Falta de uso de firmas digitales.
SW, ID, SR	Accidentales (A)	Repudio	Imposibilidad de probar el envío o recepción de un mensaje.
SW, ID, SR	Deliberadas (D)	Acceso no autorizado a datos	Comunicaciones sin cifrado.
SW, ID, SR	Deliberadas (D)	Acceso no autorizado a datos	Falta de esquema de firewall / software de detección de intrusos.
SW, ID, SR	Deliberadas (D)	Acceso no autorizado a datos	Falta de mecanismos de identificación / autenticación confiables.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, ID, SR	Deliberadas (D)	Acceso no autorizado a datos	Inadecuada segregación de funciones del personal.
SW, ID, SR	Deliberadas (D)	Acceso remoto no autorizado a la red	Falta de mecanismos de identificación / autenticación confiables.
SW, ID, SR	Deliberadas (D)	Acceso remoto no autorizado a la red	Falta de restricciones para acceso remoto.
SW, ID, SR	Deliberadas (D)	Acceso remoto no autorizado a la red	Revelación de información que pueda facilitar una conexión remota no autorizada.
SW, ID, SR	Deliberadas (D)	Cambios no autorizados a datos	Falta de logs de auditoría.
SW, ID, SR	Deliberadas (D)	Cambios no autorizados a datos	Falta de segregación entre programadores/operadores/administradores.
SW, ID, SR	Deliberadas (D)	Cambios no autorizados a datos	Indisponibilidad de backups de información digital o sistemas de backup.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, ID, SR	Deliberadas (D)	Código malicioso	Falta de lineamientos de buen uso de correo electrónico.
SW, ID, SR	Deliberadas (D)	Código malicioso	Falta de mecanismos de actualización del software antivirus.
SW, ID, SR	Deliberadas (D)	Código malicioso	Falta de software de detección de virus instalado en los equipos.
SW, ID, SR	Deliberadas (D)	Código malicioso	Indisponibilidad de backups de información digital o sistemas de backup.
SW, ID, SR	Deliberadas (D)	Destrucción de la información	Falta de un debido control de acceso lógico a usuarios.
SW, ID, SR	Deliberadas (D)	Intrusión a aplicaciones y web	Falta de esquema de firewall / software de detección de intrusos.
SW, ID, SR	Deliberadas (D)	Intrusión a aplicaciones y web	Vulnerabilidades conocidas que sean explotables debido a que no hay un proceso de cooperación o actualización con

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
			organizaciones de seguridad disponibles en línea.
SW, ID, SR	Deliberadas (D)	Negación de servicio	Explotación de debilidades de seguridad del sistema operativo por no tener la última versión / actualización.
SW, ID, SR	Deliberadas (D)	Negación de servicio	Falta de esquema de firewall / software de detección de intrusos.
SW, ID, SR	Deliberadas (D)	Negación de servicio	Vulnerabilidades conocidas que sean explotables debido a que no hay un proceso de cooperación o actualización con organizaciones de seguridad disponibles en línea.
SW, ID, SR	Entorno (E)	Terremoto	Indisponibilidad de backups de información digital o sistemas de backup.
SW, IF, ID	Deliberadas (D)	Divulgación de la información	Almacenamiento no protegido.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, IF, ID	Deliberadas (D)	Robo y Fraude	Copias no controladas de datos y software.
SW, IF, ID, HW	Entorno (E)	Tormenta	No está definido un plan de continuidad o de recuperación de información o de activos de información.
SW, IF, ID, HW, IN	Accidentales (A)	Destrucción de instalaciones, datos y equipos	Falta de seguridad física.
SW, IF, ID, HW, IN	Deliberadas (D)	Robo y Fraude	Falta de seguridad física.
SW, IF, ID, HW, PE	Deliberadas (D)	Sabotaje	Falta de conciencia en seguridad de la información.
SW, IF, ID, HW, PE	Deliberadas (D)	Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento.
SW, IF, ID, HW, PE, IN	Deliberadas (D)	Incapacidad y restauración	No está definido un plan de continuidad o de recuperación de información o de activos de información.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, IF, ID, HW, PE, IN	Deliberadas (D)	Pérdida o ausencia de personal clave	Procedimientos no documentados.
SW, IF, ID, HW, PE, IN	Deliberadas (D)	Robo y Fraude	Inadecuada revisión de antecedentes.
SW, IF, ID, HW, PE, IN	Entorno (E)	Inundación	No está definido un plan de continuidad o de recuperación de información o de activos de información.
SW, IF, ID, HW, PE, IN, SR	Deliberadas (D)	Extorsión / Corrupción	Entrenamiento o concienciación insuficiente en seguridad o falta de conocimiento y entrenamiento oportuno.
SW, IF, ID, HW, PE, IN, SR	Deliberadas (D)	Manipulación de la información	Entrenamiento o concienciación insuficiente en seguridad o falta de conocimiento y entrenamiento oportuno.
SW, IF, ID, HW, PE, IN, SR	Deliberadas (D)	Robo y Fraude	Falta de conciencia en seguridad de la información.
SW, IF, ID, HW, PE, IN, SR	Entorno (E)	Terremoto	No está definido un plan de continuidad o de recuperación de información o de activos de información.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, IF, ID, HW, PE, SR	Deliberadas (D)	Errores de usuarios y operadores	Entrenamiento o concienciación insuficiente en seguridad o falta de conocimiento y entrenamiento oportuno.
SW, IF, ID, IN	Entorno (E)	Incendio	Existencia de materiales inflamables.
SW, IF, ID, IN	Entorno (E)	Incendio	Falta de seguridad física.
SW, IF, ID, IN	Entorno (E)	Incendio	Localización en áreas susceptibles al fuego.
SW, IF, ID, IN	Entorno (E)	Incendio	No está definido un plan de continuidad o de recuperación de información o de activos de información.
SW, IF, ID, IN	Entorno (E)	Incendio	No existen sistemas o mecanismos de detección / extinción de fuego.
SW, IF, ID, IN	Entorno (E)	Temperatura / humedad extremas	Falta de protección ambiental.

ANEXO E - RELACIÓN ACTIVO Y AMENAZA (VULNERABILIDAD)			
Tipo de Activo	Tipo de Amenaza	Amenazas	Vulnerabilidades
SW, IF, ID, IN	Entorno (E)	Temperatura / humedad extremas	Localización en áreas susceptibles a estas condiciones.
SW, IF, ID, IN	Entorno (E)	Temperatura / humedad extremas	Monitoreo inadecuado de condiciones ambientales.
SW, IF, ID, IN	Entorno (E)	Temperatura / humedad extremas	No está definido un plan de continuidad o de recuperación de información o de activos de información.
SW, IF, ID, IN	Entorno (E)	Terremoto	Localización en área susceptible a terremotos.
SW, IF, ID, PE, SR	Deliberadas (D)	Divulgación de la información	Falta de acuerdos de confidencialidad.
SW, IF, ID, SR	Accidentales (A)	Destrucción de instalaciones, datos y equipos	Falta de un procedimiento de administración de privilegios de acceso.
SW, IF, ID, SR	Deliberadas (D)	Robo y Fraude	Falta de mecanismos de identificación / autenticación confiables.

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Red interna	HW	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado
Riesgo Operativo	Red interna	HW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Operativo	Red interna	HW	Falla en suministro eléctrico	3	1	Bajo	Protección de los Equipos Informáticos.	2	1	Bajo
Riesgo Tecnológico	Red interna	HW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Red interna	HW	Fluctuaciones de potencia eléctrica	2	2	Bajo	Protección de ordenadores y sistemas de comunicaciones.	1	2	Bajo
Riesgo Tecnológico	Red interna	HW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Financiero	Red interna	HW	Inundación	3	5	Extremo	Protección de las IN Protección de los Equipos Informáticos	3	3	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Protección del cableado Diseño.			
Riesgo Financiero	Red interna	HW	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Red interna	HW	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Red interna	HW	Terremoto	2	5	Extremo	Aplicación de DRP.	1	4	Alto
Riesgo Financiero	Equipos de comunicación de acceso	HW	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado
Riesgo Operativo	Equipos de comunicación de acceso	HW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Equipos de comunicación de acceso	HW	Falla en suministro eléctrico	3	1	Bajo	Protección de los Equipos Informáticos.	2	1	Bajo
Riesgo Tecnológico	Equipos de comunicación de acceso	HW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Equipos de comunicación de acceso	HW	Fluctuaciones de potencia eléctrica	2	2	Bajo	Protección de ordenadores y sistemas de comunicaciones.	1	2	Bajo
Riesgo Tecnológico	Equipos de comunicación de acceso	HW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Financiero	Equipos de comunicación de acceso	HW	Inundación	3	5	Extremo	Protección de las IN. Protección de los Equipos Informáticos. Protección del cableado Diseño.	3	3	Alto
Riesgo Financiero	Equipos de comunicación de acceso	HW	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Equipos de comunicación de acceso	HW	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Equipos de comunicación de acceso	HW	Terremoto	2	5	Extremo	Aplicación de DRP.	1	4	Alto
Riesgo Financiero	Equipos de comunicación core	HW	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado
Riesgo Operativo	Equipos de comunicación core	HW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Operativo	Equipos de comunicación core	HW	Falla en suministro eléctrico	3	1	Bajo	Protección de los Equipos Informáticos.	2	1	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Equipos de comunicación core	HW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Equipos de comunicación core	HW	Fluctuaciones de potencia eléctrica	2	2	Bajo	Protección de ordenadores y sistemas de comunicaciones.	1	2	Bajo
Riesgo Tecnológico	Equipos de comunicación core	HW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Financiero	Equipos de comunicación core	HW	Inundación	3	5	Extremo	Protección de las IN. Protección de los Equipos Informáticos. Protección del cableado Diseño.	3	3	Alto
Riesgo Financiero	Equipos de comunicación core	HW	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Equipos de comunicación core	HW	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Equipos de comunicación core	HW	Terremoto	2	5	Extremo	Aplicación de DRP.	1	4	Alto
Riesgo Financiero	Firewall	HW	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado
Riesgo Operativo	Firewall	HW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Operativo	Firewall	HW	Falla en suministro eléctrico	3	1	Bajo	Protección de los Equipos Informáticos.	2	1	Bajo
Riesgo Tecnológico	Firewall	HW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Firewall	HW	Fluctuaciones de potencia eléctrica	2	2	Bajo	Protección de ordenadores y sistemas de comunicaciones.	1	2	Bajo
Riesgo Tecnológico	Firewall	HW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Financiero	Firewall	HW	Inundación	3	5	Extremo	Protección de las IN. Protección de los Equipos	3	3	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Informáticos. Protección del cableado Diseño.			
Riesgo Financiero	Firewall	HW	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Firewall	HW	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Firewall	HW	Terremoto	2	5	Extremo	Aplicación de DRP.	1	4	Alto
Riesgo Financiero	Chasis BladeCenter	HW	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado
Riesgo Operativo	Chasis BladeCenter	HW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Chasis BladeCenter	HW	Falla en suministro eléctrico	3	1	Bajo	Protección de los Equipos Informáticos.	2	1	Bajo
Riesgo Tecnológico	Chasis BladeCenter	HW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Chasis BladeCenter	HW	Fluctuaciones de potencia eléctrica	2	2	Bajo	Protección de ordenadores y sistemas de comunicaciones.	1	2	Bajo
Riesgo Tecnológico	Chasis BladeCenter	HW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Financiero	Chasis BladeCenter	HW	Inundación	3	5	Extremo	Protección de las IN. Protección de los Equipos Informáticos. Protección del cableado. Diseño.	3	3	Alto
Riesgo Financiero	Chasis BladeCenter	HW	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Chasis BladeCenter	HW	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información.	1	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Uso de firmas electrónicas. Control de acceso físico/lógico.			
Riesgo Financiero	Chasis BladeCenter	HW	Terremoto	2	5	Extremo	Aplicación de DRP.	1	4	Alto
Riesgo Financiero	Servidor Blade	HW	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado
Riesgo Operativo	Servidor Blade	HW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Operativo	Servidor Blade	HW	Falla en suministro eléctrico	3	1	Bajo	Protección de los Equipos Informáticos.	2	1	Bajo
Riesgo Tecnológico	Servidor Blade	HW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Servidor Blade	HW	Fluctuaciones de potencia eléctrica	2	2	Bajo	Protección de ordenadores y sistemas de comunicaciones.	1	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Servidor Blade	HW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Financiero	Servidor Blade	HW	Inundación	3	5	Extremo	Protección de las IN. Protección de los Equipos Informáticos. Protección del cableado. Diseño.	3	3	Alto
Riesgo Financiero	Servidor Blade	HW	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Servidor Blade	HW	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Servidor Blade	HW	Terremoto	2	5	Extremo	Aplicación de DRP.	1	4	Alto
Riesgo Financiero	Equipo storage	HW	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Equipo storage	HW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Operativo	Equipo storage	HW	Falla en suministro eléctrico	3	1	Bajo	Protección de los Equipos Informáticos.	2	1	Bajo
Riesgo Tecnológico	Equipo storage	HW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Equipo storage	HW	Fluctuaciones de potencia eléctrica	2	2	Bajo	Protección de ordenadores y sistemas de comunicaciones.	1	2	Bajo
Riesgo Tecnológico	Equipo storage	HW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Financiero	Equipo storage	HW	Inundación	3	5	Extremo	Protección de las IN. Protección de los Equipos Informáticos. Protección del cableado. Diseño.	3	3	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Equipo storage	HW	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Equipo storage	HW	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Equipo storage	HW	Terremoto	2	5	Extremo	Aplicación de DRP.	1	4	Alto
Riesgo Financiero	Medios de respaldos	HW	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado
Riesgo Operativo	Medios de respaldos	HW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Operativo	Medios de respaldos	HW	Falla en suministro eléctrico	3	1	Bajo	Protección de los Equipos Informáticos.	2	1	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Medios de respaldos	HW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Medios de respaldos	HW	Fluctuaciones de potencia eléctrica	2	2	Bajo	Protección de ordenadores y sistemas de comunicaciones.	1	2	Bajo
Riesgo Tecnológico	Medios de respaldos	HW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Financiero	Medios de respaldos	HW	Inundación	3	5	Extremo	Protección de las IN. Protección de los Equipos Informáticos. Protección del cableado. Diseño.	3	3	Alto
Riesgo Financiero	Medios de respaldos	HW	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Medios de respaldos	HW	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Medios de respaldos	HW	Terremoto	2	5	Extremo	Aplicación de DRP.	1	4	Alto
Riesgo Financiero	Centro de Cómputo	IN	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado
Riesgo Operativo	Centro de Cómputo	IN	Falla en suministro eléctrico	3	1	Bajo	Protección de los Equipos Informáticos.	2	1	Bajo
Riesgo Financiero	Centro de Cómputo	IN	Incendio	3	5	Extremo	Aplicación de DRP.	3	4	Alto
Riesgo Financiero	Centro de Cómputo	IN	Inundación	3	5	Extremo	Protección de las IN. Protección de los Equipos Informáticos. Protección del cableado. Diseño.	3	3	Alto
Riesgo Financiero	Centro de Cómputo	IN	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Centro de Cómputo	IN	Temperatura / humedad extremas	2	4	Alto	Protección de los Equipos Informáticos. Climatización.	2	3	Moderado
Riesgo Financiero	Centro de Cómputo	IN	Terremoto	2	5	Extremo	Aplicación de DRP.	1	4	Alto
Riesgo Financiero	Oficinas JTM	IN	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado
Riesgo Operativo	Oficinas JTM	IN	Falla en suministro eléctrico	3	1	Bajo	Protección de los Equipos Informáticos.	2	1	Bajo
Riesgo Financiero	Oficinas JTM	IN	Incendio	3	5	Extremo	Aplicación de DRP.	3	4	Alto
Riesgo Financiero	Oficinas JTM	IN	Inundación	3	5	Extremo	Protección de las IN. Protección de los Equipos Informáticos. Protección del cableado. Diseño.	3	3	Alto
Riesgo Financiero	Oficinas JTM	IN	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información.	1	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Uso de firmas electrónicas. Control de acceso físico/lógico.			
Riesgo Operativo	Oficinas JTM	IN	Temperatura / humedad extremas	2	4	Alto	Protección de los Equipos Informáticos. Climatización.	2	3	Moderado
Riesgo Financiero	Oficinas JTM	IN	Terremoto	2	5	Extremo	Aplicación de DRP.	1	4	Alto
Riesgo Financiero	Buró de Crédito	SR	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Buró de Crédito	SR	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Buró de Crédito	SR	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Buró de Crédito	SR	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Buró de Crédito	SR	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado
Riesgo de Imagen	Buró de Crédito	SR	Deterioro de la calidad de SR prestados por terceros	3	2	Moderado	Aplicación de SLA.	2	2	Bajo
Riesgo Estratégico	Buró de Crédito	SR	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Operativo	Buró de Crédito	SR	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo de Imagen	Buró de Crédito	SR	Suplantación de Identidad	2	3	Moderado	Realizar análisis constantes para ver si hay virus o malware. Formación y concienciación del PE. Uso de contraseñas robustas.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Estratégico	Buró de Crédito	SR	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo de Imagen	Buró de Crédito	SR	Negación de SR	1	2	Bajo	Protección del servidor de nombres de dominio (DNS). Herramienta de análisis de vulnerabilidades.	1	1	Bajo
Riesgo Financiero	Registro Civil	SR	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Registro Civil	SR	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Registro Civil	SR	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Registro Civil	SR	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Registro Civil	SR	Destrucción de Instalaciones, datos y equipos	1	4	Alto	Protección de las IN. Protección de los Equipos Informáticos.	1	3	Moderado
Riesgo de Imagen	Registro Civil	SR	Deterioro de la calidad de SR prestados por terceros	3	2	Moderado	Aplicación de SLA.	2	2	Bajo
Riesgo Estratégico	Registro Civil	SR	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Operativo	Registro Civil	SR	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo de Imagen	Registro Civil	SR	Suplantación de Identidad	2	3	Moderado	Realizar análisis constantes para ver si hay virus o malware. Formación y concienciación del PE. Uso de contraseñas robustas.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Estratégico	Registro Civil	SR	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo de Imagen	Registro Civil	SR	Negación de SR	1	2	Bajo	Protección del servidor de nombres de dominio (DNS). Herramienta de análisis de vulnerabilidades.	1	1	Bajo
Riesgo Estratégico	Responsable de Seguridad de la Información	PE	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo de Cumplimiento	Responsable de Seguridad de la Información	PE	Extorsión / Corrupción	1	3	Moderado	Formación y concienciación. Inspecciones de seguridad.	1	2	Bajo
Riesgo Operativo	Responsable de Seguridad de la Información	PE	Falla en la elección del PE	2	2	Bajo	El proceso de selección de PE está enfocado en identificar candidatos que demuestren que encajan en la cultura de la organización y en su forma de actuar, que son idóneos para las necesidades.	1	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Cumplimiento	Responsable de Seguridad de la Información	PE	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Responsable de Seguridad de la Información	PE	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Estratégico	Responsable de Seguridad de la Información	PE	Pérdida o ausencia de PE clave	3	3	Alto	Ninguno.	3	3	Alto
Riesgo de Cumplimiento	Responsable de Seguridad de la Información	PE	Violación de las políticas de seguridad por parte de los empleados	3	2	Moderado	Ninguno.	3	2	Moderado
Riesgo Estratégico	Responsable de Seguridad del Área de TI	PE	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Cumplimiento	Responsable de Seguridad del Área de TI	PE	Extorsión / Corrupción	1	3	Moderado	Formación y concienciación. Inspecciones de seguridad.	1	2	Bajo
Riesgo Operativo	Responsable de Seguridad del Área de TI	PE	Falla en la elección del PE	2	2	Bajo	El proceso de selección de PE está enfocado en identificar candidatos que demuestren que encajan en la cultura de la organización y en su forma de actuar, que son idóneos para las necesidades.	1	2	Bajo
Riesgo de Cumplimiento	Responsable de Seguridad del Área de TI	PE	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Responsable de Seguridad del Área de TI	PE	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Estratégico	Responsable de Seguridad del Área de TI	PE	Pérdida o ausencia de PE clave	3	3	Alto	Ninguno.	3	3	Alto
Riesgo de Cumplimiento	Responsable de Seguridad del Área de TI	PE	Violación de las políticas de seguridad por parte de los empleados	3	2	Moderado	Ninguno.	3	2	Moderado
Riesgo Estratégico	Coordinadores y Analistas de las Áreas involucradas en el alcance del SGSI	PE	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo de Cumplimiento	Coordinadores y Analistas de las Áreas involucradas en el alcance del SGSI	PE	Extorsión / Corrupción	1	3	Moderado	Formación y concienciación. Inspecciones de seguridad.	1	2	Bajo
Riesgo Operativo	Coordinadores y Analistas de las Áreas involucradas	PE	Falla en la elección del PE	2	2	Bajo	El proceso de selección de PE está enfocado en identificar candidatos que	1	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
	en el alcance del SGSI						demuestren que encajan en la cultura de la organización y en su forma de actuar, que son idóneos para las necesidades.			
Riesgo de Cumplimiento	Coordinadores y Analistas de las Áreas involucradas en el alcance del SGSI	PE	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Coordinadores y Analistas de las Áreas involucradas en el alcance del SGSI	PE	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Estratégico	Coordinadores y Analistas de las Áreas involucradas en el alcance del SGSI	PE	Pérdida o ausencia de PE clave	3	3	Alto	Ninguno.	3	3	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Cumplimiento	Coordinadores y Analistas de las Áreas involucradas en el alcance del SGSI	PE	Violación de las políticas de seguridad por parte de los empleados	3	2	Moderado	Ninguno.	3	2	Moderado
Riesgo Estratégico	Aprobadores de operaciones de crédito	PE	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo de Cumplimiento	Aprobadores de operaciones de crédito	PE	Extorsión / Corrupción	1	3	Moderado	Formación y concienciación. Inspecciones de seguridad.	1	2	Bajo
Riesgo Operativo	Aprobadores de operaciones de crédito	PE	Falla en la elección del PE	2	2	Bajo	El proceso de selección de PE está enfocado en identificar candidatos que demuestren que encajan en la cultura de la organización y en su forma de actuar, que son idóneos para las necesidades.	1	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Cumplimiento	Aprobadores de operaciones de crédito	PE	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Aprobadores de operaciones de crédito	PE	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Estratégico	Aprobadores de operaciones de crédito	PE	Pérdida o ausencia de PE clave	3	3	Alto	Ninguno.	3	3	Alto
Riesgo de Cumplimiento	Aprobadores de operaciones de crédito	PE	Violación de las políticas de seguridad por parte de los empleados	3	2	Moderado	Ninguno.	3	2	Moderado
Riesgo Financiero	Instructivos de los programas de la empresa (Pols. y/o procs. internos)	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo de Imagen	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Estratégico	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Tecnológico	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la ID. Uso de firmas electrónicas.	2	4	Alto
Riesgo Operativo	Instructivos de los programas de la	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
	empresa (Pol. y/o proc. internos)									
Riesgo Financiero	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo de Cumplimiento	Instructivos de los programas de la empresa (Pol. y/o proc. internos)	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado
Riesgo Financiero	Documentos del SGSI	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Documentos del SGSI	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo de Imagen	Documentos del SGSI	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Documentos del SGSI	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Estratégico	Documentos del SGSI	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Tecnológico	Documentos del SGSI	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Documentos del SGSI	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Documentos del SGSI	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Documentos del SGSI	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Documentos del SGSI	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Operativo	Documentos del SGSI	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo
Riesgo Financiero	Documentos del SGSI	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Documentos del SGSI	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Cumplimiento	Documentos del SGSI	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado
Riesgo Financiero	Ticket de SR al Cliente	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Ticket de SR al Cliente	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo de Imagen	Ticket de SR al Cliente	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Ticket de SR al Cliente	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Estratégico	Ticket de SR al Cliente	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Ticket de SR al Cliente	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Ticket de SR al Cliente	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Ticket de SR al Cliente	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Ticket de SR al Cliente	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Ticket de SR al Cliente	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Operativo	Ticket de SR al Cliente	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Ticket de SR al Cliente	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Ticket de SR al Cliente	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo de Cumplimiento	Ticket de SR al Cliente	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado
Riesgo Financiero	Actas de entrega de comprobantes	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Actas de entrega de comprobantes	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Imagen	Actas de entrega de comprobantes	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Actas de entrega de comprobantes	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Estratégico	Actas de entrega de comprobantes	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Tecnológico	Actas de entrega de comprobantes	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Actas de entrega de comprobantes	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Actas de entrega de comprobantes	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Actas de entrega de comprobantes	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Estratégico	Actas de entrega de comprobantes	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Operativo	Actas de entrega de comprobantes	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo
Riesgo Financiero	Actas de entrega de comprobantes	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Actas de entrega de comprobantes	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo de Cumplimiento	Actas de entrega de comprobantes	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Confirmaciones bancarias	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Confirmaciones bancarias	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo de Imagen	Confirmaciones bancarias	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Confirmaciones bancarias	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Estratégico	Confirmaciones bancarias	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Tecnológico	Confirmaciones bancarias	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Confirmaciones bancarias	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Confirmaciones bancarias	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Confirmaciones bancarias	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Confirmaciones bancarias	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Operativo	Confirmaciones bancarias	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo
Riesgo Financiero	Confirmaciones bancarias	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Confirmaciones bancarias	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos.	1	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.			
Riesgo de Cumplimiento	Confirmaciones bancarias	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado
Riesgo Financiero	Hoja de negociación	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Hoja de negociación	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo de Imagen	Hoja de negociación	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Hoja de negociación	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Registro y auditoría. Análisis de logs.			
Riesgo Estratégico	Hoja de negociación	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Tecnológico	Hoja de negociación	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Hoja de negociación	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Hoja de negociación	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Hoja de negociación	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Hoja de negociación	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Hoja de negociación	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo
Riesgo Financiero	Hoja de negociación	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Hoja de negociación	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo de Cumplimiento	Hoja de negociación	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado
Riesgo Financiero	Reporte de Cartera	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Reporte de Cartera	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados.	3	2	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Copias de seguridad de los datos.			
Riesgo de Imagen	Reporte de Cartera	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Reporte de Cartera	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Estratégico	Reporte de Cartera	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Tecnológico	Reporte de Cartera	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Reporte de Cartera	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Reporte de Cartera	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Cumplimiento	Reporte de Cartera	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Reporte de Cartera	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Operativo	Reporte de Cartera	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo
Riesgo Financiero	Reporte de Cartera	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Reporte de Cartera	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo de Cumplimiento	Reporte de Cartera	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Cifrado de la información. Uso de firmas electrónicas.			
Riesgo Financiero	Informe de Cobranzas	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Informe de Cobranzas	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo de Imagen	Informe de Cobranzas	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Informe de Cobranzas	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Estratégico	Informe de Cobranzas	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Informe de Cobranzas	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Informe de Cobranzas	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Informe de Cobranzas	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Informe de Cobranzas	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Informe de Cobranzas	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Operativo	Informe de Cobranzas	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Informe de Cobranzas	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Informe de Cobranzas	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo de Cumplimiento	Informe de Cobranzas	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado
Riesgo Financiero	Análisis de Productividad	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Análisis de Productividad	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Imagen	Análisis de Productividad	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Análisis de Productividad	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Estratégico	Análisis de Productividad	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Tecnológico	Análisis de Productividad	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Análisis de Productividad	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Análisis de Productividad	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Análisis de Productividad	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Estratégico	Análisis de Productividad	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Operativo	Análisis de Productividad	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo
Riesgo Financiero	Análisis de Productividad	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Análisis de Productividad	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo de Cumplimiento	Análisis de Productividad	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Financiero	Listado de anticipos	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Listado de anticipos	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo de Imagen	Listado de anticipos	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Listado de anticipos	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Estratégico	Listado de anticipos	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Tecnológico	Listado de anticipos	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Listado de anticipos	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Listado de anticipos	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Listado de anticipos	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Listado de anticipos	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Operativo	Listado de anticipos	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo
Riesgo Financiero	Listado de anticipos	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Listado de anticipos	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos.	1	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.			
Riesgo de Cumplimiento	Listado de anticipos	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado
Riesgo Financiero	Reporte La Garantía	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Reporte La Garantía	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo de Imagen	Reporte La Garantía	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Reporte La Garantía	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Registro y auditoría. Análisis de logs.			
Riesgo Estratégico	Reporte La Garantía	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Tecnológico	Reporte La Garantía	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Reporte La Garantía	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Reporte La Garantía	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Reporte La Garantía	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Reporte La Garantía	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Reporte La Garantía	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo
Riesgo Financiero	Reporte La Garantía	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Reporte La Garantía	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo de Cumplimiento	Reporte La Garantía	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado
Riesgo Financiero	Reporte de concreción de cotizaciones	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Reporte de concreción de cotizaciones	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados.	3	2	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Copias de seguridad de los datos.			
Riesgo de Imagen	Reporte de concreción de cotizaciones	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Reporte de concreción de cotizaciones	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Estratégico	Reporte de concreción de cotizaciones	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Tecnológico	Reporte de concreción de cotizaciones	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Reporte de concreción de cotizaciones	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Reporte de concreción de cotizaciones	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Reporte de concreción de cotizaciones	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Reporte de concreción de cotizaciones	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo Operativo	Reporte de concreción de cotizaciones	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo
Riesgo Financiero	Reporte de concreción de cotizaciones	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Reporte de concreción de cotizaciones	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información.	1	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Uso de firmas electrónicas. Control de acceso físico/lógico.			
Riesgo de Cumplimiento	Reporte de concreción de cotizaciones	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado
Riesgo Financiero	Layout de Bodegas de Agencias	ID	Acceso no autorizado a datos	4	3	Alto	Aplicación de perfiles de seguridad. Control de acceso lógico.	3	2	Moderado
Riesgo Financiero	Layout de Bodegas de Agencias	ID	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo de Imagen	Layout de Bodegas de Agencias	ID	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Layout de Bodegas de Agencias	ID	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Registro y auditoría. Análisis de logs.			
Riesgo Estratégico	Layout de Bodegas de Agencias	ID	Divulgación de la información	3	3	Alto	Formación y concienciación. Registro y auditoría.	3	2	Moderado
Riesgo Tecnológico	Layout de Bodegas de Agencias	ID	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Layout de Bodegas de Agencias	ID	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Layout de Bodegas de Agencias	ID	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo de Cumplimiento	Layout de Bodegas de Agencias	ID	Ingeniería Social	4	1	Moderado	Formación y concienciación.	3	1	Bajo
Riesgo Estratégico	Layout de Bodegas de Agencias	ID	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Layout de Bodegas de Agencias	ID	Repudio	3	2	Moderado	Utilización firma electrónica o certificado digital.	2	2	Bajo
Riesgo Financiero	Layout de Bodegas de Agencias	ID	Robo y Fraude	2	4	Alto	Seguridad de las IN. Control de acceso físico/lógico.	1	3	Moderado
Riesgo Financiero	Layout de Bodegas de Agencias	ID	Sabotaje	1	4	Alto	Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas. Control de acceso físico/lógico.	1	3	Moderado
Riesgo de Cumplimiento	Layout de Bodegas de Agencias	ID	Análisis de Tráfico	3	3	Alto	Protección de la integridad de los datos intercambiados. Cifrado de la información. Uso de firmas electrónicas.	2	3	Moderado
Riesgo Financiero	Sistema BPCS	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema BPCS	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Imagen	Sistema BPCS	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema BPCS	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema BPCS	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema BPCS	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema BPCS	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema BPCS	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Estratégico	Sistema BPCS	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema BPCS	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema BPCS	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Base de Datos Sistema BPCS	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Base de Datos Sistema BPCS	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Base de Datos Sistema BPCS	SW	Demoras o no restauración de	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			los SR ante una emergencia							
Riesgo Estratégico	Base de Datos Sistema BPCS	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema BPCS	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Base de Datos Sistema BPCS	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Base de Datos Sistema BPCS	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema BPCS	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema BPCS	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Estratégico	Base de Datos Sistema BPCS	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Base de Datos Sistema BPCS	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema Operativo Sistema BPCS	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema BPCS	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Sistema BPCS	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Estratégico	Sistema Operativo Sistema BPCS	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema BPCS	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema Operativo Sistema BPCS	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Sistema BPCS	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema BPCS	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema BPCS	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema BPCS	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.			
Riesgo de Imagen	Sistema Operativo Sistema BPCS	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema Cognos	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Cognos	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Cognos	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Cognos	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Registro y auditoría. Análisis de logs.			
Riesgo Tecnológico	Sistema Cognos	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema Cognos	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Cognos	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Cognos	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Cognos	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Cognos	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Cifrado de la información. Uso de firmas electrónicas.			
Riesgo de Imagen	Sistema Cognos	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Base de Datos Sistema Cognos	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Base de Datos Sistema Cognos	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Base de Datos Sistema Cognos	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Cognos	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Base de Datos Sistema Cognos	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Base de Datos Sistema Cognos	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Base de Datos Sistema Cognos	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema Cognos	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Cognos	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Cognos	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Imagen	Base de Datos Sistema Cognos	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema Operativo Sistema Cognos	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Cognos	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Sistema Cognos	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Cognos	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Cognos	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema Operativo Sistema Cognos	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Sistema Cognos	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Cognos	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Cognos	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Cognos	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema Operativo Sistema Cognos	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Sistema Aheeva	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Aheeva	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Aheeva	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Aheeva	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema Aheeva	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema Aheeva	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Aheeva	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Aheeva	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Aheeva	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Aheeva	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema Aheeva	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Base de Datos Sistema Aheeva	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Base de Datos Sistema Aheeva	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Base de Datos Sistema Aheeva	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Aheeva	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema Aheeva	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Base de Datos Sistema Aheeva	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Base de Datos Sistema Aheeva	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema Aheeva	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Aheeva	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Aheeva	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Base de Datos Sistema Aheeva	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Sistema Operativo Sistema Aheeva	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Aheeva	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Sistema Aheeva	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Aheeva	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Aheeva	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema Operativo Sistema Aheeva	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Sistema Aheeva	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Aheeva	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Aheeva	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Aheeva	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema Operativo Sistema Aheeva	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Sistema Facturación Electrónica	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Facturación Electrónica	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Facturación Electrónica	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Facturación Electrónica	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema Facturación Electrónica	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema Facturación Electrónica	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Facturación Electrónica	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Facturación Electrónica	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Facturación Electrónica	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Facturación Electrónica	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Imagen	Sistema Facturación Electrónica	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema Operativo Sistema Facturación Electrónica	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Facturación Electrónica	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Sistema Facturación Electrónica	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Facturación Electrónica	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Sistema Operativo Sistema Facturación Electrónica	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema Operativo Sistema Facturación Electrónica	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Sistema Facturación Electrónica	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Facturación Electrónica	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Facturación Electrónica	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Estratégico	Sistema Operativo Sistema Facturación Electrónica	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema Operativo Sistema Facturación Electrónica	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema SIAC	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema SIAC	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema SIAC	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Estratégico	Sistema SIAC	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema SIAC	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema SIAC	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema SIAC	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema SIAC	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema SIAC	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema SIAC	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.			
Riesgo de Imagen	Sistema SIAC	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Base de Datos del Sistema SIAC	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Base de Datos del Sistema SIAC	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Base de Datos del Sistema SIAC	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Base de Datos del Sistema SIAC	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Registro y auditoría. Análisis de logs.			
Riesgo Tecnológico	Base de Datos del Sistema SIAC	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Base de Datos del Sistema SIAC	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Base de Datos del Sistema SIAC	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Base de Datos del Sistema SIAC	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Base de Datos del Sistema SIAC	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Base de Datos del Sistema SIAC	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Cifrado de la información. Uso de firmas electrónicas.			
Riesgo de Imagen	Base de Datos del Sistema SIAC	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema Operativo Base de Datos del Sistema SIAC	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Base de Datos del Sistema SIAC	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Base de Datos del Sistema SIAC	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Base de Datos del Sistema SIAC	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Sistema Operativo Base de Datos del Sistema SIAC	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema Operativo Base de Datos del Sistema SIAC	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Base de Datos del Sistema SIAC	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Base de Datos del Sistema SIAC	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Base de Datos del Sistema SIAC	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Base de Datos del Sistema SIAC	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Cifrado de la información. Uso de firmas electrónicas.			
Riesgo de Imagen	Sistema Operativo Base de Datos del Sistema SIAC	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema Operativo Sistema SIAC	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema SIAC	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Sistema SIAC	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema SIAC	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Sistema Operativo Sistema SIAC	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema Operativo Sistema SIAC	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Sistema SIAC	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema SIAC	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema SIAC	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema SIAC	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Imagen	Sistema Operativo Sistema SIAC	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema SIG	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema SIG	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema SIG	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema SIG	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema SIG	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema SIG	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema SIG	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema SIG	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema SIG	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema SIG	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema SIG	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Base de Datos Sistema SIG	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Base de Datos Sistema SIG	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Base de Datos Sistema SIG	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema SIG	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema SIG	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Base de Datos Sistema SIG	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Base de Datos Sistema SIG	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema SIG	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema SIG	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema SIG	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Base de Datos Sistema SIG	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Sistema Operativo Sistema SIG	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema SIG	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Sistema SIG	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema SIG	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema SIG	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema Operativo Sistema SIG	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Sistema SIG	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema SIG	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema SIG	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema SIG	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema Operativo Sistema SIG	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Sistema GTM	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema GTM	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema GTM	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema GTM	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema GTM	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema GTM	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema GTM	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema GTM	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema GTM	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema GTM	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema GTM	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Base de Datos Sistema GTM	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Base de Datos Sistema GTM	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Base de Datos Sistema GTM	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema GTM	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema GTM	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Base de Datos Sistema GTM	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Base de Datos Sistema GTM	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema GTM	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema GTM	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema GTM	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Base de Datos Sistema GTM	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Sistema Operativo Sistema GTM	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema GTM	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Sistema GTM	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema GTM	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema GTM	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema Operativo Sistema GTM	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Sistema GTM	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema GTM	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema GTM	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema GTM	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema Operativo Sistema GTM	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Sistema Intranet General	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Intranet General	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Intranet General	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Intranet General	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema Intranet General	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema Intranet General	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Intranet General	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Intranet General	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Intranet General	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Intranet General	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema Intranet General	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Base de Datos Sistema Intranet General	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Base de Datos Sistema Intranet General	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Base de Datos Sistema Intranet General	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Intranet General	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema Intranet General	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Base de Datos Sistema Intranet General	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Base de Datos Sistema Intranet General	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema Intranet General	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Intranet General	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Intranet General	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Imagen	Base de Datos Sistema Intranet General	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema Operativo Sistema Intranet General	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Intranet General	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Sistema Intranet General	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Intranet General	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Sistema Operativo Sistema Intranet General	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema Operativo Sistema Intranet General	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Sistema Intranet General	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Intranet General	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Intranet General	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Intranet General	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Cifrado de la información. Uso de firmas electrónicas.			
Riesgo de Imagen	Sistema Operativo Sistema Intranet General	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema Código de Barra	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Código de Barra	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Código de Barra	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Código de Barra	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Sistema Código de Barra	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema Código de Barra	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Código de Barra	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Código de Barra	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Código de Barra	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Código de Barra	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Imagen	Sistema Código de Barra	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema Operativo Sistema Código de Barra	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Código de Barra	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Sistema Código de Barra	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Código de Barra	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Sistema Operativo Sistema Código de Barra	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema Operativo Sistema Código de Barra	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Sistema Código de Barra	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Código de Barra	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Código de Barra	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Código de Barra	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Cifrado de la información. Uso de firmas electrónicas.			
Riesgo de Imagen	Sistema Operativo Sistema Código de Barra	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema Comisiones	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Comisiones	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Comisiones	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Comisiones	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Sistema Comisiones	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema Comisiones	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Comisiones	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Comisiones	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Comisiones	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Comisiones	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Imagen	Sistema Comisiones	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Base de Datos Sistema Comisiones	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Base de Datos Sistema Comisiones	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Base de Datos Sistema Comisiones	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Comisiones	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Base de Datos Sistema Comisiones	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Base de Datos Sistema Comisiones	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Base de Datos Sistema Comisiones	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Base de Datos Sistema Comisiones	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Comisiones	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad	2	3	Moderado
Riesgo Estratégico	Base de Datos Sistema Comisiones	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Cifrado de la información. Uso de firmas electrónicas.			
Riesgo de Imagen	Base de Datos Sistema Comisiones	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema Operativo Sistema Comisiones	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Comisiones	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Sistema Comisiones	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Comisiones	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Sistema Operativo Sistema Comisiones	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo
Riesgo Operativo	Sistema Operativo Sistema Comisiones	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Sistema Comisiones	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Sistema Comisiones	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Comisiones	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Sistema Comisiones	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
							Cifrado de la información. Uso de firmas electrónicas.			
Riesgo de Imagen	Sistema Operativo Sistema Comisiones	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Correo Electrónico	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Correo Electrónico	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Correo Electrónico	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Correo Electrónico	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Tecnológico	Correo Electrónico	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas Control de Cambios.	2	2	Bajo
Riesgo Operativo	Correo Electrónico	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Correo Electrónico	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Correo Electrónico	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP	2	3	Moderado
Riesgo Estratégico	Correo Electrónico	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Correo Electrónico	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo de Imagen	Correo Electrónico	SW	Respuesta no inmediata en la resolución de incidentes	2	5	Extremo	Aplicación de SLA.	2	4	Alto
Riesgo Financiero	Sistema operativo Correo electrónico	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema operativo Correo electrónico	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema operativo Correo electrónico	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema operativo Correo electrónico	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema operativo Correo electrónico	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema operativo Correo electrónico	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema operativo Correo electrónico	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema operativo Correo electrónico	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema operativo Correo electrónico	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema operativo Correo electrónico	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema operativo Correo electrónico	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Sistema de control de acceso a la red	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema de control de acceso a la red	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema de control de acceso a la red	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema de control de acceso a la red	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema de control de acceso a la red	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema de control de acceso a la red	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema de control de acceso a la red	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema de control de acceso a la red	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema de control de acceso a la red	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema de control de acceso a la red	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema de control de acceso a la red	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Sistema Operativo Servidor Blade	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema Operativo Servidor Blade	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema Operativo Servidor Blade	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Servidor Blade	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Servidor Blade	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema Operativo Servidor Blade	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema Operativo Servidor Blade	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema Operativo Servidor Blade	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Servidor Blade	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema Operativo Servidor Blade	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema Operativo Servidor Blade	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Directorio Activo	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Directorio Activo	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Directorio Activo	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Directorio Activo	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Directorio Activo	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Directorio Activo	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Directorio Activo	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Directorio Activo	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Directorio Activo	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Directorio Activo	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Directorio Activo	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Sistema operativo del Directorio Activo	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Sistema operativo del Directorio Activo	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Sistema operativo del Directorio Activo	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Sistema operativo del Directorio Activo	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Sistema operativo del Directorio Activo	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Sistema operativo del Directorio Activo	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Sistema operativo del Directorio Activo	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Sistema operativo del Directorio Activo	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Sistema operativo del Directorio Activo	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Sistema operativo del Directorio Activo	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Sistema operativo del Directorio Activo	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							
Riesgo Financiero	Mesa de SR	SW	Cambios no autorizados a datos	4	4	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos.	3	2	Moderado
Riesgo Tecnológico	Mesa de SR	SW	Código malicioso	3	3	Alto	Herramienta de análisis de vulnerabilidades.	2	2	Bajo
Riesgo de Imagen	Mesa de SR	SW	Demoras o no restauración de los SR ante una emergencia	2	4	Alto	Actualizaciones y Mantenimiento.	2	3	Moderado
Riesgo Estratégico	Mesa de SR	SW	Destrucción de la información	2	5	Extremo	Copias de seguridad de los datos. Registro y auditoría. Análisis de logs.	2	3	Moderado
Riesgo Tecnológico	Mesa de SR	SW	Errores de SW / programación	2	4	Alto	Protección de las Aplicaciones Informáticas. Control de Cambios.	2	2	Bajo

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
Riesgo Operativo	Mesa de SR	SW	Errores de usuarios y operadores	3	2	Moderado	Copias de seguridad de los datos. Aseguramiento de la integridad.	2	2	Bajo
Riesgo Tecnológico	Mesa de SR	SW	Fallas técnicas	3	3	Alto	Contratación de PE calificado. Mejorar competencias de PE técnico.	2	3	Moderado
Riesgo Tecnológico	Mesa de SR	SW	Incapacidad y restauración	2	4	Alto	Aplicación de DRP.	2	3	Moderado
Riesgo Estratégico	Mesa de SR	SW	Intrusión a aplicaciones y web	2	4	Alto	Aplicación de perfiles de seguridad.	2	3	Moderado
Riesgo Estratégico	Mesa de SR	SW	Manipulación de la información	2	5	Extremo	Protección de la integridad de los datos intercambiados. Copias de seguridad de los datos. Cifrado de la información. Uso de firmas electrónicas.	2	4	Alto
Riesgo de Imagen	Mesa de SR	SW	Respuesta no inmediata en la	2	5	Extremo	Aplicación de SLA.	2	4	Alto

ANEXO F - MATRIZ DE ANÁLISIS DE RIESGOS										
Tipo de Riesgo	Activo	Tipo Activo	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Riesgo Residual
			resolución de incidentes							

ANEXO G – APLICACIÓN DE CONTROLES			
Sub-Proceso (Nivel 3) COBIT 5	Sub-Proceso (Nivel 4) COBIT 5	PHVA	ISO 27001
14.1.2 Gestionar los Servicios de Seguridad (DSS05)	2.6 Aplicación de controles (Hacer)	1 Inventario y control de activos hardware.	A.8.1.1
			A.9.1.2
			A.13.1.1
		2 Inventario de Software autorizados y no autorizados	A.12.5.1
			A.12.6.2
		3 Gestión continua de vulnerabilidades	A.14.2.4
			A.14.2.8
			A.18.2.3
		4 Uso controlado de privilegios administrativos	A.12.6.1
		5 Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	A.9.1.1
			A.9.2.2
			A.9.2.6
			A.9.3.1
			A.9.4.1
			A.9.4.4
	2.7 Gestión de Incidentes (Hacer)	14.1.2.1 Definir esquemas de clasificación de incidentes y peticiones de servicio (DSS02.01)	A.16
		14.1.2.2 Registrar, clasificar y priorizar peticiones e incidentes (DSS02.02)	
		14.1.2.3 Verificar, aprobar y resolver peticiones de servicio (DSS02.03)	

		14.1.2.4 Investigar, diagnosticar y localizar incidentes (DSS02.04)	
		14.1.2.5 Resolver y recuperarse de incidentes (DSS02.05)	
		14.1.2.6 Cerrar peticiones de servicio e incidentes (DSS02.06)	
		14.1.2.7 Seguir el estado y emitir informes. (DSS02.07)	

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.5	Políticas de seguridad			
A.5.1.1	Documento de la política de seguridad de la información	Si	Tiene una aplicabilidad global en todo el SGSI.	Documento de política firmado por la alta dirección.
A.5.1.2	Revisión de la política de seguridad de la información	Si	De manera periódica se debe realizar la revisión y documentar las acciones de mejora.	Actas de revisión periódica.
A.6	Organización de la seguridad de la Información			
A.6.1.1	Compromiso de la dirección con la seguridad de la información	Si	Es fundamental, dado que tienen la responsabilidad de aprobar el SGSI como última instancia.	Actas de comité.
A.6.1.2	Coordinación de la seguridad de la información	Si	Debe haber un área que lidere la implementación del SGSI.	Equipo de trabajo conformado.
A.6.1.3	Asignación de responsabilidades para la seguridad de la información	Si	A las áreas deben asociarse las responsabilidades frente al SGSI.	Documento con la inclusión de las responsabilidades o en los cargos o en los procesos.
A.6.1.4	Procesos de autorización para los servicios de procesamiento de información	Si	Todo sistema informático debe contar con procedimientos de aceptación de los sistemas antes de su funcionamiento.	Actas de aceptación de los sistemas.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.6.1.5	Acuerdos sobre confidencialidad	Si	La información es fundamental su protección ante develado.	Cláusulas contractuales, modelos de contratos con las cláusulas de confidencialidad.
A.6.1.6	Contacto con las autoridades	Si	Las reacciones a tiempo frente a incidentes, permite la reducción de riesgos.	Protocolo para contactar a las autoridades pertinentes.
A.6.1.7	Contacto con grupos de interés especiales	Si	Es necesario mantener informado sobre los acontecimientos en seguridad, con ello, poder retroalimentar el SGSI y los incidentes de seguridad.	Inscripción a grupos de interés en seguridad de la información.
A.6.1.8	Revisión independiente de la seguridad de la información	No	La empresa no busca la certificación.	
A.6.2.1	Identificación de los riesgos relacionados con las partes externas	Si	Toda organización posee terceras partes que ayudan al objeto comercial, es imprescindible conocer sobre los riesgos.	Mapa de riesgos de terceras partes.
A.6.2.2	Consideraciones de la seguridad cuando se trata con los clientes	Si	Se debe fortalecer la confianza en el cliente.	Protocolos de trato a clientes en cuento a seguridad de la información

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes	Si	Toda organización posee terceras partes que ayudan al objeto comercial, es imprescindible conocer sobre los riesgos, así, incluir los temas de seguridad en los contratos.	Modelos de contratos con las cláusulas de confidencialidad.
A.7	Gestión de activos			
A.7.1.1	Inventario de activos	Si	Para una adecuada gestión de riesgos y tratamiento de estos, es necesario conocer los activos de información acorde al alcance.	Listado con activos de información.
A.7.1.2	Propiedad de los activos	Si	Cada activo de información debe tener un responsable.	Listado con activos de información con responsable.
A.7.1.3	Uso aceptable de los activos	Si	Todo sistema informático debe contar con procedimientos de aceptación de los sistemas antes de su funcionamiento.	Actas de aceptación de los sistemas.
A.7.2.1	Directrices de clasificación	Si	La información debe protegerse acorde a su criticidad, por ello es necesario clasificarla.	Documento con los niveles de clasificación.
A.7.2.2	Etiquetado y manejo de información	Si	La información debe protegerse acorde a su criticidad, por ello es necesario clasificarla.	Documento con los niveles de clasificación y procedimiento para etiquetado.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.8	Seguridad de los recursos humanos			
A.8.1.1	Roles y responsabilidades	Si	En las distintas áreas se deben asociar las responsabilidades frente al SGSI.	Documento con la inclusión de las responsabilidades en los descriptivos de cargo.
A.8.1.2	Selección	Si	Desde los procesos iniciales de ingreso del personal, se debe establecer parámetros de seguridad.	Inclusión de elementos de seguridad sobre los procesos de selección de personal.
A.8.1.3	Términos y condiciones laborales	Si	Propiedad intelectual de la empresa.	Modelos de contratos con las cláusulas de confidencialidad.
A.8.2.1	Responsabilidades de la dirección	Si	En las distintas áreas se deben asociar las responsabilidades frente al SGSI.	Documento con la inclusión de las responsabilidades en los descriptivos de cargo.
A.8.2.2	Educación, formación y concientización sobre la seguridad de la información	Si	Ser competitivos es de gran importancia para la implementación y mantenimiento del SGSI, esto implica tener planes de capacitación frente a los temas de seguridad.	Plan de capacitación o registros de participación.
A.8.2.3	Proceso disciplinario	Si	El control es fundamental en cualquier organización, las faltas de los empleados deben ser investigadas y sancionadas.	Inclusión de elementos de seguridad sobre los procesos de selección de personal.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.8.3.1	Responsabilidades en la terminación	Si	En las distintas áreas se deben asociar las responsabilidades frente al SGSI.	Documento con la inclusión de las responsabilidades en los descriptivos de cargo.
A.8.3.2	Devolución de activos	Si	Establecer desde el inicio los activos propios de la empresa.	Procedimiento para el paz y salvo.
A.8.3.3	Retiro de los derechos de acceso	Si	En las distintas áreas se deben asociar las responsabilidades frente al SGSI	Procedimiento para el paz y salvo.
A.9	Seguridad física y ambiental			
A.9.1.1	Perímetro de seguridad física	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Implementación de medidas físicas y procedimentales.
A.9.1.2	Controles de acceso físico	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Implementación de medidas físicas y procedimentales.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.9.1.3	Seguridad de oficinas, recintos e instalaciones	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Implementación de medidas físicas y procedimentales.
A.9.1.4	Protección contra amenazas externas y ambientales	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales. Tener contacto con las autoridades.
A.9.1.5	Trabajo en áreas seguras	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Implementación de medidas físicas y procedimentales. Tener contacto con las autoridades.
A.9.1.6	Áreas de carga, despacho y acceso público	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Implementación de medidas físicas y procedimentales. Control de acceso físico en las áreas de carga.
A.9.2.1	Ubicación y protección de los equipos	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Los equipos de misión crítica deben ser protegidos en centros de datos.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.9.2.2	Servicios de suministro	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Procedimientos y control de suministros eléctricos y utilitarios.
A.9.2.3	Seguridad del cableado	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Procedimiento de control de acceso a centro de datos y centros de cableados
A.9.2.4	Mantenimiento de los equipos	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Ejecución de contratos sobre equipos informáticos incluyendo mantenimientos preventivos y de soporte.
A.9.2.5	Seguridad de los equipos fuera de las instalaciones	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Ejecución de contratos sobre equipos informáticos incluyendo pólizas y seguros.
A.9.2.6	Seguridad en la reutilización o eliminación de los equipos	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Procedimientos de borrado seguro de información sin recuperación.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.9.2.7	Retiro de activos	Si	Los sistemas de cómputo, los recursos y las personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales.	Procedimientos para el ingreso y retiro de equipos tecnológicos a las instalaciones.
A.10	Gestión de las comunicaciones y operaciones			
A.10.1.1	Documentación de los procedimientos de operación	Si	Todos los procedimientos operativos deben estar documentados.	Documentos y manuales de operación.
A.10.1.2	Gestión del cambio	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos.	Procesos y procedimientos para la gestión del cambio.
A.10.1.3	Distribución de funciones	Si	A las áreas deben asociarse las responsabilidades frente al SGSI.	Segregación de Funciones.
A.10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos.	Documento de arquitectura para la segmentación de las redes y los ambientes de procesamiento, que incluya gestión de la capacidad y expansión de la red.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.10.2.1	Prestación del servicio	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos.	Documento de arquitectura para la segmentación de las redes y los ambientes de procesamiento.
A.10.2.2	Monitoreo y revisión de los servicios por terceras partes	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos.	Procesos y procedimientos de monitoreo de funciones ejecutadas.
A.10.2.3	Gestión de los cambios en servicios por terceras partes	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos.	Procesos y procedimientos de monitoreo de funciones ejecutadas.
A.10.3.1	Gestión de la capacidad	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos.	Documento de arquitectura para la segmentación de las redes y los ambientes de procesamiento, que incluya gestión de la capacidad y expansión de la red.
A.10.3.2	Aceptación del sistema	Si	Todo sistema informático debe contar con procedimientos de aceptación de los sistemas antes de su funcionamiento.	Actas de aceptación de los sistemas.
A.10.4.1	Controles contra códigos maliciosos	Si	Se debe controlar de manera adecuada los códigos maliciosos.	Revisiones de Ethical Hacking.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.10.4.2	Controles contra códigos móviles	Si	Se debe controlar de manera adecuada los códigos maliciosos.	Revisiones de Ethical Hacking.
A.10.5.1	Respaldo de la información	Si	Ante eventos de seguridad, es necesario contar con respaldo que permita la recuperación de la información.	Procedimientos para el respaldo de la información.
A.10.6.1	Controles de las redes	Si	El control de acceso a las redes debe permitir la reducción de los riesgos.	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.10.6.2	Seguridad de los servicios de la red	Si	El control de acceso a las redes debe permitir la reducción de los riesgos.	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.10.7.1	Gestión de los medios removibles	Si	Se debe tener control y planes de sensibilización con respecto a los medios removibles.	Procedimientos y políticas en la red para el uso de medios removibles.
A.10.7.2	Eliminación de los medios	Si	Se debe tener control y planes de sensibilización con respecto a los medios removibles.	Procedimientos de borrado seguro de información sin recuperación.
A.10.7.3	Procedimientos para el manejo de la información	Si	Tanto la clasificación como los planes de sensibilización fortalecen la reducción de riesgos sobre el inadecuado manejo de la información.	Documento con niveles de clasificación y ejecución de planes de sensibilización.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.10.7.4	Seguridad de la documentación del sistema	Si	Tanto la clasificación como los planes de sensibilización fortalecen la reducción de riesgos sobre el inadecuado manejo de la información.	Procedimientos y herramientas técnicas para la protección de la documentación.
A.10.8.1	Políticas y procedimientos para el intercambio de la información	Si	Tanto la clasificación como los planes de sensibilización fortalecen la reducción de riesgos sobre el inadecuado manejo de la información.	Documento con niveles de clasificación, ejecución de planes de sensibilización y procedimientos para el intercambio de información.
A.10.8.2	Acuerdos para el intercambio	Si	Tanto la clasificación como los planes de sensibilización fortalecen la reducción de riesgos sobre el inadecuado manejo de la información.	Documento con niveles de clasificación, ejecución de planes de sensibilización y procedimientos para el intercambio de información. Uso de herramientas técnicas para la protección de la documentación.
A.10.8.3	Medios físicos en tránsito	Si	Se debe tener control y planes de sensibilización con respecto a los medios removibles.	Procedimientos y políticas en la red para el uso de medios removibles.
A.10.8.4	Mensajería electrónica	Si	Las áreas hacen uso de la mensajería y aplicaciones de transacciones (online) como una herramienta de trabajo, por ello se debe proteger.	Procedimientos para el control de acceso sobre la mensajería, criptografía e implementación de sistemas Anti-X.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.10.8.5	Sistemas de información del negocio	Si	Las áreas hacen uso de la mensajería y aplicaciones de transacciones (online) como una herramienta de trabajo, por ello se debe proteger.	Procedimientos para el control de acceso sobre la mensajería, criptografía e implementación de sistemas Anti-X.
A.10.9.1	Comercio electrónico	Si	Las áreas hacen uso de la mensajería y aplicaciones de transacciones (online) como una herramienta de trabajo, por ello se debe proteger.	Procedimientos para el control de acceso sobre la mensajería, criptografía e implementación de sistemas Anti-X
A.10.9.2	Transacciones en línea	Si	Las áreas hacen uso de la mensajería y aplicaciones de transacciones (online) como una herramienta de trabajo, por ello se debe proteger	Procedimientos para el control de acceso sobre la mensajería, criptografía e implementación de sistemas Anti-X.
A.10.9.3	Información disponible al público	Si	Las áreas hacen uso de la mensajería y aplicaciones de transacciones (online) como una herramienta de trabajo, por ello se debe proteger.	Procedimientos de clasificación de información y aplicarlos antes de publicar.
A.10.10.1	Registro de auditorías	Si	Los logs y registros deben estar configurados y protegidos para validaciones, monitoreo y manejo de incidentes de seguridad.	Procedimiento con las recomendaciones de configuración de logs y registros de auditorías, así como la protección de estos.
A.10.10.2	Monitoreo del uso del sistema	Si	Los sistemas deben ser monitoreados de manera permanente.	Procedimientos de monitoreo.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.10.10.3	Protección de la información del registro	Si	Los logs y registros deben estar configurados y protegidos para validaciones, monitoreo y manejo de incidentes de seguridad.	Procedimiento con las recomendaciones de configuración de logs y registros de auditorías, así como la protección de estos.
A.10.10.4	Registros del administrador y del operador	Si	Los logs y registros deben estar configurados y protegidos para validaciones, monitoreo y manejo de incidentes de seguridad.	Procedimiento con las recomendaciones de configuración de logs y registros de auditorías, así como la protección de estos.
A.10.10.5	Registro de fallas	Si	Los logs y registros deben estar configurados y protegidos para validaciones, monitoreo y manejo de incidentes de seguridad.	Procedimiento con las recomendaciones de configuración de logs y registros de auditorías, así como la protección de estos.
A.10.10.6	Sincronización de relojes	Si	El tiempo es fundamental en los sistemas y más aún en las aplicaciones de tiempo real Online).	Procedimiento para la configuración de NTP.
A.11	Control de acceso			
A.11.1.1	Política de control de acceso	Si	Tiene una aplicabilidad global en todo el SGSI.	Documento de política firmado por la alta dirección.
A.11.2.1	Registro de usuarios	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.11.2.2	Gestión de privilegios	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios//equipos y privilegios en general.
A.11.2.3	Gestión de contraseñas para usuario	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de contraseñas.
A.11.2.4	Revisión de los derechos de acceso de los usuarios	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimientos para la revisión periódica de accesos.
A.11.3.1	Uso de contraseñas	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de contraseñas.
A.11.3.2	Equipo de usuario desatendido	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Control de sesiones en equipos.
A.11.3.3	Política de escritorio despejado y de pantalla despejada	Si	La información sensible debe estar coherentemente resguardada.	Planes de sensibilización sobre la protección de la información.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.11.4.1	Política de uso de los servicios de red	Si	El control de acceso a las redes debe permitir la reducción de los riesgos.	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.11.4.2	Autenticación de usuarios para conexiones externas	Si	El control de acceso a las redes debe permitir la reducción de los riesgos.	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.11.4.3	Identificación de los equipos en las redes	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de contraseñas.
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto	Si	El control de acceso a las redes debe permitir la reducción de los riesgos.	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.11.4.5	Separación en las redes	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos.	Documento de arquitectura para la segmentación de las redes y los ambientes de procesamiento, que incluya gestión de la capacidad y expansión de la red.
A.11.4.6	Control de conexión a las redes	Si	El control de acceso a las redes debe permitir la reducción de los riesgos.	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.11.4.7	Control de enrutamiento en la red	Si	Se debe controlar de manera adecuada los cambios en plataformas y sistemas de información, de modo que se reduzcan los errores operativos.	Documento de arquitectura para la segmentación de las redes y los ambientes de procesamiento.
A.11.5.1	Procedimientos de ingreso seguro	Si	El control de acceso a las redes debe permitir la reducción de los riesgos.	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.11.5.2	Identificación y autenticación de usuarios	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de contraseñas.
A.11.5.3	Sistema de gestión de contraseñas	No	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de contraseñas
A.11.5.4	Uso de las utilidades del sistema	Si	Todo sistema informático debe contar con procedimientos de aceptación de los sistemas antes de su funcionamiento.	Actas de aceptación de los sistemas.
A.11.5.5	Tiempo de inactividad de la sesión	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de sesiones.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.11.5.6	Limitación del tiempo de conexión	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de sesiones.
A.11.6.1	Restricción de acceso a la información	Si	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos.	Procedimiento para el registro de usuarios/equipos y privilegios en general, incluyendo parámetros de sesiones.
A.11.6.2	Aislamiento de sistemas sensibles	Si	Los sistemas sensibles deben tener un nivel de seguridad más alto.	Procedimiento para la separación de redes y ambientes de procesamiento.
A.11.7.1	Computación y comunicaciones móviles	Si	La movilidad es fundamental en las organizaciones de hoy y por ello, se deben proteger.	Procedimientos para la protección de equipos móviles.
A.11.7.2	Trabajo remoto	Si	El control de acceso a las redes debe permitir la reducción de los riesgos.	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.12	Adquisición, desarrollo y mantenimiento de los sistemas de información			
A.12.1.1	Análisis y especificación de los requisitos de seguridad	Si	Los desarrollos y mantenimiento de sistemas de información deben ser	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
			normados para que cumplan con las mejores prácticas.	
A.12.2.1	Validación de los datos de entrada	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones.
A.12.2.2	Control de procesamiento interno	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones.
A.12.2.3	Integridad del mensaje	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones.
A.12.2.4	Validación de los datos de salida	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones.
A.12.3.1	Política sobre el uso de controles criptográficos	Si	Los desarrollos y mantenimiento de sistemas de información deben ser	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
			normados para que cumplan con las mejores prácticas.	
A.12.3.2	Gestión de llaves	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones.
A.12.4.1	Control del software operativo	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones.
A.12.4.2	Protección de los datos de prueba del sistema	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones.
A.12.4.3	Control de acceso al código fuente de los programas	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones.
A.12.5.1	Procedimientos de control de cambios	Si	Los desarrollos y mantenimiento de sistemas de información deben ser	Procedimiento de Control de Cambios

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
			normados para que cumplan con las mejores prácticas.	
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Procedimiento de Control de Cambios.
A.12.5.3	Restricciones en los cambios a los paquetes de software	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Procedimiento de Control de Cambios.
A.12.5.4	Fuga de información	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Planes de sensibilización sobre la protección de la información, controles criptográficos.
A.12.5.5	Desarrollo de software contratado externamente	Si	Los desarrollos y mantenimiento de sistemas de información deben ser normados para que cumplan con las mejores prácticas.	Documento con los requisitos mínimos de seguridad para la adquisición de SW.
A.12.6.1	Control de vulnerabilidades técnicas	Si	Los desarrollos y mantenimiento de sistemas de información deben ser	Documento de planeación y diseño de las pruebas de seguridad periódicas a realizar.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
			normados para que cumplan con las mejores prácticas.	
A.13	Gestión de incidentes de seguridad de la información			
A.13.1.1	Reporte sobre los eventos de seguridad de la información	Si	Se requiere reportar adecuadamente para el tratamiento oportuno.	Procedimiento de Gestión de Incidentes.
A.13.1.2	Reportes sobre las debilidades de la seguridad	Si	Se requiere reportar adecuadamente para el tratamiento oportuno.	Procedimiento de Gestión de Incidentes.
A.13.2.1	Responsabilidades y procedimientos	Si	Se requiere reportar adecuadamente para el tratamiento oportuno.	Procedimiento de Gestión de Incidentes.
A.13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	Si	Se requiere reportar adecuadamente para el tratamiento oportuno.	Procedimiento de Gestión de Incidentes.
A.13.2.3	Recolección de evidencia	Si	Se requiere reportar adecuadamente para el tratamiento oportuno.	Procedimiento de Gestión de Incidentes.
A.14	Gestión de la continuidad del negocio			
A.14.1.1	Inclusión de la seguridad de la Información en el proceso de gestión de la continuidad del negocio	Si	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es necesario asegurar la información.	Documento y procedimiento para la continuidad de negocio.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
A.14.1.2	Continuidad del negocio y evaluación de riesgos	Si	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es necesario asegurar la información.	Documento y procedimiento para la continuidad de negocio.
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información	Si	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es necesario asegurar la información.	Documento y procedimiento para la continuidad de negocio.
A.14.1.4	Estructura para la planificación de la continuidad del negocio	Si	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es necesario asegurar la información.	Documento y procedimiento para la continuidad de negocio.
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	Si	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es necesario asegurar la información.	Documento y procedimiento para la continuidad de negocio.
A.15	Cumplimiento			
A.15.1.1	Identificación de legislación aplicable	Si	Es necesario conocer las reglamentaciones a nivel Colombia que aplican para el sector de las	Documento con las normas/leyes que aplican al SGSI.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
			telecomunicaciones y sistemas informáticos.	
A.15.1.2	Derechos de propiedad intelectual (DPI)	Si	Es necesario conocer las reglamentaciones a nivel Colombia que aplican para el sector de las telecomunicaciones.	Documento con las normas/leyes que aplican al SGSI.
A.15.1.3	Protección de los registros de la organización	Si	Tanto los log, registros así como las herramientas de auditoría y monitorea deben ser protegidas contra accesos no autorizados.	Procedimiento de control de acceso sobre sistemas de información y aplicaciones.
A.15.1.4	Protección de los datos y privacidad de la información personal	Si	Es necesario conocer las reglamentaciones a nivel Colombia que aplican para el sector de las telecomunicaciones.	Documento con las normas/leyes que aplican al SGSI.
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	Si	Se deben implementar controles persuasivos y disuasivos en los sistemas y plataformas.	Documento con los planes de cultura y sensibilización, procedimientos de configuración de los sistemas.
A.15.1.6	Reglamentación de los controles criptográficos	Si	Es necesario conocer las reglamentaciones a nivel Colombia que aplican para el sector de las	Documento con las normas/leyes que aplican al SGSI.

ANEXO H - DECLARACIÓN DE APLICABILIDAD				
Numeral	Dominio o descripción	Aplica	Racional	Evidencia o registro de implementación
			telecomunicaciones y sistemas informáticos.	
A.15.2.1	Cumplimiento con las políticas y normas de seguridad	Si	Es fundamental tener planes de auditoria, que validen y ajusten los objetivos del SGSI.	Documento con la planeación de auditorías anuales, incluyendo auditorias técnicas.
A.15.2.2	Verificación del cumplimiento técnico	Si	Es fundamental tener planes de auditoria, que validen y ajusten los objetivos del SGSI.	Documento con la planeación de auditorías anuales, incluyendo auditorias técnicas.
A.15.3.1	Controles de auditoría de los sistemas de información	Si	Los log y registros del sistema son fundamentales para el monitoreo y control de la seguridad, así como para investigaciones.	Documento con las especificaciones de controles de auditoria a activar.
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información	Si	Tanto los log, registros así como las herramientas de auditoría y monitorea deben ser protegidas contra accesos no autorizados.	Procedimiento de control de acceso sobre sistemas de información y aplicaciones.

ANEXO I - MAPA DOCUMENTAL DEL SGSI		
Sub-Proceso (Nivel 3)	Sub-Proceso (Nivel 4)	PHVA
14.1.1 Gestionar la Seguridad (APO13)	14.1.1.1 Establecer y mantener un SGSI (APO13.01)	1.1 Comprensión de la Organización (Planear)
		1.2 Analizar el sistema existente (Planear)
		1.3 Liderazgo y Aprobación del Proyecto (Planear)
		1.4 Ámbito de Aplicación (Planear)
		1.5 Política de Seguridad (Planear)
		2.1 Estructura de la Organización (Hacer)
		2.2 Gestión de Documentos (Hacer)

ANEXO I - MAPA DOCUMENTAL DEL SGSI		
Sub-Proceso (Nivel 3)	Sub-Proceso (Nivel 4)	PHVA
		2.3 Diseño de Controles y Procedimientos (Hacer)
		2.4 Comunicación (Hacer)
		2.5 Sensibilización y Capacitación (Hacer)
	14.1.1.2 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información (APO13.02)	1.6 Evaluación de Riesgos (Planear)
		1.7 Declaración de Aplicabilidad (Planear)
	14.1.1.3 Supervisar y revisar el SGSI (APO13.03)	3.1 Supervisión, Medición, Análisis y Evaluación (Verificar)
		3.2 Auditoria Interna (Verificar)

ANEXO I - MAPA DOCUMENTAL DEL SGSI		
Sub-Proceso (Nivel 3)	Sub-Proceso (Nivel 4)	PHVA
		3.3 Revisión por la Dirección (Verificar)
		4.1 Tratamiento de No conformidades (Actuar)
		4.2 Mejora Continua (Actuar)
14.1.2 Gestionar los Servicios de Seguridad (DSS05)	2.6 Aplicación de controles (Hacer)	1 Inventario y control de activos hardware
		2 Inventario de Software autorizados y no autorizados
		3 Gestión continua de vulnerabilidades

ANEXO I - MAPA DOCUMENTAL DEL SGSI		
Sub-Proceso (Nivel 3)	Sub-Proceso (Nivel 4)	PHVA
		4 Uso controlado de privilegios administrativos
		5 Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores
	2.7 Gestión de Incidentes (Hacer)	14.1.2.1 Definir esquemas de clasificación de incidentes y peticiones de servicio (DSS02.01)
		14.1.2.2 Registrar, clasificar y priorizar peticiones e incidentes (DSS02.02)
		14.1.2.3 Verificar, aprobar y resolver peticiones de servicio (DSS02.03)
		14.1.2.4 Investigar, diagnosticar y localizar incidentes (DSS02.04)
		14.1.2.5 Resolver y recuperarse de incidentes (DSS02.05)

ANEXO I - MAPA DOCUMENTAL DEL SGSI		
Sub-Proceso (Nivel 3)	Sub-Proceso (Nivel 4)	PHVA
		14.1.2.6 Cerrar peticiones de servicio e incidentes (DSS02.06)
		14.1.2.7 Seguir el estado y emitir informes. (DSS02.07)

ANEXO J - ENTREGABLES DEL SGSI				
Proceso	PHVA	Componente	Actividad	Documento
Gestión del Sistema de Seguridad de la Informa (SGSI)	Planear	Comprensión de la Organización	Comprensión de la Misión, objetivos, valores y estrategias de la organización	Contexto de la Organización
			Análisis del entorno interno	
			Análisis del entorno externo	
			Identificación de los principales procesos y actividades	
			Identificación de la infraestructura	
			Identificación y análisis de las partes interesadas	
			Identificación y análisis de los requisitos del negocio	
			Determinación de los objetivos del SGSI	
		Análisis del Sistema Existente	Evaluar la eficacia y madurez de los procesos vigentes dentro de la organización	Informe de Nivel de Madurez

ANEXO J - ENTREGABLES DEL SGSI				
Proceso	PHVA	Componente	Actividad	Documento
		Liderazgo y Aprobación del Proyecto	Establecer el equipo de trabajo del proyecto SGSI	Plan de Trabajo
			Determinación de recursos necesarios para la ejecución del SGSI	
			Presentación del plan de proyecto	
			Obtener la aprobación de la Dirección	
		Ámbito de Aplicación	Definir límites organizacionales del ámbito de aplicación	Alcance del SGSI
			Definir límites físicos del ámbito de aplicación	
			Definir límite de sistema de información del ámbito de aplicación	
		Política de Seguridad	Crear modelos de políticas	Política General del SGSI
			Definición del proceso de redacción de la política	

ANEXO J - ENTREGABLES DEL SGSI				
Proceso	PHVA	Componente	Actividad	Documento
			Elaboración de la política del SGSI	
			Revisión de la política de seguridad de la información	
			Redacción de políticas específicas de seguridad	Política de dispositivo sobre dispositivos móviles y teletrabajo
				Política de intercambio de información
				Política de clasificación de la información
				Política de control de acceso
				Política de claves
				Política de gestión de cambios
				Política sobre restricción de acceso a la información
				Política de eliminación y destrucción
				Política sobre el uso de controles criptográficos y claves
				Política de Uso aceptable de los activos

ANEXO J - ENTREGABLES DEL SGSI				
Proceso	PHVA	Componente	Actividad	Documento
				Política de Copias de seguridad de la información
				Política de transferencia de información
				Política sobre desarrollo seguro
				Política de pantalla y escritorio limpios
				Política de seguridad para proveedores
		Evaluación de Riesgos	Selección de metodología para evaluación de riesgos	Metodología de evaluación y tratamiento de riesgos
			Identificación de riesgos	Informe sobre evaluación de riesgos
			Análisis de riesgos	
			Estimación de riesgos	
			Tratamiento de riesgos	Plan de tratamiento de riesgos
		Declaración de Aplicabilidad	Selección de objetivos y controles de seguridad	Declaración de Aplicabilidad
			Justificación de controles elegidos	
			Justificación de controles excluidos	
			Redacción de la declaración de aplicabilidad	
	Verificar		Determinar objetivos de la medición	Metodología de supervisión y medición
			Objeto de Supervisión y Medición	

ANEXO J - ENTREGABLES DEL SGSI				
Proceso	PHVA	Componente	Actividad	Documento
		Supervisión, Medición, Análisis y Evaluación	Determinación de frecuencia y método de supervisión y medición	
			Presentación de resultados	
	Actuar	Mejora Continua	Proceso de seguimiento continuo de factores de cambio	Procedimiento para acciones correctivas y preventivas
			Mantenimiento y mejora del SGSI	
			Actualización de la documentación y registros	
			Documentación de mejoras	
Gestión de los Servicios de Seguridad (Controles)	Hacer	Diseño de Controles y Procedimientos	Diseño y descripción de los procedimientos y controles de seguridad de la información y de los registros relacionados	Inventario y control de activos hardware y software
				Gestión continua de vulnerabilidades
				Uso controlado de privilegios administrativos y operativos
				Configuración segura para hardware y software
				Mantenimiento, monitoreo y análisis de logs de auditoría
		Comunicación	Establecer objetivos de comunicación	Plan de comunicación
			Identificar las partes interesadas	

ANEXO J - ENTREGABLES DEL SGSI				
Proceso	PHVA	Componente	Actividad	Documento
			Planificar las actividades de comunicación	
			Realizar una actividad de comunicación	
			Evaluar la comunicación	
		Sensibilización y Capacitación	Definir las necesidades de capacitación	Plan de Capacitación y Concientización
			Diseño y planificación de la capacitación	
			Evaluación de los resultados de la capacitación	
		Gestión de Incidentes	Aplicación de métodos para detectar y responder a incidentes	Procedimiento de gestión de incidentes de seguridad de la información
				Procedimiento de investigación de incidentes
				Procedimiento para la obtención de pruebas
				Registro de incidentes de seguridad
			Comunicación de incidentes	Definición de equipo de Gestión de incidentes

ANEXO K – POLÍTICAS ELABORADAS Y DETALLES GENERALES			
Nombre	Objetivo	Alcance	Responsabilidades
Política De Acceso Remoto	Aclarar a todos los usuarios de acceso remoto a la infraestructura de la empresa, cuáles son sus responsabilidades, y cuáles son los riesgos y peligros potenciales para la empresa en caso del mal uso y abuso del acceso remoto por parte de los usuarios.	Este documento se enfoca en los siguientes aspectos: • Los requerimientos de Seguridad de Acceso Remoto; • Los controles apropiados utilizados para poder reducir los riesgos asociados con las conexiones de acceso remoto a la red de la empresa; y • Proveer guía en la implementación de estos requerimientos. Esta política es aplicable a: • Todos los usuarios y dispositivos de acceso remoto en el Grupo CreCos. • Administradores de red y/o acceso remoto y los que juegan un papel en la Seguridad de la Información (como está definido en la estructura organizacional).	El Usuario Solicitante es responsable de: • Completar los datos necesarios para solicitar el servicio. • Obtener las autorizaciones necesarias. • Enviar la solicitud de acceso remoto con las aprobaciones a la Mesa de Ayuda. La Mesa de Ayuda es responsable de: • Enviar la solicitud de servicio al grupo que debe atender el requerimiento. • Instalar las herramientas requeridas para que el servicio funcione correctamente en la máquina del usuario. • Probar la configuración del perfil del usuario. • Mantener actualizada el registro de conexión de todos los usuarios de acceso remoto y dispositivos asignados. El Gerente de Área es responsable de: • Aprobar las solicitudes de acceso remoto de los colaboradores que cuenten con una razón válida de negocios para otorgar tal acceso. El Líder de Seguridad de la Información es responsable de: • Monitorear semestralmente los usuarios activos de Acceso Remoto según el registro de conexión. • Autorizar las conexiones de acceso remoto. • Revisar cada tres meses el registro de acceso remoto y asegurar que la necesidad de negocio continúa. • Revocar los privilegios de los usuarios de acceso remoto cuando sea requerido.

ANEXO K – POLÍTICAS ELABORADAS Y DETALLES GENERALES			
Nombre	Objetivo	Alcance	Responsabilidades
Política De Administración De Software	Asegurar el manejo apropiado de los activos de software y por consiguiente prevenir la violación de los derechos de autor.	Esta política y este proceso son aplicables a cualquier software para Aplicaciones, Sistemas Operativos, Bases de Datos, Software Intermedio, Redes, y Desarrollos de Usuarios Finales. El mismo procedimiento utilizado para manejar licencias de software. La Política es aplicable a todos los usuarios de computadoras en CRECOS y a cualquier dispositivo que sea propiedad de CRECOS. En el contexto de CRECOS, el término “usuario” podría significar cualquiera de lo siguiente: empleado a tiempo completo, empleado a medio tiempo, consultor, contratista, voluntario, empleado de un subcontratista o cualquier otro tipo de usuario.	El Solicitante es responsable de: • Crear el requerimiento en la Mesa de Ayuda con la información correcta. La Mesa de Ayuda es responsable de: • Verificar que la información proporcionada en el ticket esté completa. • Realizas la instalación del software de acuerdo con las pautas definidas. • Informar al Solicitante acerca del estatus del ticket. El Gerente de Departamento es responsable de: • Autorizar la solicitud si hay una razón válida. • Notificar al Departamento de TI que presupueste las compras de software, como parte del proceso de presupuesto. El Gerente de Infraestructura es responsable de: • Evaluar el impacto del software en la red El Líder de Seguridad de Información es responsable de: • Evaluar el impacto del software en la seguridad de la red y los datos. El Gerente de IT es responsable de: • Custodiar la Biblioteca de Software. • Autorizar todo el software a desechar. • Registrar las entradas y salidas de software en la biblioteca.

ANEXO K – POLÍTICAS ELABORADAS Y DETALLES GENERALES			
Nombre	Objetivo	Alcance	Responsabilidades
Política de Carpetas Compartidas	El servidor de carpetas compartidas permite a los usuarios almacenar archivos a los que se puede acceder desde cualquier ordenador de la compañía. Este documento delinea las políticas internas alrededor del proceso para controlar el acceso a estos recursos. La implementación y práctica de estas políticas reducirá el acceso no autorizado a la información y tecnologías de Información.	Esta política es aplicable a todos los usuarios que pertenezcan y/u operen en las instalaciones de la empresa.	1. El personal del Área de Sistemas será el único autorizado para la creación de las carpetas compartidas en los servidores. El servidor representará un repositorio de información que se mantendrá actualizado constantemente. 2. Debe existir un colaborador por el lado del negocio que se haga responsable de la información que se almacene en la carpeta. 3. El acceso a la carpeta sólo puede ser autorizado por el dueño de la carpeta, el cual deberá indicar qué grupos necesitan acceso a cada recurso y qué nivel de acceso precisan. 4. El colaborador solicitante de la creación de la carpeta debe eliminar información histórica que no está siendo usada, dicha información puede ser respaldada en algún medio físico que el solicitante considere apropiado.
Política De Gestión De Cambios	El proceso comprende los cambios solicitados y relacionados con la infraestructura o el ambiente de las aplicaciones, incluyendo cambios iniciados por un proyecto, mejoras y tareas normales de mantenimiento.	Se aplica a todos los cambios a lo largo de Aplicaciones, Sistemas Operativos, Bases de datos, Middleware y Componentes de Red.	1. Todo cambio, modificación, mejoras que afecten al ambiente de producción debe seguir obligatoriamente el proceso de Administración de Cambios. Requerimiento de cambio que no siga el proceso no será considerado. 2. Todo cambio debe tener un análisis de riesgo e impacto. El equipo de especialistas del Área de Sistemas tiene la responsabilidad de realizar este análisis. 3. Los cambios serán categorizados en cambios normales, cambios rutinarios, cambios menores, y cambios de emergencia.

ANEXO K – POLÍTICAS ELABORADAS Y DETALLES GENERALES			
Nombre	Objetivo	Alcance	Responsabilidades
Política De Respaldo De Información	El propósito es describir los pasos a seguir a fin de llevar a cabo un apropiado respaldo y restauración de la información.	Este procedimiento aplica a las tareas de respaldo y restauración para todos los sistemas claves de propiedad de la organización para garantizar la disponibilidad de la información y la continuidad del servicio de Sistemas de Información.	El Gerente de Sistemas es responsable de: • Autorizar cualquier desviación del plan de respaldo de acuerdo con el Reporte de Evaluación de Riesgo. El Adm. de Base de Datos es responsable de: • Solicitar el respaldo o restauración de la información. • Solicitar cualquier modificación de la especificación actual de respaldo. • Determinar en coordinación con el Adm. de Centro de Cómputo el momento para iniciar la ejecución del respaldo o restauración de la información. • Verificar la ejecución correcta de los trabajos de respaldo o restauración. El Jefe de Infraestructura es responsable de: • Autorizar las solicitudes de respaldo enviados ya sea por el Propietario de Proceso de Negocio o por el Adm. de Centro de Cómputo. El Adm. de Centro de Cómputo es responsable de: • Etiquetar el respaldo de cinta. • Verificar la ejecución correcta de los trabajos de respaldo. • Recibir las nuevas cintas que se hayan solicitado. • Documentar cualquier error reportado por las herramientas de respaldo y reportar fallas de equipos.

ANEXO K – POLÍTICAS ELABORADAS Y DETALLES GENERALES			
Nombre	Objetivo	Alcance	Responsabilidades
Política De Segregación de Funciones	El propósito de la política de segregación de funciones es proveer al Grupo CRECOS la visión y principios de cómo se deben diseñar los roles para asegurar que ningún rol individual controle todos los aspectos clave de una transacción o proceso/evento.	La política de segregación de funciones es aplicable en todas las aplicaciones, sistemas operativos, bases de datos, software que conecta aplicaciones, redes y cualquier tipo de usuarios.	1. La división de obligaciones asegurará que la custodia por activos, autorización o aprobación de transacciones/procesos o eventos que afecten a aquellos activos y la grabación, reporte y auditoria sobre el activo no sea controlado por el mismo individuo. 2. Los procesos de IT serán divididos en términos de desarrollo de aplicación y mantenimiento y los procesos operacionales técnicos de IT que incluyen la administración de la base de datos, manejo de la infraestructura y el manejo de operaciones IT. 3. Los procesos de monitoreo y auditoria (procesos de autoridad) serán divididos de los procesos operacionales de IT. 4. La administración de acceso de usuarios, en donde sea posible, será divididos en términos de: • Individuos que solicitan el acceso; • Individuos que confirman acceso; • Individuos que establecen el acceso (desarrollan el mantenimiento de requerimientos de roles/acceso); • Individuos que llevan a cabo el mantenimiento de usuarios; • Individuos que monitorean las violaciones de acceso; • Individuos que usan los derechos de un usuario privilegiado (Adm. de sistema); e • Individuos que monitorean el uso del acceso de usuarios privilegiados.

ANEXO K – POLÍTICAS ELABORADAS Y DETALLES GENERALES			
Nombre	Objetivo	Alcance	Responsabilidades
Política De Administración De Usuarios y Claves	Normar el procedimiento de administración de usuarios y claves de servidores.	Grupo CRECOS.	• Los usuarios serán responsables por el mal uso o uso indebido de las claves a ellos asignadas. • Las claves de usuarios deben ser individuales y su uso debe ser personal e intransferible. Es prohibida la divulgación de las claves a otras personas, aunque se trate de usuarios autorizados. • Las claves se deben crear para permitir el desarrollo de las actividades de acuerdo a lo establecido en la descripción de funciones del cargo que desempeña el usuario. No se deben autorizar nuevas atribuciones para ningún usuario si estas no están incluidas en la descripción de sus funciones. • Se deben dar instrucciones a los usuarios sobre la conformación de la clave secreta de forma tal que no sea fácilmente descifrable; por lo tanto, las claves no deben corresponder a números en secuencia, nombres o códigos de empleados, fechas, etc. • Todo usuario debe cambiar su clave por lo menos una vez cada tres meses. El sistema mantendrá un control automático que hará que las claves caduquen cada 90 días.