Máster Universitario en Seguridad de las TIC (MISTIC)

Plan de Implementación de la norma ISO/IEC ISO 27001:2013 para un Operador de Información PILA

Trabajo Final de Máster

José Alejandro Rincón Rodríguez
Diciembre de 2019
Docente Colaborador: Antonio José Segovia Henares

TABLA DE CONTENIDO

RESUMEN

Un Sistema de Gestión de la Seguridad de la Información es un conjunto de políticas de administración de la información que conlleva la elaboración, mantenimiento y mejora de un esquema documental, un proceso de gestión de la seguridad y unos procedimientos que permitan gestionar todo el conjunto.

El objetivo de este trabajo es realizar un ejercicio de implementación de un Sistema de Gestión de Seguridad de Información para un Operador de información PILA, el cual se encarga de la liquidación de la planilla en la cual las empresas y las personas realizan sus aportes al Sistema de Seguridad Social en Colombia.

El SGSI se ha de integrar en la organización de manera que se convierta en una parte fundamental de la gestión de ésta. Un SGSI correctamente implantado permite establecer procedimientos que aseguren la Confidencialidad, Disponibilidad e Integridad de la información que se gestiona en la organización.

En el desarrollo de este trabajo se han seguido las directrices establecidas en la norma ISO 27001, que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI mediante un proceso de mejora continua.

ABSTRACT

An Information Security Management System is a set of information administration policies which involves elaborating, maintain and improve a documentation schema, a security management process and procedures to manage the whole set.

The objective of this work is to perform an exercise of implementation of an Information Security Management System for a PILA Information Operator, which is responsible for the liquidation of contributions payroll in which companies and individuals make their contributions to the social security system in Colombia.

The ISMS must be integrated in the organization to allow it to become in an essential part of its management. A correctly implanted ISMS allows to establish procedures to ensure the confidentiality, availability and integrity of the information managed by the organization.

In the development of this work we have followed the guidelines set in ISO 27001, which specify the requirements for establishing, implementing, maintaining and improving an ISMS through a process of continuous improvement.

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

1. INTRODUCCIÓN

La implementación de la norma ISO/IEC 27001:2013 es un aspecto fundamental en las organizaciones que deseen alinear sus objetivos y principios de seguridad de la información acorde a los estándares de referencia a nivel internacional.

El objetivo principal es establecer las bases de un proceso de mejora continua en temas relacionados con la seguridad de la información, que permitan a las organizaciones conocer el estado de esta e identificar las acciones que se requieran para minimizar riesgos potenciales que afecten la integridad, la confidencialidad y la disponibilidad del principal activo de las empresas: la información.

Este proyecto busca la implementación de un Sistema de Gestión de la información para una empresa encargada de realizar la liquidación de cada uno de los aportes que hacen los ciudadanos al Sistema de Seguridad Social Colombiano, que corresponde a Pensiones, Salud, Riegos laborales y Servicios Complementarios (Como Cajas de Compensación, Subsidio familiar, etc.), a través de la planilla integrada de liquidación de aportes al sistema (PILA).

La metodología está definida en las siguientes fases:

1. Documentación normativa de las mejores prácticas de seguridad de la información
2. Definición de la situación actual de la organización y de los objetivos del Sistema de Gestión de Seguridad
3. Análisis, identificación y valoración de riesgos relacionados con el Sistema.
4. Evaluación del nivel de cumplimiento de la norma ISO/IEC 27001:2013
5. Propuesta de proyectos para mejorar los esquemas de Gestión de la Seguridad de la Información
6. Esquema documental

Los entregables del proyecto serán los siguientes documentos

1. Informe de Análisis Diferencial
2. Esquema documental
3. Análisis de Riesgos
4. Plan de Proyectos de Seguridad de la Información
5. Auditoria de Cumplimiento
6. Presentación de resultados finales

2. METODOLOGÍA DE TRABAJO

Se realizará una aproximación por fases del proyecto con el objetivo de tratar cada uno de los apartados de forma que se pueda ejecutar en los tiempos definidos. Así, el cronograma de actividades es el siguiente:

- **Fase 1: Situación actual: Contextualización, objetivos y análisis diferencial**

Introducción al Proyecto. Enfoque y selección de la empresa que será objeto de estudio. Definición de los objetivos del Plan Director de Seguridad y Análisis diferencial de la empresa con respecto la ISO/IEC 27001+ISO/IEC 27002

- **Fase 2: Sistema de Gestión Documental**

  Elaboración Política de Seguridad. Declaración de aplicabilidad y Documentación del SGSI

- **Fase 3: Análisis de riesgos**

  Elaboración de una metodología de análisis de riesgos: Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.

- **Fase 4: Propuesta de Proyectos**

  Evaluación de proyectos que debe llevar a cabo la Organización para alinearse con los objetivos planteados en el Plan Director. Cuantificación económica y temporal de los mismos.

- **Fase 5: Auditoría de Cumplimiento de la ISO/IEC 27002:2013**

  Evaluación de controles, madurez y nivel de cumplimiento.

- **Fase 6: Presentación de Resultados y entrega de Informes**

  Consolidación de los resultados obtenidos durante el proceso de análisis. Realización de los informes y presentación ejecutiva a la Dirección. Entrega del proyecto final.

En el siguiente diagrama de Gantt se resumen las fases a ejecutar en el proyecto

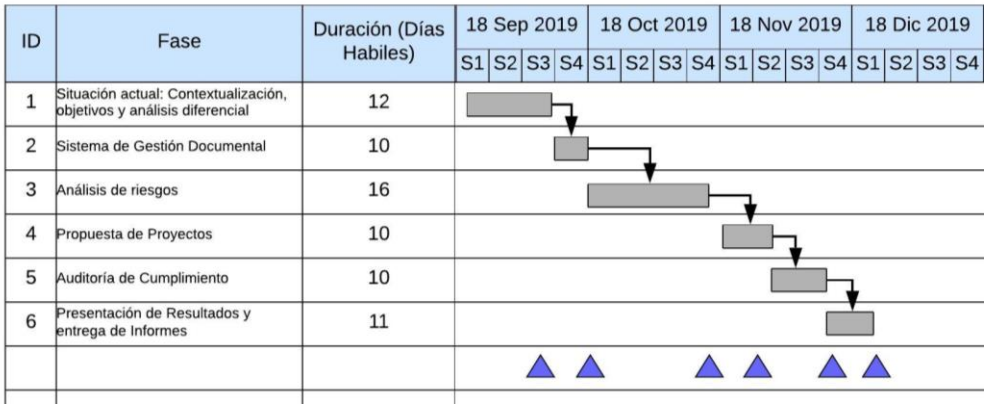

Ilustración 1 – Cronograma de Trabajo

3. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

3.1 DESCRIPCIÓN DE LA EMPRESA DE ESTUDIO

La empresa seleccionada es una empresa ficticia llamada PISIS S.A. (Pagos Integrados de Seguridad Social), cuyo objetivo principal es realizar la liquidación de pagos de seguridad social tanto a empresas grandes y pequeñas, como a trabajadores independientes. Esta organización se encuentra localizada en la ciudad de Bogotá, Colombia.

3.2 ACTIVIDAD Y ENTORNO

La compañía fue fundada en el año 2006 y de acuerdo con sus estatutos, su objetivo principal, la ejecución de todos los actos y contratos relativos al procesamiento de información, De conformidad con lo anterior, la sociedad PISIS podrá:

- Realizar actividades como operador de información y demás actividades habilitadas por disposición normativa relacionadas con manejo de información en el campo de la protección social
- Ejecutar actividades de Outsourcing y asesoría en temas relacionados en el campo de la protección y la seguridad social.

Actualmente dentro del mercado de Operadores de Información encargados de liquidar pagos a través de la planilla PILA es el segundo operador a nivel nacional, con un índice de liquidaciones promedio mensual de más de 300.000, las cuales en su mayoría (200.000) corresponden a empresas de diferentes tamaños y sectores (tanto del ámbito estatal como privadas) y el resto corresponden a trabajadores independientes de distintos sectores económicos.

3.2.1 Misión

La misión de la compañía es contribuir con el desarrollo de la sociedad entendiendo la seguridad social y acercando servicios especializados y complementarios sencillos, brindando soluciones simples e innovadoras de gestión.

3.2.2 Visión

La visión de la compañía es para el año 2020 es asegurar que los ingresos van a crecer un 70% respecto a 2015, adicionalmente se busca estar dentro de las 250 mejores empresas para trabajar en Colombia.

Para el 2035 se busca tener una participación del 70% del mercado de la planilla Integral de Liquidación de Aportes (PILA) y que se genere un 30% de los ingresos de la compañía correspondan a nuevos negocios.

3.2.3 Mapa de Procesos

La compañía cuenta con tres tipos de procesos: Estratégico, Core y de Apoyo. Dentro de esta categorización se encuentran todos los procesos que la organización utiliza para el desarrollo de su objeto social.

Los procesos también muestran interacciones entre ellos mismos siguiendo la secuencia: salidas del planear son las entradas del hacer, salidas del hacer entradas del verificar, salidas del verificar entradas del actuar. En este sentido, la organización tiene un enfoque basado en procesos para la ejecución de sus actividades, el cumplimiento de su misión y el alcance de su visión.

PISIS. como operador de información, debe garantizar a los aportantes la liquidación y pago de los aportes de seguridad social, por ende, el CORE de negocio está en la Gestión Operativa, el cual tiene como objetivo "Diseñar, implementar, monitorear y mejorar el proceso de liquidación y pago de aportes a seguridad social y parafiscales a través de la planilla única, para garantizar al aportante el fácil acceso, pago y entrega de información a las administradoras del sistema en las condiciones adecuadas"; contando con los demás procesos como sistemas habilitadores de la operación del negocio.

Los procesos Gestión del Talento, Gestión Tecnológica, Gestión Administrativa, Gestión Contable, Gestión Financiera soportan directamente la Gestión Operativa de la Organización. Los procesos Gestión Comercial, Quejas y Reclamos y Apoyo Jurídico soportan la Gestión Operativa de cara a los Clientes.

El proceso Gestión de Incidentes está establecido para gestionar y controlar los eventos tecnológicos y de seguridad internos y por ende del servicio que se presta.

Los Procesos que forman un círculo de colores, son Sistemas Habilitadores que permiten asegurar la mejora del Sistema teniendo en cuenta la dinámica del entorno donde se desarrolla el negocio de Simple S.A.

- Gestión Gerencial, Direccionar.
- Gestión de Riesgos, Prevenir.
- Gestión Documental, Estandarizar.
- Auditorias, Controlar.
- Mejora Continua, Ser proactivos.

Todos los procesos nombrados anteriormente, están relacionados e interactuando permanentemente entre sí, de manera que el canal funciona como una organización sistémica y compleja, en la cual cada proceso es necesario para el desarrollo de los demás. Esta interacción se puede ver en el siguiente gráfico:

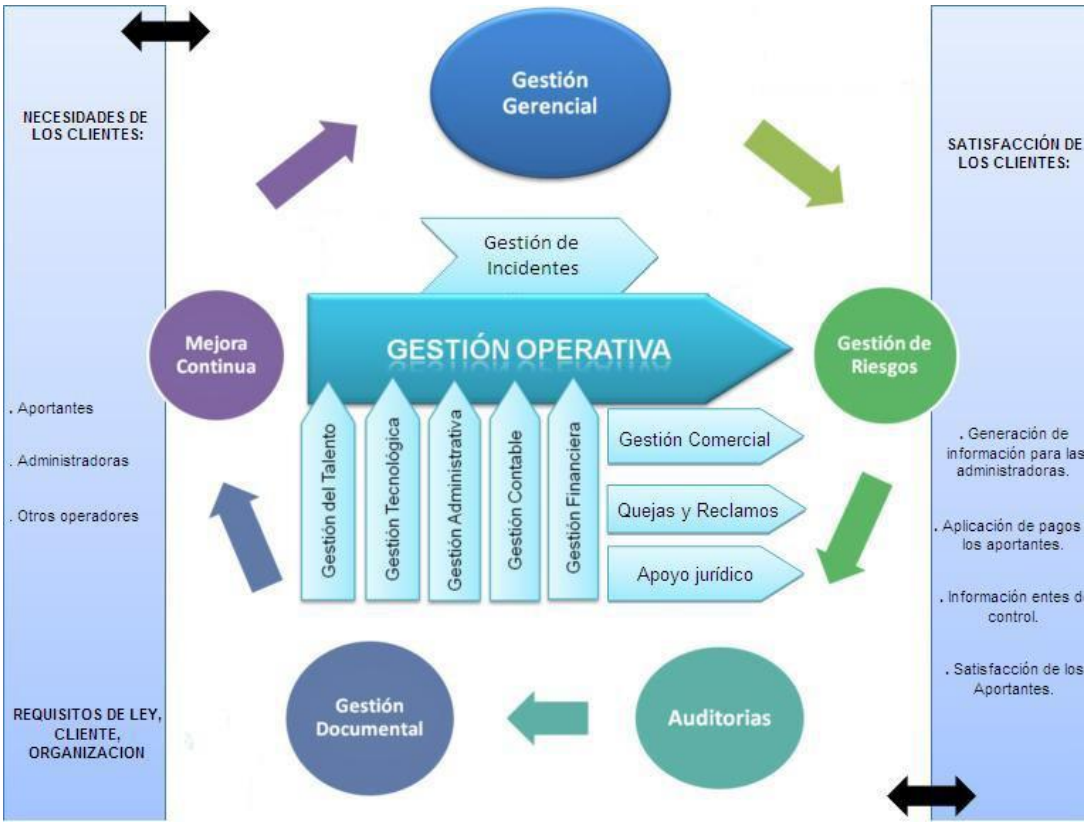

Ilustración 2 – Mapa de Procesos PISIS

3.2.4 Organigrama

La compañía se encuentra estructurada en tres áreas principales: Administrativa y financiera, Comercial y Mercadeo, y Operaciones y TI, cada una con una serie de departamentos dependientes.

Respecto al número de departamentos tenemos el siguiente personal:

- Gerente General (1)
- Gerente Financiero y Administrativo (1), Profesional de Tesorería y Planeación Financiera (2), Profesional Administrativo (1), Auxiliar Administrativo (1), profesional Contable y Tributario (2), Profesional de Procesos y Calidad (1), Auxiliar de Procesos y Calidad (1), Analista Documental (1)
- Jefe Comercial Electrónico (1), Ejecutivos de Cuentas Electrónicas (5), Jefe de Mercadeo (1), Analista de Mercadeo y Comunicaciones (1), Gestor Empresarial (1), Jefe de Servicio al Cliente (1), Analistas de Servicio al Cliente (3), Jefe Comercial Posventa Electrónico y Asistido (1), Ejecutivo Posventa Electrónico (5), Ejecutivo Posventa Asistido (5), Jefe de Nuevos Mercados (1), Ejecutivos de Nuevos Mercados (5),
- Jefe de Operaciones (1), Profesional de Operaciones (2), Analista de Operaciones (5), Jefe de Infraestructura TI, Auxiliar de Infraestructura TI (3), Jefe de Aplicaciones (1); Profesional de Aplicaciones (2), Analistas de desarrollo (5).

- Jefe de Operaciones (1), Profesional de Operaciones (2), Analista de Operaciones (5), Jefe de Infraestructura TI, Auxiliar de Infraestructura TI (3), Jefe de Aplicaciones (1); Profesional de Aplicaciones (2), Analistas de desarrollo (5).
- Director Jurídico y Secretario General (1), Profesional Jurídico (1), Analista Jurídico (2).
- Director de Control Interno y Riesgos (1), Jefe de Riesgos (2), Jefe de Control Interno (1), Profesional de Riesgos (1), Analista de Riesgos (1), Profesional de Auditoría (2), Analista de Control Interno (1).
- Dirección de Talento Humano (1), Profesional de Selección y Contratación (1), Profesional de Capacitación (1), Analista de Nomina (1), Analista de Seguridad y salud en el Trabajo (1), Mensajero Motorizado (1), Analistas de Talento Humano (2).
- Jefe de Proyectos y Planeación Estratégica (1), Profesional de Proyectos (2), Analista de Planeación Estratégica y Proyectos (2).

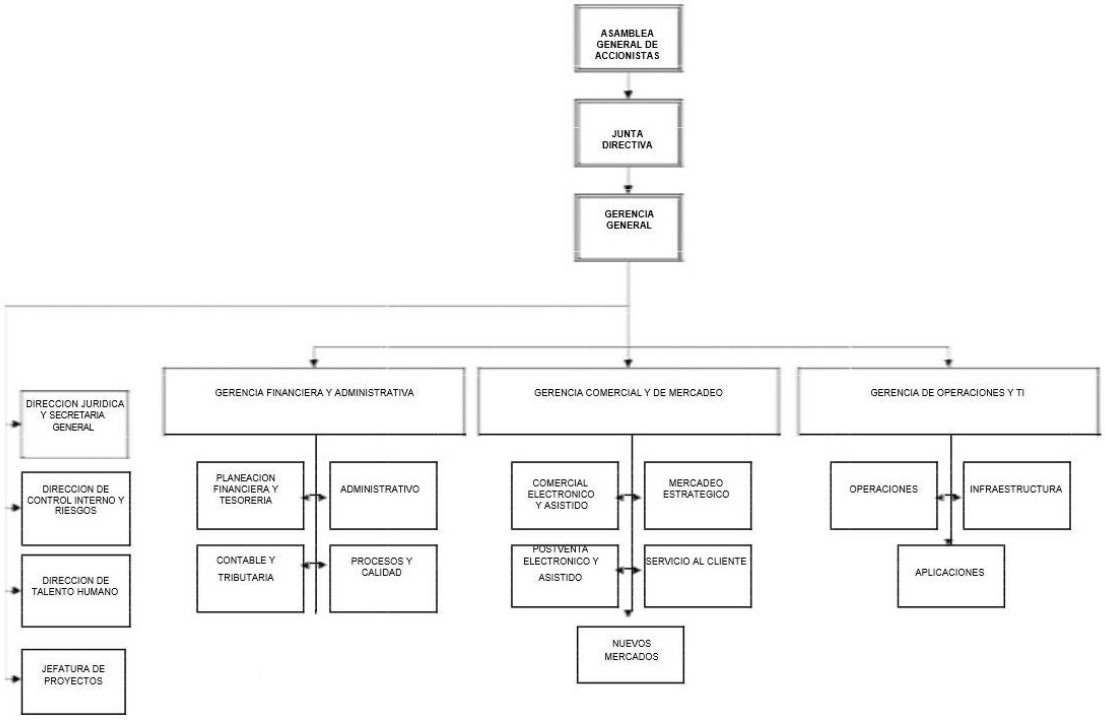

Ilustración 3 – Organigrama PISIS

3.2.5 Arquitectura de Red

La arquitectura de red con la que cuenta la compañía es muy sencilla. Se cuenta con 23 servidores, los cuales ejecutan diversas operaciones, tales como File Server, Dominio, Backup's, además de las bases de datos y servidores de aplicación del portal web encargado de realizar la liquidación de la planilla asistida, donde los usuarios pueden generarla. También se junta con una serie de conexiones protegida son Firewall para realizar la transmisión de información con las ciudades en la cuales se presentan sucursales (Cali, Medellín, Barranquilla, Pereira, Villavicencio) y hay conexiones de tipo VPN y SFTP para la transmisión de información entre las diferentes administradoras o entidades que hacen parte del sistema de seguridad social en Colombia (Tales como las Entidades Promotoras de Salud, Fondos de pensiones, Fondos de Cesantías, Cajas de Compensación, etc.), también se tiene

servicios de conexión Cloud con diferentes proveedores como CRM (Manejo de quejas y reclamos), ERP, KAWAK (Sistema de Gestión documental) y ARUS (Plataforma de administración). Finalmente se observa una conexión dedicada de internet con el Banco de la Republica, allí en los equipos del banco, se realizan las principales transacciones de ventas y compras de registros, los cuales son enviados a otras administradoras y Operadores de información, siendo este negocio, la principal fuente de ingresos de la compañía.

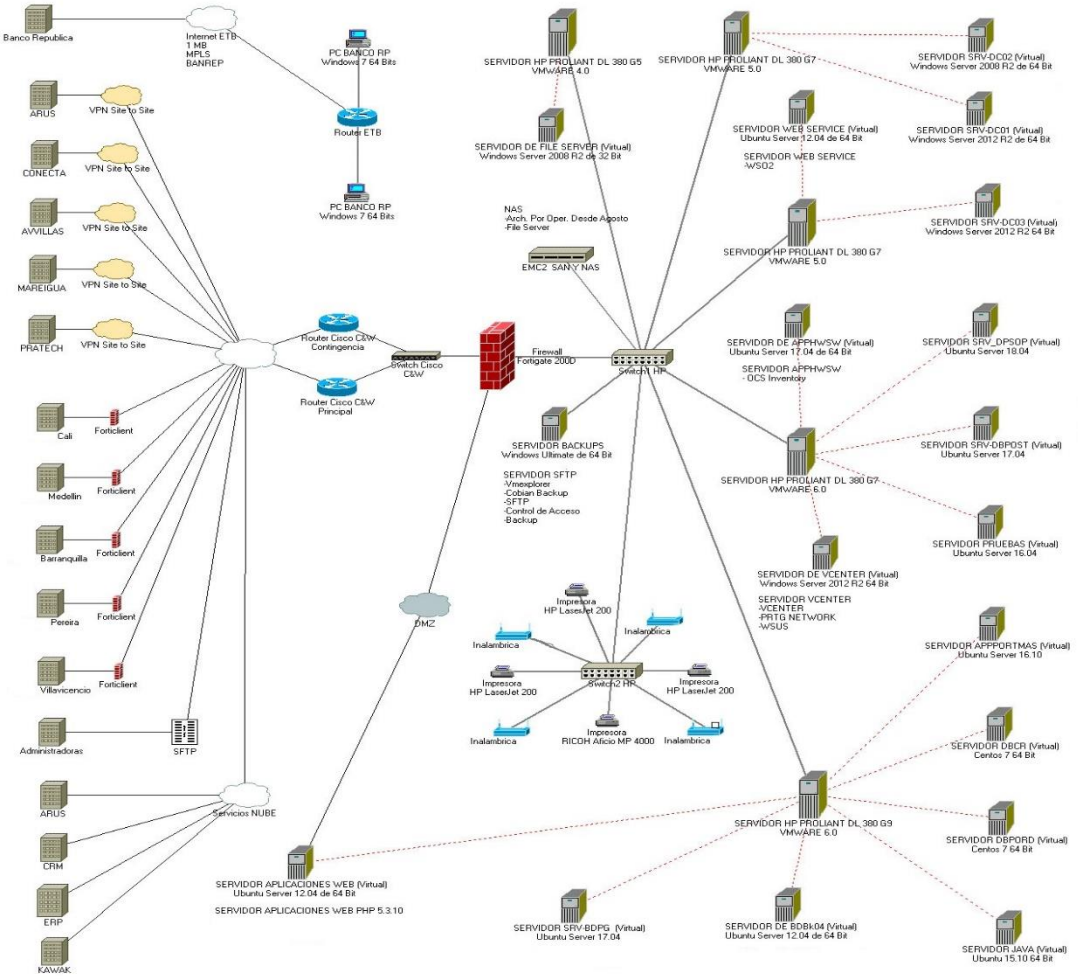

Ilustración 4 – Diagrama de Red PISIS

3.3 LA NORMA ISO/IEC 27001:2013

La ISO/IEC 27001:2013 es una de las normas definida por la ISO (International Organization for Standardization) que establece los diferentes lineamientos básicos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Este Estándar fue publicado por primera vez en el año 2005 y se realizó una actualización de este en el año 2013. La norma actual, ha sido la evolución de otros estándares de seguridad de la información como mencionamos a continuación:

- 1901 – Normas "BS": La British Standards Institution es fundada en el Reino unido y se realiza la publicación de normas con el prefijo "BS", las cuales tienen un carácter

internacional. Estas son el origen de normas actuales como ISO 9001, ISO 14001 u OHSAS 18001.

- 1995 - BS 7799-1:1995: Se define un estándar de mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Eran recomendaciones que no permitían la certificación ni establecía la forma de conseguirla.
- 1998 – BS 7799-2:1999: Se realiza una revisión de la norma mencionada anteriormente. Establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.
- 1999 – BS 7799-1:1999: Se realiza una revisión de la norma.
- 2000 – ISO/IEC 17799:2000: ISO (International Organization for Standardization) toma la norma británica BS 7799-1 que dio lugar a la llamada ISO 17799, sin experimentar grandes cambios.
- 2002 – BS 7799-2:2002: Se publicó una nueva versión que permitió la acreditación de empresas por parte de una entidad certificadora en Reino Unido y en otros países de la Commonwealth.
- 2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005: Aparece el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.
- 2007 – ISO 17799: Se renombra y se convierte en la norma ISO 27002:2005
- 2007 – ISO/IEC 27001:2007: Se publica una nueva versión de la norma.
- 2009 – Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M: 2009.

La norma puede ser adaptada en cualquier tipo de organización, independiente del sector y del tamaño de esta. Está redactada por personal cualificado en el tema y proporciona una metodología para para implementar la seguridad de la información en una empresa. También permite que las organizaciones sean certificadas en este estándar, lo cual conlleva que las entidades cumplan con los lineamientos de la norma y facilite la competitividad entre ellas, garantizando elementos mínimos que son reconocidos a nivel universal.

3.3.1 Estructura de la Norma Iso 27001

La estructura del estándar internacional ISO 27001:2013 cambia, al pasar de 8 cláusulas a 10. Esto se produce derivado de su alineación al Anexo SL de las directivas de ISO/IEC Parte 1, con lo cual ya no se basa en el modelo PDCA (Plan-Do-Check-Act), sino que ahora aplica la estructura de alto nivel, títulos de las sub-cláusulas, texto idéntico, términos comunes y las principales definiciones definidas en el Anexo SL.

Por tanto, mantiene compatibilidad con otros estándares de sistemas de gestión que también ha adoptado dicho Anexo (como ISO 22301: Business Continuity management systems — Requirements).

A nivel de controles, la nueva ISO, aunque aumentando el número de dominios de seguridad de 11 a 14, reestructura el número de controles, pasando de 133 a 114.

Entre los principales cambios que se encuentran con respecto a la norma publicada en el año 2005 son los siguientes:

- Eliminación de la referencia al enfoque de proceso de mejora continua PDCA.
- Reestructuración general de capítulos y subapartados con el fin de que todos los estándares de sistemas de gestión tengan la misma estructura.
- Mayor énfasis en el conocimiento del contexto de la organización y en el entendimiento de las necesidades de las partes interesadas. Este conocimiento debe suponer el punto fundamental para el establecimiento del sistema de gestión: definición del alcance, política, establecimiento de objetivos y análisis de riesgos.
- El proceso de análisis de riesgos se define de forma más genérica. Han sido eliminadas las referencias a la identificación de activos, amenazas y vulnerabilidades. Únicamente se hace necesario identificar riesgos (sin especificar cómo) asociados a la pérdida de confidencialidad, integridad y disponibilidad, tras analizar las potenciales consecuencias y la probabilidad para, finalmente, cuantificar el riesgo.
- Respecto a la selección de controles de seguridad para el tratamiento del riesgo, se deja a decisión de las organizaciones la selección de un marco de controles en caso de que no se desee seguir ISO 27002, aunque, de cualquier modo, se deberá comparar con los controles del Anexo A para comprobar que no se obvia ningún control.
- Se otorga una mayor importancia al liderazgo de la Dirección en el sistema de gestión, no sólo desde el punto de vista de un compromiso formal, como se especificaba en la versión anterior.
- Se otorga mayor importancia al área de monitorización y medición del SGSI.
- Se ha eliminado el listado de documentos obligatorios, aunque en el cuerpo del estándar se hace referencia a distintos requisitos documentales. Por otro lado, se elimina la separación entre documentos y registros, siendo denominados, simplemente, información documentada.
- Los cambios en el Anexo A: se pasa de 11 a 14 capítulos y el número total de controles se reduce a 114. Criptografía se ha convertido en una sección separada y ya no es (lógicamente) parte del dominio de desarrollo y adquisiciones de sistemas. Algo similar ha sucedido con las relaciones con los proveedores, se han convertido en una sección aparte. El dominio gestión de comunicaciones y operaciones se dividió en operaciones de seguridad y comunicaciones de seguridad.

3.3.2 Código de Buenas Prácticas - ISO/IEC 27002

La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como “la preservación de la confidencialidad, integridad y disponibilidad”. La norma fue publicada inicialmente como un cambio de nombre de la norma ISO 17999, la cual estaba basada en un documento publicado por el Gobierno británico que se convirtió en un Estándar en el año 1995. En el año 2000 fue publicado como norma internacional bajo el nombre indicado anteriormente y en 2005 aparece una nueva versión, integrada dentro de la norma ISO 27001. Las dos normas son totalmente complementarias.

La norma ISO 27002 se encuentra organizado en base a 14 dominios, 35 objetivos de control y 114 controles.

Los dominios de la norma son los siguientes:

1. **Políticas de Seguridad:** Sobre las directrices y conjunto de políticas para la seguridad de la información. Revisión de las políticas para la seguridad de la información.
2. **Organización de la Seguridad de la Información:** Trata sobre la organización interna: asignación de responsabilidades relacionadas a la seguridad de la información, segregación de funciones, contacto con las autoridades, contacto con grupos de interés especial y seguridad de la información en la gestión de proyectos.
3. **Seguridad de los Recursos Humanos:** Comprende aspectos a tomar en cuenta antes, durante y para el cese o cambio de trabajo. Para antes de la contratación se sugiere investigar los antecedentes de los postulantes y la revisión de los términos y condiciones de los contratos. Durante la contratación se propone se traten los temas de responsabilidad de gestión, concienciación, educación y capacitación en seguridad de la información. Para el caso de despido o cambio de puesto de trabajo también deben tomarse medidas de seguridad, como lo es des habilitación o actualización de privilegios o accesos.
4. **Gestión de los Activos:** En esta parte se toca la responsabilidad sobre los activos (inventario, uso aceptable, propiedad y devolución de activos), la clasificación de la información (directrices, etiquetado y manipulación, manipulación) y manejo de los soportes de almacenamiento (gestión de soporte extraíbles, eliminación y soportes físicos en tránsito).
5. **Control de Accesos:** Se refiere a los requisitos de la organización para el control de accesos, la gestión de acceso de los usuarios, responsabilidad de los usuarios y el control de acceso a sistemas y aplicaciones.
6. **Cifrado:** Versa sobre los controles como políticas de uso de controles de cifrado y la gestión de claves.
7. **Seguridad Física y Ambiental:** Habla sobre el establecimiento de áreas seguras (perímetro de seguridad física, controles físicos de entrada, seguridad de oficinas, despacho y recursos, protección contra amenazas externas y ambientales, trabajo en áreas seguras y áreas de acceso público) y la seguridad de los equipos (emplazamiento y protección de equipos, instalaciones de suministro, seguridad del cableado, mantenimiento de equipos, salida de activos fuera de las instalaciones, seguridad de equipos y activos fuera de las instalaciones, reutilización o retiro de equipo de almacenamiento, equipo de usuario desatendido y política de puesto de trabajo y bloqueo de pantalla).
8. **Seguridad de las Operaciones:** Procedimientos y responsabilidades, protección contra malware, resguardo, registro de actividad y monitorización, control del software operativo, gestión de las vulnerabilidades técnicas y coordinación de la auditoría de sistemas de información.
9. **Seguridad de las Comunicaciones:** Gestión de la seguridad de la red y gestión de las transferencias de información.
10. **Adquisición de sistemas, desarrollo y mantenimiento:** Requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.
11. **Relaciones con los Proveedores:** Seguridad de la información en las relaciones con los proveedores y gestión de la entrega de servicios por proveedores.
12. **Gestión de Incidencias que afectan a la Seguridad de la Información:** gestión de las incidencias que afectan a la seguridad de la información; mejoras.

13. **Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio:** Continuidad de la seguridad de la información y redundancias.
14. **Conformidad:** Conformidad con requisitos legales y contractuales y revisiones de la seguridad de la información.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 114 entre todas las secciones, aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

3.4 ALCANCE DEL SGSI

El sistema de gestión de seguridad de la información y sus procesos deben ser desarrollados con el objetivo de garantizar la seguridad de los activos de información, circunscritos en el siguiente alcance:

"*Monitoreo y control del procesamiento y administración de la información del servicio de liquidación y pago de planilla integrada para la liquidación de aportes a través del portal transaccional, para cumplir con los requisitos legales, reglamentarios que aseguren el cumplimiento de los objetivos de seguridad de la información, enmarcados en objetivos estratégicos que buscan satisfacer las necesidades de las partes interesadas.*"

Para lo cual aplican todos los procesos de la organización y a nivel tecnológico, aplica el portal transaccional, en el cual se realizan las liquidaciones de aportes al sistema de Gestión Social.

3.5 OBJETIVOS DEL PLAN DIRECTOR DE SEGURIDAD

El Plan Director de Seguridad se define como la base a las diferentes estrategias de negocio que se tengan en la empresa y sus necesidades puntuales, de modo que la identificación de procesos de negocio y de activos que lo soporten constituye un aspecto fundamental durante su desarrollo.

El motivo de la elaboración del Plan Director es definir un plan de acciones con el objetivo de cumplir con los objetivos del Sistema de Gestión de Seguridad de la Información y definirlo. El ámbito del plan director abarca toda la organización, por lo cual las medidas que se establezcan estarán orientadas a aspectos funcionales, técnicos y organizativos.

Los objetivos deseados por la compañía son los siguientes:

- Establecer la seguridad de la información como un proceso más dentro de la organización.
- Convertir la seguridad de la información en la prioridad principal en la gestión de los sistemas de información
- Establecer el marco organizativo, técnico y funcional para poder certificar la organización en la norma ISO 27001:2013
- Certificar el Sistema de Seguridad de la información con el objetivo de asegurar contratos en los cuales los clientes puedan disponer de tal certificación
- Convertir la seguridad de la información como elemento principal de la compañía y marca de calidad y compromiso.

3.5.1 Objetivos de Seguridad de la Información

Los objetivos deseados por la compañía a nivel de seguridad de la información son los siguientes:

- Establecer los roles y responsabilidades en términos de seguridad de la información.
- Apoyar la definición, implantación y pruebas del plan de continuidad del negocio con relación a la seguridad de la información.
- Establecer un marco de seguridad de la información en relación con proveedores y terceros.
- Garantizar el cumplimiento legal establecido en la normatividad nacional (Ley Protección de datos) e internacional.
- Establecer controles para minimizar los riesgos significativos y de alto impacto para el negocio, como el robo o fuga de información, accesos no autorizados, mal uso y/o cualquier otro daño que afecte la divulgación indebida de la información confidencial, la alteración o modificación de esta, y en general la continuidad de las operaciones y la reputación de la compañía.
- Desarrollar y mantener una cultura en Seguridad de la Información orientada a la identificación y análisis de riesgos.

3.6 ANÁLISIS DIFERENCIAL

Se procedió a realizar una revisión general del estado de la seguridad de la información en la empresa PISIS S.A. Como punto de referencia para hacer este análisis, se centró en dos grandes áreas, a saber:

- Presencia y Profundidad de un Sistema de Gestión de seguridad de la Información
- La valoración de los controles de Seguridad existentes en la organización, basado en los requisitos de la norma ISO 27002

Adicionalmente, para la valoración de cada uno de los controles se tomó como referencia el modelo de madurez CMMI (Capability Maturity Model Integration), el cual es utilizado para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software, de la siguiente manera:

Valor	Efectividad	Significado	Descripción
L0	0%	Inexistente	La organización no tiene una implementación efectiva de los procesos, no existe
L1	10%	Inicial	Estado inicial donde el éxito de las actividades de los procesos se basa en la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o focalizados en áreas concretas
L2	50%	Manejado	La organización gestiona los procesos y los productos resultantes se establecen, controlan y mantienen.
L3	90%	Definido	La organización utiliza procesos basados en estándares, son documentados, divulgados y comunicados

L4	95%	Manejado Cuantitativamente	La organización gestiona de forma cuantitativa los procesos. Pueden ser seguidos con indicadores numéricos o estadísticos
L5	100%	Optimizado	Los procesos se encuentran en estado de mejora continua. Están alineados con los objetivos de negocio

Tabla 1 - Niveles de Madurez CMM

Al realizar la evaluación de los controles, se obtienen los siguientes resultados:

Dominios de la Norma

Valor	Significado	No de Controles	Porcentaje
L0	Inexistente	9	36,0%
L1	Inicial	3	12,0%
L2	Manejado	12	52,0%
L3	Definido	0	0,0%
L4	Manejado Cuantitativamente	0	0,0%
L5	Optimizado	0	0,0%

Tabla 2 - Análisis Dominio PISIS

De lo anterior se puede observar que hay 9 controles definidos dentro de los dominios que no están definidos, los cuales en su mayoría pertenecen al contexto organizacional, ya que no hay implementada una política del SGSI en la organización, por lo cual no se tiene establecidos sus límites y alcance, adicionalmente no se tiene un alto compromiso de la dirección y las partes interesadas en la gestión de la Seguridad de la información.

A continuación, se describe el nivel de madurez actual ponderado para los dominios de gestión de la norma para PISIS S.A

Dominio	Porcentaje	Calificación
Contexto de la organización	0,10	Inicial
Liderazgo	0,03	Inicial
Planificación	1,5	Inicial
Soporte	1,75	Inicial
Operación	1,65	Inicial
Evaluación del Desempeño	2,5	Manejado
Mejora	1,25	Inicial
Promedio	**1,25**	**INICIAL**

Tabla 3 - Nivel de Madurez Dominios PISIS

La situación actual refleja que la gestión de la norma está en una fase INICIAL, aunque hay dos dominios, como se mencionó anteriormente, están en fases prácticamente inexistentes. La siguiente figura describe gráficamente los niveles de madurez.

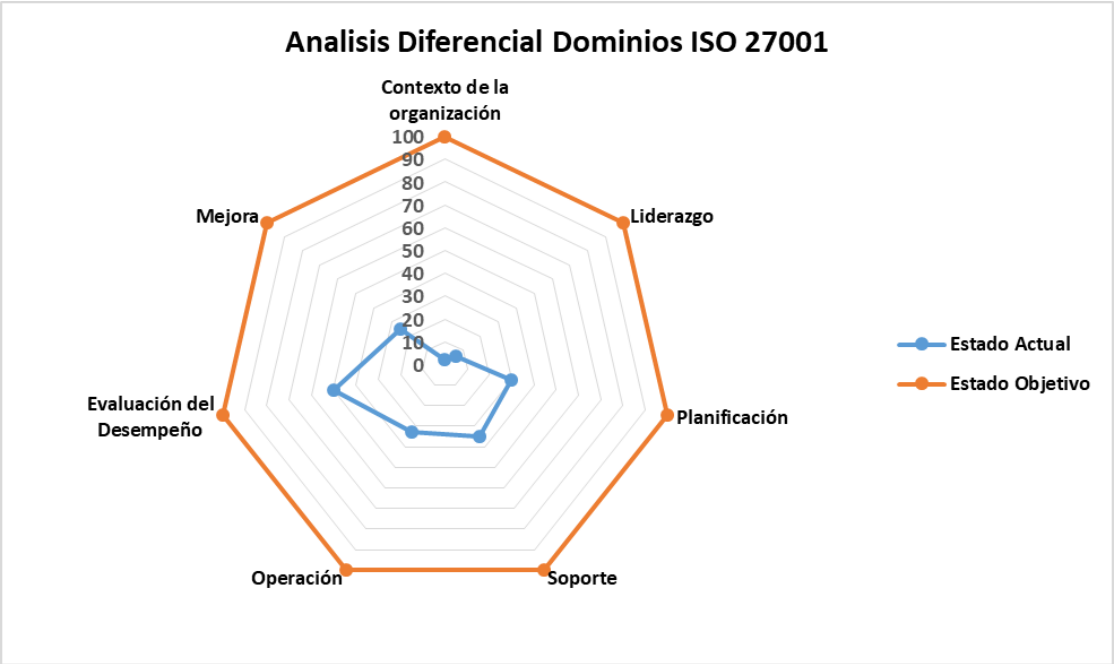

Ilustración 5 - Análisis Diferencial Dominios PISIS

Controles del Anexo A

Valor	Significado	No de Controles	Porcentaje
L0	Inexistente	12	10,5%
L1	Inicial	6	5,3%
L2	Manejado	28	24,6%
L3	Definido	54	47,4%
L4	Manejado Cuantitativamente	5	4,4%
L5	Optimizado	9	7,9%

Tabla 4 - Análisis Controles Anexo A PISIS

De lo anterior, se puede deducir que hay 63 controles que se encuentran aprobados y 51 que no lo están, de los cuales 12 no están implementados y el resto lo están, pero en un grado menor de madurez.

A continuación, se describe el nivel de madurez actual ponderado para los controles definidos en el Anexo A de la norma para PISIS S.A

Controles	Porcentaje	Calificación
Políticas de seguridad de la información	0,25	Inicial
Organización de la seguridad de la información	2,71	Manejado
Seguridad de los recursos humanos	4	Definido
Gestión de Activos	3,7	Manejado
Controles de acceso	4,11	Definido
Criptografía – Cifrado y gestión de claves	0,25	Inicial

Seguridad física y ambiental	3,58	Manejado
Seguridad operacional	3,85	Manejado
Seguridad de las comunicaciones	3,07	Manejado
Adquisición, desarrollo y mantenimiento del sistema	3,17	Manejado
Gestión de Proveedores	1,9	Inicial
Gestión de incidentes de seguridad de la información	3,93	Manejado
Gestión de la Continuidad de Negocio	1,12	Inicial
Cumplimiento	2,75	Manejado
Promedio	**2,74**	**MANEJADO**

Tabla 5 - Nivel de Madurez Anexo A PISIS

La situación actual refleja que la gestión de la norma está en una fase MANEJADA, aunque hay cuatro dominios que están una fase inicial: Políticas de seguridad de la información, ya que las políticas como tal no están definidas, Criptografía y manejo de claves, ya que no se tiene implementada una política para la gestión de claves criptográficas, Gestión de Proveedores, ya que no existe una política de seguridad de la información relacionada con proveedores y Gestión de la continuidad de negocio, ya que se tiene un plan de contingencia tecnológico, pero este no está incluido dentro de la continuidad de la operación y no se tienen consideraciones sobre la seguridad de la información dentro del plan. La siguiente figura describe gráficamente los niveles de madurez.

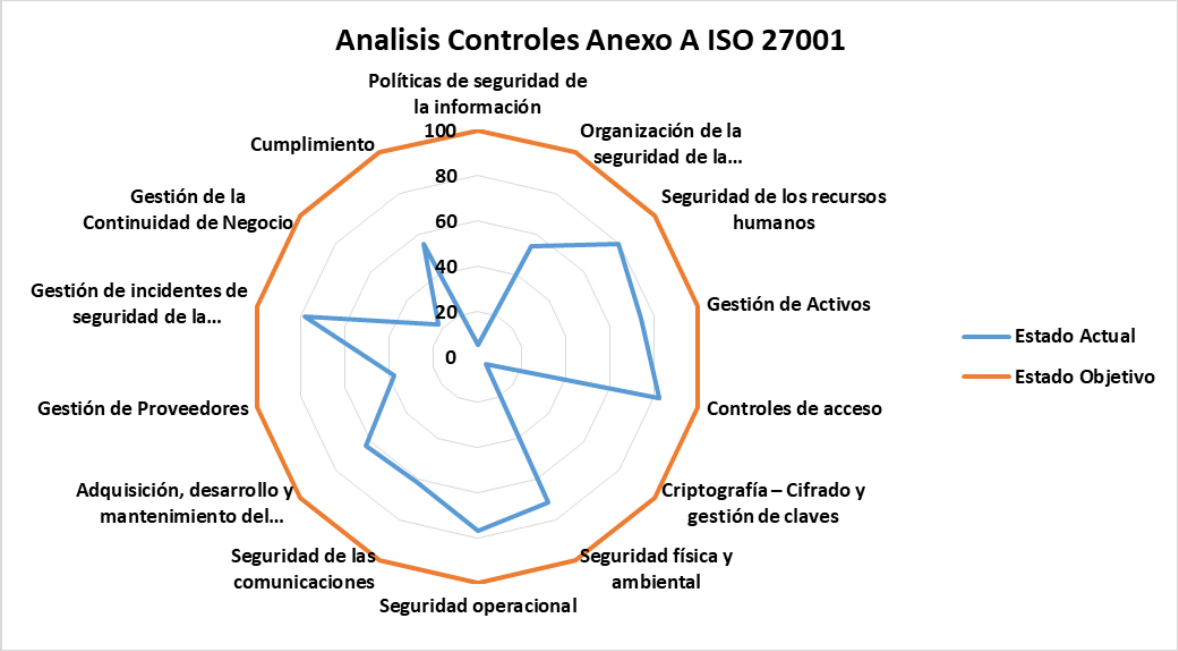

Ilustración 6 - Análisis Controles Anexo A PISIS

El detalle de la revisión se encuentra adjunta en documento "**Anexo 1 - Análisis Diferencial.pdf"**

4. SISTEMA DE GESTIÓN DOCUMENTAL

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que en el Sistema de Gestión de Seguridad de la Información se deben tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001.

Estos documentos básicos son los siguientes:

- Política de Seguridad de la Información.
- Procedimiento de auditorías Internas
- Gestión de Indicadores
- Gestión de Roles y Responsabilidades
- Procedimiento de Revisión por la dirección
- Metodología de Análisis de Riesgos
- Declaración de Aplicabilidad

4.1 ESQUEMA DOCUMENTAL

4.1.1 Política de Seguridad de la Información

La política de seguridad constituye la normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información. El contenido de la Política debe cubrir aspectos relativos al acceso de la información, uso de recursos de la Organización, comportamiento en caso de incidentes de seguridad, respaldos de información, uso de dispositivos móviles, transferencia segura de información, desarrollos de software seguros, relaciones con proveedores y/o terceros, etc.

El detalle de la política de seguridad se encuentra adjunta en documento "**Anexo 2 - Política de Seguridad de la Información.pdf"**

4.1.2 Procedimiento de Auditorías Internas

Se trata del documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia del Sistema de Gestión de Seguridad de la Información. Adicionalmente incluye los requisitos que deben tener los auditores internos. Finalmente, este procedimiento incluye algunas recomendaciones que se deben tener en cuenta en caso de la realización de auditorías por parte de terceros (Ya sea la auditoría Interna externalizada o Certificación de la norma).

Finalmente, también se incluye un programa de auditorías internas, en el cual se indican cuáles son los controles que van a ser evaluados de forma periódica con el objetivo de verificar el alcance de una potencial certificación de la entidad en la norma.

El detalle del procedimiento de Auditorías se encuentra adjunto en los documentos "**Anexo 3 - Procedimiento de Auditorías Internas y Externas.pdf", "Anexo 3.1 - Diagrama Procedimiento de Auditorías Internas y Externas.pdf" y "Anexo 12 - Programa de Auditorías Internas.xlsx"**

4.1.3 Gestión de Indicadores

Para medir el sistema se tendrá en cuenta el cumplimiento de los indicadores del SGSI y el cumplimiento de las metas asociadas a los indicadores de seguridad de la información:

a. Nombre del Indicador: Eficacia del SGSI

Objetivo: Evaluar el desempeño y la eficacia de la seguridad de la información.
Formula = Promedio cumplimiento de los Indicadores del SGSI.
Periodicidad: Trimestral
Valor Objetivo: 80%
Valor Umbral: 70%

b. Nombre del indicador: Mejoramiento Continuo

Objetivo: Promover el mejoramiento continuo en la gestión de los procesos mediante la ejecución de actividades orientadas al fortalecimiento del SGSI.
Formula = Actividades ejecutadas con la mejora continua del SGSI / Actividades relacionadas con la mejora continua del SGSI.
Periodicidad: Trimestral
Valor Objetivo: 70%
Valor Umbral: 65%

c. Nombre del indicador: Talento Humano Competente

Objetivo: Fortalecer las competencias necesarias en el talento humano de Simple que permita soportar el SGSI.
Formula = Cantidad de capacitaciones programadas / Capacitaciones ejecutadas.
Periodicidad: Trimestral
Valor Objetivo: 20%
Valor Umbral: 15%

d. Nombre del Indicador: Gestión del Riesgos

Objetivo: Minimizar la materialización de incidentes de seguridad de la información, con la implementación de acciones derivadas de la medición.
Formula = Riesgos materializados en seguridad de la información / Total de riesgos de seguridad de la información.
Periodicidad: Trimestral
Valor Objetivo: 100%
Valor Umbral: 90%

e. Nombre del Indicador: Confidencialidad, Integridad y Disponibilidad

Objetivo: Evaluar el desempeño que se tienen en los pilares de seguridad de la información (Confidencialidad e integridad de la información).
Formula: Incidentes relacionados con pérdida de Confidencialidad e integridad de la información/ Total de incidentes de Seguridad de la información.

Periodicidad: Trimestral
Valor Objetivo: 100%
Valor Umbral: 90%

f. Nombre del Indicador: Numero de dispositivos infectados

Objetivo: Detectar el número de Malware detectados y bloqueados.
Formula: Total Numero de equipos infectados / total equipos infectados en el mes anterior.
Periodicidad: Mensual
Valor Objetivo: 85%
Valor Umbral: 80%

g. Nombre del Indicador: Gestión de Seguridad de las Redes

Objetivo: Monitorear y gestionar el número de intentos de infiltración o ingresos a la red.
Formula: Número de intentos de ingresos reportados en el Mes / Número de intentos de ingresos reportados en el Mes Anterior.
Periodicidad: Mensual
Valor Objetivo: 30%
Valor Umbral: 25%

h. Nombre del Indicador: Usuarios Mal Perfilados

Objetivo: Controlar y verificar la adecuada segregación de roles y permisos a los funcionarios.
Formula: Número de Usuarios Mal Perfilados /Total de aplicativos vigentes al Mes.
Periodicidad: Bimestral
Valor Objetivo: 90%
Valor Umbral: 85%

En resumen, el procedimiento define los indicadores aplicables al Sistema de Gestión de Seguridad de la Información. El detalle de los indicadores se encuentra adjunto en el documento "**Anexo 4 - Gestión de Indicadores.xlsx**"

4.1.4 Gestión de Roles y Responsabilidades

El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de la alta dirección.

Adicionalmente, se definen los principales roles y responsabilidades para los funcionarios de la compañía, la alta dirección, el representante del sistema, los auditores internos, el Jefe de Riesgos y los dueños del proceso.

El detalle del documento donde se encuentran los roles y responsabilidades de los funcionarios se encuentra adjunta en documento "**Anexo 5 - Gestión de Roles y Responsabilidades.pdf"**

4.1.5 Procedimiento de Revisión por la Dirección

La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación con el Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001:2013 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones.

La revisión por dirección es uno de los aspectos que contempla la normativa para la revisión anualmente de los aspectos más importantes que se han presentado con relación al SGSI implantado, revisando los elementos de entrada y salida de la revisión que establece la norma. De esta manera la dirección puede verificar y/o monitorear el sistema y establecer compromisos para realizar las mejoras necesarias.

El detalle del procedimiento de la Revisión por la Dirección se encuentra adjunta en documento "**Anexo 6 - Revisión por la Dirección.pdf"**

4.1.6 Metodología de Análisis de Riesgos

Establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.

La metodología para la gestión de riesgos a utilizar por la compañía es la ISO/IEC 31000 la cual contiene los siguientes componentes:

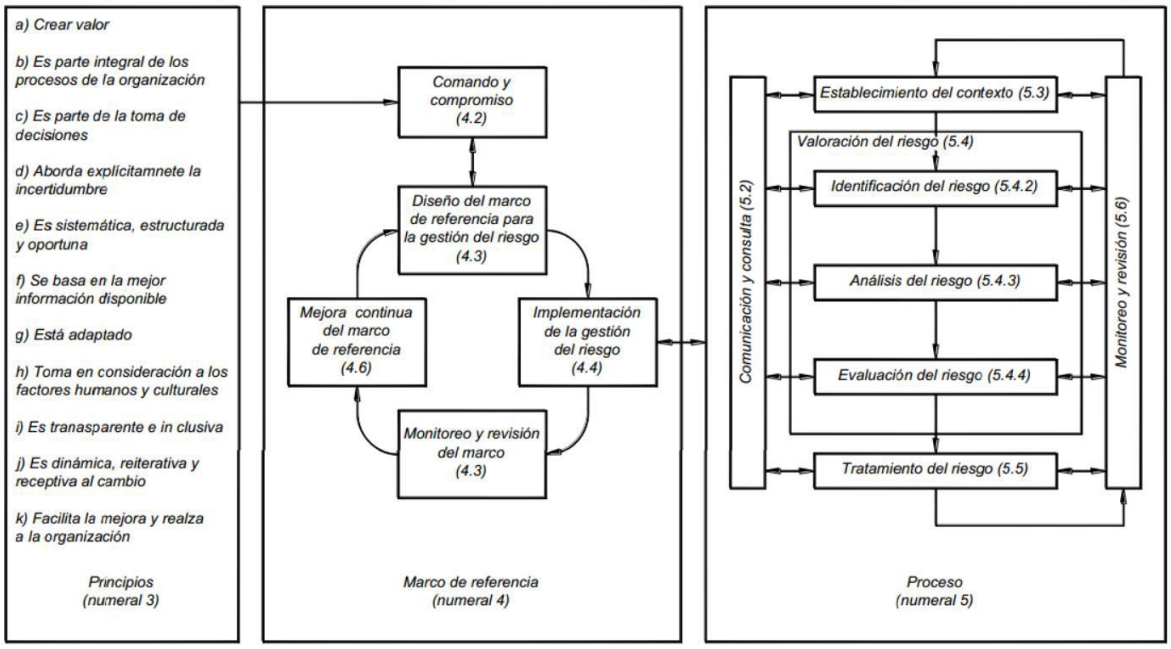

Ilustración 7 - Norma técnica de gestión de riesgo ISO 31000

Esta norma proporciona las directrices necesarias para una adecuada gestión de gestión del riesgo y puede ser aplicada a cualquier tipo de organización (independiente de su naturaleza jurídica), para nuestro caso particular, se hará una aplicabilidad sobre el alcance definido para la compañía.

La norma ISO 31000 derivada de la AS/NZS 4360:2004, se constituye como una metodología imprescindible para la gestión del riesgo empresarial, y es aplicable a cualquier industria independiente de su objeto social.

El detalle de la metodología se encuentra en el Manual del Sistema de Administración de Riesgo Operativo, el cual incluye los riesgos relacionados con la seguridad de la información. El manual se encuentra adjunto en el documento "**Anexo 7 - Manual del Sistema de Administración de Riesgo Operativo.pdf**"

4.1.7 Declaración de Aplicabilidad

Es el documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada.

La declaración incluye la tabla correspondiente al Documento de Aplicabilidad del Sistema de Gestión de Seguridad de la Información, incluyendo los controles aplicables y no aplicables, Procesos, Controles o documentos relacionados y el estado actual según el análisis diferencial realizado en la Fase 1.

La Declaración de Aplicabilidad se encuentra adjunta en documento "**Anexo 8 - Declaración de Aplicabilidad.pdf"**

5. ANÁLISIS DE RIESGOS

5.1 INTRODUCCIÓN

El análisis de riesgos es la parte más importante del ciclo de vida de la gestión de la seguridad de la información, ya que esta servirá para descubrir que carencias de seguridad tiene la empresa tras detectar cuales son las vulnerabilidades, así como las amenazas a las que está expuesta.

En esta fase en primer lugar se identifican los activos de la empresa relacionados con la seguridad de la información cuyo objetivo del SGSI es protegerlos y se calcula su valor. Después, se identifican las amenazas que pueden afectar a los activos de la empresa y las vulnerabilidades que hacen que estas amenazas deriven en un incidente de seguridad.

Una vez obtenida la información anterior, se procede a estudiar la gestión del riesgo determinando el impacto potencial que tendría la materialización de las amenazas encontradas sobre los activos identificados y se calculará el nivel de riesgo aceptable y el riesgo residual.

5.2 INVENTARIO DE ACTIVOS DE INFORMACIÓN

Un activo se define como como un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos

En este apartado se muestra un inventario de los activos relacionados con la seguridad de la información de PISIS, clasificados acorde a la metodología de Administración de Riesgos definida en el numeral 4.1.6. de este documento.

El detalle de los activos identificados se encuentra en el documento anexo "**Anexo 9 - Análisis de Riesgos.xlsx**" – Hoja "**Inv. Activos de Información**".

5.3 VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Una vez que han sido identificados los activos relacionados con la seguridad de la información, se les asigna un valor. Esta valoración se basará acorde a la metodología de Administración de Riesgos definida en el numeral 4.1.6. de este documento:

Atributos de clasificación de los activos de información				
CLASIFICACIÓN		CONFIDENCIALIDAD- EFICIENCIA	DISPONIBILIDAD- EFECTIVIDAD	INTEGRIDAD- CONFIABILIDAD
5	Critico	El activo de información contiene y/o maneja información **100% Confidencial y con las mejores practicas y recursos posibles,** por lo que su conocimiento o divulgación no autorizada impactaría negativamente al proceso y generaría ineficiencia operativa.	El activo de información **no puede estar/ser indisponible , inoportuno, incorrecto e inconsistente por más de 5 minutos en el día,** porque sino impactaría negativamente al proceso o a la organización.	El activo de información se debe contener y/o manejar en un **100% de exactitud e integridad; y ser apropiado para el desarrollo de la actividad del Operador de Información de la PILA** porque sino impactaría negativamente a su proceso relacionado o a la organización.
4	Alto	El activo de información contiene y/o maneja información **90% confidencial y con las mejores practicas y recursos posibles** , por lo que su conocimiento o divulgación no autorizada impactaría negativamente al proceso y generaría ineficiencia operativa.	El activo de información **no puede estar/ser indisponible, inoportuno, incorrecto e inconsistente por más de 52 minutos en el día** porque sino impactaría negativamente al proceso o a la organización.	El activo de información se debe contener y/o manejar en más de un **90% de exactitud; y ser apropiado para el desarrollo de la actividad del Operador de Información de la PILA e integridad** porque sino impactaría negativamente a su proceso relacionado o a la organización.
3	Medio	El activo de información contiene y/o maneja información entre un **67% y 90% confidencial y con las mejores practicas y recursos posible**s, por lo que su conocimiento o divulgación no autorizada impactaría negativamente al proceso y generaría ineficiencia operativa.	El activo de información **no puede estar/ser indisponible, inoportuno, incorrecto e inconsistente por más de 8 horas en el día** porque sino impactaría negativamente al proceso o a la organización.	El activo de información se debe contener y/o manejar entre un **67% - 90% de exactitud e integridad; y ser apropiado para el desarrollo de la actividad del Operador de Información de la PILA e integridad** porque sino impactaría negativamente a su proceso relacionado o a la organización.
2	Bajo	El activo de información contiene y/o maneja información enre un **34%- 66% confidencial y con las mejores practicas y recursos posibles** , por lo que su conocimiento o divulgación no autorizada no impactaría negativamente al proceso ni generaría ineficiencia operativa.	El activo de información **no puede estar/ser indisponible, inoportuno, incorrecto e inconsistente por más de 4 días seguidos** porque sino impactaría negativamente al proceso o a la organización.	El activo de información se debe contener y/o manejar entre un **34% - 66% de exactitud e integridad; y ser apropiado para el desarrollo de la actividad del Operador de Información de la PILA e integridad** porque sino impactaría negativamente a su proceso relacionado o a la organización.
1	Insignificante	El activo de información contiene y/o maneja información **con menos del 34% confidencial y con las mejores practicas y recursos posibles** , por lo que su conocimiento o divulgación no autorizada, no impactaría negativamente al proceso ni generaría ineficiencia operativa	El activo de información **no puede estar/ser indisponible , inoportuno, incorrecto e inconsistente por más de 36 días seguidos** porque sino impactaría negativamente al proceso o a la organización.	El activo de información se puede contener y/o manejar por debajo de en un **34% de exactitud e integridad; y ser apropiado para el desarrollo de la actividad del Operador de Información de la PILA e integridad** porque no impactaría negativamente a su proceso relacionado o a la organización.

Tabla 6 - Valoración de los activos de información según sus atributos de clasificación

5.4 DIMENSIONAMIENTO DE LOS ACTIVOS DE INFORMACIÓN

Desde el punto de vista de la seguridad, junto a la valoración en sí de los activos debe indicarse cuál es el aspecto de la seguridad más crítico. Esto será de ayuda en el momento de pensar en posibles salvaguardas, ya que estas se enfocarán en los aspectos que más nos interesen y por ello se realizan un dimensionamiento de la valoración.

Las dimensiones de valoración son las características que hacen valioso a un activo y dichas dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza.

Para obtener el dimensionamiento se realiza una valoración en la cual se tendrán en cuenta los siguientes seis elementos, definidos en la metodología de Administración de Riesgos, indicada en el numeral 4.1.6. de este documento:

- Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada.
- Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.
- Disponibilidad: La información debe estar en el momento y en la forma que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.
- Efectividad: La información debe ser pertinente y su entrega oportuna, correcta y consistente.
- Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.
- Confiabilidad: La información debe ser la apropiada para el desarrollo de la actividad del Operador de Información de la PILA.

Una vez que se tienen definidas las seis dimensiones de valoración, es necesario usar una escala clara y detallada. Para el dimensionamiento del valor de la seguridad de PISIS. se utiliza con base a la tabla descrita en el Apartado 4 del libro II de la metodología de riesgos MAGERIT, la cual se indica a continuación:

VALOR		CRITERIO
10	**Grave**	Daño Extremadamente Grave
9	**Muy Alto**	Daño Muy Alto
6 a 8	**Alto**	Daño Alto
3 a 5	**Medio**	Daño importante
1 a 2	**Bajo**	Daño menor
0	**Insignificante**	Irrelevante a términos prácticos

Tabla 7 - Valoración de los criterios de dimensiones de seguridad

A la hora de realizar las ponderaciones para cada activo se ha de tener presente la importancia o participación del activo en la cadena de valor del servicio, evitando situaciones del tipo “todo es

muy importante" y obligando así a los responsables de realizar dicha valoración a discernir entre lo que es realmente importante y lo que no lo es tanto.

La valoración respecto a las dimensiones de seguridad de los activos de información se encuentra en el documento anexo "**Anexo 9 - Análisis de Riesgos.xlsx**" – Hoja "**Valoración Activos Inf.**".

5.5 ANÁLISIS DE AMENAZAS

Los activos de una organización siempre están expuestos a amenazas que pueden afectar a aspectos de la seguridad. Por esta razón, en este apartado se va a realizar el análisis de amenazas que pueden afectar a PISIS. Además, se estimará la vulnerabilidad de cada activo ligado a las amenazas y la posibilidad de ocurrencia de estas.

Inicialmente, para realizar el análisis de amenazas se tomará la clasificación de estas definidas en la metodología MAGERIT, Libro 2 - Apartado 5. Estas se clasifican en los siguientes grupos:

- Desastres Naturales
- De origen Industrial
- Errores y fallos no intencionados
- Ataques Intencionados

El detalle de las amenazas identificadas se encuentra en el documento anexo "**Anexo 9 - Análisis de Riesgos.xlsx**" – Hoja "**Amenazas**".

Después de determinar las amenazas es necesario la elaboración del escenario de riesgos por lo que se colocaron las amenazas contra los activos y se identificó su relación respectiva, con ello se realizara el análisis de amenazas

AMENAZAS/ACTIVOS	Centro de procesamiento de Datos	Sala de departamento de Talento Humano	Sala del departamento de Mercadeo y Comercial	Sala del departamento Financiero y Administrativo	Sala del departamento de Servicio al Cliente	Sala del departamento de Operaciones	Sala del departamento de Control Interno, Riesgos y area jurídica	Sala de departamento de desarrollo de software	Sala de departamento de infraestructura Tecnológica	Sala de departamento de Proyectos	Despacho del Gerente General	Despacho del Gerente Financiero y Administrativo	Despacho del Gerente de Tecnología y Operaciones	Despacho del Gerente Comercial y de Mercadeo	Archivo Central	Recepción	Gerente General (1)	Gerente Financiero y Administrativo (1)	Profesional de Tesorería y Planeación	Profesional Administrativo (1)	Auxiliar Administrativo	Profesional
Fuego	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Daños por Agua	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Tormenta eléctrica	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Terremoto	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Fuego	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Daños por Agua	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Sobrecarga eléctrica	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Explosión	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Derrumbe	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Contaminación mecánica	x																						
Contaminación electromagnética	x																						
Avería de origen física o lógica	x																						
Corte eléctrico	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Condiciones inadecuadas de temperatura y/o humedad	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Fallo del servicio de comunicaciones	x																						
Interrupción de otros servicios y suministros esenciales	x																						
Degradación de los soportes de almacenamiento de la información	x																						
Emanaciones electromagnéticas																							
Errores de usuarios																							
Errores de los técnicos de TI	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x							
Errores de los administradores																							
Errores de monitorización (log)	x																						
Errores de configuración	x																						
Deficiencias en la organización	x																x	x	x	x	x	x	x
Difusión de software dañino																	x	x	x	x	x	x	x

Ilustración 8 – Escenario de Riesgos

El detalle del escenario de riesgos se encuentra en el documento anexo "**Anexo 9 - Análisis de Riesgos.xlsx**" – Hoja "**Escenario Riesgos**".

Para realizar el análisis se tomarán como base las dimensiones definidas en el numeral 5.4 de este documento, que corresponden a los seis elementos definidos en el numeral 10.3 de la metodología de administración de riesgos.

Y la valoración del impacto que la ocurrencia de una amenaza producirá en las dimensiones de seguridad se basará en la siguiente tabla, la cual se encuentra en el numeral 10.5 del Manual del Sistema de Administración de Riesgo Operativo, definido en el numeral 4.1.6 de este documento.

IMPACTO CUALITATIVO Y CUANTITATIVO			
NIVEL	**RANGO**	**DESCRIPCIÓN**	**NIVEL DE AFECTACIÓN**
5	Grave	Pérdida total de la confidencialidad- eficiencia, integridad-confiabilidad y disponibilidad-efectividad de la información; afectando gravemente a los elementos del negocio, las tecnologías, estrategias y niveles financieros de la organización; debido a situaciones de divulgación, alteración, perdida, daño o robo de la información; incumplimiento de los requisitos legales o normativos; ineficacia de la productividad organizacional e inadecuado funcionamiento de los sistemas de operación.	80% a 100%
4	Alto	Pérdida considerable de la confidencialidad- eficiencia, integridad- confiabilidad y disponibilidad-efectividad de la información; afectando de manera importante a los elementos del negocio, las tecnologías, estrategias y niveles financieros de la organización; debido a situaciones de divulgación, alteración, perdida, daño o robo dela información; incumplimiento de requisitos legales o normativos; ineficacia de la productividad organizacional e inadecuado funcionamiento de los sistemas de la operación.	60% a 80%
3	Medio	Pérdida moderada de la confidencialidad- eficiencia, integridad- confiabilidad y disponibilidad-efectividad de la información; afectando medianamente a los elementos del negocio, las tecnologías, estrategias y niveles financieros de la organización; debido a situaciones de divulgación, alteración, perdida, daño o robo de la información; incumplimiento de requisitos legales o normativos; ineficacia de la productividad organizacional e inadecuado funcionamiento de los sistemas de la operación.	40% a 60%

2	Mínimo	Pérdida leve de la confidencialidad- eficiencia, integridad-confiabilidad y disponibilidad-efectividad de la información; afectando mínimamente a los elementos del negocio, las tecnologías, estrategias y niveles financieros de la organización; debido a situaciones de divulgación, alteración, perdida, daño o robo de la información; incumplimiento de requisitos legales o normativos; ineficacia de la productividad organizacional e inadecuado funcionamiento de los sistemas de la operación.	20% a 40%
1	Insignificante	Pérdida trivial de la confidencialidad- eficiencia, integridad- confiabilidad y disponibilidad-efectividad de la información; afectando insignificantemente a los elementos del negocio, las tecnologías, estrategias y niveles financieros de la organización; debido a situaciones de divulgación, alteración, perdida, daño o robo de la información; incumplimiento de requisitos legales o normativos; ineficacia de la productividad organizacional e inadecuado funcionamiento de los sistemas de la operación.	0 a 20%

Tabla 8 - Impacto de Seguridad de la Información.

Después de sacar los escenarios se realiza una tabla de activos y dimensiones de seguridad, en la cual se analizará la frecuencia con que puede producirse la amenaza, como su impacto en las distintas dimensiones de la seguridad del activo.

El detalle del análisis de amenazas se encuentra en el documento anexo "**Anexo 9 - Análisis de Riesgos.xlsx**" – Hoja "**Análisis Amenazas**".

Adicionalmente, luego del cruce de escenarios, éstos se llevan al listado de riesgos acorde a la afectación de las amenazas sobre los activos y sobre este listado, se va a generar los posibles agentes generadores de esos riesgos, esto es, entes externos al sistema con potencial daño, así como las posibles causas o vulnerabilidades que puedan estar en los activos. Eso nos permitirá en los planes de tratamiento, conocer como poder reducir la probabilidad y/o el impacto.

El detalle de los agentes generadores de riesgos se encuentra en el documento anexo "**Anexo 9 - Análisis de Riesgos.xlsx**" – Hoja "**Agentes**".

5.6 IMPACTO POTENCIAL

Una vez realizado el análisis de amenazas podemos determinar el impacto potencial que puede suponer para la empresa la materialización de las amenazas. Se trata de un dato relevante, ya que permitirá priorizar el plan de acción, y a su vez, evaluar cómo se ve modificado dicho valor una vez se apliquen contramedidas.

Para esto calcularemos el riesgo actual. La determinación del riesgo para una amenaza/vulnerabilidad en particular se expresa en función de la probabilidad por el impacto de este.

Para la determinación de los valores de probabilidad se utilizará como referencia los términos utilizados en el numeral 9.4.2 del Manual del Sistema de Administración de Riesgo Operativo, definido en numeral 4.1.6 de este documento.

NIVEL	RANGO	DESCRIPCIÓN	FRECUENCIA
5	Casi seguro	El evento ocurrirá muy seguramente en la mayoría de las circunstancias	Al menos una vez en el día
4	Altamente Probable	El evento ocurrirá muy probablemente en la mayoría de las circunstancias	Al menos una vez a la semana
3	Probable	El evento ocurrirá probablemente en algún momento	Al menos una vez en el mes
2	Improbable	El evento podría ocurrir improbablemente	Al menos una vez en el año
1	Raro	El evento podría ocurrir solo bajo circunstancias excepcionales	Al menos una vez en 15 años

Tabla 9 - Probabilidad

Los valores del impacto serán los definidos en el Análisis de Amenazas, correspondientes al impacto Cualitativo y Cuantitativo en los niveles establecidos, correspondientes a las frecuencias definidas porcentualmente, las cuales se definen en el numeral 10.5 del Manual del Sistema de Administración de Riesgo Operativo.

Para la valoración es necesario tener en cuenta qué controles se tienen al respecto (controles actuales) los cuales fueron obtenidos en el paso anterior, dado que estos pueden influenciar positivamente en los niveles de riesgos finales.

El detalle del riesgo actual o impacto potencial se encuentra en el documento anexo "**Anexo 9 - Análisis de Riesgos.xlsx**" – Hoja "**Impacto Potencial**".

Para la aceptabilidad el riesgo, se ha considerado dejar el estándar propuesto en el numeral 9.4.3 del Manual del Sistema de Administración de Riesgo Operativo, indicado en el numeral 4.1.6 de este documento.

ESCALAS		DESCRIPCIÓN	PRIORIDAD DEL TRATAMIENTO	CRITERIOS DE ACEPTACIÓN
17 a 25	CRITICO	La mayoría de los objetivos o procesos no serán alcanzados o no se llevarán a cabo	P1	Nivel de riesgo no aceptable, se debe evitar (probabilidad, impacto o ambos). Probar la eficacia de los controles cada 3 meses (evaluación

				independiente), evaluación de autocontrol al menos una vez cada 6 meses.
11 a 16	IMPORTANTE	Algunos objetivos o procesos importantes no serán alcanzados o no se llevarán a cabo	P2	Nivel de riesgo no aceptable, se debe transferir (probabilidad, impacto o ambos). Probar la eficacia de los controles cada 3 meses (evaluación independiente), evaluación de autocontrol al menos una vez cada 6 meses
7 a 10	MODERADO	Algunos objetivos o procesos serán afectados	P3	Nivel de riesgo no aceptable, se debe reducir el riesgo, tomar medidas adicionales de tratamiento. Probar la eficacia de los controles cada 6 meses (evaluación independiente), evaluación de autocontrol al menos una vez al año
4 a 6	MINIMO	Impacto mínimo sobre los objetivos o procesos de la compañía	P4	Nivel de riesgo aceptable sin necesidad de tomar otras medidas de control diferentes a las que se poseen siempre y cuando los controles estén bien diseñados y aplicados.

1 a 3	INSIGNIFICANTE	Impacto insignificante sobre los objetivos o procesos de la compañía	P5	Probar la eficacia de los controles al menos 1 vez al año (evaluación independiente), evaluación de autocontrol al menos una vez cada 18 meses por parte de los responsables de los procesos (criterio de autocontrol según C.E 038 de 2009 de la SFC)

Tabla 10 - Aceptabilidad del Riesgo

El Mapa de riesgo para la organización quedaría de la siguiente forma:

ACEPTABILIDAD DEL RIESGO							
PROBABILIDAD	Casi Seguro	5	Impresora de red planta 1 Oficina central/Avería de origen		Centro de procesamiento de Datos/Errores de los técnicos de TI		
	Altamente Probable	4	Gerente General (1)/Acceso no autorizado		Centro de procesamiento de Datos/Avería de origen física o lógica		
	Probable	3	Gerente General (1)/Difusión de software dañino	Sala de departamento de Talento Humano/Indisponibilidad del personal	Centro de procesamiento de Datos/Fuego Centro de procesamiento de Datos/Tormenta		
	Improbable	2	Gerente General (1)/Pérdida de equipos	Sala de departamento de Talento Humano/Fuego	Centro de procesamiento de Datos/Contaminación mecánica	Sala de departamento de Talento Humano/Corte eléctrico	PC's tipo A (47 dispositivos)/Robo PC's tipo B (21 dispositivos)/Robo
	Raro	1	Impresora de red planta 1 Oficina central/Fuego	Sala de departamento de Talento Humano/Daños por Agua	Centro de procesamiento de Datos/Daños por Agua		
	VALORACIÓN		1	2	3	4	5
			Insignificante	Minimo	Medio	Alto	Grave
			IMPACTO				

Ilustración 9 – Mapa de Riesgos

5.7 NIVELES DE ACEPTACION DE RIESGO INHERENTE Y RESIDUAL

Los criterios de aceptación de riesgo demandados por la organización, establece que los riesgos de niveles “Critico” y “Importante” se consideran inaceptables y deben ser tratados de forma inmediata con los recursos necesarios que se requieran. Así mismo para los niveles “Moderado” y “Mínimo” su tratamiento depende del aporte del control para mitigar riesgos, la relación costo/beneficio y la contribución que este aporte al cumplimiento de los objetivos del negocio.

Para el tratamiento de los riesgos se tendrá en cuenta los siguientes mecanismos:

5.7.1 Reducir la Probabilidad

Se deben buscar mecanismos que ayuden a reducir la probabilidad de ocurrencia, puede ser a través de auditorías preventivas, formación y sensibilización, mantenimientos preventivos, contratos, pruebas de seguridad (intrusión), etc. Así mismo, está la implementación de controles detectivos, correctivos y disuasivos.

5.7.2 Reducir el Impacto

Para la reducción del impacto es posible desarrollar planes de contingencia y continuidad del negocio, control de fraudes, controles técnicos y administrativos, etc. Así mismo, está la implementación de controles detectivos, correctivos y disuasivos.

5.7.3 Transferir Total o Parcialmente

Para la transferencia del riesgo podemos recurrir a pólizas y seguros, acuerdos de confidencialidad, transferencia física a otros lugares (división del riesgo), etc.

5.7.4 Evitar

Es la decisión tomada de no iniciar o continuar con la actividad que lo origino.

5.7.5 Asumir

Para este tipo de tratamiento estaríamos considerando el **riesgo residual**, que, luego de realizar las diferentes acciones debemos retenerlo o aceptarlo. Aplicaría en primera instancia los riesgos bajos y moderados.

De acuerdo con la evaluación del impacto potencial se obtuvieron los siguientes resultados:

DISTRIBUCIÓN PORCENTUAL		
ZONA	%	Total riesgos
Insignificante	25,30%	1087
Mínimo	32,32%	1389
Moderado	14,45%	621
Importante	30,77%	1322
Critico	0,00%	0

Tabla 11 - Resultados Impacto Potencial

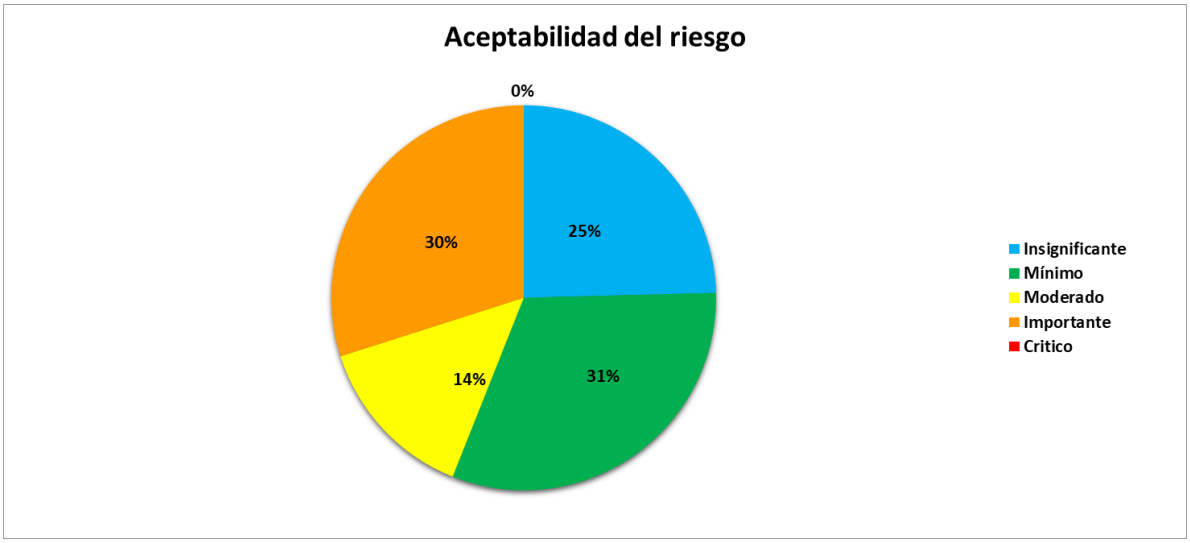

Ilustración 10 – Aceptabilidad del Riesgo

Teniendo en cuenta lo anterior, no se identificaron riesgos críticos, pero si un gran porcentaje correspondiente a riesgos importantes. Entre los riesgos que requieren tratamiento, destacamos los siguientes:

- Inconvenientes en el centro de datos por catástrofes naturales
- Inconvenientes en el Centro de datos por falta de mantenimiento preventivo/Correctivo
- Debilidades en el acceso al Centro de datos
- Problemas de fuego en el gabinete de Almacenamiento
- Averías y/o daños en el gabinete de datos
- Fuga de Información de los Servidores de la Organización
- Errores en el soporte y/o mantenimiento de los servidores
- Ataques informáticos a los servidores
- Acceso no autorizado a los servidores de la organización
- Alteraciones en la información de los servidores
- Errores de administración en el software de la compañía
- Vulnerabilidades en los programas (software)
- Análisis de tráfico y ataques al software de la compañía
- Suplantación de los usuarios del software
- Robo a la información de los programas
- Alteración de la información generada por los sistemas de información
- Uso no adecuado del software instalado

Luego de seleccionar las medidas de tratamiento, es necesario preparar e implementar los planes para el tratamiento de dichos riesgos. Así mismo, es necesaria la creación de proyectos de implementación asociados a los planes de tratamiento, donde estén considerados los diferentes controles a implementar. Dichos planes deberían estar integrados con los planes de gestión de la organización (así no quedarían desarticulados).

El detalle de las medidas de tratamiento tomadas se encuentra en el documento anexo "**Anexo 9 - Análisis de Riesgos.xlsx**" – Hoja "**Tratamiento**".

Con ello, se procederá a realizar nuevamente el cálculo del impacto potencial de los riesgos involucrados, lo cual permitirá la definición del riesgo residual para cada uno de los riesgos identificados.

6. PROPUESTA DE PROYECTOS

6.1 PLAN DE MEJORAS

Tras haber realizado el análisis de riesgo de la organización, se conoce el nivel de riesgo actual en la empresa, por lo cual se está en disposición de plantear proyectos de medidas correctivas que mitiguen estos riesgos y mejoren el estado de la seguridad de la empresa.

Las amenazas que afectan a los activos de información con niveles de riesgos críticos e importantes son los siguientes:

- Catástrofes naturales
- Falta de mantenimiento preventivo/correctivo

- Debilidades en el acceso a la infraestructura de la compañía y el centro de datos
- Fuga de Información
- Ataques informáticos
- Accesos no autorizados a la información
- Errores en el soporte y la administración de los sistemas
- Suplantación
- Robo de Información
- Uso no adecuado del software y las herramientas
- Fallas en los servicios de comunicaciones
- Vulnerabilidades en los sistemas de información
- Suplantación de usuarios

Teniendo en cuenta lo anterior, más los resultados del análisis diferencial realizado en el punto No 1 de este documento, se desarrollarán los siguientes planes de acción y/o proyectos que buscan minimizar cada una de las amenazas identificadas.

- Implementación de las políticas de seguridad de la información
- Implementación del área de seguridad de la información
- Implementación del Comité de seguridad de la Información
- Cifrado de la Información de PISIS
- Política de Gestión de Proveedores
- Fortalecimiento en la identificación y gestión de vulnerabilidades del software
- Plan de Mejora de la Seguridad en el Centro de datos
- Plan de Continuidad del Negocio
- Formación al Personal de PISIS en temas relacionados con seguridad de la información

El detalle de cada uno de los proyectos se encuentra en el archivo adjunto "**Anexo 10 - Proyectos SGSI PISIS**.xlsx"

6.2 PLANFIFICACIÓN PLAN DE MEJORAS

Tras haber realizado el análisis de riesgo de la organización, se conoce el nivel de riesgo actual en la empresa, por lo cual se está en disposición de plantear proyectos de medidas correctivas que mitiguen estos riesgos y mejoren el estado de la seguridad de la empresa. Estas medidas se pueden encontrar en el siguiente diagrama de Gantt. A cada proyecto se realizó la asignación de uno o más recursos encargados de desplegar los proyectos de mejora parta disminuir el riesgo de los activos de información a los cuales se encuentra expuesta la organización. La identificación de los responsables es la siguiente:

- OFS – Oficial de seguridad de la Información
- GG – Gerente General
- AD – Junta Directiva
- DH – Director de Talento Humano
- AS – Analista de Seguridad de la Información
- JIT – Jefe de Infraestructura Tecnológica
- GOT – Gerente de Operaciones y Tecnología
- GAF – Gerente Administrativo y Financiero

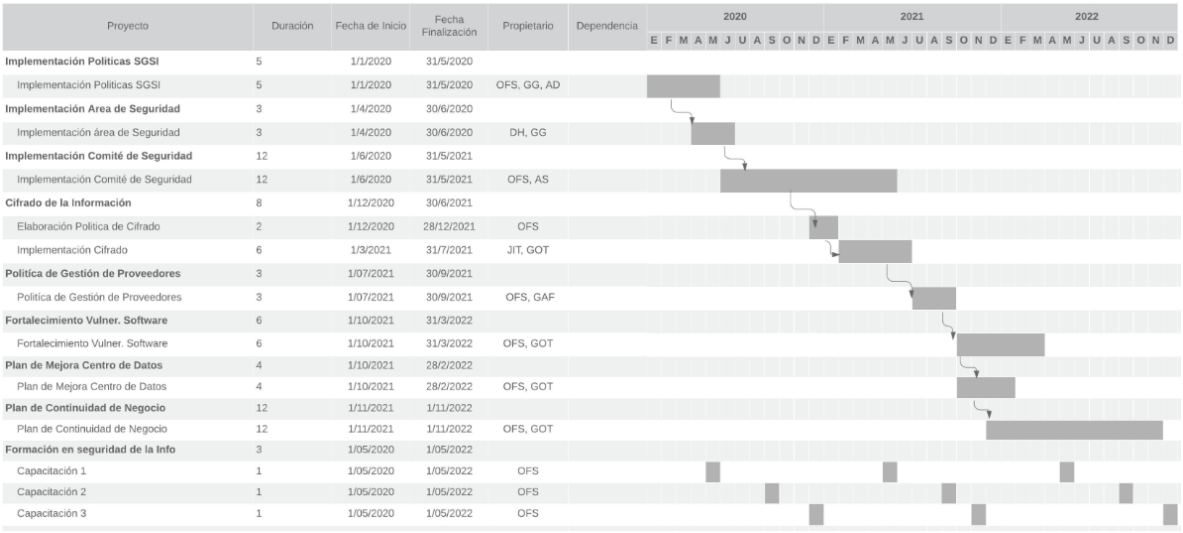

Ilustración 11 – Diagrama de Gantt de los Proyectos

6.3 ANALISIS DIFERENCIAL DESEABLE TRAS LA IMPLEMENTACIÓN

Los proyectos propuestos en esta fase del Plan Director de Seguridad tienen como objetivo la reducción del nivel de riesgo detectado. Para ello, en este apartado se va a realizar un análisis diferencial en los dominios de la ISO/IEC 27002:2013 teniendo en cuenta los proyectos presentados y será comparado con el realizado al inicio de este Plan Director donde se refleja la situación actual. Esta comparación ofrecerá un modelo predictivo de la mejora de la seguridad de la información de PISIS y la consecuente reducción del nivel de riesgo con la implantación de los mencionados proyectos.

Los resultados esperados se pueden observar en las tablas 12 y la ilustración 11 que se presentan a continuación:

Controles	Porcentaje Inicial	Calificación Inicial	Porcentaje Esperado	Calificación Esperada
Políticas de seguridad de la información	0,25	Inicial	**4,25**	Manejado
Organización de la seguridad de la información	2,71	Manejado	**4,25**	Manejado
Seguridad de los recursos humanos	4	Definido	**4,25**	Manejado
Gestión de Activos	3,7	Manejado	**4,00**	Manejado
Controles de acceso	4,11	Definido	**4,25**	Manejado
Criptografía – Cifrado y gestión de claves	0,25	Inicial	**4,00**	Manejado
Seguridad física y ambiental	3,58	Manejado	**4,00**	Manejado
Seguridad operacional	3,85	Manejado	**4,00**	Manejado
Seguridad de las comunicaciones	3,07	Manejado	**4,00**	Manejado
Adquisición, desarrollo y mantenimiento del sistema	3,17	Manejado	**4,00**	Manejado
Gestión de Proveedores	1,9	Inicial	**4,00**	Manejado

Gestión de incidentes de seguridad de la información	3,93	Manejado	**4,25**	Manejado
Gestión de la Continuidad de Negocio	1,12	Inicial	**4,00**	Manejado
Cumplimiento	2,75	Manejado	**4,00**	Manejado
Promedio	**2,74**	**MANEJADO**	**4,09**	**MANEJADO**

Tabla 12 – Nivel de Madurez esperado Anexo A PISIS

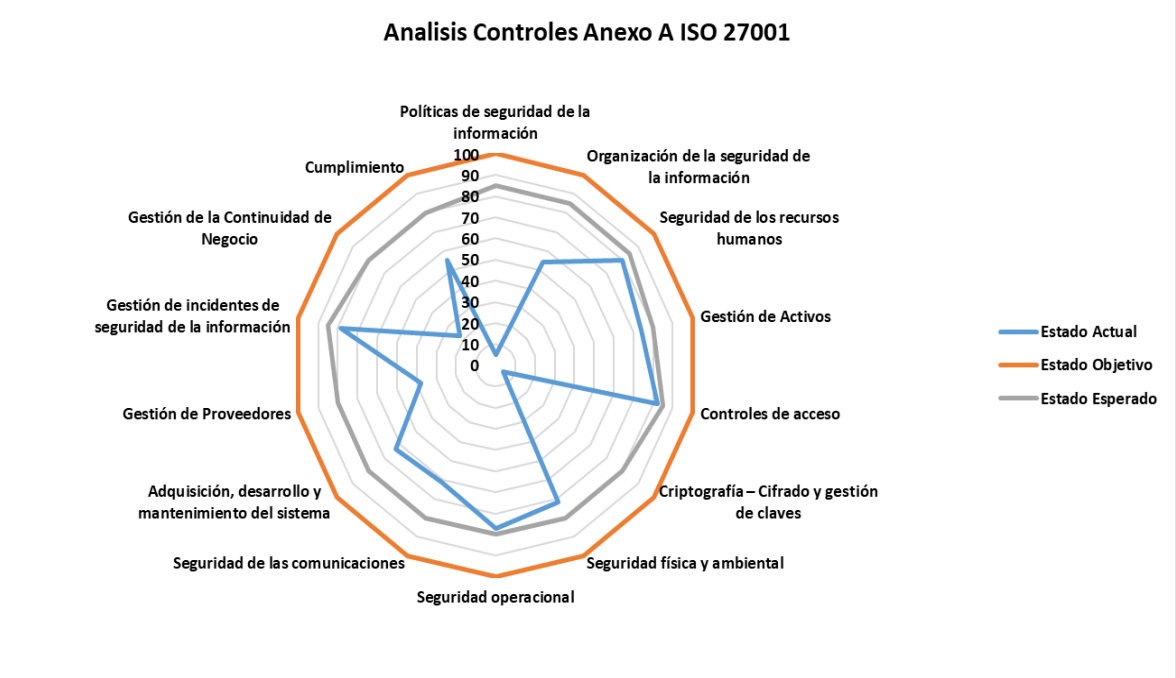

Ilustración 12 – Análisis Controles Esperados Anexo A PISIS

7. AUDITORÍA DE CUMPLIMIENTO DE LA ISO/IEC ISO 27002:2013

7.1 INTRODUCCIÓN

Una vez realizado el análisis de activos de información de la empresa, sus amenazas y sus riesgos asociados, se plantearon y planificaron una serie de proyectos a implementar en el plazo de tres años, que sirviesen para ir evolucionando en las distintas áreas que propone la norma ISO/IEC 27002:2013. La auditoría de cumplimiento analiza la evolución y estado de la gestión de la seguridad de la información en la organización. En este caso desde el nivel inicial al nivel de madurez una vez implementados los proyectos que en obligan a una evolución y revisión continua que irán optimizando el nivel de madurez en el tiempo.

Cabe destacar la importancia de estas auditorías como herramienta de análisis y revisión de la gestión de la seguridad de la información, como modo de obtener conocimiento del estado real y, por lo tanto, de las posibles acciones a implantar o mejorar.

7.2 METODOLOGÍA

El estándar ISO/IEC 27002:2013, agrupa un total de 114 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información organizado en 14 dominios y 35 objetivos de control. Éste estándar es internacionalmente reconocido y es perfectamente válido para la mayoría de las organizaciones.

Hay diferentes aspectos en los cuales las salvaguardas actúan reduciendo el riesgo, ya hablemos de los controles ISO/IEC 27002:2013 o de cualquier otro catálogo. Estos son en general:

- Formalización de las prácticas mediante documentos escritos o aprobados.
- Política de personal.
- Solicitudes técnicas (software, hardware o comunicaciones).
- Seguridad física.

La protección integral frente a las posibles amenazas requiere de una combinación de salvaguardas sobre cada uno de estos aspectos.

El objetivo de esta fase del proyecto es evaluar la madurez de la seguridad en lo que respecta a los 14 dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013, después de la implementación de los proyectos definidos inicialmente y cuyo objetivo es conseguir la certificación internacional en cumplimiento de la norma. Antes de abordar intentaremos profundizar al máximo en el conocimiento de la organización.

El estudio debe realizar una revisión de los 114 controles planteados por la norma para cumplir con los diferentes objetivos de control – el número de los cuales se indica entre paréntesis para cada uno de los 14 dominios. Esta estimación la realizaremos según la tabla del Modelo de Madurez de la Capacidad (CMM), el cual utilizamos previamente en la fase de Análisis diferencial de la organización.

7.3 RESULTADOS

En una auditoría interna se lleva a cabo una revisión del cumplimiento normativo de la organización, donde se pueden identificar los diferentes tipos de desviaciones:

- No conformidad Mayor: Incumple un apartado completo de la norma.
- No conformidad Menor: Incumple un punto de un apartado.
- Observación: No incumple nada, es sólo una recomendación, aunque si no se trata, en la siguiente auditoría se puede convertir en No conformidad.

En base a estos principios se realizará el análisis de adecuación de los diferentes controles que conforman los distintos dominios que establece la norma.

Teniendo en cuenta lo anterior, en la siguiente tabla se presentan las desviaciones identificadas, el control el cual se ve afectado por la desviación y una descripción breve del hallazgo identificado.

Desviación	Control	Descripción del Control	Descripción de la desviación
No Conformidad Mayor	Gestión de Proveedores	A.15.1.3. Cadena de suministro de tecnología de	No están incluyendo temas relacionados con la seguridad de la información para terceros en temas asociados

		información y comunicación.	con cadenas de suministro de productos y servicios de IT
No Conformidad Menor	Operación	8.1. Planificación y control operacional	Se evidencia implementación de planes para alcance de objetivos relacionados con la Seguridad de la Información, pero no están debidamente formalizados.
No Conformidad Menor	Gestión de Activos	A.8.3.1. Gestión de medios de Soporte Removibles.	Dentro del procedimiento de Administración y manejo de activos tecnológicos se definen controles de Gestión de estos, aunque no está ligado con la clasificación de la información (Ver Control A.8.2.1)
No Conformidad Menor	Controles de acceso	A.9.4.3. Sistema de Gestión de Contraseñas.	Aunque existe una política de contraseñas incluida dentro del procedimiento de Gestión de accesos, la configuración de esta depende de los sistemas y en ocasiones no cumplen con las directrices dadas.
No Conformidad Menor	Criptografía – Cifrado y gestión de claves	A.10.1.2. Gestión de Claves.	Existen controles para la gestión de claves criptográficas, pero estos no se encuentran documentados y/o formalizados.
No Conformidad Menor	Seguridad física y ambiental	A.11.1.1. Perímetro de Seguridad Física.	Se disponen de controles para perímetros de seguridad, pero estos no están formalizados.
No Conformidad Menor	Seguridad física y ambiental	A.11.1.5. Trabajo en áreas seguras.	Existe un procedimiento para el trabajo en Zonas Seguras, pero este no ha sido divulgado a la organización
No Conformidad Menor	Seguridad de las comunicaciones	A.13.2.2. Acuerdos sobre transferencia de información.	Los acuerdos de transferencia de información se realizan acorde a las necesidades del negocio y se definen directamente en los contratos, no es obligatorio incluir cláusulas obre el tema.

No Conformidad Menor	Adquisición, desarrollo y mantenimiento del sistema	A.14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones.	Existen controles que permiten la verificación de aplicaciones en caso de cambios en la plataforma, a de la operación, pero no están documentados.
No Conformidad Menor	Adquisición, desarrollo y mantenimiento del sistema	A.14.2.7. Desarrollo contratado externamente.	Dentro de los contratos suscritos con empresas de desarrollo externas, se realiza seguimientos de la actividad desarrollada, pero no hay procedimientos formalizados en el tema.
No Conformidad Menor	Cumplimiento	A.18.1.5. Reglamentación de Controles Criptográficos.	Se utilizan controles criptográficos, pero estos no se encuentran debidamente documentados y formalizados.
Observación	Gestión de Activos	A.8.1.1. Inventario de Activos.	Se dispone de un inventario de activos de Software y Hardware, los cuales incluyen activos de carácter documental, el cual no existía previamente. Se debe mantener el nivel de madurez sobre el control,
Observación	Gestión de Activos	A.8.2.1. Clasificación de la Información.	Se dispone de una clasificación de la información de acuerdo con sus niveles de confidencialidad, la cual se encuentra formalizada (no lo estaba previamente) en los documentos de la compañía. Se debe mantener el nivel de madurez sobre el control.
Observación	Gestión de Activos	A.8.3.3. Transferencia de medios de soporte físicos.	Se disponen de controles para la protección de medios de soporte removibles, los cuales se encuentran documentados y formalizados (anteriormente no lo estaba). Se debe mantener el nivel de madurez sobre el control.

Observación	Controles de acceso	A.9.2.5. Revisión de los derechos de acceso de usuarios.	Existe un procedimiento de revisión periódica de los accesos a los sistemas de información, la cual está integrada en las políticas del SGSI (originalmente no estaba integrada en la política). Se debe mantener el nivel de madurez sobre el control.
Observación	Criptografía – Cifrado y gestión de claves	A.10.1.1. Política sobre el uso de controles Criptográficos.	Existen controles criptográficos para la protección de información, los cuales se encuentran en un procedimiento el cual encuentra documentada y formalizada (Anteriormente no lo estaba). Se debe mantener el nivel de madurez sobre el control.
Observación	Seguridad física y ambiental	A.11.1.3. Seguridad de oficinas, salones e instalaciones.	Se disponen de controles de seguridad en las oficinas, salones e instalaciones de la compañía y sucursales, los cuales están formalizados en el procedimiento de Gestión de Acceso Físico.
Observación	Seguridad física y ambiental	A.11.2.7. Disposición segura o reutilización de equipos.	Se disponen de controles para la disposición segura y reutilización de equipos de cómputo, los cuales se encuentran formalizados (ante no lo estaba). Se debe mantener el nivel de madurez sobre el control.
Observación	Seguridad física y ambiental	A.11.2.9. Política de escritorio y pantalla limpios.	Se dispone de políticas relacionadas con escritorio y pantalla limpios (antes no estaban definidas). Se debe mantener el nivel de madurez sobre el control.
Observación	Seguridad operacional	A.12.1.3. Gestión de Capacidad.	Existen controles relacionados con proyecciones de aumentos de capacidad y manejo de recursos, los cuales están formalizados en las políticas de monitoreo de la

			organización (Previamente no estaban formalizados). Se debe mantener el nivel de madurez sobre el control.
Observación	Seguridad operacional	A.12.4.1. Registro de eventos.	Existen Controles relacionados con la revisión de logs y registros de los sistemas, los cuales están formalizados (No lo estaban). Se debe mantener el nivel de madurez sobre el control.
Observación	Seguridad operacional	A.12.4.2. Protección de la información de registro.	Existen controles para la protección de la información contenida en logs y registros de los sistemas de información, los cuales están formalizados (No lo estaban). Se debe mantener el nivel de madurez sobre el control.
Observación	Seguridad operacional	A.12.4.3. Registros del administrador y del operador.	Existen controles para la protección de la información contenida en logs y registros de los sistemas de información, los cuales están formalizados.
Observación	Seguridad operacional	A.12.6.1. Gestión de las vulnerabilidades técnicas.	Se dispone de controles para la Gestión de Vulnerabilidades Técnicas de los aplicativos, los cuales se encuentran formalizados y documentados (No lo estaban). Se debe mantener el nivel de madurez sobre el control.
Observación	Seguridad de las comunicaciones	A.13.1.1. Controles de redes.	Existen controles para la gestión de las redes de los sistemas de información de la compañía, los cuales se encuentran formalizados (No lo estaban). Se debe mantener el nivel de madurez sobre el control.
Observación	Seguridad de las comunicaciones	A.13.1.2. Seguridad de los servicios de red.	Existen controles para la gestión de las redes de los sistemas de información de la compañía, los cuales se

			encuentran formalizados (No lo estaban). Se debe mantener el nivel de madurez sobre el control.
Observación	Seguridad de las comunicaciones	A.13.2.3. Mensajes electrónicos.	La información enviada por e-mail se encuentra protegida a través de canales seguros y cifrado SSL, los cuales se encuentran formalizados y documentados (Antes no lo estaban). Se debe mantener el nivel de madurez sobre el control.
Observación	Adquisición, desarrollo y mantenimiento del sistema	A.14.2.8. Pruebas de seguridad de sistemas.	Se realizan pruebas de aceptación de los sistemas de información en temas relacionados con seguridad de la información, los cuales se están formalizados (No lo estaba). Se debe mantener el nivel de madurez sobre el control.
Observación	Gestión de Proveedores	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores.	Existe una política de seguridad de la información relacionada con proveedores (Anteriormente, no existía). Se debe mantener el nivel de madurez sobre el control.
Observación	Gestión de Proveedores	A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores.	Dentro de los contratos suscritos con proveedores críticos, se incluyen consideraciones sobre la seguridad de la información, los cuales se encuentran formalizados en las políticas de seguridad para proveedores. (Antes no se tenía en cuenta estas consideraciones). Se debe mantener el nivel de madurez sobre el control.
Observación	Gestión de Proveedores	A.15.2.2. Gestión de cambios a los servicios de los proveedores.	Dentro de los contratos con proveedores se realizan la gestión de cambios en el suministro de servicios, los cuales se encuentran formalizados en las políticas

			de seguridad para proveedores (No lo estaba). Se debe mantener el nivel de madurez sobre el control.
Observación	Gestión de incidentes de seguridad de la información	A.16.1.5. Respuesta a incidentes de seguridad de la información.	En el procedimiento de Gestión de incidentes tecnológicos se tienen establecidos los tiempos en los cuales se deben dar soluciona los incidentes de seguridad de la información (No estaban definidos los tiempos previamente). Se debe mantener el nivel de madurez sobre el control.
Observación	Gestión de incidentes de seguridad de la información	A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información.	Se dispone de controles relacionados con el manejo de elecciones aprendidas en el manejo de incidentes de seguridad de la información, el cual está formalizado en el procedimiento de Gestión de incidentes tecnológicos (No lo estaba). Se debe mantener el nivel de madurez sobre el control.
Observación	Gestión de incidentes de seguridad de la información	A.16.1.7. Recolección de evidencia.	Dentro del procedimiento de Gestión de Incidentes tecnológicos, se disponen de controles para la recolección y el manejo de evidencias. (No lo estaban). Se debe mantener el nivel de madurez sobre el control.

Tabla 13 – Desviaciones Identificadas Análisis de Madurez

A continuación, se presenta un detalle de los resultados de la evaluación de los niveles de madurez posterior a la aplicación de los proyectos tanto para los dominios como los controles del Anexo A de forma detallada.

7.3.1 Resultados Evaluación de los Dominios

Al realizar la evaluación de los controles relacionado con los dominios de la norma, se obtienen los siguientes resultados:

Valor	Significado	No de Controles	Porcentaje
L0	Inexistente	0	0,0%
L1	Inicial	0	0,0%
L2	Manejado	1	4,0%
L3	Definido	25	96,0%
L4	Manejado Cuantitativamente	0	0,0%
L5	Optimizado	0	0,0%

Tabla 14 - Análisis Evaluación Auditoría Dominios PISIS

De lo anterior se puede observar que hay 25 controles que ya se encuentran manejados, debido a que los planes de implementación de la norma, ya que la empresa cuenta ahora con un documento de Política de Seguridad de la Información al alcance de los afectados y tiene un plan de revisión de esta.

A continuación, se describe el nivel de madurez ponderado para los dominios de gestión de la norma para PISIS S.A después de la realización del ejercicio de la auditoria.

Dominio	Porcentaje	Calificación
Contexto de la organización	4,50	Definido
Liderazgo	4,50	Definido
Planificación	4,50	Definido
Soporte	4,50	Definido
Operación	4,25	Definido
Evaluación del Desempeño	4,50	Definido
Mejora	4,50	Definido
Promedio	**4,46**	**DEFINIDO**

Tabla 15 - Nivel de Madurez Evaluación Auditoría Dominios PISIS

La situación actual refleja que la gestión de la norma está en una fase DEFINIDA, por lo cual hay un buen grado de madurez implementado, y por lo cual, los objetivos de los proyectos definidos en la fase anterior surgieron efectos positivos. A continuación, se detalla para cada dominio el análisis detallado y los hallazgos identificados.

- **Contexto de la Organización**

El dominio correspondiente al contexto de la organización tenido una evolución de madurez óptima, por lo tanto, ha alcanzo un nivel acorde a la norma, ya que se evidencian registros o actas donde la organización determine los enfoques y propósitos del sistema de gestión de la información.

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

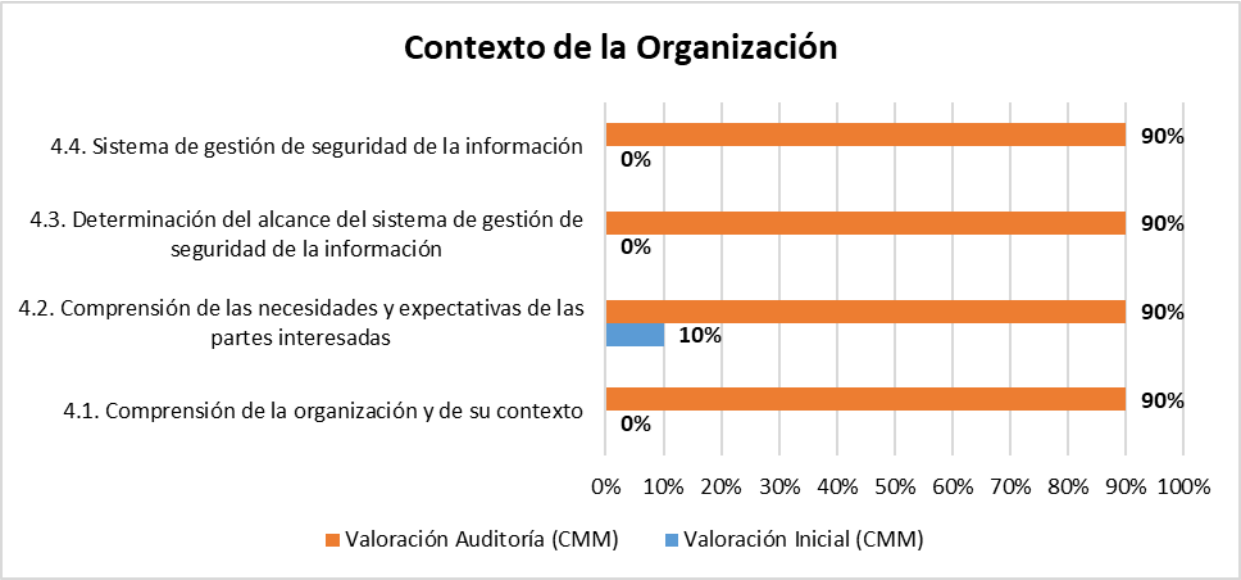

Ilustración 13 – Nivel de Madurez: Contexto de la Organización

- **Liderazgo**

El dominio correspondiente al liderazgo ha tenido una evolución de madurez óptima, por lo tanto, ha alcanzo un nivel acorde a la norma. Se disponen de las partes interesadas y sus necesidades en los documentos de las Actas de Junta Directiva, las cuales se encuentran relacionadas en las revisiones por la dirección. Además, hay un compromiso con respecto a la protección de la información, la cual está influida por el SGSI. Adicionalmente se tiene establecida una política de Seguridad de la información, la cual esta adecuada para la organización y se encuentra aprobada por la alta dirección, además de haberse definido una serie de roles y responsabilidades con respecto a la seguridad de la Información.

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

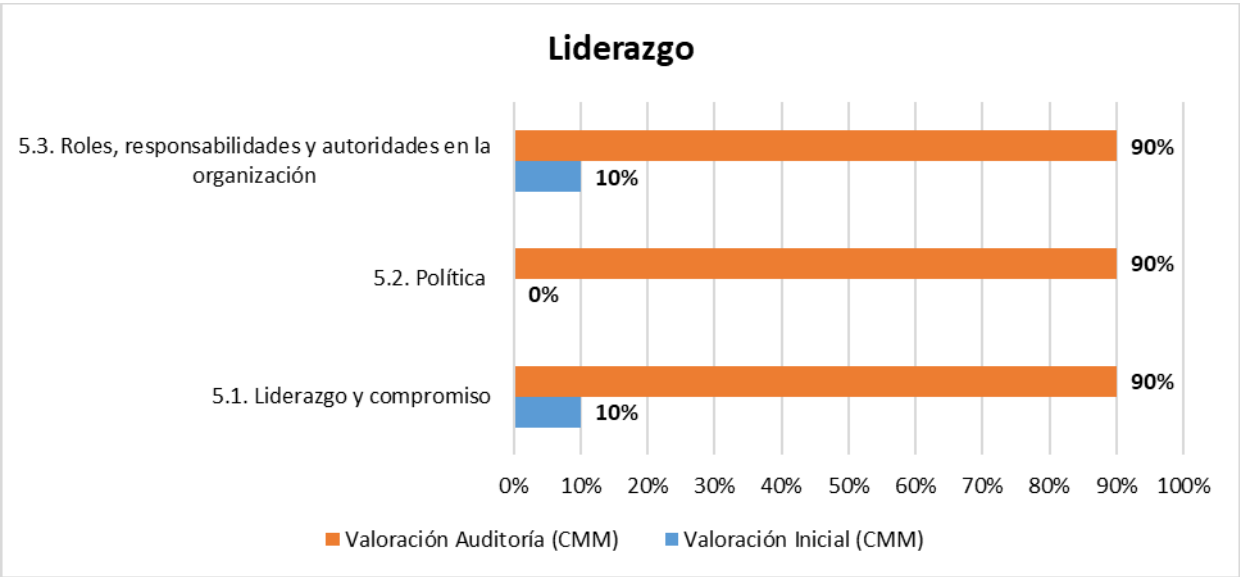

Ilustración 14 – Nivel de Madurez: Liderazgo

- **Planificación**

El dominio correspondiente a la Planificación ha tenido una evolución de madurez óptima, por lo tanto, ha alcanzo un nivel acorde a la norma Existen evidencias de métricas, de evaluación, de recursos involucrados, de responsables de seguimiento de objetivos, etc., a través de los indicadores del sistema. Adicionalmente, dentro del proceso de administración de riegos se encuentra dentro de las políticas del SGSI elementos de estos relacionados con temas de seguridad de la información, los cuales siguen las metodologías definidas de administración de riesgos (ISO 31000)

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

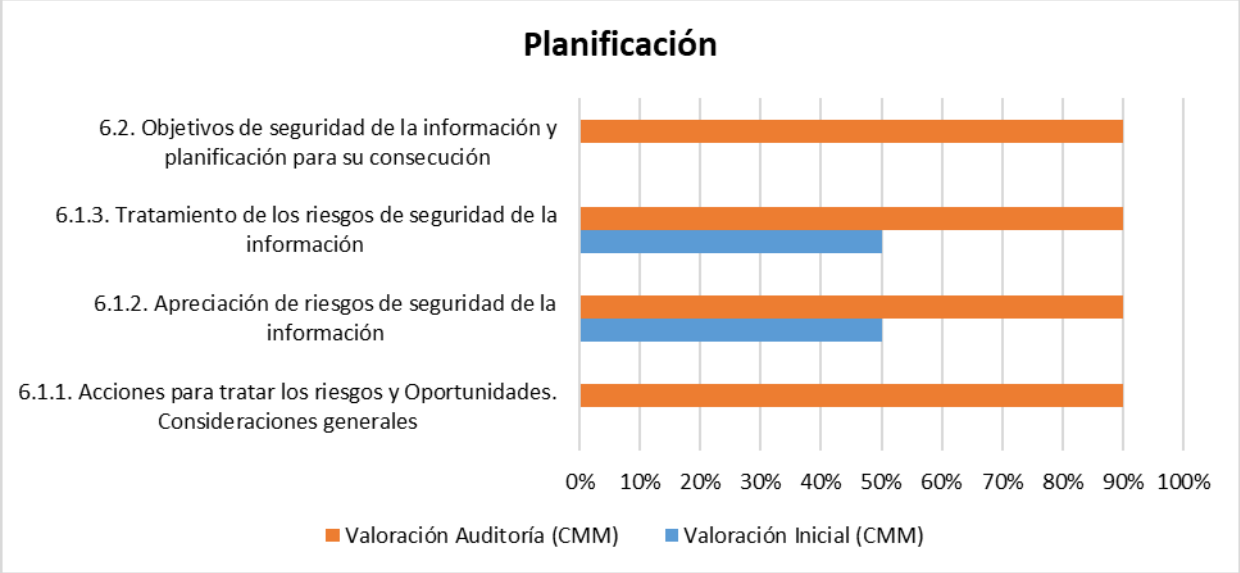

Ilustración 15 – Nivel de Madurez: Planificación

- **Soporte**

El dominio correspondiente a las Políticas de seguridad ha tenido una evolución de madurez óptima, por lo tanto, ha alcanzo un nivel acorde a la norma. Dentro de los perfiles y la guía de cargo, se encuentran establecidas responsabilidades con respecto a las competencias y responsabilidades relacionadas con el SGSI. Además, existen mecanismos de comunicación en temas relacionados con vulnerabilidades de seguridad, manejo de activos tecnológicos y protección de la información, los cuales están involucrados dentro del SGSI. Finalmente, Se dispone de controles y procedimientos para el aseguramiento de la información (Como Gestión documental), la cual está involucrada dentro del SGSI.

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

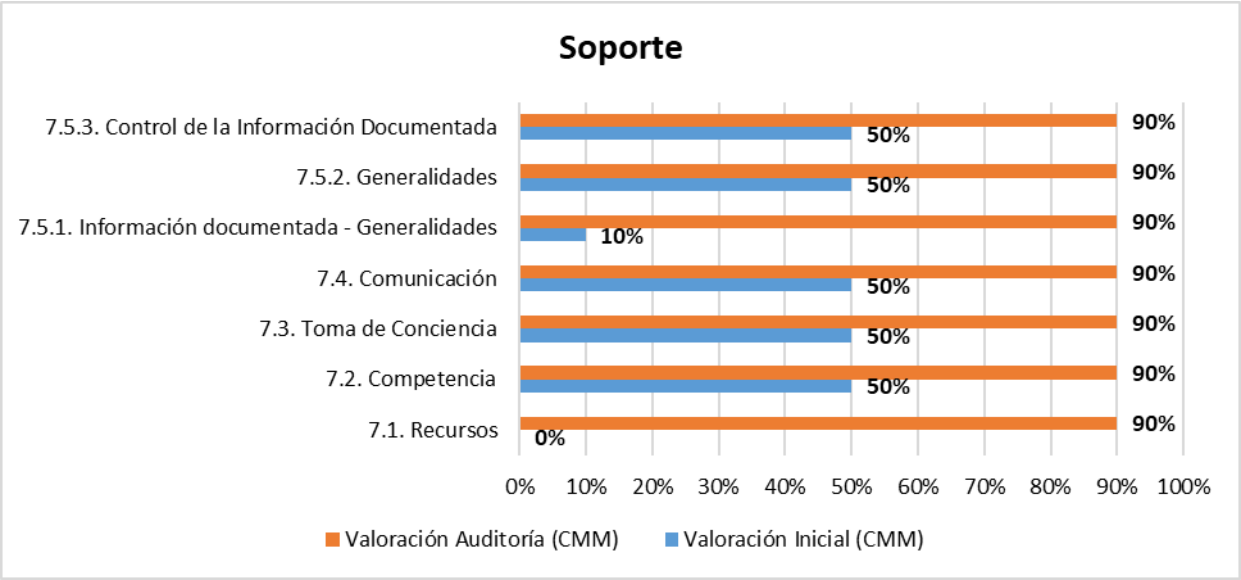

Ilustración 16 – Nivel de Madurez: Soporte

- **Operación**

El dominio correspondiente a las Políticas de seguridad ha tenido una evolución de madurez óptima, por lo tanto, ha alcanzo un nivel acorde a la norma. Se evidencia implementación de planes para alcance de objetivos relacionados con la Seguridad de la Información, los cuales están debidamente formalizados.

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

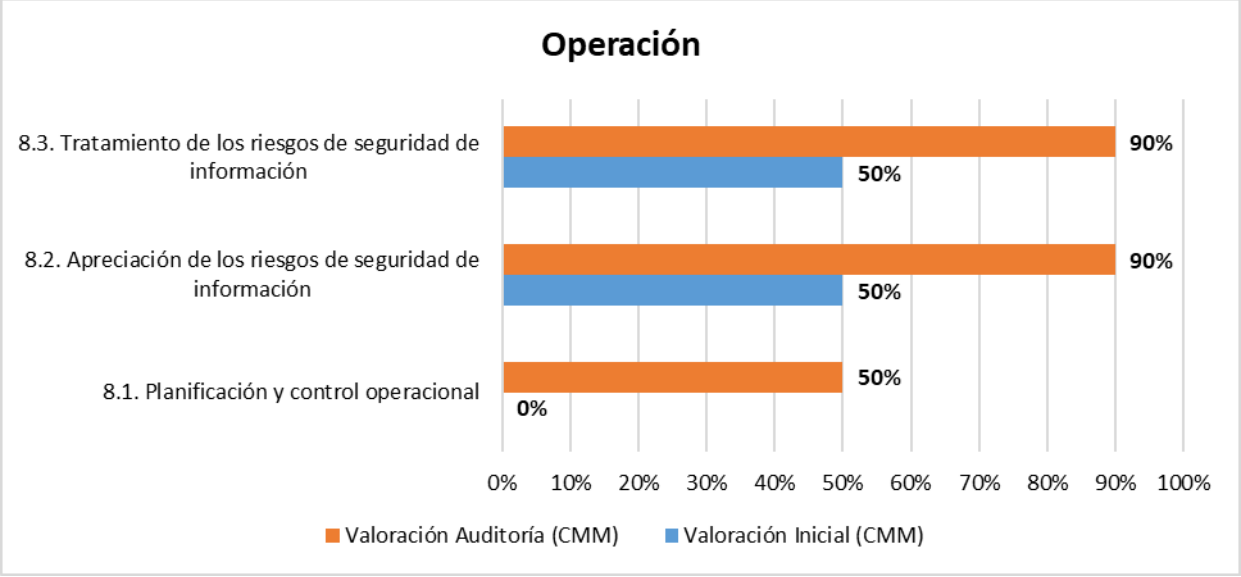

Ilustración 17 – Nivel de Madurez: Operación

- **Evaluación del Desempeño**

El dominio correspondiente a las Políticas de seguridad ha tenido una evolución de madurez óptima, por lo tanto, ha alcanzo un nivel acorde a la norma. Existe un procedimiento de auditorías internas ligadas al sistema de gestión de Seguridad de la Información, además de procedimiento definido para la realización de revisiones periódica por parte de la dirección.

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

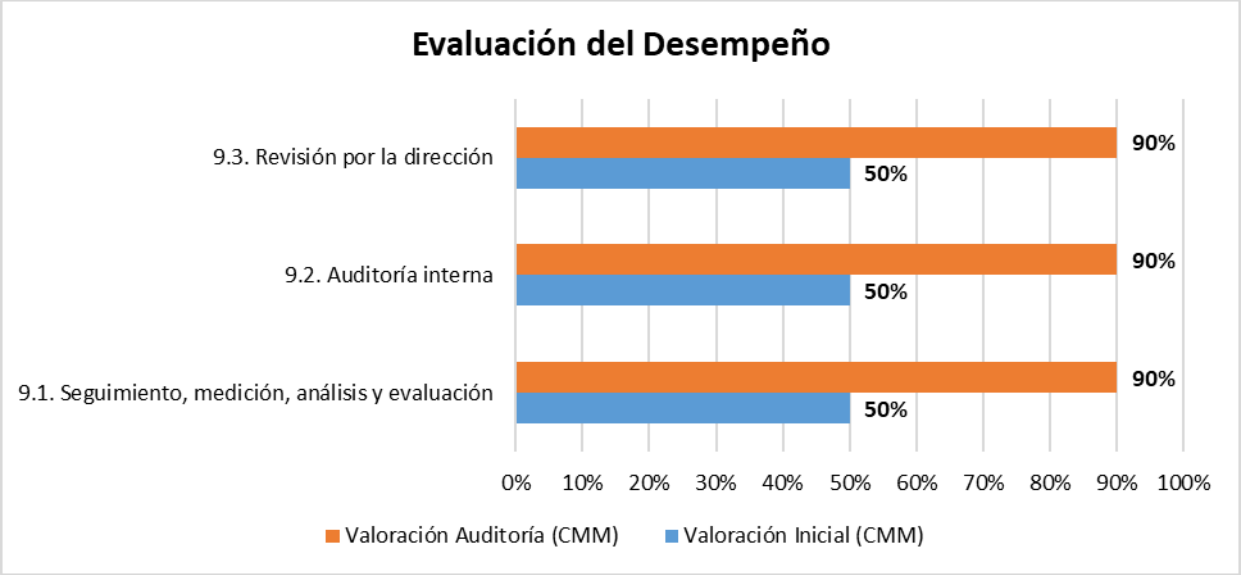

Ilustración 18 – Nivel de Madurez: Evaluación del Desempeño

- **Mejora**

El dominio correspondiente a las Políticas de seguridad ha tenido una evolución de madurez óptima, por lo tanto, ha alcanzo un nivel acorde a la norma. Se dispone de revisiones de acciones correctivas y no conformidades para los demás sistemas de gestión, incluyendo al SGSI, además de la generación de acciones de mejora continua que permiten fortalecer el Sistema de Gestión de Seguridad de la Información.

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

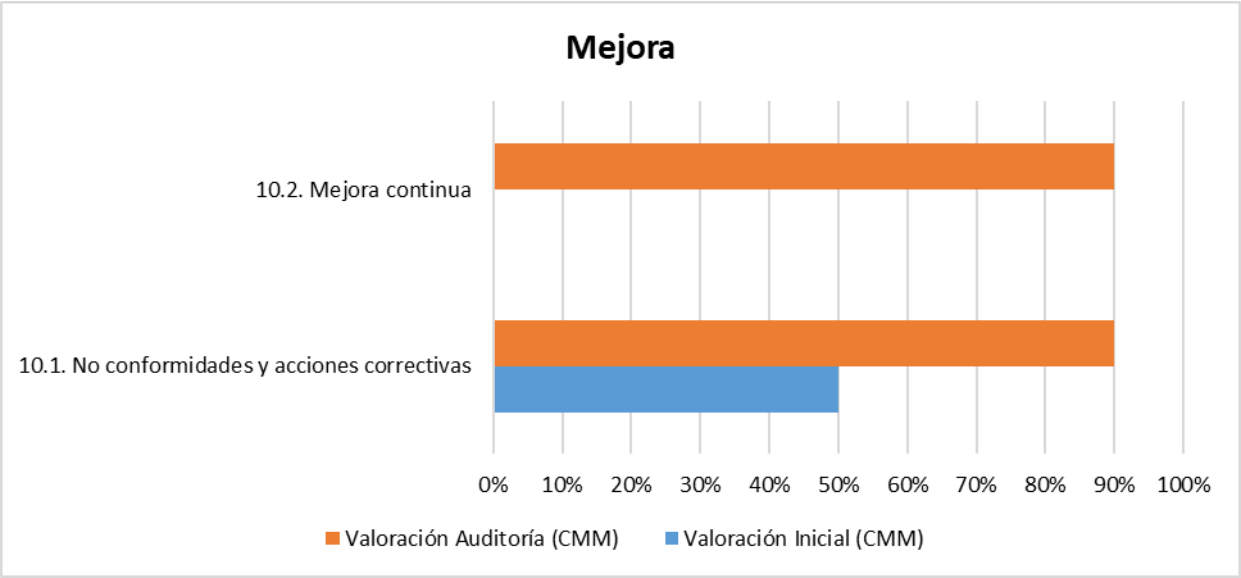

Ilustración 19 – Nivel de Madurez: Mejora

La siguiente figura describe gráficamente los niveles de madurez.

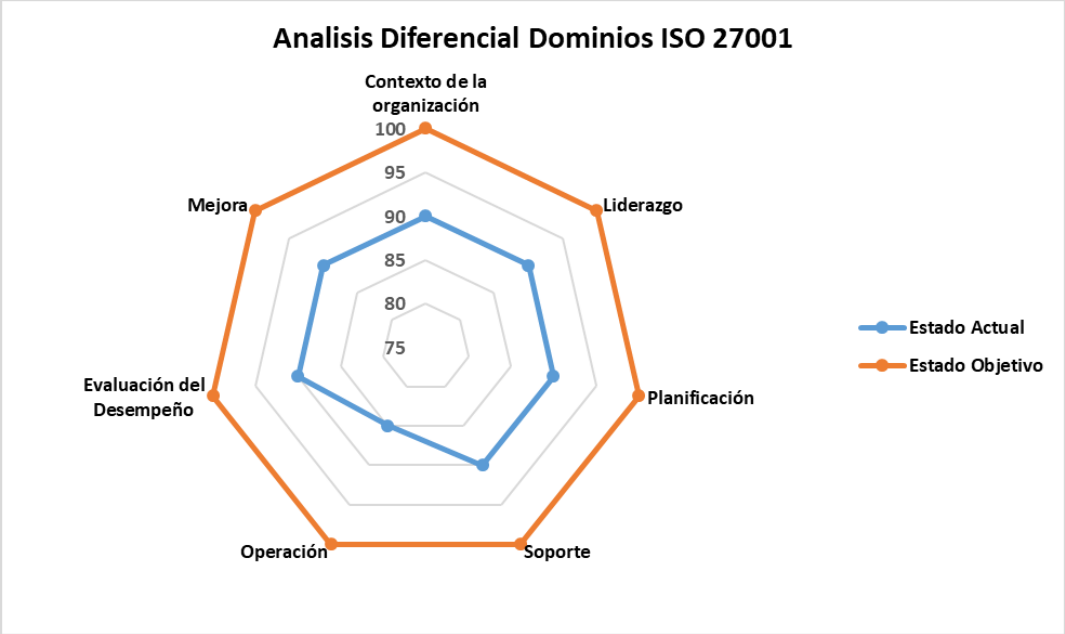

Ilustración 20 - Análisis Diferencial Dominios PISIS

7.3.2 Resultados Evaluación de los Anexos

Al realizar la evaluación de los controles relacionados con el Anexo A de la norma, se obtienen los siguientes resultados:

Valor	Significado	No de Controles	Porcentaje
L0	Inexistente	1	0,88%
L1	Inicial	1	0,88%
L2	Manejado	9	7,89%
L3	Definido	82	71,93%
L4	Manejado Cuantitativamente	17	14,91%
L5	Optimizado	4	3,51%

Tabla 16 - Análisis Controles Anexo A PISIS

De lo anterior, se puede deducir que hay un control inexistente, uno que esta implementado en fase inicial, nueve que están un a fase relativamente manejada y 103 que están implementados en un grado de madurez aceptable para la organización. A continuación, se detalla para cada dominio el análisis detallado y los hallazgos identificados.

- **Políticas de seguridad de la información**

El dominio correspondiente a las Políticas de seguridad ha tenido una evolución de madurez óptima, por lo tanto, ha alcanzo un nivel acorde a la norma. La empresa cuenta con un documento de Política de Seguridad de la Información al alcance de los afectados y tiene un plan de revisión de esta.

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

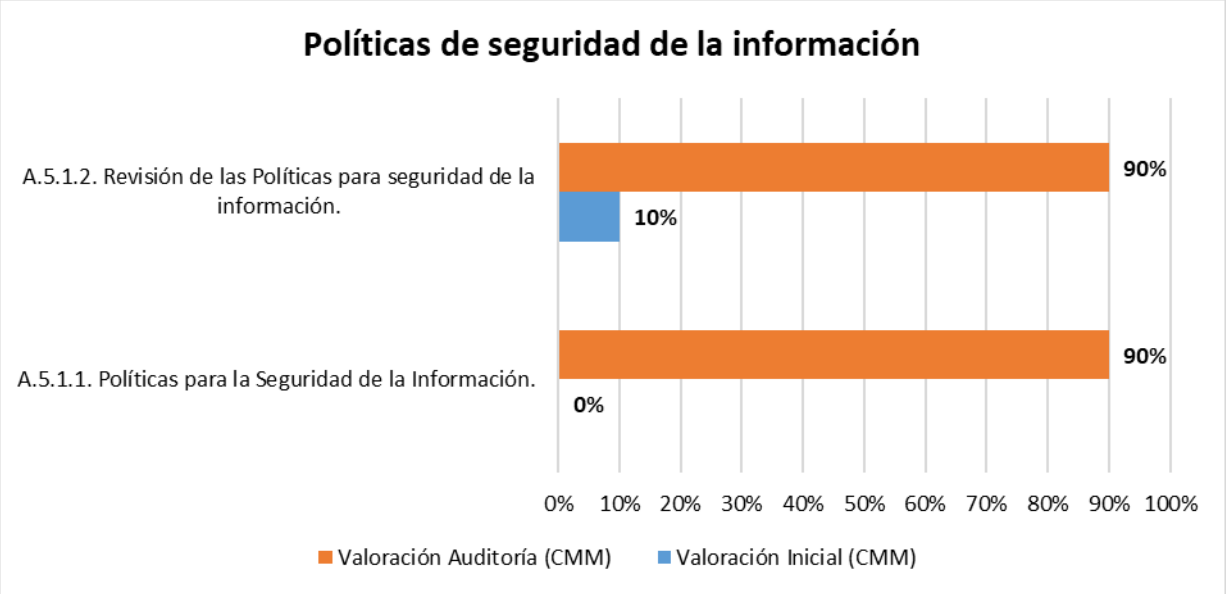

Ilustración 21 – Nivel de Madurez: Políticas de Seguridad de la Información

- **Organización de la seguridad de la información**

El dominio correspondiente a la organización de la seguridad de la información ha tenido una evolución de madurez óptima, por lo tanto, ha alcanzo un nivel acorde a la norma. La empresa se ha reforzado con respecto a los temas relacionados con contactos con autoridades y grupos de

interés, así como el establecimiento de diferentes roles y perfiles relacionados con la seguridad de la información para cada uno de los funcionarios.

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación, debido a que el control de teletrabajo no está incluido dentro de la declaración de aplicabilidad, por lo cual no se va a ver afectado por la implementación de la norma.

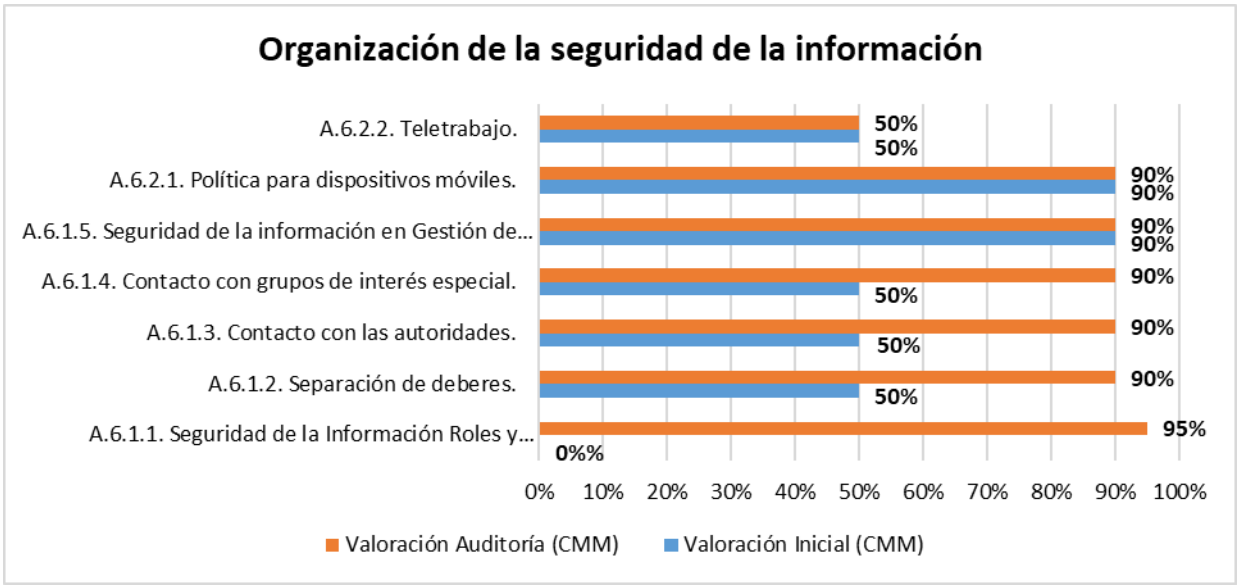

Ilustración 22 – Nivel de Madurez: Organización de la Seguridad de la Información

- **Seguridad de los recursos humanos**

Con respecto al dominio correspondiente a la seguridad de los recursos humanos se ha mantenido en un estado de madurez óptima, por lo tanto, se mantiene en niveles acordes a la norma. Por lo cual, respecto al resultado la auditoría este dominio no presenta ninguna no conformidad u observación

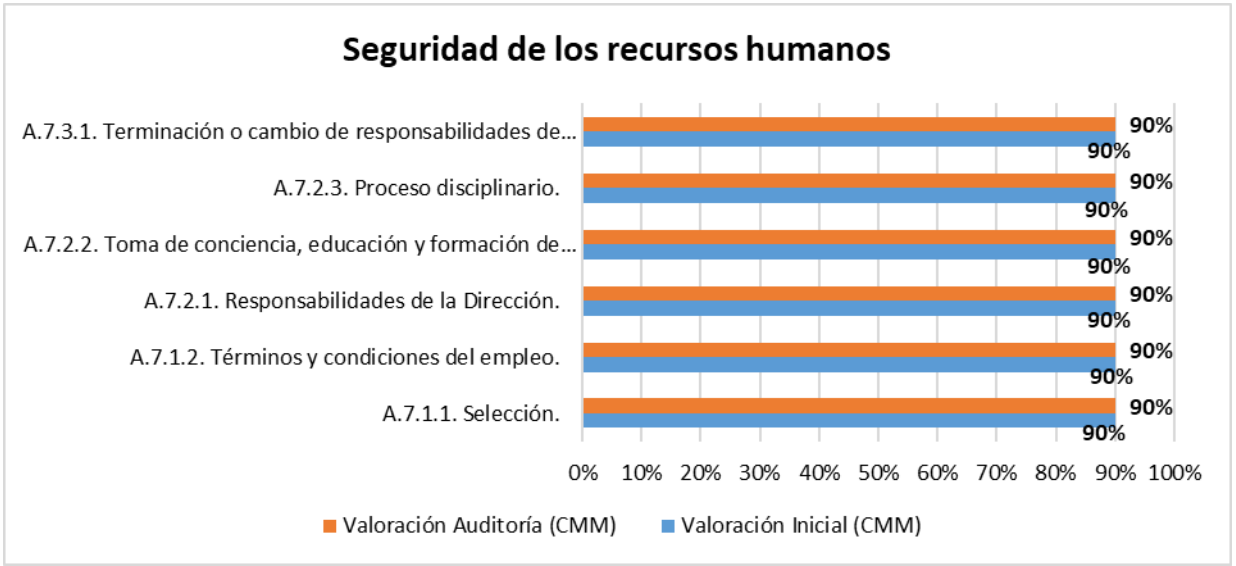

Ilustración 23 – Nivel de madurez: Seguridad de los recursos humanos

- **Gestión de Activos**

El dominio correspondiente a la gestión de activos ha tenido una evolución de madurez óptima, por lo tanto, ha alcanzo un nivel acorde a la norma. Se realizaron ajustes en los inventarios de los activos de información, incluyendo tipos de carácter documental. Así como en la clasificación de la información y la transferencia de medios de soporte físicos, la cuales se encuentran formalizadas y documentadas.

Respecto al resultado la auditoría sobre este dominio se presenta una conformidad menor focalizadas en el apartado 8.3.1 referido a la Gestión de Medios de Soporte Removibles, ya que dentro del procedimiento de Administración y manejo de activos tecnológicos se definen controles de Gestión, aunque no está ligado con la clasificación de la información, por lo cual se debe mitigar este tema

Como observaciones hay que comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo, los cuales se refieren a los numerales 8.1.1, 8.2.1 y 8.3.3

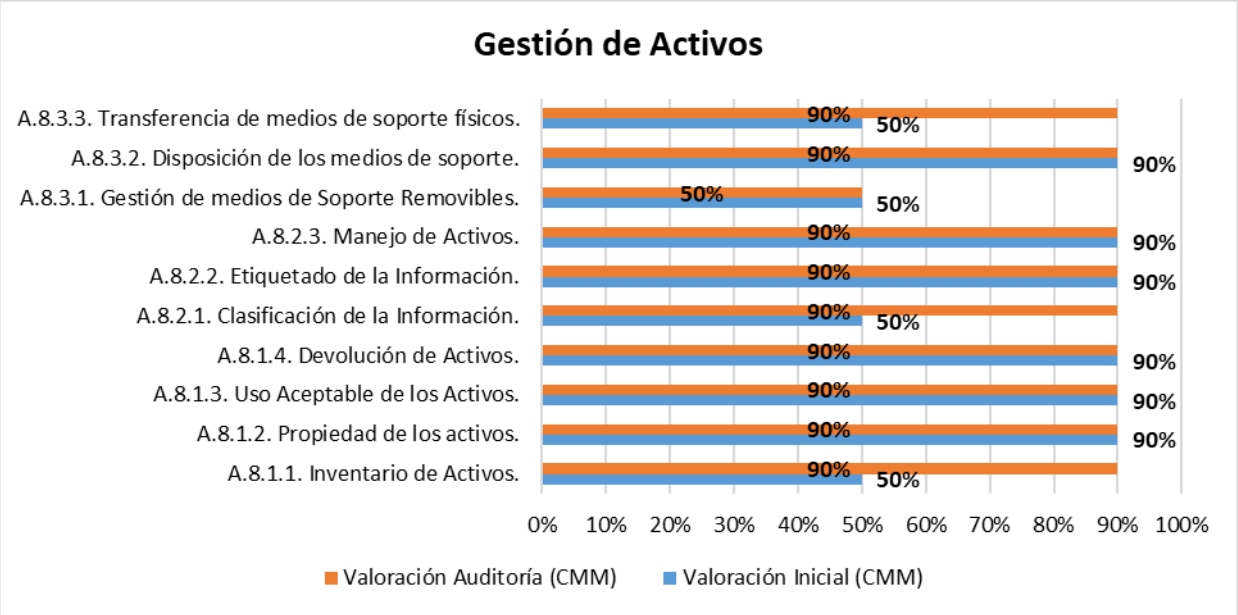

Ilustración 24 – Nivel de madurez: Seguridad de los recursos humanos

- **Controles de Acceso**

El dominio correspondiente a Control de Acceso en términos globales ha tenido una evolución de madurez óptima, por lo tanto, ha alcanzo un nivel acorde a la norma. Se realizo la implementación de un procedimiento para la gestión de accesos a los sistemas de información debidamente documentado y formalizado, por lo cual, se genera una observación en la cual se busca mantener este control funcionando en un nivel óptimo, el cual corresponde al numeral 9.2.5.

Adicionalmente se genera una no conformidad menor sobre el control 9.4.3, ya que, aunque existe una política de contraseñas incluida dentro del procedimiento de Gestión de accesos, la configuración de esta depende de los sistemas y en ocasiones no cumplen con las directrices dadas, por lo cual se recomienda realizar los ajustes para alinear las configuraciones con las políticas.

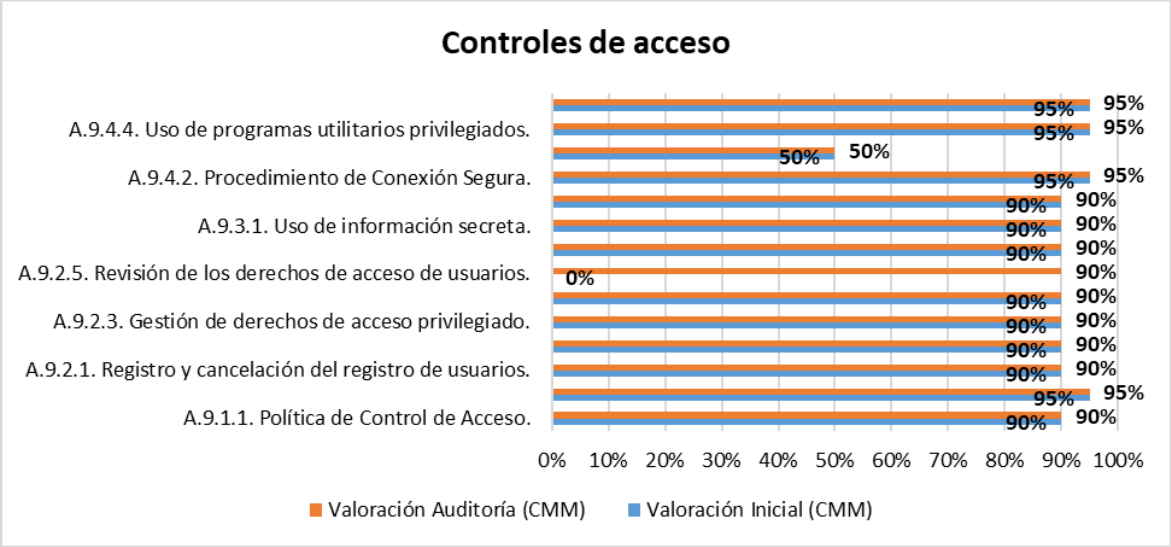

Ilustración 25 – Nivel de madurez: Controles de Acceso

- **Criptografía – Cifrado y Gestión de Claves**

El dominio correspondiente al Cifrado y Gestión de Claves ha madurado con respecto a la fase de análisis inicial, pero no ha alcanzado un grado de madurez optimo en su globalidad. Se implanto una política de Controles criptográficos la cual se encuentra integrada dentro del SGSI, por lo cual se genera una observación con el objetivo de garantizar los niveles de optimización del control a largo plazo, pero se observa que para el control 10.1.2, existen controles para la gestión de claves criptográficas, pero estos no se encuentran documentados y/o formalizados, por lo cual se genera una no conformidad menor sobre este punto en particular.

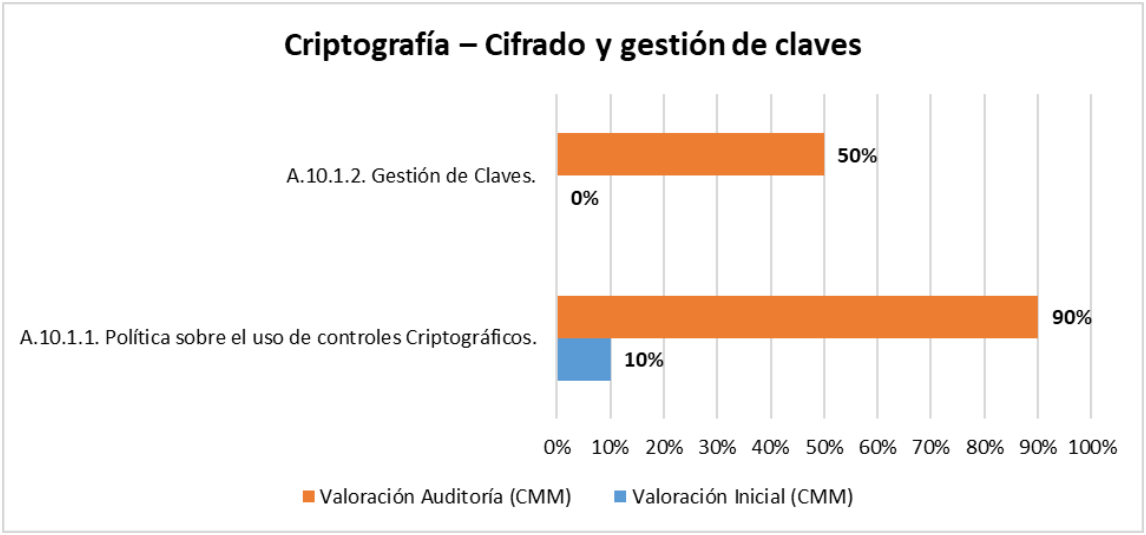

Ilustración 26 – Nivel de madurez: Cifrado y Gestión de Claves

- **Seguridad Física y Ambiental**

El dominio correspondiente a Seguridad Física y ambiental ha tenido una evolución de madurez óptima a nivel general, aunque hay algunos aspectos que se pueden mejorar para alcanzar un nivel alto. Se implemento una política de escritorio y pantalla limpias para la organización, así como se formalizaron los controles para la disposición segura y reutilización de equipos de cómputo.

Respecto al resultado la auditoría sobre este dominio se presenta dos no conformidades menores focalizadas en el apartado 11.1.5, referente a Trabajo en áreas seguras, ya que se dispone de controle definidos para el trabajo en este tipo de áreas, pero los cuales no han sido aprobados y formalizados a la organización, y la segunda en el numeral 11.1.1, ya que hay perímetros de seguridad física, pero estos no se encuentran debidamente formalizados.

Como observaciones hay que comentar que se debe mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo, los cuales se refieren a los numerales 11.1.3, 11.2.7 y 11.2.9

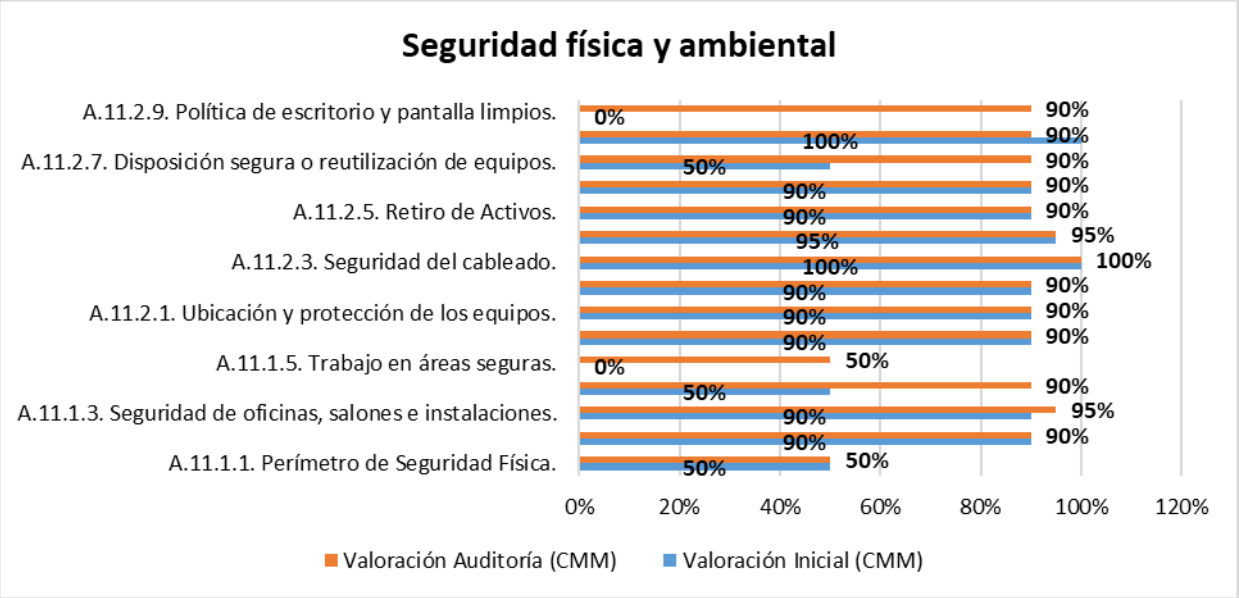

Ilustración 27 – Nivel de madurez: Seguridad Física y Ambiental

- **Seguridad Operacional**

Con respecto al dominio correspondiente a la seguridad en las operaciones ha mejorado con respecto al análisis diferencial realizado en la primera fase, por lo cual se encuentra en un estado de madurez óptima, obteniendo niveles acordes a lo definido en la norma. Se generan observaciones con relación a los controles 12.1.3, 12.4.1, 12.4.2 12.4.3 y 12.6.1, referentes a la conservación y el mantenimiento de los nuevos niveles de madurez alcanzados como consecuencia de los proyectos implementados para mejorar estos temas.

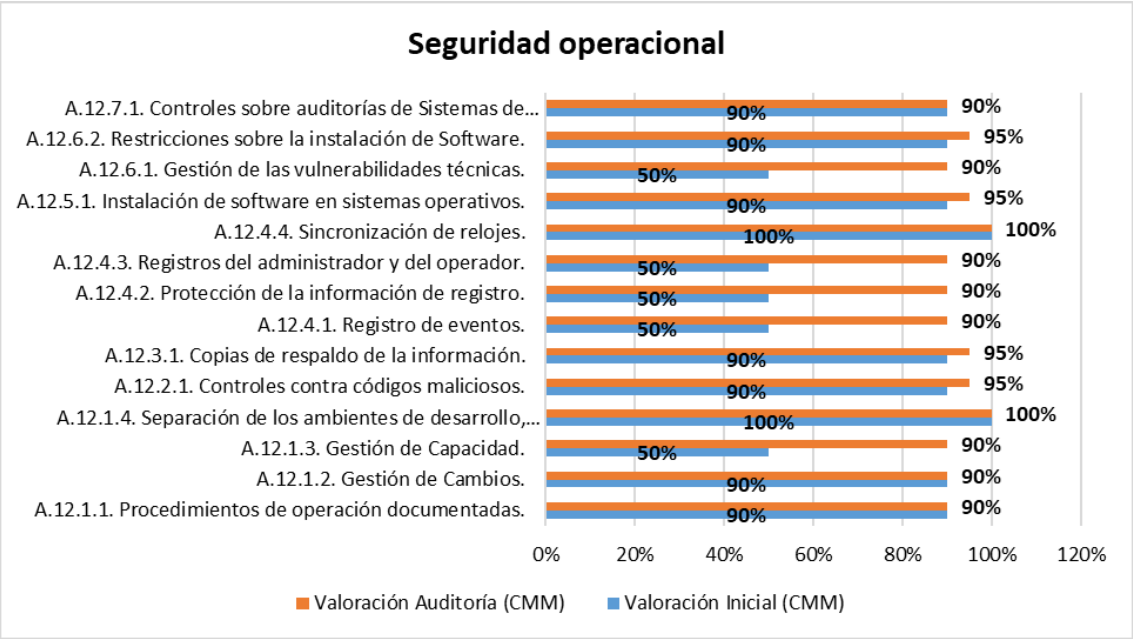

Ilustración 28 – Nivel de madurez: Seguridad Operacional

- **Seguridad de las Comunicaciones**

Con respecto a este dominio, se observa una mejora sustancial si se comparan los resultados obtenidos con relación al análisis diferencial inicial, en especial a lo referente a los controles relacionados con Controles de redes (se realizó la formalización de los controles ya preexistentes), seguridad en los servicios de red (similar al control anterior) y mensajes electrónicos (se realizó el cifrado de la información a un algoritmo SSL, que buscan asegurar la confidencialidad y la integridad de la información enviada por correos electrónicos), por lo cual se generan observaciones con el objetivo de buscar mantener en el tiempo los nuevos grados de madurez obtenidos.

Finalmente, se genera una no conformidad menor, relacionada con el control 13.2.2, la cual no ha sido implementada y fue detectada en la fase inicial, la cual consiste en que los acuerdos de transferencia de información se realizan acorde a las necesidades del negocio y se definen directamente en los contratos, pero no es obligatorio incluir cláusulas obre el tema. Se considera que se debe incluir este tipo de elementos en los contratos para asegurar legalmente las transferencias de información, más si contiene estos elementos críticos que pueden afectar a la organización por diversos factores.

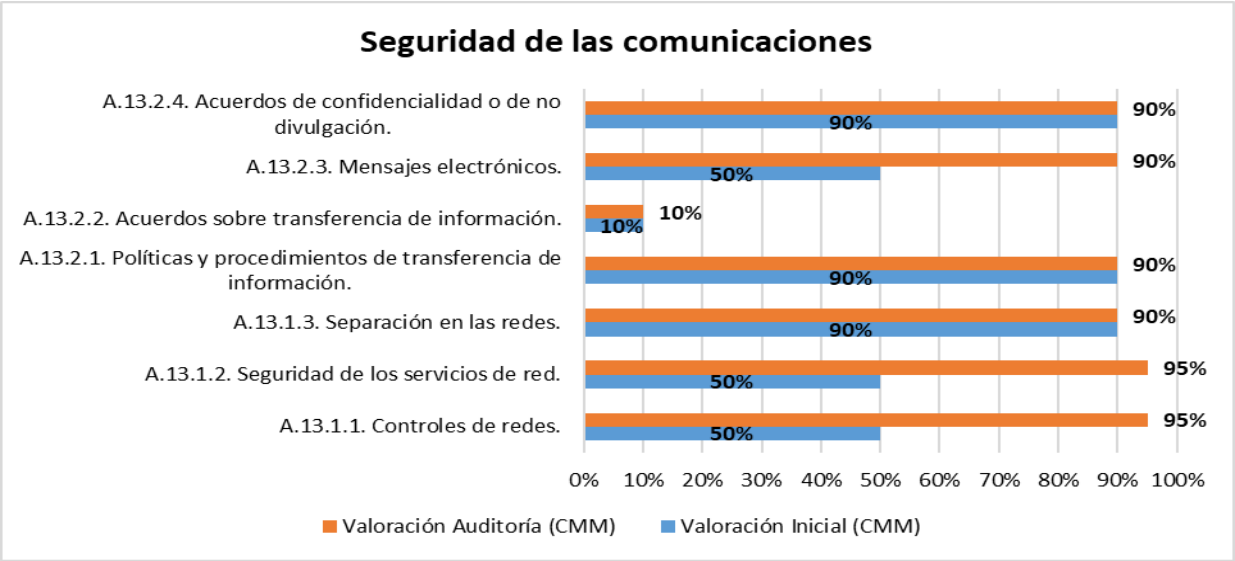

Ilustración 29 – Nivel de madurez: Seguridad en las Comunicaciones

- **Adquisición, desarrollo y mantenimiento del sistema**

En este dominio también se presentan mejoras con respecto al primer análisis realizado. En el control 14.2.8 se realizó la formalización del procedimiento de pruebas de seguridad de sistemas, las cuales ya se estaban ejecutando, pero no estaban dentro del SGSI. Tenido en cuenta lo anterior, a nivel de la auditoria se genera una observación indicando que se deben mantener los nuevos niveles de madurez adquiridos para este control.

Adicionalmente, se generan dos no conformidades menores sobre este dominio. La primera refiere al control 14.2.3, referente a la Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones, ya que no se han formalizado los controles que permiten la verificación de aplicaciones en caso de cambios en la plataforma. La segunda refiere al control 14.2.7, ya que, dentro de los contratos suscritos con empresas de desarrollo externas, se realiza seguimientos de la actividad desarrollada, pero no hay procedimientos formalizados para este tema en particular.

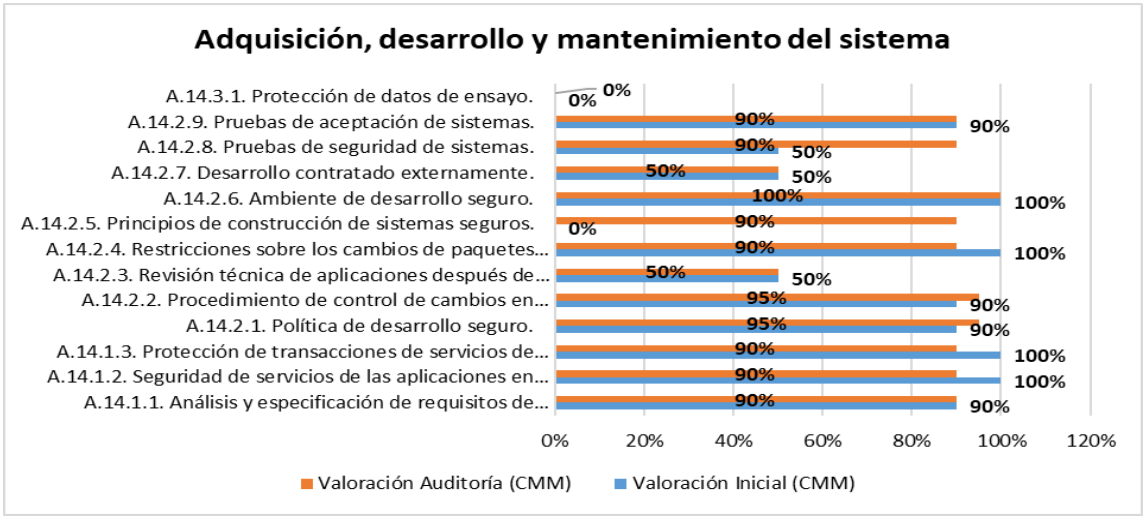

Ilustración 30 – Nivel de madurez: Adquisición, desarrollo y Mantenimiento

- **Gestión de Proveedores**

La auditoría para este dominio presenta una no conformidad mayor, relacionada con el control 15.1.3, ya que no están incluyendo temas relacionados con la seguridad de la información para terceros en temas asociados con cadenas de suministro de productos y servicios de TI. En términos globales le control presenta un cambio bastante importante con respecto al análisis inicial, por lo cual se generan observaciones cuyo objetivo primordial es mantener o mejorar los niveles de madurez en aquellos controles que alcanzan un nivel óptimo, correspondientes a los demás controles

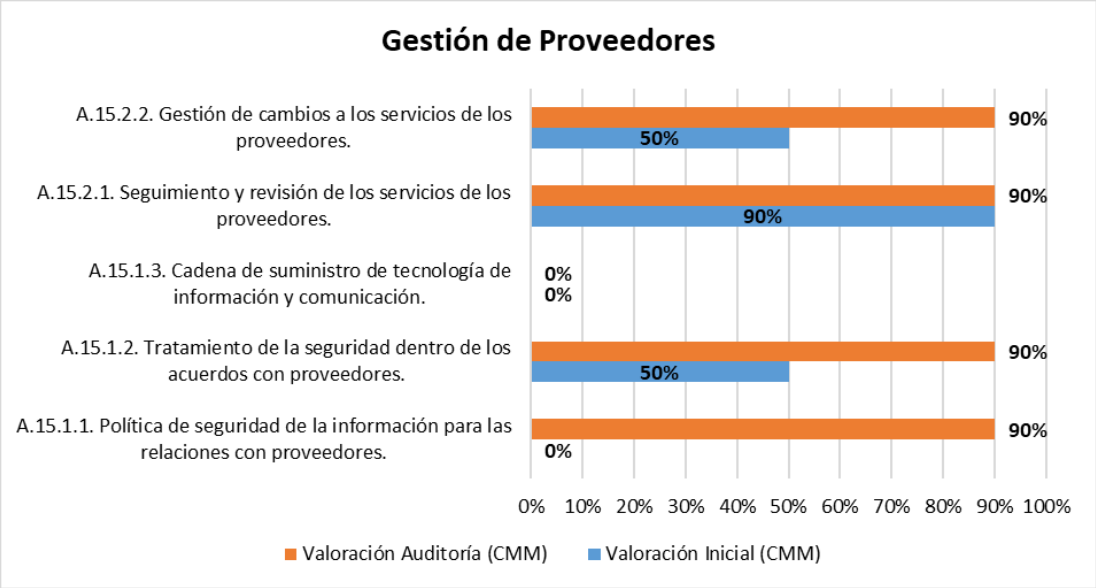

Ilustración 31 – Nivel de madurez: Gestión de Proveedores

- **Gestión de Incidentes de Seguridad de la Información**

Con respecto al dominio relacionado con la gestión de incidentes, se presentaron cambios circunstanciales con respecto a la evaluación diferencial realizada en la primera fase, como resultado de los diferentes proyectos propuestos para mejorar los niveles en seguridad de la información para la organización, se presentan mejoras con respecto a los tiempos de respuesta para los incidentes de seguridad de la información, el aprendizaje como consecuencia de los diferentes incidentes ocurridos en la organización y la recolección de evidencias y cadenas de custodia, por lo cual, como observaciones, se generan tres referentes a estos controles (16.1.5, 16.1.6 y 16.1.7) con el fin de asegurar que los niveles de madurez alcanzados se mantengan en el tiempo.

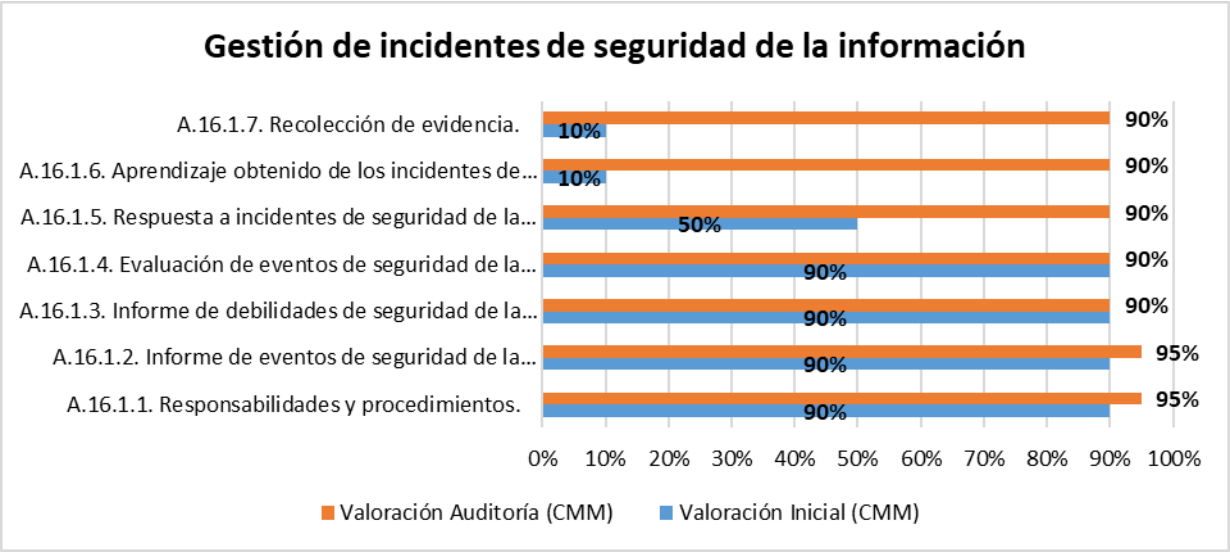

Ilustración 32 – Nivel de madurez: Gestión de Incidentes de Seguridad de la información

- **Gestión de la Continuidad de negocio**

En el análisis diferencial inicial se identificó que el dominio relacionado con la gestión de la continuidad de negocio quizá era el de menor implementación en la organización, pro en la auditoria se identificó que los diferentes planes de acción generados han dado resultado, por lo cual ya se tiene implementado un sistema de continuidad de negocio acorde a lo establecido con la norma, alcanzando un grado alto de madurez.

Respecto al resultado la auditoría sobre este dominio no presenta ninguna no conformidad u observación.

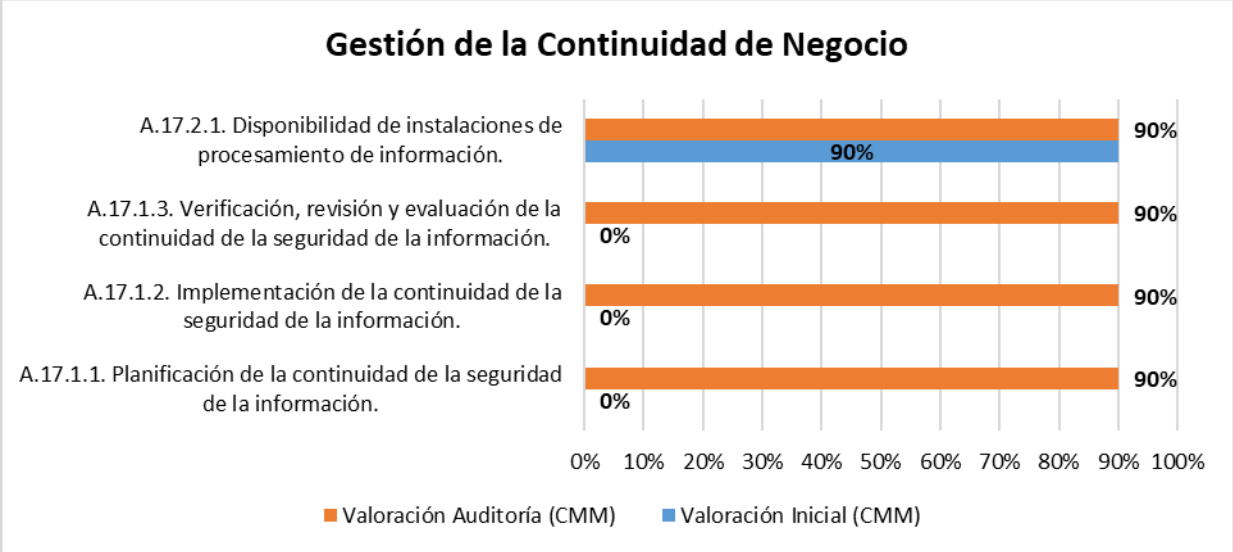

Ilustración 33 – Nivel de madurez: Gestión de la Continuidad de Negocio

- **Cumplimiento**

Con respecto al dominio de cumplimento se observa que a nivel global se tiene un nivel de madurez alto. Con respecto a la auditoria, no se presentan variaciones significativas con respecto al análisis diferencial inicial, por lo cual, se genera una no conformidad menor referente al numeral 18.1.5, ya que controles criptográficos se deberían utilizar de acuerdo con todos los contratos, leyes y reglamentaciones pertinentes, estos no están debidamente formalizados y divulgados a los funcionarios de la organización.

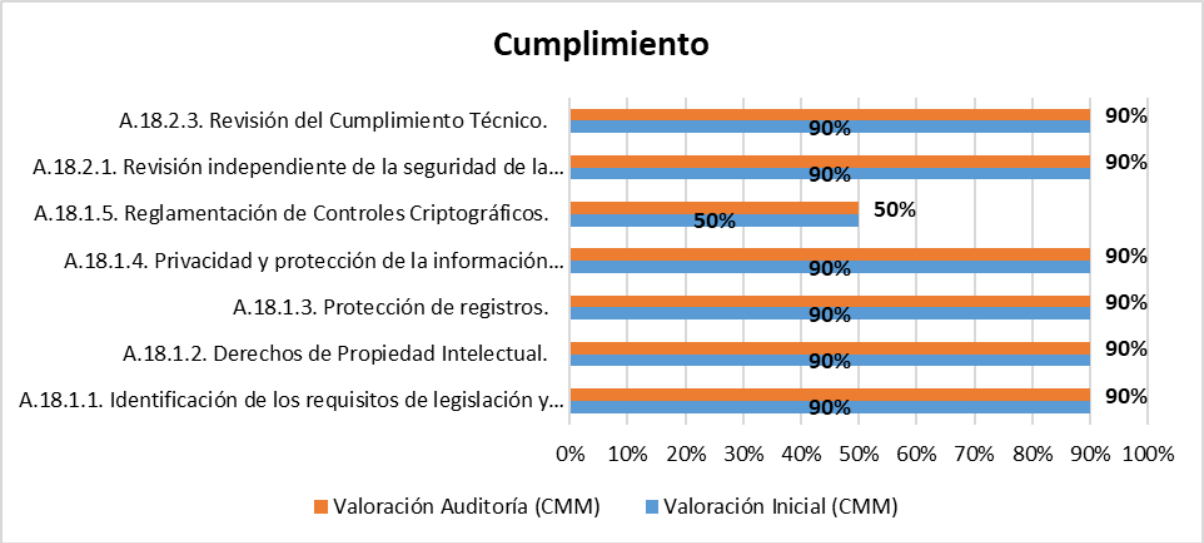

Ilustración 34 – Nivel de madurez: Cumplimiento

Finalmente, se describe el nivel de madurez actual ponderado para los controles definidos en el Anexo A de la norma para PISIS S.A, después de la ejecución de la auditoría.

Controles	Porcentaje	Calificación
Políticas de seguridad de la información	4,50	Definido
Organización de la seguridad de la información	4,25	Definido
Seguridad de los recursos humanos	4,50	Definido
Gestión de Activos	4,30	Definido
Controles de acceso	4,43	Definido
Criptografía – Cifrado y gestión de claves	3,50	Manejado
Seguridad física y ambiental	4,30	Definido
Seguridad operacional	3,75	Manejado
Seguridad de las comunicaciones	3,96	Manejado
Adquisición, desarrollo y mantenimiento del sistema	3,96	Manejado
Gestión de Proveedores	3,60	Manejado
Gestión de incidentes de seguridad de la información	4,57	Definido
Gestión de la Continuidad de Negocio	4,50	Definido
Cumplimiento	4,25	Definido
Promedio	**4,17**	**DEFINIDO**

Tabla 17 - Nivel de Madurez Anexo A PISIS

La situación actual refleja que la gestión de la norma está en una fase DEFINIDA, por lo cual, los objetivos propuestos para cada uno de los proyectos indicados en el numeral 6, han surtido el resultado esperado y la organización esta presta a cumplir los requerimientos necesarios para tener una certificación en la norma ISO 27001:2013, cumpliendo los estándares internacionales y la normatividad local para el funcionamiento de los operadores de información PILA.

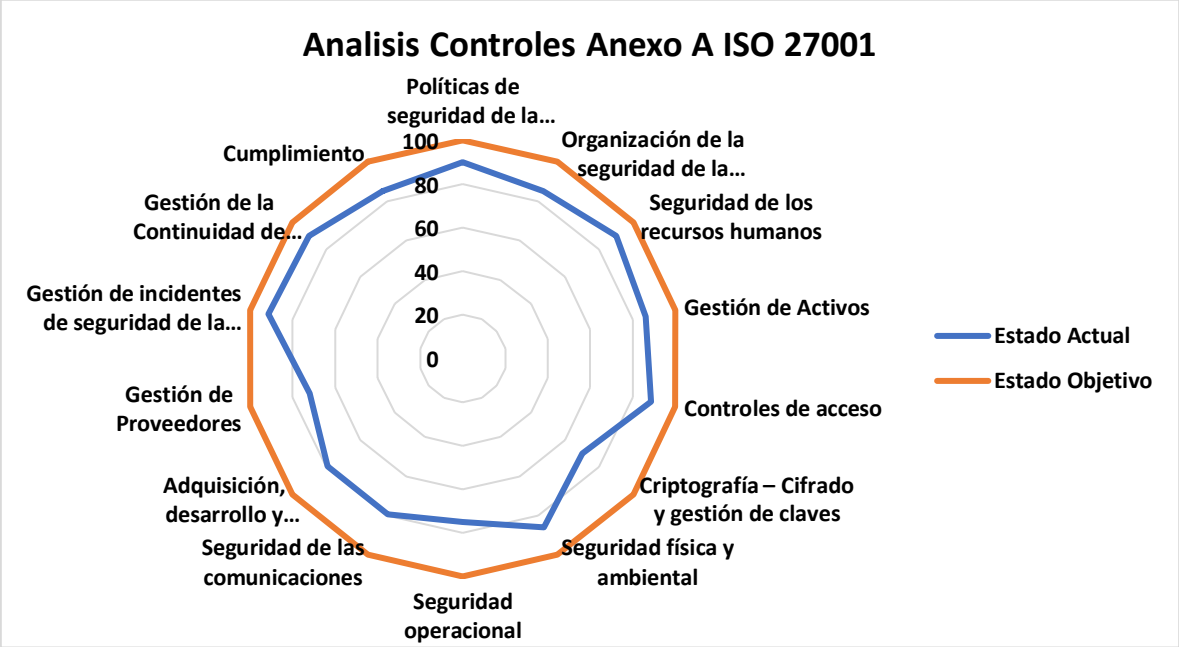

Ilustración 35 - Análisis Controles Anexo A PISIS

El detalle de la revisión se encuentra adjunta en documento "**Anexo 11 - Análisis Diferencial Auditoría Certificación.pdf"**

Como resumen final del análisis de la auditoría de cumplimiento se presenta a nivel grafico el cómputo general de no conformidades mayores, menores y observaciones tanto para los dominios como el Anexo A de la Norma ISO 27001:

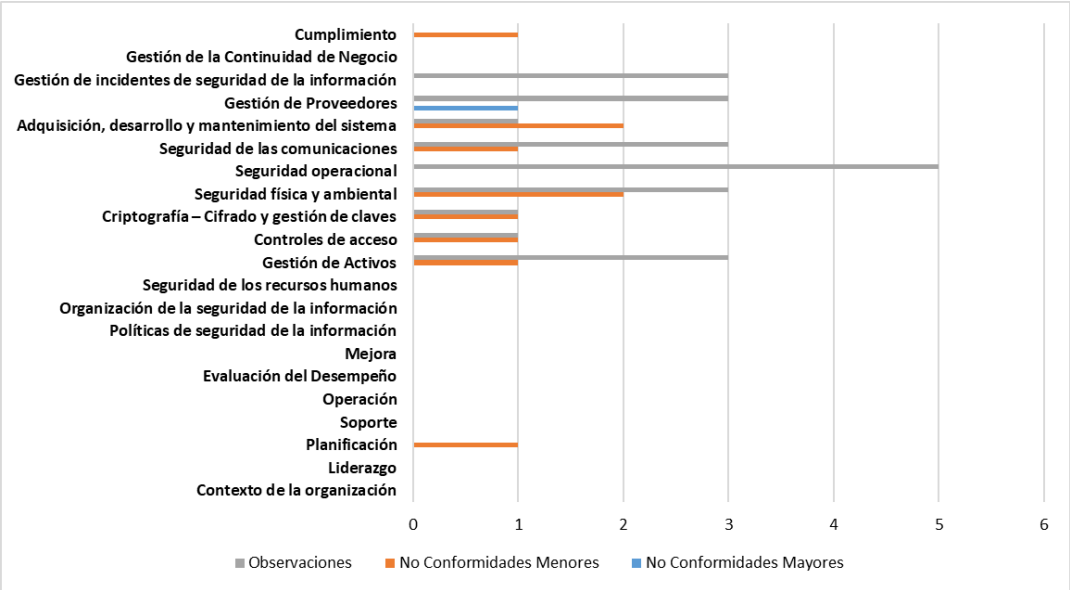

Ilustración 36 – Hallazgos Identificados Auditoría Certificación

8. CONCLUSIONES

La realización de este trabajo ha servido para que la organización tome una conciencia más fuerte sobre la importancia que tienen los sistemas de gestión de la seguridad, no solo como parte de un elemento esencial que permite a nivel legal el funcionamiento de la misma, sino hacer a la empresa más competitiva tanto a nivel nacional como internacional, y hacerla visible como poseedor de buenas prácticas, lo que ayudara a conseguir más clientes y proveedores que permitan que el servicio de liquidación de aportes a seguridad social sea más efectivo y que los objetivos propuestos tanto por la alta dirección como los stakeholders se consigan de la mejor amera posible.

La norma ISO 27001 conforma un marco de trabajo para definir un SGSI, centrándose en la visión de la gestión de la seguridad como algo continuo en el tiempo. Es imprescindible analizar y gestionar los riesgos a los que se expone una organización en relación con sus diferentes procesos. Al tiempo que se han identificado potenciales riesgos que afecten a la organización , es importante establecer la estrategia a tomar para cada uno de ellos, ya sea traspasar el riesgo a terceros; evitar el riesgo, abandonando la actividad que lo genera cuando el riesgo exceda a los beneficios que aporta; asumir el riesgo, cuando el establecimiento de las medidas supere el coste que pueda suponer la materialización del mismo; gestionar el riesgo, mediante medidas que mitiguen el riesgo, reduciendo la probabilidad de que se materialicen las consecuencias que de éste puedan resultar.

8.1 OBJETIVOS ESPERADOS

El desarrollo e implementación de este Plan Director de Seguridad de la Información ha mejorado notablemente el nivel que existía en la empresa en materia de seguridad.

Ahora se cuenta con un análisis real de la empresa, en base a la norma ISO 27001:2013, sobre el que ir trabajando y mejorando de manera continuada. Se ha definido el alcance del SGSI respecto

a la compañía para definir aquellos procesos organizativos y funcionales a los que debe afectar el sistema de gestión por ser contenedores activos de información que requieren ser protegidos.

Se ha establecido una metodología de gestión de la seguridad clara y estructurada. Se han generado los diferentes documentos o procedimientos que establece la norma:

- Política de seguridad
- Procedimiento de auditorías internas
- Gestión de indicadores
- Procedimiento de revisión de la dirección
- Gestión de roles y responsabilidades
- Metodología de análisis de riesgos
- Declaración de aplicabilidad

Se ha hecho un inventario de activos actualizado y se ha analizado y detallado este inventario. Se ha identificado a los propietarios de cada activo, su valoración cuantitativa y también criticidad por activo en referencia a las dimensiones de seguridad.

Se ha hecho un estudio, en base a la metodología de análisis de riesgos definida en la norma ISO 31000, y considerando elementos de otras metodologías como Magerit, de las amenazas a las que están expuestos dichos activos. Igualmente se ha hecho un estudio de su impacto potencial de esas amenazas en los activos. Se ha identificado al propietario del riesgo.

Con estos datos y apoyado en el código de buenas prácticas que establece la norma ISO 27002:2013 se ha realizado un plan de acción con un listado de proyectos cuya ejecución mejora el nivel de seguridad de esos activos hasta un nivel aceptado por la dirección de la compañía, al que se denomina riesgo residual.

El plan de auditorías internas de cumplimiento nos servirá para obtener una imagen del nivel de evolución del SGSI en la compañía, como medio para poder lograr a medio plazo una adecuación total y cumplir con los requerimientos legales para el funcionamiento del negocio de liquidación PILA.

Aunque hay muchos aspectos que cubrir y otros que mejorar, se ha podido comprobar desde que se comenzó el trabajo hasta este punto final que ha habido una evolución y una madurez notable en la compañía respecto a la gestión de la seguridad de la información, lo que vaticina que si sigue en esta línea vaya a lograr cumplir completamente con los requerimientos establecidos en la norma ISO 27001.

8.2 OBJETIVOS A FUTURO

Se debe seguir trabajando en mantener en nivel de madurez en aquellos dominios que ya cumplen con los requisitos de la norma.

Se debe realizar un plan de acción con un conjunto de proyectos que sirvan para ir madurando aquellos dominios que están todavía en unos niveles de incumplimiento respecto a la norma. Si bien hay limitaciones a nivel humano y financiero que impiden para poder alcanzar los objetivos a corto plazo, el proceso irá evolucionando en el tiempo hasta al proceso de evolución continua que mantenga el nivel adecuado de madurez se le vayan agregando el resto de los apartados y dominios que establece la norma.

Se deberá incidir de manera intensa en llevar a cabo el cumplimiento de los controles asociados a los dominios cuyo grado de madurez es aún muy bajo e insistir y potenciar aquellos controles que dotarían de un nivel óptimo a aquellos dominios de la norma que están en una fase mejorada de madurez.

Finalmente, se debe asegurar que los funcionarios tomen conciencia de la importancia de la seguridad de la información y como esta es un elemento transversal para la consecución de los objetivos de la compañía y permite que el crecimiento de esta se logre acorde a las estrategias definidas por la alta gerencia.

9. APENDICE

9.1 GLOSARIO

Aceptación de riesgo: Decisión de asumir un riesgo.

Activo de Información: Elemento que tiene valor para la entidad o el individuo en términos de información.

Alta dirección: Se les denomina a los directivos con más alto cargo en la organización y está conformado en el siguiente orden jerárquico que es: Gerente General, Gerentes de las distintas áreas.

Análisis de Riesgo: Proceso por el cual se estima la probabilidad y el impacto de los riesgos identificados.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución, con el fin de garantizar el origen de la información, validando el emisor para evitar suplantación de identidad.

BYOD: Bring Your Own Device (BYOD), “trae tu propio dispositivo”, hace referencia a una tendencia en la cual los empleados tienen la posibilidad de llevar y utilizar sus propios dispositivos (Smartphone y tabletas) para acceder a los recursos de la compañía.

Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Propiedad que determina que la información no sea accesible ni divulgada a individuos, organizaciones o procesos no autorizados.

Debilidad de seguridad de la información: Es la falencia o carencia de un control (vulnerabilidad) en un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.

Disponibilidad: Propiedad de que la información sea accesible y utilizable para las personas autorizadas.

Dispositivos móviles: Son los elementos como portátiles, tabletas, cámaras fotográficas, teléfonos inteligentes o Smartphone, entre otros que pueden salvaguardar, controlar, transferir y movilizar información o datos.

Escritorio limpio: Control para la protección de los papeles y dispositivos removibles de almacenamiento de información, dispuestos en estaciones de trabajo para evitar accesos no autorizados, perdida y/o daño de la información durante y fuera de las horas laborales.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información: Es la posibilidad de ocurrencia de cualquier tipo de acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema o proceso.

Gestión del riesgo: Actividades coordinadas para dirigir, controlar y monitorear una organización en relación con el riesgo.

Incidente de seguridad de la información: Es indicado por un único o una serie de eventos de seguridad de la información indeseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.

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

Información en reposo: Datos guardados en dispositivos de almacenamiento persistente (por ejemplo, cintas, copias de seguridad externas, dispositivos móviles, discos duros, entre otros).

Información en tránsito: Información que fluye a través de la red pública, como Internet, y los datos que viajan en una red privada, como una red de área local (LAN) corporativa o empresarial.

Medios removibles: Son los elementos de almacenamiento como unidades Flash, memorias USB, Discos Duros, CD, DVDs, tarjetas de memoria, Token, PKI, entre otros que pueden salvaguardar información y son fáciles de transportar y remover.

Pantalla limpia: Control para la protección de documentos electrónicos dispuestos en el escritorio del sistema operativo con el fin de evitar acceso no autorizados, perdida y/o daño de la información.

Plan Táctico: Es una forma de ejecutar los planes que no requieren administrarse como proyectos debido a su complejidad, la inversión y la duración.

Proyecto: Es todo aquello que emprende la organización con el fin de realizar una optimización, mejora o implementación que requiere inversión o implementación de nuevos negocios, o tecnologías.

Resiliencia: Es la capacidad de un mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que pudo estar sometido.

Riesgo: Posibilidad de ocurrencia de toda aquella situación que pueda entorpecer el normal desarrollo de las funciones de la compañía y le impidan el logro de sus objetivos.

Riesgo de Seguridad de la Información: Es una serie de amenazas, que pueden vulnerar los sistemas de información y afectar los activos de información de la organización pudiendo generar impactos negativos en la empresa.

Riesgo inherente: Es el riesgo a que se somete la compañía en ausencia de acciones para reducir la probabilidad de ocurrencia o el impacto.

Riesgo residual: Es el riesgo a que se somete la compañía en ausencia de acciones para reducir la probabilidad de ocurrencia o el impacto.

Riesgo aceptado: La cuantía más amplia de riesgo que la compañía está dispuesta a asumir para realizar su misión y lograr la visión.

Seguridad de la Información: Es la implementación de medidas en aras de preservar de forma íntegra, disponible y confiable la información de la organización

Seguridad informática: Conjunto de métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información en formato digital que éstos almacenen.

Sistema de gestión de la seguridad de la información: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales que se utilicen en la organización.

Tecnología de la Información: Se refiere al hardware y software operado por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la organización.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejora que permiten mitigar el riesgo.

Valoración del riesgo: Es el resultado de confrontar la evaluación del riesgo con los controles existentes.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio.

9.2 BIBLIOGRAFIA

International Standards Organization, ISO/IEC 27001: Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la seguridad de la Información (SGSI) – Requisitos.

International Standards Organization, ISO/IEC 27002: Tecnología de la Información – Técnicas de Seguridad – Código de práctica

Sistema de gestión de la seguridad de la información (Silvia Garre Guí y Daniel Cruz Allende) – Material docente de la UOC.

9.3 REFERENCIAS WEB

https://www.pmg-ssi.com/2013/12/iso27001-origen/

https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/nueva_version_iso27001

https://advisera.com/27001academy/

http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/

http://www.iso27000.es/download/doc_sgsi_all.pdf

https://www.ceupe.com/blog/estructura-de-la-norma-iso-27001-2013.html

https://es.wikipedia.org/wiki/ISO/IEC_27002

http://www.iso27001standard.com/

http://es.wikipedia.org/wiki/British_Standards_Institution

http://www.iso27000.es/glosario.html

http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf