Presentación a la Dirección

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

Máster Universitario en Seguridad de las TIC (MISTIC)
Estudiante: José Alejandro Rincón Rodríguez
Director: Antonio José Segovia Henares
Diciembre 2019

INDICE

1. Objetivo del Proyecto

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).

Para ello se tendrán en cuenta cuatro aspectos fundamentales:

- Conocimiento de la estrategia y objetivos de la organización
- Conocimiento de la situación actual en seguridad de la información
- Elaboración de propuestas y proyectos para mejorar los niveles de SI
- Evaluación del estado actual de al seguridad teniendo en cuenta los niveles de madurez de la organización.

2. Metodología

Se ha establecido como base metodológica para el desarrollo de este proyecto los siguientes elementos:

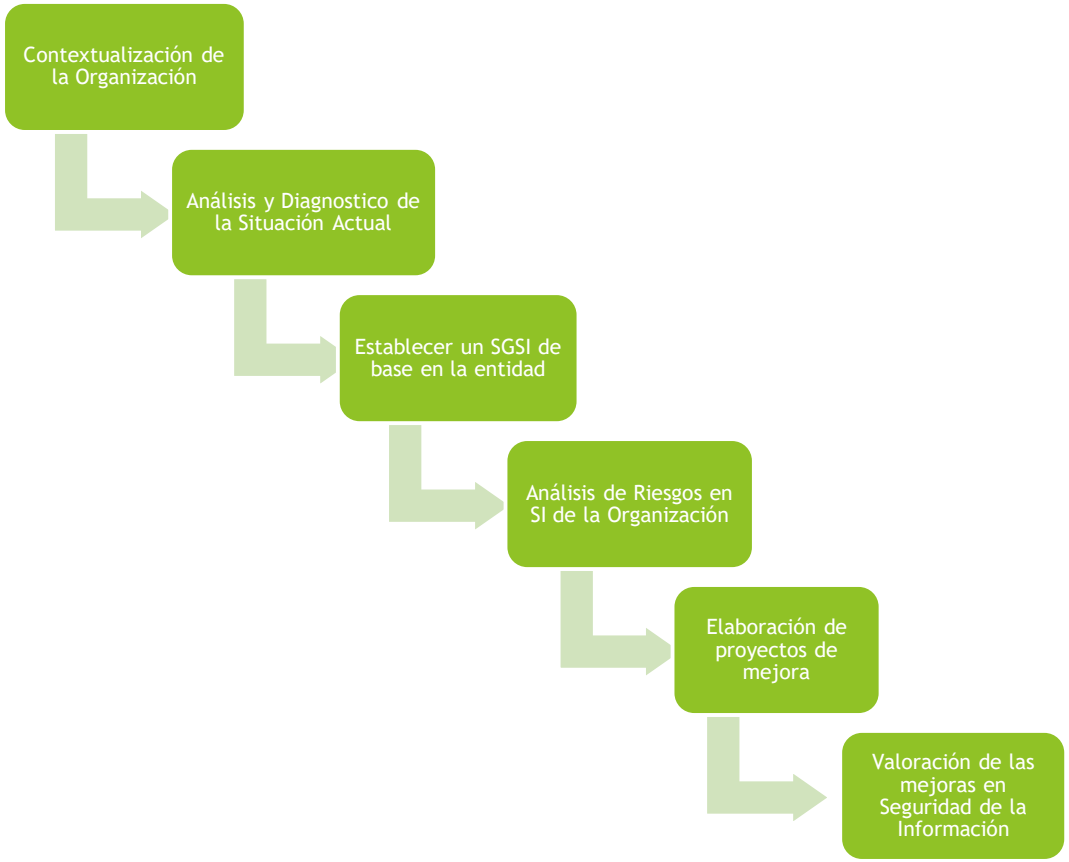
Norma ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información (SGSI) - Requisitos

Norma ISO/IEC 27002– Código de Prácticas para los controles de seguridad de la Información

Capability Maturity Model Integration (CMMI) -Modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software

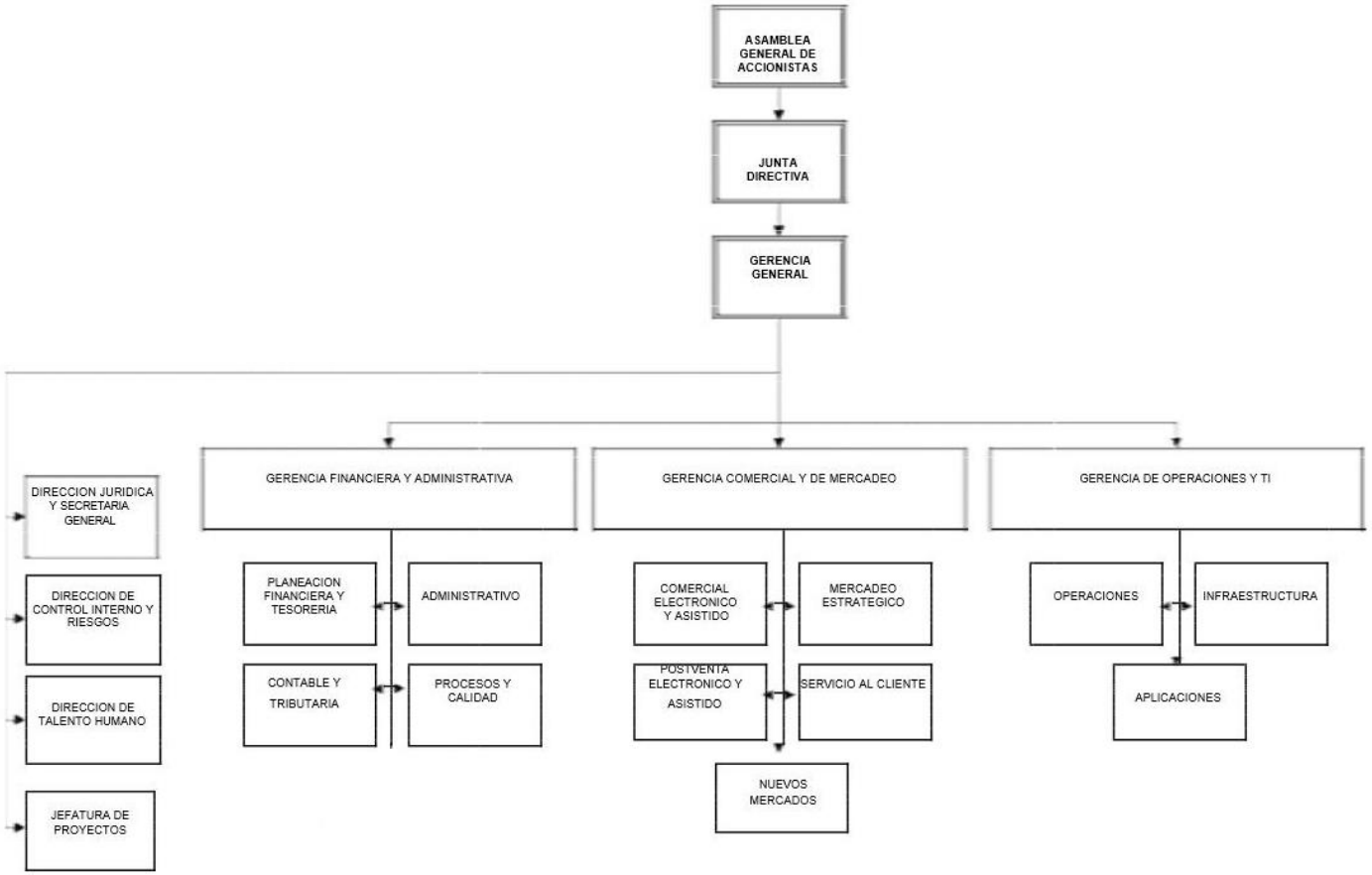
3. Descripción del Proyecto

El Proyecto se desarrollara tendiendo en cuenta las siguientes fases:



4. Contextualización de la Organización

Estructura Organizacional



4. Contextualización de la Organización

Objetivos del Plan Director de Seguridad

- 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.

4. Contextualización de la Organización

Objetivos de Seguridad de la Información

- 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.

5. Análisis y Diagnostico de la situación Actual

Análisis y Diagnostico de la Situación Actual

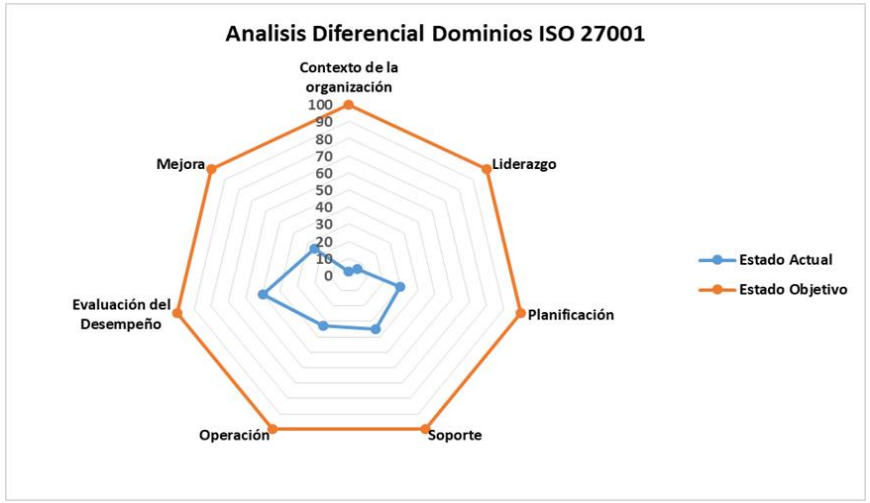
- Análisis y Diagnostico del estado actual de la Seguridad de la Información
- Estructura Organizacional, políticas y procedimientos existentes, etc.
- Practicas en seguridad, Controles de Seguridad Implementados, etc.

Informe de estado de la situación de la seguridad de la Información (Análisis Diferencial)

5. Análisis y Diagnostico de la situación Actual

Informe de Análisis Diferencial - Dominios

Dominio	Porcentaje de Efectividad	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**

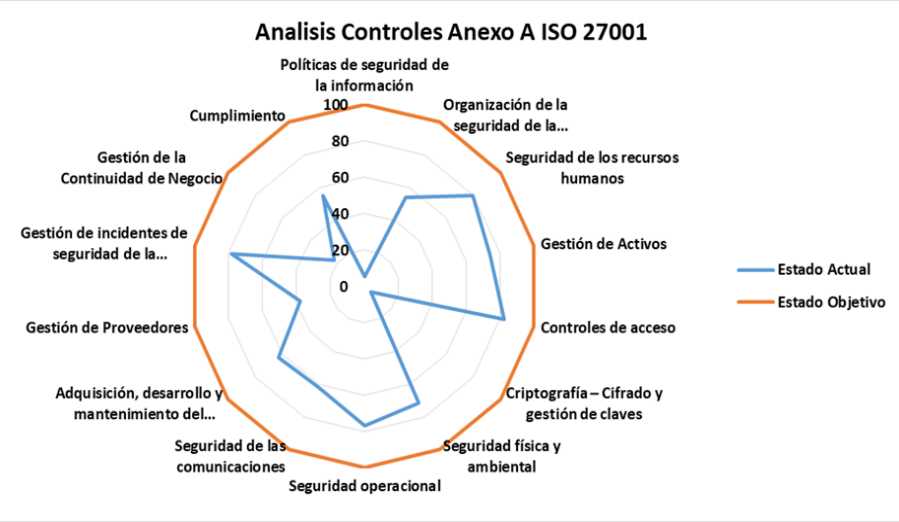


La gestión de la norma está en una fase **INICIAL**, ya que no hay implementada una política del SGSI en la organización, por lo cual no se tiene establecidos sus límites y alcance, adicionalmente no se tiene un alto compromiso de la dirección y las partes interesadas en la gestión de la Seguridad de la información.

5. Análisis y Diagnostico de la situación Actual

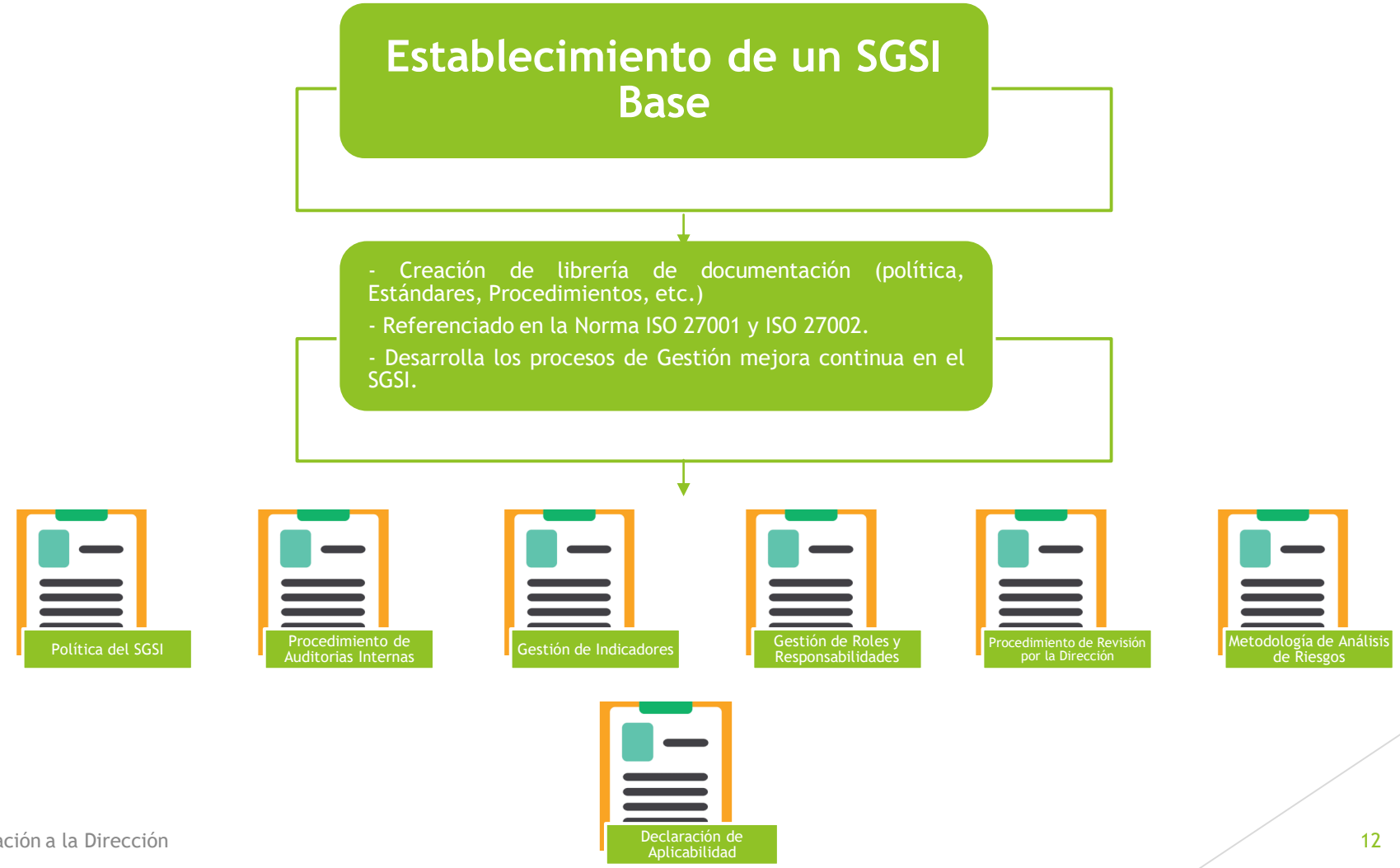
Informe de Análisis Diferencial - Controles

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**

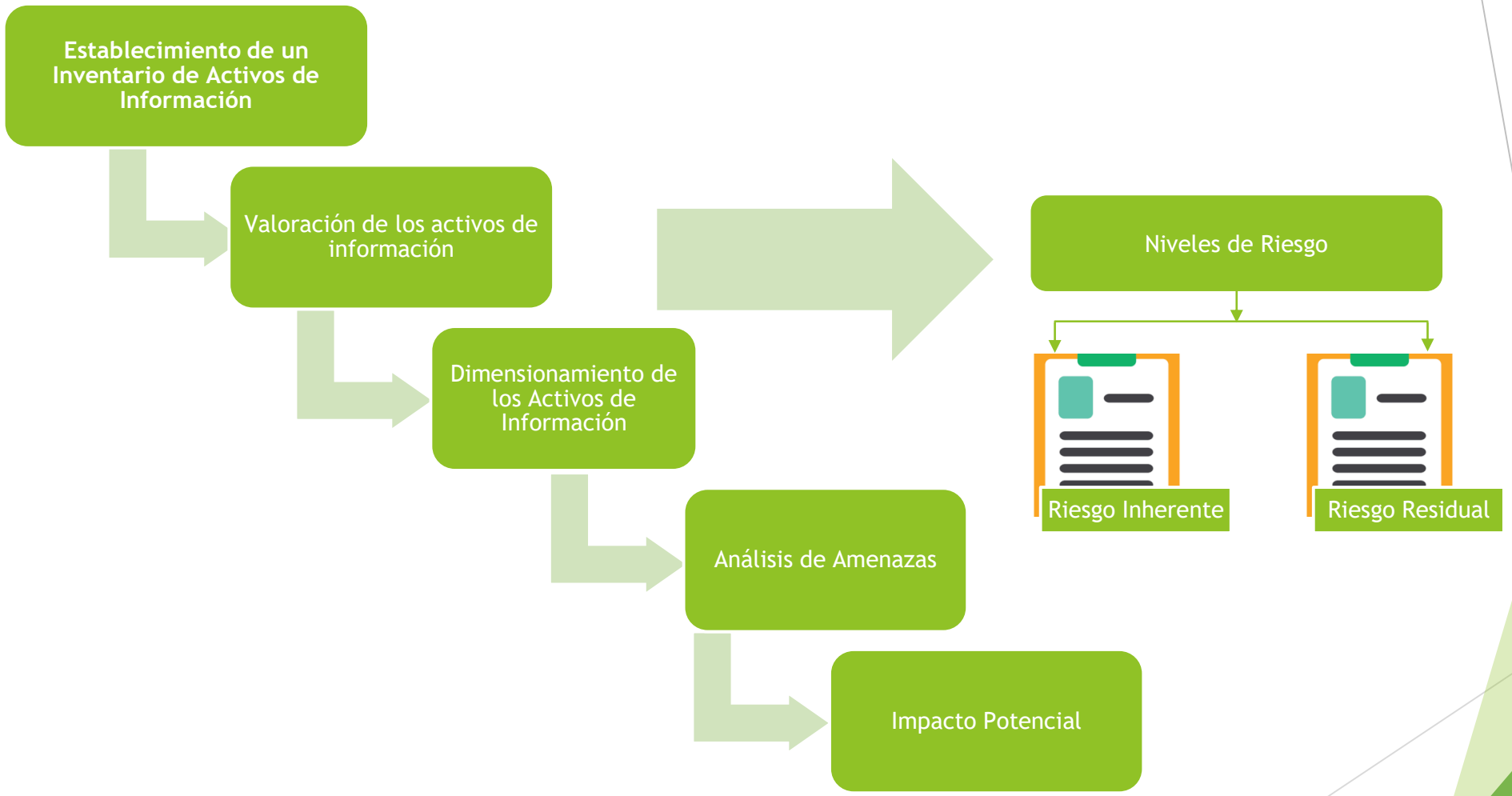


La situación actual refleja que la gestión de la norma está en una fase **MANEJADA**, aunque hay cuatro dominios que están una fase inicial: Políticas de seguridad de la información, ya que las políticas como tal no están definidas, Criptografía y manejo de claves, ya que no se tiene implementada una 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.

6. Establecer un SGSI de base en la Organización



7. Análisis de Riesgos en SI de la Organización



7. Análisis de Riesgos en SI de la Organización

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 área jurídica	Sala de departamento de desarrollo de software	Sala de departamento de Infraestructura Tecnológica	Despacho del Gerente General	Despacho del Gerente de Proyectos	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 (1)	Profesional Administrativo (1)	Pro
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	

7. Análisis de Riesgos en SI de la Organización

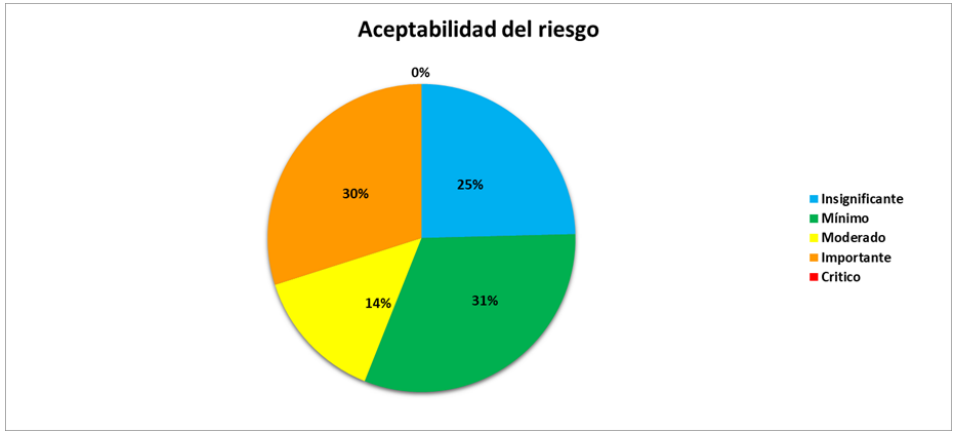
Amenaza/Activo	Frecuencia	Impacto Dimensiones					
		C	I	D	E	F	O
Centro de procesamiento de Datos/Fuego	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Daños por Agua	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Tormenta eléctrica	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Terremoto	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Fuego	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Daños por Agua	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Sobrecarga eléctrica	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Explosión	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Derrumbe	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Contaminación mecánica	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Centro de procesamiento de Datos	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Avería de origen física o lógica	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Corte eléctrico	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Condiciones inadecuadas de temperatura y/o humedad	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Fallo del servicio de comunicaciones	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Interrupción de otros servicios y suministros esenciales	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Degradación de los soportes de almacenamiento de la información	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Errores de los técnicos de TI	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Errores de monitorización (log)	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Errores de configuración	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Deficiencias en la organización	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Escapes de información	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Alteración accidental de la información	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Destrucción de información	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Fugas de información	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Vulnerabilidad de los programas (software)	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Errores de mantenimiento / actualización de programas (software)	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Errores de mantenimiento / actualización de equipos (hardware)	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Caída del sistema por agotamiento de recursos	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Pérdida de equipos	0,5	0,75	0,75	0,75	0,5	0	0,5
Centro de procesamiento de Datos/Indisponibilidad del personal	0,5	0,75	0,75	0,75	0,5	0	0,5

7. Análisis de Riesgos en SI de la Organización

Amenaza/Activo	Probabilidad	Impacto	Riesgo
Centro de procesamiento de Datos/Fuego	3	3	9
Centro de procesamiento de Datos/Daños por Agua	1	3	3
Centro de procesamiento de Datos/Tormenta eléctrica	3	3	9
Centro de procesamiento de Datos/Terremoto	1	3	3
Centro de procesamiento de Datos/Fuego	3	3	9
Centro de procesamiento de Datos/Daños por Agua	1	3	3
Centro de procesamiento de Datos/Sobrecarga eléctrica	3	3	9
Centro de procesamiento de Datos/Explosión	1	3	3
Centro de procesamiento de Datos/Derrumbe	1	3	3
Centro de procesamiento de Datos/Contaminación mecánica	2	3	6
Centro de procesamiento de Datos/Contaminación electromagnética	2	3	6
Centro de procesamiento de Datos/Avería de origen física o lógica	4	3	12
Centro de procesamiento de Datos/Corte eléctrico	4	3	12
Centro de procesamiento de Datos/Condiciones inadecuadas de temperatura y/o humedad	3	3	9
Centro de procesamiento de Datos/Fallo del servicio de comunicaciones	4	3	12
Centro de procesamiento de Datos/Interrupción de otros servicios y suministros esenciales	4	3	12
Centro de procesamiento de Datos/Degradación de los soportes de almacenamiento de la información	3	3	9
Centro de procesamiento de Datos/Errores de los técnicos de TI	5	3	15
Centro de procesamiento de Datos/Errores de monitorización (log)	3	3	9
Centro de procesamiento de Datos/Errores de configuración	2	3	6
Centro de procesamiento de Datos/Deficiencias en la organización	5	3	15
Centro de procesamiento de Datos/Escapes de información	4	3	12
Centro de procesamiento de Datos/Alteración accidental de la información	3	3	9
Centro de procesamiento de Datos/Destrucción de información	2	3	6
Centro de procesamiento de Datos/Fugas de información	5	3	15
Centro de procesamiento de Datos/Vulnerabilidad de los programas (software)	3	3	9
Centro de procesamiento de Datos/Errores de mantenimiento / actualización de programas (software)	4	3	12
Centro de procesamiento de Datos/Errores de mantenimiento / actualización de equipos (hardware)	4	3	12

7. Análisis de Riesgos en SI de la Organización

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



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

8. Evaluación de Proyectos de mejora

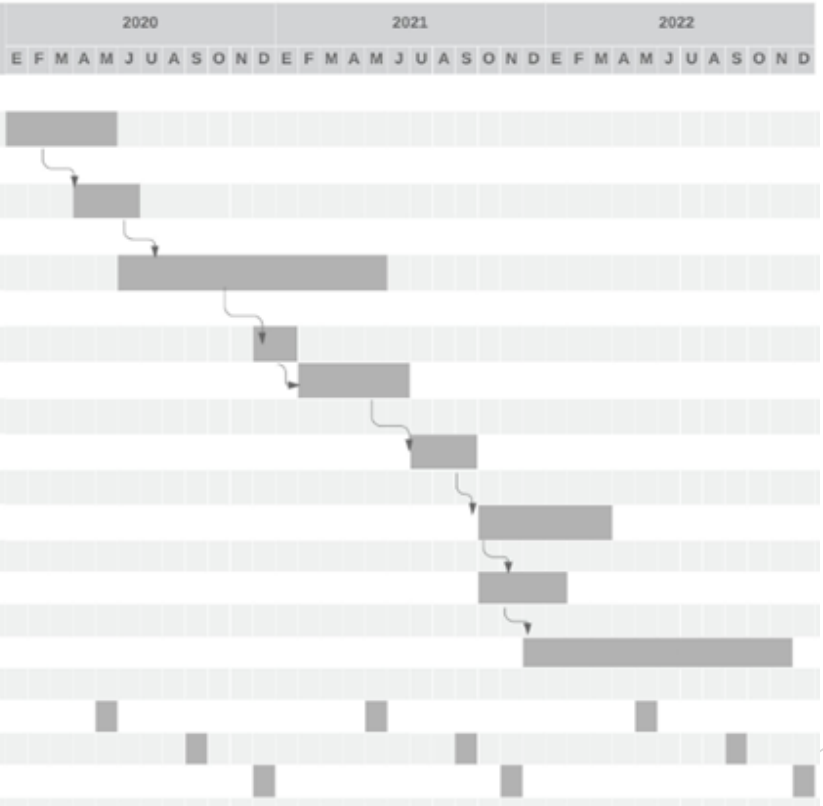
Se proponen los siguientes planes de acción y/o proyectos que buscan minimizar cada una de las amenazas identificadas en la fase anterior.

- 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

8. Evaluación de Proyectos de mejora

Planificación Global de los Proyectos

Proyecto	Duración	Fecha de Inicio	Fecha Finalización	Propietario	Dependencia
Implementación Politicas SGSI	5	1/1/2020	31/5/2020		
Implementación Politicas SGSI	5	1/1/2020	31/5/2020	OFS, GG, AD	
Implementación Area de Seguridad	3	1/4/2020	30/6/2020		
Implementación área de Seguridad	3	1/4/2020	30/6/2020	DH, GG	
Implementación Comité de Seguridad	12	1/6/2020	31/5/2021		
Implementación Comité de Seguridad	12	1/6/2020	31/5/2021	OFS, AS	
Cifrado de la Información	8	1/12/2020	30/6/2021		
Elaboración Política de Cifrado	2	1/12/2020	28/12/2021	OFS	
Implementación Cifrado	6	1/3/2021	31/7/2021	JIT, GOT	
Política de Gestión de Proveedores	3	1/07/2021	30/9/2021		
Política de Gestión de Proveedores	3	1/07/2021	30/9/2021	OFS, GAF	
Fortalecimiento Vulner. Software	6	1/10/2021	31/3/2022		
Fortalecimiento Vulner. Software	6	1/10/2021	31/3/2022	OFS, GOT	
Plan de Mejora Centro de Datos	4	1/10/2021	28/2/2022		
Plan de Mejora Centro de Datos	4	1/10/2021	28/2/2022	OFS, GOT	
Plan de Continuidad de Negocio	12	1/11/2021	1/11/2022		
Plan de Continuidad de Negocio	12	1/11/2021	1/11/2022	OFS, GOT	
Formación en seguridad de la Info	3	1/05/2020	1/05/2022		
Capacitación 1	1	1/05/2020	1/05/2022	OFS	
Capacitación 2	1	1/05/2020	1/05/2022	OFS	
Capacitación 3	1	1/05/2020	1/05/2022	OFS	



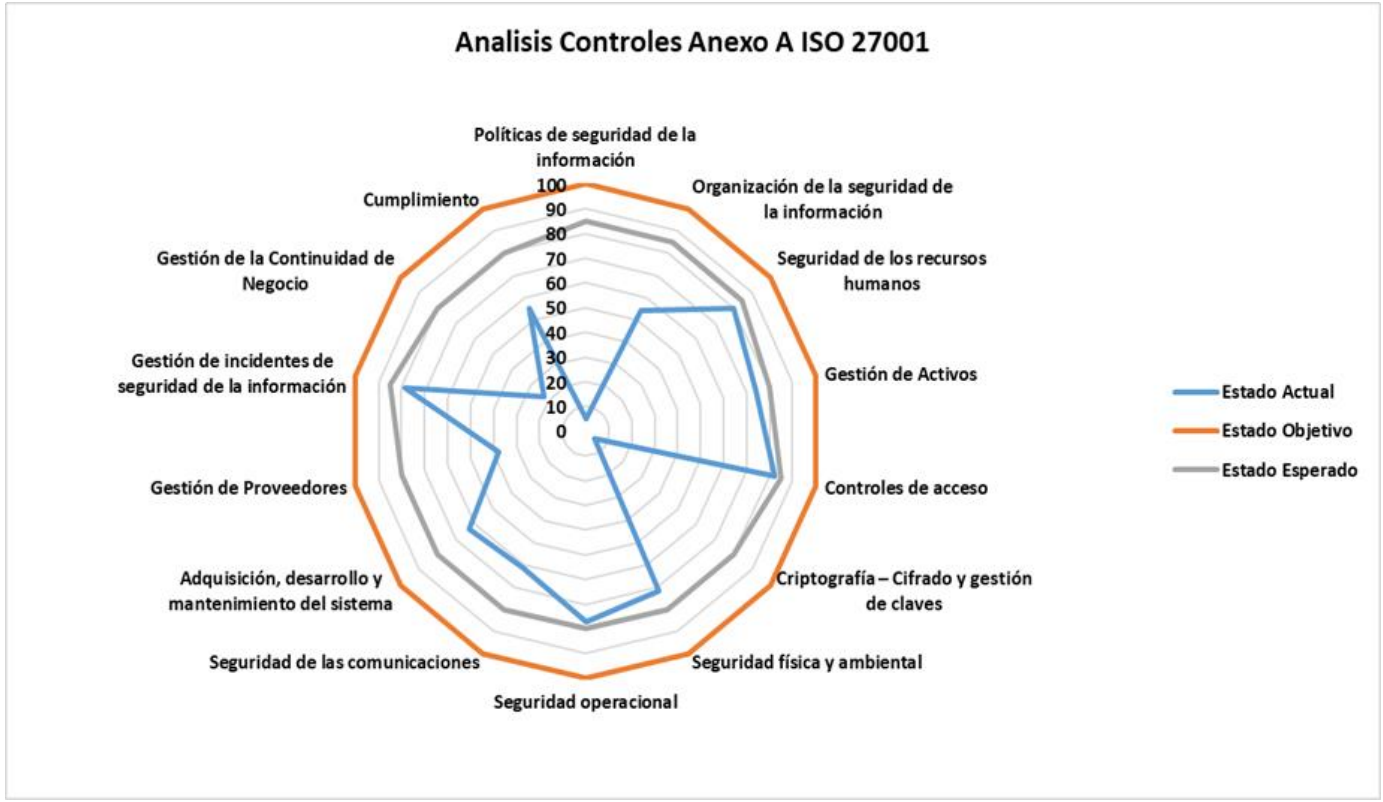
8. Evaluación de Proyectos de mejora

Análisis Diferencial Deseable tras la ejecución de los Proyectos

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**

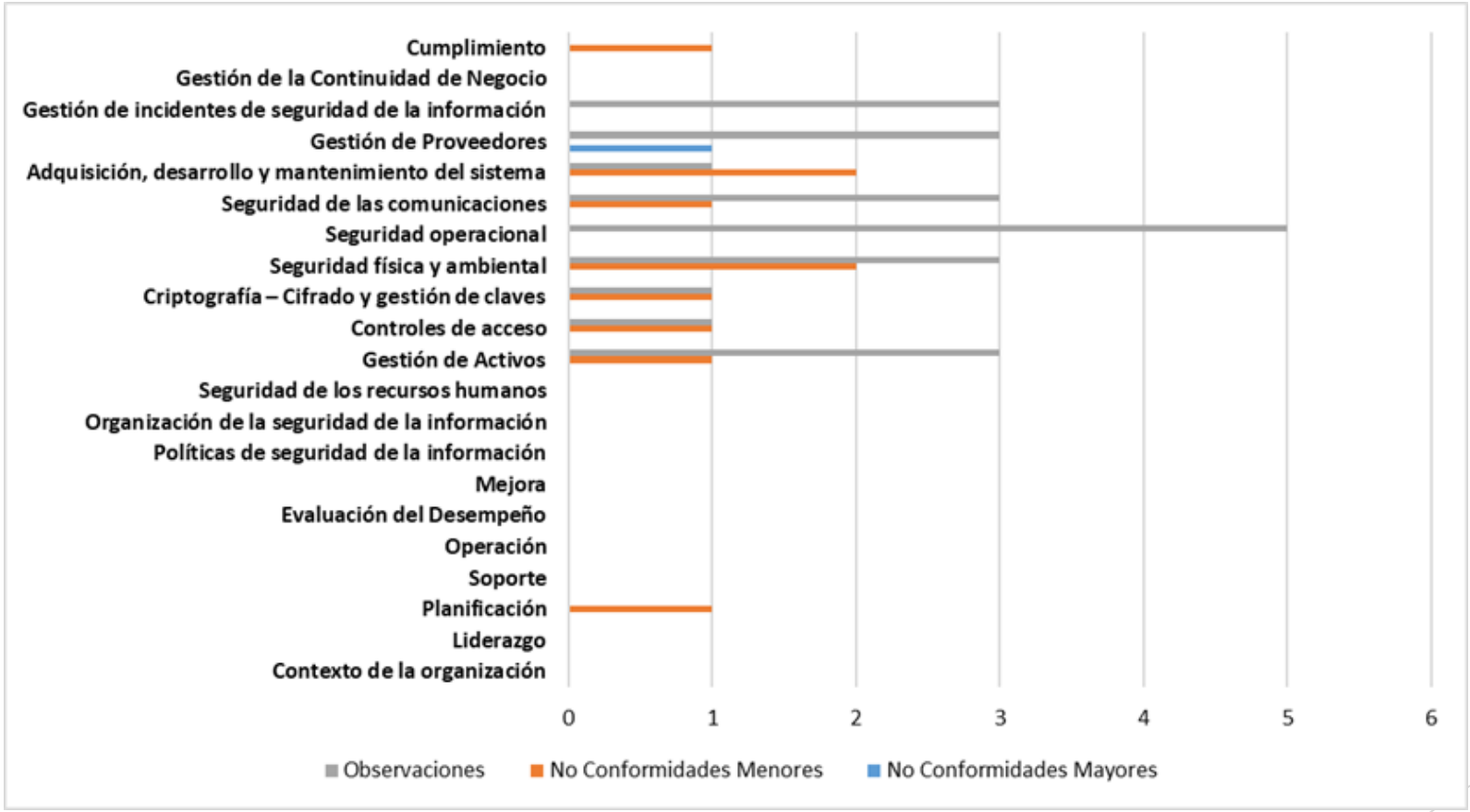
8. Evaluación de Proyectos de mejora

Análisis Diferencial Deseable tras la ejecución de los Proyectos



9. Valoración de la mejora de la seguridad de la Información

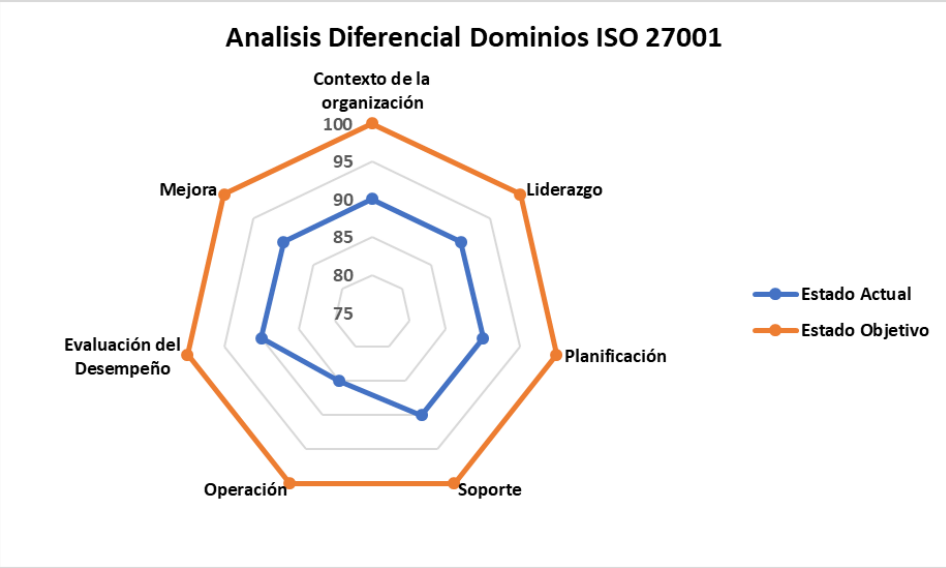
Desviaciones identificadas en el Análisis diferencial



9. Valoración de la mejora de la seguridad de la Información

Análisis Diferencial tras la ejecución de los Proyectos - Dominios

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**

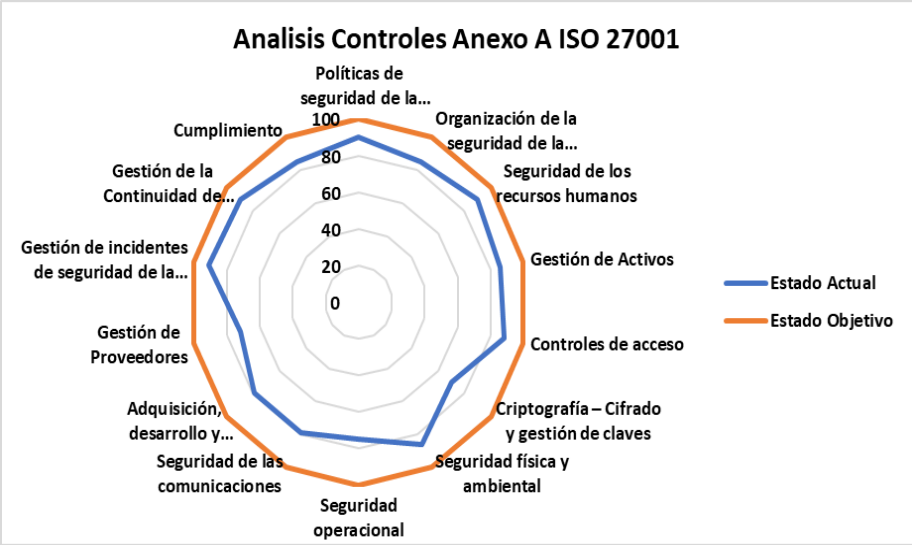


La situación actual refleja que la gestión de la norma está en una fase **DEFINIDA**, por lo cual hay un buen grado de madurez implementado, y por lo cual, los objetivos de los proyectos definidos en la fase anterior surgieron efectos positivos.

9. Valoración de la mejora de la seguridad de la Información

Análisis Diferencial tras la ejecución de los Proyectos - Controles

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**



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 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.

Muchas gracias por su atención