Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013

Trabajo final de maestría
Sistemas de Gestión de seguridad

RICARDO PULGARÍN GÓMEZ

MISTIC: Máster interuniversitario de seguridad de las tecnologías de la información y de las comunicaciones (UOC-UAB-URV)

Director TFM: Antonio José Segovia Henares
Diciembre de 2014

A mi esposa, por su paciencia, apoyo constante y amor incondicional que me brindó siempre para la realización de este proyecto.

"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los equipos"
Kevin Mitnick

Resumen:

En el presente proyecto, se analiza una empresa Colombiana del sector agropecuario con más de 5000 empleados a nivel nacional. Se plantea a implementación de un sistema de gestión de seguridad de la información basado en los requerimientos de la norma ISO/IEC 27001:2013 y la planeación de la implementación de los controles de la ISO/IEC 27002:2013. La empresa solo tiene un oficial de seguridad informática y no cuenta con una estrategia de seguridad de la información. Se realiza toda la propuesta de implementación para sustentar la necesidad de implantar un SGSI a corto plazo.

Absract

In this project, a Colombian company of the agricultural sector with over 5,000 employees nationwide is analyzed. It is planned to implement a management system for information security based on the requirements of ISO/IEC 27001:2013 and planning the implementation of the controls proposed by the ISO / IEC 27002: 2013. The company has only one official computer security and does not have a strategy for information security. Full implementation proposal is made to support the need to implement an ISMS short term.

CONTENIDO

1. INTRODUCCIÓN

La ISO 27001 expresa que un Sistema de Gestión de la Seguridad de la Información, *es un sistema de gestión que comprende la política, estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Este sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.). Este sistema proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización.*

Entendiendo la gestión de la seguridad de la información como un proceso sistemático documentado y que debe ser implantado en toda la organización, el presente Plan de Seguridad de la Información reúne la definición de la política y objetivos de seguridad, el análisis diferencial de la empresa respecto a la ISO/IEC 27001:2013 e ISO/IEC 27002:2013, el análisis de riesgos y la selección de salvaguardas, como un procedimiento corporativo alineado a los objetivos de negocio de una empresa en Colombia, junto con la propuesta de proyectos de mejora en respuesta a los objetivos estratégicos, no para garantizar la seguridad de la información, sino para proporcionar en conjunto los elementos de control que permitan reducir la aparición de incidentes o la reacción adecuada y eficiente en caso que ocurran, minimizando así su impacto.

2. CONTEXTUALIZACIÓN

A continuación se indicarán los detalles importantes de la empresa que permitirán comprender el enfoque del Plan Director de Seguridad a desarrollar.

2.1. LA EMPRESA

Es una institución sin ánimo de lucro que de forma democrática representa nacional e internacionalmente los intereses del gremio de productores colombianos de café, de manera que sean ellos mismos quienes lleguen a consensos necesarios para definir programas de beneficio común. Desarrolla políticas y estándares de calidad que aseguran el futuro del negocio orientando, organizando, fomentando y regulando la caficultura colombiana. Gestiona programas como la investigación científica para optimizar costos de producción y maximizar la calidad del fruto, la asistencia a los productores con el servicio de técnicos en el campo de sembrado, la regulación y comercialización del producto para optimizar el precio pagado al productor, promueve la exportación y la ejecución de programas gremiales de carácter económico, científico, tecnológico, industrial y comercial, entre otros.

Para llevar a cabo todas estas actividades, la institución cuenta con unidades de apoyo que prestan servicios a los cafeteros, como una fundación, un centro de investigación y las cooperativas de caficultores ubicadas en los municipios productores de todo el país, agrupados en comités departamentales. A su vez, cuenta filiales que representan sus Unidades Estratégicas de Negocio, como las tiendas de artículos y comestibles derivados del café, y los centros de almacenaje y comercialización de café.

La estructura de organización por procesos está representada en el siguiente gráfico.

Ilustración 1. Estructura de organización por procesos

La dirección administrativa de la institución, la fundación, el centro de investigación y de las dos filiales comercializadoras se encuentran centralizadas en la ciudad de Bogotá DC, desde donde se generan las directrices para los comités, fábricas, tiendas y oficinas a nivel nacional. Están ubicadas en un edificio con un departamento de tecnología y un centro de cómputo transversal para todas las empresas. Para el apoyo a los procesos críticos, la compañía cuenta con aplicaciones tanto *web based* como *client/server* están disponibles para más de 2000 los usuarios a nivel nacional a través de una WAN corporativa con la que se interconectan todas las oficinas por donde algunas salen a internet a través del canal de oficina central. Además, la organización dispone de portales transaccionales para miles de usuarios que acceden a través de internet, todos estos implementados en plataformas de diferentes sistemas operativos, tanto *Unix* como *Windows*. Las aplicaciones web más críticas para el negocio son las de geolocalización de terrenos, cultivos y subsidios de apoyo a los caficultores, luego del servicio de correo electrónico y el sistema contable/comercial. Por último, cabe destacar el servidor de

repositorio centralizado de archivos al cual tienen acceso todos los usuarios de la oficina central donde residen todas las empresas.

En el siguiente diagrama de red de alto nivel se puede apreciar cómo están interconectadas las redes y subredes y como salen a internet.

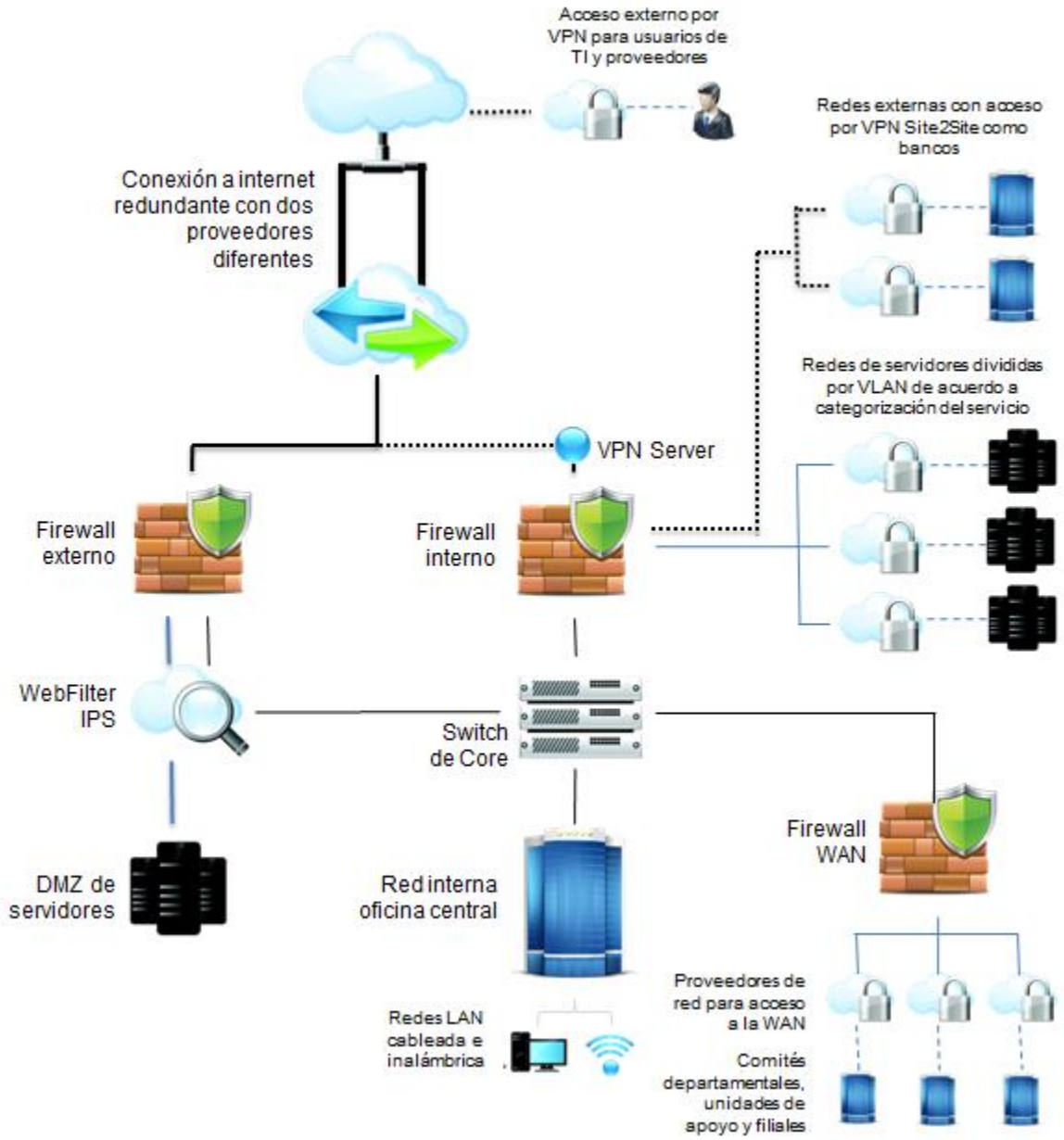

Ilustración 2. Diagrama de red de alto nivel

Esta infraestructura hasta hace 2 años, era administrada remotamente por un *bestshore*[1] localizado en Argentina. Actualmente el departamento de TI para aplicaciones e infraestructura se encuentra en sitio conformado por un equipo multidisciplinario de especialistas que se encargan de la gestión y por su parte, la gerencia de tecnología se encuentra adelantando un proceso de modernización de las plataformas y de implementación de buenas prácticas de gerencia de TI debido a que no recibió una documentación organizada del estado de los sistemas por parte del *bestshore* que pudiera plantear una estrategia de TI que evolucionara a corto y mediano plazo con las necesidades del negocio.

A este esfuerzo, se suma la necesidad de implementar una estrategia de permisos de acceso a los recursos compartidos basados en el principio de menor privilegio acorde al rol de cada funcionario de cada empresa, la gestión de riesgos de las plataformas alineados a las necesidades del negocio y el fomento de una cultura organizacional sobre el manejo de la información.

2.2. ALCANCE DEL PLAN DE SEGURIDAD

El Plan de Director se desarrollará para los activos información que estén a cargo de la Dirección de Tecnología de la información y que se encuentran en la infraestructura local de la Oficina Central para los usuarios de institución que estén ubicados en el edificio de la Oficina Central y que no pertenezcan o sean administrados por funcionarios de sus filiales o empresas asociadas. Se limitará a la infraestructura de los sistemas de información que soporten los procesos operativos o de los cuáles sea responsable por su funcionamiento exclusivamente la “Unidad de Apoyo - Tecnología de la Información” de Oficina Central de acuerdo con la Declaración de Aplicabilidad, versión 1.0.

[1] *Bestshoring*: mover los procesos o componentes de negocio a localidades o países que brinden la mejor relación costo-beneficio. Fuente: http://en.wikipedia.org/wiki/Bestshoring

3. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

3.1. OBJETIVOS GENERALES

- Estructurar el gobierno de TI de Oficina Central para que sean integradas las estrategias de la Dirección de Seguridad de la Información organizadas en un Sistema de Gestión de Seguridad de la Información acorde a los requerimientos especificados en la norma ISO/IEC 27001:2013 que puedan servir de ejemplo para ser implementado en sus filiales y empresas asociadas
- Proponer la implementación de controles de acuerdo a las recomendaciones de la ISO/IEC 27002:2013 que reduzcan los riesgos en las 5 dimensiones de seguridad para aquellos activos de información que sean administrados por la Dirección de TI de Oficina central.
- Generar confianza a las directivas, los funcionarios y asociados de la compañía en los sistemas de información y en la información que estos producen.
- Tener un programa de auditoría del SGSI que promueva su mejora y respalde la gestión de la Dirección de TI de Oficina Central

3.2. OBJETIVOS ESPECÍFICOS

La dirección de TI, consciente que los riesgos de seguridad de la información identificados pueden llegar a afectar la productividad, la buena imagen y la actividad operativa de la compañía, promueve la implementación de las mejores prácticas de la industria para llevar a cabo su operación. Para esto, se propone el cumplimiento de los requisitos de la norma ISO/IEC 27001:2013 y la implementación de controles de acuerdo a las recomendaciones de la norma ISO/IEC 27002:2013.

[OBJ-01] Alinear los procesos de la Dirección de TI de Oficina Central para cumplir con los requisitos de la norma ISO/IEC 27001:2013 y gestionar su respectiva documentación y divulgación.

[OBJ-02] Implementar los controles definidos en el documento Declaración de Aplicabilidad V1.0 en los procesos gestionados por la Dirección de TI, recursos humanos y bienes y servicios de Oficina central, con seguimientos mensuales que evalúen el grado de implementación.

Para la implementación de los requerimientos de la ISO/IEC 27001:2013, se requiere la adecuación de las políticas de segundo nivel para que abarquen la definición e implantación de los controles definidos del anexo A de la norma.

[OBJ-03] Identificar las políticas y normas necesarias que soporten la política de seguridad de la información para cubrir la implementación de los controles definidos en el documento Declaración de Aplicabilidad V1.0 y realizar una campaña de divulgación a los funcionarios de la Oficina Central y las empresas afiliadas.

En la medida que la operación logre alinearse con las recomendaciones de la norma, se podrían generar modificaciones en los procesos actuales o crearse nuevos subprocesos de apoyo. El SGSI, deberá estar alineado con el Sistema de Gestión de Calidad y para esto, se requerirá documentar y formalizar todos estos procesos.

> [OBJ-04] Identificar los procesos necesarios para desarrollar el plan de seguridad, la implementación de controles y la gestión del SGSI y a su vez, generar la documentación necesaria basada en los formatos y nomenclaturas del Sistema de Gestión Documental de la compañía.

La operación de la infraestructura tecnológica deberá funcionar de acuerdo a parámetros prestablecidos generados a partir de las recomendaciones de la norma y deben poder ser evaluados para medir su efectividad.

> [OBJ-05] Tener documentado los umbrales de uso aceptables de la capacidad de los activos de información de Oficina Central e indicadores de tiempos de disponibilidad mínimos requeridos de los servicios que hayan sido aprobados por el Comité de Riesgos
>
> [OBJ-06] Tener documentada la capacidad de la infraestructura operativa así como las incidencias, problemas y cambios que la afecten en alguna de las dimensiones de seguridad: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.
>
> [OBJ-7] Tener un cuadro de mando con los indicadores necesarios que permitan a la Dirección de TI de la Institución evaluar la efectividad y eficacia de los controles implementados y apoyar en la toma de decisiones sobre la operación de los mismos.
>
> [OBJ-8] Tener un programa de auditorías interno que garantice la confiabilidad de la ejecución de todos los procesos del SGSI y fortalezca la confianza y credibilidad de la calidad de los servicios prestados, no solo en los usuarios de Oficina Central sino en las Directivas en general, las filiales y empresas de apoyo de la Institución.

La mesa de ayuda de la compañía administra el hardware y software de los equipos de escritorio y portátiles de los funcionarios y es la encargada de gestionar su asignación y remplazo. A menudo, los usuarios requieren tener privilegios de administración sobre sus

máquinas y la taza de malware detectado en estos equipos es elevada respecto a un usuario de privilegios limitados, incurriendo en ocasiones en la reinstalación o reseteo en modo de fábrica, generando sobresfuerzos a la operación.

> [OBJ-09] Mejorar los procedimientos relacionados con el software instalado, autorización de privilegios y vida útil del hardware que incrementen los controles de seguridad en los equipos asignados a los funcionarios para reducir las incidencias de seguridad de la información.
> [OBJ-10] Divulgar los procedimientos de gestión la mesa de ayuda a las filiales y compañías asociadas para que todas trabajen bajo los mismos lineamientos debido a que utilizan una infraestructura de red y de servicios compartida.

Existe un equipo humano que se encarga de configurar y monitorear los backups de la data de los servidores. Es importante garantizar que toda la programación de backups sea ejecutada con éxito o gestionar su relanzamiento para cumplir con los respaldos.

> [OBJ-11] Garantizar que la data de las aplicaciones, bases de datos e información de los usuarios y de los servicios que operan en el centro de cómputo de Oficina Central, quede debidamente respalda y se brinden los mecanismos para su restauración de forma oportuna.

4. ANÁLISIS DIFERENCIAL

A continuación de comparará el estado de la gestión de la seguridad de la información en compañía con la norma ISO/IEC 27001 y las mejores prácticas descritas en ISO/IEC 27002 para evaluar la capacidad actual y realizar las recomendaciones y oportunidades de mejora.

Este análisis proveerá la información necesaria a la empresa para evaluar el esfuerzo, tiempo, dinero y recursos humanos requeridos para la implementación de la gestión de la seguridad de la información.

Tanto los requisitos de la norma IO/IEC27001 como los controles descritos en la ISO/IEC 27002 fueron evaluados con en el Modelo de Madurez de la Capacidad (CMM), resumido en la siguiente tabla:

%	ESTADO	DESCRIPCIÓN
0	No Existe	Ausencia absoluta de una política reconocible, procedimiento, control, etc.
10	Inicial	El desarrollo apenas está iniciando y requerirá una trabajo significativo para cumplir con el requisito
50	Limitado	Progresando muy bien pero aún incompleto
90	Definido	El desarrollo está más o menos completo aunque se carece de detalle y/o aún no se ha implementado, impartido y promovido por la alta dirección
95	Gestionado	El desarrollo está completa, el proceso/control se ha implementado y recientemente comenzó a operar
100	Optimizado	El requisito está completamente cumplido, está funcionando completamente como se esperaba, está siendo monitoreado y mejorado constantemente, y hay evidencia sustancial para demostrarlo en una auditoría
-	No aplicable	TODOS los requisitos en el cuerpo principal de la norma ISO / IEC 27001 son obligatorios SI el SGSI es para ser certificado. De lo contrario, podrían ser ignorados.

Tabla 1. Modelo de Madurez de la Capacidad (CMM)

4.1. ANÁLISIS GAP PARA ISO/IEC 27001

La norma ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y continuamente mejorar el sistema de gestión de seguridad de la información y agrupa sus requerimientos en 7 cláusulas. La siguiente matriz indica la categorización de cada cláusula de acuerdo a la valoración de procesos presentada:

Cláusula	Valoración
4. Contexto de la organización	Inicial
5. Liderazgo	Limitado
6. Planeación	Inicial
7. Soporte	Limitado
8. Operación	Inicial
9. Evaluación de rendimiento	No Existe
10. Mejora	Inicial

Tabla 2. Valoración de cláusulas de requerimientos ISO/IEC 27001:2013

El cumplimiento de los requisitos categorizados por sección, es evidenciado en el siguiente diagrama radial.

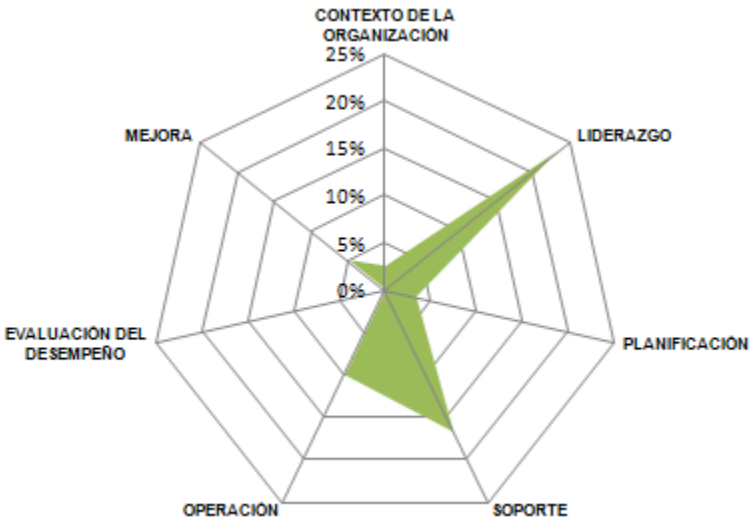

Ilustración 3. Cumplimiento de las secciones de requisitos del SGSI

La proporción de los requisitos de acuerdo al estado se evidencia en el siguiente gráfico.

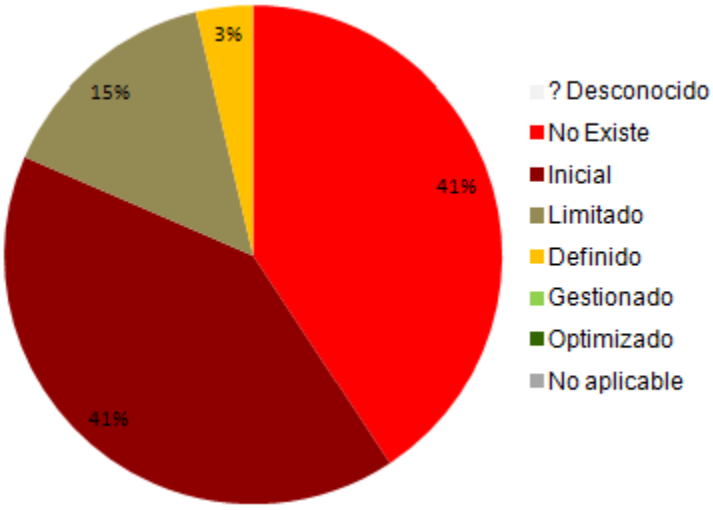

Ilustración 4. Proporción de cumplimiento de los requisitos del SGSI

La especificación del análisis se encuentra documentado en el *Anexo A. Análisis GAP de implementación ISOIEC 27001 e ISOIEC 27002*.

4.2. ANÁLISIS GAP PARA ISO/IEC 27002:2013

Esta sección describe la evaluación a alto nivel del grado de implementación de los controles y objetivos de control en los 14 dominios descritos en la ISO/IEC 27002:2013.

La valoración de cada dominio de control se realizó basada en la ponderación de las valoraciones de los objetivos de control que a su vez son el resultado de la evaluación del grado de implementación de cada control independiente y se resumen en la siguiente tabla:

DOMINIOS DE CONTROL		PROPORCIÓN DE IMPLEMENTACIÓN	
5	POLÍTICAS DE SEGURIDAD.	55%	Definido
6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	67%	Definido
7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	81%	Definido
8	GESTIÓN DE ACTIVOS.	35%	Limitado
9	CONTROL DE ACCESOS.	58%	Definido
10	CIFRADO.	30%	Limitado
11	SEGURIDAD FÍSICA Y AMBIENTAL.	84%	Definido
12	SEGURIDAD OPERATIVA.	72%	Definido
13	SEGURIDAD EN LAS TELECOMUNICACIONES.	89%	Definido
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	81%	Definido
15	RELACIONES CON PROVEEDORES.	88%	Definido
16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	40%	Limitado
17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	86%	Definido
18	CUMPLIMIENTO.	73%	Definido

Tabla 3. Proporción de implementación de controles por dominio

La especificación del análisis se encuentra documentado en el *Anexo A. Análisis GAP de implementación ISOIEC 27001 e ISOIEC 27002*.

Se puede representar más precisa la evaluación realizada de acuerdo a cada dominio de control con el siguiente gráfico:

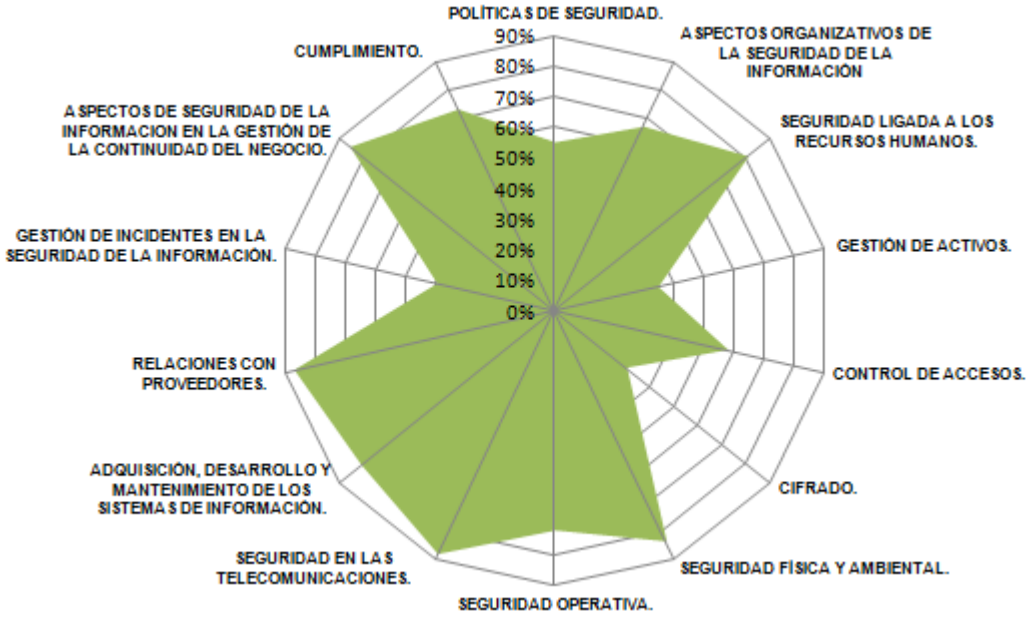

Ilustración 5. Grado de cumplimiento de Dominios de control

La proporción de los controles de acuerdo al estado se evidencia en el siguiente gráfico.

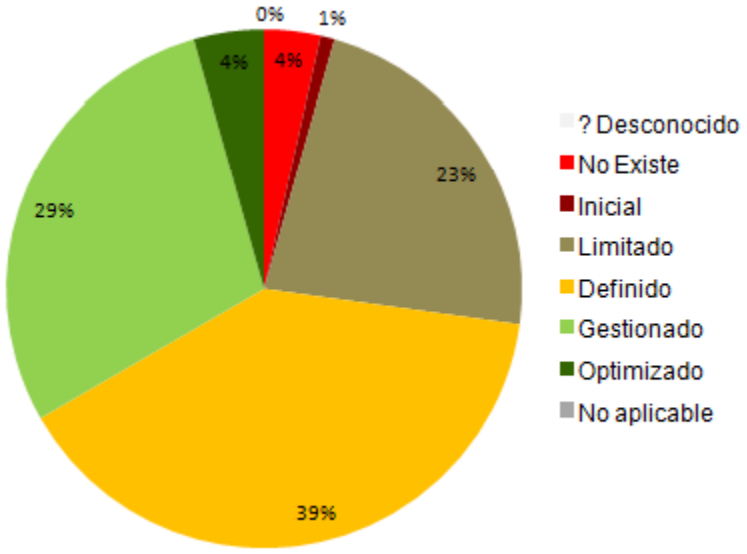

Ilustración 6. Proporción de controles por estado de implementación

5. ESQUEMA DOCUMENTAL

5.1. INTRODUCCIÓN

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. El Sistema de Gestión de Seguridad de la Información tiene una serie de documentos de acuerdo a lo establecido en la norma ISO/IEC 27001. Estos documentos son referenciados como anexos en el presente Plan de Seguridad y son descritos a continuación.

5.2. ESQUEMA DOCUMENTAL

Anexo Documental I. Políticas de Seguridad de la Información

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 establece los lineamientos globales que son detallados en normas y políticas de segundo nivel definidos en el documento “Políticas y Normas de seguridad”.

Anexo Documental II. Procedimiento de Auditorías Internas

Documento que debe describe el procedimiento para realizar las auditorías que se llevarán a cabo durante la vigencia de la certificación y requisitos que se establecerán a los auditores internos. Se anexa la documentación de los registros de los siguientes formatos:

- GSO-F-001 Formato Programa anual de auditorías
- GSO-F-002 Formato Plan de auditoría interna
- GSO-F-003 Formato Informe de auditoría interna del SGSI
- GSO-F-004 Formato Solicitud de Acción

Anexo Documental III. Procedimiento de Gestión de Indicadores

Definición de indicadores para medir la eficacia de los controles de seguridad implantados y lineamientos de medición.

Anexo Documental IV. Procedimiento de Gestión de Roles y Responsabilidades

Definición del “Comité de Seguridad” encargado de crear, mantener, supervisar y mejorar el Sistema de Gestión de Seguridad de la Información.

Anexo Documental V. Procedimiento de Revisión por la Dirección

Definición del procedimiento donde se indica que la Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información.

Anexo Documental VI. Declaración de Aplicabilidad

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

Anexo Documental VII. 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.

6. ANÁLISIS DE RIESGOS

La primera etapa hacia la consecución del Plan de Implementación de un SGSI consistirá en la evaluación de nuestros activos, considerando las dependencias existentes entre ellos y realizando una valoración de los mismos.

6.1. INVENTARIO DE ACTIVOS

Los activos más relevantes tomados en cuenta para el análisis de riesgos, es resumido en la siguiente tabla.

Código	Activo
AUX1	Equipamiento de aire acondicionado del datacenter
AUX2	Equipamiento contraincendios del datacenter
AUX3	Robot de cintas de backup
AUX4	Equipamiento de alimentación eléctrica dual
AUX5	Racks
AUX6	Cableado
COM1	Red telefónica
COM2	Red de datos Local (LAN)
COM3	Red de datos Corporativa (WAN)
COM4	Red Inalámbrica
COM5	Internet
D1	Datos de los usuarios para validación de credenciales
D2	Registros de pagos a asociados
D3	Mapas geográficos
D4	Correos electrónicos
D5	Archivos del repositorio central
D6	Registros de actividades de software
HW1	Servidor
HW2	Computador personal
HW3	Computador portátil
HW4	Móviles
HW5	Impresoras
HW6	Equipamiento de red
HW7	Central telefónica
L1	Edificio

Código	Activo
MEDIA1	Cintas de backup
P1	Usuarios externos
P2	Usuarios internos
P3	Operadores
P4	Administradores de infraestructura
P5	Coordinadores
P6	Directivas
P7	Contratistas
P8	Representantes de proveedores
S1	Canal de internet
S2	Repositorio de Archivos
S3	Páginas web
S4	Correo electrónico
SW1	Aplicativos de Ofimática
SW2	Clientes de correo electrónico
SW3	Sistema de gestión de base de datos
SW4	Sistemas operativos
SW5	Gestor de máquinas virtuales
SW6	Sistema de gestión de backups
SW7	Sistema de referenciación geográfica
SW8	Sistema de gestión de pagos a asociados

Tabla 4. Inventario de activos

Cada activo fue categorizado según la tabla de ámbitos MAGERIT y codificado de acuerdo a la siguiente nomenclatura:

Ámbitos de Activos	
[D] Datos	Datos que materializan la información
[S] Servicios	Servicios auxiliares que se necesitan para poder organizar el sistema
[SW] Software	Las aplicaciones informáticas (software) que permiten manejar los datos.
[HW] Hardware	Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
[MEDIA] Soportes de Información	Los soportes de información que son dispositivos de almacenamiento de datos.
[AUX] Equipamiento Auxiliar	El equipamiento auxiliar que complementa el material informático.
[COM] Redes de comunicaciones	Las redes de comunicaciones que permiten intercambiar datos.

Ámbitos de Activos	
[L] Instalaciones	Las instalaciones que acogen equipos informáticos y de comunicaciones.
[P] Personal	Las personas que explotan u operan todos los elementos anteriormente citados.

Tabla 5. Ámbitos de activos

6.2. VALORACIÓN DE LOS ACTIVOS

Para la valoración de los activos, se utilizó la escala que propone MAGERIT en su Libro III (punto 2.1), completándolo con una estimación cuantitativa representada en términos monetarios para la organización.

	Valor	Abreviatura	Descripción
Valoración de los activos (COP$ millones)	valor > 200'	MA	Muy alto
	200' > valor > 100'	A	Alto
	100' > valor > 50'	M	Medio
	50' > valor > 10'	B	Bajo
	10' > valor > 1'	MB	Muy bajo

Tabla 6. Criterios de valoración de los activos

En el *Anexo B. Análisis de Riesgos* hoja *Activos* se encuentran documentados los activos con su respectiva valoración.

6.3. DIMENSIONES DE SEGURIDAD

Desde el punto de vista de la seguridad, junto a la valoración en sí de los activos se debe indicar cuál es el aspecto de la seguridad más crítico de manera que se pueda seleccionar las salvaguardas enfocadas en los aspectos más relevantes. Por esta razón, para cada activo fue valorada la criticidad en las cinco dimensiones de la seguridad de la información manejada por el proceso de negocio para permitir estimar el impacto que tendrá la materialización de una amenaza sobre la parte de activo expuesto no cubierto por las salvaguardas en cada una de las dimensiones teniendo presente qué representa cada dimensión, explicadas en la siguiente tabla.

Dimensiones de valoración de los activos	
[D] Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[I] Integridad de los datos	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] Confidencialidad de la información	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[A] Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008] (Importancia del No Repudio)
[T] Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008] (Auditabilidad)

Tabla 7. Dimensiones de valoración de los activos

6.4. ANÁLISIS DE AMENAZAS

Se realizó la estimación de cuán vulnerable es cada activo a la materialización de la amenaza, la frecuencia estimada con que pueden producirse y el impacto en las distintas dimensiones de la seguridad. Para determinar las amenazas posibles, se utilizó la tabla inicial de amenazas usadas en MAGERIT en su libro 2 "Catálogo de Elementos" (Punto 5). Las amenazas están clasificadas en los siguientes grandes bloques:

Tipos de Amenazas	
[N] Desastres naturales	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
[I] De origen industrial	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas puede darse de forma accidental o deliberada.
[E] Errores y fallos no intencionados	Fallos no intencionales causados por las personas.
[A] Ataques intencionados	Fallos deliberados causados por las personas.

Tabla 8. Tipos de amenazas

Se valoraron los activos como de importancia “Muy Alta”, “Alta”, “Media”, “Baja” o “Despreciable” a la vez que se le asignó a cada activo en cada dimensión una valoración siguiendo los siguientes criterios:

Valor	Abreviatura	Descripción
0	D	Despreciable - Irrelevante a efectos prácticos
1-3	B	Bajo - Daño menor a la organización
4-6	M	Medio - Daño importante a la organización
7-8	A	Alto - Daño grave a la organización
10	MA	Muy Alto - Daño muy grave a la organización

Tabla 9. Criterios de valoración de criticidad de los activos

Para el análisis de la frecuencia estimada de materialización de amenazas, se utilizó la siguiente escala de tiempo basada en la cantidad incidencias en un período menor a un año.

Valor	Abreviatura	Descripción
1	EF	Extremadamente frecuente (1 vez al día)
0,071	MF	Muy frecuente (1 vez cada 2 semanas)
0,016	F	Frecuente (1 vez cada 2 meses)
0,005	PF	Poco Frecuente (1 vez cada 6 meses)
0,003	MPF	Muy poco frecuente (1 vez cada año)
0	D	Despreciable

Tabla 10. Escala de valoración de Frecuencia (Vulnerabilidad - Probabilidad de ocurrencia)

En el *Anexo B. Análisis de Riesgos*, se encuentran los registros del análisis realizado por cada activo.

6.5. ANLÁLISIS DE IMPACTO POTENCIAL

Una vez valorada la criticidad por dimensión de seguridad y la probabilidad de materialización de cada amenaza y dado que se conoce el valor de los diferentes activos, es posible determinar el impacto potencial que puede suponer para la empresa la materialización de las amenazas.

En el *Anexo B. Análisis de Riesgos* hoja *Activos*, se encuentra determinado el impacto potencial por cada activo de acuerdo al análisis realizado por cada una de las amenazas. Esta información permitirá priorizar el plan de acción y la selección de salvaguardas, y a su vez, servirá de línea base para comparar cómo se ve modificado dicho valor una vez se apliquen contramedidas.

El impacto puede resumirse como el tanto por ciento del valor del activo que se pierde en el caso de que suceda un incidente sobre él. Para el presente ejercicio, se tomó la siguiente escala de valoración.

Valor	Abreviatura	Descripción
valor > 80%	MA	Muy alto
60% > valor > 80%	A	Alto
40% > valor > 60%	M	Medio
20% > valor > 40%	B	Bajo
valor < 20%	MB	Muy bajo

Tabla 11. Escala de valoración del impacto – degradación del activo

6.6. ANÁLISIS DE RIESGOS

Para la estimación del riesgo, se realizó una combinación entre el impacto y la frecuencia, detallada en la siguiente tabla.

RIESGO		Impacto				
		MA	A	M	B	MB
Frecuencia	EF	MA	MA	MA	MA	MA
	MF	MA	MA	A	A	M
	F	A	A	M	M	B
	PF	M	M	B	B	MB
	MPF	B	B	MB	MB	MB
	D	MB	MB	MB	MB	MB

Tabla 12. Tabla de estimación del riesgo

Para efectos de cálculo de la matriz de riesgos, la misma tabla puede ser representada en valores numéricos de acuerdo a las escalas definidas de la siguiente manera:

RIESGO		Impacto				
Frecuencia	1	100,00%	80,00%	60,00%	40,00%	20,00%
	0,071	7,12%	5,70%	4,27%	2,85%	1,42%
	0,016	1,64%	1,32%	0,99%	0,66%	0,33%
	0,005	0,55%	0,44%	0,33%	0,22%	0,11%
	0,003	0,27%	0,22%	0,16%	0,11%	0,05%
	0,000	0,00%	0,00%	0,00%	0,00%	0,00%

Tabla 13. Tabla del cálculo de estimación del riesgo.

Para efectos prácticos, se utilizó la siguiente escala de valores para la relación enter impacto y frecuencia, determinando el nivel de riesgo por cada amenaza para cada activo en cada dimensión y en la tabla de resumen de impacto potencial por activo.

Valor	Abreviatura	Descripción
valor > 4,5%	MA	Muy alto
4,5% > valor > 1%	A	Alto
1% > valor > 0,4%	M	Medio
0,4% > valor > 0,2%	B	Bajo
valor < 0,2%	MB	Muy bajo

Tabla 14. Escala de riesgos

Nivel de riesgo aceptable

Para elaborar el plan de tratamiento de amenazas, se tomarán en cuenta los riesgos de clase Muy Alto y Alto, por lo tanto, el nivel de riesgo aceptable por lo menos en esta etapa de implementación del SGSI y para la definición de los proyectos de mejora en un plan de choque será para los niveles Medio, Bajo y Muy Bajo.

Ejemplo práctico

Para un activo de información dado:

- Seleccionar las amenazas del catálogo MAGERIT para el tipo de activo.
- Indicar la frecuencia o probabilidad de ocurrencia de la amenaza.
- Indicar la criticidad del activo.
- Calcular el impacto de acuerdo a asociación del valor de la frecuencia y la criticidad indicadas.
- Calcular el riesgo de acuerdo a la asociación del valor de la frecuencia y el impacto de un incidente.
- Calcular el valor más alto de cada dominio de control por todas las amenazas del tipo de activo y calcular la tabla resumen de activos.

COM3 Red de datos Corporativa (WAN)				Valor del activo: MA															
Código	Tipos de Activos afectados	Amenaza	Frecuencia	Criticidad					Impacto					Riesgo					
				[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[I.8]	[COM]	Fallo de servicios de comunicaciones	F	9					90%					1,44%				
[E.2]	[D][K][S][SW][HW][COM][Media]	Errores del administrador	PF	9	1	1			90%	10%	10%			0,45%	0,05%	0,05%		
[E.3]	[S][SW][COM]	Errores de [re-]encaminamiento	MPF			0					0%					0,00%		
[E.10]	[S][SW][COM]	Errores de secuencia	D		0					0%					0,00%			
[E.14]	[D][SW][COM]	Escapes de información	MPF			1					10%					0,03%		
[E.15]	[D][K][S][SW][COM][Media][L]	Alteración accidental de la información	MPF		5					50%					0,15%			
[E.18]	[D][K][S][SW][COM][Media][L]	Destrucción de información	D	0					0%					0,00%				
[E.19]	[D][K][S][SW][COM][Media][L][P]	Fugas de información	D			0					0%					0,00%		
[E.24]	[S][HW][COM]	Caída del sistema por agotamiento de recursos	MF	2					20%					1,42%				
[A.5]	[D][K][S][SW][COM]	Suplantación de la identidad del usuario	D		0	2	9			0%	20%	90%			0,00%	0,00%	0,00%	
[A.6]	[D][K][S][SW][HW][COM]	Abuso de privilegios de acceso	D	0	0	0			0%	0%	0%			0,00%	0,00%	0,00%		
[A.7]	[S][SW][HW][COM][Media][AUX][L]	Uso no previsto	MF	7	0	1			70%	0%	10%			4,97%	0,00%	0,71%		
[A.9]	[S][SW][COM]	[Re-]encaminamiento de mensajes	D			0					0%					0,00%		
[A.10]	[S][SW][COM]	Alteración de secuencia	D		0					0%					0,00%			
[A.11]	[D][K][S][SW][HW][COM][Media][AUX][L]	Acceso no autorizado	MPF		0	2				0%	20%				0,00%	0,06%		
[A.12]	[COM]	Análisis de tráfico	F			1					10%					0,16%		
[A.14]	[COM]	Interceptación de información (escucha)	D			0					0%					0,00%		
[A.15]	[D][K][S][SW][COM][Media][L]	Modificación deliberada de la información	D		0					0%					0,00%			
[A.19]	[D][K][S][SW][COM][Media][L]	Divulgación de información	D			0					0%					0,00%		
[A.24]	[S][HW][COM]	Denegación de servicio	F	10					100%					1,60%				
Código	Dependencias			[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
		Totales por dominio:		10	5	2	9	0	100%	50%	20%	90%	0%	4,97%	0,15%	0,71%	0,00%	0,00%

6.7. RECOMENDACIONES

De acuerdo al análisis de riesgos realizado y el nivel de riesgo aceptable definido por la organización para el plan de implementación, a continuación se documentan las recomendaciones de mejora, iniciando con los tratamientos de riesgos Muy Alto.

[REC A] Monitorear los comportamientos causantes de la saturación de los canales de internet con estadísticas de utilización que permitan definir bien sea medidas de reducción y buen de uso o que sirvan de soporte para sustentar un aumento del recurso por necesidades del negocio

[REC B] Definir sensores de monitoreo que permitan detectar el uso no previsto del canal y se eviten saturación con anticipación

[REC C] Garantizar que los medios de redundancia de los canales de internet funcionen adecuadamente y brinden capacidades de respaldo aceptables para el funcionamiento de la operación del negocio

[REC D] Implementar laboratorios y herramientas de monitoreo que permitan identificar las fallas en la infraestructura de red inalámbrica y documentar los hallazgos para sustentar los recursos necesarios que solucionen los problemas de las comunicaciones por este medio y que es percibida por los usuarios en general como una denegación del servicio.

[REC E] Implementar un proceso controlado de alta de usuarios en la red inalámbrica interna para garantizar que los dispositivos conectados estén autorizados en esa red.

[REC F] Implementar en lo posible mecanismos de control de uso de la red inalámbrica que eviten la saturación del medio, en especial en las redes de invitados

[REC G] Generar el inventario de los directorios compartidos por el servidor de archivos con la relación del personal autorizado y los privilegios de acceso y modificación de los contenidos, para disminuir la posibilidad que pueda ser borrada o modificada la información almacenada o los permisos asignados a otros usuarios.

[REC H] Publicar los directorios exclusivamente para los usuarios que tienen acceso a su contenido, para evitar que las personas puedan ver la totalidad de los recursos compartidos por el servidor de archivos

[REC I] Asignar un propietario o responsable de cada directorio compartido que defina los usuarios autorizados para la eliminación de archivos dentro del recurso

[REC J] Definir una norma que determine qué tipo de información puede ser almacenada en los recursos compartidos para evitar el uso del almacenamiento con archivos que no son propios de la compañía o para el funcionamiento del negocio. (p.e. música o archivos personales)

[REC K] Habilitar en el servidor la auditoría de eliminación de archivos que permita la trazabilidad del usuario cuando se lleve a cabo la eliminación de archivos

[REC L] Restringir el acceso a las carpetas compartidas a solo usuarios del directorio activo para que la modificación de la información sea controlada por políticas de dominio

[REC M] Garantizar en lo posible que exista un mecanismo de contingencia de acceso a la información en caso de afectación de alguno de los elementos tecnológicos que componen el servicio de directorios compartidos

[REC N] Identificar los recursos de la plataforma de correo que puedan estar sufriendo cuellos de botella y optimizarlos o fortalecerlos

[REC O] Definir normas de uso del correo electrónico para evitar el despacho masivo de correos en horarios que puedan afectar a los usuarios

[REC P] Identificar y depurar los buzones de correo tanto genéricos como de distribución, generar una nomenclatura estándar y documentar la autorización de creación y los usuarios responsables de su uso

[REC Q] Identificar los factores recurrentes de errores de los usurarios en el uso de las contraseñas de dominio y generar las capacitaciones necesarias para reducir el índice de casos de soporte de este tipo

[REC R] Identificar y eliminar el uso de usuarios genéricos en todos los directorios de autenticación existentes

[REC S] Definir una nomenclatura estándar y documentar las contraseñas, depurar y asignar responsables a los usuarios de servicios que deban existir en el directorio activo

[REC T] Monitorear las incidencias por degradación o daño de los servidores con estadísticas de recurrencia que permitan tomar medidas preventivas o que sustenten una renovación o remplazo de los mismos para evitar impactos negativos a corto plazo en la operación de los servicios de TI

[REC U] Actualizar los sistemas operativos de los servidores a sus versiones más recientes para reducir las vulnerabilidades técnicas del producto

[REC V] Crear un esquema de roles de backup de los administradores de infraestructura de manera que haya otra persona que pueda ejecutar actividades operativas de un cargo en caso que el responsable no se encuentre disponible

[REC W] Definir el procedimiento de solicitud y autorización de software en los equipos asignados a los usuarios así como la definición de los responsables para su instalación

[REC X] Comprobar que el software actualmente instalado en los computadores de usuario cumplan con el licenciamiento adquirido por la organización

[REC Y] Documentar la autorización de usuarios administradores de computadores de trabajo y registrar la aceptación de responsabilidades de uso y cumplimiento de las normas de seguridad de la información con los privilegios que conlleva este rol

[REC Z] Asignar una contraseña maestra para el usuario administrador local de los computadores de usuario que sea diferente según la empresa o filial registrada en el directorio activo y sea administrada por los funcionarios de cada mesa de ayuda correspondiente

[REC AA] Definir un esquema de actualizaciones automáticas del sistema operativo de los computadores de usuario para mitigar las vulnerabilidades técnicas propias de cada sistema

[REC BB] Definir un esquema de alta disponibilidad por redundancia o clusterización de los servicios críticos de la compañía como DHCP y aplicaciones web transaccionales

[REC CC] Definir un procedimiento de autorización y registro de actividades de mantenimiento de los componentes de hardware de tecnología del centro de cómputo

7. PROPUESTA DE PROYECTOS

7.1. INTRODUCCIÓN

Los proyectos de mejora ayudan a mitigar el riesgo actual de la organización y encaminar la evolución del cumplimiento ISO hasta un nivel adecuado. Se derivan y agrupan las recomendaciones identificadas en la fase de análisis de riesgos asociadas a las amenazas encontradas. Además, son cuantificados económicamente y planificados en el tiempo, estableciendo plazos de consecución de sus objetivos (en general, corto, medio y largo plazo) con puntos de control que permitan considerar realmente el Plan de Implementación del SGSI como un proceso de mejora continua.

7.2. PROYECTOS

Se definieron 10 proyectos relevantes que mitigan los riesgos de mayor impacto. La documentación de las recomendaciones del análisis de riesgos que tratan, los recursos necesarios y el cronograma de actividades, se encuentra definido en documento *Anexo C. Proyectos de mejora*.

Código y Nombre		Impacto	Prioridad
PRJ 01	Mejoramiento de los canales de internet	Alto	Baja
PRJ 02	Optimización de la red inalámbrica	Alto	Alta
PRJ 03	Optimización del servicio de carpetas compartidas	Medio	Media
PRJ 04	Optimización del servicio de correo electrónico	Alto	Alta
PRJ 05	Depuración de los Directorios de Autenticación de usuarios	Bajo	Media
PRJ 06	Mejoramiento de los servidores	Alto	Media
PRJ 07	Conformación de equipos de apoyo de administradores de infraestructura	Medio	Alta
PRJ 08	Aseguramiento de los equipos de usuario	Medio	Media
PRJ 09	Alta disponibilidad de los servicios críticos para la Institución	Medio	Alta
PRJ 10	Implementación de mejores prácticas de seguridad de la información relacionada con datacenters	Bajo	Baja

8. AUDITORÍA DE CUMPLIMENTO

8.1. INTRODUCCIÓN

Llegados a esta fase, conocemos los activos de la empresa y hemos evaluado las amenazas. Es el momento de hacer un alto en el camino y evaluar hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad. La ISO/IEC 27002:2005 nos servirá como marco de control del estado de la seguridad.

8.2. METODOLOGÍA

El estándar ISO/IEC 27002:2005, agrupa un total de 133 controles o salvaguardas sobre buenas prácticas para la Gestión de la Seguridad de la Información organizado en 11 áreas y 39 objetivos de control. La protección integral frente a las posibles amenazas, requiere de una combinación de salvaguardas sobre cada uno de estos aspectos.

El estudio debe realizar una revisión de los 133 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 dominios-. Esta estimación la realizaremos según el Modelo de Madurez de la Capacidad (CMM)

8.3. ANÁLISIS DE CUMPLIMIENTO

La norma ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y continuamente mejorar el sistema de gestión de seguridad de la información y agrupa sus requerimientos en 7 cláusulas.

Luego de haber implementado los proyectos sugeridos y revisado nuevamente a través de la auditoría la implementación de controles y cumplimiento de los requisitos de la norma, se encontró el siguiente avance en términos estadísticos:

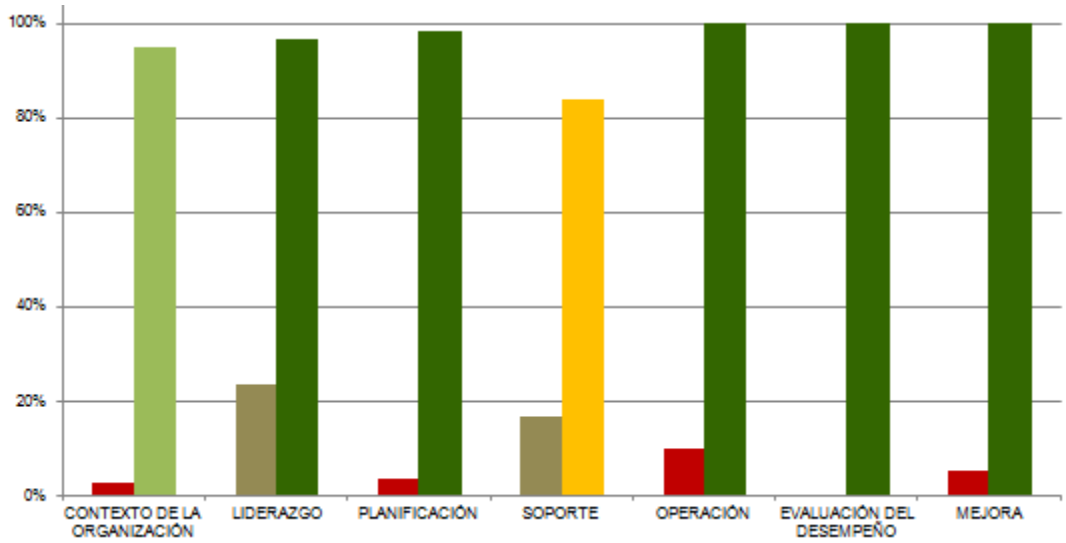

Ilustración 7. Comparación de porcentaje de implementación

La siguiente matriz indica la categorización de cada cláusula de acuerdo a la valoración de procesos presentada:

REQUISITO	REQUERIMIENTOS SGSI	PROPORCIÓN DE CUMPLIMIENTO	
4	CONTEXTO DE LA ORGANIZACIÓN	95%	Gestionado
5	LIDERAZGO	97%	Optimizado
6	PLANIFICACIÓN	98%	Optimizado
7	SOPORTE	84%	Definido
8	OPERACIÓN	100%	Optimizado
9	EVALUACIÓN DEL DESEMPEÑO	100%	Optimizado
10	MEJORA	100%	Optimizado

Tabla 15. Valoración de cláusulas de requerimientos ISO/IEC 27001:2013

El cumplimiento de los requisitos categorizados por sección, es evidenciado en el siguiente diagrama radial.

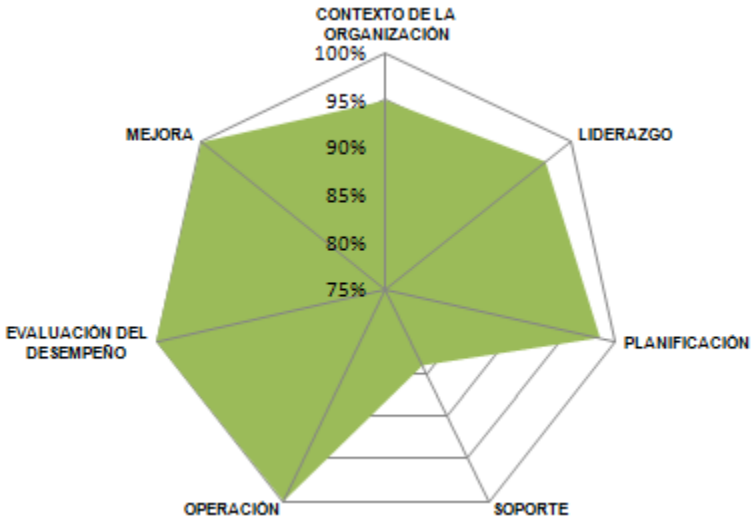

Ilustración 8. Cumplimiento de las secciones de requisitos del SGSI

La proporción de los requisitos de acuerdo al estado se evidencia en el siguiente gráfico.

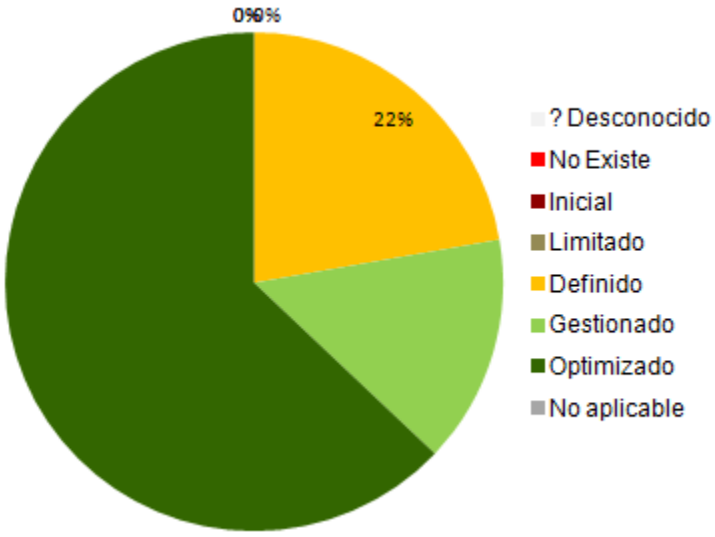

Ilustración 9. Proporción de cumplimiento de los requisitos del SGSI

La especificación del análisis se encuentra documentado en el *Anexo D. Análisis GAP de implementación ISOIEC 27001 e ISOIEC 27002*.

La valoración de cada dominio de control de la la ISO/IEC 27002:2013 se realizó basada en la ponderación de las valoraciones de los objetivos de control que a su vez son el resultado de la evaluación del grado de implementación de cada control independiente y se resumen en la siguiente tabla:

DOMINIOS DE CONTROL DE SEGURIDAD DE LA INFORMACIÓN		PROPORCIÓN DE IMPLEMENTACIÓN	
5	POLÍTICAS DE SEGURIDAD.	98%	Optimizado
6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	88%	Definido
7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	88%	Definido
8	GESTIÓN DE ACTIVOS.	90%	Definido
9	CONTROL DE ACCESOS.	86%	Definido
10	CIFRADO.	60%	Definido
11	SEGURIDAD FÍSICA Y AMBIENTAL.	90%	Gestionado
12	SEGURIDAD OPERATIVA.	89%	Definido
13	SEGURIDAD EN LAS TELECOMUNICACIONES.	85%	Definido
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	86%	Definido
15	RELACIONES CON PROVEEDORES.	93%	Gestionado
16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	93%	Gestionado
17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	95%	Gestionado
18	CUMPLIMIENTO.	89%	Definido

Tabla 16. Proporción de implementación de controles por dominio

La especificación del análisis se encuentra documentado en el *Anexo D. Análisis GAP de implementación ISOIEC 27001 e ISOIEC 27002*.

Se puede representar más precisa la evaluación realizada de acuerdo a cada dominio de control con el siguiente gráfico:

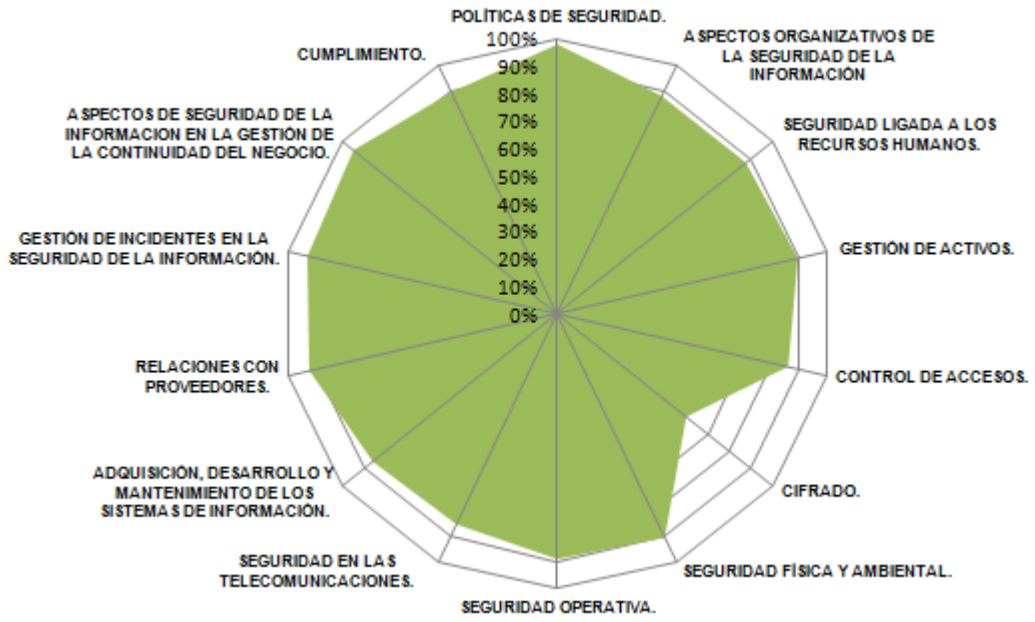

Ilustración 10. Grado de cumplimiento de Dominios de control

La proporción de los controles de acuerdo al estado se evidencia en el siguiente gráfico.

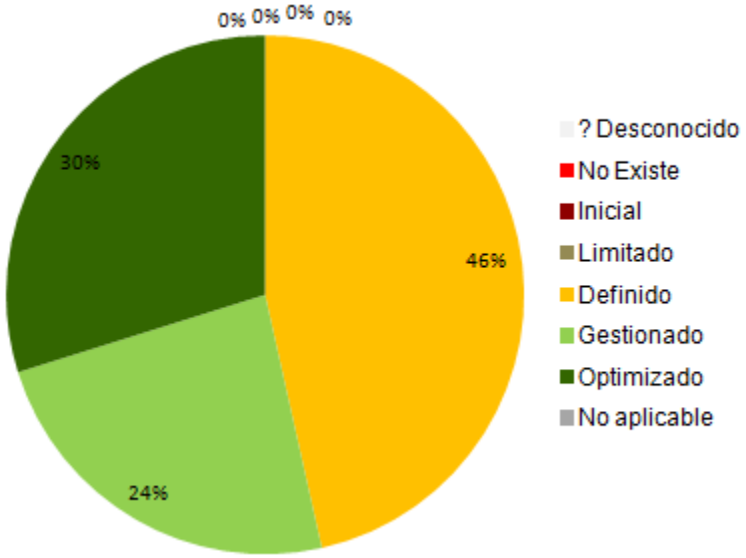

Ilustración 11. Proporción de controles por estado de implementación

9. INFORMES DE RESULTADOS

En el presente apartado se mencionarán los informes de resultados del Plan de Seguridad de la Información.

9.1. RESUMEN EJECUTIVO

(Anexo E. Presentación1 - Resumen ejecutivo) Presentación enfocada a la Alta Dirección donde se haga un resumen del proyecto

9.2. PRESENTACIÓN Y CONCIENCIACIÓN EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

(Anexo F. Presentación2 - Campanna Sensibilización) Presentación enfocada a instruir al personal de la Organización en materia de Seguridad de la Información

9.3. RESUMEN DEL ESTADO DE CUMPLIMIENTO DE LOS CONTROLES

(Anexo G. Presentación3 - Resumen estado de controles) Presentación enfocada a mostrar el estado de cumplimiento de los controles y estado de ejecución de los proyectos.

9.4. PRESENTACIÓN RESULTADOS

(Anexo H. Presentación4 - Resultados) Presentación enfocada a presentar los resultados del proyecto a la Alta Dirección. Esta presentación puede tener una duración de 1 hora.

10. ANEXOS

ANEXO A. ANÁLISIS GAP DE IMPLEMENTACIÓN ISOIEC 27001 E ISOIEC 27002

ANEXO B. ANÁLISIS DE RIESGOS

ANEXO C. PROYECTOS DE MEJORA

ANEXO D. ANÁLISIS GAP DE IMPLEMENTACIÓN ISOIEC 27001 E ISOIEC 27002

ANEXO E. PRESENTACIÓN1 - RESUMEN EJECUTIVO

ANEXO F. PRESENTACIÓN2 - CAMPANNA SENSIBILIZACION

ANEXO G. PRESENTACIÓN3 - RESUMEN ESTADO DE CONTROLES

ANEXO H. PRESENTACIÓN4 - RESULTADOS

11. REFERENCIAS

- http://www.iso27001security.com/
- http://www.iso27001standard.com/
- Sistema de Gestión Documental de la institución
- http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI/
- http://www.iso27000.es/sgsi_implantar.html
- http://video.anetcom.es/editorial/Seguridad_empresa.pdf
- https://seguridadinformaticaufps.wikispaces.com/MAGERIT
- https://www.ccn-cert.cni.es/publico/herramientas/pilar5/exs/index.html
- http://gr2dest.org/metodologia-de-analisis-de-riesgos-magerit/
- Libros I y II de MAGERIT v.3

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS