Este TFM permite guiar a la mesa directiva de la organización en el proceso de implementación de un plan director para la seguridad de la información con el fin de preservar como activo más valorado la información de sus clientes.

TFM

ELABORACIÓN DE UN PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2013 PARA UNA EMPRESA DE LA INDUSTRIA COSMÉTICA

Borbon, Diana

Universitat Oberta de Catalunya
uoc.edu

TFM: ELABORACIÓN DE PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2013 PARA UNA EMPRESA DE LA INDUSTRIA COSMÉTICA

ELABORADO POR:
DIANA BORBÓN

TUTOR A CARGO:
ANTONIO JOSE SEGOVIA

TFM- SISTEMAS DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN
UNIVERSITAT OBERTA DE CATALUNYA
2018

© Diana Borbón

Reservados todos los derechos. Está prohibida la reproducción total, o parcial de esta obra por cualquier medio o procedimiento, comprendidos la impresión, la reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler y préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual.

ÍNDICE

TABLA DE ILUSTRACIONES

TABLA DE ANEXOS

1. INTRODUCCIÓN

La información se ha establecido como uno de los activos más importantes de las organizaciones, por ende, garantizar su seguridad debe ser una prioridad para los directivos. Un gran número de organizaciones se han enfocado en garantizar criterios mínimos de seguridad para la información como lo son: confidencialidad, Integridad y confiabilidad. La empresa para quien se realiza el análisis ha ingresado en el ciclo de toma de conciencia y sensibilización frente a los riesgos que puede acarrear la falta de protección a la información.

De otro lado, el modelo de seguridad de la información se ha venido implementando con mayor fuerza en países latinoamericanos durante los últimos años, y Colombia no es ajeno a ello. Este país ha reforzado su legislación para proteger los datos personales de sus ciudadanos a través de la Ley 1273 de 2009, 1266 de 2008 y 1581 de 2012. El gobierno nacional ha propendido la implementación de sistemas de gestión de seguridad de la información basados en el estándar ISO 27001:2013, ISO 27002 e ISO 27005 en las instituciones de carácter público a través de la estrategia de gobierno en línea.

Tras lo anterior, el SGSI se convirtió en un sello de calidad y protección a los datos de la población colombiana que garantiza el cumplimiento de estándares mínimos sobre la seguridad de la información. Por tal razón, este TFM (Trabajo Final de Máster) se orienta a la definición de un plan Director de Seguridad enfocado en el estudio realizado a una empresa y basado en los estándares ISO 27001:2013 y 27002.

2. GLOSARIO DE TÉRMINOS

- **Amenaza.** Es una acción que se vale de una vulnerabilidad para penetrar la seguridad de un sistema de información, pueden ser de tipo físico, lógico o factores humanos.
- **Auditoría Informática.** Es un proceso que se establece como esencial en la implementación de un SGSI donde se recopilan, agrupan y evalúan evidencias para determinar la eficiencia y eficacia de un SGSI a través de la prueba de controles y procedimientos.
- **Confidencialidad.** Sólo las personas autorizadas deben tener acceso a la información sensible o restringida.
- **Control.** Es un proceso o medida de carácter preventivo o correctivo generada con el fin de contener, mitigar o disminuir un riesgo existente o probable.
- **Criptografía.** Ciencia que se ocupa del diseño de métodos para el cifrado de datos.
- **Declaración de Aplicabilidad.** También conocida como SoA (Statement of Applicability) es un documento que según la norma ISO 27001:2013 contiene 114 controles donde el comité de la seguridad de la información define cuáles de éstos se aplican a la organización.
- **Disponibilidad.** Término que hace referencia a la disponibilidad de la información para usuarios autorizados cuando lo necesiten.

- **Eficacia.** Es la capacidad para lograr un objetivo o algo esperado.
- **Eficiencia.** Capacidad de emplear recursos adecuadamente para la consecución de un fin.
- **Evidencia.** Es un medio para probar las conclusiones dadas generalmente por el auditor, puede ser física, digital, procesos o procedimientos.
- **Hallazgo.** Es una debilidad del SGSI encontrada y debidamente reportada por el auditor.
- **Integridad.** La información y sus métodos de procesamiento no pueden ser manipulados sin autorización existente.
- **Incidente.** Evento o serie de eventos de la seguridad de la información cuyo origen es inesperado por la organización ya que compromete la seguridad.
- **Impacto.** Nivel de resultado de un incidente o del efecto que puede producir una amenaza.
- **No conformidad.** Es un incumplimiento a un requisito del sistema sea especificado o no. Puede clasificarse como no conformidad mayor o menor según la gravedad de afectación al sistema de gestión de información.
- **Política.** Documento gestionado, aprobado y publicado por la organización a sus colaboradores, funcionarios y demás con el fin de informarlos sobre directrices o normatividades que se deben acatar.
- **Procedimiento.** Es un compendio escrito sobre las actividades que se llevan a cabo durante la ejecución de un proceso.
- **Riesgo.** Probabilidad de que se produzca un incidente de seguridad en el sistema.
- **Riesgo Residual.** Es el riesgo que permanece luego de haber sido evaluado por los controles y las directivas de la organización.
- **Salvaguarda.** Procedimiento, método o mecanismo tecnológico para reducir un riesgo.
- **Seguridad de la Información.** Se encarga de la protección de la información sin importar su forma o recipiente, garantizando la disponibilidad, integridad y confidencialidad de la misma.
- **S.G.S.I.** Siglas de Sistema de Gestión de la Seguridad de la Información.
- **Vulnerabilidad.** Fallo o debilidad de una aplicación o sistema de información que lo expone a ser atacado comprometiendo su seguridad.

3. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

En términos generales, aunque la organización carece de políticas robustas para la seguridad de la información, ha dado los primeros pasos para asegurar que los procesos que intervienen con la seguridad de la información sean certificados a través de la implementación de estándares internacionales como las normas ISO 27001 y 27002.

3.1 DEFINICIÓN DE EMPRESA

La empresa seleccionada es una entidad local que se dedica a la venta de productos cosméticos. Con más de 15 años en el mercado, su domicilio principal se encuentra ubicado en una zona industrial cercana a la ciudad de Bogotá, posee 4 sucursales a nivel nacional y una sede administrativa ubicada en la capital de la república. Su fuerza laboral se compone de una plantilla de más de 100 trabajadores, de los cuales el 40% es de tipo administrativo y el 60% restante desempeñan funciones operativas. Catalogándose, así como una empresa de tamaño medio.

3.2 ORGANIGRAMA

Como se denota en el organigrama, el área de IT es de tipo transversal en la compañía y tiene dependencia directa a la Gerencia General, en cuanto al departamento responsable de la seguridad de la información, por la asignación de responsabilidades dentro de la organización, éste debe ser un órgano independiente a las demás gerencias y con reporte directo al presidente de la organización o gerente general.

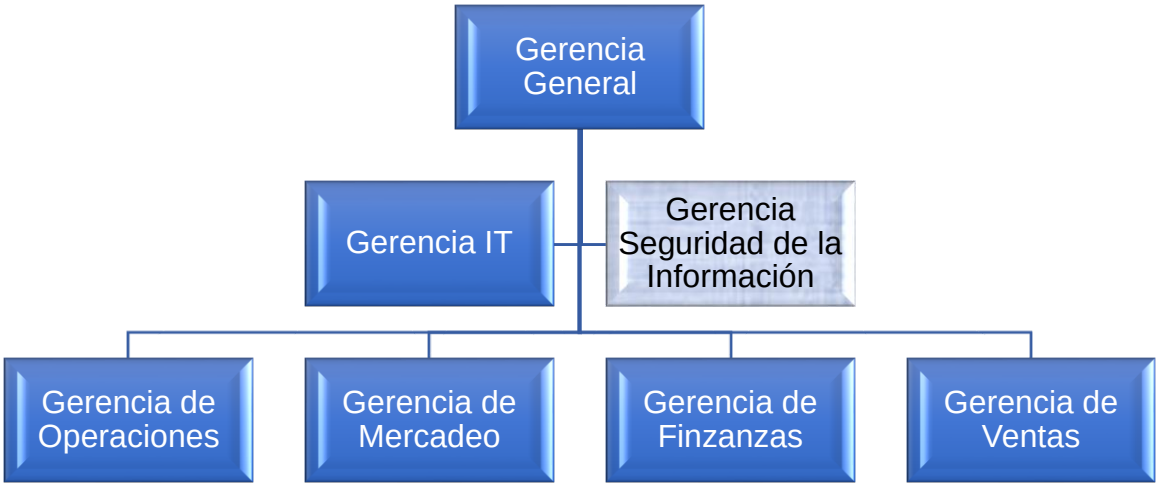

Gráfico 1. Organigrama de la compañía seleccionada. Vista primer nivel.

3.3 OBJETIVOS

3.3.1 Objetivo General

Desarrollar el plan Director de seguridad de la información para una compañía del sector cosmético, siguiendo los parámetros establecidos previamente por los estándares ISO 27001 y 27002 de 2013.

3.3.2 Objetivos Específicos

- Garantizar a los funcionarios, proveedores y contratistas la integridad, confidencialidad y disponibilidad de los datos cedidos debido al origen de los vínculos comerciales a través del desarrollo de controles de seguridad de la información.
- Cumplir con los estándares y/o normativas de seguridad de la información recomendados por el MINTIC -Ministerio de las tecnologías de la información y las comunicaciones.
- Concienciar a los miembros de la organización sobre las responsabilidades y los roles asignados en cuanto a la seguridad de la información.
- Mejorar los niveles existentes de seguridad de la información dentro de la organización creando una cultura de sensibilización para la identificación y prevención de riesgos.
- Identificar y clasificar los riesgos según sus niveles de criticidad, especificando las acciones de mitigación y los actores que intervienen en cada caso.
- Generar sensibilidad a la mesa de directivos sobre la importancia de la seguridad de la información en la organización, para así gestionar acceso a recursos y apoyo.

3.4 ALCANCE

Este plan Director de la seguridad de la información se enfocará en el análisis de los procesos catalogados como críticos por la organización y que son administrados o gestionados por el área de IT, aplicando la normativa descrita en las normas ISO 27001 y 27002 de 2013 para ser entregado a la mesa directiva de la organización.

Se entienden como procesos críticos de IT todos aquellos que con su detención tienen como consecuencia perdida de operatividad total de la organización en función a la seguridad de la información y su objeto de negocio.

3.5 TRANSICIÓN DE SISTEMAS DE INFORMACIÓN

La empresa inició sus operaciones sobre los años 90s adquiriendo desde su casa matriz un software tipo DOS para sus operaciones internas, es decir, administrado por los empleados de la compañía. Los clientes contaban con una plataforma online para sus transacciones, en cuento a la base de datos se encontraba centralizada en un motor local. Posteriormente y tras el crecimiento sostenido de la organización, se decidió migrar a un ERP desarrollado en tecnología Oracle que mejoró notablemente la velocidad de

procesamiento de las transacciones llevadas a cabo por los empleados y clientes. Dicho ERP es empleado actualmente.

3.6 ESTADO ACTUAL

La empresa carece de controles sobre la seguridad de la información, no existen políticas creadas o comunicadas y tampoco una matriz de análisis de riesgos, nunca se ha realizado un análisis de vulnerabilidades o sensibilización a los usuarios. Esto se debe en parte a que la junta directiva de la compañía ha restado recursos al departamento de IT infiriendo verla como soporte a usuario final. Las aplicaciones diseñadas por la compañía tienen parámetros de seguridad para ingreso y gestión de acceso.

El departamento de IT es administrado por un Coordinador de tecnología y un Ingeniero de Soporte. El coordinador es el primer responsable sobre anomalías de seguridad de la Información, fallas de aplicaciones o carencia de disponibilidad en los servicios de red. Reportan a una gerencia local y a una regional.

En esta compañía, IT se encuentra dividido en dos grandes áreas: Lógica de Negocio e infraestructura, este departamento se contempla como tipo trasversal y no funcional dentro de la organización.

El departamento entrega cada año a Finanzas un acta de reporte de gestión del año inmediatamente anterior para cumplir con el requisito de auditoría general. La empresa nunca ha llevado a cabo una auditoría de sistemas.

3.7 INFRAESTRUCTURA DE IT

El área de Infraestructura se encarga de gestionar los activos tecnológicos y tangibles de la compañía, así como también la administración de networking, gestión de disponibilidad de servicios de conectividad y mantenimientos.

La organización posee una distribución de red centralizada y gestionada desde su sucursal administrativa, cada sede cuenta con servicios de Internet y MPLS, así como Wifi administrado desde un WLC, como lo muestra el siguiente esquema de alto nivel:

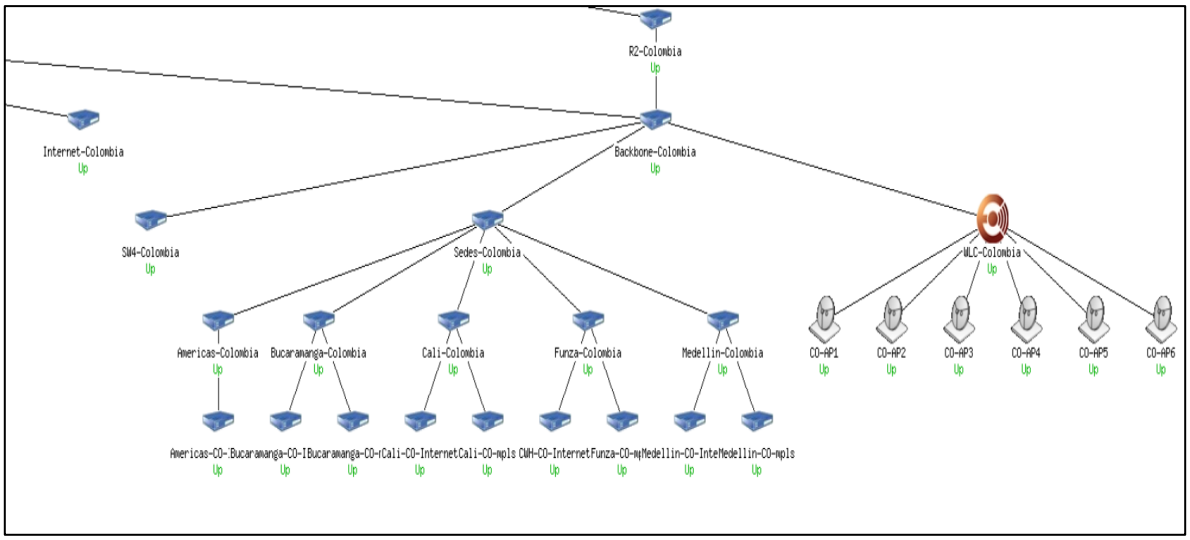

Gráfico 2. Diagrama de red de alto nivel

Según la sede, la compañía se compone de lo siguiente:

a) Centros de Cómputo:

i. Sistema de UPS redundantes (sólo para almacén y sede administrativa) para las demás, existen reguladores de sistema eléctrico.
ii. Banco de Baterías que respaldan la continuidad eléctrica en el almacén y sede administrativa durante máximo 2 horas con consumo mínimo.

iii. Networking:
- Routers Cisco de administración y de proveedores de servicio.
- Switches Cisco Capa 3.
- AP Cisco para la gestión de redes wifi.

iv. Servidores:
- Storage Dell con redundancia de Discos.
- Virtualización con gestión de VWare.
- Impresión centralizada.

v. Sistema de Aires Acondicionados.
vi. Sistema de control de acceso Biométrico.
vii. Sistema de detección de incendios.
viii. Sistema de video vigilancia en la sede administrativa.

b) Hardware para operatividad:

i. Desktops y Laptops con un tiempo de vida útil no mayor a 5 años.
ii. Lectores de códigos de barras (manuales y de mesa)
iii. Impresoras multifuncionales, de etiquetas y colillas de pago.

iv. Proyectores de video.

c) Software y aplicativos:

Todo el software se encuentra soportado con su debido licenciamiento.

i. Office 365 licenciamiento a 1 año
ii. Symantec cloud Endpoint
iii. Suite gráfica Abode
iv. Software de gestión contable
v. Motor de gestión de BD PL/SQL
vi. Windows License OEM (7, 10, server 2008 y 2012 R2)
vii. Team Viewer versión 11.0
viii. Además de lo anterior, la empresa cuenta con un software de gestión interna diseñado en PHP y para uso Intranet que usa para control de asistencia y gestión de compras, el motor de base de datos es sqlserver.
ix. Sitio web corporativo. Diseñado como plataforma ecommerce para transacciones de los clientes: Compra de productos, acceso a reportes, gestión de reclamaciones, chat e información corporativa.
x. ERP Oracle: Gestión interna de empleados, módulos de: gestión de órdenes, clientes, finanzas, ventas, mantenimiento, usuarios, inventario y compras de producto.
xi. Repositorios de información tipo sharepoint.
xii. Active Directory. Los usuarios y máquinas deben pertenecer al dominio para la autenticación en red.
xiii. Software de control de turnos de tipo externo para atención de clientes en las sucursales.
xiv. Cisco VPN para conexión de usuarios fuera de las instalaciones de la compañía.

d) Comunicaciones:

i. Canal de Internet dedicado en oficina principal. 30 Mb
ii. Servicios de Internet banda ancha en las demás sedes (8 Mb)
iii. Servicio de MPLS en todas las sucursales (2 Mb)
iv. Sip Trunk (telefonía IP) 90 canales como canal Principal
v. Sip Trunk 30 canales como canal de respaldo.
vi. Servicio de MPLS internacional (2 Mb)
vii. Mensajería webservice y de texto a través de proveedor externo.
viii. Internet banda ancha para visitas y clientes en la sede administrativa.
ix. Administración de dispositivos cisco a través de contratos Smartnet.

e) Servicios Externos Contratados:

i. Ingeniero de Soporte en IT
ii. Aseo y vigilancia en las instalaciones
iii. Impresión
iv. Asesoría Jurídica.
v. Transporte de mercancías.

3.8 LÓGICA DE NEGOCIO DE IT

Esta área es la encargada del tratamiento de la información y operaciones transaccionales entre el ERP, el sitio web y la base de datos. Aunque tiene acceso a la Base de datos de producción, no interviene en el área de desarrollo y testing.

3.9 ANÁLISIS DIFERENCIAL ENTRE ISO 27001:2013 – ISO 27002:2013

El análisis diferencial permite entender el estado actual de la organización visto desde la seguridad de la información, este análisis contempla áreas de gestión administrativa, legales y técnicas. Tras la obtención e interpretación de los resultados, se puede generar conciencia sobre el equipo directivo de las necesidades y/o falencias actuales, así como también tener un conjunto de directrices para el diseño del plan Director de Seguridad de la información y desde luego, enfocar a la organización para la implementación de un SGSI.

3.9.1 ISO 27001 y 27002:2013

"*El origen de la norma ISO 27001 se remonta a 1998 y se basa en la BSI (British Standard Institution) norma británica certificable. La primera versión certificable de la ISO 27001 fue publicada el 15 de Octubre de 2005.*

ISO 27001 contiene un anexo A, que considera los controles de la norma ISO 27002 para su posible aplicación en el SGSI que implante cada organización (justificando, en el documento denominado "Declaración de Aplicabilidad", los motivos de exclusión de aquellos que finalmente no sean necesarios). ISO 27002 es para ISO 27001, por tanto, una relación de controles necesarios para garantizar la seguridad de la información.

Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Actualmente, la última edición de 2013 este estándar se encuentra en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013. Desde el 12 de Noviembre de 2014, esta norma está publicada en España como UNE-ISO/IEC 27001:2014 y puede adquirirse online en AENOR. En 2015, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2014/Cor 1:2015) y en Diciembre de 2015 una segunda modificación (ISO/IEC 27001:2013/Cor.2:2015) esta última matizando especificaciones en la declaración de aplicabilidad. Otros países donde también está

publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27001), Chile (NCh-ISO27001) o Uruguay(UNIT-ISO/IEC 27001).

ISO 27002 es un conjunto de buenas prácticas en seguridad de la información. Contiene 114 controles aplicables (en relación a la gestión de la continuidad de negocio, la gestión de incidentes de seguridad, control de accesos o regulación de las actividades del personal interno o externo, entre otros muchos), que ayudarán a la organización a implantar medidas que reduzcan sus riesgos en cuanto a seguridad de la información. Su origen está en la norma de BSI (British Standards Institution) BS7799-Parte 1, que fue publicada por primera vez en 1995. No es certificable.

A partir del 1 de Julio de 2007, ISO 17799:2005 pasó a denominarse ISO 27002:2005, cambiando únicamente su nomenclatura. Actualmente, la última edición de 2013 este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013."[1]

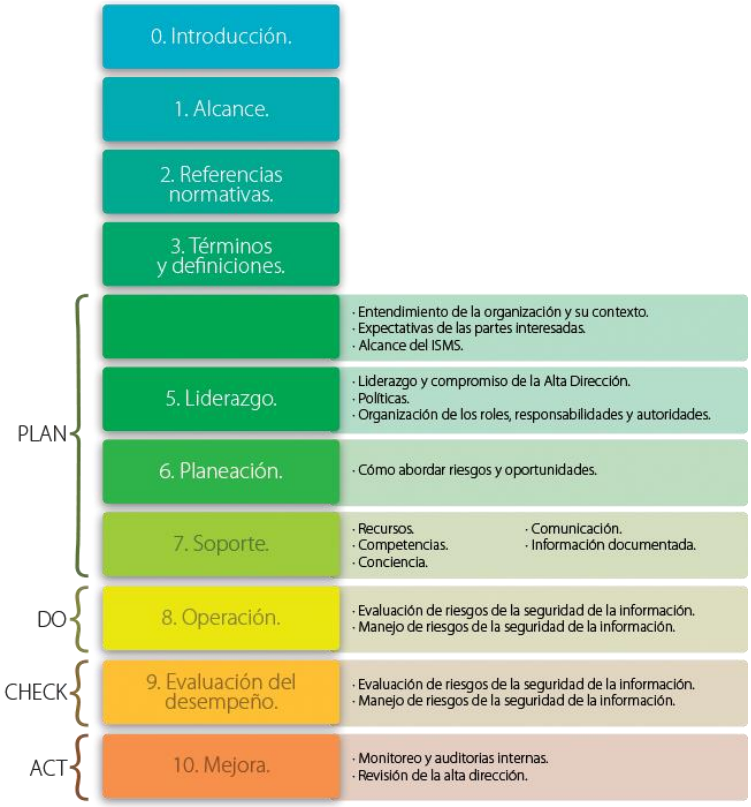

Gráfico 3. Nuevo Esquema ISO 27001:2013

Fuente: http://www.magazcitum.com.mx/?p=2397#.WDR9nH1tXsY

[1] http://www.iso27000.es/faqs.html. Evolución e historia de las normas ISO 27001 y 27002.

A continuación, se detalla el resumen ejecutivo de la evaluación de los controles detallados en la norma y aplicados a la situación actual de la empresa.

Como se muestra en el gráfico, la organización presenta un nivel se seguridad de la información deficiente, ya que sólo alcanza un porcentaje mayor al 50% en la fase inicial de contexto de la organización, lo que demuestra el compromiso de la dirección para transformar su situación a un ambiente de confianza en torno a la gestión de la seguridad de la información.

De los 7 dominios evaluados, 3 tienen una gestión de cumplimiento nula, 3 son menores al 20% pudiéndose interpretar según los criterios de evaluación que han sido planeados más no se encuentran en desarrollo. La organización tan sólo alcanza un 75% sobre el dominio de contexto de la organización.

Dicho lo anterior, se hace imperativo gestionar el plan Director de la seguridad de la información.

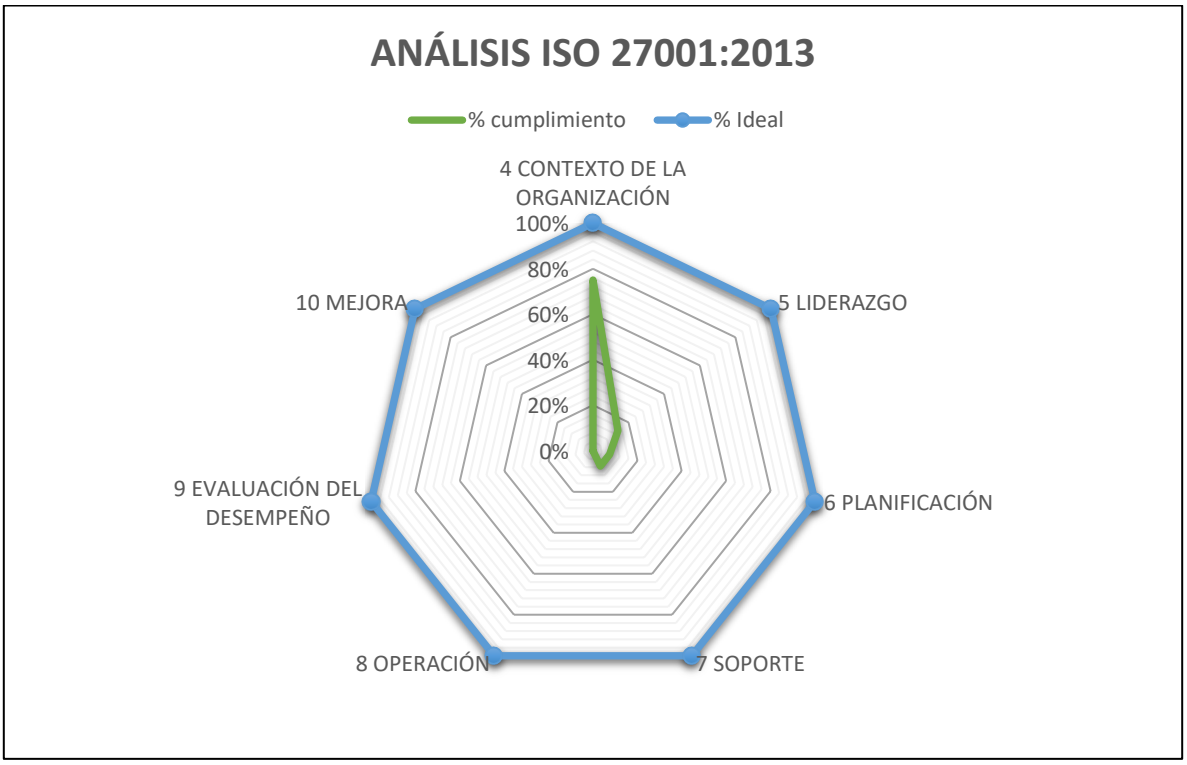

Gráfico 4. Análisis de la organización frente a la ISO 27001:2013

En cuanto a la norma ISO 27002:2013 el gráfico muestra una amplia madurez en la seguridad de las operaciones y grandes oportunidades de mejora en el cumplimiento de los demás controles. A partir de la visualización del siguiente gráfico se puede concluir que la organización necesita enfocarse en la formalización y comunicación de los procesos relacionados a la seguridad de la información, pues la mayoría de sus controles se encuentran en un estado de madurez entre el 20 y 30% sobre un estado máximo del 100%. Como soporte de la evaluación, se genera el siguiente documento anexo:

Anexo 1. Análisis diferencial.xlsx

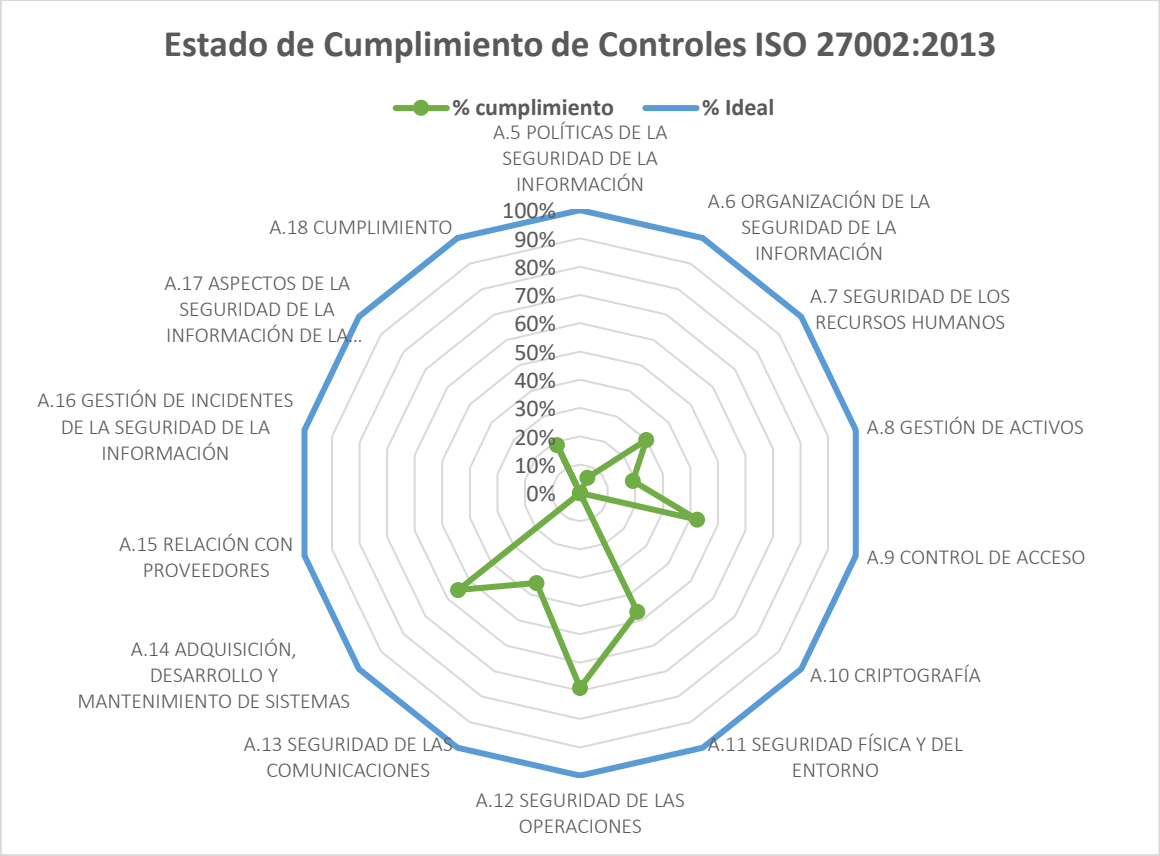

Gráfico 5. Análisis de la organización frente a los controles de la norma ISO 27002:2013.

3.10 RESULTADOS

El análisis de las gráficas obtenidas muestra un bajo nivel de madurez en la organización en cuanto al manejo de políticas documentales enfocadas en la seguridad de la Información. Aunque mediante el análisis numérico se puede inferir que la organización ha venido adelantando políticas y controles para procesos críticos de IT, aún no alcanza el umbral de tolerancia requerido para salvaguardar la seguridad de la información.

Según lo anterior, la organización en su estado actual tiene varias oportunidades de mejora que pueden sanearse a través de la implementación de un SGSI. La ventaja aparente, es la toma de conciencia de la línea directiva para fortalecer la seguridad de la información.

Tras analizar el estado actual de la compañía en su línea de seguridad de la información se adoptan las siguientes fases para el desarrollo del proyecto:

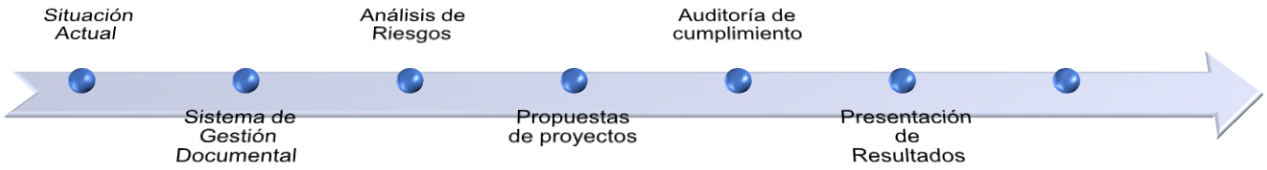

Gráfico 6. Fases para el desarrollo del plan director de seguridad de la información.

4. SISTEMA DE GESTIÓN DOCUMENTAL

Esta fase del plan director está constituida por la documentación formal que soporta el SGSI, tales como: políticas y procedimientos aprobados por la dirección, publicadas y comunicadas a los actores que intervienen en el SGSI.

4.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo con la norma ISO 27001:2013, la alta dirección debe generar una política que sea comunicada, esté disponible a las partes interesadas y debe estar documentada. Esta política propende la cultura y conciencia sobre la seguridad de la información a empleados, proveedores y contratistas. Las políticas de seguridad de la información deben ser de obligatorio cumplimiento por parte de cualquier individuo que tenga relación con la organización. Para dar cumplimiento a lo anterior, la dirección establece lo siguiente:

4.1.1 Objetivo

Definir la estrategia para asegurar la protección a la seguridad de la información en la organización basada en la norma ISO 27001:2013.

4.1.2 Aplicabilidad

Estas políticas aplican a todos los individuos u organizaciones de cualquier índole que tengan relación con la organización, entre ellos: empleados, clientes, proveedores y contratistas.

4.1.3 Directrices

a) Todos los individuos y organizaciones que tengan relación con la información son responsables y están obligados a cumplir con las normas, políticas y procedimientos de la seguridad de la información relacionadas en la presente política.
b) Se debe realizar un control periódico para garantizar que se revisen, modifiquen e implementen las políticas de seguridad de la información.
c) Establecer un sistema educacional para clientes, empleados, proveedores y contratistas que promueva la cultura organizacional en torno a la seguridad de la información.
d) Generar y monitorear el plan de auditoría sobre el SGSI que garantice el cumplimiento de lo establecido.
e) Los gerentes y jefes de área deben garantizar que se cumpla la reglamentación establecida en torno a la seguridad de la información.
f) Debe existir un compromiso y respaldo constante por parte de la dirección de la organización a lo establecido en el SGSI.

Como anexos a este documento se generan las siguientes políticas que complementan este capítulo:

Anexo 2. Política para la organización de la seguridad de la información.docx
Anexo 3. Política para uso de dispositivos móviles. docx
Anexo 4. Política de seguridad de la información para recursos humanos. docx
Anexo 5. Política de gestión de activos.docx
Anexo 6. Política de uso de equipos de cómputo.docx
Anexo 7. Política de uso de internet.docx
Anexo 8. Política de clasificación de la Información.docx
Anexo 9. Política de control de acceso.docx

4.2 PROCEDIMIENTO DE AUDITORÍAS INTERNAS

La norma ISO 27001:2013 determina que la organización debe llevar a cabo auditorías periódicas para proporcionar información acerca del estado del SGSI que determinarán el grado de madurez y de cumplimiento del SGSI. Dicho procedimiento debe plantear los objetivos, alcance y criterios de selección y valoración del equipo auditor, así como las NO conformidades y su tratamiento.

Para conformidad de este numeral, la organización ha generado el siguiente documento anexo:

Anexo 10. Procedimiento de Auditoría Interna.docx

4.3 GESTIÓN DE INDICADORES

Además de los controles relacionados por la norma ISO 27002:2013, las métricas asociadas al SGSI permiten conocer su evolución e impacto en la organización, por tal razón deben contener como mínimo las siguientes características:

a) Relacionar impactos financieros y se seguridad con los objetivos planteados por el SGSI.
b) Generar proyección tras el análisis numérico.
c) Estar relacionadas con los objetivos de negocio.
d) Demostrar la evolución de la cultura de la seguridad de la información dentro de la organización.

El responsable de medir y monitorear estos indicadores debe ser el administrador de sistemas bajo la supervisión del auditor designado. Dichos resultados, serán publicados mensualmente a la organización y expuestos en el comité de seguridad de la información donde los miembros evaluarán su continuidad y progreso. La organización debe conservar soporte de estas mediciones como evidencia del proceso de gestión.

Según lo anterior, las métricas de gestión se determinan en el siguiente archivo y tendrán un período de revisión mensual:

Anexo 11. Gestión de Indicadores.xlsx

4.4 PROCEDIMIENTO DE REVISIÓN POR DIRECCIÓN

La dirección de la organización es responsable de la promoción y adopción del SGSI como cultura organizacional, así como de respaldar todo lo que ello conlleve. Durante la fase de implementación, la dirección deberá tener al menos 1 reunión mensual para determinar el porcentaje de avance y la revisión de documentación. Tras la Implementación y prueba, las reuniones del comité se realizarán de forma trimestral para evaluar los indicadores de gestión del SGSI, siempre que no exista un cambio que altere el SGSI. Los documentos mínimos por evaluar son:

Además, la dirección en conjunto con el comité de la seguridad de la Información se compromete a:

Proceso – Procedimiento	Documento de Soporte Final
Analizar el informe de resultados concernientes al análisis de riesgos, así como el avance en los planes de seguimiento y mejora continua.	Acta de compromiso firmada por la dirección y plan de tratamiento de riesgos.
Informe de mejora continua.	Acta firmada por la dirección.
Informes de auditorías identificando NO conformidades y los planes de acción efectuados.	Plan de acción modificado por la dirección y el comité.
Revisión de políticas de seguridad y su aplicabilidad en la organización.	Políticas modificadas y acta de comunicación a la organización.
Análisis de conformidad según la normatividad legal vigente.	Acta firmada por la dirección.
Indicadores de gestión.	Gráficos de análisis, acta firmada por la dirección.
Informe de incidentes y vulnerabilidades de la SI	Acta firmada por la dirección.
Informe de Implementación de controles para la mitigación de riesgos	Acta firmada por la dirección.
Informe financiero y costos asociados a la Seguridad de la Información.	Acta firmada por la dirección.

Gráfico 7. Responsabilidades de participación de la dirección.

Tras cada comité, se debe elaborar un acta con las conclusiones y/o acuerdos y debe ser enviada a cada miembro del equipo para las acciones pertinentes.

4.5 GESTIÓN DE ROLES Y RESPONSABILIDADES

Se asignan los siguientes roles dentro de la organización para el cumplimiento del SGSI, éstos pertenecen al departamento de Seguridad de la Información y son también parte del comité de seguridad de la información:

Oficial de Seguridad de la Información

Este rol es uno de los más importantes en la implementación del SGSI, básicamente otorga los lineamientos luego de analizar la estrategia corporativa y situación actual. Dentro de sus funciones se establecen las siguientes:

- Analizar los riesgos de forma frecuente y detallada.
- Diseñar los cronogramas de reuniones y auditorias.
- Ejecutar las acciones correctivas del SGSI.
- Establecer los requerimientos mínimos de seguridad para aplicaciones de software e implementación de hardware en la compañía.
- Elaborar un plan de mejora continua para la prevención y detección de vulnerabilidades.
- Establecer de manera permanente comunicación con las autoridades pertinentes para el caso de reportes de vulnerabilidades o ataques perpetrados contra la seguridad de la información, así como también con grupos de actualización, profesionales o colaborativos que permitan reforzar el SGSI.
- Emitir un informe trimestral para la dirección y el comité donde se evidencie su gestión dentro de la organización y la comunicación con entidades externas especializadas en seguridad de la información.

Jefe de Proyectos

Es el planeador del SGSI, la ejecución de recursos, tiempos y procesos será su responsabilidad, es la columna vertebral en la implementación del SGSI. Dentro de sus funciones se detallan las siguientes:

- Responsable de la ejecución de cada hito del SGSI.
- Gestionar los recursos y validar progresos.
- Designar a los líderes de cada departamento que deben integrar el comité de SGSI.
- Implementar las mejoras o recomendaciones referidas tras las auditorías del SGSI o revisión del Oficial de la seguridad.
- Realizar el levantamiento de perfiles y manual de funciones de los miembros que integran el SGSI.
- Llevar el control de las actas y acuerdos de las reuniones del comité de SGSI.
- Generar planes de capacitación para el staff y miembros del comité de SGSI.
- Redacción de documentación que soporta al SGSI.
- Emitir un informe trimestral para la organización donde se evidencie su gestión dentro de la organización y esté acorde al rol asignado dentro del SGSI.

Auditor de Seguridad de la Información

Su rol está orientado a validar y garantizar que el SGSI cumpla con lo esperado por la organización. Dentro de sus funciones se encuentran las siguientes:

- Validar la efectividad de los controles diseñados.
- Ejecutar pruebas periódicas para el análisis de vulnerabilidades.
- Garantizar el cumplimiento de la ley de protección de datos personales.
- Realizar documentación sobre cada actividad de control desarrollada.
- Generar recomendaciones a la alta gerencia sobre el desempeño del SGSI dentro de la organización.
- Validar la calidad de los resultados de cada actividad del SGSI.

Gerente de TI

Debe ser el enlace hacia la alta dirección de la organización, es el responsable de que la línea administrativa y que de la gestión no impida el avance de la implementación.

- Responsable de la toma de decisiones en conjunto con la alta gerencia.
- Alinear el SGSI con la estrategia IT y la estrategia corporativa.
- Revisar las políticas y objetivos del SGSI.
- Tomar decisiones tras el análisis de datos del SGSI para asegurar la mejora continua.
- Aprobar los recursos necesarios para el SGSI.
- Garantizar una correcta comunicación dentro de la organización entorno al SGSI.
- Garantizar en el staff el cumplimiento de políticas establecidas con relación al SGSI.

Administrador de Sistemas de la Seguridad de la Información

Es el rol que gestiona la varga operativa del SGSI. Dentro de sus funciones se encuentran:

- Gestionar incidencias de seguridad.
- Gestionar accesos.
- Realizar gestión de indicadores.
- Realizar la planeación de mantenimientos.
- Identificación de activos críticos.
- Ejecutar las acciones preventivas del SGSI.
- Gestionar el correcto inventario de activos de la compañía.

El comité de la seguridad de la Información se conforma además con los siguientes miembros:

- Gerente General
- Gerente de Operaciones
- Gerente Financiero
- Gerente de Ventas

- Finance Controller

4.5.1 Funciones del Comité de SGSI

- Revisar y aprobar periódicamente los cambios planteados al SGSI en su estructura, como: políticas, controles, documentación.
- Aprobar el plan de mejora continua plasmado como resultado de auditorías y controles internos.
- Revisar continuamente el estado general de la seguridad, a través de los reportes entregados por el líder de seguridad de la información y el auditor.
- Analizar los incidentes de seguridad y revisar los planes para eliminarlos o prevenirlos.
- Promover el apoyo a la política de seguridad de la información dentro de la organización generando una cultura organizacional para la adopción de la seguridad de la información.
- Gestionar los recursos para implementación y mantención del SGSI.

Como soporte de la asignación de responsabilidades, se genera el siguiente anexo para este numeral:

Anexo 12. Matriz RACI.xlsx

4.6 METODOLOGÍA DE ANÁLISIS DE RIESGOS

El análisis de riesgos es un pilar fundamental en todo SGSI, el objetivo es identificar aquellos activos y vulnerabilidades que pueden catalogarse como un riesgo para la organización y deben ser mitigados a través de los correspondientes controles para aceptar, disminuir, evitar o trasferir el riesgo. La organización ha decidido optar por la metodología MAGERIT -fue creada por el ministerio de administración pública- y contiene los siguientes elementos de riesgo potencial:

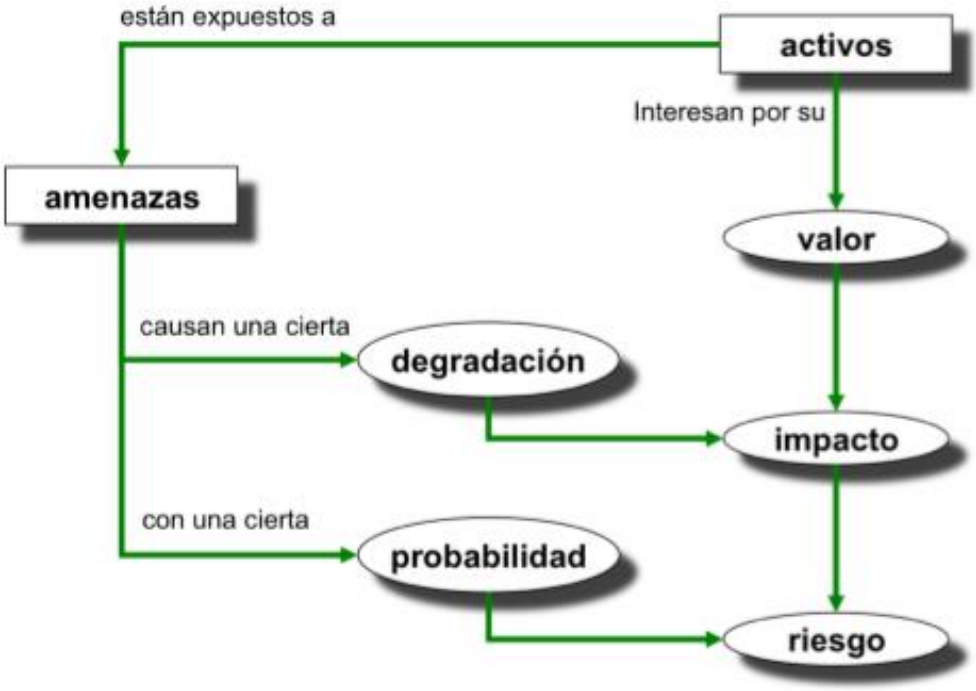

Gráfico 8. Elementos del análisis de riesgo potencial [2]

De acuerdo con la norma ISO 31000, la gestión de riesgo se estructura a través de las siguientes fases de aplicación a la organización:

[2] https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i.../file.html

Gráfico 9. Esquema de gestión de riesgos – análisis metodológico MAGERIT-

En la gestión de riesgos, se espera obtener lo siguiente:

a) Listado de activos. Valoración de acuerdo con los criterios de la organización, se debe especificar: Información y/o servicios que administra, valoración económica, cuantitativa y cualitativa, valor estimado de acuerdo con la interrupción del servicio, dependencia y dimensionamiento (confidencialidad, disponibilidad e integridad).
b) Identificación y clasificación de amenazas. Determinar la fuente que provee la vulnerabilidad y su relación con cada activo.
c) Valoración de las amenazas. Determinar el impacto que tendrá la vulnerabilidad sobre el activo en cuanto a degradación (daño causado por el incidente) y probabilidad ante la ocurrencia. Dicho impacto según Magerit puede ser evaluada bajo la siguiente referencia:

	Impacto	Valoración
MA	Muy Alta	100
A	Alta	10
M	Media	1
B	Baja	1/10
MB	Muy Baja	1/100

d) Determinación de riesgo potencial. Es la medida del posible daño sobre un sistema. El riesgo es directamente proporcional al impacto y la probabilidad. Se sugiere un mapa de calor para la identificación de la zona de riesgo:

   a. Zona 1. Riesgos muy probables y de alto impacto.
   b. Zona 2. Impacto medio, rango de situaciones improbables, impacto bajo.
   c. Zona 3. Riesgos improbables y de bajo impacto.
   d. Zona 4. Riesgos improbables, pero de alto impacto.

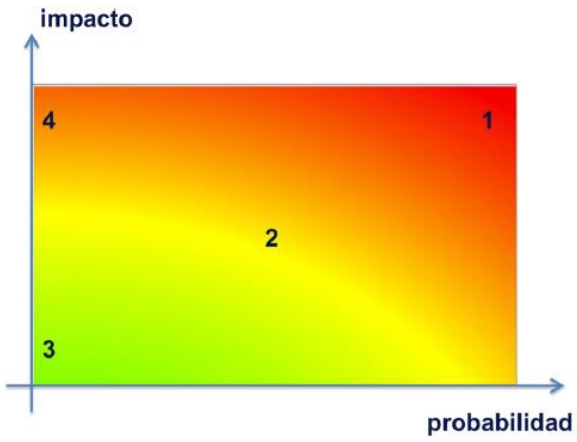

Gráfico 10. Riesgo en función del impacto y la probabilidad. [3]

e) Salvaguardas. Definidos como los controles o medidas de mitigación de riesgos. Pueden reducir la probabilidad de las amenazas y limitar el daño causado. Se debe relacionar el tipo de protección: prevención, disuasión, eliminación, reducción y detección que aplica en la organización.
f) Informe de vulnerabilidades. Detalla las salvaguardas necesarias, pero no existentes o no implementados.

[3] https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i.../file.html

4.7 DECLARACIÓN DE APLICABILIDAD

Este documento plantea los controles acogidos por la organización para el SGSI basado en el Anexo A del estándar ISO 27001:2013. Define la justificación de cada control y plantea evidencia de soporte para cada caso. La declaración de aplicabilidad se encuentra detallada en el siguiente documento anexo:

Anexo 13. Declaración de Aplicabilidad.xlsx

5. ANÁLISIS DE RIESGOS

Para el análisis y gestión de riesgos, se adopta la metodología Magerit 3.0 En esta fase, se consideran los activos, amenazas y salvaguardas del SGSI. Listando estos elementos, se puede valorar el impacto, probabilidad y el riesgo asociado a los activos de la organización.

5.1 TIPOS DE ACTIVOS

Según la metodología seleccionada, se tienen los siguientes tipos de activos para ser evaluados en la organización:

TIPO DE ACTIVOS	DESCRIPCIÓN
Activos Esenciales	**Datos importantes para la Organización:** Aquellos relevantes para la Organización, cuya afectación podría causar grave daño sobre la gestión de continuidad del negocio o afectar el cumplimiento legal de la legislación vigente. **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). **Datos Clasificados o Calificados:** Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Datos / Información	**Aquel que es almacenado mediante soporte digital, como archivos y bases de datos, puede ser trasladado de un lugar a otro.** Ejemplo: Copias de Respaldo, archivos, Datos de Gestión Interna, Datos de Configuración, Credenciales (Contraseñas), Datos de Validación de Credenciales (Autenticación), Datos de Control de Acceso, Registros de Actividad (Log), Matrices de Roles y Privilegios.

TIPO DE ACTIVOS	DESCRIPCIÓN
Servicios	**Toda aquella actividad de soporte encaminada al funcionamiento y estabilidad de los procesos de la Organización en el SGSI.** Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de archivos y su transferencia, intercambio electrónico de datos, Gestión de Identidades (altas y bajas de usuarios del sistema), Gestión de Privilegios, Intercambio electrónico de datos, entre otros.
Software / Aplicaciones Informáticas	**Todo el software ejecutado por el staff de la organización o inclusive el empleado solamente a través de scripts para funciones o controles.** Ejemplo: Desarrollo Inhouse, Desarrollo Subcontratado, Estándar, Navegador, Servidor de Presentación (www), Servidor de Aplicaciones (app), Cliente de Correo Electrónico, Servidor de Correo Electrónico, Servidor de Ficheros (file), Sistemas de Gestión de Bases de Datos (dbms), Monitor Transaccional, Ofimática, Antivirus, Sistema Operativo (OS), Sistema de Backup o Respaldo, Gestor de Máquinas Virtuales.
Hardware / Infraestructura	**Medios físicos cuyo objetivo es servir de soporte a las aplicaciones, almacenamiento de información y datos,** Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Dispositivos Móviles, Equipo de videovigilancia, Equipos de Respaldo, Periféricos, Dispositivos Biométricos, Servidores de Impresión, Impresoras, Escáneres, Equipos Virtuales (vhost), Soporte de la Red (Network), Módems, Hubs, switches, routes y otros dispositivos de red.
Redes de Comunicaciones	**Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro.** Ejemplo: Red de comunicaciones, servicios de telefonía IP, troncales SIP, Internet, MPLS.
Soportes de Información	**Dispositivos físicos que permiten el almacenamiento de la información.** Ejemplo: Discos, Almacenamiento en Red, Memorias USB, CDROM, DVD, Tarjetas de Memoria, Material Impreso, entre otros.
Equipos Auxiliares	**Equipos que permiten el funcionamiento o sirven de soporte a los medios de almacenamiento o contención de Información.** Ejemplo: Fuentes de alimentación, Aires Acondicionados, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, mobiliarios, cajas fuertes, entre otros.
Instalaciones	Lugares físicos donde se instalan los sistemas de información.
Personal	Usuarios internos, proveedores, y otros terceros (visitantes).

Gráfico 11. Clasificación de Activos según Magerit.
Basado en: Libro II – Magerit V3. Catálogo de Elementos.

5.2 VALORACIÓN DE LOS ACTIVOS

La valoración se orienta a cuán valioso puede llegar a ser un activo para una organización, pero no sólo en torno al valor de adquisición o comercial, está orientada al valor que tendría el activo en el caso de materialización de una amenaza. Ésta puede darse de forma cuantitativa o cualitativa, pero estimar aquellos activos de información tales como bases de datos es en extremo difícil, por tal razón, se selecciona una valoración de tipo cualitativa de acuerdo a la necesidad de protección que impere en la organización, el valor de un activo será directamente proporcional a la necesidad de protección; dicho valor puede ser asignado directamente el activo, o puede ser un resultado acumulado basado en un esquema de jerarquía de activos. Para ello, se obtiene la siguiente valoración sugerida:

Valoración Cualitativa	Valoración cuantitativa
Muy Alto	>=4.001 €
Alto	3.001 -4.000 €
Medio	2.001 -3.000 €
Bajo	1.001 - 2.000 €
Muy Bajo	1 - 1.000 €

Gráfico 12. Tabla con valores de estimación de riesgo

5.3 DIMENSIONES DE SEGURIDAD

Acorde a Magerit 3.0, luego de valorar a los activos, éstos deben dimensionarse de acuerdo con la seguridad de la Información y su criticidad, ello implica asignarles una escala según su confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad. Esta escala denominada ACIDT permite dimensionar el impacto que tendría la materialización de una vulnerabilidad sobre un activo determinado.

Dimensión	Definición
Autenticidad [A]	El objeto siempre debe ser quién dice ser. ¿Qué importancia tendría que quien accede al equipo no sea realmente quien se cree?

Dimensión	Definición
Confidencialidad de la información [C]	La información sólo debe estar disponible para las personas autorizadas. ¿Qué perjuicio causaría que alguien no autorizado conozca el activo?
Integridad de los datos [I]	Garantizar que la información no hay sido manipulada o esté corrupta. ¿Qué importancia tendría que los datos fueran modificados fuera de control?
Disponibilidad [D]	Los servicios pueden ser usados cuando se necesiten. ¿Qué importancia tendría que el activo no estuviera disponible?
Trazabilidad [T]	Registro o log de control durante el ciclo de acceso a la información. ¿Qué daño causaría no saber quién accede al activo y qué hace con ellos?

Gráfico 13. Conceptualización – Dimensiones de Seguridad de la Información
Basado en: Libro II – Magerit V3. Catálogo de Elementos.

Valor	Criterio
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Gráfico 14. Valoración de dimensiones de seguridad para un activo

Los activos también deben mostrar jerarquía, existen activos superiores que pueden verse afectados por las vulnerabilidades de activos inferiores. Para dar cumplimiento a la aplicabilidad de los puntos anteriores, se genera el siguiente documento como anexo donde se detallan los activos por sede:

Anexo 14. Inventario y Valoración de Activos.xlsx

A partir del siguiente gráfico se puede inferir que los activos más relevantes para la organización de acuerdo con una valoración cualitativa son aquellos clasificados como superiores y se agrupan en las categorías de Redes de comunicaciones, Aplicaciones, Datos y Hardware. Estas categorías representan un 50% o más de la valoración asignada por la organización:

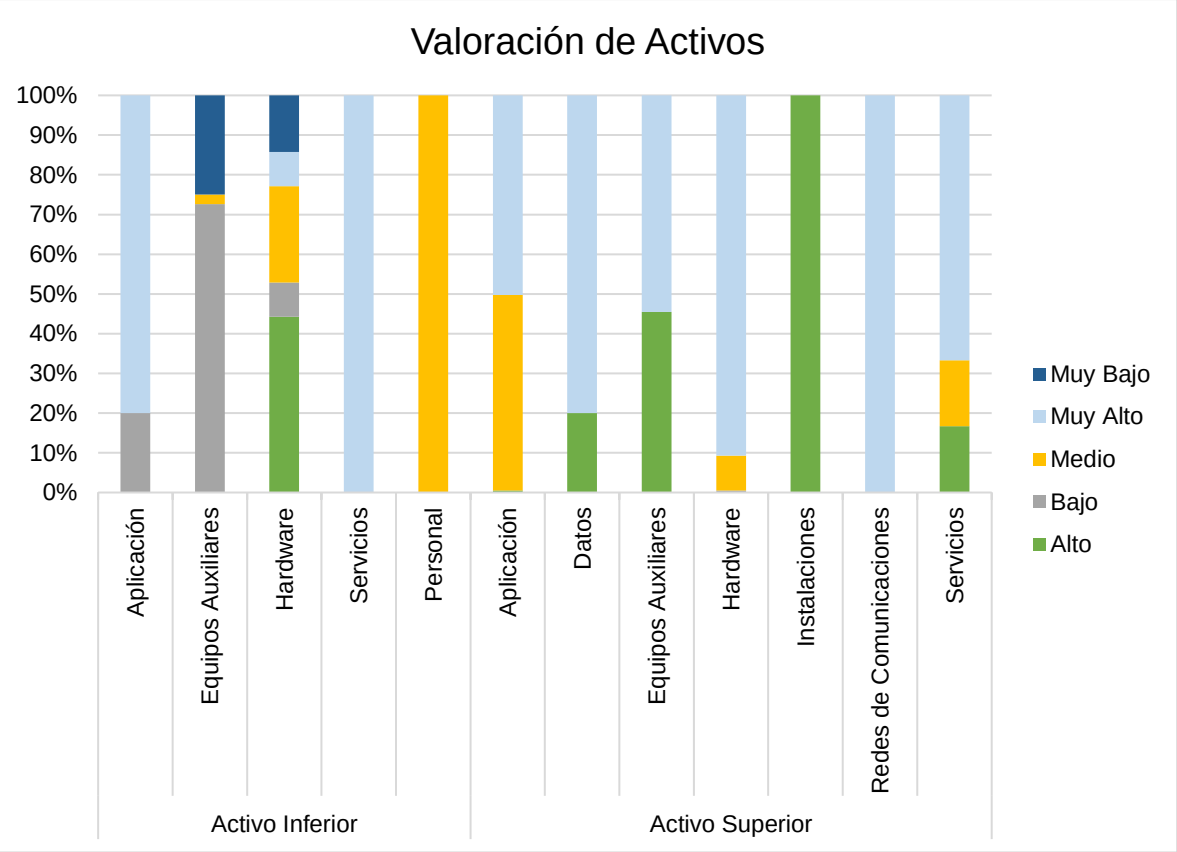

Gráfico 15. Valoración cualitativa de activos de la organización.

5.4 ANÁLISIS DE AMENAZAS

Todo activo de la organización puede estar expuesto a una amenaza, por ello, es relevante realizar un análisis que exponga a la dirección el grado de degradación, probabilidad e impacto que podría tener la materialización de una amenaza, de acuerdo con Magerit. Libro II – Catálogo de Elementos, se genera el siguiente documento anexo para este punto:

Anexo 15. Análisis de Amenazas.xlsx

Retomando, lo descrito en el numeral 4.6 se asigna la siguiente estimación de probabilidad y degradación sobre cada uno de los activos afectados por las amenazas descritas en el catálogo de Magerit:

	Probabilidad	Valoración	Degradación	Escala %
MA	Muy Alta	100	Muy Alta	>50
A	Alta	10	Alta	41-50
M	Media	1	Media	31-40
B	Baja	0,10	Baja	21-30
MB	Muy Baja	0,01	Muy Baja	0-20

Gráfico 16. Tabla de valores de probabilidad y degradación basada en Magerit.

El siguiente gráfico permite analizar la probabilidad de materialización de amenazas sobre los activos de la organización, notoriamente se puede observar que la categoría con mayor probabilidad de ocurrencia (46%) es la de Errores y fallos no intencionados, por tanto, los controles a desarrollar deberían estar enfocados en las amenazas que califican dentro de este grupo sin dejar atrás los desastres de origen Industrial, la probabilidad de afectación a causa de desastres naturales es casi nula:

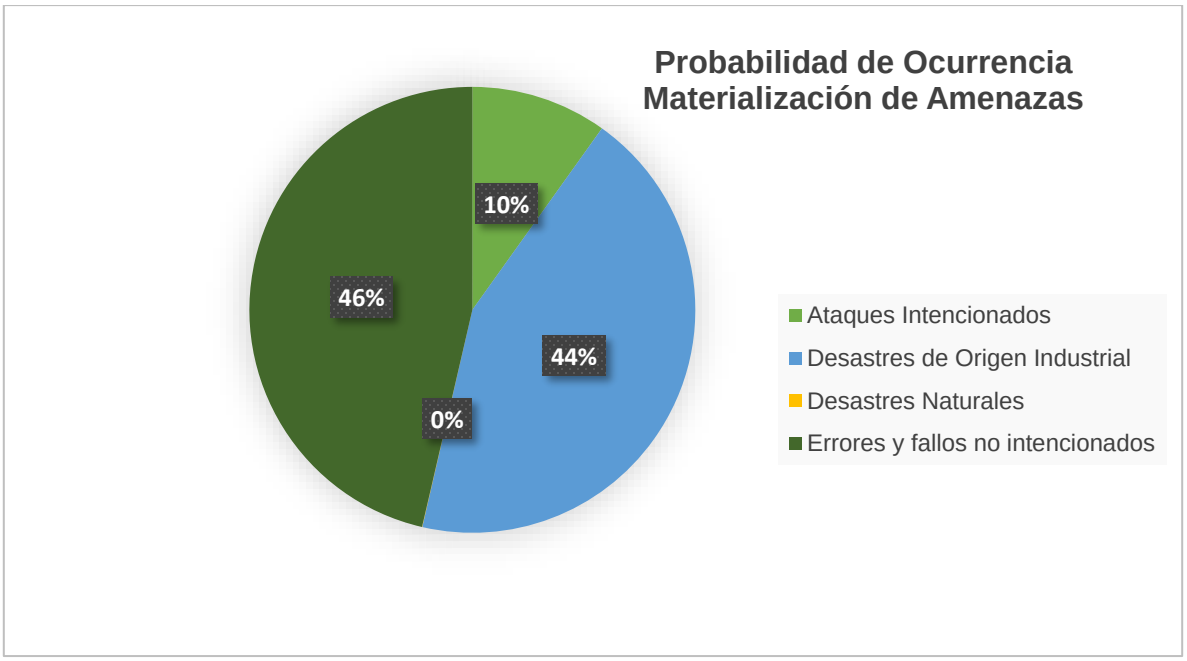

Gráfico 17. Probabilidad de Ocurrencia – Materialización de Amenazas.

En cuanto a la degradación de los activos, luego de la materialización de amenazas, el siguiente gráfico demuestra que, según las categorías de clasificación, los activos tienen una mayor degradación cuando se materializa un ataque malintencionado, por tanto, la organización debe enfocarse en mitigar dicho riesgo.

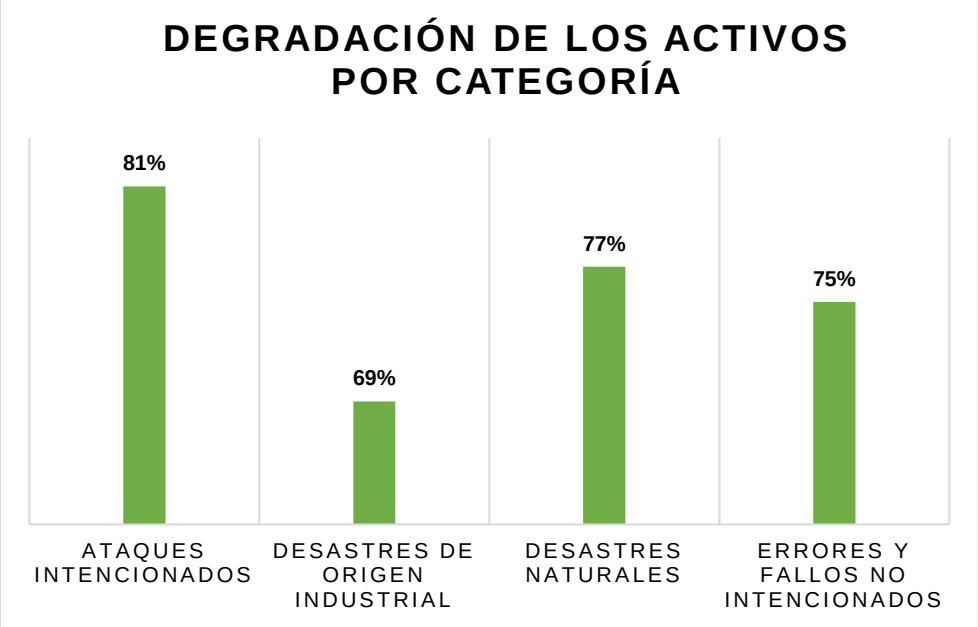

Gráfico 18. Degradación de los activos por categoría tras materialización de amenazas.

5.5 IMPACTO POTENCIAL

Consiste en medir el impacto de la materialización de una amenaza sobre el activo. Las variables que aplican son: valor de activos (dimensionamiento) y la degradación que causa la amenaza sobre éstos. Básicamente el valor se obtiene mediante:

Impacto Potencial = Valor del activo * Degradación.

El siguiente gráfico muestra el impacto monetario sobre las categorías de activos de la organización, el impacto de la materialización de vulnerabilidades representa un 77% sobre el valor total de los activos. La categoría que representa un mayor riesgo a nivel económico para la organización es la de ataques intencionados.

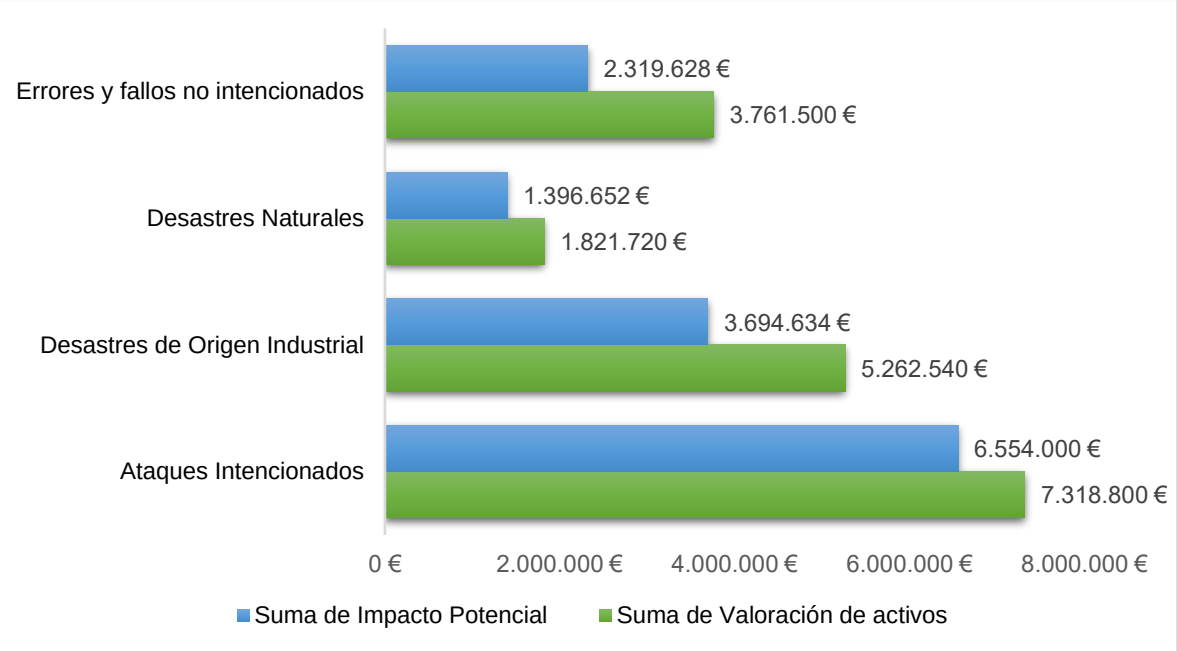

Gráfico 19. Impacto Potencial sobre activos.

5.6 NIVEL DE RIESGO ACEPTABLE Y RESIDUAL

El riesgo intrínseco es aquel que se evalúa sin tener en cuenta controles o medidas tomadas por la organización. La probabilidad y el impacto son directamente proporcionales, lo que quiere decir que el riesgo intrínseco será mayor si están dos variables son crecientes o en caso contrario, disminuirá.

Riesgo Intrínseco = Probabilidad * Impacto

El siguiente mapa de calor denota la relación dependiente de probabilidad e impacto como riesgo intrínseco según el modelo adoptado por la metodología Magerit. En riesgo extremo se encuentran los activos cuya clasificación se denote como: **MA-MA, MA-A, MA-M, A-MA, A-A, M-MA, M-A.** Para el caso, el 30% de los activos están evaluados dentro de esta zona de riesgo muy alta. Del mismo modo, se realizar la categorización como riesgos potenciales, acorde a Magerit del 1 al 4 y que se detalla en el numeral 4.6 de este documento.

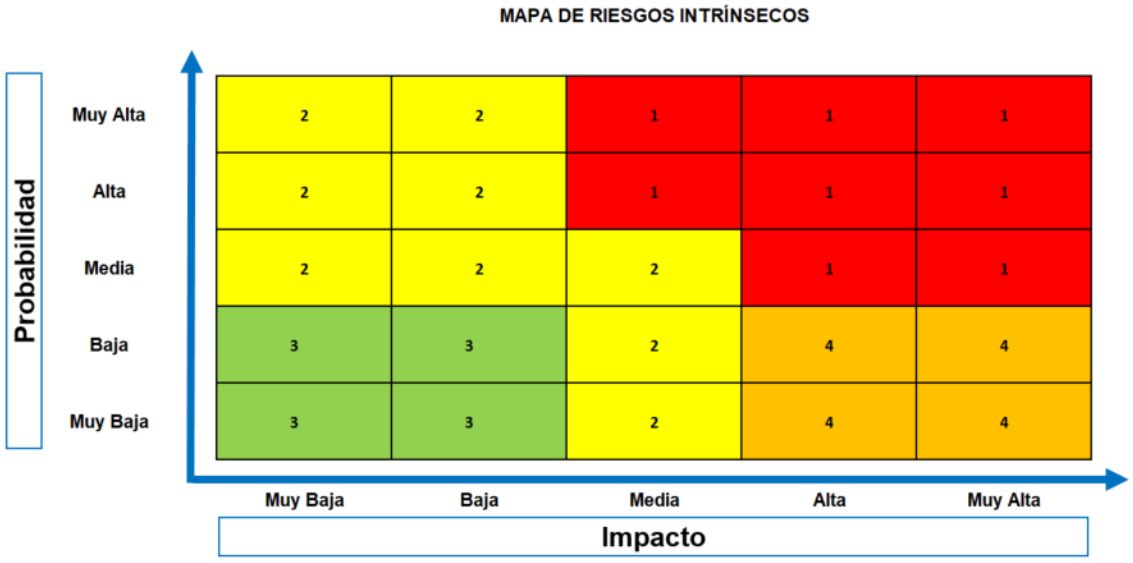

Gráfico 20. Mapa de calor para riesgos intrínsecos.

El nivel de riesgo aceptable por la organización se encuentra dentro del siguiente intervalo identificable en el gráfico 20 con el numeral 3 color verde, variables (probabilidad, Impacto):

a) MB-MB, MB-B, B-MB, B-B.

R1	Deben ser mitigados de inmediato, requiere un plan de tratamiento y atención inmediata por parte de la dirección y el SGSI.
R2	Requieren ser discutidos en el comité de seguridad del SGI para prevenir un aumento en el nivel de riesgo y la degradación del activo.
R3	El riesgo es asumido por la organización, se trata de mitigar con controles procedimentales.
R4	La probabilidad de ocurrencia es baja, pero por el acto impacto que una amenaza podría generar sobre los activos, éstos deben ser tratados y puestos en cola luego de evaluar R1 y R2.

Gráfico 21. Tabla de nivel de riesgo - aceptación

El siguiente gráfico evidencia la necesidad intrínseca de establecer controles a las vulnerabilidades que se originan por ataques intencionados ya que el 50% de los activos de la organización son susceptibles a esta categoría.

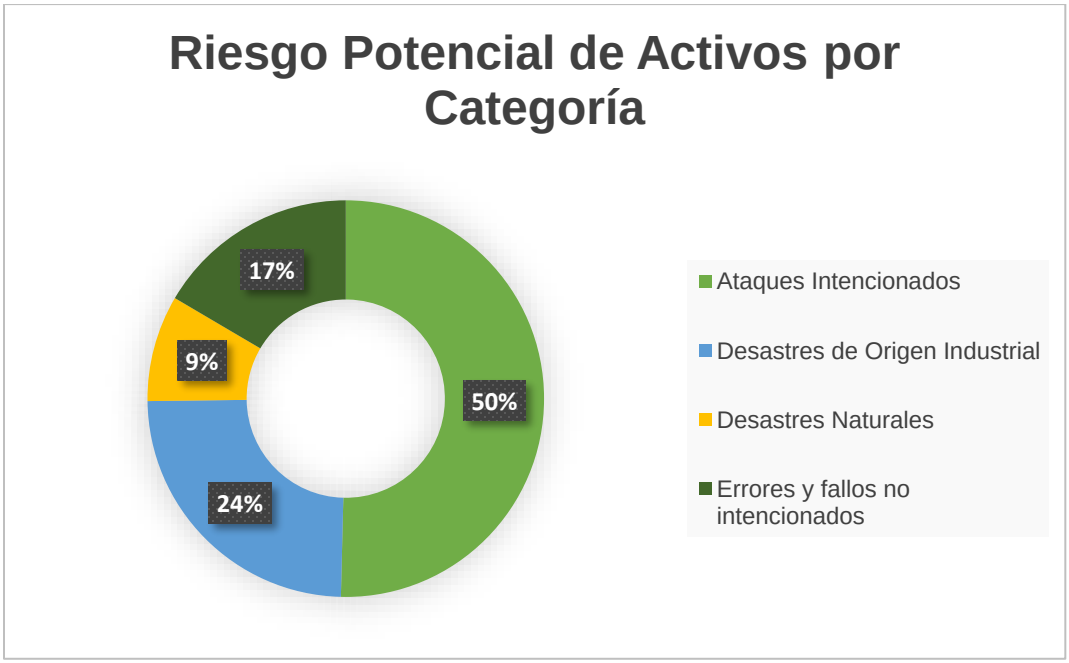

Gráfico 22. Riesgo Potencial de activos por categoría.

El riesgo residual es el que se obtiene luego de que la organización ha decidido la aprobación de los controles, o en su defecto decide aceptarlo. Se debe realizar una medición que determine la efectividad de los controles para disminuir el riesgo asociado a cada activo.

Estos deben ser evaluados en conjunto con el comité de Seguridad de la Información y aceptados por la dirección para su tratamiento.

Acorde al tratamiento de riesgos, se puede mencionar lo siguiente:

Tratamiento	Definición
Evitar el riesgo	El costo del tratamiento es muy superior a los beneficios.
Reducir o mitigar el riesgo	Seleccionar e implementar controles o medidas adecuadas que hagan que se reduzca la probabilidad y el impacto.
Transferir el riesgo	El costo del tratamiento por parte de un tercero otorga mayores beneficios que el tratamiento directo por parte de la organización.
Retener o aceptar el riesgo	Sólo monitorear, no es necesario implementar controles adicionales.

Gráfico 23. Ejemplo de criterios para tratamiento de riesgos. Incibe.

6. PROPUESTA DE PROYECTOS

En esta fase se analizan las opciones de proyectos que permitan cumplir con los objetivos del SGSI, se tiene en cuenta el resultado del análisis de riesgos de la fase anterior, en especial la aplicabilidad de controles sobre el despliegue de amenazas que pueden afectar a la organización. Estos proyectos deben presentar a la dirección una validación económica de origen cuantitativo y dar origen a un cronograma de aplicabilidad que denote realmente un ciclo de mejora continua en la organización.

La eliminación del riesgo es algo prácticamente improbable de llevar a cabo, pero como organización, la dirección debe decidir cuál es la mejor propuesta de aplicabilidad para la mitigación del riesgo e implementación de controles conservando la directriz de inversión económica a menor costo.

Acorde con la metodología Magerit V3.0, se trabajan las siguientes salvaguardas con el propósito de mitigar los riesgos en la organización:

N°	Grupo	Descripción Salvaguarda
1	[H]	Protecciones generales
2	[D]	Protección de la Información
3	[S]	Protección de los servicios
4	[SW]	Protección de las aplicaciones informáticas
5	[HW]	Protección de los equipos informáticos
6	[COM]	Protección de las comunicaciones
7	[AUX]	Elementos Auxiliares
8	[PS]	Gestión del personal
9	[G]	Organización
10	[BC]	Continuidad del negocio
11	[E]	Relaciones Externas

Gráfico 24. Lista de salvaguardas. Magerit 3.0

Según el cuadro anterior, en esta fase de desarrollarán 11 proyectos correspondientes a los grupos mencionados. Los detalles de las salvaguardas, impacto, y detalles del proyecto de seguridad se encuentran relacionados en el siguiente anexo:

Anexo 16. Proyectos de Seguridad.xlsx

La aplicación de proyectos de seguridad afecta directamente el nivel de riesgo, impacto y la valoración económica que generaría la materialización de la amenaza, por tal razón se realiza una modificación al siguiente anexo visualizando los resultados luego de la aplicación de los proyectos de seguridad:

Anexo 15. Análisis de Amenazas.xlsx

Se puede concluir a partir del siguiente gráfico que se reduce notablemente el valor del impacto potencial de los activos tras la implementación de proyectos de seguridad, reduciendo con ello las pérdidas o afectación material que tendría la organización en caso de sufrir la materialización de las amenazas contempladas en el anexo 15. El costo total de la implementación y mantenimiento de los proyectos es de: **202.000 EUR.**

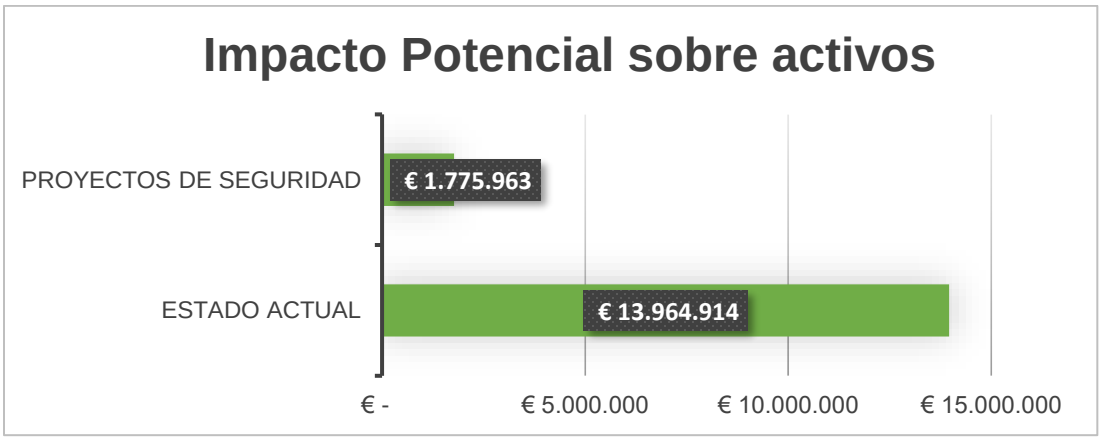

Gráfico 25. Análisis de Impacto potencial sobre activos vs. Proyectos de seguridad.

Antes de la implementación de los proyectos de seguridad, el impacto potencial sobre los activos tras la materialización de una amenaza equivale al **77%** del total de los mismos, mientras que, si la organización decide invertir **202.000 EUR** (1,11% del valor total de los activos) en proyectos de seguridad, la materialización de las amenazas sólo afectará los activos en un **10%** de su valor total como se especifica en el siguiente cuadro:

Categoría	Estado Actual	Proyectos de Seguridad
Impacto Potencial sobre activos	**€ 13.964.914**	**€ 1.775.963**
Valor porcentual de Impacto sobre el total de los activos	**77%**	**10%**
Valor total de los activos de la organización	**€ 18.164.560**	
Costo Total de Implementación de Proyectos	**€ 202.000**	

Gráfico 26. Análisis de costos tras la implementación de proyectos de seguridad.

6.1 CRONOGRAMA DE EJECUCIÓN DE PROYECTOS

La ejecución de todos los proyectos planteados para la compañía tiene una duración de 262 días o un año en horas laborales, el siguiente diagrama contiene la vista general del tiempo esperado para el desarrollo de cada etapa:

Estado	Proyectos de Seguridad	Fecha de Inicio	Fecha final
	Protecciones Generales	01/06/18	02/07/18
	Protección de la Información	03/07/18	03/09/18
	Protección de los servicios	04/09/18	28/09/18
	Protección de las Aplicaciones Informáticas	01/10/18	31/10/18
	Protección de los equipos Informáticos	01/11/18	30/11/18
	Protección de las Comunicaciones	03/12/18	31/12/18
	Elementos Auxiliares	01/01/19	01/02/19
	Gestión del Personal	04/02/19	02/05/19
	Organización	03/05/19	03/05/19

Gráfico 27. Cronograma para ejecución de proyectos de seguridad.

6.2 EVOLUCIÓN DE LA ISO 27001:2013 EN PROYECTOS DE SEGURIDAD

Con la implementación de proyectos de seguridad, se modifica el nivel de cumplimiento de los controles contenidos en la norma ISO 27002:2013. Para ello se obtiene el siguiente gráfico, donde se puede inferir que la organización definitivamente no invertirá en controles criptográficos pues su objeto de negocio no lo requiere. De otro lado, la organización alcanza un nivel de madurez importante con ayuda de los proyectos de seguridad, con un nivel de cumplimiento cercano al 90% en los dominios de la norma.

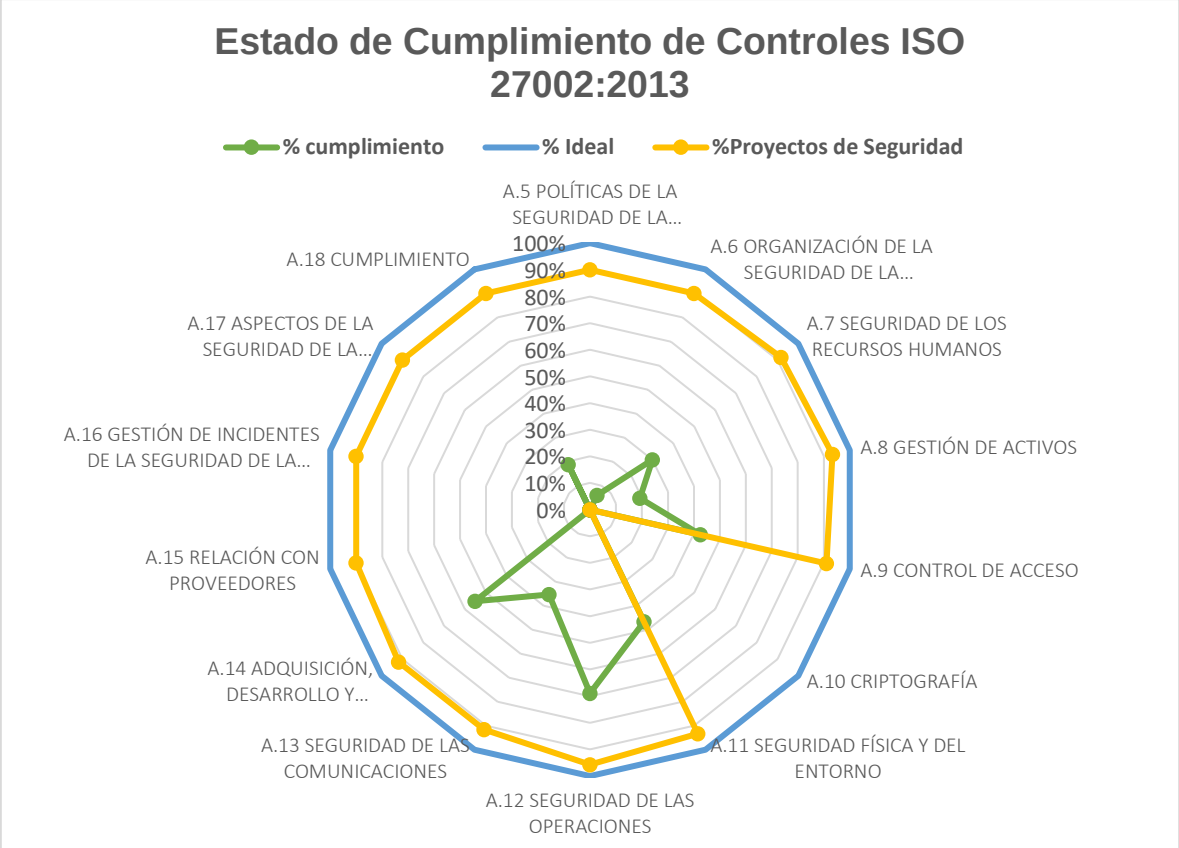

Gráfico 28. Nivel de cumplimiento ISO 27002:2013 tras la implementación de proyectos de seguridad.

7. AUDITORÍA DE CUMPLIMIENTO

En esta fase se pretende valorar el grado de madurez alcanzado por la organización tras la evaluación del análisis de riesgos la aplicación de salvaguardas, para ello se acude a la norma ISO 27002:2013 que incluye 14 dominios, 35 objetivos y 114 controles como marco normativo de seguridad y al CMM (Capability Maturity Model) desarrollado por el SEI (Software Engineering Institute) y provee una gran ayuda para determinar el nivel de madurez de la organización. A continuación, se muestra la lista de dominios de la norma ISO 27002:2013:

Sección	Dominio
A.5	Políticas de la seguridad de la información
A.6	Organización de la seguridad de la información
A.7	Seguridad de los recursos humanos
A.8	Gestión de activos
A.9	Control de acceso
A.10	Criptografía
A.11	Seguridad física y del entorno
A.12	Seguridad de las operaciones
A.13	Seguridad de las comunicaciones
A.14	Adquisición, desarrollo y mantenimiento de sistemas
A.15	Relación con proveedores
A.16	Gestión de incidentes de la seguridad de la información
A.17	Aspectos de la seguridad de la información de la gestión de continuidad de negocio
A.18	Cumplimiento

Gráfico 29. Dominios Norma ISO 27002:2013

De otro lado, el CMM permite la referencia de gestión de procesos implementados en la organización, los pilares de este modelo son la calidad y el mejoramiento continuo cimentados en su nivel de madurez. Se acude a la siguiente referencia de la Universidad Politécnica de Valencia para aclarar la madurez de un proceso:

"Un proceso puede considerarse maduro si cumple con los siguientes criterios:

- *Está definido: El proceso es claro, sistemático y suficientemente detallado. Además, existe acuerdo entre el personal, la gerencia y los proyectos respecto al proceso que se va a utilizar.*
- *Está documentado: Esta escrito en un procedimiento publicado, aprobado y fácilmente accesible.*
- *El personal ha sido entrenado en el proceso: Los ingenieros de software y la gerencia han recibido cursos y entrenamiento en cada proceso que aplica a su trabajo*
- *Es practicado: El proceso definido debe ser usado en las tareas habituales llevadas a cabo por los proyectos. El entrenamiento y la adaptación del proceso a la realidad de la empresa debieran garantizar su aplicación en la vida real.*
- *Es mantenido: El proceso es revisado regularmente, para asegurarse que está adaptado para satisfacer las necesidades reales de los proyectos.*

- *Está controlado: Los cambios y puestas al día del proceso son revisados, aprobados y comunicados oportunamente a todos los usuarios.*
- *Se verifica: La gerencia mantiene mecanismos para asegurarse de que todos los proyectos siguen el proceso vigente.*
- *Se valida: Se asegura que el proceso mantiene concordancia con los requerimientos y estándares aplicables.*
- *Se mide: La utilización, los beneficios y el rendimiento resultante del proceso se miden regularmente.*
- *Puede mejorarse: Existen mecanismos y apoyo de la gerencia para revisar e introducir cambios en el proceso, de manera que se pueda mejorar su eficacia e incorporar nuevas metodologías."* [4]

Entendido lo anterior, cada control ISO se asocia con un nivel de madurez descrito a continuación, ello permite evidenciar el avance del SGSI y evaluar el robustecimiento de los procesos y controles organizacionales. La siguiente tabla detalla la medición otorgada por el modelo CMM:

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	L1	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	L2	Reproducible pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en

[4] http://users.dsic.upv.es/asignaturas/facultad/lsi/trabajos/082000.doc

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
			base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	L4	Gestionado y Medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	L5	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Gráfico 30. Definición de niveles CMM tomado de guía TFM.

La evaluación de los controles según CMM se registra en el siguiente anexo:

Anexo 17. Estado CMM

7.1 ESTADO DE MADUREZ

El siguiente gráfico permite inferir que la organización aún se encuentra fortaleciendo gran parte de sus procesos, el 51% de éstos, se ubican en la categoría L4 – Gestionado y medible. De otro lado y aunque con un resultado menor pero no insignificante, se contrasta la categoría L2- Reproducible pero intuitivo con un 17% del total de controles, en esta área se recomienda fortalecer el entrenamiento a los usuarios, gestionar el conocimiento,

formalizar políticas y/o procedimientos y delimitar responsabilidades. Se puede concluir que la organización sigue estrictamente las recomendaciones para alcanzar el nivel de madurez óptimo.

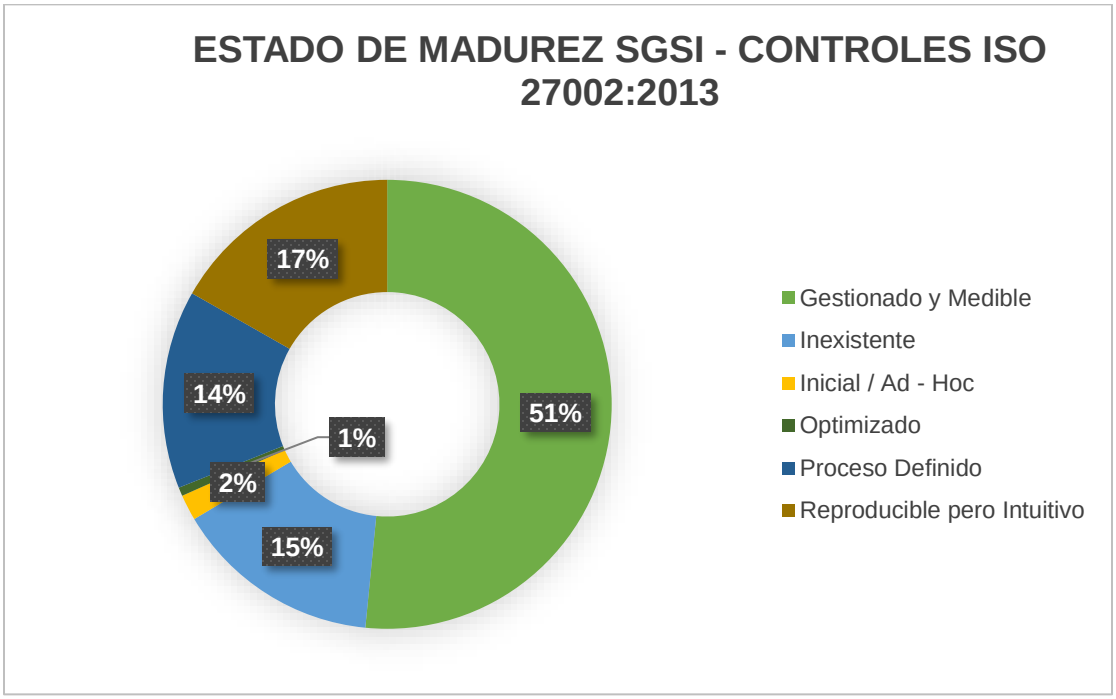

Gráfico 31. Estado de Madurez SGSI. Evaluación ISO 27001:2013

7.2 CUMPLIMIENTO DE CONTROLES EN AUDITORÍA

De otro lado, el siguiente gráfico radial permite evidenciar el nivel de madurez de la organización según los controles y dominios de la norma ISO 27002:2013. La organización ha mostrado significativos avances en el fortalecimiento de la seguridad de la información y la participación de la dirección en el SGSI, sin embargo, se requiere la formalización de algunas políticas y procedimientos que puedan ser medibles y evaluables a través del tiempo. Como se estableció con anterioridad, la organización decide asumir los riesgos asociados a la no implementación del dominio de criptografía, aún así, en el dominio 15. Relación con proveedores se necesita una estructuración de políticas y procedimientos ya que la auditoría demuestra que actualmente carece de formalización. En general, el nivel de cumplimiento es muy bueno y siempre existirá oportunidad de mejora.

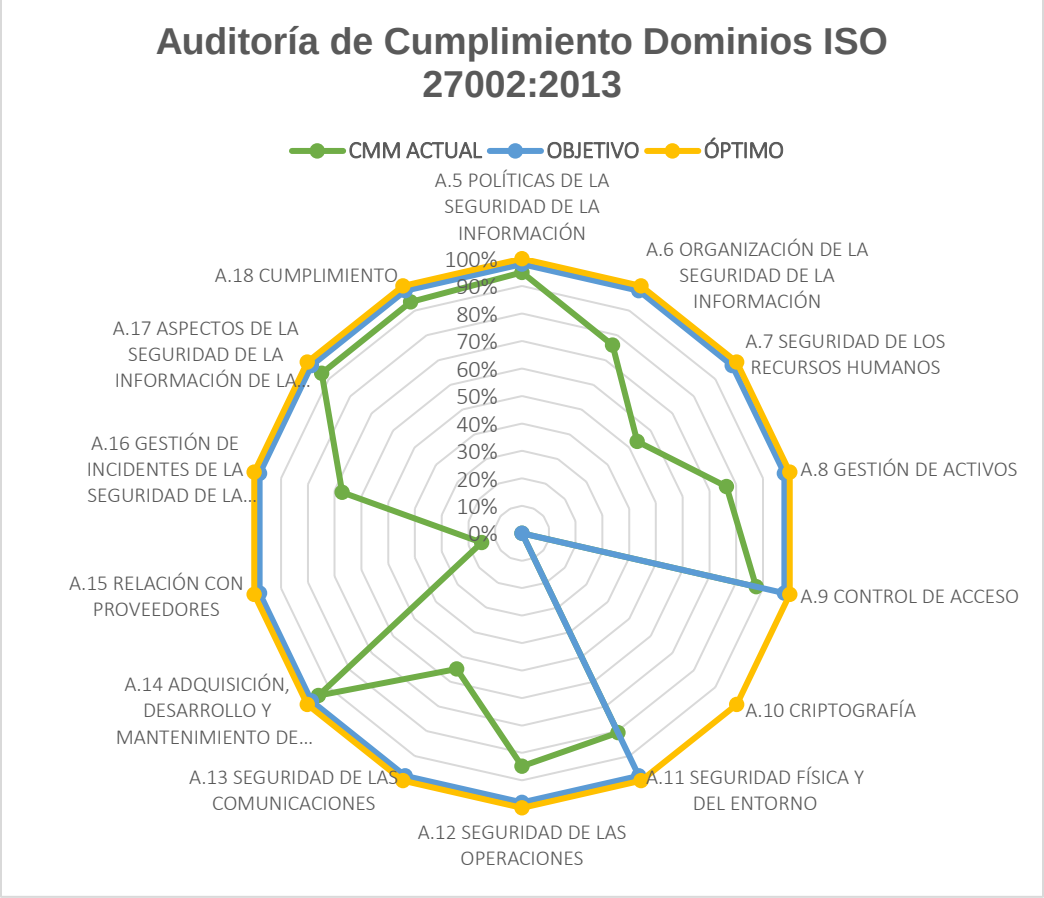

Gráfico 32. Resultados Auditoría de cumplimiento. Dominios ISO 27002:2013

7.3 HALLAZGOS

En cuanto a los resultados de la auditoría, se establecen 15 recomendaciones como oportunidades de mejora, 13 no conformidades menores y 15 no conformidades mayores que pueden finiquitar en alcanzar el umbral objetivo de madurez luego de su implantación, el detalle de los hallazgos por dominio se visualiza en el siguiente gráfico, se deben tomar acciones inmediatas sobre el dominio de relación con proveedores y seguridad física y del entorno.

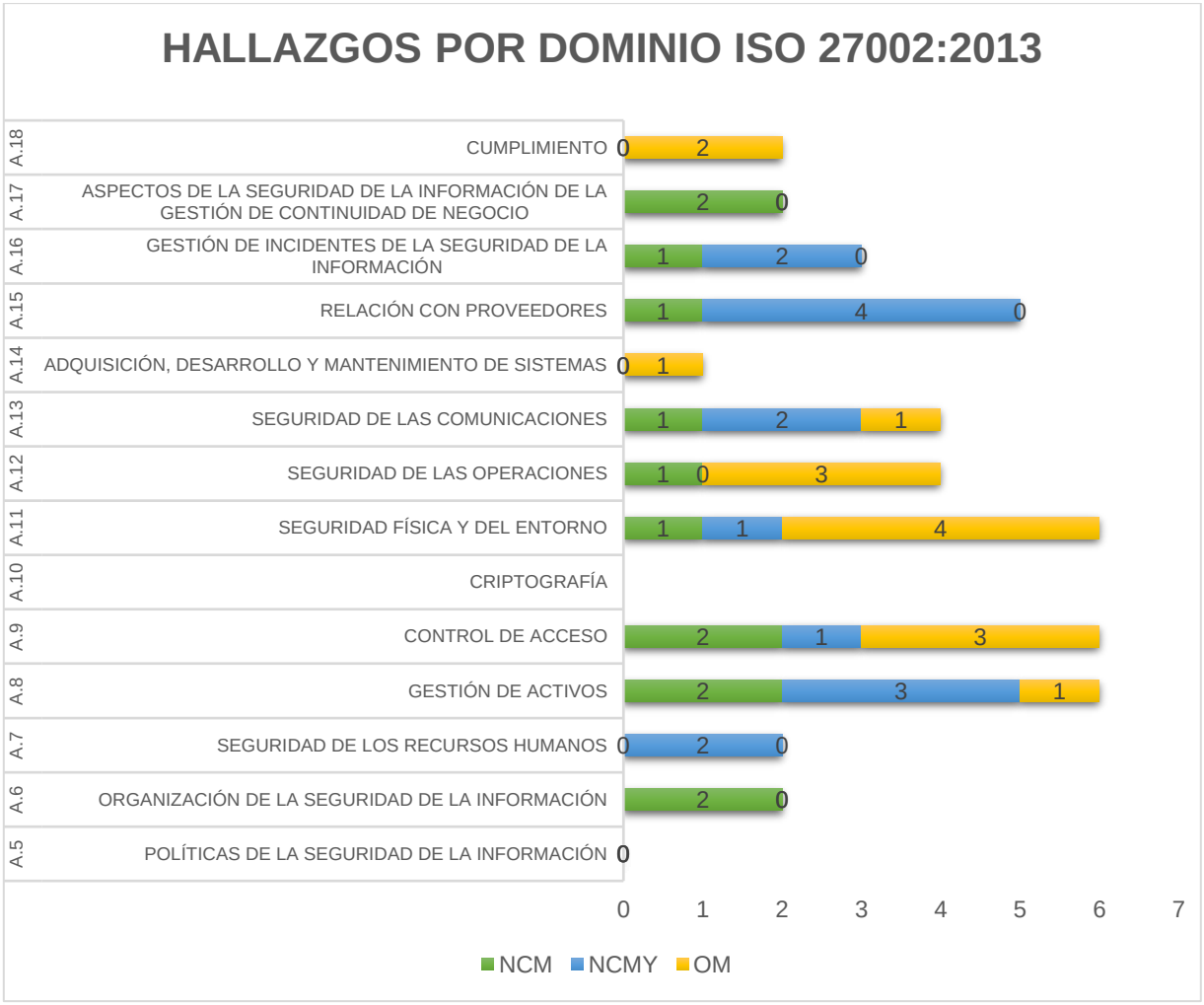

Gráfico 33. Hallazgos por dominio auditoría de cumplimiento ISO 27002:2013.

	NCM	No conformidad Menor
	NCMY	No conformidad Mayor
	OM	Oportunidad de Mejora

El informe de auditoría generado para la evaluación de cada dominio y el cumplimiento del SGSI con respecto al estándar ISO 27001:2013, se puede consultar en el siguiente documento anexo:

Anexo 18. Auditoría de Cumplimiento.

7.4 CUMPLIMIENTO DE DOMINIOS ISO 27001:2013

El diagrama radial muestra un notorio avance en el cumplimiento de dominios de la norma 27001:2013 en el SGSI luego de su implementación, es evidente que la organización ha llevado alcanzado casi en su mayoría el porcentaje de cumplimiento ideal, existen grandes oportunidades de mejora para los dominios evaluación del desempeño y mejora, éstas requieren atención directa de la dirección para su implementación y medición.

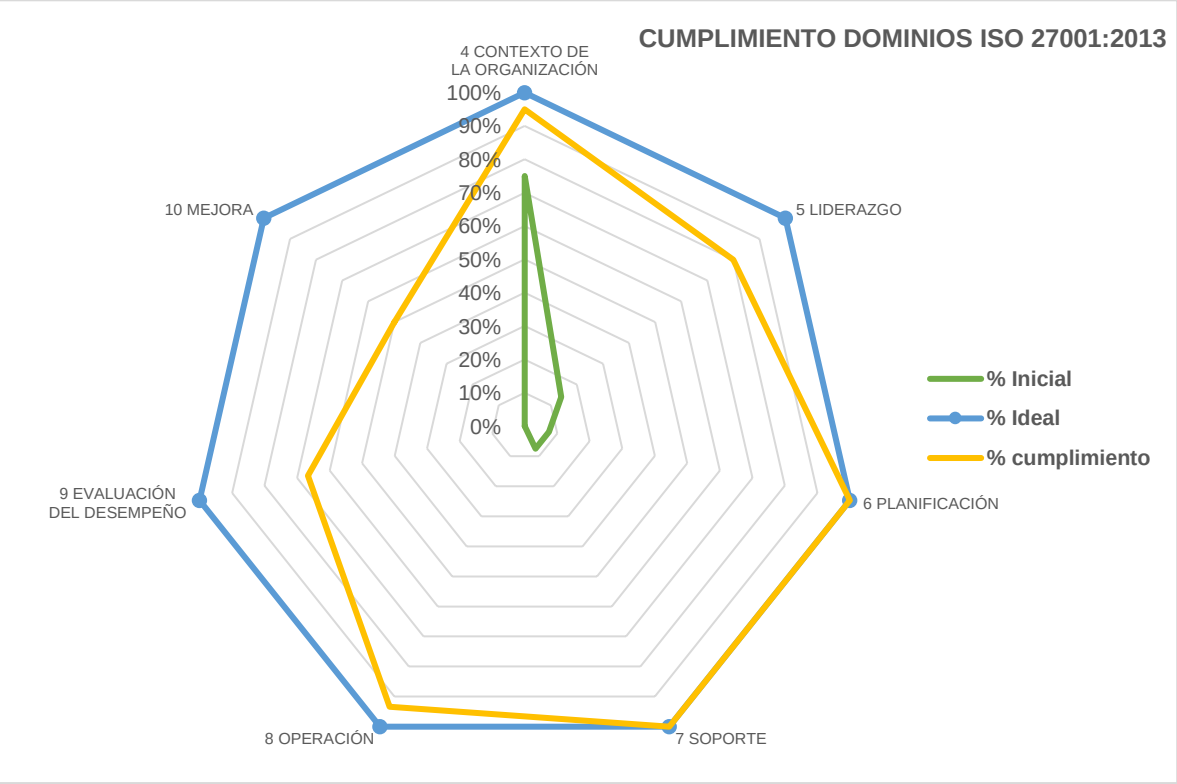

Gráfico 34. Cumplimiento de dominios ISO 27001:2013 tras auditoría.

Id	Ítem	% Inicial	% Ideal	% cumplimiento	Resultado
4	CONTEXTO DE LA ORGANIZACIÓN	75%	100%	95%	CUMPLE
5	LIDERAZGO	14%	100%	80%	CUMPLE
6	PLANIFICACIÓN	8%	100%	100%	CUMPLE
7	SOPORTE	8%	100%	100%	CUMPLE
8	OPERACIÓN	0%	100%	93%	CUMPLE
9	EVALUACIÓN DEL DESEMPEÑO	0%	100%	67%	NO CUMPLE
10	MEJORA	0%	100%	50%	NO CUMPLE

Gráfico 35. Resultados de cumplimiento por dominios ISO 27001:2013.

Los dominios 9 y 10 han sido desatendidos por parte de la organización, existen controles que no han sido implementados y requieren atención inmediata, por tal razón no se cumple con lo requerido por la norma en estos dos puntos.

8. CONCLUSIONES

- Se ha diseñado el plan director para la implementación de un SGSI en una empresa de la industria cosmética, tras el análisis generado en cada fase se puede concluir que la seguridad de la información mejoró notablemente y cumple a cabalidad con los parámetros establecidos dentro de la norma ISO 27001 y 27002:2013.

- Cabe destacar que el SGSI diseñado provee una gran oportunidad de mejora que depende en su mayoría de las decisiones tomadas por la dirección y la disposición de la empresa para invertir en Seguridad de la Información.

- Tras la implementación del SGSI, la empresa está en capacidad absoluta de garantizar la confidencialidad, integridad y disponibilidad de los datos cedidos y propios cumpliendo con los requerimientos legales que en el estado colombiano apliquen.

- El análisis de riesgos provee a la dirección información de alta relevancia para la toma de decisiones, permite proyectar la inversión para mitigar o ceder riesgos y valorar realmente los activos en cada una de las dimensiones de seguridad.

- Los proyectos sugeridos para mitigar los riesgos representan una baja cuantía económica de inversión vs el dinero que puede llegar a perder la compañía si no toma acciones sobre los riesgos mencionados.

- Los usuarios del SGSI están ampliamente familiarizados con el real significado de la seguridad de la Información y generan conciencia sobre los posibles riesgos que pueden desencadenar si no acatan las pautas dadas.

- Se ha sensibilizado a la junta directiva y a toda la compañía en general sobre la relevancia de la seguridad de la información y los impactos que se tendrían al no cumplir con los requerimientos normativos.

9. PRESENTACIÓN DE RESULTADOS Y ENTREGA DE INFORMES

La síntesis consolidada del proyecto se entrega a la dirección en los siguientes anexos:

Anexo 19. Presentación global del proyecto.

Anexo 20. Gestión de riesgos.

10. BIBLIOGRAFÍA Y REFERENCIAS

- Cruz Allende, Daniel; Garre Gui Silvia (2011). Sistema de gestión de la seguridad de la información. Barcelona: UOC.

- ICONTEC (2013). NTC-ISO-IEC 27001:2013 (Primera Actualización). Norma Técnica Colombiana. Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Colombia: ICONTEC.

- ICONTEC (2009). NTC-ISO-IEC 31000:2009 (Primera Actualización). Norma Técnica Colombiana. Gestión del riesgo. Principios y Directrices. Colombia: ICONTEC.

- Ministerio de hacienda y administración pública de España (2012). Magerit Version 3.0. Metodología de Análisis y gestión de riesgos de los sistemas de información. Libro I – Método. Madrid: Centro de publicaciones.

- Colegio Oficial de Ingenieros de Telecomunicación. Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001.

- Tur Hartmann, Juan Enrique (2016). Elaboración de un plan de implementación de la ISO/IEC 27001:2013 en un Ayuntamiento. Barcelona: UOC.

- Laboratorio de Sistemas de Información. Capability Maturity Model. Universidad Politécnica de Valencia. http://users.dsic.upv.es/asignaturas/facultad/lsi/trabajos/082000.doc

- https://www.aec.es/web/guest/centro-conocimiento/no-conformidad

- https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

- https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf