PROPUESTA PARA MEJORES PRÁCTICAS EN EL PROCESO DE GESTIÓN DE INFRAESTRUCTURA E INTERCONEXIONES, ALINEADO CON LA NORMA ISO 27001:2013, PARA LA COMPAÑÍA SISTEMAS SATELITALES DE COLOMBIA (SSC).

PROPOSAL FOR BEST PRACTICES IN THE MANAGEMENT PROCESS OF INFRASTRUCTURE AND INTERCONNECTIONS, ALIGNED WITH THE ISO 27001:2013 STANDARD, FOR THE COMPANY SISTEMAS SATELITALS DE COLOMBIA (SSC).

Ing. Yuri Xiomara Becerra Rozo. Fundación Universitaria Los Libertadores. Bogotá, Colombia. Contacto: yxbecerrar@libertadores.edu.co[i]

Ing. Rubén Darío Betancourt Manjarres. Fundación Universitaria Los Libertadores. Bogotá, Colombia. Contacto: rdbetancourtm@libertadores.edu.co[ii]

Ing. Yenny Isabel Serrato Rodríguez. Docente Fundación Universitaria Los Libertadores. Bogotá, Colombia. Contacto: yiserrator@libertadores.edu.co[iii]

RESUMEN

La seguridad de la información en la actualidad ha pasado a ser una prioridad para las empresas, debido a que, sistemas de información que son expuestos hacia internet, no cuentan con la suficiente protección y pueden ser vulnerados con frecuencia. Por ello, la importancia de establecer controles de seguridad de la información, que permita a las empresas ser competitivas y confiables.

Es por esto, que se realiza un análisis GAP, a partir de la norma ISO 27001:2013. Por medio de este análisis se obtiene el estado actual versus el estado deseado, permitiendo encontrar la brecha entre estos. Posteriormente, basado en la metodología MAGERIT V3, se realiza valoración de riesgos de los activos críticos del proceso, se definen los lineamientos para la adopción de mejores prácticas, teniendo en cuenta, las cláusulas del anexo A de la norma.

Estas recomendaciones son proporcionadas, con el fin de ser implementadas a voluntad, para mitigar los riesgos relacionados con seguridad de la información en el proceso mencionado anteriormente. Permitiendo así, mantener un nivel aceptable dentro del mercado actual,

minimizando el riesgo reputacional y posibilitando la implementación prospectiva de un sistema de gestión de seguridad de la información (SGSI).

Palabras clave: Seguridad de la información, ISO 27001:2013, análisis GAP, gestión de riesgos, MAGERIT.

ABSTRACT

Nowadays, Information Security has become a high priority for companies, since information systems that do not have the correct protection and are exposed to the Internet could be vulnerable to failures and under attack daily. Therefore, the importance of establishing information security controls that allow companies to be reliable and competitive.

A GAP analysis is performed based on the ISO 27001:2013 standard. As a result of this analysis the current and the desired state are obtained, allowing to find the differences between them. Subsequently, based on the MAGERIT V3 methodology, a risk assessment of the critical assets of the process is performed, and the guidelines for improvement actions and adoption of best practices are defined considering the clauses of Annex A of the standard.

These recommendations are provided to be implemented at will, to mitigate the risks related to information security in the current process. This allows to have an acceptable level within the current market by minimizing risks of reputational loss and enabling the prospective implementation of an Information Security Management System (ISMS).

Keywords: Information Security, ISO 27001:2013, gap analysis, Risk management, MAGERIT.

1. INTRODUCCIÓN

La compañía Sistemas Satelitales de Colombia SA ESP, se encuentra en el sector de las telecomunicaciones y está dedicada a prestar servicios de telefonía larga distancia nacional e internacional y son operadores de telefonía local en Colombia. Adicionalmente, ofrece alquiler de servidores Linux y Windows, configuración y soporte sobre plataformas de uso libre como Issabel, y desarrollos propios basados en Asterisk; lo anterior, virtualizado desde su infraestructura On-Premise. Además, presta sus servicios a clientes en todo el territorio nacional, enfocando su core de mercado al sector de las PYMES; dentro de sus acciones para mejora continua, está iniciando el proceso de certificación con la norma ISO 9001:2015.

Actualmente, la empresa se encuentra en constante crecimiento, esto implica que debe replantear la forma en que se está llevando a cabo la ejecución de los procesos de seguridad de la información, garantizando confidencialidad, integridad y disponibilidad a sus clientes, proveedores y aliados.

Este proyecto comprende la realización de una propuesta con recomendaciones de buenas prácticas y aplicación de controles, para que la empresa pueda adoptarlas fortaleciendo la seguridad de la información y seguridad informática, dando cumplimiento a las políticas de seguridad que apliquen de acuerdo con el estándar internacional ISO 27001:2013 y su anexo.

Para determinar las recomendaciones aplicables, es necesario realizar un análisis GAP, posteriormente, valorar activos críticos y determinar su nivel de riesgo basado en metodología MAGERIT v3.

2. REFERENTES TEÓRICOS

2.1. Seguridad de la información

Son todas las medidas preventivas y de reacción del individuo, la organización y las tecnologías, para proteger la información; buscando mantener la confidencialidad, disponibilidad e integridad.

Hay que tener claro que los términos Seguridad de la información y Seguridad Informática son diferentes. La segunda trata solamente de la seguridad en el medio informático, mientras que la primera es para cualquier tipo de información, sea esta digital o impresa.

La seguridad de la información abarca muchas cosas, pero todas en torno a la información. Por ejemplo, la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.[1]

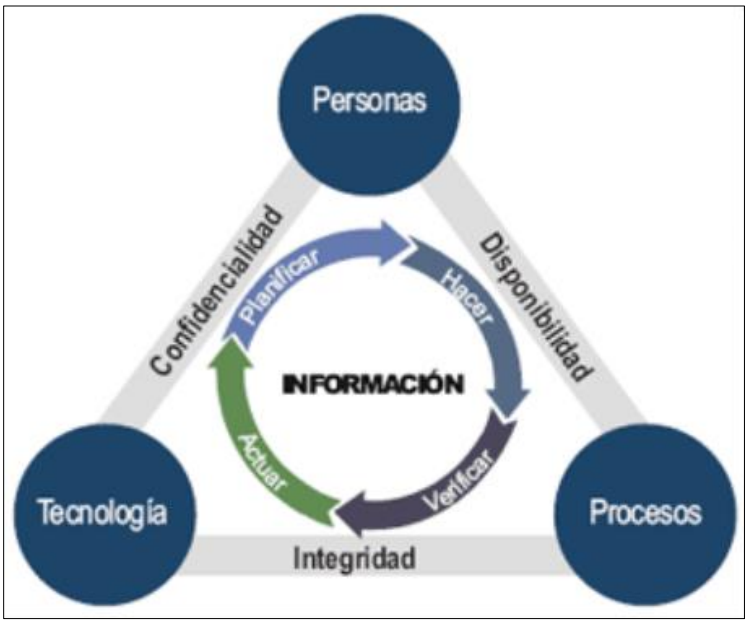


Ilustración 1 Seguridad de la información - Triada[2]

[1] (Universidad Libre sede Bogotá, 2015)

[2] (ASNET, 2022)

2.2. Confidencialidad

Implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como need-to-know. Con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso. Ejemplos de falta de confidencialidad son: el robo de información confidencial por parte de un atacante a través de Internet, la divulgación no autorizada a través de las redes sociales de información confidencial o el acceso por parte de un empleado a información crítica de la compañía ubicada en carpetas sin permisos asignados, a la que no debería tener acceso.[3]

2.3. Disponibilidad

Hace referencia a que la información esté accesible cuando la necesitemos. Algunos ejemplos de falta de disponibilidad de la información son: cuando nos es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando se sufre un ataque de denegación de servicio, en el que el sistema «cae» impidiendo accesos legítimos. Ambos tienen implicaciones serias para la seguridad de la información. [4]

2.4. Integridad

El diccionario define el término como "estado de lo que está completo o tiene todas sus partes". La integridad hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina.[5]

---

[3] (INCIBE)
[4] (INCIBE)
[5] (firma-e Consultoría y desarrollo TI, 2014)

2.5. ¿Qué es ISO 27001?

La ISO 27001:2013 es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de garantizar confidencialidad, integridad y disponibilidad continua de los datos, así como cumplimiento legal.

La implantación de la ISO 27001 es la respuesta ideal a los requisitos legislativos y de los clientes, incluyendo el y otras amenazas potenciales, incluyendo: Crimen cibernético, violación de los datos personales, vandalismo / terrorismo, fuego / daños, uso malintencionado, robo y ataque de virus.

En 2019, cerca del 32% de los negocios sufrieron una violación de datos personales o recibieron ataques en los últimos 12 meses[6].

La norma ISO 27001 se estructura para ser compatible con otras normas de sistemas de gestión, como la ISO 9001 y es neutral respecto a tecnología y proveedores, lo que significa que es completamente independiente de la plataforma de IT. Por ello, todos los miembros de la organización deben ser educados sobre el significado de la norma y cómo se aplica en la organización.

Conseguir la certificación ISO 27001 demuestra que su empresa está comprometida con seguir las mejores prácticas de seguridad de la información. Adicionalmente, la certificación ISO 27001 proporciona una evaluación experte de si la información de su empresa está adecuadamente protegida.[7]

[6] (Admin Tecno-Office, 2021)
[7] (nqa, s.f.)

2.6. ¿Qué es ISO 31000?

ISO 31000:2018 es la norma internacional para la gestión del riesgo. Al proporcionar principios integrales y directivas, esta norma ayuda a las organizaciones con su análisis y evaluación de riesgos. Sea que trabaje en una empresa pública, privada o comunitaria, se puede beneficiar de ISO 31000, porque se aplica a la mayoría de las actividades comerciales, incluyendo la planeación, operaciones de gestión y procesos de comunicación. Mientras que todas las organizaciones manejan el riesgo en cierta medida, las recomendaciones de mejores prácticas de esta norma internacional se desarrollaron para mejorar las técnicas de gestión y garantizar la seguridad y protección en todo momento en el lugar de trabajo.

Al implementar los principios y directivas de ISO 31000 en su organización, será capaz de mejorar la eficiencia operativa, gobernanza y confianza de las partes interesadas, a la vez que minimiza las pérdidas. Esta norma internacional también le ayuda a impulsar el desempeño de salud y seguridad, establecer un fuerte fundamento para la toma de decisiones y alentar la gestión proactiva en todas las áreas.[8]

2.7. ¿Qué es MAGERIT?

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones, teniendo en cuenta, los riesgos derivados del uso de tecnologías de la información.[9]

[8] (The British Standards Institution, 2022)
[9] (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. Gobierno de España, 2012)

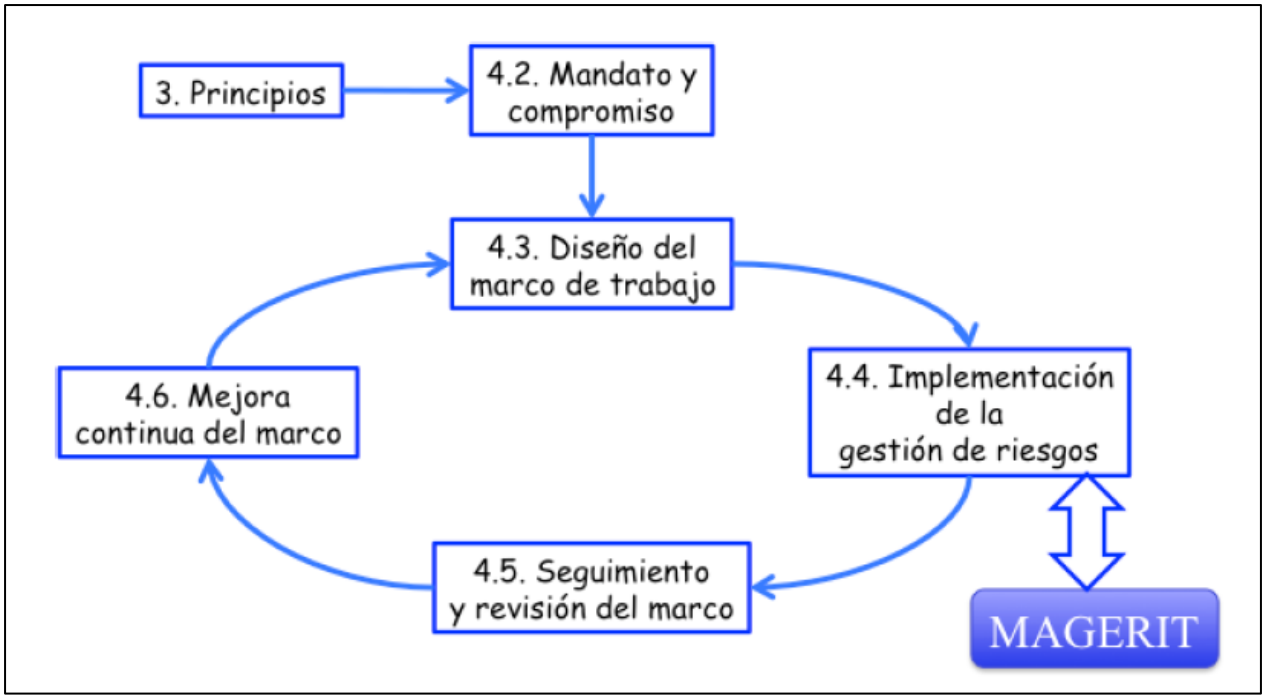


Ilustración 2. ISO 31000 - Marco de trabajo para la gestión de riesgos. Tomado MAGERIT v3 Libro 1 - Método[10]

2.8. ¿Qué es el análisis de brechas o GAP?

El análisis de brechas se define como un método para evaluar las diferencias entre el desempeño real y el desempeño esperado en una organización o negocio.

El término "brecha" se refiere al espacio entre "donde estamos ahora" (el estado actual) y donde "queremos estar" (el estado objetivo). Un análisis de brechas también puede ser referido como análisis GAP evaluación de necesidades o análisis de brechas de necesidades.

Se puede realizar un análisis de brechas:

- **A nivel estratégico:** Para comparar la condición o nivel del negocio vs. los estándares de la industria

[10] (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. Gobierno de España, 2012)

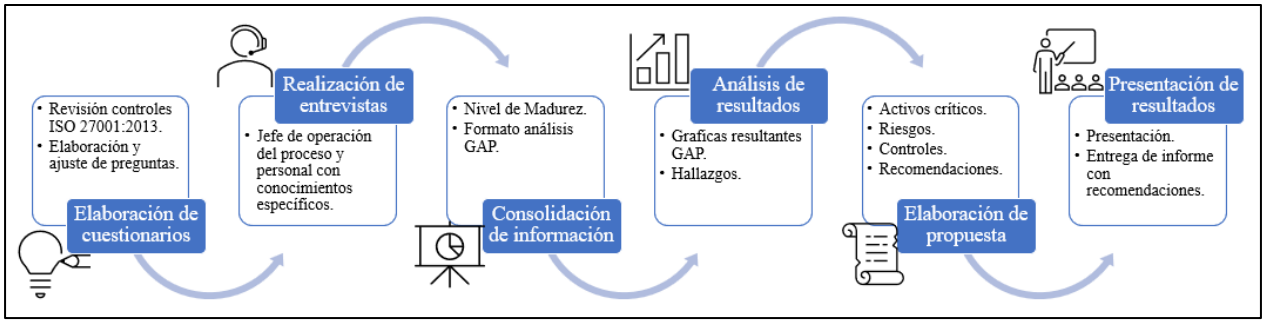
- **A nivel Operativo:** Para comparar el estado actual o rendimiento de su negocio con lo que has deseado.

Aquí es donde el análisis de brechas juega un papel crucial en la comprensión de dónde está el producto y qué es lo que le falta, dónde necesita estar el producto para asegurar su lugar en el mercado y darle batalla a la competencia.[11]

3. METODOLOGÍA

Se realiza un análisis de brechas (GAP), entrevistando personal encargado de la parte operativa del proceso. Por medio de este análisis se determina el estado actual y deseado de la empresa, evaluando las vulnerabilidades presentes en los sistemas de información e informáticos que, con adopción de los controles y políticas de seguridad basados en la norma ISO 27001:2013, permitirán mitigar o minimizar las brechas de seguridad, en el proceso de infraestructura e interconexiones.

Se plantea una propuesta, que la empresa puede tomar como guía para mejorar sus prácticas en seguridad, la cual se construye con la siguiente metodología:



lustración 3 Metodología de trabajo. Fuente propia

[11] (www.questionpro.com, 2022)

A continuación, se presentan las actividades a realizar en cada fase.

3.1. Elaboración de cuestionarios:

a) Revisión de controles ISO 27001:2013, búsqueda de formato de base de GAP.

b) Elaboración y ajuste de preguntas.

3.2. Realización de entrevistas:

a) Entrevista a jefe de operación del proceso a evaluar.

b) Entrevista a personal con conocimiento puntual sobre temáticas diferentes a operación.

3.3. Consolidación de resultados:

a) Nivel de madurez.

b) Consolidación en formato de análisis GAP.

3.4. Análisis de resultados:

a) Validación de gráficas resultantes del análisis GAP:

b) Establecimiento de cláusulas a fortalecer.

c) Selección de hallazgos representativos.

3.5. Elaboración de propuesta:

a) Identificación de activos críticos.

b) Definición de riesgos.

c) Definición de controles.

d) Elaboración de recomendaciones.

3.6. Presentación de resultados:

a) Presentación ejecutiva.

b) Entrega del informe guía mejores prácticas.

4. RESULTADOS

4.1. Elaboración de cuestionarios

Se elaboran cuestionarios de acuerdo con las cláusulas de la norma ISO 27001:2013, teniendo en cuenta, la necesidad de identificar el estado actual para tener un punto de partida y generar el análisis GAP, este cuestionario se realiza apoyado de plantilla ISO/IEC 27001:2013 ISMS Status, Statement of Applicability (SoA) and Controls Status (gap análisis) workbook de ISO 27001 Security.[12]

4.2. Realización de entrevistas

Se implementan cuestionarios con base a la normativa de la ISO 27001 y su anexo, dirigido al personal encargado del departamento de TI, cada pregunta tiene un valor o puntuación lo que permite evaluar y diagnosticar aspectos importantes en el proceso de infraestructura e interconexiones, para posteriormente definir el estado actual de la empresa y su nivel de madurez.

4.3. Consolidación de resultados

4.3.1. Nivel de madurez

Se establecen los siguientes criterios para medir el nivel de madurez en el que se encuentra cada objetivo de control y controles del anexo A, lo que permite evaluar el avance de la empresa con respecto al cumplimiento de los criterios definidos en la siguiente tabla:

[12] (iso27001security, 2014)

Estado	n	Criterios
Inexistente	0	Total falta de cualquier proceso reconocible, la organización no ha reconocido que hay un problema a tratar, no se aplican controles.
Inicial	20	Hay evidencia de que la organización ha reconocido que existe un problema y que hay que tratarlo, no hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva, se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Definido	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Administrado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.
No aplicable	NA	No aplica.

Tabla 1 Escala de valoración - Instrumento de evaluación MSPI[13]

4.3.2. *Consolidación en formato de análisis GAP*

Se realiza la correlación de respuestas producto de la entrevista, dentro del formato de análisis GAP. Con lo anterior se obtiene información sobre el estado actual de los objetivos de control aplicados en el proceso evaluado.

Nivel de madurez objetivos de control					
Numeral	Cláusula	Estado GAP	Brecha	Estado Deseado	GAP
4	Contexto de la organización	16	64	80	INICIAL
5	Liderazgo	13	67	80	INICIAL
6	Planificación	0	80	80	INEXISTENTE
7	Soporte	9	71	80	INICIAL
8	Operación	0	80	80	INEXISTENTE
9	Evaluación de desempeño	7	73	80	INICIAL
10	Mejora	0	80	80	INEXISTENTE

Tabla 2 Nivel de Madurez Objetivos de control – Fuente propia

Como se puede observar en la tabla anterior, los numerales 4, 5, 7 y 9 se encuentran en un estado inicial, por lo que ha sido interés de la compañía dar sus primeros pasos para alinearse a las expectativas y requerimientos de la norma, sin embargo, los numerales 6, 8 y 10 se encuentran en un estado inexistente, razón por la cual, a lo largo de este documento, serán

[13] (Ministerio de Tecnologías de la Información y las Comunicaciones, s.f.)

objeto de análisis para aportar a un fortalecimiento en temas de seguridad de la información.

Al relacionar los datos de la entrevista respecto a los controles del Anexo A, se obtiene el estado actual:

Nivel de madurez Controles					
Numeral	**Cláusula**	**Estado GAP**	**Brecha**	**Estado esperado**	**GAP**
A.5	Política de seguridad de la información	0	80	80	**INEXISTENTE**
A.6	Organización de seguridad de la información	9	71	80	**INICIAL**
A.7	Seguridad de los recursos humanos	30	50	80	**REPETIBLE**
A.8	Gestión de activos	20	60	80	**INICIAL**
A.9	Control de acceso	24	56	80	**REPETIBLE**
A.10	Criptografía	0	80	80	**INEXISTENTE**
A.11	Seguridad Física	40	40	80	**REPETIBLE**
A.12	Gestión de operaciones	16	64	80	**INICIAL**
A.13	Seguridad de las comunicaciones	20	60	80	**INICIAL**
A.14	Adquisición, desarrollo y mantenimiento de sistemas	18	62	80	**INICIAL**
A.15	Relaciones con los proveedores	24	56	80	**REPETIBLE**
A.16	Gestión de incidentes seguridad de la información	14	66	80	**INICIAL**
A.17	Continuidad de seguridad de la información	15	65	80	**INICIAL**
A.18	Cumplimiento	7	73	80	**INICIAL**

Tabla 3 Nivel de Madurez controles Anexo A - Fuente propia

En los controles del anexo A de la norma, los numerales A7, A9, A11 y A15, se encuentran en un estado repetible, lo cual quiere decir, que los procesos siguen un patrón regular y se han replicado hasta el punto en que son seguidos por los empleados, sin embargo, no hay información documentada al respecto y se pueden presentar errores al momento de ejecutar alguna actividad, mientras que A6, A8, A12, A13, A14, A16, A17 y A18 se localizan en un nivel inicial, indicando que, la implementación de un control es principalmente reactiva y depende de cada colaborador, también existe documentación, pero no se difunde correctamente o no se aplica. A5 y A10 se evidencian inexistentes pues no tienen procedimientos aplicados a estas cláusulas.

El objetivo de la compañía es alcanzar un nivel de madurez del 80% (Administrado), siendo éste el esperado para un SGSI. En términos generales y alineado con la norma, el estado actual es del 17% considerando una brecha del 63% para llegar al deseado, para esto se realiza una serie de recomendaciones por cada una de las cláusulas detalladas en el contenido del documento. Una vez alcanzado el objetivo, la empresa estará en la capacidad de medir y monitorear el cumplimiento de sus procesos o procedimientos, de tal forma que, tenga la capacidad de tomar decisiones de un control que no esté funcionando eficientemente.

4.4. Análisis de resultados

4.4.1. Validación de gráficas resultantes del análisis GAP

Con la aplicación del cuestionario, se obtienen las siguientes gráficas:

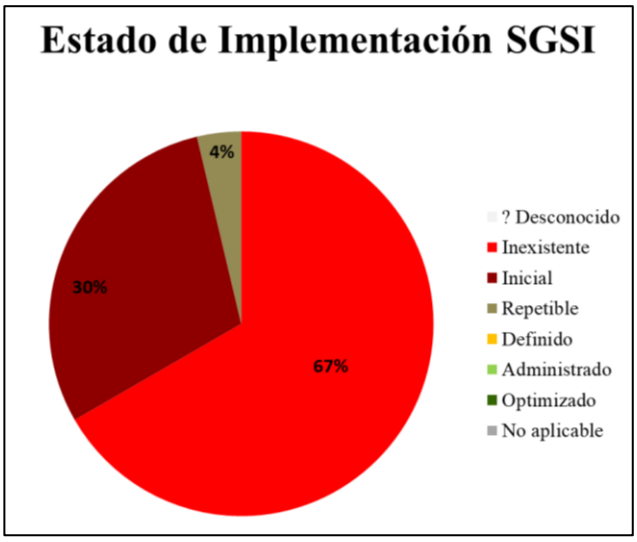


Ilustración 4 Estado de implementación SGSI - Basado en formato análisis GAP[14]

En la gráfica anterior se observa el análisis del estado de implementación del SGSI, se puede evidenciar que la mayoría de los objetivos de control son inexistentes y otros se encuentran en

[14] (iso27001security, 2014)

estado inicial, lo que significa que la compañía presenta alta exposición a riesgos de seguridad de la información.

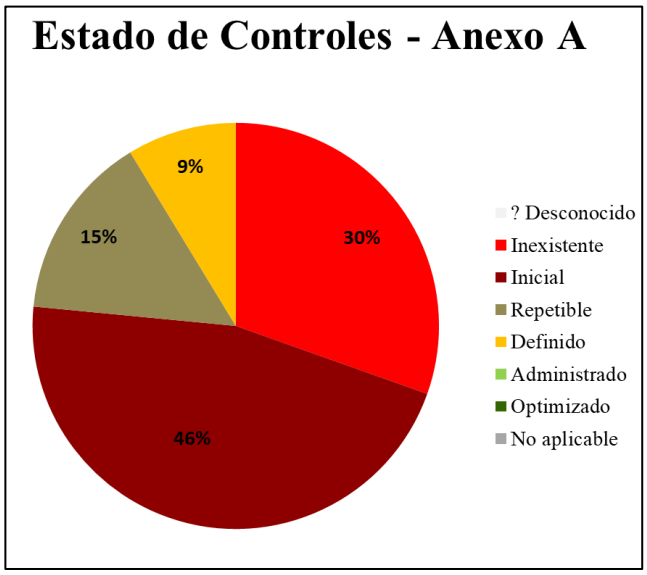
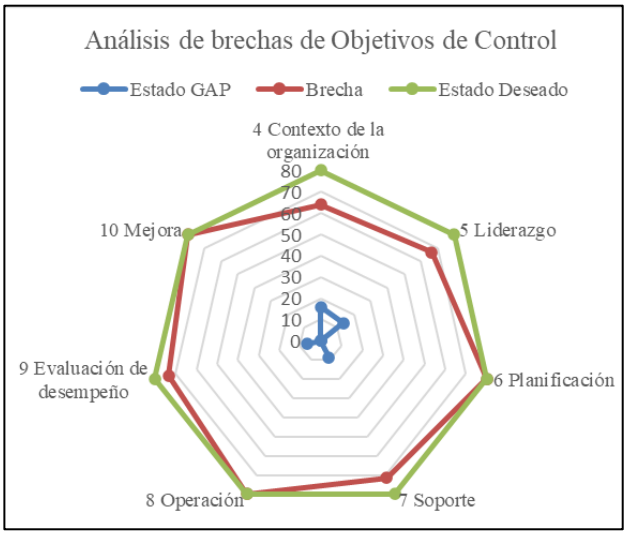


Ilustración 5 Estado de controles Anexo A - Basado en formato análisis GAP[15]

Con la anterior imagen se evidencia que el 46% de los controles se encuentran en estado inicial, el 30% en un nivel inexistente y tan solo el 9% definido. Por esto, se hace necesario hacer especial énfasis en los controles catalogados como inexistente e inicial y construir desde allí la propuesta de un SGSI.



[15] (ISO27001security.com, 2014)

Ilustración 6 Gráfico análisis GAP Objetivos de control - Fuente propia

En la ilustración 6 se relaciona la información en un diagrama radial que facilita la comprensión del análisis GAP en términos de objetivos de control, con esto, es claro que la brecha es casi igual al estado deseado.

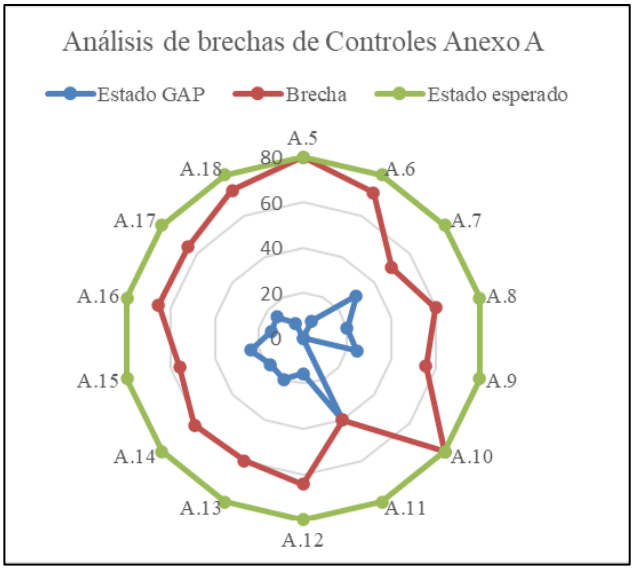


Ilustración 7 Gráfico análisis GAP Controles Anexo A - Fuente propia

En la imagen anterior se identifica, en cuanto a controles del anexo, que la brecha no es tan amplia como en los objetivos de control, sin embargo, es importante fortalecer los puntos débiles que son los ítems cuya brecha es más cercana al estado esperado.

4.4.2. Establecimiento de cláusulas a fortalecer

Recurriendo al juicio de experto y el resultado del análisis GAP sobre el proceso de infraestructura e interconexión, se seleccionan las cláusulas más relevantes sobre las cuales se deben implementar acciones para fortalecer su seguridad:

Nivel de madurez objetivos de control		
Numeral	**Cláusula**	**Estado actual GAP**
4	Contexto de la organización	16%
5	Liderazgo	13%
6	Planificación	0%
7	Soporte	9%
8	Operación	0%
10	Mejora	0%

Tabla 4 Objetivos de control para hacer énfasis en fortalecimiento. Fuente propia

Nivel de madurez Controles		
Numeral	**Cláusula**	**Estado actual GAP**
A.5	Política de seguridad de la información	0%
A.6	Organización de la seguridad de la información	9%
A.8	Gestión de activos	20%
A.9	Control de acceso	24%
A.10	Criptografía	0%
A.11	Seguridad Física	40%
A.12	Gestión de operaciones	16%
A.13	Seguridad de las comunicaciones	20%
A.14	Adquisición, desarrollo y mantenimiento de sistemas	18%
A.16	Gestión de incidentes de seguridad de la información	14%
A.17	continuidad de seguridad de la información	15%
A.18	Cumplimiento	8%

Tabla 5. Controles para hacer énfasis en fortalecimiento. Fuente propia

De acuerdo con las tablas anteriores se establecen los puntos a profundizar en este documento, se realizará especial énfasis en las cláusulas mencionadas las cuales son fundamentales para la operación del proceso de infraestructura e interconexiones.

4.4.3. Selección de hallazgos representativos.

Cláusula	Descripción	Hallazgos
6	Planificación	
	Acciones para tratar los riesgos y oportunidades	
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportunidades	La organización no tiene contemplado un análisis de riesgos, las partes interesadas no son tenidas en cuenta en el momento de contemplar o evaluar los riesgos de la compañía, no se tiene establecido un proceso para el
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	
	Objetivos de seguridad de la información y planificación para su consecución	
6.2	Establecer y documentar los planes y objetivos de la seguridad de la información	La organización carece de un planteamiento de objetivos de seguridad de la información, en esa medida, las funciones relevantes de la organización no tienen estipulada una hoja de ruta que favorezca los objetivos de seguridad.

Tabla 6. Hallazgos objetivo de control de planificación. Fuente propia

Cláusula	Descripción	Hallazgos
7	Soporte	
	Recursos	
7.1	Determinar y asignar los recursos necesarios para el SGSI	A la organización no se le ha manifestado la importancia o el requerimiento de recursos de seguridad de la información, sin embargo, si se realizara la debida solicitud con su justificación, la compañía otorgaría los recursos necesarios.
	Competencia	
7.2	Determinar, documentar hacer disponibles las competencias necesarias	Las competencias son evaluadas por medio de procedimientos no formales, esta competencia se valida previa posesión del cargo, sin embargo, no hay un procedimiento establecido y autorizado.
	Concienciación	
7.3	Implementar un programa de concienciación de seguridad	Teniendo en cuenta que la compañía no tiene políticas de seguridad de la información, esta información no se replica con el personal, sin embargo, previa posesión del cargo, se realiza una breve inducción sobre las condiciones mínimas a cumplir para garantizar la seguridad, esto es un proceso no formal y no se tiene documentación autorizada.
	Comunicación	
7.4	Determinar las necesidades de comunicación internas y externas relacionadas al SGSI	Se requiere establecer políticas de comunicación internas y externas relacionadas con el SGSI de acuerdo al tipo de comunicación y la clasificación de información.
	Información documentada	
7.5.1	Proveer documentación requerida por el estándar más la requerida por la organización	Diseñar políticas de seguridad de la información acorde a un análisis de riesgos. La política debe ser divulgada a todos los miembros de la organización
7.5.2	Proveer un titulo, autor, formato consistente, revisión y aprobación a los documentos	El documento de las políticas de seguridad de la información debe ser actualizado y versionado. La empresa debe realizar ajustes a la política teniendo en cuenta el nivel de crecimiento y madurez, con el fin de atacar problemas que no se evidenciaron en versiones anteriores.

Tabla 7 Hallazgos objetivo de control de Soporte. Fuente propia

Cláusula	Descripción	Hallazgos
8	Operación	
	Planificación y control operacional	
8.1	Planificar, implementar, controlar y documentar el proceso de gestión de riesgos del SGSI (Tratamiento de riesgos)	No se tiene documentado un proceso de control de cambios para mitigar riesgos asociados. Falta plan de tratamiento de riesgos.
	Apreciación de los riesgos de seguridad de la información	
8.2	Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios	
	Tratamiento de los riesgos de seguridad de la información	
8.3	Implementar un plan de tratamiento de riesgos y documentar los resultados.	

Tabla 8 Hallazgos objetivo de control de Operación. Fuente propia

Cláusula	Descripción	Hallazgos
10	Mejora	
	No conformidad y acciones correctivas	
10.1	Identificar, remediar y reaccionar ante no conformidades para evitar su recurrencia documentando las acciones.	No se cuenta con proceso de auditoría por lo que no se tiene en cuenta las no conformidades y acciones para evitar su recurrencia.
	Mejora continua	
10.2	Mejora continua del SGSI	No se tiene establecido proceso para mejora continua.

Tabla 9 Hallazgos objetivo de control de Mejora. Fuente propia

4.5. Elaboración de propuesta

4.5.1. Identificación de activos críticos

De acuerdo con la información brindada por la organización se realiza identificación y análisis de sus activos críticos. En la siguiente tabla se presenta un resumen de estos activos, sin embargo, para ampliar información es necesario remitirse al anexo2 – Activos y riesgos, ver pestaña Listado de activos SSC.

Activo	Prioridad	Tipo de Activo	Clasificación
Chasis IBM Flexsystem	Alta	Infraestructura IT	Confidencial
Firewall Perimetral	Alta	Hardware	Confidencial
Equipos de interconexion E1 Operadores - IMG	Alta	Software	Confidencial
Switch Core ISP	Alta	Hardware	Confidencial
Softwarte para virtualizacion RedHat	Alta	Software	De uso interno
Equipos Operadores moviles	Alta	Servicio	Confidencial
Servidor Contabilidad	Alta	Software	De uso interno
Plataforma Sipmovil	Alta	Servicio	De uso interno
Correo Electronico Zimbra	Alta	Servicio	De uso interno
Servidor de facturación	Alta	Servicio	De uso interno
Servicio de directorio activo y DNS	Alta	Servicio	De uso interno
Operadores Tecnicos (NOC)	Alta	Servicio	De uso interno
Ambientes de Desarrollo	Alta	Infraestructura TI	Confidencial

Tabla 10. Identificación y valoración de activos de información. Fuente Propia

4.5.2. Definición de riesgos

Al identificar los activos críticos, se define un riesgo por cada activo, a su vez, se relaciona una amenaza y una vulnerabilidad, con esta información se valoran el impacto a confidencialidad, integridad y disponibilidad, así como, la probabilidad de ocurrencia, como resultado se obtiene el valor del riesgo ponderado y se sugieren los controles aplicables para mitigar el riesgo según el anexo A de la norma ISO 27001:2013. Para ampliar información ver Anexo 2 – Activos y riesgos – Pestaña Análisis SSC.

# Riesgo	Activo	Riesgo	Riesgo Ponderac	Requiere ser Tratad
1	Chasis IBM Flexsystem	Empleados sin la responsabilidad para realizar mantenimiento de la infraestructura instalada.	Alto	Si
2	Equipos Switch CORE Stratus Telecomunications	Acceso a información sensible debido a que las contraseñas de los usuarios no son seguras	Alto	Si
3	Servidor Contabilidad	Daño o pérdida de la información del sistema. La	Alto	Si
4	Plataforma SIP móvil	Saturación de la red por solicitudes malintencionadas	Alto	Si
5	Correo Electrónico Zimbra	Infección y distribución de código malicioso dentro de la organización	Alto	Si
6	Servidor NEXTCLOUD para gestión de documentos	Robo, divulgación, pérdida, destrucción o retiro de la información	Alto	Si
7	Servidor de facturación	Robo, divulgación, pérdida, destrucción o retiro de la información	Alto	Si
8	Estaciones de trabajo	Fallas en dispositivos o software	Alto	
9	Servicio de directorio activo y DNS	Afectación en disponibilidad de la información	Alto	No
10	Base de Conocimiento	Modificación o Eliminación de los repositorios por errores	Alto	Si
11	Operadores Técnicos (NOC)	Errores de naturaleza humana, por ejecución inapropiada de scripts o procedimientos de limpieza	Alto	Si
12	Ambientes de desarrollo	Riesgos para la productividad	Alto	Si

Tabla 11. Relación de riesgos por activo. Fuente propia

Esta ponderación se basa en metodología Magerit V3 y se crea un mapa de calor que permita identificar gráficamente la criticidad de los riesgos definidos por cada activo, de acuerdo con su valoración, se ubican por número de riesgo en el siguiente mapa.

PROBABILIDAD \ IMPACTO		Muy Bajo	Bajo	Medio	Alto	Muy Alto
		1	2	3	4	5
Muy Alto (5)	Muy frecuente					
Alto (4)	Frecuente				**[4][8][10]**	
Medio (3)	Normal			**[20][21][22][24] [25][26]**	**[3][5][6][7][9] [11][12]**	**[1][2]**
Bajo (2)	Poco Frecuente			**[15][16][17][19]**	**[23]**	
Muy bajo (1)	Muy Poco Frecuente			**[13][14][18]**		

Tabla 12. Mapa de calor para valoración de riesgos. Fuente propia

1 AL 2	MB
3 AL 6	B
8 AL 10	M
12 AL 16	A
20 AL 25	MA

Tabla 13. Niveles de riesgo. Fuente propia

4.5.3. Definición de controles

Se determinan los controles aplicables a cada amenaza y vulnerabilidad de acuerdo con el anexo A de la norma ISO27001:2013, esta información se puede validar en el Anexo 2 – Activos y riesgos – Pestaña Análisis SSC.

4.5.4. Elaboración de recomendaciones

Con el análisis anterior, se establecen las recomendaciones para implementación de mejores prácticas basado en las cláusulas del Anexo A de la norma, dentro de las recomendaciones, que pueden verse en el Anexo1 ISO27k Versión Final pestaña Recomendaciones, es importante diseñar políticas de seguridad de la información acorde a las necesidades de la organización, así mismo, es necesario divulgarlas a todos los miembros de la compañía y partes interesadas, éstas deberán ser revisadas periódicamente o cuando se produzcan cambios significativos con el fin de garantizar su eficiencia.

Cláusula	Descripción	Recomendación
A5.1	**Directrices de gestión de la seguridad de la información**	**Recomendación**
A5.1.1	Políticas para la seguridad de la información	Diseñar políticas de seguridad de la información. Sugerencia en Anexo3. La política debe ser divulgada a todos los miembros de la organización y partes interesadas. Estas políticas deben ser aprobadas por la dirección y encontrarse publicadas para toda la compañía.
A5.1.2	Revisión de las políticas para la seguridad de la información	La política de seguridad de la información debe ser revisada en intervalos establecidos o cuando se producen cambios significativos con el fin de garantizar que la política continúe siendo suficiente y eficaz.
A6.1	**Organización interna**	**Recomendación**
A6.1.1	Roles y responsabilidades en seguridad de la información	Sumar a las funciones de cada puesto de trabajo, aquellas que tengan que ver con seguridad de la información (si es pertinente), cuando se definan estas funciones, deben ser comunicadas a cada persona implicada en la seguridad de la información. Hacer partícipes a las partes externas que sean pertinentes, como usuarios, proveedores o clientes.
A6.1.2	Segregación de tareas	Evitar usos o accesos indebidos a la información o a las aplicaciones o sistemas mediante la separación de funciones asignando distintos perfiles o áreas de responsabilidad.
A6.1.3	Contacto con las autoridades	En caso de incidentes de seguridad de la información, podría ser necesario mantener informados a los organismos de control del estado. Consultar CONPES 3701 de 2011, las empresas públicas y privadas deberán reportar sus incidentes al COLCERT.
A6.1.4	Contacto con grupos de interés especial	Mantenerse al día en cuanto a noticias sobre seguridad de la información, suscripción al sitio de internet https://cc-csirt.policia.gov.co/, con el fin de obtener información relevante sobre análisis malware en archivos y urls, así como boletines informativos
A6.1.5	Seguridad de la información en la gestión de proyectos	Realizar evaluación de riesgos, centrada en seguridad de la información, al inicio de cualquier proyecto para identificar amenazas, vulnerabilidades y riesgos asociados al mismo.
A6.2	**Los dispositivos móviles y el teletrabajo**	**Recomendación**
A6.2.1	Política de dispositivos móviles	Implementar políticas respaldadas por medidas o controles de seguridad para reducir el riesgo que representan los dispositivos móviles remotos. Se puede considerar el registro de nuevos dispositivos, cancelación de registro de dispositivos móviles, control de software, control de acceso y encriptación en reposo y de dispositivos en tránsito. Restricción de conexión a redes públicas o desconocidas.
A6.2.2	Teletrabajo	Evaluar activos de información que están involucrados con el teletrabajo, realizar evaluación de riesgos aplicada a los activos de información y a las actividades de teletrabajo, implementar VPN para conexión remota segura, preferiblemente con doble factor de autenticación, provisión de escritorio virtual con el fin de impedir el almacenamiento de información sobre el equipo que no sea de la compañía, acuerdos de licencia de software legal, protección ante software malicioso y requisitos de firewall.

Tabla 14 Fragmento de pestaña recomendaciones - Ver Anexo1 ISO27k Versión final.xlsx. Fuente propia

Es necesario, asignar los roles y responsabilidades en cuanto a seguridad de la información, definir funciones y comunicarlas a las personas implicadas, segregar tareas evitando uso o accesos indebidos a la información, aplicaciones o sistemas; establecer la ruta de contacto con las autoridades pertinentes en caso de ocurrencia de un incidente de seguridad, esto se encontrará alineado con la legislación nacional y evitará multas por falta de reporte a las autoridades competentes.

Implementar acciones para teletrabajo, trabajo remoto y uso de dispositivos móviles, tener en cuenta el riesgo que representa el trabajo fuera de las oficinas y generar las restricciones adecuadas que permitan ejecutar la operación sin descuidar la seguridad.

En cuanto al manejo de información, inicialmente, se debe llevar a cabo un inventario de activos, se podrá trabajar bajo el esquema de CMDB, este es un concepto de ITIL – ISO 20000 para facilitar la gestión de servicios TI, es una base de datos que contiene detalles relevantes de cada ítem de configuración (CI) y la relación entre ellos, allí se puede especificar nombre, serial, software asociado, licencias de software en uso, MAC, IP, usuario asignado, ubicación y demás información que se considere relevante para nuestro inventario. Teniendo la CMDB o un documento similar se hace más sencillo establecer quien es el propietario del activo, el uso aceptable para éste y su proceso de devolución.

La clasificación es vital para conocer lo que se debe proteger, se sugiere clasificar la información de acuerdo con el siguiente ejemplo:

- **Confidencial:** acceso restringido y de uso exclusivo para la alta dirección.
- **Restringido:** directores de área y empleados de confianza tienen acceso.
- **Interno:** relativo a la información accesible solo los miembros de la organización, pero en cualquier nivel.

- **Público:** todas las personas, dentro y fuera de la organización, tienen acceso[16].

Partiendo de la clasificación se puede establecer el etiquetado de esta y llevar a cabo el respectivo manejo de activos, apoyado en las políticas de seguridad de la información.

Para la gestión de soportes extraíbles, por ejemplo, las unidades USB o discos duros externos, se recomienda mantener un registro de estos dispositivos (activos e inactivos), cifrar datos para proteger aquellos que se consideran importantes, preservar la información almacenada con copias de seguridad, adicionalmente implementar mecanismos de protección para unidades externas en los equipos de cómputo, apoyar la restricción en el antimalware y/o alguna herramienta tipo DLP; establecer un protocolo para desechar estos equipos, diseñar protocolos para manejo de información física, tener registro de entrada y salida de los soportes para su cotejo con la transportadora y establecer lista de transportadores autorizados.

Establecer reglas de control de acceso a la información, asignar la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de un sistema, conceder los privilegios solamente por el tiempo que sea necesario para el desarrollo de la actividad, apoyarse en la política de control de accesos y allí especificar los procesos de emisión de permisos o cuentas de usuario, modificación, cancelación y determinación del ciclo de vida del Id de usuario.

Instaurar procedimientos seguros para inicio de sesión, hacer uso de doble o múltiple factor de autenticación y establecer horarios para acceso a las aplicaciones; fijar políticas para complejidad de contraseña, bloqueo por número de intentos fallidos, vencimiento de contraseña, cambio periódico de esta, limitación para configurar una contraseña usada con anterioridad, sugerir a los usuarios que no almacenen sus contraseñas en archivo plano, Excel

[16] (Escuela europea de excelencia, 2019)

o texto en sus equipos, que no escriban en papel pues pueden ser visibles para alguien no autorizado.

Proteger el código fuente mediante acceso restringido, hacer uso de registros de auditoría de los cambios realizados, así como las entradas y salidas del código. El desarrollo debe estar sujeto a un ambiente de pruebas previo lanzamiento a producción, entre otras.

5. CONCLUSIONES

A raíz del análisis realizado se puede concluir que hace falta toma de conciencia y orientación en seguridad de la información y ciberseguridad en muchas empresas, en este caso, una empresa dedicada a telecomunicaciones la cual cuenta con falencias y vulnerabilidades en seguridad de la información debido a que no ha tenido asesoramiento sobre la importancia de este eje, de forma transversal, para cualquier área de la compañía.

El análisis GAP realizado facilita tener un panorama claro del estado actual y deseado, adicionalmente, brinda un punto de partida para reforzar los ítems específicos que se encuentran más expuestos, de esta manera, no invertir esfuerzo en los que han alcanzado un nivel de madurez aceptable.

El estado actual del Sistema de Gestión de seguridad de la información (SGSI) en la compañía SSC es inexistente, sin embargo, lo que se espera en una primera fase, es mejorar las capacidades de seguridad de la información, por ello se realizan sugerencias que aporten a mejorar esta postura y a medida que se vayan madurando los procedimientos y adoptando mejores prácticas, se pueda contemplar la implementación de un SGSI.

6. FINANCIAMIENTO

Se realizará la investigación y desarrollo del proyecto de aplicación con recursos propios con el aval de la empresa Sistemas satelitales de Colombia y la Fundación Universitaria los libertadores.

7. REFERENCIAS BIBLIOGRÁFICAS

Admin Tecno-Office. (27 de Agosto de 2021). *http://www.tecno-office.com/*. Obtenido de http://www.tecno-office.com/certificaciones-iso-iec-27000/#:~:text=En%202019%2C%20cerca%20del%2032,Crimen%20cibern%C3%A9tico

ASNET. (2022). *www.asnetla.com*. Obtenido de https://www.asnetla.com/inicio/seguridad/

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. Gobierno de España. (Octubre de 2012). *PAE*. Obtenido de Portal de administración electrónica: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Escuela europea de excelencia. (27 de Agosto de 2019). *www.escuelaeuropeaexcelencia.com*. Obtenido de https://www.escuelaeuropeaexcelencia.com/2019/08/clasificacion-de-la-informacion-segun-iso-27001/#:~:text=Interno%3A%20relativo%20a%20la%20informaci%C3%B3n,de%20la%20organizaci%C3%B3n%2C%20tienen%20acceso.

firma-e Consultoría y desarrollo TI. (14 de 10 de 2014). *firma-e.* Obtenido de https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

INCIBE. (s.f.). *www.incibe.es.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

iso27001security. (2014). *ISO27001security.* Obtenido de www.ISO27001security.com

ISO27001security.com. (2014). *www.ISO27001security.com.* Obtenido de https://www.iso27000.es/assets/files/ISO27k%20ISMS%20and%20controls%20status%20with%20SoA%20and%20gaps%20Spanish.xlsx

Ministerio de Tecnologías de la Información y las Comunicaciones. (s.f.). *https://gobiernodigital.mintic.gov.co/*. Obtenido de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

nqa. (s.f.). *www.nqa.com.* Obtenido de https://www.nqa.com/es-co/certification/standards/iso-27001#:~:text=La%20ISO%2027001%3A2013%20es%20la%20norma%20internacional%20que%20proporciona,informaci%C3%B3n%2C%20as%C3%AD%20como%20cumplimiento%20legal

The British Standards Institution. (2022). *www.bsigroup.com*. Obtenido de https://www.bsigroup.com/es-CO/gestion-de-riesgo-iso-31000-/#:~:text=%C2%BFQu%C3%A9%20es%20ISO%2031000%3F,an%C3%A1lisis%20y%20evaluaci%C3%B3n%20de%20riesgos

Universidad Libre sede Bogotá. (10 de Junio de 2015). *https://www.unilibre.edu.co.* Obtenido de https://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion

www.questionpro.com. (2022). *questionpro*. Obtenido de https://www.questionpro.com/blog/es/analisis-de-brechas/

---

[i] **Y.X. Becerra Rozo**. Colombia. Candidata a Especialista en seguridad de la información de la Fundación Universitaria Los Libertadores e Ingeniera en Telemática de la Universidad Distrital Francisco José de Caldas. Email: yuri.becerra.rozo@gmail.com. Auditor interno ISO 27001:2013, diplomado en seguridad de la información, certificada en fundamentos de ethical hacking, blue team y red team de la Universidad Santiago de Chile (Capacitación USACH), Threat Hunting de Trend Micro. Se ha desempeñado como administradora de consolas de antimalware (Kaspersky, Netskope, Symantec, CrowdStrike y Trend Micro), EDR, XDR, email security, PGP, DLP, CAS, plataformas de virtualización y sistemas operativos Windows, soporte técnico, CCTV, analista mesa de ayuda.

[ii] **R.D. Betancourt Manjarres.** Colombia. Candidato a Especialista en seguridad de la información de la Fundación Universitaria Los Libertadores e Ingeniero Electrónico con énfasis en telecomunicaciones de la Fundación Universitaria los Libertadores. Email: rubenbeta123@gmail.com. Es certificado en Oracle Cloud Infrastructure Foundations 2021, Certified Associate Linux Essentials - Linux Professional Institute, Scrum SFPC, entre otros. Adicional, posee experiencia en administración de servidores Linux, AIX y Windows, Directorio Activo, DNS, DHCP, plataformas de virtualización RedHat, VMware, PowerVM, conocimientos en redes, Switches SAN y LAN para ambientes de virtualización.

[iii] **Y.I. Serrato Rodríguez.** Colombia. Especialista en Seguridad de la Información de la Universidad Sergio Arboleda e Ingeniera en Telemática de la Universidad Distrital Francisco José de Caldas. Email: yiserrator@gmail.com. Es certificada como: CEH, Auditor Líder e interno ISO 27001:2013, Auditor interno ISO 22301:2019, ITIL, Cobit, Scrum Foundations, entre otros. Adicional, posee conocimientos en informática forense, ciberseguridad, auditoría interna y manejo de proyectos. Se ha desempeñado como Oficial de seguridad de la información para empresas multinacionales, consultor para empresas públicas y privadas liderando equipos de trabajo multidisciplinarios, además docente universitario en varias universidades.