Sistema de Gestión de Seguridad de la Información (SGSI) Para Planeta, Proyectos y Obras S.A.S.

Steven Ortiz Vásquez

Universidad Distrital Francisco José De Caldas

Facultad Tecnológica

Ingeniería de Producción por ciclos Propedéuticos

Bogotá D.C, Julio 2022

Sistema de Gestión de Seguridad de la Información (SGSI) Para Planeta, Proyectos y Obras S.A.S.

Steven Ortiz Vásquez Código 20192377062

Trabajo de grado presentado como requisito para optar al título de

INGENIERO DE PRODUCCIÓN

Modalidad: Pasantía Empresarial

MSc. Ing. Martha Edith Pinzón Rueda

Directora

Universidad Distrital Francisco José de Caldas

Facultad Tecnológica

Ingeniería de Producción por Ciclos Propedéuticos

Bogotá D.C, Julio 2022

Bogotá D.C. 22 de julio de 2022

Agradecimientos

Agradezco a Dios, por darme la oportunidad de estudiar una carrera profesional y ver reflejado este sueño con la culminación de mi carrera.

A mis padres José Ortiz y Sor Vásquez, por su apoyo incondicional en todo mi proyecto académico e inculcarme valores y principios que me llevaron a ser la persona que soy hoy en día.

A la Ing. Martha Edith Pinzón, por su apoyo incondicional, su colaboración, sus valiosas enseñanzas y conocimientos para hacer realidad este proyecto de grado.

A la Universidad Distrital Francisco José de Caldas en especial a la Facultad Tecnológica por permitirme cumplir y ver materializado este sueño, por formarme académicamente y como profesional.

Y sobre todo a la empresa Planeta, Proyectos y Obras S.A.S. por brindarme el espacio para dejar ejecutar los conocimientos adquiridos a lo largo de mi carrera en la compañía.

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

Ing. Martha Edith Pinzón

Firma Directora del Proyecto

_____

Yesenia Barrera Gomez

Firma Director Externo

Bogotá D.C. 22 de julio de 2022.

Tabla de contenido

Pág.

Glosario 9
Resumen 13
Introducción 14
Justificación 15
1. Generalidades del proyecto 16
1.1. Problema 16
1.1.1. Planteamiento del problema 16
1.1.2. Formulación 17
1.2. Objetivos 17
1.2.1. Objetivo general 17
1.2.2. Objetivos específicos 17
1.3. Alcance 17
1.4. Metodología 18
2. Marco de Referencia 20
2.1. Marco histórico 20
2.2. Marco normativo 21
2.3. Marco Teórico 21
2.3.1. Generalidades de la seguridad de la información 21
2.3.2. Gestión de Seguridad de la Información 22
2.4. Sistema de Gestión de Seguridad de la Información 23
2.4.1. Ciclo de mejora continua (PHVA) 24
2.5. Norma ISO 27001 25
3. Presentación de la empresa 27
3.1. Generalidades 27
3.1.1. Reseña histórica 27
3.1.2. Objetivo social 27
3.1.3. Líneas de negocio 27
3.1.4. Generalidades de la empresa 28

3.2. Direccionamiento estratégico 29
3.2.1. Misión: 29
3.2.2. Visión: 29
4. Diagnóstico 30
4.1. Identificación de activos 33
4.2. Identificación de amenazas 33
4.3. Identificación de vulnerabilidades 36
4.4. Identificación de riesgos. 38
4.5. Probabilidad de ocurrencia 39
4.6. Impacto potencial 40
4.7. Indicador de riesgo 41
4.8. Identificación de partes interesadas y requisitos pertinentes 42
5. Desarrollo del sistema de gestión de seguridad de la información 46
5.1. Alcance del SGSI 46
5.2. Objetivos del SGSI 46
5.3. Política del SGSI 47
5.4. Interfaces y dependencias (partes interesadas) 48
5.5. Roles, responsabilidades y autoridades en la organización 50
5.6. Planificación 51
5.6.1. Identificación de peligros, evaluación de riesgo y determinación de controles. 51
5.7. Políticas de seguridad 54
5.7.1. Política de copias de respaldo de la información (Backup). 54
5.7.2. Política de Logs o registro de actividades. 55
5.7.3. Política de gestión de cambios 56
5.7.4. Política de Gestión de Incidentes de Seguridad de la Información. 56
5.7.5. Política de responsabilidad del usuario. 57
5.7.6. Política – Creación, revisión y difusión de políticas de seguridad. 58
5.8. Soporte 60
5.8.1. Recursos 60
5.8.2. Competencia 61

5.8.3. Toma de conciencia 61
5.8.4. Comunicación 61
5.8.5. Información documentada 62
5.9. Operación 62
5.9.1. Planificación y control operacional 62
5.9.2. Valoración de riesgos de la seguridad de la información 62
5.9.3. Tratamiento de riesgos de la seguridad de la información 63
5.10. Evaluación del desempeño 63
5.10.1. Seguimiento, medición, análisis y evaluación 63
5.10.2. Auditoría interna 64
5.10.3. Revisión de la alta dirección 64
5.11. Mejora 64
5.11.1. No conformidad y acciones correctivas 64
5.11.2. Plan de mejora 65
6. Conclusiones 66
7. Referencias 68
8. Anexos 70

Lista de tablas

Tabla 1. *Metodología.* 18
Tabla 2. *Generalidades de la empresa.* 28
Tabla 3. *Categorización para la calificación.* 30
Tabla 4. *Calificación diagnóstica.* 30
Tabla 5. *Identificación de activos.* 33
Tabla 6. *Identificación de amenazas.* 34
Tabla 7. *Identificación de vulnerabilidades* 36
Tabla 8. *Identificación de riesgos.* 38
Tabla 9. *Categorización de la ocurrencia.* 40
Tabla 10. *Categorización del impacto potencial.* 41
Tabla 11. *Identificación de partes interesadas.* 43

Tabla 12. *Categorización del impacto potencial.* 63

Lista de figuras

Figura 1. *Ciclo de mejora continua (Ciclo Deming)* 24
Figura 2. *Resultado del diagnóstico inicial SGSI.* 32
Figura 3. *Análisis de activos y riesgos de PPO.* 41
Figura 4. *Mapa de procesos.* 49
Figura 5. *Mapa de organizacional.* 51

Glosario

- **Acción correctiva:** acción tomada para eliminar la causa de una no conformidad detectada u otra situación no deseable.

- **Acción de mejora:** acción de optimización del sistema de gestión en seguridad y salud en el trabajo – SG-SST, para lograr mejoras en el desempeño de la organización en la seguridad y salud en el trabajo de forma coherente con su política.

- **Acción preventiva:** acción para mitigar la(s) causa(s) de una no conformidad potencial u otra situación potencial no deseable.

- **Alta dirección:** persona o grupo de personas que dirigen y controlan una empresa.

- **Ambiente de trabajo:** es el medio donde se desarrolla el trabajo, el cual está determinado por las condiciones térmicas, el ruido, la iluminación, las vibraciones y las radiaciones, así como por los contaminantes químicos y biológicos. El ambiente de trabajo adquiere relevancia porque en este se encuentran los contaminantes y por el tiempo que se permanece allí.

- **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Confiabilidad de la Información**: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

- **Diseño y desarrollo**: Conjunto de procesos que transforma los requisitos en características especificadas o en la especificación de un producto, proceso o sistema.

- **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

- **Factores de riesgo**: Son aquellas variables o características que incrementan la probabilidad de sufrir un suceso.

- **Gestión**: Actividad administrativa que busca mejorar los procesos de una organización para ver los resultados en la productividad y la competitividad de la misma.

- **Indicador**: Referencia que brindan información cualitativa o cuantitativa, conformada por uno o varios datos, constituidos por percepciones, números, hechos, opiniones o medidas, que permiten seguir el desenvolvimiento de un proceso y su evaluación, y que deben guardar relación con el mismo.

- **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones.

- **Mejora continua**: Proceso recurrente de optimización del Sistema de Gestión en Seguridad y Salud en el Trabajo, para lograr mejoras en el desempeño en este 12 campo, de forma coherente con la política de Seguridad y Salud en el Trabajo SST de la organización.

- **Organización**: Conjunto de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones.

- **Parte interesada**: persona o grupo que tiene un interés en el desempeño o éxito de una organización.

- **Peligro**: Fuente, situación o acto con potencial de causar daño en la salud de los trabajadores, en los equipos o en las instalaciones. Es la inminencia de sufrir un accidente o enfermedad.

- **Política**: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la organización, en ella se contemplan las normas y responsabilidades de cada área de la organización. Las políticas son guías para orientar la acción; son lineamientos generales a observar en la toma de decisiones, sobre algún problema que se repite una y otra vez dentro de una organización. En este sentido, las políticas son criterios generales de ejecución que complementan el logro de los objetivos y facilitan la implementación de las estrategias.

- **Política de seguridad y salud en el trabajo**: Es el compromiso de la alta dirección de una organización con la seguridad y la salud en el trabajo, expresadas formalmente, que define su alcance y compromete a toda la organización.

- **Proceso**: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

- **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- **Proveedor**: Organización o persona que proporciona un producto.

- **Riesgo**: Identifica la probabilidad de sufrir un suceso. Los riesgos se cuantifican en probabilidades de sufrir un suceso, se denominan factores de riesgo.

- **Salud en el trabajo**: Es el conjunto de técnicas y procedimientos que tienen por objeto, eliminar o disminuir el riesgo de que se produzcan enfermedades laborales.

- **Seguridad en el trabajo**: Es el conjunto de técnicas y procedimientos que tienen como propósito eliminar o disminuir la posibilidad de que se produzcan los accidentes de trabajo.

- **Sistema**: Es un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo. Los sistemas reciben entradas y proveen salidas.

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

- **Tecnología de la Información**: Se refiere al hardware y software operados por un tercero que procese información en su nombre, para llevar a cabo una función propia de la organización, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo. (Universidad Nacional De Cordoba, 2008)

- **valoración del riesgo**: Consiste en emitir un juicio sobre la tolerancia o no del riesgo estimado.

- **Vigilancia epidemiológica**: Es la recolección sistemática y continúa de datos relacionados con la presencia de posibles efectos en la salud o enfermedades laborales asociadas con un factor de riesgo ocupacional.

Resumen

Palabras clave: Seguridad de la información, sistema de gestión de seguridad de la información, valoración de riesgos de la seguridad de la información.

Planeta, Proyectos y Obras S.A.S. es una empresa dedicada a la licitación de obras públicas, enfocada en el mejoramiento de los procesos empleando tecnología de punta y teniendo como premisa la satisfacción de sus clientes, la seguridad y el bienestar de sus colaboradores.

La documentación e implementación de los sistemas de gestión refleja el compromiso de la empresa con sus clientes y colaboradores, a través de la divulgación de la política, los objetivos y el cumplimiento de las normas legales vigentes. El seguimiento, medición y mejora continua del Sistema de Gestión de Seguridad de la Información permite mejorar la seguridad y la eficiencia de los procesos de la compañía.

Este proyecto documenta e implementa el Sistema de Gestión de Seguridad de la Información para la empresa Planeta, Proyectos y Obras S.A.S. bajo los lineamientos de las normas ISO 27001:2013 empleando el ciclo PHVA: Planear, hacer, verificar y actuar.

Introducción

Las empresas cuentan con información importante y sensible para su uso, que le ayuden a operar y alcanzar los objetivos trazados para su adecuado funcionamiento y desarrollo; independientemente de su tamaño u operaciones, se enfrentan a diario a multitud de amenazas y riesgos derivados de una amplia gama de incidentes que afectan a la información procesada y almacenada en los equipos de TI afectando la buena reputación y nombre de la organización.

Todas las organizaciones están expuestas a las vulnerabilidades y a la realidad de que no solamente existen las amenazas externas, sino las internas, ya que no se puede subestimar los malware diseñados para causar un daño o perjuicio. Por ello en este trabajo se busca fomentar e implementar un Sistema de Gestión de Seguridad de la Información que contribuya a mitigar los riesgos.

La información es uno de los activos más importantes para las empresas y sus procesos de negocio es por ello es que se busca proteger la confidencialidad, integridad y acceso a la información.

El diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) debe estar directamente relacionado con los objetivos y las necesidades de la organización, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

Un SGSI tiene como propósito definir un conjunto de políticas, procedimientos y directrices junto con los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales. Además, puede abarcar otras propiedades como la autenticidad, la responsabilidad y la fiabilidad.

Justificación

Planeta, Proyectos y Obras S.A.S, es una empresa que basa su actividad en prestación de construcción de proyectos de servicio público, su actividad se realiza bajo la premisa de brindar un excelente servicio, buscando la satisfacción de sus clientes internos y externos. Dentro del desarrollo de sus actividades su información está expuesta a ciertos peligros, ya sea en labores administrativos u operativos, que si no reciben el tratamiento adecuado pueden materializarse a través de la perdida de la información.

Es por ello por lo que Planeta, Proyectos y Obras S.A.S refleja la necesidad de desarrollar e implementar el sistema de seguridad de gestión de la información, con el fin de identificar, desarrollar y mejorar los procesos de la empresa, ofreciendo al cliente un servicio de calidad, dando cumplimiento a la normatividad vigente y mejorando su seguridad de la información.

En sus años de trayectoria Planeta, Proyectos y Obras S.A.S ha logrado el reconocimiento de sus clientes como lo son Instituto Nacional de Vías (INVIAS). Es de saber que sus clientes son empresas que tienen información sensible, por lo cual las partes interesadas han decidido emprender el desarrollo de este sistema de gestión, también con el fin de disminuir la amenaza de la pérdida de datos ante cualquier tipo de ciberataque.

Es por ello por lo que este proyecto de grado es de relevancia y prioridad para la empresa Planeta, Proyectos y Obras S.A.S., ya que en la búsqueda la disminución de la perdida de información y su preservación es vital contar con el sistema de gestión de seguridad de la información. A nivel profesional el presente trabajo ofrece una oportunidad muy amplia para adquirir y evidenciar conocimientos en la gestión de calidad y la seguridad de la información, permitiendo ser una clave estratégica para la competitividad y el desarrollo de la empresa.

1. Generalidades del proyecto

1.1. Problema

1.1.1. Planteamiento del problema

Planeta, Proyectos y Obras S.A.S, es una empresa dedicada a la prestación del servicio de construcción de proyectos de servicio público, su oficina principal se encuentra actualmente ubicada en la cuidad de Bogotá.

Con el propósito de prestar servicios de construcción de proyectos de servicio público, Planeta, Proyectos y Obras S.A.S, fundamenta su crecimiento en la gestión exitosa de sus recursos, por lo tanto, se tomó la decisión de prestar sus servicios por medio de teletrabajo, utilizando el internet como herramienta principal de comunicación entre las partes interesadas. Sin embargo, los beneficios de la era digital también acarrean una serie de riesgos e inconvenientes que pueden afectar el desarrollo de las actividades y generar grandes pérdidas si no se cuenta con los mecanismos de control adecuados. Así como el internet se puede usar para el teletrabajo hay ciberdelincuentes desarrollan programas maliciosos y virus para aprovechar las vulnerabilidades de los sistemas en la web y de esta manera acceder de forma mal intencionada a los recursos depositados en la red.

Al no contar con un sistema o procedimientos claros y definidos sobre seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información; y no poseer los adecuados controles sobre la información que maneja, es la potencial pérdida de información, afectando la confidencialidad y los procesos de la empresa.

Teniendo en cuenta lo anterior; no se está realizando un manejo adecuado de la información de los proyectos atendidos por la empresa Planeta, Proyectos y Obras SAS. Se tienen fallas en la protección de activos que contienen información sensible de clientes, y el uso descuidado de los datos puede afectar la imagen de la empresa e incumplir con la protección de datos personales, entre otros.

1.1.2. Formulación

De acuerdo con lo mencionado anteriormente, este proyecto pretende diseñar el Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa Planeta, Proyectos y Obras S.A.S, acorde a sus necesidades, usando un enfoque basado procesos para garantizar la confidencialidad, integridad y disponibilidad de la información.

1.2. Objetivos

1.2.1. Objetivo general

Desarrollar el sistema de gestión de seguridad de la información (SGSI) para Planeta, Proyectos y Obras S.A.S. acorde a los requerimientos establecidos en la ISO 27001:2013.

1.2.2. Objetivos específicos

- Realizar el diagnóstico de la gestión de la información en la empresa.
- Planificar la propuesta de implementación del sistema de gestión de seguridad de la información de la empresa.
- Formular y documentar las medidas de acción con lo establecido por la ISO 27001:2013.
- Determinar mecanismos de seguimiento y control que permitan la gestión de la seguridad de la información.
- Realizar la fase de socialización del sistema de gestión de seguridad de la información con cada uno de los integrantes de la organización.

1.3. Alcance

El alcance del proyecto abarca el diseño un Sistema de Gestión de Seguridad de la información para la empresa Planeta, Proyectos y Obras SAS., el cual está orientado a cubrir la primera fase de la implementación de un Sistema de Gestión de Seguridad de la Información, que corresponde a la etapa de planeación.

Para el desarrollo del proyecto se utilizará como guía principal la norma ISO 27001:2013, que corresponde a un estándar referente a nivel mundial que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

1.4. Metodología

Para la documentación e implementación del sistema de gestión de seguridad de la información para Planeta, Proyectos y Obras S.A.S. se emplea la metodología en la que se fundamentan todos los sistemas de gestión, el clico PHVA: Planear, hacer, verificar y actuar.

Tabla 1. *Metodología***.**

OBJETIVO	ACTIVIDADES
Realizar el diagnóstico de seguridad de la información en la empresa.	-Verificación de los requerimientos de la ISO 27001. -Contextualización de la empresa. -Diagnóstico de la situación actual con respecto a la seguridad de la información. -Valoración de riesgos de seguridad de la información.
Planificar el proceso de elaboración del sistema de gestión de seguridad de la información de la empresa.	-Elaboración de la política, objetivos, procesos y procedimientos del SGSI. -Definición de roles, funciones y frecuencia de seguimientos. -Asignar el responsable del SGSI.
Formular y documentar las medidas de acción con lo establecido por la ISO 27001:2013.	-Documentar los tratamientos de riesgo de seguridad de la información. -Objetivos de seguridad de la información y planes para lograrlos.

Determinar mecanismos de seguimiento y control que permitan la disminución de riesgo de seguridad de la información.	-Determinar controles de acceso a la información. -Definir indicadores para la política de seguridad de la información. -Definir la periodicidad para la medición de los indicadores.
Realizar la fase de socialización del Sistema de Gestión de Seguridad de la Información con cada uno de los integrantes de la organización.	-Documentar programa de capacitación en Seguridad de la información. -Definir la frecuencia en la que se deben presentar las evidencias de las capacitaciones.

Fuente: Autor.

2. Marco de Referencia

2.1. Marco histórico

En los años 80's y principios de los 90's, la seguridad a nivel computacional comienza a tomar relevancia debido a que los sistemas informáticos comenzaron a ser blanco de amenazas como virus, y personas que aprovechaban las vulnerabilidades de los sistemas para tomar provecho o ventaja de los mismos. Es por eso que en 1989 se reúne un grupo de altos ejecutivos y especialistas en seguridad de las principales empresas británicas entre ellas (Shell, BT, Mark & Spencer, Nationwide Building Society, BOC), quienes deciden acordar controles claves para la seguridad, que las organizaciones pudieran cumplir. (Ugas, 2002)

Posteriormente en 1995, el British Standard Institute - (BSI) recoge el conjunto de 10 controles claves de seguridad, inicialmente publicado por el (DTI - Department Trade & Industry), como el Código de Buenas Prácticas para la Administración de la Seguridad Parte 1, y publica la norma BS-7799.

En el año 1998 el BSI genera la Parte 2, donde se detallan más de 100 controles como parte de un ISMS (Sistema de Administración de Seguridad de la Información), basado en una estrategia formal de Análisis de Riesgos. (Travieso, 2003)

El estándar era conocido inicialmente como estándar británico o BS- 7799. Más adelante, se convirtió en el estándar ISO/IEC 17799 cuando fue adoptado por el comité técnico del IEC (Comisión Electrotécnica Internacional) de la ISO para uso internacional.

En el año 1998 es publicada la segunda parte del estándar, (BS 7799-2), la cual establecía los requisitos de un sistema de seguridad de la información (SGSI), con el objetivo de certificar a una organización por parte de una entidad independiente. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO sin cambios sustanciales, en diciembre del año 2000. En este momento fue entregado el status ISO, o norma internacional a la Parte 1 "Código de Buenas Prácticas", y fue publicada la norma con el nombre de la ISO/IEC 17799 – Código de Buenas Prácticas.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión, y solo hasta el año 2005 con más de 1700 empresas certificadas en BS 7799-2, se publicó con algunos cambios, el estándar ISO/IEC 27001 (Sistema de Gestión de Seguridad de la información. Requisitos). Al mismo tiempo, se inició la revisión y actualización de la ISO/IEC 1779, la cual se renombró como ISO/IEC 27002:2005. Código de Práctica la Gestión de la Seguridad de la información. (ISO, 2022)

Luego de una nueva revisión de la ISO/IEC 27001:2005 e ISO 27002:2005, se publican nuevas versiones en 2013 de la ISO/IEC 27001:2013 y de la ISO/IEC27002:2013, la cual tiene cambios en sus dominios y controles en relación con su versión anterior. (ISO, 2022)

2.2. Marco normativo

Para el desarrollo del proyecto se tomará como base la norma ISO 27001:2013 por la cual se enmarcan los Sistemas de Gestión de Seguridad de la Información.

2.3. Marco Teórico

2.3.1. Generalidades de la seguridad de la información

- Información

Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- Seguridad de la Información

La Seguridad de la Información, de acuerdo a la norma ISO 27000:2013, se define como la preservación de la confidencialidad, integridad y disponibilidad de la información.

De acuerdo a la Asociación Española para la Calidad, la Seguridad de la Información tiene como propósito la protección de la información y de los sistemas de la información contra

las amenazas y eventos que atenten con el acceso, uso, divulgación, interrupción y destrucción de forma no autorizada. (Asociación Española para la Calidad (AEC), 2022)

La información representa uno de los activos más valioso de las organizaciones, lo que implica que es indispensable asegurar su protección contra amenazas y eventos que puedan llegar comprometer su confidencialidad, integridad y disponibilidad. La información puede existir en diferentes medios tanto físicos como electrónicos, pero independientemente del medio, es necesario que las organizaciones garanticen y aseguren la debida protección de la información durante su recolección, almacenamiento, tratamiento y uso. (Asociación Española para la Calidad (AEC), 2022)

La seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de la información mediante el establecimiento de un conjunto coherente de procesos, normas y herramientas para la gestión eficaz de acceso a la información, y la implementación de mecanismos y medidas de seguridad tanto físicas como lógicas, orientadas a la prevención y detección de amenazas internas y externas que puedan atentar contra la seguridad de la organización y la continuidad del negocio. (Asociación Española para la Calidad (AEC), 2019)

2.3.2. Gestión de Seguridad de la Información

La gestión de la seguridad de la información es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (Asociación Española para la Calidad (AEC), 2019)

La gestión de la seguridad de la información requiere la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de la información, así como el debido control de acceso a los recursos y activos de información. (López & Ruiz, 2005)

2.4. Sistema de Gestión de Seguridad de la Información

Con el objetivo de garantizar que las organizaciones realizan una correcta gestión de la seguridad de la información, es necesario contar con un proceso sistemático, documento, conocido y adoptado por toda la organización, basado en un enfoque de gestión de riesgos. Este proceso, es el que constituye un Sistema de Gestión de Seguridad de la Información.

De acuerdo a la norma NTC-ISO-IEC 27001:2013, un sistema de gestión de seguridad de la información tiene por finalidad preservar la confidencialidad, integridad y disponibilidad de la información, a través de la aplicación de un proceso de gestión del riesgo. (ISO, 2022)

Un Sistema de Gestión de Seguridad de la Información, les permite a las organizaciones gestionar de manera efectiva los riesgos asociados a la seguridad sobre sus activos de información mediante la identificación de las amenazas que puedan llegar con comprometer la seguridad sus activos de información, lo cual, genera confianza en sus partes interesadas debido a que demuestra que los riesgos de la organización son debidamente gestionados. (ISO, 2022)

Un Sistema de Gestión de Seguridad de la Información permite el establecimiento de un gobierno de seguridad, soportado en una estructura organizacional, responsabilidades, políticas, procedimientos, procesos y recursos, para gestionar de manera adecuada la seguridad de la información. Proporciona una herramienta que le ayuda a las organizaciones a establecer políticas, procedimientos, medidas y controles de seguridad alineados a los objetivos de negocio, y provee los elementos adecuados para la debida gestión de los riesgos con propósito de poder mantener el riesgo por debajo del nivel definido por la organización.

Un Sistema de Gestión de la Seguridad de la Información les permite a las organizaciones tener una visión general del estado de protección y vulnerabilidad de sus activos de información y de la efectividad de las medidas de seguridad que se implementen, insumos que son fundamentales para apoyar la toma de decisiones por parte de la alta directiva con relaciones a las estrategias a seguir.

La implementación de un Sistema de Gestión de Seguridad de la Información, le provee a las organizaciones un proceso de mejora continua que asegura la debida y continua gestión de los riesgos de seguridad y permite la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de los activos de información de la organización. (ISO 27001:2013, 2015)

2.4.1. Ciclo de mejora continua (PHVA)

El ciclo de mejora continua, también conocido como ciclo PDCA (del inglés plando-check-act) o PHVA (planificar-hacer-verificar-actuar) o Ciclo de Deming por ser Edwards Deming su creador, es uno de los sistemas más usados para la implementación de un sistema de mejora continua, el cual establece los siguientes cuatro pasos o fases esenciales que de forma sistemática las organizaciones deben llevar a cabo para lograr la mejora continua de sus sistemas de gestión:

Figura 1. *Ciclo de mejora continua (Ciclo Deming)*

Fuente: https://www.pdcahome.com/wp-content/uploads/2013/08/ciclo-pdca.jpg

- **Planificar**: En esta fase se debe realizar un análisis del estado actual de la empresa, definir el alcance y los objetivos del SGSI y realizar la identificación de los activos con los que cuenta la empresa. Esta etapa es muy importante y es la que permite el

desarrollo de las otras, lo que indica que si no planeamos bien los resultados en las otras 3 etapas no serán confiables.

- **Hacer**: Las tareas que se deben ejecutar en esta etapa son: Realizar la valoración de los activos, la identificación y valoración de las vulnerabilidades y amenazas, adicionalmente también se deben identificar, analizar y evaluar los riesgos con el fin de definir controles para mitigarlos.
- **Verificar**: En esta etapa se debe monitorear y revisar el SGSI, medir la eficacia de los controles aplicados y revisar los riesgos residuales, adicionalmente también se deben generar auditorías internas al SGSI
- **Actuar**: Las actividades que se deben realizar en esta fase son: Implementar las mejoras identificadas, implementar las acciones preventivas y correctivas y finalmente comprobar la eficacia de las acciones y mejoras implementadas

2.5. Norma ISO 27001

La familia de las normas ISO/IEC 27000, son un marco de referencia de seguridad a nivel mundial desarrollado por la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización. Estas normas especifican los requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información. (ISO 27001:2013, 2015)

En Colombia, el Instituto Colombiano de Norma Técnicas y Certificaciones, ICONTEC, es el organismo encargado de normalizar este tipo de normas.

- **ISO/IEC 27001**. La última versión de esta norma fue publicada a finales del 2013, y corresponde a la principal norma de la serie 27000 debido a que contiene los diferentes requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información en las organizaciones independiente de su tipo, tamaño o naturaleza. Esta norma también

incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adoptadas a las necesidades de la organización.

La versión 2013 de la norma ISO 27001, alineo su estructura conforme a los lineamientos definidos en el Anexo SL12 de las directivas ISO/IEC, con el objetivo de mantener la compatibilidad entre las normas ISO de sistemas de gestión que se han ajustado a este anexo. Este enfoque de la estructura de la nueva ISO27001:2013 basado en el Anexo SL, le ayuda a las organizaciones que deseen integrar sus diferentes sistemas de gestión, como el de Calidad, Ambiental, Seguridad de la Información, etc., en un único sistema integrado de gestión, debido a que las normas ISO que se han ajustado al Anexo SL, manejan aspectos comunes como, la misma estructura de alto nivel e idénticos títulos de numerales, textos y términos.

3. Presentación de la empresa

3.1. Generalidades

3.1.1. Reseña histórica

Planeta, Proyectos y Obras SAS fue constituida en octubre de 2016, inicialmente, estaba vinculada accionarialmente a la empresa española Construcciones Vera S.A. (uno de los líderes del sector de construcción en el sur de España). Pero desde enero de 2017, el único accionista es Emilio Sánchez Vera (Exdirector Gerente de la compañía en España). Desde su constitución, Vera Colombia SAS ha resultado adjudicataria de 5 contratos de obra; actualmente, 3 se encuentran concluidos y 2 están en ejecución con un elevado grado de avance.

3.1.2. Objetivo social

Planeta, Proyectos y Obras S.A.S es una compañía de carácter privado que suministra soluciones en cuanto a licitaciones públicas, dedica a construcción de proyectos de servicio público, entre otros, apoyada en tecnología de la información y la comunicación de última generación buscando siempre la absoluta satisfacción de sus clientes.

Proporciona a sus clientes servicios de mayor valor, con soluciones eficientes y optimización de licitaciones. Cuenta con un equipo altamente capacitado, confiable y posee la mejor disposición para atender todos los requerimientos de los clientes que solicitan sus servicios.

3.1.3. Líneas de negocio

La línea de negocio de Planeta, Proyectos y Obras SAS:

La actividad de construcción constituye la columna vertebral de la organización, tanto por su trayectoria y experiencia, como por su volumen de facturación, ya que supone la mayor proporción de los ingresos del grupo empresarial.

Este negocio principal desarrolla y ejecuta proyectos de obra civil y edificación, tanto para las administraciones públicas, bien sean de carácter estatal, autonómico o local, como para clientes privados.

3.1.4. Generalidades de la empresa

Tabla 2. *Generalidades de la empresa.*

GENERALIDADES	INFORMACIÓN
Razón social	PLANETA, PROYECTOS Y OBRAS SAS
NIT	901020571-8
Sigla	PPO
Logo	PLANETA PROYECTOS Y OBRAS
Dirección	Calle 90 # 12-28
Teléfono	3206667747-3178664867
Gerente	Yesenia Barrera Gómez
Actividad económica	4220: Construcción de proyectos de servicio público.
Tipo de organización	Sociedad por acciones simplificada
Número de empleados	Gerente, Asistente administrativo, Ingeniero Civil. (3)
Fecha de constitución	1° de noviembre de 2016
Implementador de los sistemas de Gestión	Steven Ortiz Vasquez
Código CIIU	4210: Construcción de proyectos de servicio público

Fuente: Autor.

Planeta, Proyectos y Obras SAS fue constituida en octubre de 2016, inicialmente, estaba vinculada accionarialmente a la empresa española Construcciones Vera S.A. (uno de los líderes del sector de construcción en el sur de España). Pero desde enero de 2017, el único accionista es Emilio Sánchez Vera (Exdirector Gerente de la compañía en España).

3.2. Direccionamiento estratégico

3.2.1. Misión:

"Planeta, Proyectos y Obras SAS, Desarrolla proyectos de construcción e ingeniería basados en principios empresariales de alta calidad con un capital humano calificado, buscando la satisfacción de los clientes, el crecimiento económico y el mejoramiento de la sociedad." (Gonzalez, 2016)

3.2.2. Visión:

"Consolidarnos como una empresa líder a nivel nacional en el sector de proyectos de construcción e ingeniería cumpliendo con los tiempos establecidos, con alta calidad y con total respeto al medio ambiente, logrando así demostrar nuestra experiencia." (Gonzalez, 2016)

4. Diagnóstico

El diagnóstico permite evidenciar la situación actual de Planeta, Proyectos y Obras SAS respecto al cumplimiento de cada uno de los requisitos que están estipulados en la ISO 27001:2013. De acuerdo con este diagnóstico se plantean las actividades que deben ser desarrolladas para la implementación del Sistema Integrado de Seguridad de la Información.

En la siguiente tabla se evidencia el puntaje obtenido en cada numeral de acuerdo con el diagnóstico realizado teniendo en cuenta los siguientes parámetros de calificación:

Tabla 3. *Categorización para la calificación.*

% de Cumplimiento	Detalle
0%	No cumple
25%	Cumple parcialmente
50%	Cumple medianamente
75%	Cumple significativamente
100%	Cumple completamente
N/A	No aplica

Fuente: Autor.

Tabla 4. *Calificación diagnóstica.*

Requisitos	Requerimientos	Puntaje
Contexto de la organización	• Conocimiento de la organización y de su contexto • Comprensión de las necesidades y expectativas de las partes interesadas • Determinación del alcance del sistema de gestión de la seguridad de la información • Sistema de gestión de la seguridad de la información	12,5%
Liderazgo	• Liderazgo y compromiso • Política	8,8%

	• Roles, responsabilidades y autoridades en la organización	
Planificación	• Acciones para tratar riesgos y oportunidades • Objetivos de seguridad de la información y planes para lograrlos	0,0%
Soporte	• Recursos • Competencia • Toma de conciencia • Comunicación • Información documentada	19,8%
Operación	• Planificación y control operacional • Valoración de riesgos de la seguridad de la información • Tratamiento de riesgos de la seguridad de la información	8,3%
Evaluación del desempeño	• Seguimiento, medición, análisis y evaluación • Auditoría interna • Revisión por la dirección	19,3%
Mejora	• No conformidades y acciones correctivas • Mejora continua	56,3%
Promedio general	Total	15,2%

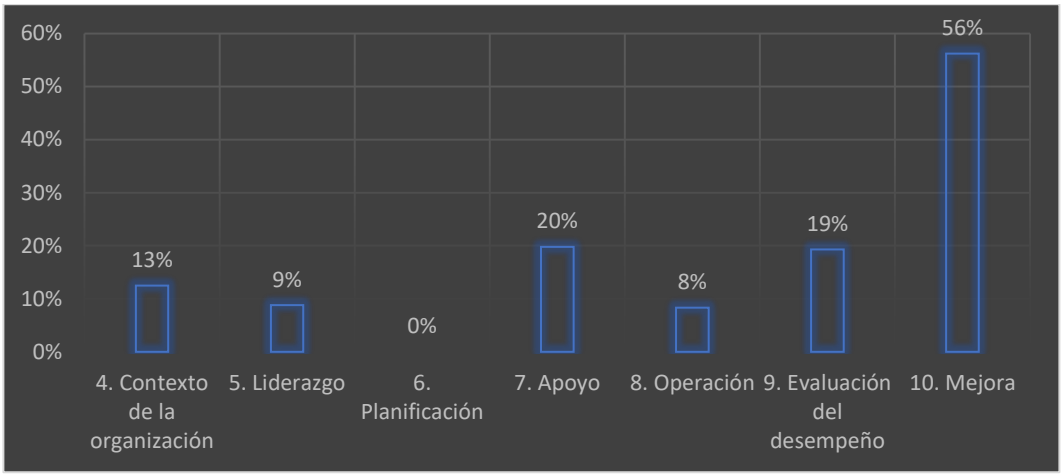
Fuente: Autor.

El 15,3% obtenido como resultado del diagnóstico evidencia que el Sistema de Gestión de Seguridad de la Información está en una etapa verbal, por lo tanto, es necesario desarrollarlo desde su fase inicial, es decir, desde el proceso de planeación y de implementación de este. Para ver en detalle el puntaje otorgado a cada uno de los requisitos de la ISO 27001:2013 (ver Anexo A).

La siguiente gráfica representa el nivel de cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información, a partir de ahora se enunciará como (SGSI), que se

cumplen parcial y totalmente, y los que no se cumplen, el resultado es tomado del diagnóstico mencionado anteriormente.

Figura 2. *Resultado del diagnóstico inicial SGSI.*



Fuente: Autor

Considerando el resultado del diagnóstico inicial del SGSI que se realizó para la empresa Planeta, Proyectos y Obras S.A.S se realizó un plan de trabajo con el fin de dar cumplimiento a los requisitos establecidos en la ISO 27001:2013 en cuanto a su documentación y posterior sensibilización.

Tomando como base lo mencionado anteriormente se debe proceder compilando toda la información requerida para comenzar a ejecutar cada uno de los pilares mencionados en la ISO 27001:2013, en los cuales se debe dar cumplimiento a los aspectos necesarios.

Elaborar una estrategia acorde a las necesidades reales de la compañía, definiendo el alcance que se debe tener a nivel interno y externo proponiendo planes que mitiguen los riesgos comunes del sector. Como se debe tener un ciclo de mejora continúa aplicando PHVA este se debe tener con un mapeo que desglose y exprese cada uno los ítems requeridos y las variables que dependan cada factor que se tenga, en caso de una eventualidad obtenida tener cada plan de acción de cada variable.

4.1. Identificación de activos

Para realizar la identificación de los activos se utilizará el inventario proporcionado por la Gerencia y se determinara el tipo de activo al que pertenece de las áreas seleccionadas en el alcance, los cuales son:

Tabla 5. *Identificación de activos.*

ACTIVOS	TIPO DE ACTIVO
Documentación en papel	Información y datos
Documentación digital	Información y datos
Administrador del sistema	Personal
Servidor de almacenamiento	Información y datos
Drive	Información y datos
Computador portátil marca ASUS	Información y datos
Internet (dos canales de 50MB) y telefonía	Información y datos
Impresoras marca Epson	Información y datos

Fuente: Autor.

4.2. Identificación de amenazas

La identificación de amenazas tiene el propósito de delimitar cuales son las amenazas que están aquejando a los activos de información actualmente en la entidad y se deben tener en cuenta como una parte focal del desarrollo del SGSI. Las siguientes tablas muestran cada una de las amenazas que pueden llegar a materializarse en la empresa Planeta, Proyectos y Obras SAS.

Tabla 6. *Identificación de amenazas.*

AMENAZAS	DESCRIPCIÓN
Fuego	En caso de que esta amenaza se materialice y dependiendo de la magnitud del desastre, es probable que se pierdan los equipos que soportan a los activos de información de clientes, del personal, las aplicaciones de uso diario, etc. También puede verse afectada la integridad del material impreso y de las instalaciones en general. La degradación generada por esta amenaza es muy alta.
Acceso no autorizado	La degradación se considera alta, ya que actualmente, la empresa no cuenta con las normas de seguridad para el acceso a sus oficinas, dejando vulnerables los equipos informáticos a terceros.
Daño por agua	Los daños por agua pueden llegar a ser significativos debido al posicionamiento actual de los equipos de cómputo y de red. En caso de que la amenaza se materialice, afectaría la disponibilidad de la información y/o aplicaciones por los daños que puedan presentarse en los equipos. La degradación que esta amenaza proporciona a los activos se cataloga como muy alta y su frecuencia es baja.
Humedad	Esta amenaza proporciona un alto nivel de degradación a los activos de información en caso de materializarse debido al posible daño que puedan sufrir los equipos por mantenerse en zonas sin ventilación y con temperaturas inadecuadas.
Fenómeno sísmico	Los daños que pueden llegar a provocar un fenómeno sísmico de mucha intensidad implican un riesgo para la integridad de las instalaciones de la organización, adicionalmente pueden verse afectados los equipos informáticos y los soportes de información que se encuentran dentro de las instalaciones. La amenaza puede afectar la disponibilidad de la información teniendo en cuenta posibles daños estructurales o perdida de la locación.
Perdida de la información	Al materializarse esta amenaza, se pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de la misma. La degradación se cataloga como alta, ya que la empresa está perdiendo información que puede afectarla o a sus clientes directamente.
Fallo del disco	Es importante tener una copia de seguridad ya que en dado caso de materializarse puede resultar en perdida de información. Puede llegar a generar una amenaza muy alta.

Virus	La degradación de esta amenaza se cataloga como muy alta. Las fallas en el diseño del software en materia de seguridad son una puerta abierta para que atacantes accedan a información crítica para la empresa.
Modificar información	Esta amenaza va muy ligada al abuso de privilegios de acceso en cuanto a la importancia del manejo de logs. La degradación de los activos de información es muy alta.
Indisponibilidad de este empleado	La degradación de esta amenaza es media. Dentro del plan de continuidad del negocio, debe mantenerse un registro de qué usuarios son backup de los otros, en caso de que suceda alguna eventualidad. En caso de que un usuario no asista a cumplir sus labores, otro siempre debe respaldarlo.
Uso de información privada de la empresa sin autorización	La degradación se considera alta, ya que actualmente, la empresa no cuenta con las normas de seguridad para el acceso a sus oficinas, dejando vulnerables los equipos informáticos a terceros.
Errores frecuentes	Los errores de los usuarios pueden llegar a impactar gravemente en todas las dimensiones, teniendo en cuenta que son ellos los encargados de realizar la operación de la entidad y tienen acceso a información crítica para la empresa. La degradación que puede llegar a generar esta amenaza es muy alta.
Perdida del usuario y/o contraseña	Los errores de los usuarios pueden llegar a impactar gravemente en todas las dimensiones, teniendo en cuenta que son ellos los encargados de realizar la operación de la entidad y tienen acceso a información crítica para la empresa. La degradación que puede llegar a generar esta amenaza es muy alta.
Daño del servidor	En el caso de que esta amenaza se materialice y dependiendo de la magnitud, es posible que se pierdan los activos de la información.
Acceso a la red o al sistema de información por personas no autorizadas	La degradación se considera alta, ya que actualmente, la empresa no cuenta con las normas de seguridad para el acceso a sus oficinas, dejando vulnerables los equipos informáticos a terceros.
Daño físico	En el caso de que esta amenaza se materialice y dependiendo de la magnitud, es posible que se pierdan los activos de la información.
Pérdida y/o robo de computadores	El robo y/o perdida de equipos informáticos o de información impresa conlleva una degradación muy alta de los activos. Afecta las dimensiones disponibilidad y confidencialidad de la información. Debe prevenirse desde el punto lógico y físico en las instalaciones de la entidad.

Sensibilidad del equipo a los cambios de voltaje	En el caso de que esta amenaza se materialice y dependiendo de la magnitud, es posible que se pierdan los activos de la información.
No disponibilidad del servicio Intermitencias	La degradación para esta amenaza es muy alta porque en caso de que se sufra algún daño y se pierda el acceso a internet en la empresa, los servicios a utilizados a nivel internos se verán seriamente afectados.
Pérdida de electricidad	Un corte de suministro eléctrico puede afectar la disponibilidad de los equipos de la organización en caso de que sea por una larga duración. La degradación que presenta esta amenaza es muy alta teniendo en cuenta que podría dejar a la organización inhabilitada para realizar sus tareas diarias.

Fuente: Autor.

4.3. Identificación de vulnerabilidades

La identificación de las vulnerabilidades tiene como objetivo determinar las debilidades que se encuentran en un activo y que pueden ser explotadas por una amenaza, lo cual se convertiría en un riesgo de seguridad.

La siguiente tabla muestra las vulnerabilidades identificadas en la empresa Planeta, Proyectos y Obras SAS.

Tabla 7. *Identificación de vulnerabilidades***.**

AMENAZAS	VULNERABILIDADES
Fuego	♦ Los documentos no se almacenan en gabinetes a prueba de fuego.
Acceso no autorizado	♦ No existe copia de seguridad.
Fenómeno sísmico.	♦ Ausencia del plan de continuidad de negocio. ♦ Condiciones de la estructura de la empresa
Humedad	♦ Los documentos no se almacenan en gabinetes a prueba de humedad.
Daño por agua	♦ Los documentos no se almacenan en gabinetes a prueba de agua.
Perdida de la información	♦ Los documentos no se almacenan en gabinetes a prueba de violaciones.

Fallo del disco	♦ No hay copia de seguridad del documento.
Virus	♦ El programa antivirus no se actualiza de forma oportuna.
Modificar información	♦ El esquema de control no ha sido definido de forma adecuada
Acceso no autorizado	♦El esquema de control no ha sido definido de forma adecuada. ♦ Existe un acceso indiscriminado.
Indisponibilidad de este empleado	♦ No hay alguien más que ocupe esta posición.
Pérdida de electricidad.	♦ Ausencia del plan de continuidad de negocio. ♦ Condiciones de la estructura de la empresa
Uso información privada de la empresa sin autorización	♦El esquema de control no ha sido definido de forma adecuada. ♦ Existe un acceso indiscriminado.
Errores frecuentes	♦ Muchos empleados no han recibido capacitación adecuada.
Perdida del usuario y/o contraseña	♦ El esquema de control no tiene copia de ellas
Daño del servidor	♦ El esquema de control no ha sido definido de forma adecuada
Perdida del usuario y/o contraseña	♦ Eliminación de medios de almacenamiento sin eliminar datos.
Uso de información privada de la empresa sin autorización	♦ El esquema de control no tiene copia de ellas
Acceso a la red o al sistema de información por personas no autorizadas. Amenaza o ataque con bomba.	♦ Contraseñas predeterminadas no modificadas.
Daño físico, bloqueo por virus	♦ Falta de formación y conciencia sobre seguridad. ♦ Mantenimiento inadecuado.
Pérdida, robo de computadores	♦ Protección física no apropiada.
Sensibilidad del equipo a los cambios de voltaje	♦ Sensibilidad del equipo a la humedad, temperatura o contaminantes.
No disponibilidad del servicio Intermitencias	♦ Inadecuada gestión de red. ♦ Respaldo inapropiado o irregular.
Suspensión por pago	♦ No prestación de servicio adecuado a las partes interesadas.
Pérdida de electricidad	♦ No prestación de servicio adecuado a las partes interesadas.

Acceso no autorizado	♦ Falta de formación y conciencia sobre seguridad. ♦ Mantenimiento inadecuado.
Daño y/o falla de la impresora	♦ No prestación de servicio adecuado a las partes interesadas.

Fuente: Autor.

4.4. Identificación de riesgos.

La identificación de riesgos expuesta a continuación se propone identificar las incertidumbres a las que Planeta, Proyectos y Obras SAS.

Tabla 8. *Identificación de riesgos***.**

RIESGO	RESULTADO
Incendio	• Daño de los equipos de tecnología afectados por las llamas. • Heridas al personal que se encuentre cerca del área afectada. • Perdida de la información impresa en la entidad. • Deterioro o Perdida de las instalaciones.
Sismo	• Degradación o perdida de las instalaciones y equipos.
Inundación	• Daño de los equipos de tecnología afectados por el agua. • Deterioro en el cableado de las instalaciones. • Deterioro y posible humedad dentro de la entidad.
Fallas y/o errores humanos	• Perdida de la confidencialidad, integridad y/o disponibilidad de la información de clientes o empleados debido a la falta de capacitación de seguridad de la información a los colaboradores que tienen relación con las aplicaciones de uso diario.
Acceso a individuos no autorizados	• Acceso no autorizado a los sistemas y a la información confidencial de la entidad. • Acceso no autorizado a los dispositivos instalados de telecomunicaciones, servidores y equipos de cómputo por parte de terceros.

	• Acceso no autorizado a la información impresa que se encuentre en la entidad.
Tecnología obsoleta	• Desconexión a la red local e internet. • Tiempos de caída en las aplicaciones Web de la entidad. • Retrasos en la operación de los usuarios y clientes.
Controles incompletos o inadecuados	• La integridad de la información se puede ver comprometida debido a Logs incompletos de las bases de datos y aplicaciones que permitan identificar los cambios y su procedencia dentro del sistema.
Instalación de software no autorizado	• Posibilidad de infección por virus, malware o troyano dentro de la red de la empresa. • Incumplimiento en adquisición de licencias del software no autorizado.
Hacking	• Afecta la confidencialidad de la información de los usuarios y clientes. • Robo de información
Interrupción del servicio de energía	• Retrasos en la operación de los usuarios y clientes. • Tiempos de caída en los equipos de telecomunicaciones y de cómputo.
Alto consumo de banda	• Saturación en el tráfico de la red, impidiendo el óptimo desempeño de las aplicaciones.

Fuente: Autor.

4.5. Probabilidad de ocurrencia

La probabilidad de ocurrencia tiene como objetivo dar un porcentaje a que la vulnerabilidad ocurra, de esta manera dar un valor a dicha vulnerabilidad, a continuación, se presentan los parámetros de clasificación propuestos por parte del autor:

- **Muy baja**: la probabilidad de que ocurra un riesgo, es decir, que se materialice, es demasiado baja, casi nula.
- **Baja**: la probabilidad de que ocurra es baja, aunque puede presentarse.
- **Media**: el riesgo puede materializarse en cualquier momento.
- **Alta**: la materialización del riesgo es alta, de hecho, suele presentarse.

- **Muy alta**: es muy alta la probabilidad de ocurrencia del riesgo.

Tabla 9. *Categorización de la ocurrencia.*

% de Ocurrencia	Valor cualitativo
0 - 20%	Muy baja
20,1% - 40%	Baja
40,1% - 60%	Media
60,1% - 80%	Alta
80,1% - 100%	Muy alta

Fuente: Autor.

4.6. Impacto potencial

El impacto potencial tiene como objetivo dar un valor cuantitativo al impacto que tendría en la organización si dicha amenaza y/o vulnerabilidad ocurriera dando alcance a las actividades diarias de la organización, a continuación, se presentan los parámetros de clasificación propuestos por parte del autor:

- **Muy baja**: el impacto, si se materializa, es demasiado baja, casi nula.
- **Baja**: el impacto, si se materializa, es bajo, aunque puede presentarse y traer problemas para el correcto funcionamiento de la organización.
- **Media**: el impacto puede materializarse en cualquier momento y traer problemas para el correcto funcionamiento de la organización.
- **Alta**: el impacto, si se presenta puede traer grandes problemas para el correcto funcionamiento de la organización.
- **Muy alta**: el impacto si se materializa, puede traer problemas bastante grandes y preocupantes para el correcto funcionamiento de todos los procesos de la organización.

Tabla 10. *Categorización del impacto potencial.*

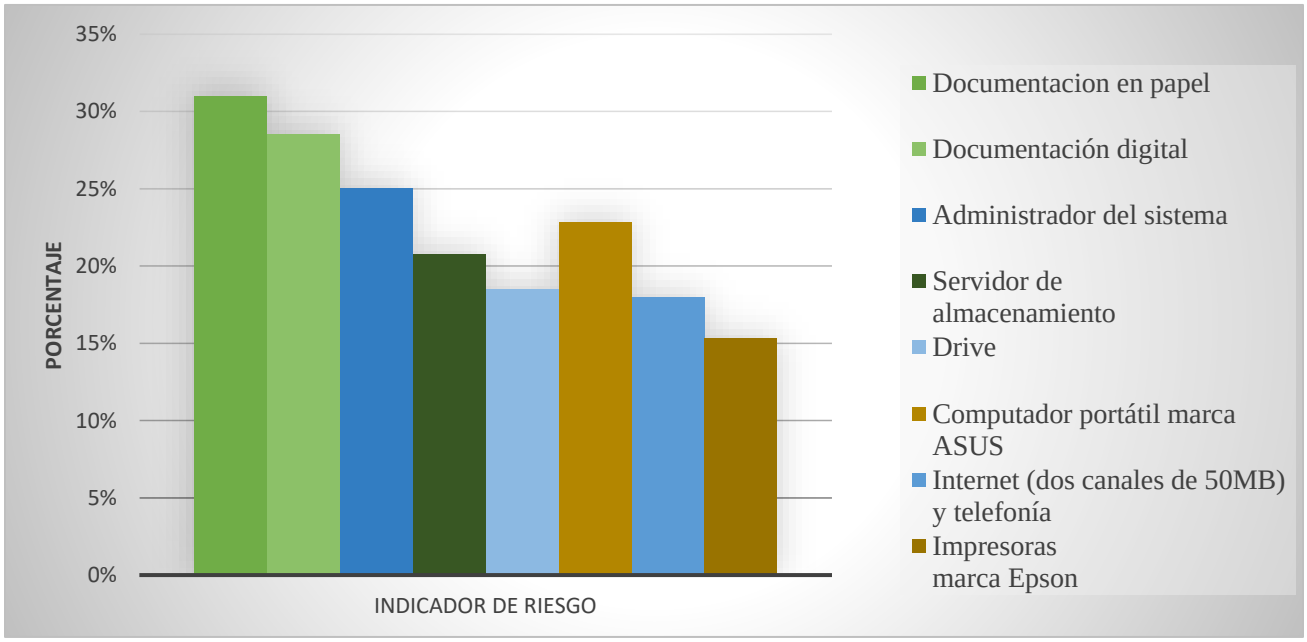
Impacto	Valor cualitativo
0 – 2	Muy baja
3 - 4	Baja
5 - 6	Media
7 - 8	Alta
9- 10	Muy alta

Fuente: Autor.

4.7. Indicador de riesgo

Se presenta el indicador de riesgo por activos de la información de la organización dado la valoración de cada riesgo y amenaza, probabilidad de ocurrencia e impacto potencial que tendría esta amenaza en la organización, con el fin de analizar el efecto que posee cada activo y de esta manera reducir su posible afectación que tiene sobre el Sistema de Gestión de la Información. (Ver Anexo B).

Figura 3. *Análisis de activos y riesgos de PPO.*



Fuente: Autor

Se observa que la vulnerabilidad más alta que encontramos es documentación de papel con un (17%) con respecto a todos los demás activos (Ver Figura 3), el cual es el riesgo más alto del sistema para la organización; así mismo se observa que la documentación digital no está alejada del más alto con un (16%), dando que la documentación que no se encuentra en la nube da una sumatoria de (33%) siendo el riesgo más alto al sistema de información.

4.8. Identificación de partes interesadas y requisitos pertinentes

Se presenta la identificación de las necesidades, expectativas y requerimientos del SGSI de las partes interesadas de Planeta, Proyectos y Obras SAS., con el fin de analizar el efecto que poseen sobre la organización y la posible afectación que tienen sobre el Sistema de Gestión de Seguridad de la Información. (Ver anexo C)

Tabla 11. *Identificación de partes interesadas.*

PARTE INTERESADA	CONTEXTO	NECESIDAD	EXPECTATIVA	RESPONSABLE	SEGUIMIENTO	REQUISITOS
Cliente	Externo	• Entregar proyectos con los requerimientos solicitados y altos estándares de calidad. • Brindar una adecuada atención al cliente. • Realizar entregas oportunas y puntuales acorde al cronograma establecido por la entidad.	• Ofrecer precios competitivos y acordes a los requerimientos de la entidad.	• Ingeniero. • Ventas y Comercialización. • Gestión de la Dirección. • Gestión de HSEQ.	• Control de inventarios • bitácora del proyecto. • Actas de avance del proyecto. • Evaluación de satisfacción.	• Requisitos legales. • Plataforma especializada. • Información pertinente de la entidad.
Proveedores	Externo	• Cumplir con los plazos de pagos y montos acordados, • Decepcionar y aceptar las materias primas, insumo o suministros. • Hacer la recepción de los pedidos de manera ágil para proceder con el conteo respectivo.	• Mantener compromiso y responsabilidad en las negociaciones. • Brindar relaciones comerciales estratégicas y de larga duración. • Generar constante órdenes de compra.	• Gestión de Compras. • Gestión de la Dirección. • Producción.	• Reportes contables. • Comprobantes de pago. • Actas de recepción. • Generar acuerdos entre las partes interesadas.	• Requisitos legales. • Plataforma especializada. • Información pertinente de la entidad.

PARTE INTERESADA	CONTEXTO	NECESIDAD	EXPECTATIVA	RESPONSABLE	SEGUIMIENTO	REQUISITOS
Entes Reguladores (Gobierno, DIAN, Secretaría Distrital de Ambiente, entre otros)	Externo	• Cumplir con las obligaciones tributarias. • Reportar los estados financieros ante la Cámara de Comercio. • Cumplir con las obligaciones del empleador. • Cumplir con las normativas ambientales. • Mantener una correcta ejecución de los sistemas de gestión.	• Generar empleo. • Contribuir con el crecimiento económico del país. • Brindar condiciones adecuadas a los trabajadores.	• Gestión de la Dirección. • Gestión de HSEQ.	• Control del cumplimiento de las obligaciones tributarias. • Comprobantes pago de nómina. • Reportes contables. • Estudios de caracterización de las aguas. • Certificaciones legales.	• Requisitos legales. • Plataforma especializada. • Información pertinente de la entidad.
Trabajadores y/o Contratistas	Interno	• Realizar pagos de sueldo oportunamente. • Garantizar óptimas condiciones laborales. • Suministrar la dotación necesaria.	• Brindar una buena remuneración. • Ofrecer estabilidad laboral. • Asegurar un adecuado ambiente laboral. • Ofrecer las capacitaciones correspondientes.	• Gestión de la Dirección. • Gestión de HSEQ. • Gestión de Compras.	• Desprendibles de nómina. • Evaluación de desempeño. • Evaluación de clima laboral. • Plan de capacitaciones.	• Requisitos legales. • Plataforma especializada. • Acuerdo de confidencialidad. • Controles de acceso.

PARTE INTERESADA	CONTEXTO	NECESIDAD	EXPECTATIVA	RESPONSABLE	SEGUIMIENTO	REQUISITOS
Accionista (Dueño)	Interno	• Generar e incrementar las utilidades y rentabilidad de la producción. • Mantener estabilizados los procesos llevados a cabo en la compañía. • Eliminar las brechas existentes durante las diferentes etapas de producción. • Mantener altos estándares de calidad en el producto final. • Cumplir con las obligaciones legales teniendo un comportamiento ético organizacional.	• Optimizar los recursos en la ejecución de las actividades, disminuyendo los desperdicios. • Lograr la fidelización de los clientes. • Generar ventajas competitivas para un posicionamiento en el sector. • Alcanzar un reconocimiento en el mercado. • Obtener nuevas oportunidades de negocio. • Ampliar la participación en el mercado incrementando su capacidad productiva.	Todos los procesos.	• Reportes contables. • Cumplimiento de los objetivos y metas. • Reportes de los estados de avance de los sistemas de gestión. • Control de inventarios. • Evaluación de satisfacción del cliente. • Registro de ventas.	• Requisitos legales. • Plataforma especializada. • Acuerdo de confidencialidad. • Controles de acceso.

Fuente: Autor.

5. Desarrollo del sistema de gestión de seguridad de la información

El siguiente capítulo desarrolla las actividades descritas en la metodología escogida para el diseño del Sistema de Gestión de Seguridad de la información de la empresa Planeta, Proyectos y Obras SAS. Estas actividades como un conjunto permitirán establecer un diseño que satisfaga las necesidades de la empresa y que esté alineado con la misión y visión de esta.

5.1. Alcance del SGSI

Geográficamente, el SGSI será implementado de forma remota dado que la empresa no tiene un lugar específico, sino que los procesos administrativos, financieros, tecnológicos y operativos se realizan desde la casa de cada colaborador. El sistema de gestión de seguridad de la información incluye dentro de su alcance la identificación y valoración de amenazas, riesgos y vulnerabilidades que aquejan a la empresa Planeta, Proyectos y Obras SAS.

Teniendo en cuenta que el alcance del Sistema de Gestión de Seguridad de la Información de la organización debe estar debidamente documentado y publicado con el fin de permanecer disponible para las partes interesadas, en el anexo D se encuentra el diseño gráfico que divulgará esta información e indicará los límites, aplicabilidad de los procesos, las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones.

5.2. Objetivos del SGSI

El objetivo principal que tiene el SGSI es garantizar que los activos de información utilizados en las diferentes funciones de negocio en la empresa Planeta, Proyectos y Obras SAS. se encuentren en un entorno seguro con el fin de adquirir un alto nivel de confianza por parte de los clientes actuales y futuros.

Este objetivo principal, se cumplirá con los siguientes objetivos planteados en el diseño del SGSI:

- Definir y optimizar criterios de seguridad que permitan mantener bajo control las vulnerabilidades de la organización.
- Garantizar la disponibilidad, confiabilidad e integridad de la información en la empresa Planeta, Proyectos y Obras SAS.
- Establecer criterios de seguridad sobre la información dependiendo de sus niveles de criticidad.
- Velar por la seguridad e integridad de los activos de la empresa.

5.3. Política del SGSI

La política del Sistema de Gestión de Seguridad de la Información en Planeta, Proyectos y Obras SAS tiene como finalidad ayudar al fortalecimiento y progreso de sus operaciones, se encuentra alineado con su misión, visión y busca que todos los individuos involucrados en el negocio de la compañía utilicen las herramientas necesarias para incrementar la seguridad de la información en la empresa.

La política del SGSI existe con el fin de incrementar las medidas de seguridad de la información durante todo su ciclo de vida, aprovechando al máximo todos los recursos que haya disponibles desde el humano hasta el tecnológico para asegurar la confidencialidad, disponibilidad e integridad de la información.

A estos efectos, Planeta, Proyectos y Obras SAS busca:

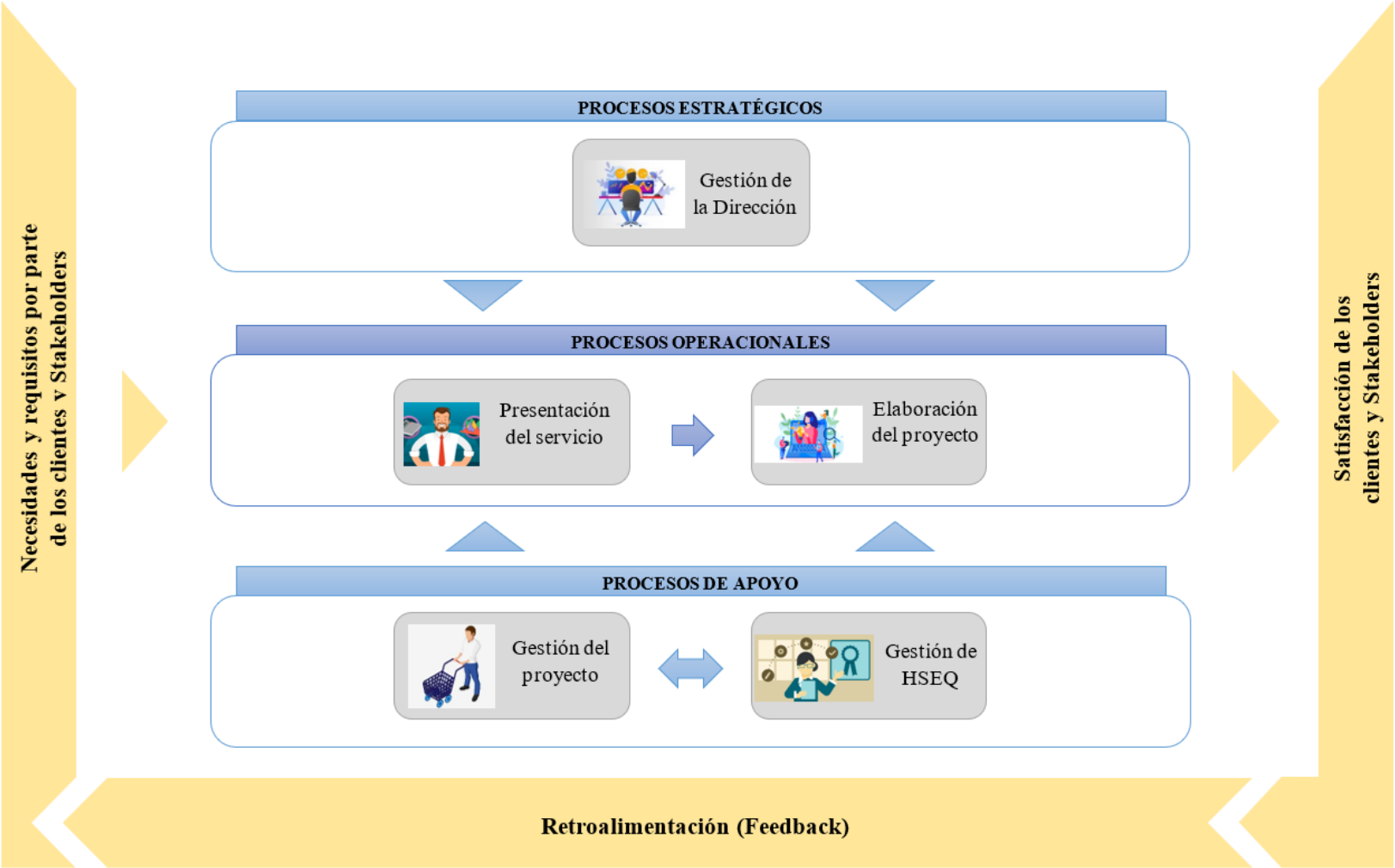
- Crear, mantener y fortalecer una cultura de seguridad de la información entre todos los miembros de la organización.
- Utilizar prácticas de seguridad acorde al nivel tecnológico y humano existente en la organización con el objetivo de mantener Disponibilidad, Integridad y Confidencialidad de la información de los empleados y clientes.
- Establecer anualmente objetivos referentes a las prácticas de Seguridad de la información dentro de la compañía.
- Identificar y cumplir con los requisitos de negocio, obligaciones contractuales y legales reglamentarias inherentes a la seguridad de la información.

5.4. Interfaces y dependencias (partes interesadas)

Finalmente, como parte de la definición del alcance descrita en los requisitos del estándar, se deben identificar las interfaces y dependencias entre actividades desempeñadas por la organización, y aquellas que se realizan por otras organizaciones.

Una forma de abordar la definición del alcance es a través del enfoque de procesos, por lo que la organización necesita identificar los procesos que soportan las actividades críticas (dependencias), así como los puntos por los cuales interactúan entradas y salidas de esos procesos (interfaces), en el anexo D podemos encontrar más detalles de estas partes interesadas.

Figura 4. *Mapa de procesos.*



Fuente: Autor.

5.5. Roles, responsabilidades y autoridades en la organización

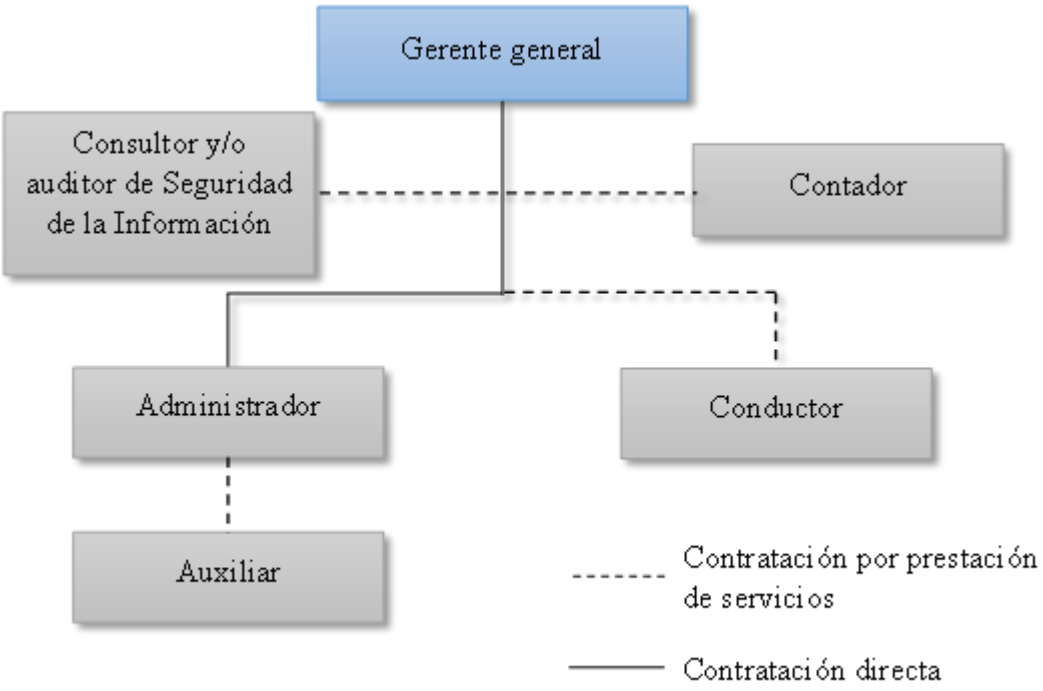
La alta dirección de Planeta, Proyectos y Obras SAS. mediante los perfiles de cargo asegura que las responsabilidades y autoridades para los roles desempeñados se asignan, comunican y se entienden en toda la organización. (Ver anexo F).

Por lo tanto, el Gerente General de la compañía tiene la responsabilidad y autoridad en el Sistema de Gestión de Seguridad de la Información, de modo que se asegura que:

- El Sistema de Gestión de Seguridad de la Información está conforme a los requisitos aplicables de la norma ISO 27001:2013.
- Los procesos están generando y proporcionando los resultados y salidas previstas.
- Se informa y conoce en la alta dirección el desempeño tanto del Sistema de Gestión de Seguridad de la Información como de las oportunidades de mejora.
- La integridad del Sistema de Gestión de Seguridad de la Información se mantiene cuando se planifican e implementan cambios en este.

De acuerdo a los procesos que se desarrollan en Planetas, Proyectos y Obras S.A.S. se realizó la Estructura Organizacional la cual se presenta a continuación:

Figura 5. *Mapa de organizacional.*



Fuente: Autor.

El nivel de responsabilidad y alcance de aplicación de los procedimientos y registros se detalló en los diagramas de flujo y en las caracterizaciones de cada proceso, que especifican punto a punto las operaciones y actividades que afecten la calidad con los responsables de su aplicación en Planetas, Proyectos y Obras S.A.S.

5.6. Planificación

5.6.1. Identificación de peligros, evaluación de riesgo y determinación de controles.

La identificación de peligros es un punto de partida para garantizar un adecuado control de los peligros y/o amenazas a los que los activos fijos pueden verse expuestos.

- Desastres naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

  - Fuego

- Daños por agua
- Desastres naturales

- De origen industrial: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada. Origen: Natural (accidental)

  - Fuego
  - Daños por agua
  - Desastres industriales
  - Contaminación electromagnética
  - Avería de origen físico o lógico
  - Corte de suministro eléctrico
  - Condiciones inadecuadas de temperatura o humedad
  - Fallo de servicios de comunicaciones
  - Interrupción de otros servicios y suministros esenciales
  - Degradación de los soportes de almacenamiento de la información
  - Emanaciones electromagnéticas

- Errores y fallos no intencionados: Fallos no intencionales causados por las personas. Origen: Humano (accidental.

  - Errores de los usuarios
  - Errores del administrador
  - Errores de monitorización
  - Errores de configuración
  - Difusión de SW dañino
  - Errores de [re]-encaminamiento
  - Errores de secuencia
  - Alteración accidental de la información
  - Destrucción de la información

- Fugas de información
- Vulnerabilidades de los programas (SW)
- Errores de mantenimiento / actualización de programas (SW)
- Errores de mantenimiento / actualización de equipos (HW)
- Caída del sistema por agotamiento de recursos
- Pérdida de equipos
- Indisponibilidad del personal

- Ataques intencionados: Fallos deliberados causados por las personas. Origen: Humano (deliberado)

  - Manipulación de los registros de actividad (log)
  - Manipulación de la configuración
  - Suplantación de la identidad del usuario
  - Abuso de privilegios de acceso
  - Uso no previsto
  - Difusión de software dañino
  - [Re-]encaminamiento de mensajes
  - Alteración de secuencia
  - Acceso no autorizado
  - Análisis de tráfico
  - Repudio
  - Interceptación de información (escucha)
  - Modificación deliberada de la información
  - Destrucción de información
  - Divulgación de información
  - Manipulación de programas
  - Manipulación de los equipos
  - Denegación de servicio
  - Robo

- Ataque destructivo
- Ocupación enemiga
- Indisponibilidad del personal
- Extorsión
- Ingeniería social (picaresca)

5.7. Políticas de seguridad

Las políticas de seguridad que se plantean a continuación para la empresa Planeta, Proyectos y Obras S.A.S, se basan en las falencias encontradas en el proceso de análisis de amenazas, vulnerabilidades y riesgos realizado previamente en este documento. Estas políticas administrarán la seguridad de la información en la entidad y las responsabilidades de todos los miembros de la organización.

5.7.1. Política de copias de respaldo de la información (Backup).

Garantizar que se realice periódicamente copias de seguridad de los activos de información de la empresa Planeta, Proyectos y Obras S.A.S, con el fin de dar cumplimiento al plan de continuidad del negocio.

- Las copias de seguridad generadas tienen que incluir valores acordes a las operaciones que existan actualmente dentro del sistema, independientemente de qué tipo de información manejen los datos.
- Las copias de seguridad (Backup) deben suministrarse al equipo de sistemas para que se realice una validación de la integridad de la información.
- Los métodos de generación de backups y los procedimientos de restauración en los sistemas, deben ser probados de manera periódica para revisar y valorar su eficiencia.
- Las copias de seguridad físicas deben estar almacenadas dentro de las instalaciones de la entidad o en el área designada por el Líder del Área de sistemas. Este espacio físico debe contar con protección ambiental y se debe

generar una lista del personal autorizado a retirar dichas copias almacenadas en el sitio interno o externo.

5.7.2. Política de Logs o registro de actividades.

Garantizar que se realice un registro completo de las actividades que se realizan dentro de los sistemas de la empresa Planeta, Proyectos y Obras S.A.S., con el fin de minimizar los riesgos de seguridad en el uso de estos sistemas y permitir la monitorización de incidentes de seguridad generados por cambios no autorizados.

- Todos los sistemas, aplicaciones y bases de datos que manejen información crítica de la empresa Planeta, Proyectos y Obras S.A.S. deben generar logs, en los que se muestre los registros de modificaciones, adiciones o eliminaciones de la información.
- Los Logs deben ser monitoreados periódicamente para la detección temprana de posibles errores de configuración, mal uso o vulnerabilidades en la seguridad de los mismos.
- Los logs de los procesos más importantes de la empresa deben proporcionar información suficiente para soportar auditorías y contribuir a la eficiencia y cumplimiento de medidas de seguridad.
- El proceso de depuración de Logs debe ser realizarse en un periodo de por lo menos un mes, con el fin de cumplir con los controles de auditoría.
- Todos los sistemas y equipos de la empresa Planeta, Proyectos y Obras S.A.S., deben tener el mismo horario y calendario, con el fin de garantizar la facilidad en actividades de rastreo mediante los logs de los sistemas y la integridad de la información almacenada.
- Se debe garantizar que solamente las personas autorizadas tengan acceso a los Logs, restringiendo el proceso de modificación y eliminación dentro de los mismos.

5.7.3. Política de gestión de cambios

Garantizar que se realice el proceso de gestión de cambios en los sistemas de información de la empresa Planeta, Proyectos y Obras S.A.S.

- Establecer un proceso de documentación de cambios en el que se registre la naturaleza del cambio, motivo y beneficios, tiempo estimado para la realización del cambio y el nombre del solicitante.
- El grupo de gestión de cambios deberá evaluar el impacto y realizar un análisis de los resultados del cambio con el fin de identificar las posibles vulnerabilidades en la seguridad que se generen como consecuencia del cambio.
- Se debe identificar a todas las partes interesadas en aprobar los cambios propuestos, con el fin de que sean notificados en tiempo y forma acerca de la modificación. El grupo de gestión de cambios estará a cargo del monitoreo, mantenimiento y seguimiento de las solicitudes relacionadas a las modificaciones.
- Para el proceso de implementación del cambio se debe garantizar la integridad por medio de pruebas de regresión, preparación operativa, etc. El responsable de realizar la modificación deberá desarrollar un plan de recuperación en caso de un cambio fallido.
- Los entornos de producción solamente pueden ser modificados con la aprobación previa de las directivas de Planeta, Proyectos y Obras S.A.S. y deben ser documentados correctamente.

5.7.4. Política de Gestión de Incidentes de Seguridad de la Información.

Establecer los lineamientos generales para la gestión de incidentes de seguridad de la información, con el fin de prevenir y limitar el impacto de los mismos.

- Adoptar medidas de seguridad eficientes para proteger los activos de información críticos.

- Disponer de los recursos necesarios con el fin de brindar una apropiada gestión de los incidentes de seguridad de la información, mediante la designación de un equipo responsable de la gestión de incidentes de seguridad de la información.
- Difundir la presente política a todo el personal de la entidad Planeta, Proyectos y Obras S.A.S., independiente del cargo que desempeñe o su tipo de contrato.
- Reportar los eventos de seguridad que detecte al equipo responsable de gestión de incidentes de seguridad de la información, siguiendo los procedimientos operativos establecidos.
- Analizar los eventos de seguridad informática para determinar si se trata de un incidente de seguridad de la información.
- Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática que afecte a los activos de información críticos la entidad Planeta, Proyectos y Obras S.A.S.
- Ejecutar procedimientos de repuesta a incidentes para mitigar el incidente.
- Documentar y clasificar los incidentes de acuerdo con las indicaciones la entidad Planeta, Proyectos y Obras S.A.S.
- Responder por la integridad de la información generada o en su poder.
- Reparar las consecuencias de los incidentes de seguridad de la información.
- Emprender actividades post-incidentes, como mejoras a los procesos operativos de gestión de incidentes de seguridad de la información o asegurar la retención de evidencias.

5.7.5. Política de responsabilidad del usuario.

El personal de Planeta, Proyectos y Obras S.A.S tiene responsabilidad acerca de la seguridad y deberá entender su participación y responsabilidades para minimizar los riesgos de seguridad, además de comunicar o reportar estos riesgos a los niveles directivos apropiados.

- Es responsabilidad del personal de Planeta, Proyectos y Obras S.A.S cuidar y mantener de manera adecuada la integridad y confidencialidad de la información de la empresa, protegiéndola contra la modificación o eliminación no autorizada,

y jamás, revelar de forma premeditada la información o procesos de Planeta, Proyectos y Obras S.A.S.

- Todos los usuarios de los sistemas de información de Planeta, Proyectos y Obras S.A.S., redes, aplicaciones e información allí contenida deberán salvaguardar y proteger adecuadamente la respectiva cuenta de usuario y la contraseña.
- Las estaciones de trabajo deberán solicitar la validación del usuario al inicio de la sesión y proteger la pantalla con bloqueo (por ejemplo, activará protectores de pantalla con contraseñas y se implementará la desconexión por expiración de la sesión), si el empleado debe dejar desatendido su puesto de forma temporal.
- Todo el personal de Planeta, Proyectos y Obras S.A.S. deberá participar del entrenamiento de seguridad brindado por la compañía.

5.7.6. Política – Creación, revisión y difusión de políticas de seguridad.

Las directivas de Planeta, Proyectos y Obras S.A.S. Son las responsables de las Políticas de Seguridad de Planeta, Proyectos y Obras S.A.S., y son ellos quienes promueven la creación, revisión y difusión de las mismas, con el fin de proporcionar continuamente una protección a la infraestructura de la información de Planeta, Proyectos y Obras S.A.S.

- Los diferentes departamentos funcionales de Planeta, Proyectos y Obras S.A.S son responsables del desarrollo e implementación de procedimientos detallados, así como por el monitoreo del cumplimiento de esas Políticas y Estándares.
- Los directivos de Planeta, Proyectos y Obras S.A.S. Son responsables por la ejecución de planes que faciliten el cumplimiento permanentemente.
- Los encargados de la seguridad o auditoría interna deberán ofrecer apoyo al negocio a través de la medición de cumplimiento. Una vez al año, será hecha la medición del cumplimiento y deben trabajar conjuntamente con la alta dirección del Negocio para asegurar que las solicitudes de excepción sean registradas apropiadamente, de acuerdo a las necesidades, para alcanzar el cumplimiento total, como se han definido las Excepciones a las Políticas y Estándares.

- Las alteraciones a las Políticas y Estándares de Control Clave deberán ser hechas de acuerdo a la necesidad. La Presidencia de Planeta, Proyectos y Obras S.A.S puede someter las solicitudes de alteración al Departamento de Seguridad. El nivel de prioridad de las solicitudes de alteración será Crítico o Normal, basado en su importancia para el negocio. La clasificación Crítica es usada para las alteraciones que necesitan ser atendidas de inmediato por su posibilidad de provocar un impacto significativo al negocio. Las demás serán consideradas como alteración Normal.
- El Comité de Seguridad deberá realizar la solicitud y votará, aprobando o rechazando la solicitud. Si la solicitud fuera rechazada, su promotor podrá apelar la decisión en el Comité Ejecutivo. Si el recurso fuera presentado, La dirección deberá revisar la solicitud y decidir con su voto la aprobación o rechazo de dicha solicitud.
- En caso de ser aprobadas, las modificaciones clasificadas como Críticas serán ejecutadas de inmediato a las Políticas y Estándares de Seguridad. Las demás modificaciones serán hechas en la próxima revisión anual de las Políticas y Estándares. El Departamento de Seguridad es responsable de asegurar que las principales modificaciones o inclusiones sean comunicadas al personal de Planeta, Proyectos y Obras S.A.S a la brevedad.
- Las Políticas deberán ser revisadas periódicamente para asegurar su coherencia y el tratamiento adecuado a los siguientes puntos:
    - ✓ Las necesidades de la compañía y el ambiente comercial
    - ✓ Ambiente tecnológico interno.
    - ✓ Exigencias legales y contractuales.
- Las Políticas y Estándares de Seguridad son aprobadas por La dirección de Planeta, Proyectos y Obras S.A.S.
- Las Políticas y Estándares serán revisadas por el Comité de Seguridad cuando se cumplan las siguientes condiciones:
    - ✓ Cada doce meses una revisión que contemple los cambios acumulados durante el año.

- ✓ Cuando sea identificado algún cambio en la tecnología, negocios, proceso y/o ambiente reglamentario que pudiera causar algún impacto a la postura de Planeta, Proyectos y Obras S.A.S ante el riesgo.
- ✓ Tras un grave incidente de seguridad.
- ✓ Luego de una revisión interna o externa que identifique alguna necesidad de modificación.

- Las Políticas y Estándares de Seguridad deberán ser comunicadas y estar permanentemente a disposición de todos los empleados de Planeta, Proyectos y Obras S.A.S.
- Sólo cuando exista la necesidad de que las Políticas y Estándares de Seguridad de Planeta, Proyectos y Obras S.A.S sean comunicadas a terceras partes, se hará con previa aprobación de las directivas. Esa aprobación sería concedida después de determinar que dicha divulgación no pondría a Planeta, Proyectos y Obras S.A.S.
- En una posición de desventaja comercial o que representa un riesgo.

5.8. Soporte

5.8.1. Recursos

La organización Planeta, Proyectos y Obras SAS. determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información de modo que se garantice su correcto desarrollo y desempeño; por lo cual la alta dirección es responsable de garantizar y presupuestar los recursos necesarios. Además, la compañía considera y se encuentra al pendiente de las capacidades y limitaciones de los recursos internos existentes y sobre aquellos aspectos o elementos que se necesitan obtener de proveedores externos.

- Personas
- Infraestructura
- Ambiente para la operación de procesos
- Recursos de seguimiento y medición
- Conocimientos de la organización

5.8.2. Competencia

La organización, cuenta con perfiles de cargo donde se estipulan las competencias necesarias tanto para la ejecución de las operaciones como para el desempeño y eficacia del Sistema de Gestión de Seguridad de la Información se puede dirigir al anexo F Matriz de perfiles de cargo. De igual forma, el proceso de gestión de la dirección mediante estos perfiles asegura que se cuente con el personal competente e idóneo de acuerdo a su educación, formación y/o experiencia.

5.8.3. Toma de conciencia

Con el objetivo que el personal que realiza labores dentro de la compañía tome conciencia sobre la organización, en el anexo D se encuentra el diseño gráfico que permitirá divulgar la política de seguridad, su alcance y objetivos de seguridad. Adicionalmente, mediante capacitaciones se reforzarán estos temas y se comunicará la importancia de los colaboradores sobre la contribución a la eficacia del Sistema de Gestión de Seguridad de la Información, los beneficios de una mejora del desempeño y las implicaciones del incumplimiento de los requisitos normativos y legales.

5.8.4. Comunicación

La organización ha determinado las comunicaciones internas y externas pertinentes al Sistema de Gestión de Seguridad de la Información, las cuales se encuentran definidas en el anexo J.

5.8.5. Información documentada

Con el fin de dar cumplimiento a este requisito, la organización posee la información documentada requerida por la ISO 27001:2013 y la de aquella que se considera necesaria para la eficacia del Sistema de Gestión de Seguridad de la Información teniendo en cuenta los numerales no aplicables para Planeta, Proyectos y Obras SAS, debido a las actividades que desarrolla; de esta manera la compañía cuenta con:

- Caracterizaciones
- Formatos
- Manuales
- Procedimientos
- Matrices

5.9. Operación

5.9.1. Planificación y control operacional

La organización, ha establecido los procesos necesarios para el Sistema de Gestión de Seguridad de la Información tal como se evidencia en el mapa de procesos, los objetivos y la política de seguridad, así como su divulgación.

5.9.2. Valoración de riesgos de la seguridad de la información

La organización ha establecido la valoración de los riesgos y sus criterios de aceptación según la siguiente tabla:

Tabla 12. *Categorización del impacto potencial.*

Impacto	Valor cualitativo
0 – 2	Muy baja
3 - 4	Baja
5 - 6	Media
7 - 8	Alta
9- 10	Muy alta

Fuente: Autor.

5.9.3. Tratamiento de riesgos de la seguridad de la información

En el Anexo K, se relacionan los controles de la norma ISO 27001 que permiten hacer el tratamiento de los riesgos de cada activo del proceso de gestión comercial.

5.10. Evaluación del desempeño

5.10.1. Seguimiento, medición, análisis y evaluación

La organización, hace seguimiento, medición, análisis y evaluación a cada uno de los procesos del Sistema de Gestión de la Seguridad de la Información, de manera que en las caracterizaciones se determinan los indicadores necesarios para evaluar cada proceso con el fin de que los resultados y análisis de los mismos contribuyan a desarrollar e implementar las estrategias de mejora continua.

Por ello, la compañía cuenta tanto con revisiones de la dirección y como realización de auditorías internas que permiten ejecutar la evaluación respectiva sobre el desempeño y eficacia del Sistema de Gestión de Seguridad de la Información teniendo en cuenta el cumplimiento de requisitos aplicables de la norma; además, la compañía conserva como información documentada los resultados obtenidos en estas verificaciones y las acciones tomadas según corresponda.

5.10.2. Auditoría interna

La organización llevará a cabo auditorías internas a intervalos planificados para determinar si el Sistema de Gestión de Seguridad de la Información cumple tanto con los requisitos propios de la compañía como con los requisitos de la norma ISO 27001:2013, además permitiendo evidenciar que este se ha implementado y mantiene su desempeño de forma eficaz.

5.10.3. Revisión de la alta dirección

La alta dirección será la encargada de revisar el Sistema de Gestión de Seguridad de la Información de forma periódica con el fin de garantizar su cumplimiento, conveniencia, adecuación, eficacia y alineación continua con la dirección estratégica de la organización, donde además se tiene en cuenta las oportunidades de mejora y los cambios que se requieran para mantener su correcto y adecuado desempeño.

5.11. Mejora

5.11.1. No conformidad y acciones correctivas

Cuando la organización detecta una no conformidad por parte de los clientes originada por una queja de los mismos, estas se registran y para aquellas provenientes por un incumplimiento de algún requisito de la norma, la empresa cuenta con el formato de acciones correctivas; estos registros se llevan con el fin de tomar las acciones pertinentes para su control y corrección haciendo frente a las consecuencias presentadas por ello.

Por lo tanto, mediante el formato de acciones correctivas se evalúa la necesidad de tomar acciones para eliminar las causas de las no conformidades garantizando la eliminación del origen del problema mediante la revisión y análisis, determinación de las causas e identificación de no conformidades similares o potenciales. (Ver anexo H – Control de no conformidades y acciones correctivas).

5.11.2. Plan de mejora

Para mejorar el Sistema de Gestión de la Seguridad de la Información se tomarán como fuentes:

- La medición a la planificación de los sistemas de gestión.
- Resultados de auditorías internas. ϖ Resultados de revisión por la gerencia.
- Acciones correctivas y preventivas. ϖ Medición de satisfacción del cliente.
- Cambios en el “Direccionamiento estratégico” trazados en el Sistema de Gestión de la Seguridad de la Información de Planeta, Proyectos y Obras S.A.S.

6. Conclusiones

A través del diagnóstico realizado para evidenciar la situación del Sistema de Gestión de la Seguridad de la Información de Planeta, Proyectos y Obras S.A.S. y realizar la implementación del mismo, se evidenció la falta de requerimientos por parte de la norma ISO 27001:2013, tampoco había una estructura clara de los procesos que integran la organización, con los documentos que se desarrollaron se lograron identificar los procesos y desarrollar la trazabilidad de la información que aporta cada uno.

Esta labor debe comenzar con el compromiso demostrable de la alta directiva hacia la seguridad de la información, labor que no es nada fácil cuando no se tiene concebida la seguridad de la información dentro de los objetivos estratégicos de la organización. El apoyo de la alta directiva, es indispensable para poder concebir un modelo de Seguridad de la Información que realmente apoye y apalanque la misión y visión de la organización, el cual es fundamental que se tenga antes de comenzar a diseñar un Sistema de Gestión de Seguridad de la Información, ya que si este no se logra conseguir, es casi seguro que cualquier iniciativa de seguridad que se pretender adelantar, no alcancen los resultados esperados y si por el contrario, genere el rechazo o el poco apoyo o interés por parte de la organización..

El nivel de cumplimiento de la entidad frente de los requerimientos del anexo A de la norma ISO/IEC 27001:2013, es del 15,2%, lo que significa que la implementación del Sistema de Gestión de Seguridad de la información le implicará a la entidad un esfuerzo considerable debido a la ausencia de controles o al bajo grado de cumplimiento de muchos de ellos.

La falta de controles orientados a proteger la información que se intercambia con terceros, puede generar consecuencias graves para la entidad y afectar de manera negativa su imagen ante sus partes interesadas, por tal razón, es urgente que la entidad implemente mecanismos de cifrado con el objetivo de garantizar la integridad, confidencialidad y autenticidad de esta información.

Se requiere implementar controles adecuados y efectivos y fortalecer los existentes, con el objetivo de asegurar que la seguridad de la información sea parte del ciclo de vida del

desarrollo de aplicaciones de la entidad y con ello garantizar que los cambios que se realizan en producción no afecten la operación ni la seguridad de la información de la entidad.

Es necesario implementar un mecanismo que control de acceso de los dispositivos de la red de la empresa, con el objetivo de garantizar que solo puede acceder los dispositivos que autorizados.

El desarrollo del sistema de gestión le permite a Planeta, Proyectos y Obras S.A.S. identificar sus fortalezas, debilidades y amenazas para lograr la medición de sus procesos y así potencializar sus procesos y expandir su cadena de clientes.

7. Referencias

Asociación Española para la Calidad (AEC). (2019). *SEGURIDAD DE LA INFORMACIÓN*. Obtenido de SEGURIDAD DE LA INFORMACIÓN: https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

Asociación Española para la Calidad (AEC). (2022). *Asociación Española para la Calidad*. Obtenido de Asociación Española para la Calidad: https://www.aec.es/

Cano, J. (2012). Seguridad de la información y privacidad: dos conceptos convergentes. *Sistemas*, 04-09.

DANE. (Marzo de 2020). *Departamento Administrativo Nacional de Estadística.* Obtenido de https://www.ccmpc.org.co/wp-content/uploads/2021/07/Clasificacion-DANE-CIIU_Rev_4_AC2020.pdf

Figueroa, J. (2018). *La seguridad informática y la seguridad de la información.* Obtenido de Polo del Conocimiento: https://dx.doi.org/10.23857/pc.v2i12.420

Gonzalez, J. (2016). Mision y Vision. *Acta de apertura*, (pág. 2). Bogota.

ISO. (2022). *International Organization for Standardization.* Obtenido de International Organization for Standardization.: https://www.iso.org/home.html

ISO 27001:2013. (2015). *International Organization for Standardization.* Obtenido de International Organization for Standardization: https://www.iso.org/standard/75652.html

López, A., & Ruiz, J. (2005). *iso27000*. Obtenido de iso27000: https://www.iso27000.es/sgsi.html

Pérez, A. (9 de Octubre de 2017). *OBS Business School*. Obtenido de OBS Business School: https://www.obsbusiness.school/blog/seguridad-de-la-informacion-un-conocimiento-imprescindible

Rocha, C., & Lcdo. (2011). La Seguridad Informatica. *Revista Ciencia Unemi*, 26-33.

Travieso, Y. (6 de Diciembre de 2003). *ACIMED.* Obtenido de scielo: http://scielo.sld.cu/scielo.php?pid=S1024-94352003000600012&script=sci_arttext&tlng=pt

Ugas, L. (2002). SEGURIDAD EN ORGANIZACIONES CON TECNOLOGÍAS DE. *Revista Electrónica de Estudios Telemáticos*, 02-10.

Universidad Nacional De Cordoba. (2008). *Universidad Nacional De Cordoba.* Obtenido de Universidad Nacional De Cordoba: https://www.unc.edu.ar/sites/default/files/PoliticadeSeguridad08.pdf

8. Anexos

Anexo A - Evaluación Inicial SGSI

Anexo B - Valoración de activos y riesgos del SGSI

Anexo C - Identificación de partes interesadas y requisitos pertinentes SGSI

Anexo D - Divulgación alcance, política, objetivos, interfases y dependencias

Anexo E - Mapa de Procesos

Anexo F - Matriz de Perfiles de Cargo

Anexo G - Manual de seguridad de la información

Anexo H - Control de no conformidades y acciones correctivas

Anexo I. Informe de Revisión Alta Dirección

Anexo J - Matriz de Comunicación Interna y Externa

Anexo K - Controles Anexo A para aplicar a los riesgos de los activos