FACULTAD DE ESTUDIOS EN AMBIENTES VIRTUALES

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN Y PROYECTOS TECNOLÓGICOS

TRABAJO DE GRADO

“MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN GEOCONSULT CS”

Ing. OMAR ANDRES FONSECA HERRERA
Autor

Ing. ALIX ERICA ROJAS HERNANDEZ
Directora de la tesis

BOGOTÁ D.C., MARZO DE 2019

¡¡A Dios por guiarme siempre por el camino!!
¡¡A mi esposa Ángela por ser una fuente maravillosa de inspiración para que yo dé lo mejor de mí!!
¡¡A mis padres, hermana y sobrino por el apoyo incondicional que me brindan para que yo cumpla mis sueños!!

TABLA DE CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

En una era de globalización, en donde la tecnología ha permitido impulsar el desarrollo de las empresas, alcanzar eficiencias operativas y lograr entrar a mercados y clientes que antes jamás se habían pensado, los datos y la información se convierten en uno de los activos más importantes en las organizaciones. Los cuales están expuestos a nuevos riesgos, amenazas y vulnerabilidades que pueden afectar la seguridad de estos activos.

El objetivo de este documento es presentar un modelo de un sistema de gestión de la seguridad de la información, alineado con la norma NTC-ISO-IEC 27001:2013, que aplique a cualquier organización, y que les permita conocer su estado actual con respecto a la seguridad de la información, y de una manera sistémica y eficaz implementar los controles, procedimientos y políticas necesarias para preservar la integridad, confidencialidad e integridad de los activos de información. Dicho modelo se aplica a una organización llamada Geoconsult CS, quien presta servicios de gestión y administración de información técnica en el sector de hidrocarburos.

Los resultados y los datos obtenidos de la aplicación del modelo en esta organización fueron muy exitosos, permitiendo a Geoconsult CS conocer y analizar el estado actual de la organización de acuerdo a los requisitos y objetivos de control y controles que tiene la norma, analizar su contexto organizacional, definir su estructura de seguridad, las políticas de seguridad de la información y los recursos necesarios para certificar su sistema de gestión. Adicionalmente, se identificó los activos de información, las vulnerabilidades técnicas y los riesgos aplicados a todos los procesos.

Palabras Claves: modelo, seguridad, información, activos, riesgos

1 INTRODUCCIÓN

Los datos, la información y los sistemas de información son indispensables en las organizaciones para cumplir los objetivos estratégicos, alcanzar eficiencias operativas, lograr una ventaja competitiva y obtener un valor diferenciador con respecto a la competencia. La información representa un invaluable activo para las empresas del gremio del petróleo y los hidrocarburos, pero su verdadero valor solo se ve reflejado cuando estos son incorporados en los procesos y en la toma efectiva de decisiones del negocio. Lau (2017), especialista en soluciones y licencias de Microsoft del grupo SEGA, especifica como la información se ha convertido en el segundo activo más importante de las organizaciones después de las personas.

En la actualidad son más frecuentes los riesgos y amenazas que pueden afectar la seguridad de la información, afectando la confidencialidad, disponibilidad e integridad de los activos de las compañías, perturbando tanto a las grandes como a las pequeñas empresas. Los hackers, los virus informáticos, el espionaje cibernético y las fallas en la infraestructura, son solo una muestra de todas las amenazas que sufre tener un mundo cada vez más comunicado, y que pueden conllevar a consecuencias como robo o fuga de información confidencial, interrupción de servicios, fallas en los sistemas y afectaciones económicas. Los daños económicos del crimen cibernético según Inter Security en el 2017, asciende aproximadamente a USD 600 millones anuales, lo cual corresponden al 15 por ciento de los actos ilícitos cometidos a empresas en Colombia. Según Lugo (2016), directora regional de ventas de Intel Security, uno de los puntos débiles de las compañías, es el bajo presupuesto que destinan a la seguridad informática, lo cual no abarca las necesidades actuales de las organizaciones.

Debido a los riesgos que presenta la información, es indispensable para las organizaciones de Colombia contar con una estrategia que le permita de una manera sistémica y eficiente salvaguardar adecuadamente sus activos. Esta estrategia corresponde al diseño e implementación de un sistema de gestión de seguridad de la información, basado en normas internacionales que aseguren las mejores y más actuales

prácticas. Uno de los estándares más reconocidos a nivel mundial es la NTC-ISO-IEC 27001 en su versión 2013, la cual establece los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información.

El presente trabajo tiene como finalidad diseñar un modelo de un sistema de gestión de seguridad de la información que cubra todos los procesos actuales de la organización Geoconsult CS, y a corto plazo, sirva como inicio para su implementación y posterior certificación en la norma ISO27001.

El contenido del trabajo se desarrolla en cinco secciones o capítulos:

1. Introducción, en la primera parte del documento se especifica la identificación del problema detectado en la organización, se definen los objetivos, la justificación del trabajo, el alcance donde se delimita el ámbito para el cual tiene validez los resultados aportados y la metodología utilizada.
2. Marco Teórico, en la segunda sección se presenta los conocimientos y conceptos necesarios para el desarrollo del modelo y finalmente la descripción de la empresa a la que va dirigida el presente trabajo dirigido.
3. Modelo, en la tercera sección de presenta el modelo propuesto de un Sistema de Gestión de Seguridad de la Información desarrollado en 3 fases para su implementación, (diagnóstico, preparación y planificación).
4. Modelo Aplicado, en esta sección se desarrolla el modelo propuesto en capitulo anterior en la organización Geoconsult CS.
5. Conclusiones y Recomendaciones, finalmente se hace una síntesis de las recomendaciones realizadas a la organización, las conclusiones del trabajo y las líneas de investigación o mejoras que puede tener el modelo.

1.1 Formulación del problema

En la actualidad las empresas colombianas se enfrentan a nuevos riesgos que afectan la seguridad de los activos de información, causados por los cambios tecnológicos, culturales y organizacionales. Estos cambios han producido nuevas amenazas como virus informáticos, códigos maliciosos, delincuencia cibernética, ataques de fuerza bruta, denegación de servicios y suplantación de identidad, que acompañados de amenazas tradicionales como desastres naturales, fuga de información por parte de empleados descontentos y robo por delincuencia común, constituyen un aspecto muy importante a considerar por parte de las directivas de las compañías. Lastimosamente los gerentes no definen los suficientes recursos a proteger sus activos de información; según reporta PC World, en promedio las empresas asignan solo el 5% del presupuesto de IT a la seguridad (Gartner, 2016), y muy pocas empresas en Colombia cuentan con el certificado de su SGSI en la norma ISO27001, lo cual se demuestra en los solos 221 certificados que al final del 2017 tenía Colombia, los cuales no se compararan con los 8945 que tiene Japón. (ISOTools, 2017)

Geoconsult CS, una empresa colombiana especializada en el manejo y tratamiento de información técnica del sector de petróleos e hidrocarburos, carece de un sistema de gestión de seguridad de la información, que le permita preservar la confidencialidad, integridad y disponibilidad de la información, tanto en sus procesos administrativos como operativos. Esta carencia le ha impedido trabajar con algunas entidades públicas y privadas, que se han vuelto cada vez más exigentes en cuanto a los controles y políticas de seguridad de la información que ofrecen las compañías contratistas en la operación del servicio. Asimismo, al no tener un modelo implementado de un SGSI[1] se expone a riesgos latentes que pueden impactar negativamente la operación de su servicio.

Geoconsult CS, no cuenta con copias de respaldo de información (*backups*) en sitios alternos, no ha realizado una identificación y clasificación de activos, en algunos equipos conectados a la red interna de la empresa se ha detectado software sin licenciar y

[1] SGSI (Sistema de Gestión de Seguridad de la Información)

códigos maliciosos, existe información personal en los equipos de la organización e incumplimiento de las pocas políticas de seguridad que tiene la compañía. Todos estos hallazgos a un corto o mediano plazo, pueden incurrir en incumplimientos con los clientes, inconvenientes legales y fallas en la operación que pueden desencadenar en incidentes de seguridad graves que afecten directa o indirectamente la estabilidad, la operación y la imagen de la empresa.

Uno de los clientes de Geoconsult CS, la Agencia Nacional de Hidrocarburos (ANH) sufrió uno de los casos más renombrados en Colombia en relación a pérdida de información, como fue la desaparición de dos discos secretos de la petrolera Repsol en Junio de 2015, donde información confidencial, fue extraída de la ANH, la cual estaba grabada en dos discos duros con contenido de datos técnicos de un contrato suscrito por la ANH con la compañía española Repsol, quien aportó 17 millones de dólares para realizar estudios sísmicos en el pacífico. (El tiempo, 2017). Lo anterior demuestra el valor económico y estratégico de la información que administra y resguarda Geoconsult CS, y la necesidad de manera inmediata de un Sistema de Gestión de la Seguridad de la Información que le permita brindar a sus clientes la seguridad de que sus datos están debidamente protegidos.

Según cifras de la DIJÍN, el cibercrimen y los delitos informáticos aumentaron un 28% en Colombia durante el 2017 y causaron pérdidas superiores a los 50.000 millones de pesos. En las empresas privadas una modalidad que va en aumento es la suplantación de los correos corporativos, registrando pérdidas por 380 millones de pesos durante el 2017. Los cuales se pudieron haber evitado de contar con un sistema de gestión de seguridad de la información. (Revista Semana, 2017)

1.1.1 Pregunta general

¿Cuáles son los elementos de seguridad de la información necesarios en el modelo de un SGSI que abarque todos los procesos y áreas de la organización Geoconsult CS de acuerdo a la norma NTC-ISO-IEC 27001:2013?

1.1.2 Preguntas específicas

¿Cuál es el estado actual de los procesos de Geoconsult CS con respecto a la seguridad de la información?

¿Existen políticas de Seguridad de la Información implementados en los sistemas de información de la organización Geoconsult CS?

¿Cuáles son los activos más importantes de Geoconsult CS?

¿Existe una identificación, análisis y evaluación de los riesgos asociados a la seguridad de la información de los activos de Geoconsult CS?

¿El acceso a la información y las instalaciones de procesamiento está debidamente limitado y controlado?

¿La empresa cuenta con controles criptográficos apropiados para proteger la información de Geoconsult CS?

¿Existen copias de respaldo de la información, software y sistemas de la empresa?

1.2 Objetivos

1.2.1 Objetivo general

Diseñar un modelo de un sistema de gestión de la seguridad de la información, que aplique a todos los procesos y áreas de la organización Geoconsult CS, alineado con la norma NTC[2]-ISO[3]-IEC[4] 27001:2013

1.2.2 Objetivos específicos

- Diagnosticar el estado actual de cumplimiento de Geoconsult CS con respecto a los dominios y objetivos de control de la norma NTC-ISO-IEC 27001:2013.

- Definir un conjunto de políticas y procedimientos para la seguridad de la información aplicadas a todos los procesos actuales de la organización de acuerdo a la norma NTC-ISO-IEC 27001:2013.

- Definir los elementos del modelo del sistema de gestión de la seguridad información de Geoconsult CS en todos los procesos de la organización alineado con la norma NTC-ISO-IEC 27001:2013.

- Validar el modelo propuesto de un sistema de gestión de la seguridad de la información en la organización Geoconsult CS.

- Realizar las recomendaciones necesarias con relación a la implementación del modelo de gestión de la seguridad de la información en la organización de acuerdo a las condiciones establecidas en la norma NTC-ISO-IEC 27001:2013.

[2] NTC (Norma Técnica Colombiana)
[3] ISO (Organización Internacional de Normalización)
[4] IEC (Comisión Electrotécnica Internacional)

1.3 Justificación

En una era de globalización y conocimiento, en donde la tecnología es el motor de las empresas y los datos son el nuevo petróleo en la sociedad, la información se convierte en uno de los activos más importantes en las organizaciones. El valor estratégico es inmenso, nos ayuda a tomar las mejores decisiones, brinda un alto nivel de competitividad, apoya los procesos de la compañía y en muchas ocasiones puede ser el producto final de una empresa. Sin embargo, la información está sujeta a diferentes amenazas y riesgos, tanto de tipo natural como humano, lo cual hace fundamental contar con actividades y procesos dentro de un marco de un sistema de gestión que permita preservar la confidencialidad, integridad y disponibilidad de la información.

Como lo indica ICONTEC[5] (2013), la adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El diseño de un modelo un SGSI es un elemento clave en las estrategias generales de las organizaciones del sector de la tecnología, ya que le permite lograr un mejor nivel de seguridad, estar preparados ante las nuevas y futuras amenazas que puedan afectar los activos de información, y obtener un valor agregado en la operación de sus servicios. Debido a que el SGSI cubre todos los procesos de la organización, todas las áreas van a ser beneficiadas; en el área financiera, la empresa reducirá costos vinculados a la pérdida de los activos, además de disminuir las primas de los seguros con los clientes, según la firma Ponemon Institute, los costos en promedio por pérdida de algún activo de información pueden ser superiores a los 63 millones de pesos (Instituto Ponemon, 2016); en el área de gestión humana se mejoraría el proceso de selección a partir de estudios de seguridad, capacitación y sensibilización al personal; en el área comercial, se generaría mayor credibilidad, mejoraría la imagen de la empresa y le permitirá participar en licitaciones más exigentes.

Alineados a los objetivos estratégicos de la compañía de mantener la optimización de los procesos y ofrecer a sus clientes servicios que cuenten con los mejores estándares a nivel mundial, diseñar un modelo de un Sistema de Gestión de Seguridad de la

[5] ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación)

Información que se encuentre acorde a los requerimientos de la norma ISO27001:2013 y funcione como un medio eficaz que permita preservar la confidencialidad, la integridad y la disponibilidad de la información administrada por la organización, permitirá brindar la confianza requerida a sus clientes en el tratamiento de sus datos e información.

La pertinencia del estudio del diseño de un modelo de un Sistema de Gestión de Seguridad de la información en la organización Geoconsult CS, con en el programa de maestría de Gerencia de Sistemas de información y proyectos tecnológicos, es directo. En el desarrollo del modelo se abordará un estudio, análisis y comprensión de todos los sistemas de información de la organización, incluyendo los riesgos de seguridad de la información asociados a estos. Asimismo, en el desarrollo del modelo del SGSI se emplearán todos los conocimientos adquiridos en las modelos gerenciales para el aseguramiento de la información, factores de éxito en la gerencia de proyectos tecnológicos, arquitectura de los sistemas de información, entre otros.

Diseñar un modelo de gestión de seguridad de la información en Geoconsult CS, tiene las condiciones operativas necesarias para realizar una correcta investigación en la empresa, debido a que se cuenta con el acceso a la información, el apoyo y los permisos por parte del área directiva; incluso la organización manifiesta un gran interés en el proyecto ya que puede ser a corto plazo una ventaja competitiva para la compañía. Además, permitirá identificar y clasificar los activos más importantes de información, evidenciar los riesgos de SI, proporcionará datos y procedimientos que se tendrán como base para implementar el sistema y lograr la certificación bajo la norma ISO27001. Implícitamente la solución del problema traerá beneficios en el ámbito de competitividad de la empresa, que se entienden desde la percepción del cliente en cuanto al valor agregado que la compañía adquiere al tener un SGSI, y el obtener por parte de la compañía un 3% más de probabilidad de éxito en las licitaciones, debido al puntaje que otorgan clientes como Ecopetrol por tener el certificado de la norma ISO27001:2013.

1.3.1 Contribuciones esperadas

Un modelo de un Sistema de Gestión de Seguridad de la Información es un elemento muy importante en el plan estratégico de la organización, debido a que le permite obtener un valor agregado en la operación de sus servicios, y sirve como sustento en la obtención de los objetivos de Geoconsult CS. A continuación, se presenta las contribuciones esperadas.

Incrementa la buena imagen que tiene la empresa. Un SGSI ofrecerá a los clientes de Geoconsult, servicios que cuenten con los mejores estándares a nivel mundial en sus procesos operativos de manejo de información técnica en el sector petrolero, garantizando la debida protección y administración de los activos que los clientes ponen a su disposición.

Disminuir costos. Un correcto diseño de un modelo de un Sistema de Gestión de Seguridad de la Información impacta positivamente el área de finanzas de la empresa, reducirán costos vinculados a la pérdida de los activos y las inversiones innecesarias en seguridad y tecnología, además de reducir o eliminar el pago de los seguros con los clientes a causa de eventos o incidentes de seguridad de la información. Según la firma Ponemon Institute el ahorro que pueden tener las empresas que contratan soluciones digitales enfocadas en seguridad puede ir hasta los $1.9 millones de dólares al año (Instituto Ponemon, 2016).

Mejoras en los procesos. Debido a que el Sistema de Gestión de Seguridad de la Información cobija todos los procesos de Geoconsult CS, se beneficiarían todas las áreas de la organización; en el área de Gestión Humana se optimizaría el proceso de selección a partir de mejorar los procesos de reclutamiento y capacitación; en el área de TI se estandarizarían y corregirían procedimientos claves como la gestión de activos, copias de respaldo, entre otras; en el área comercial se ampliaría la calificación de la compañía en los procesos licitatorios.

1.4 Alcance y limitaciones

1.4.1 Alcance

El presente trabajo de grado comprende la etapa de diseño y generación de un modelo de un Sistema de Gestión de Seguridad de la Información. El modelo aplica los procesos de tecnología de la información, dirección, administración, comercial y de proyectos de la empresa Geoconsult CS, con sede en Bogotá Colombia.

El modelo del SGSI se basará en el análisis de la norma NTC-ISO-IEC 27001 en su versión 2013.

1.4.2 Limitaciones

El presente trabajo de grado no incluye las fases de implementación, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información, únicamente aplica a la etapa de diagnóstico, diseño y generación del modelo del SGSI.

El modelo no aplica a las áreas y procesos que tiene la organización Geoconsult CS en las sedes de Ecuador y Perú.

En el diseño y generación del modelo Sistema de Gestión de Seguridad de la Información de Geoconsult CS se debe excluir los siguientes controles del anexo A de la norma NTC-ISO-IEC 27001, debido a que en ningún proceso de la empresa se realiza desarrollo de aplicaciones o software, ni se realiza labores de teletrabajo.

- A.6.2.2 Teletrabajo
- A14.2.1 Política de desarrollo seguro
- A14.2.6 Ambiente de desarrollo seguro
- A14.2.7 Desarrollo contratado externamente

1.5 Metodología

1.5.1 Diseño general

La metodología formulada busca cumplir los objetivos específicos definidos, con el fin de lograr el objetivo general del trabajo de grado, teniendo en cuenta el marco de referencia de la norma NTC-ISO-IEC 27001:2013, incluyendo la totalidad de los 10 numerales y el anexo A, que especifica los requerimientos, objetivos de control y actividades que se deben desarrollar para el diseño del SGSI.

Es importante considerar en el diseño metodológico que el orden en que se presentan los requisitos del anexo A de la norma, no refleja su importancia ni el orden en el que se deben implementar.

1.5.2 Enfoque

El enfoque utilizado de investigación para el diseño de un modelo de un Sistema de Gestión de Seguridad de la Información en la organización Geoconsult CS, es cualitativo tomando como referencia que esta investigación se enfoca en comprender los fenómenos explorándolos desde la perspectiva de los participantes en su ambiente normal y en relación con su contexto. Teniendo en cuenta lo recomendado por Marshall (2011), se utiliza el enfoque cualitativo, debido a que el tema de estudio ha sido poco explorado en la organización (Batista, Hernández y Fernández, 2010).

1.5.3 Tipo de investigación

El desarrollo de este trabajo de investigación se realiza como aplicativo y descriptivo, ya que se plantea una solución al problema, debido a que se identifican los hallazgos y las situaciones del objeto de estudio, desarrollando un modelo, pero sin dar las causas que originaron los hechos. Van Dalen y William J. Meyer (1986) especifican como el objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, y actitudes

predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas. Para varios autores, la investigación descriptiva se convierte en la base de otros tipos de investigación, debido a que de alguna manera tienen aspectos de carácter descriptivo.

1.5.4 Tipo de estudio y Población

La metodología de estudio utilizada es descriptiva, teniendo en cuenta que se recolectaron datos que describen la situación real de la organización y pueden ser medidos. De igual forma, es transversal debido a que se recolectan los datos en un solo momento, realizando un panorama real de un momento específico (Hernández Sampiere, 2010). Debido a que la organización está considerada como una pequeña empresa, la población que se aborda en este modelo cubre la totalidad de los empleados de la organización Geoconsult CS, los cuales representan aproximadamente 30 personas, incluyendo el personal del área administrativa y del área operativa.

1.5.5 Instrumentos de recolección de Información

Para el diseño del modelo de un Sistema de Gestión de Seguridad de la Información en la organización Geoconsult CS se utilizan los siguientes recursos para la recolección de los datos:

- Entrevistas
- Cuestionarios
- Revisión de la documentación existente
- Levantamiento de procesos
- Observación

1.6 Glosario

Acción Correctiva: Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable para evitar que vuelva a ocurrir.

Acción Preventiva: Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencialmente indeseable, para evitar que ocurra.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Corrección: Acción emprendida para eliminar una “no conformidad”.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Eficiencia: Capacidad de disponer de alguien o de algo para conseguir un efecto determinado.

Eficacia: Capacidad de lograr el efecto que se desea o se espera.

Evento de Seguridad de la Información: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias o una situación anterior desconocida que podría ser relevante para la seguridad.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Incidente de Seguridad de la Información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Riesgo Residual: Nivel restante de riesgo después del tratamiento de riesgo.

No conformidad: Incumplimiento de un requisito. Puede ser no conformidad de los servicios, de los procesos o del Sistema de Gestión de Seguridad de la Información.

Mejora Continua: Actividad recurrente para aumentar la capacidad para cumplir con los requisitos.

SGI: Sistema de Gestión Integrado.

SGSI: Sistema de Gestión de Seguridad de la Información, parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar operar hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

SI: Seguridad de la Información, preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo

2 MARCO TEÓRICO

El siguiente marco teórico se desarrolla en 3 partes significativas, iniciando de lo general a lo específico. La primera parte describe el tema de Seguridad de la Información y las diferentes alternativas de los modelos de un Sistema de Gestión de Seguridad de la información, la segunda se enfoca directamente sobre el estándar internacional NTC-ISO-IEC 27001 en su más reciente versión, y en la última parte se describe la organización donde se aplica el diseño del modelo.

2.1 Seguridad de la Información

Cada vez se tiende a depender más de los sistemas, para administrar los datos, convirtiendo a la información en uno de los activos más importantes para las empresas, en donde perderla representa graves afectaciones económicas, competitivas y legales. La información, los datos, la infraestructura tecnológica, las personas y los sistemas de información son activos muy importantes para cualquier compañía. Diseñar estrategias para proteger la información es fundamental para resguardar secretos comerciales u operativos, y mantener los niveles de competitividad. La información se maneja en forma impresa y digital, la primera está tendiendo a desaparecer, aunque aún muchas empresas gestionan y administran su información análoga en carpetas y archivadores. La información digital se encuentra en su mayoría en ordenadores, discos duros, servidores, y dispositivos móviles que pueden dañarse, pueden ser robados, deteriorarse, o simplemente por obsolescencia de la tecnología usada, se generan brechas importantes para consultar la información (Mirk, 2015).

En una era de tecnología y un mundo globalizado, las organizaciones dependen cada día más de los sistemas de información, donde el uso de la tecnología en desarrollar, preservar y transferir activos, como datos, información y conocimiento son claves para el logro de los objetivos estratégicos. Pero del mismo modo, depender en gran medida de los sistemas de información y la tecnología, nos lleva a considerar unos riesgos y amenazas que vienen asociados con el uso y evolución de los datos. Entre ellas se

encuentran los virus informáticos, delincuentes cibernéticos, ataques de negación de servicios, caída en las redes, software malicioso y eventos naturales, como incendios, terremotos e inundaciones (Costas, 2011). Debido a lo anterior las organizaciones deben crear y asegurar un ambiente que permita proteger los tres principios fundamentales de la seguridad de la información: confidencialidad, disponibilidad e integridad. Los cuales se presentan con más detalle en la siguiente tabla.

Tabla 1. Principios Fundaméntales de la Seguridad de la Información

Principio	Descripción
Confidencialidad	Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, conservando las restricciones adecuadas en el acceso y divulgación de esta.
Integridad	Propiedad de salvaguardar la exactitud y estado completo de los activos. Únicamente puede ser modificada por las personas autorizadas. Salvaguardando el acceso contra la indebida alteración o eliminación de la información.
Disponibilidad	La información debe estar en el momento y en el formato que se requiera, al igual que los recursos necesarios para su uso, asegurando el funcionamiento y usabilidad del servicio cuando sea solicitado por las personas autorizadas.

Fuente. Elaboración propia adaptado de (ICONTEC, 2013)

2.1.1 Amenazas y riesgos a la seguridad de la información

La tecnología está en inquebrantable cambio y crecimiento, todos los días se desarrolla o se mejora una nueva aplicación, software, base de datos, etc. Pero así mismo se descubren nuevas vulnerabilidades, los delincuentes buscan nuevas formas de ataque, por lo cual es muy importante conocer los tipos de amenaza y detectar los diferentes riesgos a los que se expone la información. Las amenazas en un sistema de información, pueden derivar de diferentes fuentes externas e internas. Externas, como un delincuente cibernético que entra al sistema a través de explotar una vulnerabilidad en la red local de

la empresa, e interna como el personal de la organización, que conoce las debilidades de la compañía y se aprovecha para acceder a información privilegiada a la cual no debe tener acceso (Gómez, 2011). A continuación, se presentan las principales amenazas:

Figura 1. Principales amenazas a la seguridad de la información

Fuente. (SENA, 2015)

Virus: Los Virus Informáticos son programas maliciosos que "infectan" a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior de un archivo (normalmente un ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y, por tanto, una nueva fuente de infección (Gómez, 2007).

Ingeniería social: Es la práctica o forma de obtener información confidencial a través de la manipulación de las personas, donde los atacantes por medio del engaño intentan obtener documentación privada, claves de correo electrónico o privilegios en algún sistema (Gómez, 2007).

***Phishing*:** es uno de los ataques de ingeniería social más conocidos y exitosos, consiste en la suplantación de identidad o simulación de un sistema autentico, para posteriormente obtener información como claves bancarias y de correo, control de su equipo y/o archivos confidenciales (Benavides, 2012).

***Ransomwares*:** Es un código malicioso que cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este disponga. Este es el más

popular en la actualidad y fue el ataque informático registrado recientemente en casi 80 países alrededor del mundo (Surhone, 2011).

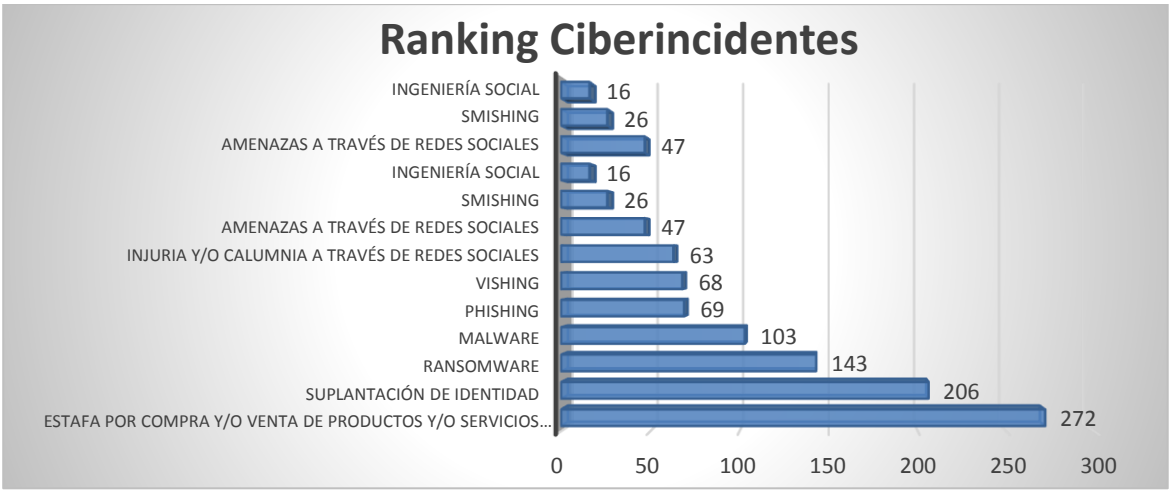
***Spyware*:** También conocido como software espía es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento (Benavides, 2012).

***Hacker*:** Término para describir un experto en programación, es utilizado con frecuencia con un sentido negativo, para describir a una persona, que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa, aunque no siempre tiene que ser esa su finalidad (Gómez, 2007).

Ataque de denegación de servicio: También llamado DOS, *Deny of Service*, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, provocando la pérdida de la conectividad de las redes por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima (Benavides, 2012).

En la siguiente figura se presentan los datos estadísticos de los ataques informáticos denunciados a la Policía Nacional de Colombia durante año 2017.

Figura 2. Estadística Ciber incidentes en Colombia en el año 2017



Fuente. Propia basado en (Ministerio de Defensa Nacional Policial de Colombia, 2017)

2.1.2 Sistema de Gestión de Seguridad de la Información

Un Sistema de Gestión de Seguridad de la Información, en su abreviación en español SGSI, es una herramienta de la que dispone la gerencia para dirigir y controlar la seguridad de la información. Está conformado por un proceso sistemático, documentado y conocido por toda la organización, en el cual se desarrollan estrategias y políticas con el fin de preservar y asegurar la confidencialidad, disponibilidad e integridad de los activos información, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con la implementación de un SGSI, la organización identifica los riesgos a los que está sometido sus activos de información y los asume, mitigando, transfiriendo o controlándolos. Brindando confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente. Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de gestión total de la información de la organización y que esté integrado con ellos, teniendo en cuenta que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles (ICONTEC, 2013).

Un Sistema de Gestión de Seguridad de la Información le permite a cualquier organización la implementación de un gobierno de seguridad, basado en una estructura organizacional, donde se definen roles y responsabilidades, políticas, procedimientos, procesos y recursos, para gestionar de manera adecuada los activos de información. Un SGSI proporciona una herramienta eficaz que le permite a las organizaciones establecer políticas, procedimientos y controles de seguridad de la información alineados a los objetivos estratégicos de la compañía. Asimismo, la implementación de un SGSI brinda a la empresa un proceso de mejora continua, que le permite reaccionar ante cualquier amenaza, tomando las acciones correctivas y preventivas para controlar cualquier incidente que afecte la seguridad de la información (Areitio, 2008).

2.1.3 Modelos de un Sistema de Gestión de Seguridad de la Información

Los esfuerzos realizados por las compañías con el fin de enfrentar los riesgos que conlleva la pérdida de la confidencialidad, integridad o disponibilidad de los activos de información, han llevado a que los gerentes de las organizaciones inviertan mayores recursos para reducir en el nivel de su exposición al riesgo. Estas inversiones se convierten en proyectos que van desde la adquisición de un software, que compone un control de seguridad específico para la información, hasta proyectos para definir e implementar modelos de seguridad que permitan hacer una gestión continua de una estrategia de SI[6], que debe implementarse y constantemente mejorarse (Kim & Salomon, 2012).

Un modelo de un sistema de gestión de la seguridad de la información, SGSI, ayuda a identificar las vulnerabilidades, riesgos existentes y futuros, ayuda a establecer políticas, elementos y procedimientos de seguridad con el objetivo de tener el menor impacto posible en la eventualidad de que se materialice un riesgo (Kim & Salomon, 2012). Un modelo de un sistema de gestión de seguridad de la información puede estar alineado con las mejores prácticas ya sea de uno o más referentes, como ISO27001, COBIT, ITIL, entre otros. A continuación, se realiza una breve reseña de estos.

La norma ISO27001 suministra los requisitos para el diseño, establecimiento, implementación mantenimiento y mejora de un sistema de gestión de la seguridad de la información, pertenece al conjunto de estándares que compone la norma ISO27000 y su última versión es la 2013. (ICONTEC, 2013).

COBIT (*Control Objectives for Information Systems and related Technology*) es un modelo para auditar la gestión y control de sistemas de información y tecnología, fue lanzando en 1996 y está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos agrupados de forma natural para proveer la información pertinente y confiable que requiera una compañía para lograr sus metas. (Universidad EAFIT, 2007)

---

[6] SI: Seguridad de la Información

ITIL (*Information Technology Infraestructure Library*) proporciona un planteamiento sistemático para la provisión de servicios de TI con calidad. Fue desarrollado en las décadas de los 80 y 90, y desde entonces se ha conformado como un marco basado en las mejores prácticas, su actual versión es la 2011 (Baud, 2015).

A continuación, se presenta una tabla de comparación de estos tres modelos:

Tabla 2. Comparación de ITIL, COBIT e ISO27001

CRITERIO	ITIL	COBIT	ISO27001
Creador	OGC	ISACA	ISO
Objetivo	Gestión de niveles de servicios	Auditorias de sistemas de información	Definir un sistema de gestión de seguridad de la información
¿Es certificable?	NO	NO	SI
Ventajas	• Los servicios se detallan en lenguaje de cliente • se enfoca más a los procesos de negocios.	• Ayuda a aumentar el valor del área de TI • Proporciona roles y responsabilidades	• Adaptación a la legislación vigente • Aplica para cualquier tipo de organización • Incluye activos de información como el conocimiento del personal y la información impresa
Desventajas	Falta de comprensión o conocimientos sobre la adopción de ITIL	Es muy ambicioso y difícil de implementar	Exceso de documentación

Fuente. Elaboración propia basado en (Baud, 2015)

Como lo Indica Cano (2011), asegurar una efectiva estrategia de seguridad de la información, no es sólo cuestión de elegir un modelo como guía, o instalar y mantener artefactos tecnológicos especializados y costosos, sino comprender de manera sistémica las relaciones propias entre la estrategia corporativa, los procesos y los individuos. Para así considerar los cambios dinámicos y la constante exigencia de la alta gerencia de tener la información disponible para la toma de decisiones

2.2 ISO-IEC 27001 técnicas de seguridad/requisitos de un SGSI

La norma internacional ISO-IEC 27001, es la norma principal de la serie ISO27000 y contiene los requisitos de un sistema de gestión de seguridad de la información. Ha sido presentada como un modelo para el diseño, establecimiento, implementación, operación, seguimiento, control, mantenimiento y mejora continua de un SGSI información en cualquier tipo de organización. En su anexo A, se enumera en forma de resumen los objetivos de control y controles, para que sean seleccionados por las empresas en el desarrollo de su sistema (ICONTEC, 2013).

2.2.1 Series ISO 27000 estándares de seguridad de la información

ISO ha reservado la serie de numeración 27000 para las normas relacionadas con sistemas de gestión de seguridad de la información. En la siguiente tabla se presentan las demás normas que componen la serie ISO27000.

Tabla 3. Normas de la Serie ISO 27000

Norma	Descripción
ISO 27000	Se describe la visión general y el vocabulario de SGSI, y referencia la familia de normas de sistemas de gestión de la seguridad de la información con los términos y definiciones relacionadas.
ISO 27002	Esta norma es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a SI. No es certificable y contiene los objetivos de control y los controles, agrupados en los dominios.
ISO 27003	Es una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.
ISO 27004	Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.
ISO 27005	Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la SI basada en un enfoque de gestión de riesgos

Norma	Descripción
ISO 27006	Esta norma específica los requisitos para la acreditación de entidades de auditoría y certificación de un SGSI.
ISO 27008	Es un estándar que suministra orientación acerca de la implementación y operación de los controles técnicos. Es aplicable a cualquier tipo y tamaño de empresa, tanto pública como privada que lleve a cabo revisiones relativas a la seguridad de la información y los controles de seguridad de la información.
ISO 27011	Es una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU[7].
ISO 27031	Es una guía de continuidad de negocio en cuanto a tecnologías de la información y las comunicaciones.
ISO 27032	Es en una guía referente a la ciberseguridad.
ISO 27033	Es una norma consistente gestión de redes.
ISO 27034	Es una guía de seguridad en aplicaciones.
ISO 27099	Consiste en una guía para implantar la Norma ISO 27002 específica para entornos médicos.

Fuente. Elaboración propia basado de (ICONTEC, 2013)

2.2.2 Componentes principales de un SGSI basado en la norma ISO27001

La norma NTC- ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos:

- **Alcance del SGSI:** ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (ICONTEC, 2013).

- **Política y objetivos de seguridad:** documento de contenido genérico que establece el Compromiso de la Alta Dirección y el enfoque de la organización en la gestión de la seguridad de la información (ICONTEC, 2013).

[7] ITU: Unión Internacional de Telecomunicaciones

- **Estándares, Procedimientos, y Guías que soportan el SGSI:** aquellos documentos y mecanismos que regulan el propio funcionamiento del SGSI. Documentación necesaria para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados –Métricas (ICONTEC, 2013).

- **Metodología de Evaluación de riesgos:** descripción de la metodología a emplear cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado, tratamiento y desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables (ICONTEC, 2013).

- **Informe de evaluación de riesgos:** estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización (ICONTEC, 2013).

- **Plan de tratamiento de riesgos:** documento que identifica las acciones de la Alta Dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc. (ICONTEC, 2013).

- **Registros:** documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI (ICONTEC, 2013).

- **Declaración de aplicabilidad:** documento que contiene los objetivos de control y los controles contemplados por el SGSI, en este se presentan las exclusiones y la evidencia de cumplimiento (ICONTEC, 2013).

2.2.3 Requisitos de la norma ISO27001:2013

En Colombia, el Instituto Colombiano de Normas Técnicas adopta la norma ISO/IEC 27001:2013 por traducción bajo la referencia NTC-ISO-IEC 27001, y establece una serie de requisitos que son indispensables. Estos requisitos indispensables son los numerales 4, 5, 6, 7, 8, 9 y 10 que se detallan a continuación en la siguiente tabla:

Tabla 4. Requisitos de la norma ISO-IEC 27001:2013

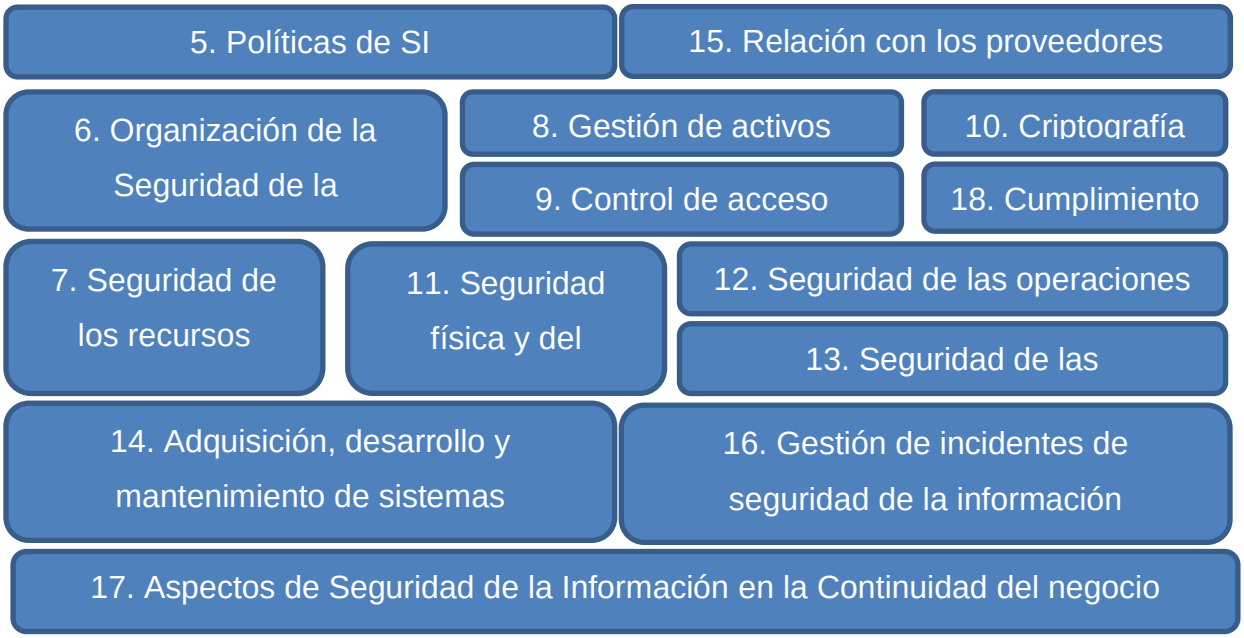
Numeral norma ISO-IEC 27001:2013	Descripción General
4. Contexto de la Organización	La organización debe determinar las cuestiones internas y externas que podrían influir en los resultados deseados de la seguridad de la información, así como comprender las necesidades de los interesados y determinar su alcance, límites y capacidad.
5. Liderazgo	La dirección de la organización debe dirigir el SGSI, velando por que se cumplan los requerimientos de la norma, garantizando los recursos, documentando las políticas y objetivos de seguridad propuestos, asignando las responsabilidades para cada una de las actividades y promoviendo el mejoramiento continuo.
6. Planificación	La organización debe definir acciones para tratar los riesgos, escoger una metodología de clasificación, análisis y valoración, formando criterios para establecer los controles de seguridad y así aplicar un proceso de tratamiento adecuado. Además de definir los objetivos de seguridad y los planes para lograrlos
7. Soporte	La organización debe garantizar los recursos, determinar la competencia de las personas, velar por comunicar las políticas de seguridad de la información a sus empleados y que éstos se comprometan al mejoramiento continuo del SGSI. Asimismo, se deben crear, actualizar y controlar la información documentada.

Numeral norma ISO-IEC 27001:2013	Descripción General
8. Operación	La organización debe documentar y planear los procesos para llevar a cabo las actividades, incluyendo las valoraciones de los riesgos de la seguridad de la información y el plan para tratarlos.
9. Evaluación del desempeño	La organización debe evaluar el desempeño de la SI y la eficacia del SGSI mediante auditorías internas a intervalos planificados y por medio de la revisión por la dirección.
10. Mejora	La organización debe reaccionar ante las no conformidades y emplear las acciones preventivas y correctivas, asegurando la mejora continua

Fuente. Elaboración propia adaptado de (ICONTEC, 2013)

La norma ISO-IEC 27001: 2013 presenta un Anexo A, el cual toma los controles de seguridad donde se presentan los 14 Dominios, 35 Objetivos de Control y 14 Controles de Referencia. A continuación, se presenta el detalle en la siguiente figura:

Figura 3. Dominios de Seguridad norma ISO-IEC 27001: 2013



Fuente. Elaboración Propia adaptado de (ICONTEC, 2013)

2.3 Descripción de la Entidad Geoconsult CS

Geoconsult Consultoría y Servicios Petroleros y Mineros Ltda., en adelante Geoconsult CS, es una empresa colombiana con operación multinacional, principalmente en Latinoamérica, con sedes en Colombia, Ecuador y Perú, que provee productos, servicios y soluciones de manejo de información técnica, interventoría de proyectos y consultoría geocientífica para la industria petrolera y de hidrocarburos. Fue constituida el 22 de marzo de 1995, y a través de sus más de 23 años de trayectoria se ha caracterizado por manejar los más grandes estándares de tecnología, mantener un continuo proceso de mejoramiento, especialización y aumento de su conocimiento, lo que le ha permitido mantener relaciones comerciales con diversos clientes naciones e internacionales, como Ecopetrol o la Agencia Nacional de Hidrocarburos, en donde ha complementado y potencializado sus capacidades, demostrando su estabilidad organizativa y posicionamiento en el sector (Geoconsult CS, 2015).

2.3.1 Misión de la Entidad

> Brindar al sector energético y minero una seria alternativa en consultoría y servicios especializados de exploración y producción, usando los más altos estándares de calidad y eficiencia a nivel internacional. Ofrecer a la Industria las mejores soluciones de manejo de información, incluyendo productos y servicios que incrementen la eficiencia de nuestros clientes.
>
> Proveer Interventorías confiables y de calidad para proyectos de Manejo de Información, Exploración y Producción, y Tecnologías de Información en la Industria Petrolera y el sector minero. Para lograr nuestra misión trabajaremos con los mejores profesionales y asesores del mercado, usaremos las mejores y más eficientes tecnologías, y complementaremos nuestras soluciones mediante alianzas con las mejores empresas del mercado. Nuestro trabajo estará enmarcado en un ambiente de respeto al cliente, de generación de bienestar y progreso para la gente que nos rodea. (Geoconsult CS, 2018).

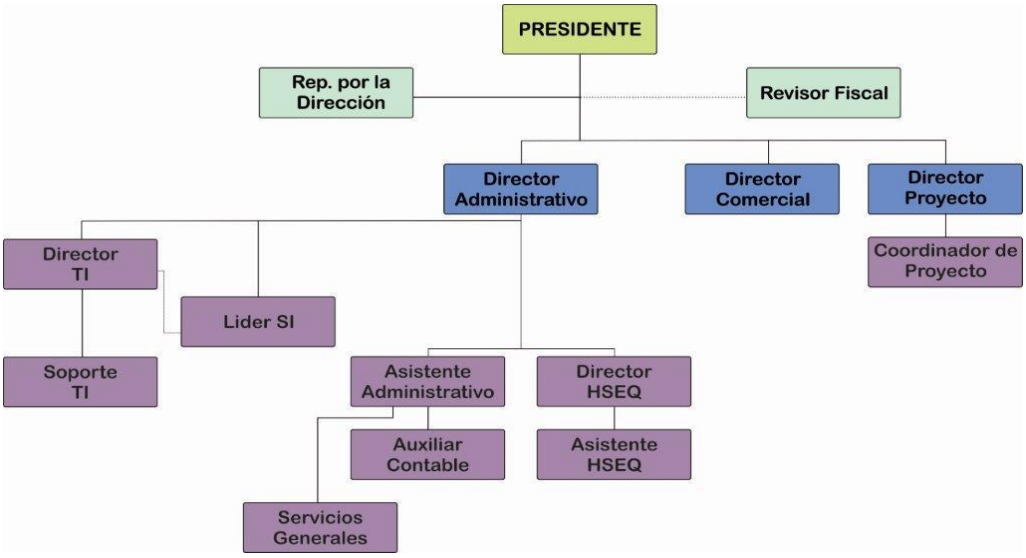
2.3.2 Visión de la Entidad

> Geoconsult CS ha establecido para el año 2020, ser una empresa con Participación en el mercado latinoamericana y reconocida en la Industria del Petróleo, como una de las mejores empresas del sector, apoyado por personal idóneo, capacitado y una buena capacidad financiera que genere y demuestre confianza a nuestros clientes y a su vez ofrezca bienestar a los miembros de la empresa y la comunidad en general. (Geoconsult CS, 2018)

2.3.3 Estructura organizacional

La estructura que se maneja en la empresa es de tipo funcional y se rige bajo el principio de la especialización lo que garantiza un buen desempeño en las actividades correspondientes a los diferentes departamentos y en cada uno de los cargos estipulados. En la siguiente figura se muestra la jerarquía que existe dentro de la organización, en la cual la mayor parte de la toma de decisiones es realizada por la Presidencia y la Dirección Administrativa, quienes adicionalmente dictan las políticas y estrategias de la compañía. La Gerencia Comercial se encarga de la atención al cliente, identificación y análisis de la viabilidad de los proyectos, los cuales una vez concretados pasan a ser parte de una o varias de las gerencias especializadas dependiendo de las áreas (manejo de información, consultoría, TI) que atañen al proyecto. Dichas gerencias son las encargadas de llevar a cabo los proyectos y tienen participación directa durante todo su ciclo de vida. (Geoconsult CS, 2015)

Figura 4. Organigrama de la Empresa



Fuente. Geoconsult CS (2015)

2.3.4 Portafolio de servicios

Manejo de Información: A través del conocimiento, experiencia y selecto grupo de profesionales con que se cuenta, se ofrecen soluciones integrales en manejo de información, las cuales van desde la creación e implantación de pequeñas bases de datos, hasta el montaje y administración de complejos sistemas de información corporativos, o bancos de datos, para grandes empresas o entidades gubernamentales. Los mayores retos y logros en esta área han estado en la industria petrolera, en la cual se han manejado con éxito enormes volúmenes de información en todos los formatos existentes (Geoconsult CS, 2015).

Consultoría Geocientífica: Geoconsult CS, como empresa líder en el manejo de datos geocientíficos respalda su conocimiento en la ejecución de estudios y trabajos de campo, en diferentes áreas de la geología y la ingeniería, los cuales abarcan todo el territorio colombiano, y se extienden a otras regiones de Latinoamérica. La empresa se destaca en proyectos de consultoría que incluyen: Interpretación sísmica, evaluación de proyectos de exploración y producción, estudios geológicos regionales, geoestadística y simulación de yacimientos. (Geoconsult CS, 2015)

Interventoría de Proyectos: La especialización de Geoconsult CS en proyectos de exploración y producción, en manejo especializado de datos para la industria petrolera y otros sectores, así como su conocimiento en tecnologías de información, han propiciado el fortalecimiento en el área de interventoría de proyectos. Actualmente, se especializa en interventorías para la industria petrolera en las siguientes áreas: Proyectos de manejo de información para la industria petrolera, proyectos de tecnologías de información y proyectos de exploración y producción de hidrocarburos. (Geoconsult CS, 2015).

2.3.5 Contexto de la Empresa

La organización Geoconsult CS se ha posicionado en el mercado como una de las empresas líderes en Colombia en el manejo de información técnica de la industria petrolera. Actualmente, dentro de sus clientes más importantes se destacan Ecopetrol y la Agencia Nacional de Hidrocarburos, a los cuales les ha ofrecido soluciones que asegurado altos niveles de eficiencia, seguridad y reducción de costos en sus procesos. En la siguiente Tabla se presentan los aliados estratégicos, clientes y principales competidores.

Tabla 5. Aliados estratégicos, clientes y principales competidores

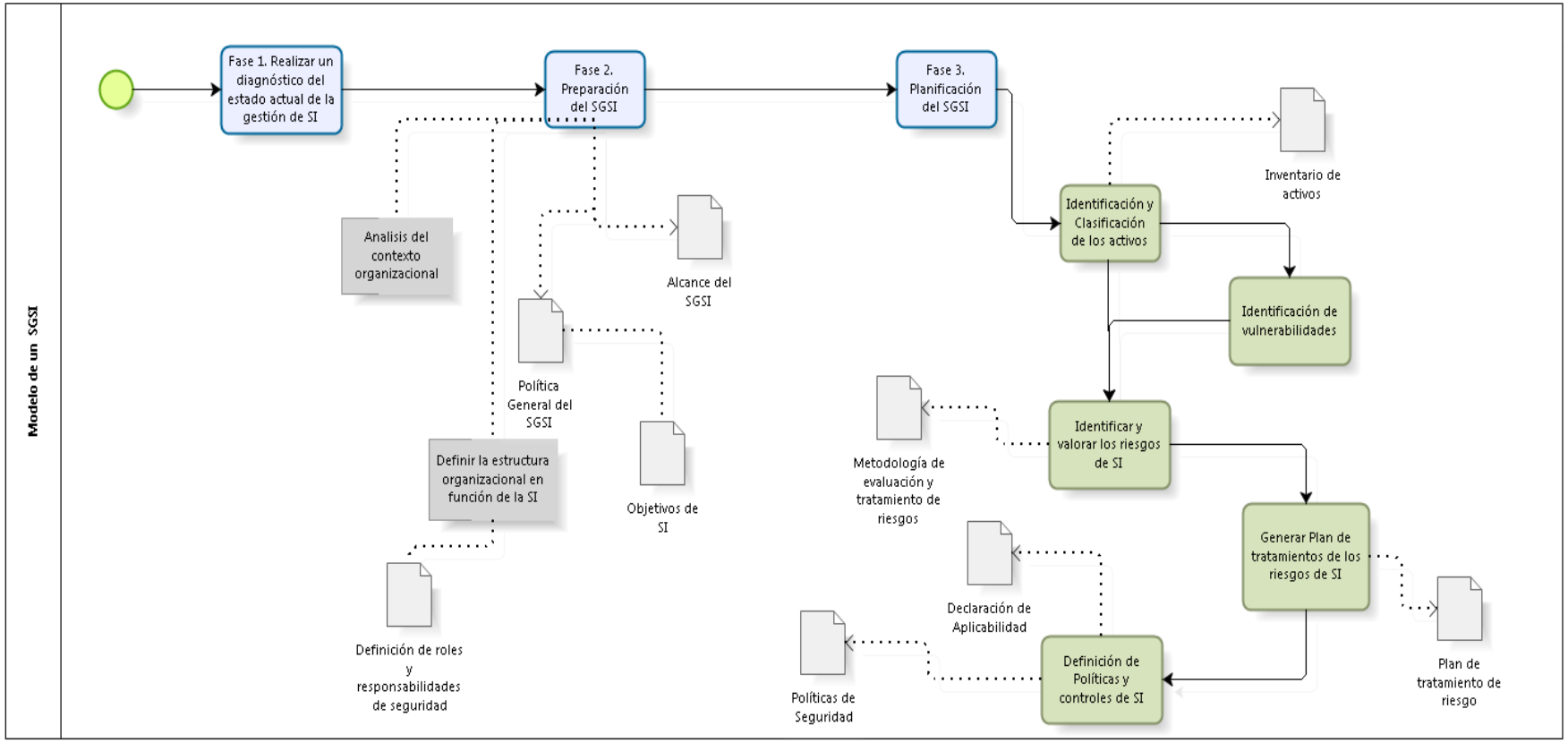
Organización	Principales Clientes	Aliados Estratégicos	Competidores
Geoconsult CS	Ecopetrol	Oracle	Inforpetrol
	ANH[8]	Microsoft	P&Z
	ICP[9]	Open Spirit	Iron Mountain
	Ingeominas	IHS	Indra

Fuente. Geoconsult CS (2018)

[8] ANH: Agencia Nacional de Hidrocarburos
[9] ICP: Instituto Colombiano de Petróleos

3 MODELO DEL SGSI

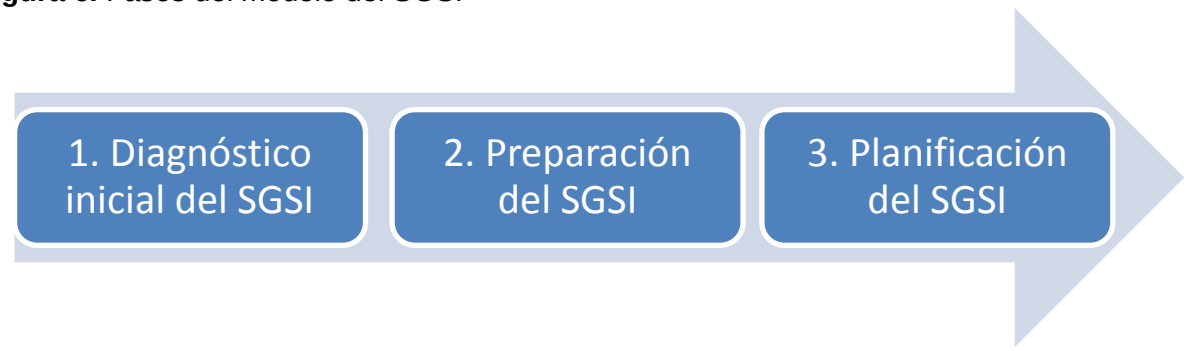
Figura 5. Modelo general del SGSI



Fuente. Propia

De acuerdo al marco de referencia de la norma NTC-ISO-IEC 27001:2013 para el diseño del modelo de un Sistema de Gestión de Seguridad de la Información en la organización Geoconsult CS, se establecen 3 fases para el desarrollo e implementación

Figura 6. Fases del modelo del SGSI



Fuente. Propia

En la Fase 1 Diagnóstico inicial del SGSI, se identificará el nivel preliminar de la organización con respecto al modelo de seguridad de la información que se especifica en la norma NTC-ISO-IEC 27001:2013. En esta fase se inspeccionará la información existente, se realizará entrevistas con las directivas de la organización y con los dueños de los procesos para establecer las exclusiones y evidencias de desempeño; con el fin de diligenciar un cuestionario para identificar el estado de cumplimiento de la empresa con respecto a los dominios y controles de la norma.

En la Fase 2 Preparación del SGSI, se identificará el contexto de la organización y las expectativas de las partes interesadas con el fin de generar el alcance del Sistema. Adicionalmente en esta fase se define los límites, la política general, los objetivos del SGSI y la estructura organización de la empresa correspondiente a la seguridad de la Información

En la Fase 3 Planificación del SGSI, se establecerá la identificación, valoración y tratamiento de los riesgos de SI, las vulnerabilidades, los activos, las políticas y los controles necesarios para el SGSI

3.1 Fase 1: Diagnóstico Inicial

La primera actividad al iniciar un diagnóstico de la operación actual del sistema de gestión de seguridad de la información es contar con el apoyo de la alta dirección para posteriormente realizar una evaluación completa de los requisitos, los objetivos de control y controles de la norma NTC-ISO-IEC 27001:2013 a partir del uso de los siguientes recursos para la recolección de los datos:

- Entrevistas con los líderes de los departamentos para determinar la estructura de las áreas, el clima organizacional y estado de los procesos.
- Cuestionario con veintiséis preguntas orientadoras para evaluar el estado de cumplimiento de los requisitos de la norma. (Ver Anexo 4).
- Revisión y lectura de la documentación existente (misión, visión, objetivos organizacionales, planeación estratégica, políticas, procesos, procedimientos, instructivos, manuales, normatividad entre otros).
- Observación de las actividades del día a día.

3.1.1 Evaluación de los requisitos de la norma NTC-ISO-IEC 27001:2013

Para determinar el nivel de madurez que presenta la organización con respecto a los temas relacionados con Seguridad de la Información, se debe realizar una entrevista utilizando el cuestionario del anexo 4 a los dueños de los procesos con el fin de evaluar todos los requerimientos obligatorios de los numerales del cuatro al diez de la norma NTC-ISO-IEC 27001:2013.

Cada numeral se debe evaluar a partir de cualquiera de los siguientes tres estados:

Tabla 6. Criterios de Evaluación en el Diagnóstico

ESTADO	DESCRIPCIÓN
Cumple Satisfactoriamente	Existe, es gestionado, está documentado, se está cumpliendo con lo requerido por la norma y es conocido por todo el personal involucrado de la empresa. Cumple 100%.
Cumple Parcialmente	De acuerdo a lo requerido por la norma, se está realizando de manera parcial, no está completamente documentado, se definió, pero no se gestiona, ni se conoce en la organización. Cumple 50%.
No Cumple	No existe, y/o no se está realizando, y/o no se había determinado su necesidad. Cumple 0%.

Fuente. Propia

3.1.2 Evaluación los objetivos de control y controles de la norma NTC-ISO-IEC 27001:2013

Para continuar con las actividades de esta fase se debe determinar el estado de los 114 controles del anexo A de la norma NTC-ISO-IEC 27001:2013, utilizando el documento existente de la organización destinado para la declaración de aplicabilidad. Si la organización no cuenta aún con este documento se puede utilizar como base el formato del Anexo 5 y cada objetivo de control se debe evaluar a partir de los estados de la tabla anterior.

Finalmente se termina esta fase con la entrega del informe final de diagnóstico donde se determina el porcentaje de cumplimiento e incumplimiento tanto de los requisitos como de los controles de la norma, incluyendo el nivel de cumplimiento general y un análisis a los hallazgos detectados, dando fin a la fase 1, e iniciando a la siguiente etapa de preparación del SGSI.

3.2 Fase 2: Preparación del SGSI

3.2.1 Análisis del contexto organizacional

En el primer paso de la fase 2, correspondiente a la preparación del SGSI, la organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que generan algún impacto positivo o negativo para lograr los resultados deseados del sistema de gestión de seguridad de la información.

La identificación de las partes interesadas es una parte muy importante en el análisis del contexto, debido a que se definen los requisitos tácitos, legales, reglamentarios y contractuales de la organización, accionistas, empleados, instituciones financieras, clientes, proveedores, gobierno, comunidad y medio ambiente, entre otros.

La metodología propuesta para identificar el contexto y las partes interesadas es realizar un análisis DOFA[10] para conocer las características internas, los riesgos y las oportunidades que pueden venir del exterior. Adicionalmente se debe enumerar todos los entes, tanto privados como gubernamentales que afectan el SGSI, especificando sus intereses y sus necesidades.

3.2.2 Estructura organizacional en función de la SI

El segundo paso de la preparación del SGSI, es definir la estructura organizacional con respecto a la seguridad de la información. En esta etapa se debe utilizar como base el organigrama de la empresa y los cargos que se mencionen en este. Con el fin de definir los roles y responsabilidades dentro del sistema de gestión de seguridad de la información.

[10] DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas)

3.2.2.1 Definición de roles y responsabilidades

Definir los roles y responsabilidades para la seguridad de la información de las personas que intervienen en las diferentes áreas de una organización es la última actividad de la etapa de planificación, pero no por eso es la menos importante.

En esta actividad es crucial definir los perfiles definidos en cada nivel y describir las responsabilidades generales y las condescendientes a la seguridad de la información de la forma menos general y más detallada posible. Asimismo, se deben especificar aspectos importantes como el departamento o área, jefe inmediato y número de cargos iguales, entre otros.

3.2.3 Definición de recursos

El tercer paso de la preparación del SGSI, es definir y asegurar los recursos necesarios para la implementación y mejora del sistema de gestión de seguridad de la información. En esta actividad la alta dirección debe demostrar liderazgo y compromiso asegurando que estén disponibles las personas, los equipos, el dinero y los insumos necesarios.

En este paso es crucial definir un presupuesto donde se detallen como mínimo los siguientes campos: tipo de recursos, actividad, descripción, año y valor.

3.3 Fase 3: Planificación del SGSI

3.3.1 Identificación y clasificación de los activos

Una vez culminadas las actividades de la fase 2 de la preparación del SGSI, se inicia la etapa de planificación con la identificación y clasificación de los activos de información de la organización. En esta actividad se deben identificar en un inventario los activos asociados con la información, los cuales corresponden a las instalaciones de procesamiento de información, la infraestructura, el conocimiento de las personas de la empresa y la información en medio impreso y digital. Este inventario debe ser un registro que tenga como mínimo las siguientes 8 columnas:

Tabla 7. Columnas mínimas en el registro de activos

1 Nombre del Activo	2 Descripción General	3 Tipo de Activo	4 Objetivo Seguridad			5 Nivel de criticidad	6 Prioridad del Negocio	7 Responsable del Activo	8 Ubicación
			C	I	D				

Fuente. Propia

- En la columna 1 se debe especificar el nombre del activo de información, por ejemplo: equipos de cómputo, servidores, documentación impresa, conocimientos valiosos, etc.
- En la columna 2 se debe detallar lo más amplio posible la descripción de ese tipo de activo, incluyendo su uso y objetivo, por ejemplo: Servidor Dell poweredge T30 conectado en la red donde se almacena toda la documentación de los procesos de la empresa.
- En la columna 3 se debe especificar si este tipo de activo es información, infraestructura, personas o sistemas de información.
- En la columna 4 se debe determinar el objetivo de seguridad en términos de los principios de seguridad de la información Confidencialidad (C), Integridad (I) y Disponibilidad (D) como alto (A), medio (M) o bajo (B).

- En la columna 5 el nivel de criticidad corresponde a un valor automático producto del cálculo matemático de la calificación dada en los anteriores objetivos de seguridad, es decir, (A=3), medio (M=2) y bajo (B=1). Obteniendo un valor el cual puede ir desde 3 hasta 9.
- En la columna 6 se encuentra la prioridad del negocio, la cual depende directamente del nivel de criticidad del activo, y puede ser 1, 2 o 3.
- En la columna 7 se debe incluir el propietario del activo, el cual corresponde al responsable de su gestión apropiada durante todo su ciclo de vida.
- En la columna 8 se debe incluir la ubicación tanto física o digital del activo.

El inventario de activos debe ser exacto, actualizado, consistente y alineado con otros inventarios.

3.3.2 Identificación de vulnerabilidades

Las vulnerabilidades identificadas en un sistema de gestión de seguridad de la información deben ser sobre procesos, personas y tecnología. Basado en la norma ISO27005 se presenta en la hoja 5 del anexo 3 un listado de 63 vulnerabilidades comunes que puede tener cualquier compañía con respecto a su personal, su infraestructura física, su software, su red y sus procesos.

La verificación al estado de la seguridad informática es fundamental en las labores de aseguramiento y vigilancia a los componentes tecnológicos que integran un sistema de gestión de seguridad de la información; es el punto de partida para la aplicación de medidas y/o contramedidas que garanticen el normal desempeño de los ambientes informáticos y de los procesos de la organización.

El objetivo principal en la evaluación de vulnerabilidades a nivel de tecnología es identificar los riesgos potenciales de seguridad informática y oportunidades de mejoramiento a partir de la realización de pruebas de seguridad internas ejecutadas sobre las estaciones de trabajo y servidores. Para finalmente establecer algunas recomendaciones de acuerdo a las buenas prácticas de seguridad de la información.

El software a utilizar en la identificación de vulnerabilidades a nivel tecnológico es Microsoft Baseline Security Analizer 2.3, el cual servirá como fuente dentro de la siguiente metodología para la identificación, análisis y seguimiento de las pruebas de vulnerabilidad. A continuación, se presenta la metodología propuesta para esta actividad:

Figura 7. Metodología Análisis y seguimiento de la seguridad de la Información

Fuente. Propia

Recolección de la información:

En esta primera etapa de la identificación de vulnerabilidades, se debe realizar un levantamiento de la información tecnológica de los servidores, equipos de escritorio, portátiles y todo equipo conectado dentro de la red. Identificando las direcciones IP y/o nombre del Dominio, la enumeración de los usuarios, la identificación de sistemas operativos y el diseño de la segmentación de la red.

Análisis de vulnerabilidades

En este segundo paso, se realiza una inspección y revisión de todos los elementos de la red con el software de diagnóstico Microsoft Baseline Security Analizer versión 2.3.

Resultados y vulnerabilidades

En esta etapa se detalla los hallazgos que tiene en cuenta el software de diagnóstico, bajo tres criterios:

Figura 8. Tipo de Hallazgos Análisis de vulnerabilidades

Check failed (critical)	Falla Crítica
Check failed (non-critical)	Falla No Crítica
Check passed	Parámetro Conforme

Fuente. Propia basada en (Microsoft Baseline Security Analizer versión 2.3)

Falla Crítica: Cuando la falla permite poner indisponible algún elemento de la infraestructura tecnológica o poder tomar control sobre alguno de ellos con privilegios de administrador. Por ejemplo, ataques de denegación de servicio al servidor o ataques de ejecución de código arbitrario que permite la obtención de privilegios en el servidor para su control total o parcial.

Falla No Critica: Cuando la vulnerabilidad me permite obtener accesos o servicios no autorizados, pero sin llegar a la posibilidad de tomar el rol de administrador del acceso o servicio. Por ejemplo, utilización de protocolos no seguros y/o utilización de contraseñas débiles que comprometen la confidencialidad de la información, permisos de acceso y visualización de estructuras internas del servidor.

Parámetro Conforme: La conformidad con relación a uno o varios de los parámetros que son considerados dentro del proceso de revisión, para lo cual el equipo ha reunido la configuración que permite mantenerlo a salvo de la vulnerabilidad evaluada.

Análisis de resultados y recomendaciones

En esta última etapa se presentan los resultados de los hallazgos encontrados y las recomendaciones a realizar

3.3.3 Gestión de riesgos de seguridad de la información

Esta actividad de la fase 3 en la planificación del SGSI, correspondiente a la gestión de riesgos, es uno de los aspectos más importantes dentro del sistema de gestión de seguridad de la información. La organización debe establecer las acciones para identificar, evaluar, clasificar y convenir la estrategia para mitigar los riesgos de seguridad de la información a niveles aceptables, por medio de mecanismos que faciliten su desarrollo de manera permanente, repetible y medible.

A continuación, se presenta un modelo basado en un ciclo de gestión PHVA, con el fin de realizar el análisis, valoración, tratamiento de riesgos e implementación de controles de seguridad de la información, que aplica a todos los procesos y a los servicios considerados en el alcance de cualquier sistema.

Tabla 8. Criterios de evaluación en el diagnóstico

CICLO	ACTIVIDAD
P	Generar lineamientos y directrices sobre la gestión de riesgos, valoración, tratamiento y controles de seguridad de la información.
	Diseñar las acciones necesarias para tratar los riesgos de seguridad de la información.
H	Ejecutar las acciones definidas para el tratamiento de riesgos y los controles de seguridad de la información de acuerdo con el diseño establecido.
	Asegurar la generación y disponibilidad de las evidencias resultantes
	Autoevaluar la eficacia las acciones implementadas para el tratamiento de riesgos
V	Evaluar la eficacia las acciones implementadas para el tratamiento de riesgos.
	Asegurar que el SGSI logre los resultados previstos en cuanto al análisis, valoración y tratamiento de riesgos.
A	Desarrollar las acciones de mejora requerida para tratar los riesgos y reducir las brechas identificadas por las evaluaciones y/o auditorias, a nivel de operación de los procesos y de ser necesario rediseñar los controles de seguridad de la información.

Fuente. Propia

3.3.4 Definición de políticas y controles de seguridad de la información

En esta última actividad de la fase 3 se proponen unas políticas y normas mínimas que debe conocer y cumplir todo colaborador en cualquier empresa que tenga o pretenda tener un sistema de Gestión de Seguridad de la Información en relación con el uso de los recursos y los activos de información.

- Política de Contraseña Segura.
- Política de Uso de Controles Criptográficos.
- Política de Seguridad en Sistemas Físicos.
- Política de Uso de Software Legal.
- Política de Derechos de Autor.
- Política de Uso de Internet.
- Política de Uso de Correo Electrónico.
- Política de escritorio y pantalla limpia.

Algunas de estas políticas son obligatorias de acuerdo a los requisitos del anexo A de la norma NTC-ISO-IEC27001, y otras ayudan a gestionar adecuadamente los recursos de la organización. Adicionalmente se puede generar otras para cumplir requisitos contractuales con el cliente como pueden ser políticas de transferencia de información, política anticorrupción, entre otras.

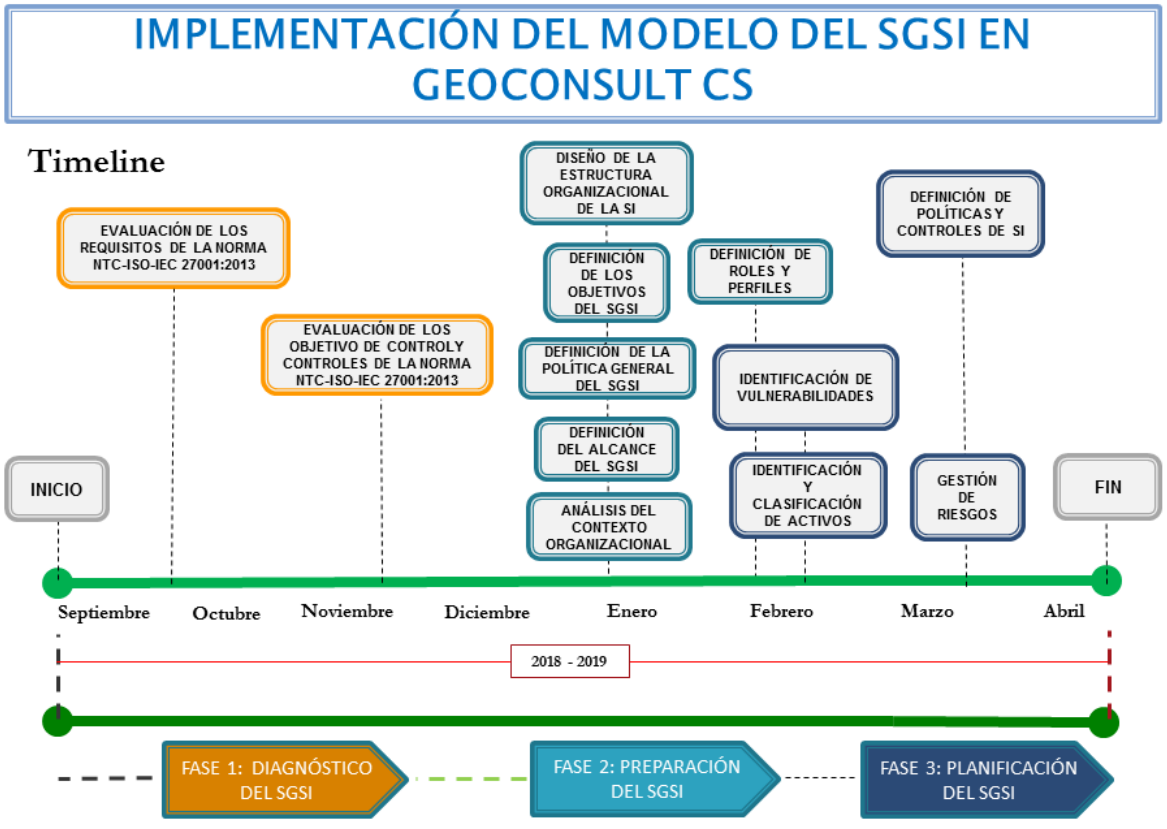
Una vez se haya terminado todas las actividades de las tres fases, cualquier empresa sin importar su sector o razón social, contará con un sistema de gestión de la seguridad de la información, aplicado a todos los procesos y áreas determinados en su alcance, el cual estará alineado con la norma NTC-ISO-IEC 27001:2013.

4 MODELO DEL SGSI APLICADO A GEOCONSULT CS

De acuerdo al marco de referencia de la norma NTC-ISO-IEC 27001:2013 y al modelo de un Sistema de Gestión de Seguridad de la Información presentado durante todo el capítulo 3. A continuación, se presenta su implementación en la organización Geoconsult CS, respetando estrictamente todas las actividades y pasos detallados en las tres fases de este modelo.

El tiempo de implementación de este modelo tardó aproximadamente ocho meses y se ejecutó de la siguiente manera:

Figura 9. Línea de tiempo de la implementación del modelo en Geoconsult CS



Fuente. Elaboración propia

4.1 Diagnóstico Inicial

4.1.1 Evaluación de los requisitos de la norma NTC-ISO-IEC 27001:2013

En el siguiente capítulo se presenta el diagnóstico realizado en la organización Geoconsult CS, con el fin de conocer el estado actual de cumplimiento de la norma NTC-ISO-IEC 27001:2013.

Dicha validación se ejecutó bajo los criterios de evaluación establecidos en la Tabla 5 de este documento.

Tabla 9. Estado de Cumplimento de la Norma ISO/IEC 27001:2013. Contexto de la Organización

Requisito	4. Contexto de la Organización	Pregunta	Estado de Cumplimiento	Evidencia
4.1	Conocimiento de la organización y de su contexto.	¿La empresa ha identificado los aspectos internos y externos que pueden afectar el SGSI?	Cumple Parcialmente	La organización si ha determinado las cuestiones externas que pueden afectar los resultados previstos del SGSI, como son los competidores, proveedores y requerimientos de cliente. Pero no ha determinado las cuestiones internas.
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	¿La empresa ha identificado las partes interesadas y sus necesidades?	Cumple Parcialmente	La organización si ha determinado algunas necesidades por parte de la dirección, pero se desconoce las expectativas de los clientes, y dueños de los procesos de la empresa.
4.3	Determinación del alcance del Sistema de Gestión de la Seguridad de la información	¿La empresa ha identificado los límites, la aplicabilidad del SGSI, y ha determinado su alcance?	Cumple Parcialmente	La alta dirección si ha determinado un alcance inicial del SGSI, pero este no se encuentra como información documentada, ni es conocido por el personal de la compañía.
4.4	Sistema de Gestión de la Seguridad de la Información	¿La organización ha planeado, establecido o implementado un SGSI?	No Cumple	La organización Geoconsult CS actualmente no tiene implementado un Sistema de Gestión de Seguridad de la Información.

Fuente. Propia basado en (ICONTEC, 2013)

Tabla 10. Estado de Cumplimento de la Norma ISO/IEC 27001:2013. Liderazgo

Requisito	5. Liderazgo	Pregunta	Estado de Cumplimiento	Evidencia
5.1	Liderazgo y Compromiso	¿La alta dirección ha asegurado la disponibilidad de los recursos necesarios para el SGSI, ha establecido la Política y los objetivos de Seguridad de la Información	Cumple Parcialmente	La dirección no ha establecido la Política, ni los objetivos de la Seguridad de la Información, Pero si ha definido un presupuesto para el SGSI
5.2	Política	¿En la organización existe un documento de la Política del Sistema de Gestión de Seguridad de la Información, el cual ha sido aprobado por la Dirección?	No Cumple	La dirección no ha establecido una Política de la Seguridad de la Información
5.3	Roles, Responsabilidades y autoridades en la organización.	¿En la organización existe un documento de roles, responsabilidades y autoridades en SI?	No Cumple	No se evidencia en la empresa la definición de roles, responsabilidades y autoridades en Seguridad de la Información

Fuente. Propia basado en (ICONTEC, 2013)

Tabla 11. Estado de Cumplimento de la Norma ISO/IEC 27001:2013. Planificación

Requisito	6. Planificación	Pregunta	Estado de Cumplimiento	Evidencia
6.1	Acciones para tratar riesgos y oportunidades	¿La organización ha realizado una identificación de riesgos con respecto a la SI?	Cumple Parcialmente	No se han identificado riesgos a gran escala, ni existe una metodología formal para gestionarlos.
6.1.1	Generalidades	¿La organización ha determinado los riesgos y oportunidades con respecto a la SI?	Cumple Parcialmente	La organización ha identificado algunos riesgos de seguridad informática, pero no están documentados.
6.1.2	Valoración de riesgos de la seguridad de la información	¿En la organización existe un proceso de valoración de riesgos de SI?	No Cumple	No existe un proceso de gestión de riesgos de SI, en el que se establezca los criterios de aceptación, valoración y priorización de los riesgos.
6.1.3	Tratamiento de riesgos de la seguridad de la información	¿En la organización han definido y aplicado un proceso de tratamiento de riesgos de SI?	No Cumple	La organización no cuenta con un plan de tratamiento de riesgos documentado.
6.2	Objetivos de seguridad de la información.	¿En la organización se han establecido los objetivos de SI?	No Cumple	No están documentados los Objetivos de Seguridad de la Información

Fuente. Propia basado en (ICONTEC, 2013)

Tabla 12. Estado de Cumplimento de la Norma ISO/IEC 27001:2013. Soporte

Requisito	7. Soporte	Pregunta	Estado de Cumplimiento	Evidencia
7.1	Recursos	¿La dirección ha determinado los recursos necesarios para el SGSI?	Cumple Satisfactoriamente	Se ha definido un presupuesto para el SGSI.
7.2	Competencia	¿La organización ha determinado la competencia necesaria de todo el personal?	Cumple Parcialmente	Se encuentra documentado el nivel de competencia del 80% del personal de la organización, pero no se ha identificado la formación, educación y experiencia de 5 cargos de un personal administrativo que lleva más de 10 años en la empresa.
7.3	Toma de conciencia	¿El personal de la organización tiene conciencia de la política de seguridad de la información y la importancia del SGSI en la empresa?	No Cumple	Existen acuerdos de confidencialidad de los empleados vinculados a los proyectos con el cliente, pero no existen políticas de seguridad de la información a seguir, ni conocimientos básicos del personal con respecto a la SI.
7.4	Comunicación	¿La empresa tiene definido un modelo de comunicaciones tanto internas como externas	No Cumple	Existen medios de comunicación como correo electrónico, carteleras y capacitaciones regulares, pero nunca han

Requisito	7. Soporte	Pregunta	Estado de Cumplimiento	Evidencia
		respecto a la seguridad de la información?		sido utilizados para temas relacionados con seguridad de la información.
7.5	Información Documentada	¿Existe en la empresa un proceso o procedimiento para el control de la información documentada?	Cumple Parcialmente	La empresa cuenta con un proceso de Calidad en el cual se encuentra el procedimiento PM-GC-001 PROC CONTROL DE DOCUMENTOS y PM-GC-002 PROC. CONTROL DE REGISTROS, pero no se ha vinculado el SGSI dentro de este proceso.
7.5.1	Generalidades	¿La organización tiene la información referente al Sistema de Gestión de Seguridad de la Información debidamente documentada y controlada?	No Cumple	No se tiene la información documentada del Sistema de Gestión de Seguridad de la Información. Pero si se tiene documentada información de los procesos de la compañía a partir del proceso del Sistema de Gestión de Calidad.
7.5.2	Creación y actualización	¿La información documentada del SGSI cuenta con una identificación y descripción?	No Cumple	No se evidencia información documentada del SGSI, se encontró información de soporte en el área de TI, pero esta no cumple con especificaciones mínimas de identificación como título, fecha o versión.

Requisito	7. Soporte	Pregunta	Estado de Cumplimiento	Evidencia
7.5.3	Control de la información documentada	¿La información del SGSI está protegida adecuadamente?	Cumple Parcialmente	Existe muy poca información debidamente documentada del SGSI, la cual reposa digitalmente en un servidor que cumple con las condiciones adecuadas de seguridad y de protección, No obstante, la organización no está considerado la retención, disposición y control de cambios.

Fuente. Propia basado en (ICONTEC, 2013)

Tabla 13. Estado de Cumplimento de la Norma ISO/IEC 27001:2013. Operación

Requisito	8. Operación	Pregunta	Estado de Cumplimiento	Evidencia
8.1	Planificación y control operacional	¿En los diferentes procesos de la compañía se tiene considerado aspectos de seguridad de la información?	Cumple Parcialmente	La organización únicamente tiene considerado en el proceso de TI el cumplimiento de los requisitos de seguridad de la información, pero en las diferentes áreas de la compañía no existe una planificación, ni control operacional con respecto al SGSI.
8.2	Valoración de riesgos de la seguridad de la información	¿En la organización se lleva a cabo una valoración a intervalos planificados de los riesgos de SI?	No Cumple	No se ha identificado, ni valorado correctamente los riesgos que puede afectar la seguridad de la información.
8.3	Tratamiento de riesgos de la seguridad de la información	¿En la organización han implementado un plan de tratamiento de riesgos de SI?	No Cumple	La organización no cuenta con un plan de tratamiento de riesgos documentado. Debido a que no ha realizado una correcta identificación y evaluación.

Fuente. Propia basado en (ICONTEC, 2013)

Tabla 14. Estado de Cumplimento de la Norma ISO/IEC 27001:2013. Evaluación del Desempeño

Requisito	9. Evaluación del Desempeño	Pregunta	Estado de Cumplimiento	Evidencia
9.1	Seguimiento, medición, análisis y evaluación	¿La organización evalúa el desempeño de la seguridad de la información y la eficacia del SGSI?	No Cumple	La organización no tiene considerado indicadores para evaluar el desempeño del sistema de gestión de seguridad de la información
9.2	Auditoria interna	¿La organización lleva a cabo auditorías internas al SGSI?	No Cumple	Nunca se ha realizado una Auditoria interna que proporcione información acerca del sistema de gestión de seguridad de la información
9.3	Revisión por la dirección	¿La alta revisión revisa el SGSI a intervalos planificados?	Cumple Parcialmente	La alta dirección revisa periódicamente el comportamiento de los procesos de la organización, pero esta revisión no se ha documentado.

Fuente. Propia basado en (ICONTEC, 2013)

Tabla 15. Estado de Cumplimento de la Norma ISO/IEC 27001:2013. Mejora

Requisito	10. Mejora	Pregunta	Estado de Cumplimiento	Evidencia
10.1	No conformidades y Acciones Correctivas	¿Se han detectado no conformidades en las Auditorías internas?	No Cumple	Nunca se ha realizado una Auditoria interna que proporcione información acerca del sistema de gestión de seguridad de la información
10.2	Mejora Continua	¿La organización ha mejorado continuamente la conveniencia, adecuación y eficacia del sistema de gestión de la seguridad de la información?	No Cumple	Debido a que a la fecha no se considera que exista un Sistema de gestión de seguridad de la información, no se puede evaluar su mejora.

Fuente. Propia basado en (ICONTEC, 2013)

De acuerdo a la revisión realizada a cada uno de los requisitos mínimos y obligatorios de los numerales del cuatro al diez de la norma NTC-ISO-IEC 27001:2013, a continuación, se presenta el resumen del nivel de cumplimiento y madurez:

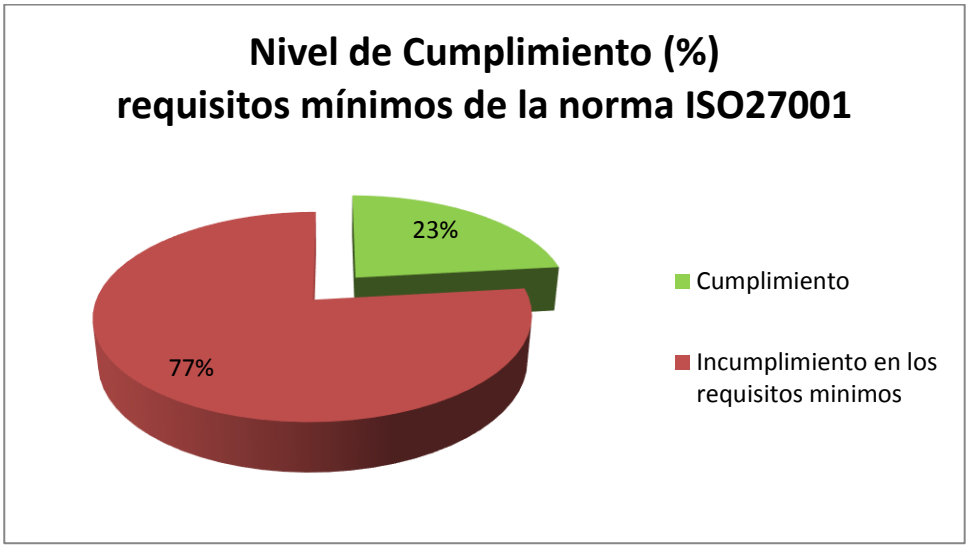
Tabla 16. Nivel de cumplimiento de los requisitos de la norma NTC-ISO-IEC 27001:2013.

Numeral / Requisito	Cumple	No Cumple
4. Contexto de la Organización	37.5%	63.5%
5. Liderazgo	16.5%	83.5%
6. Planificación	20%	80%
7. Soporte	31.25%	68.75%
8.Operación	16.5%	83.5%
9. Avaluación del desempeño	16.5%	83.5%
10. Mejora	0%	100%

Fuente. Elaboración propia

El nivel de cumplimiento y madurez general que se presenta actualmente en Geoconsult referente a todos los requisitos mínimos de la norma es:

Figura 10. Nivel de cumplimiento General de la norma NTC-ISO-IEC 27001:2013.



Fuente. Elaboración propia

De acuerdo a los resultados de la evaluación de todos los requerimientos obligatorios de los numerales del cuatro al diez de la norma NTC-ISO-IEC 27001:2013, se puede evidenciar el compromiso e interés que tiene la alta dirección de Geoconsult CS con respecto al Sistema de Gestión de Seguridad de la Información; no obstante se evidencia 21 falencias en los 22 requisitos evaluados, específicamente en la generación de la información documentada requerida por la norma, en la identificación y acciones para tratar los riesgos y en los bajos niveles de conciencia con respecto a la seguridad de la información por parte del personal operativo de la compañía.

La organización únicamente tiene considerado en el proceso de TI el cumplimiento de los requisitos de seguridad de la información. En las demás áreas de la empresa no se han considerado aspectos de SI dentro de los procedimientos y procesos. No obstante, los dueños de las áreas y participes en los procesos, si consideran la importancia y los beneficios que les puede aportar un Sistema de Gestión de Seguridad de la Información.

4.1.2 Evaluación de los objetivos de control y controles de la Norma NTC-ISO-IEC 27001:2013

Con el fin de realizar un diagnóstico completo de todos los requerimientos de la norma, se realizó una validación de los 114 objetivos de control y controles que se obtienen directamente del anexo A de la norma NTC-ISO-IEC 27002:2013, en los numerales 5 a 18, los cuales se deben usar en contexto con el numeral 6.1.3 de la misma norma. Dicha validación se ejecutó bajo los mismos criterios de evaluación de la Tabla 5 de este documento.

El diagnóstico detallado de los 114 controles que se realizó en la organización Geoconsult CS se puede consultar en el Anexo 1 “Estado de cumplimento del anexo A de la Norma ISO/IEC 27001:2013 en la organización Geoconsult CS”

De acuerdo a la revisión realizada a cada uno de los requisitos de los objetivos de control y controles enumerados del cinco al dieciocho del Anexo A de la norma NTC-ISO-IEC 27001:2013, a continuación, se presenta el resumen del nivel de cumplimiento y madurez:

Tabla 17. Nivel de cumplimiento de los requisitos del anexo A de la norma NTC-ISO-IEC 27001:2013.

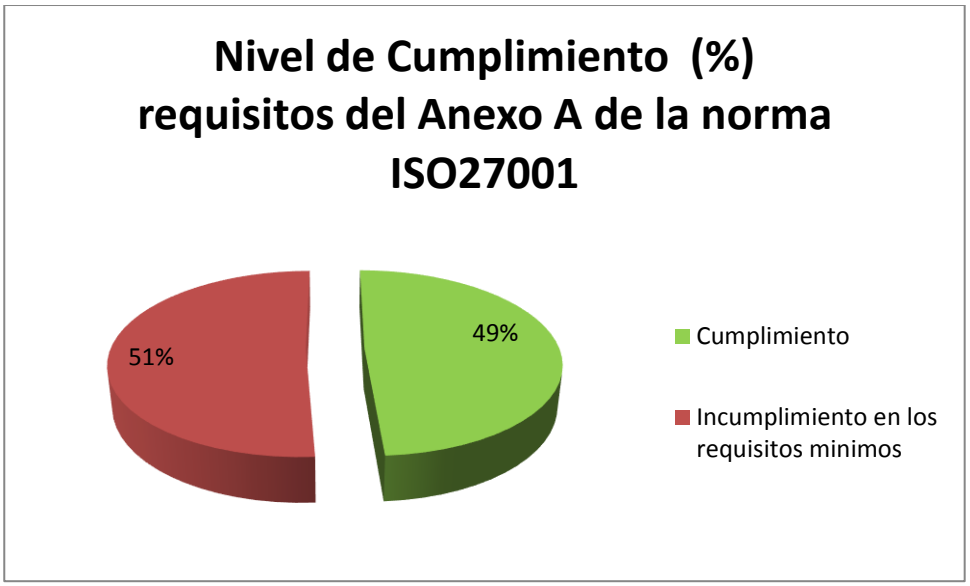
Numeral / Requisito	Total Controles	Controles Excluidos	Controles a evaluar	Cumple	No Cumple	%
A5. Políticas de la seguridad de la información	2	0	2	0	2	0%
A6. Organización de la seguridad de la información	7	1	6	3,5	2,5	58%
A7. Seguridad de los recursos humanos	6	0	6	3	3	50%
A8. Gestión de activos	10	0	10	2	8	20%
A9. Control de acceso	14	0	14	4	10	29%
A10. Criptografía	2	0	2	0	2	0%
A11. Seguridad física y del entorno	15	0	15	13,5	1,5	90%
A12. Seguridad de las operaciones	14	0	14	8,5	5,5	61%
A13. Seguridad de las comunicaciones	7	0	7	3,5	3,5	50%

Numeral / Requisito	Total Controles	Controles Excluidos	Controles a evaluar	Cumple	No Cumple	%
A14. Adquisición, desarrollo y mantenimiento de sistemas	13	4	9	5	4	56%
A15. Relaciones con los proveedores	5	0	5	1,5	3,5	30%
A16. Gestión de incidentes de seguridad de la información	7	0	7	5,5	1,5	79%
A17. Aspectos de seguridad de la información de la gestión de continuidad de negocio	4	0	4	1	3	25%
A18. Cumplimiento	8	0	8	2,5	5,5	31%

Fuente. Elaboración propia

El nivel de cumplimiento y madurez general que se presenta actualmente en Geoconsult referente a todos los controles y objetivos de control del Anexo A de la norma es:

Figura 11. Nivel de cumplimiento General de los controles del Anexo A



Fuente. Propia

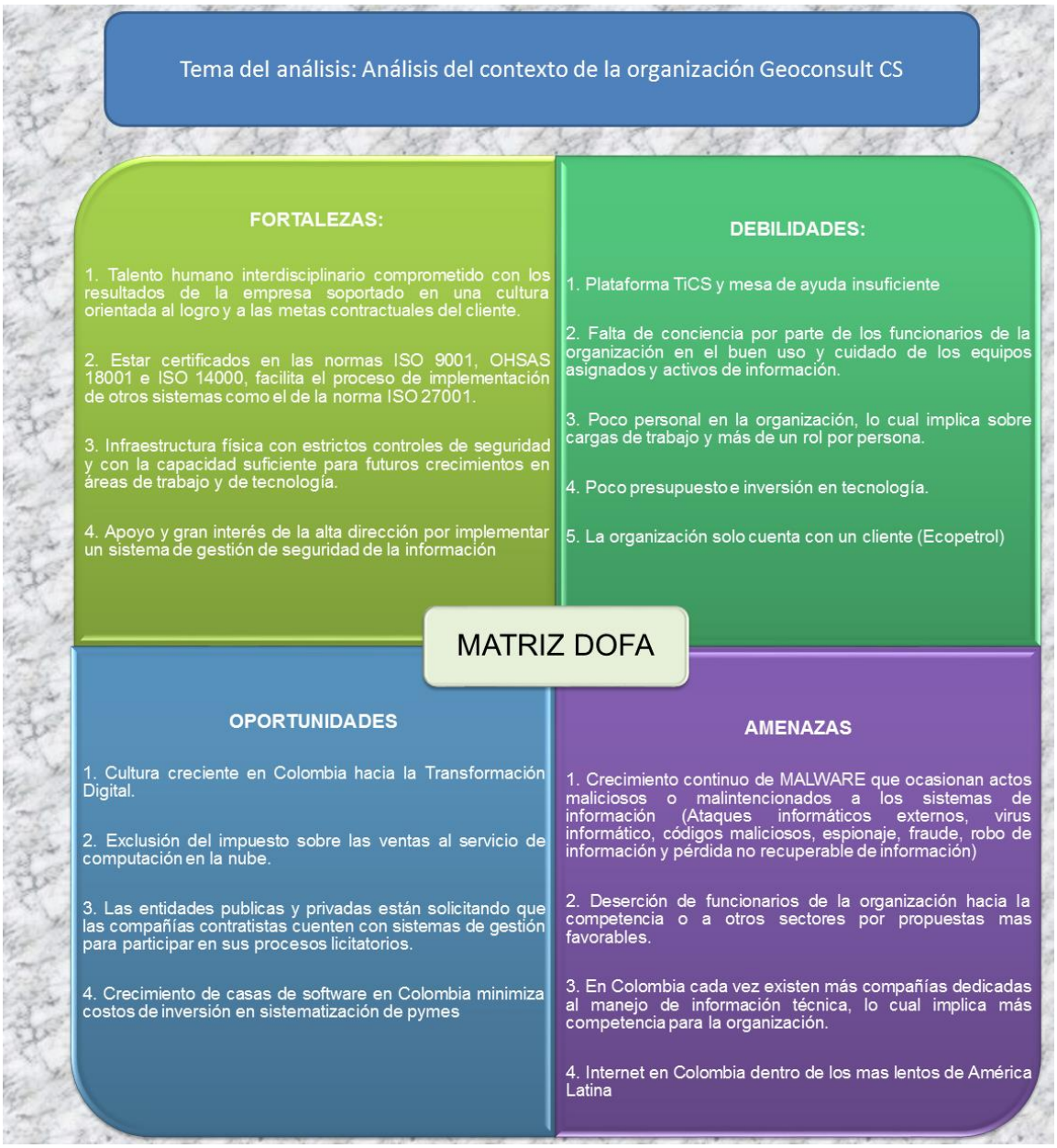
De acuerdo a los resultados de la evaluación de todos los controles y objetivos de control de los numerales del cinco al dieciocho del anexo A de la norma NTC-ISO-IEC 27001:2013, se puede evidenciar un avance significativo en 64 de los 114 controles, gracias a las acciones implementadas especialmente en la seguridad física y del entorno y en la gestión de incidentes de seguridad de la información; no obstante se evidencia muchas falencias específicamente en la generación de las políticas de seguridad de la información, gestión de activos, controles criptográficos y aspectos de seguridad de la gestión de continuidad de negocio.

4.2 Preparación del SGSI

4.2.1 Análisis del contexto organizacional

Para identificar el contexto de la organización en Geoconsult CS, se determinó las siguientes cuestiones externas e internas con el siguiente análisis DOFA.

Figura 12. Análisis DOFA



Fuente. Propia

Tabla 18. Partes interesadas.

CONTEXTO	PARTE INTERESADAS	NECESIDADES	EXPECTATIVAS
INTERNO	EMPLEADOS	**1.** Contar con una infraestructura tecnológica segura y rápida	**1.** Automatización de procesos
		2. Confidencialidad de la información entregada.	**2.** Realización de actividades de bienestar.
		3. Respuesta oportuna a requerimientos realizado al área de soporte de TI	**3.** Posibilidad de ascenso.
		4. Repuesta oportuna a requerimientos.	**4.** Mejoras salariales
	DIRECCIÓN	**1.** Información financiera integra y disponible.	**1.** Mejoras en los procesos que aumenten la utilidad del negocio.
		2. Información oportuna de la gestión de actividades.	**2.** Ausencia de conflictos jurídicos.
		3. Confidencialidad de la información.	**3.** Ampliación de la estructura del negocio.
		4. Cumplimiento de los requisitos legales aplicables.	**4.** Respuesta inmediata a requerimientos.
		5. Satisfacción de las necesidades y expectativas del cliente.	**5.** Certificaciones de los sistemas de gestión.
EXTERNO	GOBIERNO	**1.** Cumplimiento de los requisitos legales aplicables.	**1.** Cumplimiento de aspectos extralegales.
		2. Recepción de la información en los plazos requeridos.	**2.** Cero errores en la información entregada.
		3. Información recibida íntegra y verás.	**3.** Respuesta inmediata a requerimientos.
	CLIENTE	**1.** Cumplimiento de los requisitos contractuales.	**1.** Superar el cumplimiento de los requisitos contractuales.
		2. Cumplimiento de los indicadores.	**2.** Reducción constante de las PQR.
		3. Calidad en la prestación de los servicios.	**3.** Mayor automatización de las actividades.
		4. Satisfacción del usuario final.	**4.** Certificación de los sistemas de gestión.
		5. Efectividad en los tiempos de respuesta.	**5.** Respuesta inmediata a requerimientos.
	PROVEEDORES	**1.** Confidencialidad de la información suministrada.	**1.** Mejores canales de comunicación.
		2. Pago del producto y/o servicio en los plazos estipulados.	**2.** Participación en actividades para el mejoramiento conjunto.

Fuente. Elaboración Propia

4.2.1.1 Alcance del SGSI

Servicios de consultoría geocientífica, manejo de información y operación de centros de información técnica para la industria petrolera.

Excluye los siguientes controles:

A.6.2.2 Teletrabajo

A14.2.1 Política de desarrollo seguro

A14.2.6 Ambiente de desarrollo seguro

A14.2.7 Desarrollo contratado externamente

La justificación de las exclusiones de los anteriores controles del anexo A de la norma NTC-ISO-IEC 27001, se deben a que en ningún proceso o área de la empresa se realiza desarrollo de software, ni labores de teletrabajo. Para verificar la aplicabilidad y las exclusiones de cada control se debe consultar el anexo 1.

4.2.1.2 Política General del SGSI

Geoconsult CS realiza consultorías geocientíficas, manejo especializado de información y operación de centros de información técnica, en proyectos del sector energético y minero. Para cumplir nuestros objetivos de seguridad de la información contamos con talento humano preparado y competente; lo cual nos permite comprometernos con la satisfacción de nuestros clientes, la gestión segura de la información y el cumplimiento de los requisitos legales, contractuales y aplicables, garantizando las características de confidencialidad, disponibilidad e integridad.

Geoconsult CS reconoce que la seguridad de la información es un compromiso inherente a todos los procesos desarrollados y a cada uno de sus empleados. Su apropiada gestión tiene incidencia positiva en la calidad de la información y en la mejora continua de nuestros procesos y del sistema de gestión de la seguridad de la información.

4.2.1.3 Objetivos del SGSI

- Gestionar los riesgos de seguridad de la información, para que sean conocidos y según su impacto sean asumidos, transferidos, minimizados y/o eliminados de una forma documentada, repetible, eficiente y adaptada a los cambios que se produzcan en la empresa, el entorno y la tecnología.

- Fomentar en los empleados de Geoconsult CS las buenas prácticas y comportamientos seguros en el manejo de información.

- Realizar la correcta gestión de las acciones preventivas y correctivas que se deriven del reporte de eventos e incidentes de seguridad de la información.

- Proteger la información de nuestros clientes y la tecnología utilizada para su procesamiento, asegurando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.

- Asegurar el mejoramiento continuo del SGSI para responder a los cambios futuros.

4.2.2 Estructura organizacional en función de la SI

A continuación, se definen los roles y las responsabilidades para la seguridad de la información de las personas que intervienen en las diferentes áreas de Geoconsult CS, los cuales fueron definidos a partir del organigrama de la empresa (ver figura 4)

4.2.2.1 Definición de roles y responsabilidades

Tabla 19. Definición del rol y responsabilidades del presidente

PRESIDENTE	
DEPARTAMENTO: GERENCIAL **JEFE INMEDIATO: NINGUNO** **No. DE CARGOS IGUALES:** CERO	
RESPONSABILIDAD PRINCIPAL: Planear y controlar todas las actividades administrativas, financieras y del SGSI de la empresa.	
RESPONSABILIDADES GENERALES	**RESPONSABILIDADES CON EL SGSI**
Elaboración y proyección de presupuestos.	Realizar la revisión por la dirección al SGSI.
Cumplir y hacer cumplir las decisiones adoptadas por la Asamblea y la Junta Directiva.	Establecer y realizar revisión a las políticas y los objetivos de SI de la organización.
Representar a la empresa ante terceros, autoridades del orden administrativo o judicial, como representante legal de la empresa.	Analizar los datos arrojados por el SGSI y tomar las decisiones necesarias para garantizar el mantenimiento y mejoramiento del sistema.
Consecución de dinero, asegurando la disponibilidad de recursos.	Asignar los recursos necesarios a los procesos del SGSI.
Control de manejo de recursos.	Reportar e identificar los riesgos, incidentes o eventos de seguridad de la información.
Analizar las cotizaciones, informes y documentos para los clientes.	Velar por la eficaz comunicación al interior de la organización.
Presentar a la Junta Directiva, el informe semestral de actividades.	Garantizar el logro de la política y objetivos de Seguridad de la Información.
Planeación de mercado y Análisis de la competencia de la empresa.	Respetar y cumplir los principios básicos de seguridad de la información.

Fuente. Elaboración propia

Tabla 20. Definición del rol y responsabilidades del director de HSEQ

DIRECTOR HSEQ	
DEPARTAMENTO: HSEQ **JEFE INMEDIATO:** PRESIDENTE	**No. DE CARGOS IGUALES:** CERO
RESPONSABILIDAD PRINCIPAL: Verificar y coordinar el cumplimiento del funcionamiento de las Normas ISO, y OHSAS	
RESPONSABILIDADES GENERALES	**RESPONSABILIDADES CON EL SGSI**
Establecer los lineamientos y procesos referentes a implementación de Sistemas de Calidad, Ambiental, Salud Ocupacional y Seguridad Industrial.	Reportar e identificar actos y condiciones inseguras durante el desarrollo de las actividades.
Realizar el seguimiento a las acciones correctivas y preventivas generadas en la compañía.	Cumplir con el plan mínimo de capacitación definido en el SGSI.
Reportar e identificar los riesgos e incidentes que se generen en las actividades desarrolladas a su cargo.	Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
Elaborar informes mensuales sobre las actividades desarrolladas en ejercicio de sus funciones.	Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización
Velar por el buen funcionamiento del proceso de HSEQ	Implementar las mejoras identificadas en el SGSI

Fuente. Elaboración Propia

Tabla 21. Definición del rol y responsabilidades del Director Administrativo

DIRECTOR ADMINISTRATIVO	
DEPARTAMENTO: ADMINISTRATIVO **JEFE INMEDIATO: PRESIDENTE** **No. DE CARGOS IGUALES:** CERO	
RESPONSABILIDAD PRINCIPAL: Velar por el correcto uso y administración de los recursos de la compañía (Físicos y humanos).	
RESPONSABILIDADES GENERALES	**RESPONSABILIDADES CON EL SGSI**
Revisar y aprobar las órdenes de compra requeridas por la prestación del servicio.	Cumplir y hacer cumplir los principios de seguridad de la información en el procedimiento establecido para compras.
Elaborar los contratos del personal que lo requieran	Verificar que los nuevos candidatos cumplen con los perfiles de cargo diseñados.
Garantizar que las vacantes que se presenten sean cubiertas en el menor tiempo posible	Participar en la elaboración del programa de capacitación del SGSI y velar por su cumplimiento.
Velar por el cumplimiento del programa de capacitación.	Reportar e identificar actos y condiciones inseguras durante el desarrollo de las actividades.
Brindar al personal capacitación constante, y velar por el buen clima organizacional.	Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
Custodiar las hojas de vida.	Cumplir con el plan mínimo de capacitación definido en el SGSI.
Asegurarse que todo el personal que entra a laborar, cuenta con exámenes médicos de ingreso, afiliaciones, inducción y entrega de elementos de protección personal.	Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización.
Vigilar que los recursos físicos presentes en la empresa cumplen con parámetros de funcionamiento y seguridad.	Implementar las mejoras identificadas en el SGSI.

Fuente. Elaboración propia

Tabla 22. Definición del rol y responsabilidades del Director Comercial

DIRECTOR COMERCIAL	
DEPARTAMENTO: COMERCIAL **JEFE INMEDIATO: PRESIDENTE** **No. DE CARGOS IGUALES:** CERO	
RESPONSABILIDAD PRINCIPAL: Encargado de elaborar el plan comercial de la compañía y asegurar su sostenibilidad económica.	
RESPONSABILIDADES GENERALES	**RESPONSABILIDADES CON EL SGSI**
Seleccionar y formar al personal del departamento comercial, así como establecer una política de retribución e incentivos del personal.	Cumplir y hacer cumplir los principios de seguridad de la información en el procedimiento establecido para comercial.
Realizar supervisiones, seguimientos y asesoramiento del personal de ventas.	Reportar e identificar actos y condiciones inseguras durante el desarrollo de las actividades.
Elaborar los presupuestos de ventas y los presupuestos de gastos anuales del departamento adaptándolos y ajustándolos a los objetivos y recursos disponibles.	Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización.
Elaborar y estimar los objetivos comerciales.	Implementar las mejoras identificadas en el SGSI.
Generar demanda de los productos y/o servicios de la empresa, y establecer el plan de marketing, seguimiento y control de gastos del mismo.	Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Fuente. Elaboración propia

Tabla 23. Definición del rol y responsabilidades del director TI

DIRECTOR TI	
DEPARTAMENTO: TECNOLOGÍA **JEFE INMEDIATO:** PRESIDENTE **No. DE CARGOS IGUALES:** CERO	
RESPONSABILIDAD PRINCIPAL: Velar por el correcto uso y administración de los recursos informáticos de la compañía.	
RESPONSABILIDADES GENERALES	**RESPONSABILIDADES CON EL SGSI**
Coordinación y apoyo en labores de auditoría y consultoría, manejo de información, diseño y desarrollo de software, soporte de aplicaciones y mantenimiento e implementación de infraestructura tecnológica.	Generar el cronograma de mantenimiento de equipos
	Control del Inventarios de activos
	Participar en la elaboración del programa de capacitación del SGSI y velar por su cumplimiento.
	Cumplir con el plan mínimo de capacitación definido en el SGSI.
Coordinación y apoyo en el diseño, planeación e implementación de proyectos correspondientes al área de TI tanto corporativos como externos	Reportar e identificar actos y condiciones inseguras durante el desarrollo de las actividades.
Administración del área TI, responsable por la disponibilidad, desempeño, crecimiento y operación de la plataforma tecnológica, centro de datos y sistemas de comunicaciones de la compañía en Colombia y Ecuador; incluyendo la administración de hardware, software, acceso a recursos y el cumplimiento de los estándares corporativos a nivel tecnológico	Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
	Implementar las mejoras identificadas en el SGSI.
	Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización.

Fuente. Elaboración propia

Tabla 24. Definición del rol y responsabilidades del Soporte TI

SOPORTE TI	
DEPARTAMENTO: TECNOLOGÍA **JEFE INMEDIATO:** DIRECTOR TI	**No. DE CARGOS IGUALES:** DOS
RESPONSABILIDAD PRINCIPAL: Implementar procedimientos y técnicas para mejorar la eficiencia de la Red y el correcto funcionamiento de los equipos de cómputo bajo la supervisión del Gerente TI.	
RESPONSABILIDADES GENERALES	**RESPONSABILIDADES CON EL SGSI**
Realizar el mantenimiento preventivo de los equipos informáticos.	Completar las hojas de vida de equipos y actualizar el inventario de activos
Solucionar problemas relacionados con el hardware.	Cumplir con el cronograma de mantenimiento de equipos.
Instalar o supervisar instalación de hardware con el software de base necesario.	Implementar las acciones correctivas y preventivas.
Responder consultas relacionadas con el manejo de las aplicaciones a los usuarios.	Reportar e identificar actos y condiciones inseguras durante el desarrollo de las actividades.
Gestionar el estado y el acceso a la red y administrar restricciones y excepciones en base a la seguridad informática.	Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
Construcción de guías de ayuda y capacitar a personal no informático en el uso de las aplicaciones básicas	Cumplir con el plan mínimo de capacitación definido en el SGSI.
Respaldar la información importante de la compañía.	Implementar las mejoras identificadas en el SGSI.
Instalar y mantener antivirus locales en estaciones de trabajo.	Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización.

Fuente. Elaboración propia

Tabla 25. Definición del rol y responsabilidades del Líder de Seguridad de la Información

LÍDER DE SEGURIDAD DE LA INFORMACIÓN	
DEPARTAMENTO: TECNOLOGÍA **JEFE INMEDIATO:** DIRECTOR TI	**No. DE CARGOS IGUALES:** CERO
RESPONSABILIDAD PRINCIPAL: Verificar y coordinar el cumplimiento del funcionamiento de las Norma ISO27001:2013	
RESPONSABILIDADES GENERALES	**RESPONSABILIDADES CON EL SGSI**
Establecer los lineamientos y procesos referentes a la implementación y operación del SGSI.	Encaminar a la organización al cumplimiento de los requisitos de Seguridad de la Información exigidos por el cliente.
Realizar el seguimiento a las acciones correctivas y preventivas generadas en la compañía.	Planear, participar y realizar actividades de Seguridad de la Información que involucren a todo el personal de la compañía.
Reportar e identificar los riesgos e incidentes que se generen en las actividades desarrolladas a su cargo.	Ejercer seguimiento y control del SGSI, aplicando los correctivos y ajustes necesarios para el logro de los objetivos, informando a la alta dirección sobre el desempeño del sistema.
Elaborar informes mensuales sobre las actividades desarrolladas en ejercicio de sus funciones.	Emplear la información, los procedimientos, el talento humano y los recursos materiales y financieros para el desarrollo de las actividades del SGSI adecuadamente.
Asegurar que el SGSI sea conforme con los requisitos de la norma ISO27001	Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la organización.
Velar por el cumplimiento de los requisitos legales con respecto a la seguridad de la información	Cumplir con el plan mínimo de capacitación definido en el SGSI.
Implementar las mejoras identificadas en el SGSI.	Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Fuente. Elaboración propia

4.2.3 Definición de recursos

En el anexo 6 se presenta el presupuesto para el año 2020 destinado a la implementación del sistema de gestión de seguridad de la información.

4.3 Planificación del SGSI

4.3.1 Identificación y clasificación de los activos

A continuación, se presenta la identificación de los activos asociados con información en la organización Geoconsult CS.

4.3.1.1 Inventario de activos

Tabla 26. Identificación de activos

Nombre del Activo	Descripción General	Tipo de Activo	Objetivo Seguridad			Nivel de criticidad	Prioridad del Negocio	Responsable del Activo	Ubicación
			Confidencialidad	Integridad	Disponibilidad				
Documentación Proceso Comercial	Licitaciones, propuestas comerciales, propuesta económicas.	Información	A	M	M	7	2	Gerente Comercial	Servidor Eniac-01, Servidor geofs.
Documentación Proceso Compras	Solicitudes de compra, solicitudes de cotización a proveedores, órdenes de compra, remisiones de insumos.	Información	B	M	M	5	3	Directora Administrativa, Y/O Asistente Administrativa	Servidor Eniac-01, Servidor geofs, SIIGO y Archivo físico.
Documentación Proceso Consultoría	Informes, manuales, procedimientos, procesos, guías y/o formatos que se utilizan para la prestación del servicio	Información	A	A	A	9	1	Gerente del Proyecto	Servidor Eniac-01, Servidor geofs, Archivo físico

Nombre del Activo	Descripción General	Tipo de Activo	Objetivo Seguridad			Nivel de criticidad	Prioridad del Negocio	Responsable del Activo	Ubicación
			Confidencialidad	Integridad	Disponibilidad				
Documentación Proceso Gestión de Calidad	Procedimientos, registros, manuales, actas, control de documentos	Información	A	B	M	6	2	Director HSEQ	Servidor Eniac-01, Servidor geofs.
Documentación Proceso Gestión Humana	Hojas de vida, solicitudes de contratación, pruebas de habilidades, resultados de entrevistas, exámenes ingreso, nominas, información de contratación, evaluaciones de desempeños	Información	A	A	B	7	2	Directora Administrativa, Y/O Asistente Administrativa	Servidor Eniac-01, Servidor geofs, SIIGO y Archivo físico.
Documentación Proceso HSE	Información HSE, ausentismo laboral, programas de gestión, información psicolaboral, requisitos legales, solicitudes de exámenes.	Información	B	B	M	4	3	Director HSEQ	Servidor Eniac-01, Servidor geofs.
Documentación Proceso Informática	Inventario de activos TI, hojas de vida de los equipos y responsables, cronogramas de mantenimiento preventivo	Información	B	A	M	6	2	Gerente TI Y/O Soporte TI	Servidor Eniac-01, Servidor geofs.
Documentación Proceso Planeación Estratégica	Presupuestos, procedimientos de planeación estratégica, manual de sistema de Gestión Integral, matriz de objetivos, actas de designación.	Información	A	A	B	7	2	Presidente y Responsables de los procesos	Servidor Eniac-01, Servidor geofs, Archivo físico
Memoria Técnica Documental (MTD)	Informes finales, acuerdos de confidencialidad, contratos, cotizaciones, indicadores, instructivos, Informes de calidad, informe de avance, manuales, procedimientos, guías y formatos	Información	A	A	A	9	1	Dueño de la información	Servidor Eniac-01, Servidor geofs

Nombre del Activo	Descripción General	Tipo de Activo	Objetivo Seguridad			Nivel de criticidad	Prioridad del Negocio	Responsable del Activo	Ubicación
			Confidencialidad	Integridad	Disponibilidad				
	que se utilizan para la gestión del servicio de la información del cliente								
Conocimientos del Presidente	Representante de la empresa ante terceros, autoridades del orden administrativo o judicial, como representante legal de la empresa. Encargado de planear y controlar todas las actividades administrativas, financieras y del SGSI de la empresa. Además de realizar actividades de mercadeo y supervisión de compras.	Personas	A	A	A	9	1	Presidente	Oficinas de Geoconsult, Av. Dorado
Conocimientos Director Administrativo	Profesional Administrativo encargado de velar por el correcto uso y administración de los recursos de la compañía (Físicos y humanos)	Personas	A	A	A	9	1	Presidente	Oficinas de Geoconsult, Av. Dorado
Conocimientos Gerente comercial	Profesional encargado de establecer relaciones con potenciales clientes, buscar y presentar licitaciones, cerrar negocios con los clientes.	Personas	A	M	M	7	2	Director Administrativo	Oficinas de Geoconsult, Av. Dorado
Conocimientos Director TI	Profesional encargado por velar por el correcto uso y administración de los recursos informáticos de la compañía.	Personas	M	M	M	6	2	Director Administrativo	Oficinas de Geoconsult, Av. Dorado

Nombre del Activo	Descripción General	Tipo de Activo	Objetivo Seguridad			Nivel de criticidad	Prioridad del Negocio	Responsable del Activo	Ubicación
			Confidencialidad	Integridad	Disponibilidad				
Conocimientos Director HSEQ	Profesional encargado de establecer los lineamientos y procesos referentes a la implementación de Sistemas de Calidad, Ambiental, Salud Ocupacional y Seguridad Industrial.	Personas	M	M	M	6	2	Director Administrativo	Oficinas de Geoconsult, Av. Dorado
Conocimientos soporte TI	Técnico encargado de brindar asistencia y soporte preventivo/correctivo a los demás trabajadores de la oficina, así como a la plataforma tecnológica disponible	Personas	M	M	M	6	2	Gerente TI	Oficinas de Geoconsult, Av. Dorado
Conocimientos Líder de Seguridad de la Información	Profesional encargado de garantizar o propender la operación segura de la información para los flujos de trabajo que conforman la compañía y al SGSI.	Personas	M	M	M	6	2	Gerente TI	Oficinas de Geoconsult, Av. Dorado
Infraestructura física de procesamiento de información	Conjunto de elementos físicos que conforman la compañía, necesarios para su adecuado funcionamiento. (Sillas, mesas, escritorios, Aire acondicionado, etc.)	Infraestructura	A	B	B	5	3	Director Administrativo	Oficinas de Geoconsult, Av. Dorado
Hardware TI	Conjunto de componentes físicos tecnológicos, que trabajan o interactúan de algún modo con la computadora. (teclados, monitores, mouse, escáner, impresoras, enrutadores, lectoras, cámaras)	Infraestructura	B	B	A	5	2	Gerente TI Y/O Soporte TI	Oficinas de Geoconsult, Av. Dorado apliquen

Nombre del Activo	Descripción General	Tipo de Activo	Objetivo Seguridad			Nivel de criticidad	Prioridad del Negocio	Responsable del Activo	Ubicación
			Confidencialidad	Integridad	Disponibilidad				
Servidor Eniac-01	Computador conectado en la red donde se almacena toda la documentación de los procesos de la empresa.	Infraestructura	A	A	A	9	1	Gerente TI Y/O Soporte TI	Oficinas de Geoconsult, Av. Dorado
Servidor geofs	Computador conectado en la red con 12 discos duros de 2TB donde se respalda toda la información de la empresa	Infraestructura	A	A	B	7	2	Gerente TI Y/O Soporte TI	Oficinas de Geoconsult, Av. Dorado
Discos Duros de almacenamiento	Discos duros de almacenamiento temporal y/o de respaldo	Infraestructura	M	B	B	4	3	Gerente TI Y/O Soporte TI	Oficinas de Geoconsult, Av. Dorado
Equipo de Trabajo Siigo	Computador de escritorio donde se encuentra la herramienta SIIGO e información relativa de los procesos de Compras y Gestión Humana.	Infraestructura	A	A	B	7	2	Director Administrativo	Oficinas de Geoconsult, Av. Dorado
Estaciones de trabajo	Computadores de escritorio	Infraestructura	M	M	M	6	2	Soporte TI	Oficinas de Geoconsult, Av. Dorado
Portátiles	Computadores portátiles	Infraestructura	M	M	B	5	3	Soporte TI	Oficinas de Geoconsult, Av. Dorado
Licencias y software	Licencias, aplicativos y desarrollos utilizados para las labores propias de las áreas y servicios prestados por la empresa.	Infraestructura	A	M	M	7	2	Gerente TI Y/O Soporte TI	Oficinas de Geoconsult, Av. Dorado

Fuente. Elaboración propia

4.3.2 Identificación de vulnerabilidades

De acuerdo a la metodología propuesta en la sección 3, se realizó una identificación de vulnerabilidades sobre los procesos, personas y tecnología. En la columna F de la hoja 1 en el anexo 5 se presentan 13 vulnerabilidades detectadas en la organización Geoconsult CS, donde se destacan a nivel de infraestructura del edificio, deficiencias físicas en los tubos del edificio Torre Central donde se encuentra ubicada la oficina; a nivel de procesos se detectó en el área administrativa impresiones de información administrativa en papel químico que con el tiempo se tiende a borrar; y a nivel del personal se detectó un limitado conocimiento del nivel de sensibilidad de la información y una falta de capacitación en SI a los empleados de la empresa. Todas las vulnerabilidades fueron tratadas como riesgos, y se formuló un plan de tratamiento para su mitigación, ver anexo 3.

Con el fin de detectar una mayor cantidad de vulnerabilidades a nivel de tecnología se utilizó el software Microsoft Baseline Security Analizer 2.3, el cual fue instalado en un equipo conectado en la red, para así realizar una revisión completa de las estaciones y servidores que se encuentran activos. Para la realización de estas pruebas fue necesario contar con el apoyo del departamento de tecnología, encabezado por el Director TI.

4.3.2.1 Recolección de la información.

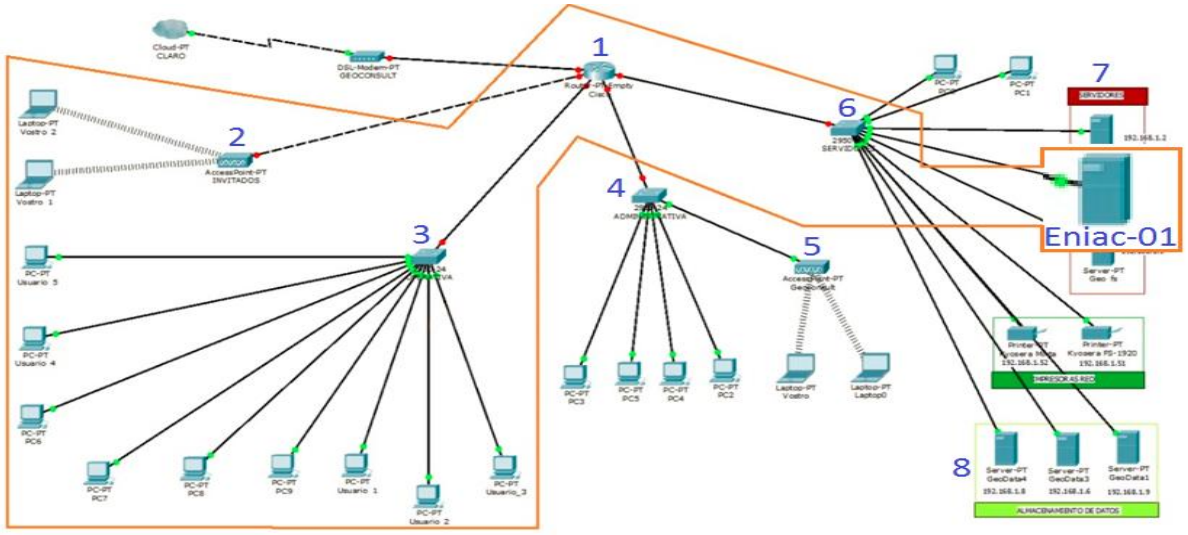
A continuación, se presentan los equipos activos de la red de Geoconsult CS, a la cual se le realizará la identificación de vulnerabilidades

Tabla 27. Lista de equipos para la identificación de vulnerabilidades

Computer Name	IP Address	Sistema Operativo
GEOCONSULTCS\GEO-04-0005	192.168.1.136	Windows 7
GEOCONSULTCS\GEO-04-0495	192.168.1.114	Windows 10
GEOCONSULTCS\GEO-04-0265	192.168.1.152	Windows 7
GEOCONSULTCS\GEO-03-0412	192.168.1.177	Windows 7
GEOCONSULTCS\GEO-04-0012	192.168.1.122	Windows 7
GEOCONSULTCS\GEO-04-0402	192.168.1.154	Windows 7
GEOCONSULTCS\ENIAC-01	192.168.1.4	Windows Server 2012

Fuente. Elaboración propia

Figura 13. Diagrama de red de la organización



Fuente. Geoconsult CS (2015)

4.3.2.2 Análisis de vulnerabilidades.

Con la ayuda del software Baseline Security Analyzer se realizó el escaneo en la red de Geoconsult CS encontrando vulnerabilidades de nivel tecnológico en el servidor de dominio y en algunos equipos de la red.

Se escogió esta herramienta de identificación de vulnerabilidades a nivel tecnológico, debido a que todos los equipos de la organización tienen Windows como sistema operativo instalado, es gratuita y está diseñada para identificar vulnerabilidades de nivel de seguridad informática en las pymes.

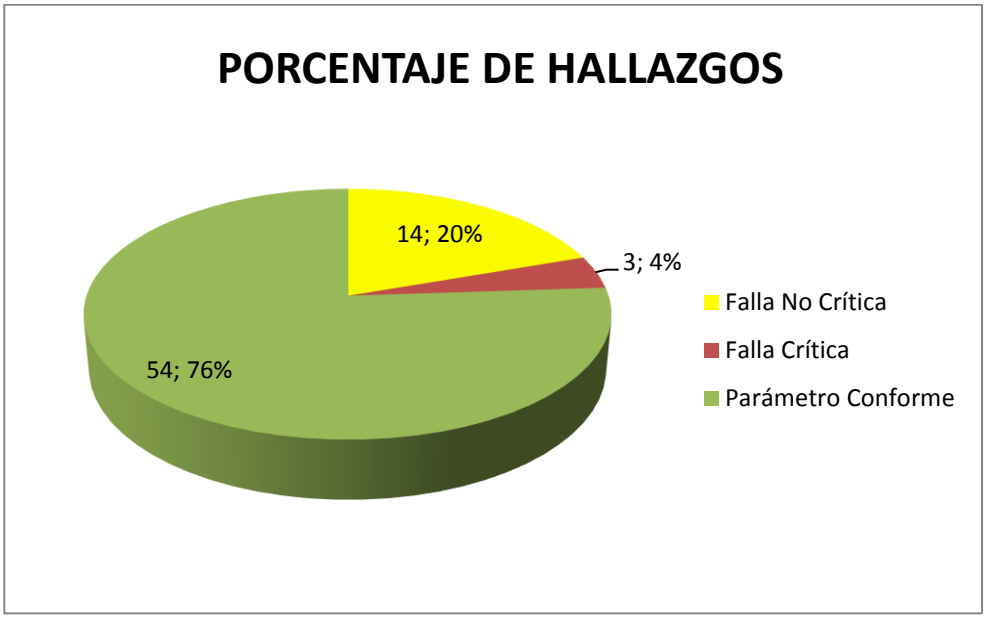
El análisis de las vulnerabilidades detectas a nivel de procesos, personas y locaciones físicas pueden ser consultadas en el anexo 3.

4.3.2.3 Resultados y vulnerabilidades.

Los resultados y las vulnerabilidades detectas a nivel de procesos, personas y locaciones físicas pueden ser consultadas en el anexo 3.

A continuación, se presentan las fallas detectadas una vez terminado el análisis de las vulnerabilidades a nivel tecnológico con el software de Baseline Security Analizar

Figura 14. Porcentaje de hallazgos detectados



Fuente. Propia

Fallas Críticas: A continuación, se presenta el detalle de las 3 fallas críticas detectadas en los equipos de la red de Geoconsult CS. Es importante mencionar que la herramienta identifica estas fallas, cuando el problema permite indisponibilidad de cualquier elemento en la infraestructura tecnológica, de la red o puede tomar control sobre alguno de estos con privilegios de administrador. Dentro de estos se puede encontrar ataques de denegación de servicio a algún servidor o ataques de ejecución de código arbitrario o malicioso que permite obtener privilegios en el servidor para su control.

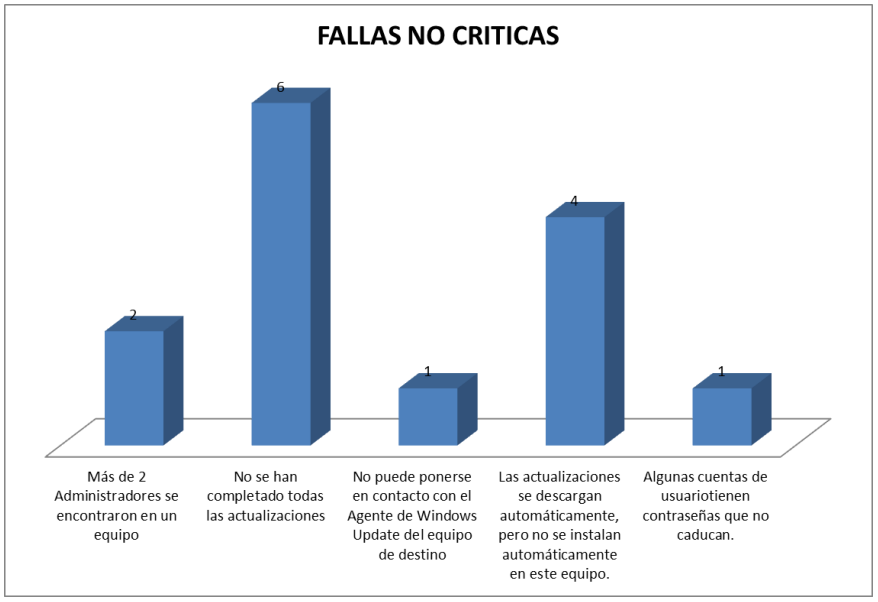
Tabla 28. Fallas críticas detectadas

Score	Computer name:	Issue	Result
Check failed (critical)	ENIAC-01	Automatic Updates	The Automatic Updates system service is not running.
Check failed (critical)	GEO-04-0495	Windows Security Updates	Security updates are missing.
Check failed (critical)	GEO-04-0495	IE Zones	Internet Explorer zones do not have secure settings for some users.

Fuente. Propia a partir de (Microsoft Baseline Security Analizer versión 2.3)

Fallas no críticas: En la siguiente gráfica se presenta el detalle de las 14 fallas No críticas detectadas en los equipos de la red de Geoconsult CS. Es importante mencionar que la herramienta de Microsoft Baseline Security Analyzer identifica estas fallas, cuando la vulnerabilidad permite obtener accesos o servicios no autorizados, pero sin llegar a la posibilidad de tomar control total de equipo ni obtener el rol de administrador del acceso o servicio. Por ejemplo, puertos inseguros que estén abiertos o contraseñas débiles que comprometen la confidencialidad de la información.

Figura 15. Fallas no críticas detectadas



Fuente. Propia a partir de (Microsoft Baseline Security Analizer versión 2.3)

4.3.2.4 Análisis de resultados y recomendaciones en la identificación de vulnerabilidades

La vulnerabilidad crítica sobre el servidor ENIAC-01 no es significativa, debido a que únicamente se identificó que en este no se encontraba habilitada la opción de actualizaciones automáticas para instalar los últimos parches de seguridad, lo cual está intencionalmente hecho por el director de TI para evitar reinicios del equipo inesperados y no controlados que puedan afectar la operación de la empresa. La instalación de las actualizaciones y parches de seguridad se realizan los sábados para no afectar la operación.

Sin embargo, sobre las vulnerabilidades No críticas, es necesario aplicar las actualizaciones y recomendaciones propuestas a continuación con el fin de dar cierre a las posibles amenazas.

- Es importante revisar la lista de miembros de los administradores locales y grupos de dominio Administradores para garantizar que todos los usuarios con autoridad administrativa estén justificados y autorizados.

- Es necesario involucrar a todas las áreas de la empresa para que trabajen con el departamento de tecnología, conocer su infraestructura tecnológica y adaptar las soluciones de seguridad a sus requerimientos y necesidades con el fin de lograr una sinergia totalmente referente al aseguramiento de la compañía.

- En el momento del aseguramiento de los recursos de la organización, una adecuada configuración de los diferentes dispositivos, servicios y aplicaciones le permite a la empresa solucionar en gran proporción las brechas de seguridad que estos presentan, disminuyendo así la probabilidad de un posible ataque por parte de terceros que aprovechen tal vulnerabilidad.

- Se deben generar políticas, estándares y procedimientos de seguridad de la información que definan los lineamientos de la organización para asegurar sus

sistemas, sin embargo, estas por sí solas no constituyen una garantía para la seguridad, por lo tanto, debe haber un esfuerzo conjunto en los buenos hábitos y en el compromiso de todo el personal de Geoconsult con la seguridad de la información.

- Las cuentas locales identificados en el informe de seguridad que tienen contraseñas que no caducan deben ser revisados para determinar por qué la opción está establecida y si deben ser eliminados.

4.3.3 Gestión de Riesgos de Seguridad de la Información

4.3.3.1 Procedimiento de Evaluación y Tratamiento de Riesgos

En el anexo 2 se presenta el procedimiento de análisis, valoración y tratamiento de riesgos de seguridad de la información

4.3.3.2 Identificación de Riesgos y Plan de Tratamiento

En el anexo 3 se presenta el registro de la identificación en Geoconsult CS de trece riesgos de seguridad de la información con su respectivo plan de tratamiento.

4.3.4 Definición de Políticas y Controles de Seguridad de la Información

4.3.4.1 Políticas de Seguridad de la Información

Con el fin de proporcionar a los empleados de Geoconsult CS, las bases conceptuales, los principios y acciones que deben conocer, entender y cumplir con el fin de proteger los activos y recursos informáticos para mitigar el riesgo de fuga o pérdida de Información restringida a continuación se presentan las políticas se seguridad de la información.

Política de Contraseña segura

Una vez el empleado de Geoconsult CS recibe su usuario y contraseña con el cual puede ingresar a su correo electrónico corporativo y directorio activo, debe proceder a cambiarla en su primer ingreso. Las siguientes son algunas indicaciones que deben seguir para crear contraseñas seguras, con el fin de evitar que personas no autorizadas tengan acceso a los sistemas de información de Geoconsult CS:

- Utilice contraseñas que no sean fáciles de adivinar.
- Construya contraseñas con una longitud mínima de ocho caracteres. Debe estar compuesta por letras, números, caracteres especiales que no sean consecutivos ni idénticos.
- Absténgase de usar el mismo nombre de usuario como contraseña.
- Memorice la contraseña: no la escriba
- Cambie la contraseña, mínimo cada 60 días o cuando sienta que la misma ha sido comprometida.
- Evite reutilizar contraseñas anteriores
- Absténgase de usar combinaciones obvias de teclado, como por ejemplo "qwerty"

Política de Uso de Controles Criptográficos

Se utilizarán controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión en memorias USB o discos duros de información restringida, fuera del ámbito del Organismo

Se recomienda utilizar el cifrado BitLocker que ya viene instalado en los equipos con Windows 10

Política de Seguridad con Sistemas Físicos

Los empleados de Geoconsult CS son responsables de custodiar y proteger tanto los elementos físicos como la Información contenida en ellos, teniendo en cuenta las siguientes recomendaciones para proteger dichos activos y su información:

- Absténgase de dejar descuidados y/o desatendidos los equipos de cómputo o elementos que estén bajo su custodia.
- Si tiene asignado un computador portátil, asegúrelo al escritorio con la guaya, teniendo en cuenta que su ubicación sea realmente segura y que no pueda ser retirada de forma fácil.
- Cada vez que se retire de su estación de trabajo bloquee la sesión.
- Al dejar su área de trabajo o al final del día apague su estación de trabajo.
- Cierre su oficina con llave si trabaja en una oficina cerrada y llévese la llave.
- Asegure los cajones que contengan información o recursos informáticos asignados a su cargo.
- Absténgase de realizar acciones riesgosas o inadecuadas tanto para su seguridad física como para la del elemento y la información contenida en él.
- Trasladar o mover los equipos en condiciones no seguras, exponiéndolos a daño o hurto.
- Continuar utilizando el equipo de cómputo, portátil, dispositivo móvil, tableta o cualquier otro elemento electrónico cuando se detecte o sospeche que el mismo se encuentre infectado por un virus.
- Abrir directamente o permitir a personas no autorizadas destapar los equipos, extraer, manipular y/o cambiar sus partes.
- Golpear o utilizar de forma inadecuada los equipos informáticos.

Política de Uso de Software Legal

Los empleados de Geoconsult CS solo podrán utilizar software legalmente adquirido y/o autorizado por la Empresa. Se puede hacer copia o duplicación de software licenciado por parte de los funcionarios, sólo cuando esta explícitamente permitido en los términos y condiciones de la licencia. Si un funcionario requiere instalar un software específico, debe tener la aprobación formal del área de tecnología, área que analizará las implicaciones a nivel de licencia y uso que este software pueda tener en la infraestructura de TI y soluciones de información.

De acuerdo a lo anterior el usuario del software, debe abstenerse de:

- Copiar, vender, regalar, distribuir o enajenar el software sin permiso del autor.
- Estimular, permitir, obligar o presionar a los empleados a crear o utilizar copias no autorizadas.
- Prestar los programas para que sean copiados.
- Ejecutar un programa en dos o más computadores simultáneamente, a no ser, que esté específicamente permitido en la licencia.
- Utilizar hardware o software de monitoreo de actividades (analizadores de protocolos, software catalogado como "hacking", etc.) sin la debida autorización.
- Utilizar aplicaciones que no sean debidamente autorizadas por el área de TI.
- Utilizar software o servicios de red que permitan el intercambio de información sin el debido aval y autorización por parte del área de TI.
- Utilizar software que permitan el control remoto sobre cualquier tipo de equipo conectado en la red de datos.
- Usar software o hardware que permita vulnerar o evadir los controles establecidos por Geoconsult CS
- No está permitido realizar modificaciones a los paquetes de software.

Política de Derechos de Autor

Geoconsult CS protege y exalta los Derechos de Autor tanto para las obras impresas como en la protección del software que utilizan sus empleados. Por ello, los siguientes son los lineamientos con relación a los derechos de autor:

- Usar únicamente software debidamente licenciado.
- En presentaciones, documentos, informes y demás documentos que utilicen los empleados para las labores de su cargo debe mencionarse la fuente de donde se extrajo la Información.
- Abstenerse de realizar copias parciales o totales de libros, artículos, reportes y otros documentos; que no estén permitidos por la ley de derecho de autor.
- La información de Geoconsult CS es propiedad de la Entidad, por lo cual, no puede ser utilizada para ningún fin diferente al establecido y requerido en la ejecución de las labores correspondientes a su cargo. Por lo tanto, no podrá ser utilizada como fuente de información para temas promocionales, comerciales, entre otros.

Política de Uso de Internet

Internet es una herramienta que entrega Geoconsult CS a sus empleados para adelantar exclusivamente las labores propias de sus cargos y debe ser utilizada de manera austera y eficiente. Por ello, los siguientes son los lineamientos del buen uso de esta herramienta:

- Abstenerse de ejecutar herramientas de hacking
- Abstenerse de colocar información de Geoconsult CS independientemente de su formato (Word, Excel, Power Point, pdf, avi, mp3, mp4 o cualquier otro formato actual o futuro) en sitios de internet o los denominados discos, carpetas virtuales o cualquier sistema de publicación de documentos, actual o futuro dentro o fuera de las instalaciones de Geoconsult CS.

- Abstenerse de publicar material que pueda ser considerado como inapropiado, ofensivo, racial, sexual o irrespetuoso a otros, y de igual manera no acceder a dicho tipo de material.
- Abstenerse de utilizar aplicaciones que permitan evadir los controles implementados por Geoconsult CS.
- El acceso a cualquier portal de internet con contenido inapropiado no se encuentra restringido, por lo cual es responsabilidad de cada empleado abstenerse de ingresar a páginas web para fines diferentes a los laborales.

Política de Uso de Correo Electrónico

Todos los empleados de Geoconsult deben tener en cuenta los siguientes lineamientos frente al uso de su cuenta de correo electrónico corporativa:

- La cuenta de correo corporativo asignada a cada empleado es para uso exclusivo de las labores propias del cargo. Por lo mismo, no está autorizado el reenvío de correos electrónicos ni de agendas del buzón de Geoconsult CS a cuentas de correo públicas como Gmail, Hotmail u otras. Recuerde que el uso de cuentas de correo público no está asegurado y la información que intercambie a través de este medio puede ser accedida por personas no autorizadas.
- No está permitido usar el correo electrónico para el envío de propagandas, ofertas, negocios personales, avisos publicitarios o cualquier otra información ajena a las labores que desempeña en su cargo.
- No está permitido el envío de correos con mensajes difamatorios, discriminatorios, de acoso o intimidación, imágenes o videos con contenido ilegal, racista, ofensivo, indecente, obsceno o con material sexual explícito.
- No está permitido el envío de correos masivos sin autorización.
- Todo correo electrónico de procedencia desconocida, llamado SPAM que sea recibido en los buzones de correo de Geoconsult CS debe ser eliminado, ignorado y reportado al área de soporte de TI con el fin de evitar posibles infecciones por código malicioso o virus. Geoconsult CS puede aplicar controles técnicos que prevengan la recepción de correos provenientes de estos individuos u

organizaciones. Es responsabilidad de los usuarios la no propagación de dichos correos a cuentas corporativas o personales.

- Antes de responder un correo electrónico, valide si requiere incluir el historial del mismo. Enviar este historial sin validar si el remitente requiere o no tener conocimiento del mismo puede estar exponiendo información restringida a personas no autorizadas.
- Absténgase de usar el correo electrónico como una herramienta de mensajería instantánea.
- Recuerde que los mensajes de correo electrónico revisten la misma fuerza probatoria ante la Ley colombiana como la tienen los documentos impresos.

Política de escritorio y pantalla limpia

Geoconsult CS garantiza que los colaboradores y partes interesadas, que tengan acceso a las instalaciones físicas de la empresa, sistemas de información y equipos de compito, mantenga sus escritorios libres de documentos o dispositivos de almacenamiento, guardándolos en sitios seguros, después de la jornada laboral o cuando no estén siendo utilizados. Adicionalmente no se permite tener accesos directos de información sensible en el escritorio del computador y el usuario debe bloquear sesión cuando se ausente de su puesto de trabajo y/o deje el equipo desatendido, para proteger el acceso a la documentación digital, aplicaciones y servicios de la empresa.

4.3.4.2 Declaración de Aplicabilidad

De acuerdo al diagnóstico realizado en la organización Geoconsult de todos los requerimientos de los 114 objetivos de control y controles del anexo A de la norma NTC-ISO-IEC 27002:2013, se generó el Anexo 1 “Estado de cumplimento del anexo A de la Norma ISO/IEC 27001:2013 en la organización Geoconsult CS” el cual corresponde a la fuente inicial de la declaración de aplicabilidad, ya que este se encuentran las exclusiones y todos los controles actuales que presenta la organización para demostrar su cumplimiento.

5 CONCLUSIONES Y RECOMENDACIONES

5.1.1 Recomendaciones

La organización Geoconsult CS, únicamente cuenta con unas políticas de seguridad de la información en el proceso de TI, las cuales están enfocadas a controles de acceso físico y lógico. Pero no cuenta con políticas que protejan los activos de la información en los demás procesos de la compañía. Se recomienda definir un conjunto de políticas para la seguridad de la información que aplique a todas las áreas, sean aprobadas por la dirección, publicadas y comunicadas a todos los empleados y partes externas pertinentes.

Geoconsult CS no tiene definido ningún lineamiento para el uso adecuado de los dispositivos móviles en ningún documento. El único control identificado es una guaya de seguridad para portátiles. Se recomienda implementar controles criptográficos para proteger las memorias USB, discos duros y celulares en los que se almacene información de la empresa. Para los equipos que tienen Windows se puede utilizar la herramienta BitLocker que ya viene instalado en este sistema operativo

Geoconsult CS no cuenta con un programa de formación y toma de conciencia en seguridad de la información, se recomienda que todos los empleados de la organización, y en donde sea pertinente, reciban la educación y la formación apropiada sobre las políticas y procedimientos de la organización pertinentes para su cargo, los principios de seguridad de la información y las responsabilidades y deberes que tienen como usuarios y dueños de procesos dentro del SGSI.

Geoconsult CS no tiene establecido un procedimiento formal donde se detallen las actividades y responsables para emprender acciones contra empleados que hayan cometido alguna violación a la seguridad de la información, se recomienda incluir este procedimiento dentro del reglamento interno de trabajo.

La organización Geoconsult CS no cuenta con una guía de responsabilidades de los usuarios en el acceso, uso de los activos de información y recursos informáticos de la

compañía. Se recomienda realizar un procedimiento donde se reglamente el uso de los recursos de información tales como y sin limitarse a: computadores personales, impresoras, sistemas de información, redes, software y sus licencias, correo electrónico, Internet e información confidencial de cada área.

En Geoconsult CS, no se evidencia un documento que establezca una clasificación y un etiquetado de los activos de información. Se identificó solamente la marcación con un código de barras a los equipos informáticos, pero la información impresa no cuenta con ninguna clasificación, no obstante, al interior de la organización si se tiene identificado cual es la información más importante en función de su criticidad. Se recomienda establecer tres niveles de clasificación como confidencial, interna y publica.

En la organización no se identifica que los sistemas de información aseguran la calidad de las contraseñas de ingreso. Se recomienda que todos los equipos de la empresa se encuentran dentro de un dominio, lo cual permitirá una correcta gestión de contraseñas, debido a que el sistema asegura que el usuario tenga una contraseña de calidad. Adicionalmente se podrán implementar controles por dominio como bloqueo de sesión por inactividad, y bloqueos de puertos USB a las personas que no tenga autorización.

En Geoconsult CS, únicamente el director TI, o el personal administrativo encargado son los únicos autorizados para permitir las salidas de equipos o información. Pero no se identifican controles sobre los equipos que ingresan. Se recomienda llevar un control físico de entrada y salida de activos de información.

Geoconsult CS cuenta con un procedimiento en el área informática PM-TI-001 donde se detallan las actividades de Copias de Respaldo, en la cual se realiza una copia diaria del servidor donde se almacena toda la información de la empresa en el mismo servidor. Se recomienda hacer un *backup* periódico en un lugar distinto al servidor de información, y se ubique en un lugar diferente al cuarto de equipos.

Geoconsult CS no cuenta con controles de seguridad para proteger la mensajería electrónica. Se recomienda implementar una renuncia de responsabilidad debajo de la

firma en los correos, y políticas formales para la transferencia de información, que incluya protección con contraseña de la información que sea confidencial.

Geoconsult CS no tiene establecido, documentado ni implementado una guía sobre el mecanismo propuesto a seguir, cuando se presente un incidente que potencialmente pueda afectar y generar una interrupción en la operación del servicio. Se recomienda establecer un plan de continuidad y recuperación ante desastres, y que estos sean probados mínimo cada 6 meses, con el fin de garantizar que la compañía entienda claramente como debe ser ejecutado.

Geoconsult CS dentro de su sistema de Gestión Integral tiene definido los requisitos de legislación y contractuales aplicables con su cliente, pero no se ha identificado en la matriz de requisitos legales los aspectos contractuales de seguridad de la información. Se recomienda elaborar una matriz tanto con los requisitos contractuales y legales l relacionados con los derechos de propiedad intelectual, protección de datos personales y el uso de productos de software patentados

Con base en el avance realizado en la aplicación del modelo propuesto de un sistema de gestión de seguridad de la información en Geoconsult CS, se propone el siguiente plan de acción, con las siguientes acciones y actividades a realizar para la implementación completa del SGSI y obtener la certificación en la norma ISO27001 en los siguientes 6 meses:

Tabla 29. Plan de acción, actividades y cronograma

Implementación completa de un modelo de un SGSI en Geoconsult.			**Semanas de Ejecución**	**Tiempo del proyecto en meses (6 meses)**																							
Fase	**Actividades a desarrollar**			**Mes 1**				**Mes 2**				**Mes 3**				**Mes 4**				**Mes 5**				**Mes 6**			
Fase 1 Diagnóstico inicial	1	Comunicar el estado actual de la Gestión de Seguridad identificado en este documento	1																								

Implementación completa de un modelo de un SGSI en Geoconsult.			Semanas de Ejecución	Tiempo del proyecto en meses (6 meses)																															
Fase	Actividades a desarrollar			Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6												
	2	Realizar las correcciones propuestas a la información existente.	1																																
	3	Socializar los resultados del cuestionario realizado en este documento con respecto al estado de cumplimiento de lo requerido por la norma.	1																																
Fase 2 Preparación del SGSI	4	Culminar las actividades del análisis del contexto de la organización	0.5																																
	5	Identificar todas las expectativas de las partes interesadas, especialmente las internas	0.5																																
	6	Aprobar el alcance y los objetivos del SGSI por parte de la dirección	1																																
	7	Aprobar por parte de la dirección la estructura	0.5																																

Implementación completa de un modelo de un SGSI en Geoconsult.			Semanas de Ejecución	Tiempo del proyecto en meses (6 meses)																							
Fase	Actividades a desarrollar			Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6			
		organización con respecto a la SI																									
Fase 3 Planificación del SGSI	8	Determinar los roles y responsabilidades en el SGSI que no hayan sido identificados en este documento.	0.5																								
	9	Aprobar por parte de la dirección la política general del SGSI	1																								
	10	Identificar los activos de información	2																								
	11	Identificar, valorar los riesgos de SI por parte de los dueños de los procesos	3																								
	12	ejecutar los planes de acción para tratar los riesgos de SI	1																								
	13	Elaborar procedimiento para la gestión de incidentes	1																								
	14	Definición de políticas de SI en todos los procesos	1																								

Implementación completa de un modelo de un SGSI en Geoconsult.			Semanas de Ejecución	Tiempo del proyecto en meses (6 meses)																							
Fase	Actividades a desarrollar			Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6			
	15	Definición del Plan de Continuidad de la organización	1																								
	16	Elaboración de la declaración de aplicabilidad	5																								
Revisión y seguimiento	17	Realizar la auditoria interna	1																								
	18	Realizar la revisión por la dirección al SGSI	1																								
	19	Cerrar los hallazgos respectivos	1																								
	20	Realizar auditoria de certificación	1																								

Fuente. Elaboración propia

5.1.2 Conclusiones

En este proyecto se planteó un modelo para un sistema de gestión de seguridad de la información que aplica de una forma adecuada a todos los procesos actuales de una organización y a corto plazo servirá como base para su implementación y posterior certificación en la norma NTC-ISO-IEC 27001:2013. Dicho modelo puede aplicarse a cualquier empresa sin importar su sector o tamaño, con el fin de cumplir requisitos legales, obtener una ventaja competitiva o simplemente como una decisión gerencial para proteger sus activos de información.

El modelo presentado es totalmente ajustable a una nueva actualización de la norma ISO27001 y es compatible con estándares como COBIT e ITIL. Por tanto, le permite responder de una manera eficaz a los cambios tecnológicos y a las nuevas amenazas que se puedan generar. Adicionalmente, dados todos los elementos que lo componen puede ser la base para establecer un gobierno de tecnologías de la información en cualquier organización.

El modelo de un Sistema de Gestión de Seguridad de la Información es un elemento clave dentro del plan estratégico de cualquier organización, especialmente en las empresas del sector petrolero, financiero y de tecnologías de la información. Debido a que más allá, de cumplir requisitos contractuales y proteger sus activos, le permite obtener un valor diferenciador dentro de la operación de sus servicios, incrementa la percepción positiva de la imagen de la empresa, mejora los procesos y disminuye costos.

Se logró el cumplimiento de todos los objetivos planteados inicialmente, diseñando un modelo de un sistema de gestión de la seguridad de la información compuesto por tres fases fundamentales. En la fase 1 se especifica la realización de un diagnóstico inicial del SGSI; en la fase 2 se realiza la preparación del SGSI, el cual se compone por la identificación del contexto de la organización, las expectativas de las partes interesadas, los límites, la política general, el alcance y la estructura organización con respecto a la seguridad de la Información; y en la fase 3, llamada la planificación del SGSI, se realiza la identificación, valoración y tratamiento de los riesgos de SI, la

identificación de las vulnerabilidades, la tipificación de los activos y la implementación de las políticas y los controles necesarios en la operación del SGSI.

Por otra parte, para obtener resultados más precisos en la identificación de vulnerabilidades se deben considerar ataques por códigos maliciosos, ingeniería social y ataques de denegación de servicios. Lo cual permitirá identificar más riesgos, e implementar controles y políticas más adecuadas.

Un adecuado análisis del contexto de la organización es un aspecto fundamental dentro de las primeras actividades en la implementación de un sistema de gestión de seguridad de la información, debido a que se determinan las cuestiones externas e internas que pueden afectar los resultados previstos del SGSI. En este análisis, se deben evaluar las necesidades y expectativas de clientes, competidores, proveedores y personal interno. Adicionalmente se deben evaluar las condiciones físicas de los alrededores de la organización y considerar todos estos aspectos como una fuente en la identificación de riesgos.

El liderazgo y compromiso por parte de la dirección es fundamental en la implementación de un sistema de gestión de seguridad de la información, ya que son ellos quienes aseguran que se establezca un alcance adecuado, se genere la política integral y los objetivos de la seguridad de la información. Y adicionalmente otorgan los recursos necesarios y aseguran la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización. Por lo cual un SGSI que no cuente con el apoyo de la dirección está destinado al fracaso.

Los datos obtenidos en la aplicación del modelo propuesto en la organización Geoconsult CS han permitido determinar que la fase de diagnóstico y planificación del SGSI fue todo un éxito y se formuló correctamente. Principalmente, para analizar el estado actual de la organización, definir los activos de información y definir una adecuada gestión de riesgos. No obstante, se ha identificado que esta última fase está sujeta a mejoras en una mayor identificación de vulnerabilidades de todos los procesos de la organización y no solamente de TI.

En la realización del diagnóstico se presentaron dificultades en las entrevistas con los dueños de los procesos, ya que veían esta etapa como una auditoria, e intentaban ocultar la situación actual de sus áreas para evitar llamados de atención. Razón por lo cual fue necesario realizar una reunión con la dirección de la empresa, donde se explicó la intención los objetivos del diagnóstico, se infundo la iniciativa de mejorar todas las áreas y proteger los activos de información de la empresa.

El proceso de aplicación del modelo en la organización Geoconsult CS estaba diseñado para realizarse aproximadamente en seis meses, pero el tiempo real de implementación de este modelo tardó aproximadamente ocho meses, debido a que la fase de diagnóstico fue más larga de lo esperado. Es importante considerar en una próxima aplicación del modelo, el tamaño de la organización y la cantidad de áreas que compone la empresa en el cálculo de tiempos de ejecución del diagnóstico.

En este documento se presentaron los elementos fundamentales que debe tener un modelo de un sistema de gestión de seguridad de la información, las principales amenazas, riesgos, mejores prácticas y referentes mundiales. No obstante, este modelo es sensible a una mejora continua. Para una próxima versión se puede incluir en la fase 2 la elaboración de un plan de entrenamiento y capacitación; y con respecto a la fase 3 se puede desarrollar un plan de continuidad.

6 REFERENCIAS

Areito J. B. (2008). Seguridad de la Información, Redes, Informática y Sistemas de Información. Colombia. Paraninfo.

Baud, J. L. (2015). Preparación para la certificación ITIL Foundation V3. España. Ediciones ENI.

Benavides, M. L. (2012). Módulo Riesgos y Control Informático. Pasto: UNAD.

Cano, J. (2011). Gerencia de la Seguridad de la Información. Evolución y Retos. ISACA Journal 5.

Costas, S. J. (2011). Seguridad Informática. España. Editorial Ra-MA.

El tiempo. (01 de junio de 2017). Eltiempo.com. Obtenido de http://www.eltiempo.com/archivo/documento/CMS-15867464.

Gartner. (2016). https://www.ituser.es/seguridad. Obtenido de https://www.ituser.es/seguridad/2016/12/las-empresas-destinan-un-56-de-su-presupuesto-de-ti-a-la-seguridad

Geoconsult CS. (2018). Manual del Sistema de Gestión Integral de Geoconsult CS. Colombia.

Geoconsult CS. (2015). Manual de Calidad de la organización. Colombia.

Gómez. A. (2007). Enciclopedia de la seguridad informática. México. Editorial Alfaomega

Gómez. V. A. (2011) Seguridad Informática Básica. Colombia. Ediciones ECOE.

Hernández, R. Sampieri. (2010) Metodología de la investigación. México. McGraw Hill.

ICONTEC. (2013). *Norma Técnica Colombiana NTC-ISO-IEC 27001 Técnicas de Seguridad y Requisitos para un Sistema de Gestión de Seguridad de la Información*. Colombia.

ICONTEC. (2013). *Norma Técnica Colombiana NTC-ISO-IEC 27002 Técnicas de Seguridad, Código de Práctica para Controles de Seguridad de la Información*. Colombia.

ICONTEC. (2013). *Norma Técnica Colombiana NTC-ISO-IEC 27005 Técnicas de Seguridad, Gestión de Incidentes de Seguridad de la Información*. Colombia.

ICONTEC. (2013). *Norma Técnica Colombiana NTC-ISO-IEC 27035 Técnicas de Seguridad, Gestión de Riesgos de Seguridad de la Información*. Colombia.

Instituto Ponemon. (2016). Modelo de Costos de Ponemon. Global Analysis.

ISOTools. (2017). *https://www.pmg-ssi.com. Obtenido de https://www.pmg-ssi.com/2017/09/situacion-norma-iso-27001-sudamerica/*

KIM, D., & SALOMON, M. G. (2012) Fundamentals of Information System Security. United States of America: Jones & Bartlett Learning International.

Ministerio de Defensa Nacional Policial de Colombia. (01 de 10 de 2017). Obtenido de https://caivirtual.policia.gov.co: https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico.

Mirk, S. (2015). File Data Recovery Secrets Tips and Tricks for Recovering Data. USA: Lulu Press.

Revista Semana. (28 de 12 de 2017). *El cibercrimen en 2017: la amenaza crece sobre Colombia*. Obtenido de https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979

Sena (2015) Activos de información y normatividad de la seguridad informática. Colombia.

Surhone L, (2011), Lambert M Surhone, Mariam T Tennoe, Susan F Henssonow. USA, Betascript Publishin.

Unidad de Delitos Informáticos de la Dijin, Panda Security, Microsoft. (2016). Eltiempo.com. Obtenido de http://www.eltiempo.com/archivo/documento/CMS-16493604

Universidad EAFIT. (2007). Boletín 54 Área de auditoría y control. Colombia.

LISTA DE ANEXOS