DISEÑO DE UN SGSI PARA EL ÁREA DE AUTOMATIZACIÓN DEL PROCESO DE BÁSCULA, DE LA EMPRESA MINERA SANOHA LTDA UBICADA EN NOBSA –BOYACÁ

ING. YENNY STELLA NÚÑEZ ÁLVAREZ
Cód. 23.810.642

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS, BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SOGAMOSO- BOYACÁ
2015

DISEÑO DE UN SGSI PARA EL ÁREA DE AUTOMATIZACIÓN DEL PROCESO DE BÁSCULA, DE LA EMPRESA MINERA SANOHA LTDA UBICADA EN NOBSA –BOYACÁ

ING. YENNY STELLA NUÑEZ ALVAREZ
Cód. 23.810.642

Monografía como Trabajo de Grado presentado ante la Escuela de Ciencias Básicas, Tecnología e ingeniería (ECBTI) como parte de los requisitos para optar al Título Académico de Especialista en Seguridad Informática.

Director de Proyecto
MSC. ARMANDO ARÉVALO MURILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS, BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SOGAMOSO- BOYACÁ
2015

Nota de Aceptación:

_____

_____

_____

_____

Firma del Presidente Jurado

_____

Firma del Jurado

_____

Firma del Jurado

SOGAMOSO DIA: MES: AÑO: 2015

DEDICATORIA

Este triunfo fue posible gracias a Dios y a la Virgen que me fortalecieron espiritualmente.
A mis padres porque me apoyan en todos los aspectos de mi vida.
A mi incondicional esposo porque es mi centro y el mayor critico de mi trabajo.
A mis hijos porque llenan de amor y energía mi vida haciendo que nunca desfallezca y hacen que sean mi inspiración siempre.
A mi amiga Mónica Hernández por su amistad, colaboración y conocimiento en los procesos de SANOHA apoyando mi investigación y desarrollo del presente proyecto.

AGRADECIMIENTOS

A las directivas de SANOHA LTDA por permitirme desarrollar mi proyecto en base a sus procesos y brindarme su apoyo para desarrollar las diferentes actividades que dieron como producto el presente proyecto.

A la Ingeniera Mónica Hernández Báez Jefe de la División de sistemas, por su conocimiento, experiencia, orientación y supervisión en todos los procesos relacionados de Sanoha Ltda.

A mi director de proyecto, MSC. Armando Arévalo, por su excelente acompañamiento, su conocimiento, críticas objetivas y observaciones que fortalecieron mi proceso de aprendizaje y la construcción de este proyecto.

A la Universidad Nacional Abierta y a Distancia UNAD, por brindarme profesionales calificados y muy competentes para mi formación como Especialista en Seguridad informática.

A todas aquellas personas que directa e indirectamente brindaron su conocimiento y experiencia en las áreas relacionadas con la investigación y diseño del presente proyecto.

Para todos, Muchas gracias y Mil bendiciones

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTADO DE TABLAS

LISTA DE ANEXOS

RESUMEN

El proyecto permite conocer el contexto de la empresa Sanoha Ltda, revisando sus diferentes áreas y procesos con el objetivo de diseñar un SGSI que apoye los diferentes procedimientos y actividades allí efectuados, facilitando el análisis de riesgos a los que se ve expuesta la información en el caso particular del área de automatización del proceso de báscula, donde se busca poder asumir, minimizar y controlar amenazas que pueden estar presentes en el sistema informático, mediante estrategias y planes definidos, documentados y conocidos para ser revisados y ser actualizados constantemente, con el uso de una metodología que permitiera indagar como era su funcionamiento y la incidencia directa e indirecta sobre el medio operativo de la empresa, ya que de esta depende la productividad y el quehacer de Sanoha Ltda como empresa minera y que basa sus procesos en el suministro, pesaje y remisión de material (carbón).

El desarrollo del proyecto está basado en la normativa de gestión de seguridad ISO 27001, específicamente la Norma vigente ISO/IEC 27001:2013 la cual especifica los dominios, objetivos y controles a tener en cuenta al momento de implantar un sistema de gestión de seguridad. La metodología empleada fue PHVA o PDCA (Planificar, Hacer, Verificar y Actuar) utilizada en el diseño de sistemas de gestión y mejora continua de calidad, además permite lograr un mejor nivel de calidad administrativa y de servicios con el objetivo de perfeccionarlos y continuar en un proceso de mejora continua.

El Diseño del SGSI fue elaborado con el fin proporcionar un conjunto de actividades de gestión que deben realizarse mediante procesos sistemáticos enfocados en el proceso de automatización de báscula, proceso que influye en la continuidad negocio y del funcionamiento de los demás procesos dentro de la empresa. Su objetivo no está orientado a garantizar la seguridad sino a generar políticas y controles para que los riesgos de la seguridad de la información para que sean conocidos, asumidos, gestionados y minimizados por la empresa Sanoha Ltda, de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la misma, los riesgos, el entorno y las tecnologías.

La estructura del proyecto se desarrolla en primer lugar el capítulo 5 con un marco de referencia que describe teóricamente un SGSI, la normatividad que especifica los estándares de implementación del mismo, hace un paralelo entre la norma ISO/IEC 27001:2005 y la ISO/IEC 27001:2013 y los conceptos necesarios para comprender el contexto del proyecto. El capítulo 6 y 7 se explican los mecanismos de recolección de información y la metodología empleada y sus ventajas. El capítulo 8 abarca análisis y recopilación exhaustiva de los procesos del área de automatización de báscula, haciendo una breve reseña de la empresa, el sistema organizativo enfatizando en la división de sistemas y el departamento de Acopio y

Abastecimiento, este último responsable del manejo del área de automatización del proceso de báscula que está basado en la utilización del software a medida denominado SIRMAB(Base de datos que registra todos los proceso efectuados en bascula y es compartido en la red según perfiles de usuario). También se describen los procesos que intervienen en esta área y su funcionamiento. Además de mencionar el sistema informático actual de Sanoha Ltda. El capítulo 9 se identifica y valora las vulnerabilidades y amenazas de acuerdo a los activos identificados. El capítulo 10 se evalúa los riesgos. El capítulo 11 se genera un modelo de gestión según la norma y por último en el capítulo 12 se recomienda un plan de acción según los riesgos más relevantes y que tienen un mayor nivel de prioridad.

ABSTRACT

The project allows to know the context of the company Sanoha Ltda, checking its different areas and processes with the goal of designing an ISMS that supports the different procedures and activities conducted there, easing the analysis of risks that information is exposed in the particular case of the area of automation of scale process, which seeks to assume, to minimize and control the threats that may be present in the computer system, through strategies and defined plans, documented and known to be reviewed and constantly updated, using a methodology that allows to investigate how its performance was and the direct and indirect impact on the operating environment of the company, since it depends on productivity and work of Sanoha Ltda as mining company and its processes are based on the supply, weighing and remission of material (coal)

The project is based on the rules of security management ISO 27001, specifically the current standard ISO / IEC 27001: 2013 which specifies the domains, objectives and control to take into account when implementing a system of safety management. The methodology used was PDCA (Plan, Do, Check and Act) used in the design of management systems and the continuous quality improvement, it also allows to achieve a higher level of management quality and service in order to perfect and continue a process of continuous improvement.

The design of the ISMS was developed in order to provide a set of management activities that must be done through systematic processes focused in the automation of the scale, a process that influences in the business continuity and performance of the other processes inside the company. Its goal is not geared to guarantee safety but to generate policies and controls for the risks of information security to be known, assumed, managed and minimized by the company Sanoha

Ltda, a documented, systematic, structured, continuous, repeatable, efficient and adapted to the changes that occur in it, the risks, the environment and the technology.

The project structure is developed first on chapter 5 with a reference framework that describes theoretically an ISMS, the regulations that specify the implementation standards thereof, a parallel is done between the normative ISO / IEC 27001: 2005 and ISO / IEC 27001: 2013 and the concepts needed to understand the context of the project. In the Chapter 6 and 7 mechanisms for data collection and methodology and its advantages are explained. On Chapter 8 includes exhaustive analysis and collection of the processes of the scale automation area, with a brief overview of the company, the organizational system emphasizing t on the Systems Division and the Department of Storage and Supply, the latter responsible for managing of the area of automation of process scale that is based on the use of custom software called SIRMAB (A database that records all process conducted in scales and is shared on the network according to user profiles). It is also described the processes that involve in this area and its performance. In addition to mentioning the current Sanoha's Ltda computer system. On Chapter 9 it is identified and assessed the threats and vulnerabilities according to the identified assets. On Chapter 10 the risks are assessed. On Chapter 11, a management model is generated according to the standard and finally on chapter 12 an action plan is suggested according to the most significant risks which have a higher level of priority.

INTRODUCCIÓN

Las organizaciones adaptan sus procesos industriales, comerciales, logísticos y de servicios a la tecnología de la información y la comunicación como medios de expansión proporcionándoles la reducción de tiempos y tareas. Sin embargo no es suficiente limitar la seguridad informática a la configuración de robustos firewalls o adquirir costosos mecanismos de seguridad , sino que se debe buscar que los sistemas informáticos tengan la mejor inversión costo-beneficio y que no sean blanco fácil de intrusos en los que se vean expuestos a amenazas internas y externas que comprometan la información confidencial , gestionando de forma eficaz los parámetros, estándares, planes, controles e implantaciones necesarias que garanticen la seguridad de los datos y mensajes que frecuentemente se trasmiten en las redes corporativas e internet, evitando gastos innecesarios, ineficientes o mal dirigidos y poder contrarrestar de manera razonable amenazas y riesgos , garantizándose simultáneamente una respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio. Con un SGSI, las organizaciones conocen los riesgos a los que está sometida su información y de esta manera tener la ventaja de poder asumirlos, minimizarlos y controlarlos mediante una gestión definida, documentada y conocida por todos, que se revisaría y se actualizaría constantemente . Es decir a través del SGSI se proporciona un conjunto de objetivos, políticas, procedimientos y acciones que se implementarían para identificar, medir, vigilar, limitar, informar y revelar los riesgos a que se encuentre expuesta sus sistemas informáticos . Un SGSI establece un completo plan de acciones que colaboran a solucionar los problemas de seguridad técnicos, organizativos y legislativos mediante el análisis de riesgos, mejorando y manteniendo la seguridad de la información corporativa y garantizando una continuidad de negocio.

1. TITULO

Diseño de un SGSI para el área de automatización del proceso de báscula, de la empresa minera SANOHA LTDA ubicada en Nobsa –Boyacá

2. DEFINICIÓN DEL PROBLEMA

2.1 FORMULACIÓN DEL PROBLEMA

¿Cómo gestionar eficazmente la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal dirigidas y poder contrarrestar amenazas y riesgos, para garantizar una respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, en el área automatización del proceso de báscula de la empresa minera Sanoha Ltda. Ubicada en Nobsa Boyacá?

2.2 DESCRIPCIÓN DEL PROBLEMA

Sanoha es una empresa que se dedica a la explotación y comercialización de yacimientos de minerales básicos, planeación y ejecución de proyectos forestales, logística y conocimiento en la elaboración de estudios y trámites para la obtención de títulos mineros y licencias ambientales de proyectos mineros. Cuenta con una red corporativa, correos corporativos, pagina web y dos bases de datos distribuidos, una para el manejo de báscula y otra para manejo de pedidos, nómina y ventas. Sin embargo hay que resaltar que el proceso de automatización de báscula es pieza clave en el funcionamiento de los demás procesos de la empresa y en la continuidad del negocio. Conociendo de forma general el área de automatización del proceso de báscula, es pertinente que se reflexione sobre qué pasaría si hay un riesgo o riesgos que evoquen la posibilidad de que ocurra un contratiempo o se produzca un daño que pongan en peligro el funcionamiento o continuidad del negocio. Haciendo necesario analizar responsablemente los riesgos que afectarían seriamente el proceso de automatización de báscula, con el objetivo de valorar los riesgos, comprenderlos, medirlos y establecer límites de riesgo aceptables y qué tipos de riesgos deben ser prevenidos, gestionados y que implican cambios, si fuera necesario teniendo en cuenta las Normas y estándares de Implantación de un SGSI. Básicamente el proyecto involucra directamente a los directivos de la empresa, las personas que conocen y manejan el proceso y las expectativas de ambas. Teniendo en cuenta esto la organización Sanoha Ltda. está interesada en que se implemente un SGSI en su departamento de sistemas, área de automatización del proceso de bascula, porque es básicamente una área primordial para el funcionamiento de la misma e influye directamente en los demás departamentos que tiene la empresa; quiere que se analicen los riesgos a los que está sometida toda su información, se evalué qué niveles de riesgo asumen, que se implanten controles (no sólo tecnológicos, sino también organizativos y legales), documentar las políticas y procedimientos relacionados con la seguridad informática y que se efectué un proceso continuo de revisión y mejora de todo el sistema.

3. JUSTIFICACIÓN

Un SGSI facilita el análisis de riesgos a los que se ve expuesta la información en el caso particular del área de automatización de báscula, donde se busca poder asumir, minimizar y controlar amenazas que pueden estar presentes en el sistema informático, mediante estrategias y planes definidos, documentados y conocidos para ser revisados y se actualizados constantemente . A parte de esto un SGSI le proporcionaría a la organización un conjunto de objetivos, políticas, procedimientos y acciones que se implementarían para identificar, medir, vigilar, limitar, informar y revelar los factores sensibles de vulnerabilidad que intervienen en los procesos de seguridad de la base de datos SIRMAB(Sistema de Recepción de Materiales en Báscula), encargada de la automatización del proceso de bascula en la realización de sus operaciones. Cabe decir que la implementación de un SGSI en Sanoha tiene como característica principal apoyar su desarrollo en las normativas internacionales ISO/IEC 27001 que permiten administrar, transformar y optimizar de forma conjunta con los objetivos estratégicos de seguridad requeridos por la Organización.

4. OBJETIVOS

4.1 GENERAL

Diseñar un Sistema de Gestión de la Seguridad de la Información para la empresa minera Sanoha Ltda en el área de automatización del proceso de báscula usando la norma ISO/IEC 27001:2013.

4.2 ESPECÍFICOS

- Revisar el estado del arte de la Seguridad de la información teniendo en cuenta la normatividad que se aplica en este campo.
- Identificar los diferentes riesgos de seguridad informática mediante un análisis y recopilación exhaustiva de los procesos del área de automatización de báscula.
- Establecer el Mapa de Riesgos Tecnológicos y de Información para los procesos del área de automatización de báscula.
- Documentar las Políticas de Seguridad de la Información aplicables para la Empresa minera Sanoha Ltda para los procesos del área de automatización de báscula.

5. MARCO DE REFERENCIA

5.1 SISTEMA DE GESTIÓN

Un Sistema de Gestión implementa los procesos que permiten que una Organización realice un servicio o producto de manera confiable y en conformidad con unas especificaciones internacionales[1].

5.2 NORMATIVAS DE GESTIÓN DE LA SEGURIDAD

Se refieren a los lineamientos necesarios para que las organizaciones puedan orientar, planear, diseñar e implantar un sistema de gestión de la seguridad de la información. Este sistema de gestión se realiza a través de un proceso ordenado con una serie de fases donde se definen los mecanismos primordiales de seguridad de forma documentada y lógicamente conocida por la totalidad de los individuos de la empresa u organización.

Sin embargo es importante que se tenga claro que la implantación de un SGSI no garantiza la protección en su totalidad ya que su propósito es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnología. Las normativas para la creación del SGSI se constituyen en:

- Normativas que involucra a las buenas prácticas para la seguridad de la información, en las cuales se encuentran los códigos de buenas prácticas que sirven para que las empresas la utilicen para mejorar la seguridad de su información.

- Normativas que involucra las especificaciones de los SGSI, que sería la documentación que deben tener las empresas que deseen certificarse su SGSI[2].

[1] Tomado del documento sistema de gestión de seguridad de la información, ISO 27001 Elaborado: Centro Europeo de empresas de innovación Albacete (2010)

[2] Tomado del módulo curso 233003 de sistema de gestión de seguridad de la información SGSI Unad 2013

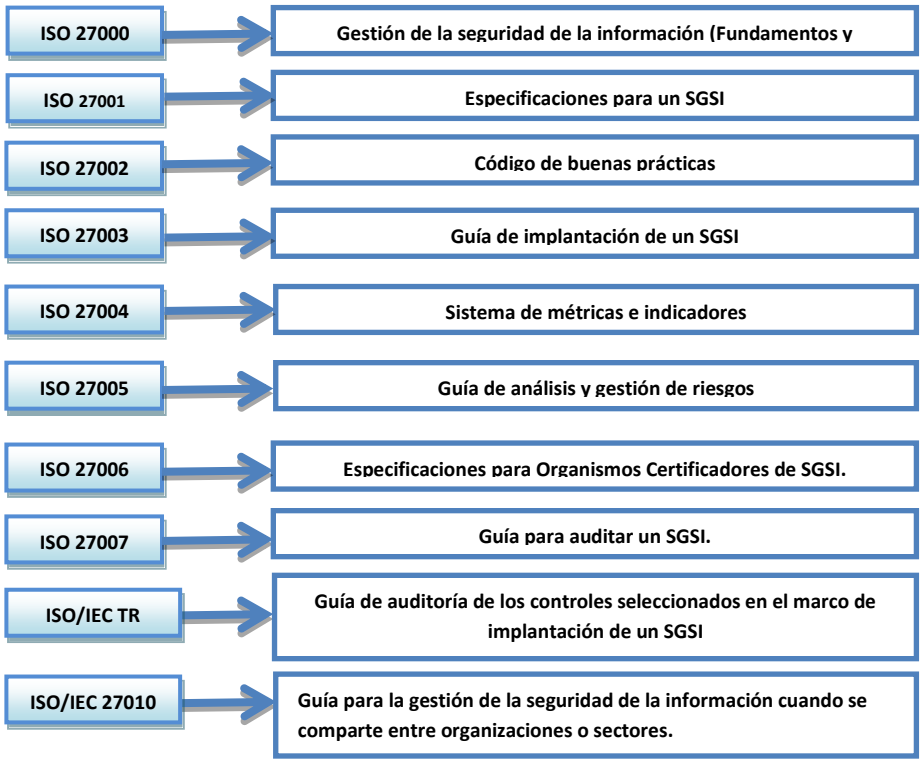
5.3 NORMAS ISO/IEC 27000:2005

La serie ISO/IEC 27000, es un conjunto de normas de gestión de la seguridad de la información con la IEC (International Electrotechnical Commission), comisión internacional de electrotecnia, tiene algunas similitudes a la familia de las normas de gestión de la calidad ISO 9000. Cada una de las normas de la familia 27000, define y centra todos los aspectos importantes en el contexto de la gestión de la seguridad de la información en cualquier empresa pequeña, mediana o grande, así como públicas y privadas. Las normas 27000 básicamente son una serie de estándares sus rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044, pero a continuación se describen hasta 27007 y 2 de la IEC. Ver figura 1.

5.3.1 Norma ISO 27000

Gestión de la seguridad de la información (Fundamentos y vocabulario) .Esta norma fue publicada el 1 de mayo de 2009 y contemplan en forma introductoria todos los aspectos fundamentales que enfoca un sistema de gestión de seguridad de la información (SGSI), una descripción del ciclo PDCA, al igual que las definiciones de los términos que se emplean en toda la serie 27000.

Figura 1 Serie de las normas ISO/IEC 27000



Fuente: Resultados de investigación

5.3.2 Norma ISO 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.
ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.
Detalla los parámetros para un SGSI, la cual describe los requisitos y/o especificaciones del sistema de Gestión de la seguridad de la información. Son reconocidas las normas ISO 27001:2005[3] y la norma vigente ISO/IEC27001:2013.

Características:

- Es certificable en la actualidad por los auditores externos de los SGSI de las diferentes empresas.
- Enumera especificando los objetivos de control y controles para ser elegidos por las empresas y que les interesa implantar en su sistema de gestión de seguridad.
- Hay que tener en cuenta aunque no es obligatorio implementar todos los controles de esta norma, la organización debe argumentar ante los auditores la no aplicabilidad de los controles cuando estén en el proceso de evaluación para una certificación.
- En Colombia a través del El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) y en otros países como España, Venezuela, Argentina, Chile, México y Uruguay se pueden adquirir las normas en el idioma Español.

5.3.3 Norma ISO 27002

Esta norma no certificable, es una guía de buenas prácticas que detalla los objetivos de control y controles recomendables en los aspectos de seguridad de la información. En cuanto a seguridad de la información. Esta norma se encuentra publicada en Español a través de la empresa AENOR y en Colombia NTC-ISO IEC 27002), así mismo se pueden encontrar en Perú, chile, entre otros países latinoamericanos[4].

[3] Tomado de Familia de las normas ISO/IEC 27000 Disponible en: : http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/22__leccin_7_familia_de_las_normas_isoiec_27000.html

[4] Tomado del módulo curso 233003 de sistema de gestión de seguridad de la información SGSI Unad 2013

5.4 ISO/IEC27001:2005 Vs ISO/IEC27001:2013

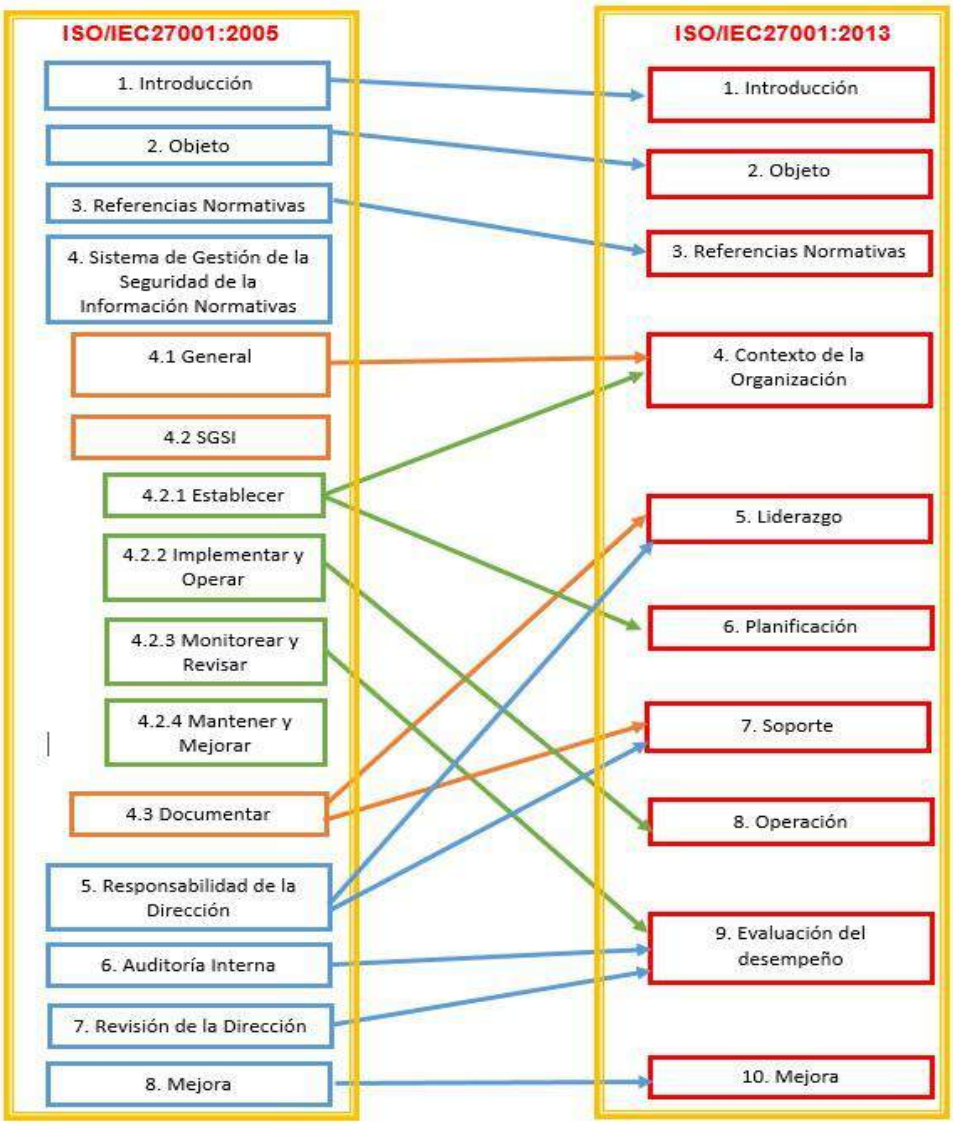
1. Las cláusulas que definen ISO/IEC27001:2005 son eficaces dentro del contexto de la implementación de SGSI, sin embargo son modificadas en la ISO/IEC27001:2013 para potencializar y subir el nivel de aplicabilidad y efectividad de los diferentes dominios y controles para proveer confianza dentro del mercado de bienes y servicios, en la capacidad de una organización para cuidar de la información de forma segura.
2. La nueva estructura ISO/IEC27001:2013 tiene una visión de alto nivel y hace una integración directa cuando se implemente más de un sistema de gestión.
3. Hay cambios en la terminología respecto de la ISO/IEC27001:2005 a ISO/IEC27001:2013 donde algunas definiciones se han eliminado o reubicado en el nuevo estándar para mayor efectividad en el diseño e implementación de un SGSI.
4. Los requerimientos de la evaluación de riesgos se han alineado con BS ISO 31000[5]
5. Los requerimientos del compromiso de gestión se han enfocado en el "liderazgo"
6. Las Acciones de mejoramiento se han reemplazado con "acciones para hacer frente, riesgos y oportunidades"
7. Los requerimientos de SOA son semejantes, evidenciándose más claridad en la necesidad de determinar los controles por el proceso de tratamiento de riesgos
8. Los controles han sido modificados ISO/IEC27001:2005 a ISO/IEC27001:2013 para reflejar las amenazas variantes, eliminar la duplicidad y tener una agrupación más lógica. Los controles específicos también han sido agregados alrededor de la criptografía y seguridad en las relaciones con proveedores
9. Hay relevancia en establecer objetivos, monitorear el desempeño del sistema y las medidas a implementar según la norma.
10. ISO/IEC 27001:2013 detalla los requerimientos para constituir, implementar, mantener y mejorar continuamente un SGSI, definiendo la manera de optimizarlo y que este sea totalmente operacional.
11. Estructuralmente ISO/IEC 27001:2013 luce distinto a ISO/IEC 27001:2005. No existe requerimientos repetidos y están descritos de una forma que permite mayor libertad de elección sobre cómo implementarlos en una organización.

[5] "Norma internacional para la gestión de riesgos que proporciona principios y directrices generales para realizar análisis y evaluaciones de riesgos. Facilitando a todas las organizaciones la administración los riesgos y desarrollar recomendaciones de buenas prácticas a partir de este estándar internacional para mejorar las técnicas de gestión y garantizar la seguridad general y la seguridad en el lugar de trabajo en todo momento". Extraído del sitio web BSI Disponible en: http://www.bsigroup.com/en-GB/iso-31000-risk-management/

5.4.1. Cambios PDCA de acuerdo a la mejora continua ISO/IEC27001:2005 Vs ISO/IEC27001:2013

Entre la norma 2005 y 2013 se evidencia similitudes en ciertos conceptos sin embargo el cambio sustancial se observa en el punto 4 representados de color verde y naranja de la ISO/IEC27001:2005, en donde algunos conceptos no se utilizan y otros se dividen en nuevos, como lo son: contexto de organización, liderazgo, planificación, soporte, operación y evaluación de desempeño en la ISO/IEC27001:2013.

Figura 2 ISO/IEC27001:2005 VS ISO/IEC27001:2013



Fuente: Basado en el estudio de AENOR sobre las principales Novedades de la ISO 27001/ISO 27002

5.4.3. Los nuevos conceptos de ISO/IEC27001:2013

1) **Contexto de la organización:** Se refiere al entorno en el que la organización funciona e interactúa.
2) **Problemas, riesgos y oportunidades:** Substituye a las Acciones de mejoramiento de la ISO/IEC27001:2005.
3) **Partes interesadas:** Es sustituido por el concepto de accionistas
4) **Liderazgo:** Es fijado de acuerdo a los requerimientos definidos por la alta gerencia.
5) **Comunicación:** Existen requerimientos definidos ajustados para comunicaciones internas y externas.
6) **Objetivos de seguridad de la información:** Los objetivos de seguridad de la información ejercen un papel fundamental actuando como niveles de mejoramiento y funciones de proyección.
7) **Evaluación de riesgos:** La identificación de activos, amenazas y vulnerabilidades que eran de gran importancia en la ISO/IEC27001:2005, no son camisa de fuerza dentro del análisis de riesgos y seguridad de la información en un SGSI.
8) **Propietario de riesgo:** Sustituye al propietario de los activos que se definía en la norma ISO/IEC27001:2005.
9) **Plan de tratamiento de riesgos**: Es primordial la efectividad del plan de tratamiento de riesgos en la implementación de un SGSI sobre la efectividad de los controles.
10) **Controles:** Los controles en la ISO/IEC27001:2013 son fijados en el transcurso del proceso de tratamiento de riesgos.
11) **Información documentada:** Sustituye a los denominados documentos y registros.
12) **Evaluación del desempeño:** Abarca las medidas del SGSI y define la eficacia de las diferentes acciones diseñadas consignadas en el plan de tratamiento de riesgos.
13) **Mejora continua:** En la ISO/IEC27001:2013 abre las posibilidades en cuanto a la utilización de metodologías diferentes a Planear-Hacer-Verificar-Actuar (PDCA).

5.4.2. Clausulas ISO/IEC27001:2005 Vs ISO/IEC27001:2013

Como se puede observar en la tabla 1 la norma ISO/IEC27001:2013 mantiene 94 controles, se elimina 39 y se generan 20 nuevos respecto a la norma ISO/IEC27001:2005. Y en la tabla 2 se aprecia una comparación de los dominios y objetivos de cada una de las normas.

Tabla 1 Modificaciones de la norma 2005 a 2013

NORMAS	No. DE CONTROLES	DOMINIOS DE SEGURIDAD	OBJETIVOS DE CONTROL	REQUISITOS DE GESTION
ISO/IEC27001:2005	133	11	39	102
ISO/IEC27001:2013	114	14	35	130

Tabla 2 Comparación de dominios y objetivos de la norma ISO/IEC27001:2005 Vs ISO/IEC27001:2013

ISO/IEC27001:2005	ISO/IEC27001:2013
5. POLÍTICA DE SEGURIDAD.	**5. POLÍTICAS DE SEGURIDAD.**
5.1 Política de seguridad de la información.	5.1 Directrices de la Dirección en seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	**6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.**
6.1 Organización interna.	6.1 Organización interna.
6.2 Terceros.	6.2 Dispositivos para movilidad y teletrabajo.
7. GESTIÓN DE ACTIVOS.	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**
7.1 Responsabilidad sobre los activos.	7.1 Antes de la contratación.
7.2 Clasificación de la información.	7.2 Durante la contratación.
7.2.1 Directrices de clasificación.	7.3 Cese o cambio de puesto de trabajo.
7.2.2 Etiquetado y manipulado de la información.	**8. GESTIÓN DE ACTIVOS.**
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	8.1 Responsabilidad sobre los activos.
8.1 Antes del empleo.	8.2 Clasificación de la información.
8.2 Durante el empleo.	8.3 Manejo de los soportes de almacenamiento.
8.3 Cese del empleo o cambio de puesto de trabajo.	**9. CONTROL DE ACCESOS.**
9. SEGURIDAD FÍSICA Y DEL ENTORNO.	9.1 Requisitos de negocio para el control de accesos.
9.1 Áreas seguras.	9.2 Gestión de acceso de usuario.
9.2 Seguridad de los equipos.	9.3 Responsabilidades del usuario.
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.	9.4 Control de acceso a sistemas y aplicaciones.
10.1 Responsabilidades y procedimientos de operación.	**10. CIFRADO.**
10.2 Gestión de la provisión de servicios por terceros	10.1 Controles criptográficos.
10.3 Planificación y aceptación del sistema.	**11. SEGURIDAD FÍSICA Y AMBIENTAL.**
10.4 Protección contra el código malicioso y descargable.	11.1 Áreas seguras.
10.5 Copias de seguridad.	11.2 Seguridad de los equipos.
10.6 Gestión de la seguridad de las redes.	**12. SEGURIDAD EN LA OPERATIVA.**
10.7 Manipulación de los soportes.	12.1 Responsabilidades y procedimientos de operación.
10.8 Intercambio de información.	12.2 Protección contra código malicioso.
10.9 Servicios de comercio electrónico.	12.3 Copias de seguridad.
10.10 Supervisión.	12.4 Registro de actividad y supervisión.
11. CONTROL DE ACCESO.	12.5 Control del software en explotación.
11.1 Requisitos de negocio para el control de acceso.	12.6 Gestión de la vulnerabilidad técnica.
11.2 Gestión de acceso de usuario.	12.7 Consideraciones de las auditorías de los sistemas de información.
11.3 Responsabilidades de usuario.	**13. SEGURIDAD EN LAS TELECOMUNICACIONES.**
11.3.1 Uso de contraseñas.	13.1 Gestión de la seguridad en las redes.

11.3.2 Equipo de usuario desatendido.	13.2 Intercambio de información con partes externas.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.	**14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**
11.4 Control de acceso a la red.	14.1 Requisitos de seguridad de los sistemas de información.
11.5 Control de acceso al sistema operativo.	14.2 Seguridad en los procesos de desarrollo y soporte.
11.6 Control de acceso a las aplicaciones y a la información.	14.3 Datos de prueba.
11.7 Ordenadores portátiles y teletrabajo.	**15. RELACIONES CON SUMINISTRADORES.**
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.	15.1 Seguridad de la información en las relaciones con suministradores.
12.1 Requisitos de seguridad de los sistemas de información.	15.2 Gestión de la prestación del servicio por suministradores.
12.2 Tratamiento correcto de las aplicaciones.	**16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**
12.3 Controles criptográficos.	16.1 Gestión de incidentes de seguridad de la información y mejoras.
12.4 Seguridad de los archivos de sistema.	**17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**
12.5 Seguridad en los procesos de desarrollo y soporte.	17.1 Continuidad de la seguridad de la información.
12.5.1 Procedimientos de control de cambios.	17.2 Redundancias.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	**18. CUMPLIMIENTO.**
12.5.3 Restricciones a los cambios en los paquetes de software.	18.1 Cumplimiento de los requisitos legales y contractuales.
12.5.4 Fugas de información.	18.2 Revisiones de la seguridad de la información.
12.5.5 Externalización del desarrollo de software.	
12.6 Gestión de la vulnerabilidad técnica.	
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	
13.1 Notificación de eventos y puntos débiles de seguridad de la información.	
13.2 Gestión de incidentes y mejoras de seguridad de la información.	
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	
15. CUMPLIMIENTO.	
15.1 Cumplimiento de los requisitos legales.	
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.	
15.3 Consideraciones sobre las auditorías de los sistemas de información.	

5.5. MARCO CONCEPTUAL

CONFIDENCIALIDAD: se define como el uso autorizado de la información donde se puede acceder a contenidos, sistemas, bases de datos o aplicaciones si se cuenta con previos permisos de usuario. Por ende la información no puede ser revelada a terceros, ni puede ser pública, por lo tanto debe ser protegida.

INTEGRIDAD: se refiere al estado intacto y que no ha sido sometida a borrado, copia o modificación en su transmisión, recepción o procesamiento.

DISPONIBILIDAD: es la característica de la información donde a través de permisos es obtenida en el momento preciso cuando lo solicita el usuario y de este modo se realiza el procesamiento de la información sin ningún tipo de interrupciones.

AUTENTICIDAD: Comprobación de la información y su estado de validez en cuanto a contenido y permisos de seguridad.

CONTROLES PREVENTIVOS: Acciones que permiten reducir la ocurrencia de un incidente.

CONTROLES DECTIVOS: Actividades que facilitan detección de incidente de manera rápida.

CONTROLES REPRESIVOS: Tratan los incidentes de forma efectiva para que no sigan dañando el sistema.

CONTROLES CORRECTIVOS: Acciones directas y contundentes que recuperan el funcionamiento de un sistema después de un incidente o daño causado.

CONTROLES EVALUATIVOS: Identifican y analizan los incidentes sus causas y efectos además de los controles que se aplicaron para contrarrestarlos.

PESO BRUTO: Peso efectuado con carga

PESO TARA: Peso efectuado sin carga

PESO NETO: Es la diferencia entre el peso efectuado con carga y el Peso efectuado sin carga.

INDICADOR DE PESAJE ELECTRÓNICO: Aparato electrónico que a través de bit y vibraciones o baudios captura los pesos de báscula.

6. DISEÑO METODOLÓGICO PRELIMINAR

TIPO DE INVESTIGACIÓN

Para el diseño metodológico se utilizara los 2 tipos de investigación cuantitativo y cualitativo con el propósito de abarcar variables, aspectos y comportamientos completos del sistema. Además proporcionan las herramientas para estudiar los datos recolectados sobre el problema planteado y conocer el tipo de incidencia del mismo.

Investigación descriptiva: Se hace uso de la investigación descriptiva porque permite ordenar los resultados de las observaciones de las conductas, las características, los factores, los procedimientos y otras variables de fenómenos y hechos.

Variables: sistemas informáticos, Incidentes, riesgos, vulnerabilidades, activos, personal de la empresa, controles existentes

TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

La entrevista estructurada: Esta permite registrar de forma estandarizada a través de preguntas precisas información sobre el sistema.

Observación sistemática regulada o controlada: este instrumento facilita observar de forma directa y continúa los procedimientos reales que suceden en el sistema. Ver anexo B y C.

Estadísticas, fuentes secundarias de datos: ya que en los temas de seguridad informática y sistemas de gestión son muy amplios, es pertinente hacer uso de investigaciones, estudios estadísticos y reportes sobre los mismos, porque permiten enriquecer la investigación y desarrollo del proyecto.

7. METODOLOGÍA

7.1 PROCEDIMIENTOS

- Se cuenta con la autorización de los administrativos del Sanoha Ltda .Ver anexo A.
- Es importante que estos se Involucren y sensibilicen en la planificación de la implementación de SGSI acordando compromisos con el cumplimiento y preparación de los prerrequisitos y así mismo de los requisitos los cuales la empresa debe cumplir.
- Es primordial que se definan y se documenten las responsabilidades y funciones a las personas que van a estar encargadas dentro de la empresa en el proceso del diseño del SGSI.
- Para el proceso de diseño del sistema de gestión de seguridad informática se realizan las siguientes actividades:
  - ✓ Programación de varias reuniones con el personal encargado de administrativas y operativas del proceso de en el diseño del SGSI, que facilita debatir y contar con la aceptación de los controles de la norma ISO 27001 a diseñar en Sanoha Ltda.
  - ✓ La finalidad de estas reuniones es construir las bases del proceso de mejora continua en materia de seguridad, permitiendo a la empresa Sanoha conocer el estado del mismo y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales. Para ello se abordarán los siguientes aspectos: Documentación normativa sobre las mejores prácticas en seguridad de la información. Identificación y valoración de los activos y amenazas sobre los activos. Diseño de controles y políticas de seguridad según la norma ISO 270001.

7.2 CICLO PDCA (EDWARD DEMING)

En vista que se busca implementar un SGSI, la metodología que mejor se adapta es la planteada en el ciclo de Demming o ciclo de mejora PDCA, porque brinda los instrumentos necesarios para el desarrollo de las diferentes fases y actividades requeridas para este tipo de proyectos. A continuación se describe las características de este modelo metodológico.

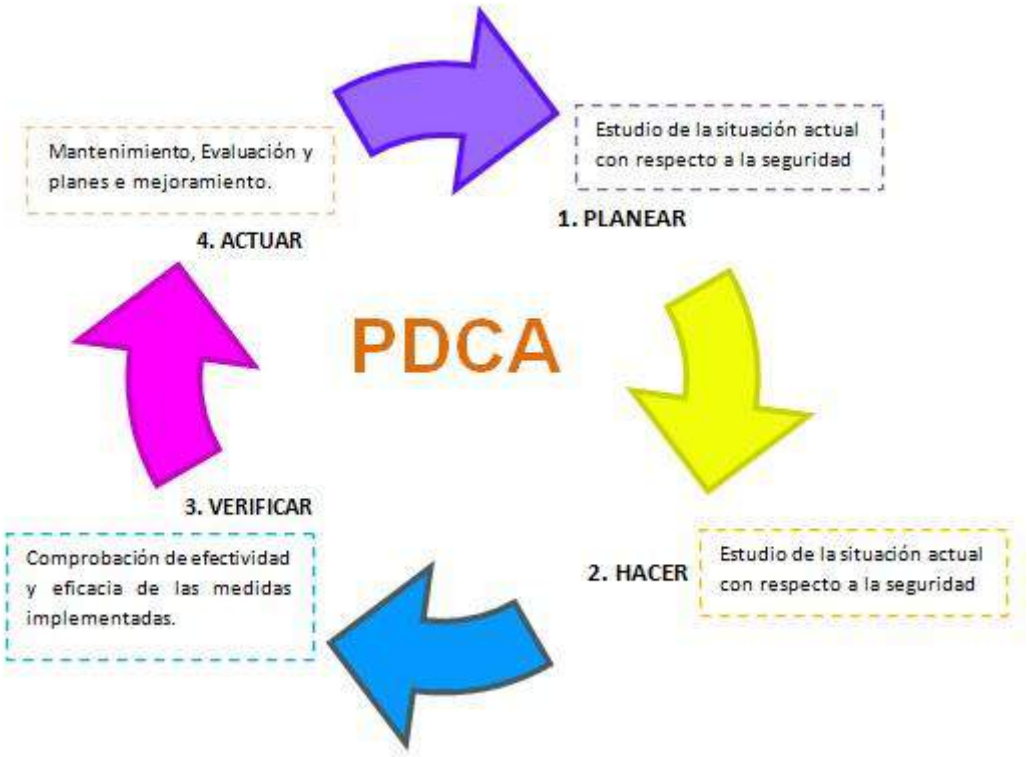
Modelo PDCA (Plan, do, check, act), se trata de Planificar, Hacer, Verificar y Actuar (PHVA), sus características son:

- Facilita el desarrollo de actividades que requieran un orden lógico para llevar organizado todo el proceso.

- Modelo utilizado para implantación de sistemas de gestión y mejora continua de calidad.
- Su implementación permite lograr un mejor nivel de calidad administrativa y de servicios con el objetivo de perfeccionarlos y continuar en un proceso de mejora continua.
- Estrategia efectiva para la organización y documentación del proceso de implementación del SGSI.
- Permanece en una constante revaluación respecto a las medidas de prevención, corrección y evaluación, manteniendo un constante ciclo que por sus características no podría terminar buscando la mejora continua en la implantación de SGSI.

Con el objetivo de comprender mejor el modelo PDCA se describe los 4 pasos que utiliza en la figura No.3

Figura 3 Pasos del PDCA



Fuente: Resultados de investigación

Aplicando el modelo PDCA las etapas del SGSI definido por la ISO 27001 es como sigue:

Plan: Establecimiento del SGSI. Pautas más importantes

- Delimitación del escenario que cubre el SGSI.
- Definición de la política de seguridad incluyendo objetivos y estrategia de gestión de riesgos.
- Diseño del método de gestión de riesgos.
- Evaluación de riesgos inicial, delimitación de riesgo residual.
- Estado de aplicabilidad, definición de controles y excepciones.

Hacer: Implementación y operación del SGSI.

- Plan de acción para el tratamiento de los riesgos.
- Implementación de los controles.
- Formación y adiestramiento.

Chequear: Supervisión y verificación del SGSI

- Seguimiento de los objetivos marcados.
- Adaptación de buenas prácticas.
- Programas de revisiones y auditorias.

Actuar: Mejoramiento y actualización del SGSI

El hecho de que un SGSI este certificado por la norma ISO 27001 aporta a la organización las siguientes ventajas:

- Demuestra a los clientes que la seguridad de su información es lo primordial.
- Analiza los riesgos de la organización, evaluándolos y gestionándolos al tiempo que formaliza unos procedimientos para proteger la información.
- Demuestra que la dirección de la organización está comprometida a garantizar la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales.

7.3. SGSI SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Este sistema consiste en un conjunto de actividades de gestión que deben realizarse mediante procesos sistemáticos y documentados que son conocidos por Sanoha Ltda enfocados en el proceso de automatización de báscula, proceso que influye en la continuidad negocio y del funcionamiento de los demás procesos dentro de la empresa. Su objetivos no están orientados a garantizar la seguridad sino a generar políticas y controles para que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la empresa Sanoha Ltda, de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la misma, los riesgos, el entorno y las tecnologías.

7.3.1 Beneficios de la implantación de un SGSI

- Aplica una arquitectura de gestión de la seguridad con normatividad internacional para la aplicación de buenas prácticas.
- Identifica y evalúa los riesgos que afectan al negocio e incidencia de los mismos.
- Implanta contramedidas, procesos y procedimientos pertinentes controles y tratamientos y para una mejora continua
- Gestiona de una forma eficaz la seguridad de la información, evitando los costos innecesarios e ineficientes.
- Permite de forma organizada y sistémica, mantener la seguridad de la información que maneja la empresa con un alto grado de confiabilidad, integridad y disponibilidad.
- Proporciona una sólida estructura de políticas de seguridad que preparan a la empresa para afrontar incidentes que alteren las medidas de seguridad implantadas y estar en la capacidad de poner en funcionamiento rápidamente la empresa y que estos tengan el mínimo impacto.
- Protege adecuadamente los objetivos de la empresa para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio.
- Reduce el riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad. Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Ayuda a la empresa a ser un elemento diferenciador ante la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y competitividad del personal en el manejo de procesos y claridad en los procedimientos de seguridad a seguir.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la
- compra sistemática de productos y tecnologías.
- Permite conocer los riesgos a los que está sometida su información y activos y los asume, minimiza, transfiere o controla mediante una metodología definida, documentada y conocida por todos, que se revisa y mejora constantemente.

8. ANÁLISIS Y RECOPILACIÓN EXHAUSTIVA DE LOS PROCESOS DEL ÁREA DE AUTOMATIZACIÓN DE BÁSCULA.

8.1 ESTADO ACTUAL

SANOHA LTDA MINERIA MEDIO AMBIENTE Y FORESTAL La empresa se encuentra ubicada en la localidad de NOBSA, en el departamento de BOYACA. El domicilio social de esta empresa es VI NOBSA KM 4. Ver

Figura 4 Logo corporativo de Sanoha Ltda

Fuente: Proporcionada por la administracion de Sanoha Ltda

8.1.1 Descripción de la empresa

SANOHA LTDA es una organización privada con características de empresa familiar, cuyo objeto principal es el desarrollo de actividades para los sectores minero, forestal, energético y ambiental. Tiene un enfoque en la división de actividades con la centralización de una compañía líder, la existencia de una estructura que garantiza el desarrollo de un grupo sin perder el control de las filiales con numerosas responsabilidades.

Cuenta con una experiencia específica de más de 15 años en la explotación y comercialización de yacimientos de minerales básicos, planeación y ejecución de proyectos forestales, servicios de Ingeniería, logística e inversiones participativas, amplia trayectoria y conocimiento en la elaboración de estudios y trámites para la obtención de títulos mineros y licencias ambientales de proyectos mineros.

Actividad comercial

La forma jurídica de SANOHA LTDA MINERIA MEDIO AMBIENTE Y FORESTAL es SOCIEDAD LIMITADA y su principal actividad **es "Extracción y aglomeración de hulla (carbón de piedra)".** Como se evidencia en la ilustración 2.

Figura 5 Patio de acopio de material

Fuente: Proporcionada por la administracion de Sanoha Ltda

8.1.2 Reseña histórica de la organización

Luego de haber laborado por espacio de cinco (5) años en una sociedad familiar de hecho, las familias Chiquillo Londoño y Chiquillo Puentes tomaron la decisión de crear la persona jurídica Minerales Sanoha, hoy Sanoha Ltda. En el año 1988 la Empresa había iniciado con 8 trabajadores. Julio de 1994: se incorpora la actividad forestal a las actividades económicas de la empresa. Año de 1995: Importaciones directas desde EE.UU. de maquinaria para la empresa y para terceros.

Identificación de los momentos históricos para la empresa

- Se incrementó en los años 2005 y 2006 la exportación de carbón térmico para países como Chile, Perú y Brasil a través de una alianza estratégica con una comercializadora internacional. Cumpliendo con las exigencias en cuanto a calidad, legalidad, manejo ambiental, cumplimiento en sus entregas y competitividad en sus precios, Sanoha Ltda. Logró posicionarse como una de las opciones más seguras para los clientes internacionales.
- La Empresa ha ido en constante crecimiento, a la fecha están vinculados de manera directa 260 trabajadores directos y cerca de 1000 familias tienen nexos económicos con Sanoha Ltda.
- La situación actual, sin embargo es de dificultad, pues los mercados nacionales son muy competidos y se corre el riesgo de saturarse con una sobreoferta del

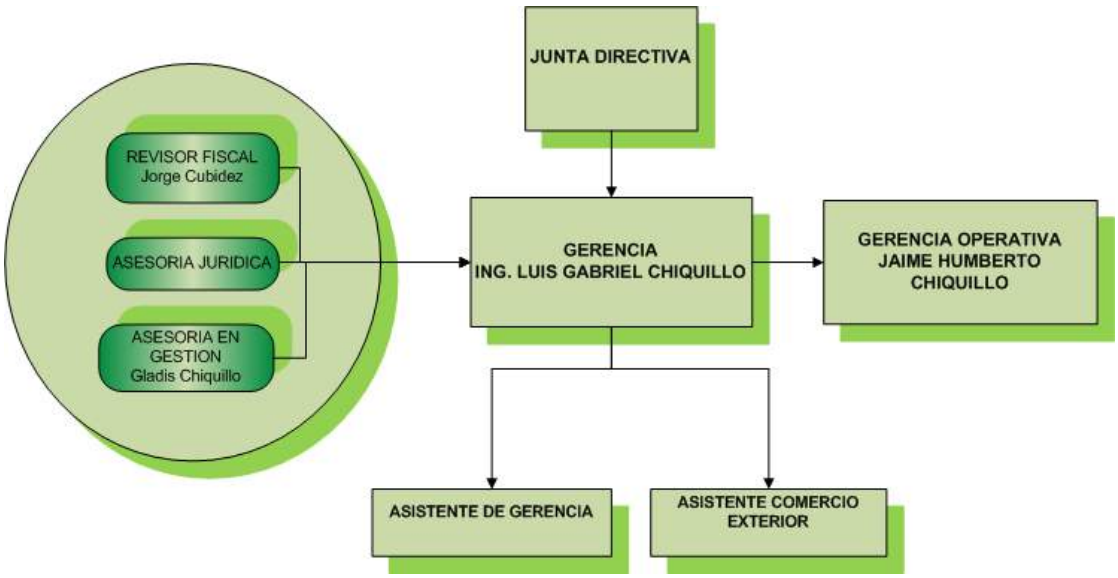
producto, pero al igual que en épocas anteriores asumen las dificultades, como retos a superar descubriendo nuevas posibilidades de diversificar e innovar.

8.2 ESTRUCTURA INSTITUCIONAL

8.2.1 Departamentos de alta gerencia

Está conformada por la Junta Directiva, Gerencia, Gerencia Operativa, Asistente de Gerencia, Asistente De Comercio Exterior, Revisor Fiscal, Asesoría Jurídica y Asesoría en Gestión. Como se observa en la figura 4.

Figura 6 Organigrama de Alta Gerencia

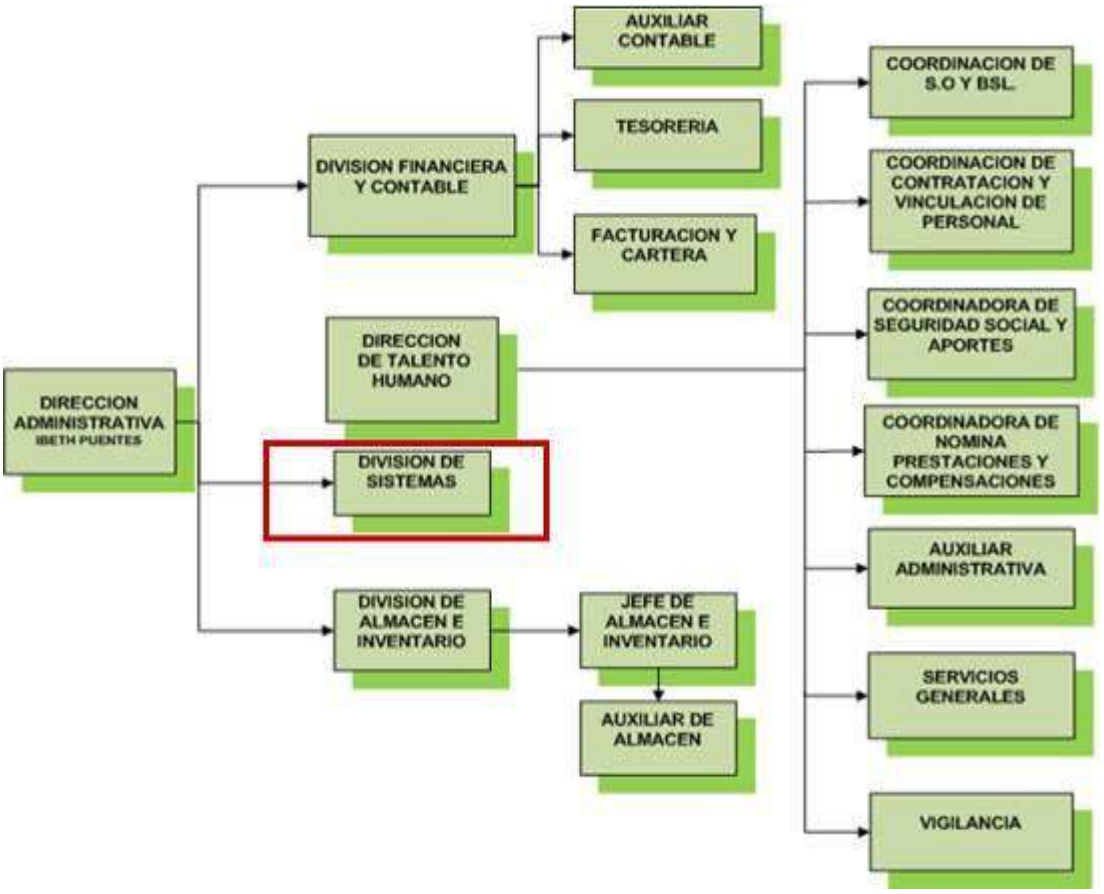


Fuente: Documentación proporcionada por Sanoha Ltda.

8.2.2 Departamentos administrativos

Están conformados por la Dirección administrativa: División Financiera y Contable, Auxiliar Contable, Tesorería, Facturación y Cartera, Dirección de Talento Humano, Coordinación de S.O (Salud Ocupacional) y BSL, coordinación de contratación y vinculación de personal, Coordinadora de seguridad social y aportes, Coordinadora de nómina, prestaciones y compensaciones, Auxiliar administrativa, Servicios Generales, Vigilancia, División de Sistemas, División de Almacén e Inventario, Jefe de almacén e Inventario y Auxiliar de Almacén. Como se observa en la figura 5.

Figura 7 Organigrama de Departamentos Administrativos



Fuente: Documentación proporcionada por Sanoha Ltda.

8.2.2.1 División de sistemas, cargos y funciones.

La división de sistemas en SANOHA LTDA tiene como responsabilidad evaluar y mantener permanentemente todos los procesos automatizados que se operan en cada una de las unidades administrativas, financieras y operacionales de la organización, así como garantizar el buen funcionamiento de toda la red informática de la misma. En la figura 9 se visualiza su organización.

Figura 8 Jerarquía de la división de sistemas SANOHA Ltda.

Funciones generales de la división de sistemas

1. Mantener en condiciones óptimas la infraestructura de comunicaciones vía Internet
2. Ofrecer asesoría y asistencia técnica en el área de redes
3. Promover y gestionar las mejoras tecnológicas que aseguren el buen funcionamiento de los recursos computacionales con que cuenta la organización, y que al mismo tiempo satisfagan los requerimientos de automatización de información que surjan como consecuencia de los cambios en el medio tecnológico.

Funciones Personal del Área de Redes y Telecomunicaciones

- Administrar las redes de comunicación
- Administrar los servicios de Telefonía IP.
- Instalar y dar mantenimiento a la red de Video-vigilancia.
- Administrar los servicios del correo electrónico corporativo
- Diseñar, implementar y mantener nuevas redes de comunicación y de servicios, basados en tecnologías de comunicación emergentes.
- Diseñar y analizar topologías de redes físicas y lógicas para la empresa.
- Diseñar, implementar y administrar los sistemas de monitoreo y seguridad de los equipos de comunicación y los servicios de red.
- Brindar consultoría y asesoría técnica en el área de redes y comunicación a la comunidad en general.
- Presentar estudios de factibilidad técnica, económica y operativa para asesorar a la dirección en la toma de decisiones.
- Evaluar y proponer nuevas tecnologías y servicios relacionados con redes de comunicación.

Funciones Personal del Área de Desarrollo de Sistemas de Información

- Analizar, diseñar, programar, implementar, evaluar, documentar y mantener permanentemente todos los procesos automatizados que se operan en cada una de las unidades administrativas, financieras y operacionales de la empresa.
- Administrar eficientemente la operación de las bases de datos con el fin de garantizar la integridad de los mismos, bajo una adecuada definición, diseño, mantenimiento y seguridad de la información compartida en el sistema de Base de Datos de la empresa.
- Adecuar los sistemas existentes a las necesidades de las diferentes unidades administrativas y capacitar a los funcionarios en las diferentes aplicaciones desarrolladas para cada área específica.
- Administrar la base de datos en forma óptima, evaluando el rendimiento de misma y la confiabilidad de los datos.

- Mantener el flujo de datos efectiva y eficientemente, y proporcionar el mantenimiento de la Base de Datos de acuerdo a los parámetros de seguridad que se han establecido.
- Desarrollar y mantener los sistemas de información de la empresa.

Funciones personal del área de Soporte Técnico

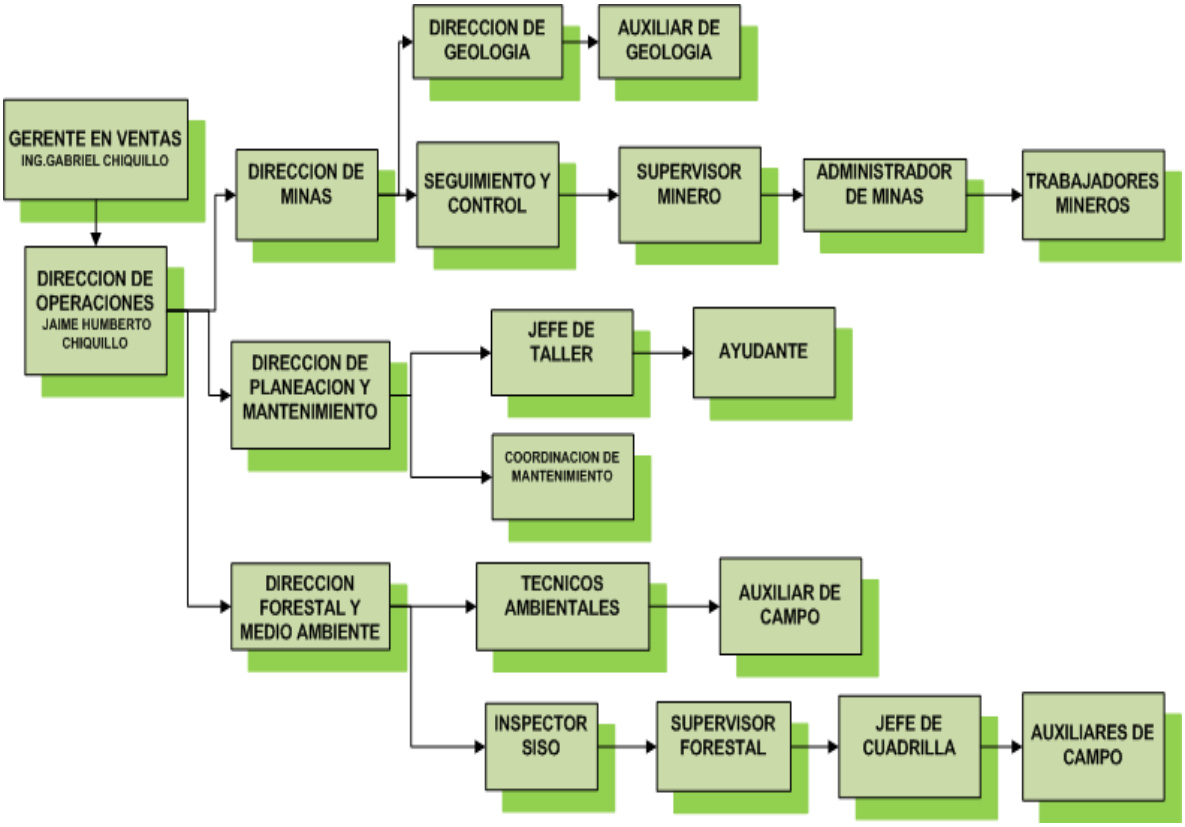
- Instalar los equipos informáticos y telefónicos, elementos de conectividad y recursos informáticos, garantizando su buen funcionamiento.
- Evaluar e implementar la topología física y lógica de la red de la empresa.
- Diagnosticar Problemas en los equipos informáticos, de telefonía, conectividad y sistemas operativos de usuarios finales de la empresa.
- Efectuar las reparaciones que se requieran en los equipos informáticos y de telefonía de acuerdo a los procedimientos establecidos.
- Tramitar las garantías de los equipos informáticos y de telefonía de la empresa.
- Instalar y dar mantenimiento a los Sistemas de Video-Vigilancia.
- Mantener un inventario actualizado de todos los equipos y recursos informáticos de la empresa.
- Presentar estudios de factibilidad técnica, económica y operativa para asesorar a la Dirección en la toma de decisiones.
- Investigar, proponer y evaluar nuevas tecnologías y servicios relacionados con equipos informáticos y de telefonía, conectividad y sistemas operativos.

8.2.3 Departamentos comerciales y de operaciones

Este departamento es el encargado de toda la parte operativa, técnica, ambiental de seguimiento y control en cuanto a la parte comercial, producción y mantenimiento de las diferentes Minas de carbón propiedad de Sanoha Ltda, además de los diferentes procesos que estas conllevan.

Están conformados por el Gerente de Ventas, Dirección de Operaciones, Dirección de Minas, Dirección de Geología, Auxiliar de Geología, Seguimiento y Control, Supervisor Minero, Administrador de Minas, Trabajadores Mineros, Dirección de Planeación y Mantenimiento, Jefe de Taller, Coordinación de Mantenimiento, Ayudante, Dirección Forestal y Medio Ambiente, Técnicos Ambientales, Auxiliar de Campo, Inspector SISO (Sistema de seguridad y Salud Ocupacional), Supervisor Forestal, Jefe de Cuadrilla y Auxiliares de Campo. Como se observa en la figura 6

Figura 9 Organigrama de los Departamentos comerciales y de operaciones



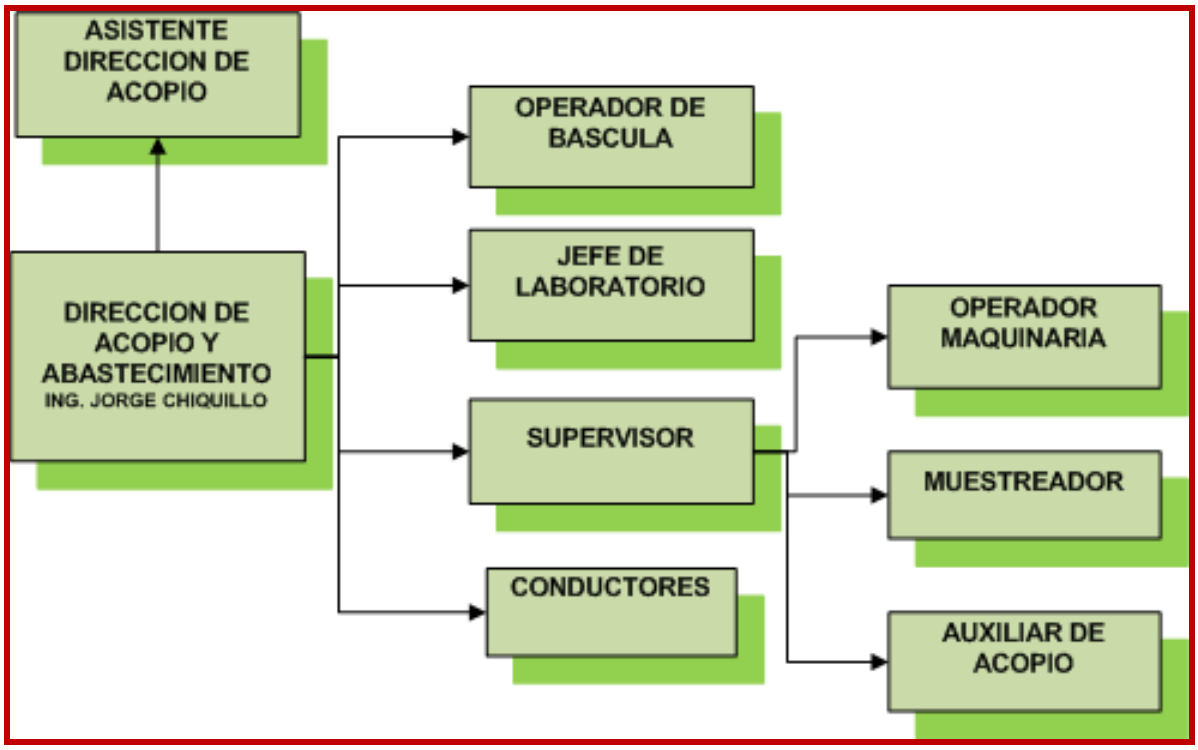
Fuente: Documentación proporcionada por Sanoha Ltda.

8.2.4 Departamentos de acopio y abastecimiento encargados del manejo del proceso de automatización de Báscula (SIRMAB)

El departamento de acopio y abastecimiento como se aprecia en la figura 7, cuenta con los siguientes cargos:

- 1 Director de acopio
- 1 Asistente de dirección de acopio
- 2 Operadores de báscula
- 1 Jefe de laboratorio
- 1 Supervisor de operador de maquinaria
- 1 muestreador
- 1 Auxiliar de acopio
- Conductores

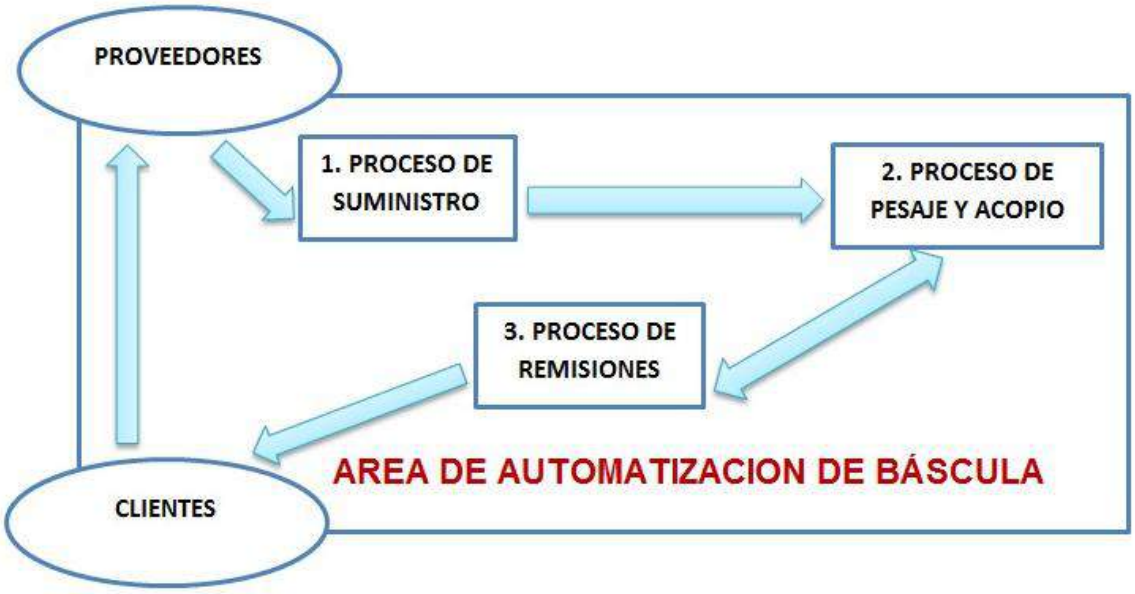
Figura 10 Departamento de acopio y abastecimiento



Fuente: Documentación proporcionada por Sanoha Ltda.

Este departamento es el encargado de manejar y controlar el proceso de automatización de báscula (SIRMAB) base de datos localizada en un servidor Local el cual es controlado y supervisado por la división de sistemas, el área de desarrollo de sistemas informáticos. Los servicios de la base de datos son utilizados por las estaciones de trabajo ubicadas en las oficinas del departamento operativo y la otra esta principalmente departamento de acopio y abastecimiento. SIRMAB (Sistema de Recepción de Materiales en Báscula), software creado en PostgreSQL y Visual Basic para automatizar el proceso de acopio, abastecimiento y remisión de carbón. Es un software que se encarga de procesos fundamentales (suministro material, pesaje, acopio y remisiones de material) para el funcionamiento de Sanoha Ltda. Ver figura 8

Figura 11 Procesos de los que se encarga SIRMAB



Fuente: Autor

En este departamento se focaliza todo el estudio del proyecto para el diseño del sistema de gestión de seguridad informática y en el cual se efectúa un análisis minucioso de vulnerabilidades, amenazas y niveles de riesgo en los sistemas informáticos siguiendo las normas ISO 27001 que proporcionan los estándares para generar políticas y controles de seguridad que permiten garantizar los procedimientos a seguir en casos de incidencias que pongan en riesgo la continuidad de los procesos desarrollados en esta área primordial de la Empresa Sanoha Ltda .

8.3 FUNCIONAMIENTO DEL PROCESO DEL ÁREA DE AUTOMATIZACIÓN DE BÁSCULA (SIRMAB)

8.3.1 Descripción de la automatización de báscula

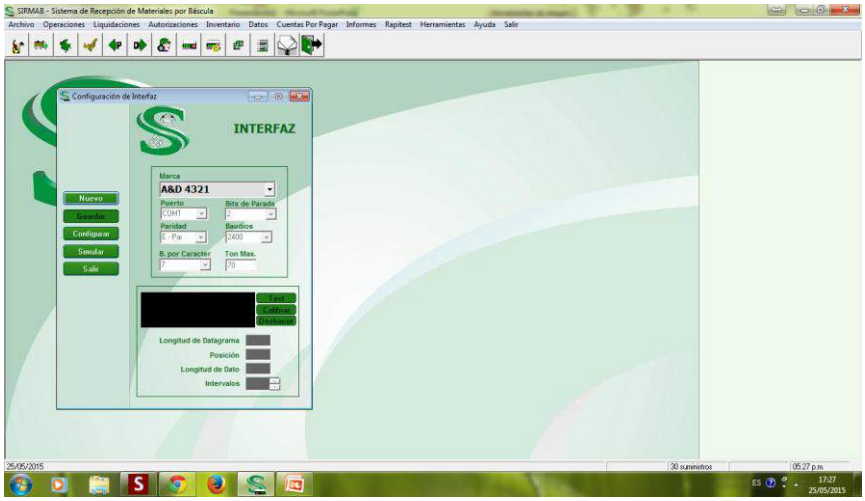
Sanoha Ltda. Implemento desde el año 2006 la base de datos **SIRMAB (Sistema de Recepción de Materiales en Báscula)**, programa realizado en PostgreSQL y Visual Basic para automatizar el proceso de acopio, abastecimiento y remisión de carbón. Desde esa época ha venido creciendo en módulos, opciones y funcionalidad hasta el punto que todos los departamentos dependen directa e indirectamente de la información consignada en él.
La empresa tiene varios departamentos entre ellos la división de sistemas, este se encarga de la gestión informática de varias áreas, sin embargo una de las más importantes es manejar, monitorear y controlar la base de datos llamada SIRMAB

(Sistema de Recepción de Materiales en Báscula) con la que se tiene automatizado el proceso de báscula y el departamento de acopio y abastecimiento es el encargado de operar este sistema que tiene como función primordial de capturar los pesos de las entradas de suministro y las salidas de remisiones, los cuales se guardan en esta base de datos.

Funcionamiento de báscula

La báscula es electromecánica que cuenta con un **INDICADOR DE PESO** electrónico, el cual genera el **peso BRUTO (peso camión cargado)** y el **peso TARA (peso de camión descargado)** Ver figura 10, que son capturados por el puerto COM 5432 a través de la lectura de bits y baudios es decir vibraciones que son registrados por la base de datos (SIRMAB) para procesarlos a través del mecanismo. Cabe aclarar que la calibración de la báscula y del indicador de peso electrónico se realiza cada año con una empresa certificada BÁSCULAS SSAP S.A.S. proveedor de servicios de mantenimiento preventivo y correctivo de este tipo de máquinas de pesaje.

Figura 12 Interfaz con el indicador electrónico de pesos



Fuente: División de sistemas Sanoha Ltda

8.3.1.1 Proceso de Suministro

En este proceso se tiene en cuenta 3 aspectos:

- **Proveedor:** quien suministra la carga peso tara, peso neto, peso bruto.
- **Procedencia:** transportador: procedencia donde viene el carbón.
- **Tipo de material:** el cual describe que carbón es si es térmico o coquizable.

1. El proveedor previamente debe dirigirse a la empresa y llevar una muestra de 10 Kg de material (tipo de carbón), Rut y Autorización de la DIAN para facturar.
2. El proveedor debe adicionalmente registrar su nombre completo, NIT, Nombre y dirección de la mina de carbón, las placas de los diferentes vehículos de carga, nombres e identificación de los conductores para que estos ya estén registrados en el SIRMAB cuando se reciba y pese la carga en la báscula.
3. El laboratorio de Sanoha Ltda recibe la muestra y analiza las propiedades físico químicas (humedad, cenizas) según el tipo de carbón. Este proceso se realiza para conocer la calidad del material, la pila correspondiente para acopio y el valor a liquidar según los resultados que se registran en la base de datos SIRMAB para procesarlos y que estén disponibles para su consulta en el departamento de acopio y abastecimiento. El Muestreo de carbón se realiza de la siguiente manera:

    - El cual se hace según el tipo de carbón se toma una muestra de 40 kg a esta muestra se le otorga un número.
    - Para hacer referencia el cual pasa a laboratorio en donde se hace un proceso de caracterización físico químico, en donde se determinan las cenizas, la humedad y poder calorífico.
    - Los datos obtenidos de los resultados según las características físicas químicas se clasifican según una tabla de precios que cuenta el sistema se da un valor al carbón, por ejemplo: si el carbón tiene cenizas por encima de 12 el carbón puede valer $90.000. Todo este proceso se realiza para hacer liquidación del carbón por proveedores. De este proceso de muestreo se determinan las siguientes operaciones fundamentales para la empresa:
        - ✓ **Se realizan los descuentos** ya que la empresa provee combustible y artículos mineros.
        - ✓ **Sale la liquidación** la cual tiene un número que la identifica y sus respectivas retenciones.
        - ✓ **Se realiza una facturación a cada liquidación**. Es un proceso automático del sistema SIRMAB el cual se realiza de acuerdo al periodo liquidado. Luego estos mismos datos también de forma automática se guardan en el módulo de cuentas por pagar. Al momento de pagar, se guarda la fecha de pago y el número de comprobante; estos datos se vuelven históricos para consultar. Este es el proceso de suministro.

8.3.1.2 Proceso de Pesaje

1. Los vehículos de carga hacen fila según orden de llegada.
2. Si se registra sobrecarga del vehículo siguiendo la RESOLUCION 004100 DE 2004 (diciembre 28) por la cual se adoptan los límites de pesos y dimensiones en los vehículos de transporte terrestre automotor de carga por carretera, para su operación normal en la red vial a nivel nacional. El vehículo deberá entrar al

patio de acopio y debe dirigirse al área asignada para quitar excedente de carga y nuevamente hacer la fila para pesaje.

3. Los vehículos de carga antes de entrar a báscula deben validar en el SIRMAB la placa del carro, identificación y nombre del transportador, además de la procedencia (mina de carbón) del proveedor. Esta información es diligenciada dentro del SIRMAB por el operario de báscula de turno.
4. El operario de báscula se encarga de realizar los procedimientos en el SIRMAB para el registro de pesaje del vehículo de carga con el peso bruto, descarga en el acopio de acuerdo a la pila correspondiente teniendo en cuenta el tipo de material y el análisis del laboratorio según sus características físicas químicas analizadas previamente.
5. En el SIRMAB el operador de báscula debe seleccionar la placa del vehículo, el nombre de proveedor, transportador y procedencia y oprimir la tecla F5 para que se cargue automáticamente de la báscula el peso bruto del vehículo de carga.
6. El vehículo descarga el material vuelve a bascula y se pesa nuevamente con el peso Tara.
7. En el SIRMAB el operador de báscula debe seleccionar la placa del vehículo, el nombre de proveedor, transportador y procedencia nuevamente y oprimir la tecla F9 para que se cargue automáticamente de la báscula el peso Tara del tractocamión. Ver figura 11.

Características específicas de pesaje para el proceso de suministros

- El vehículo de carga validado previamente por el operador de báscula, debe **pesarse de frente** para calcular el **PESO BRUTO**
- Entra al patio de acopio descarga el material en la pila correspondiente guiado por el supervisor y el auxiliar de acopio, luego sale y pesa el peso tara.

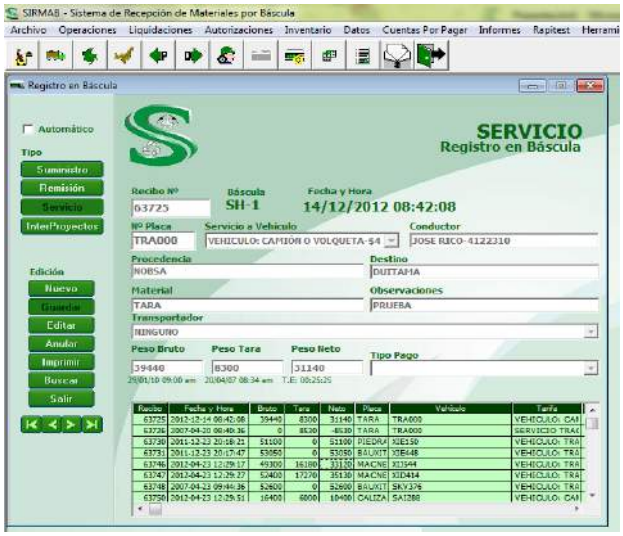
Características específicas de pesaje para el proceso de remisiones

- El vehículo de carga validado previamente por el operador de báscula, debe **pesarse de frente** para calcular el **PESO TARA.**
- Entra al patio de acopio lo carga el operador de maquinaria de acuerdo a la pila correspondiente según las características solicitadas en el pedido de los clientes y guiado por el supervisor y auxiliar de acopio , luego sale y pesa el peso bruto.

Características específicas para pesaje a empresas independientes que pagan por este servicio.

Se realiza con el método de suministros o de remisiones ya que no influye porque no hay una liquidación de carga de material, ni se tienen en cuenta muestras de ningún tipo porque es un servicio de pesaje exclusivamente.

Figura 13 Módulo de Servicios Registro de báscula

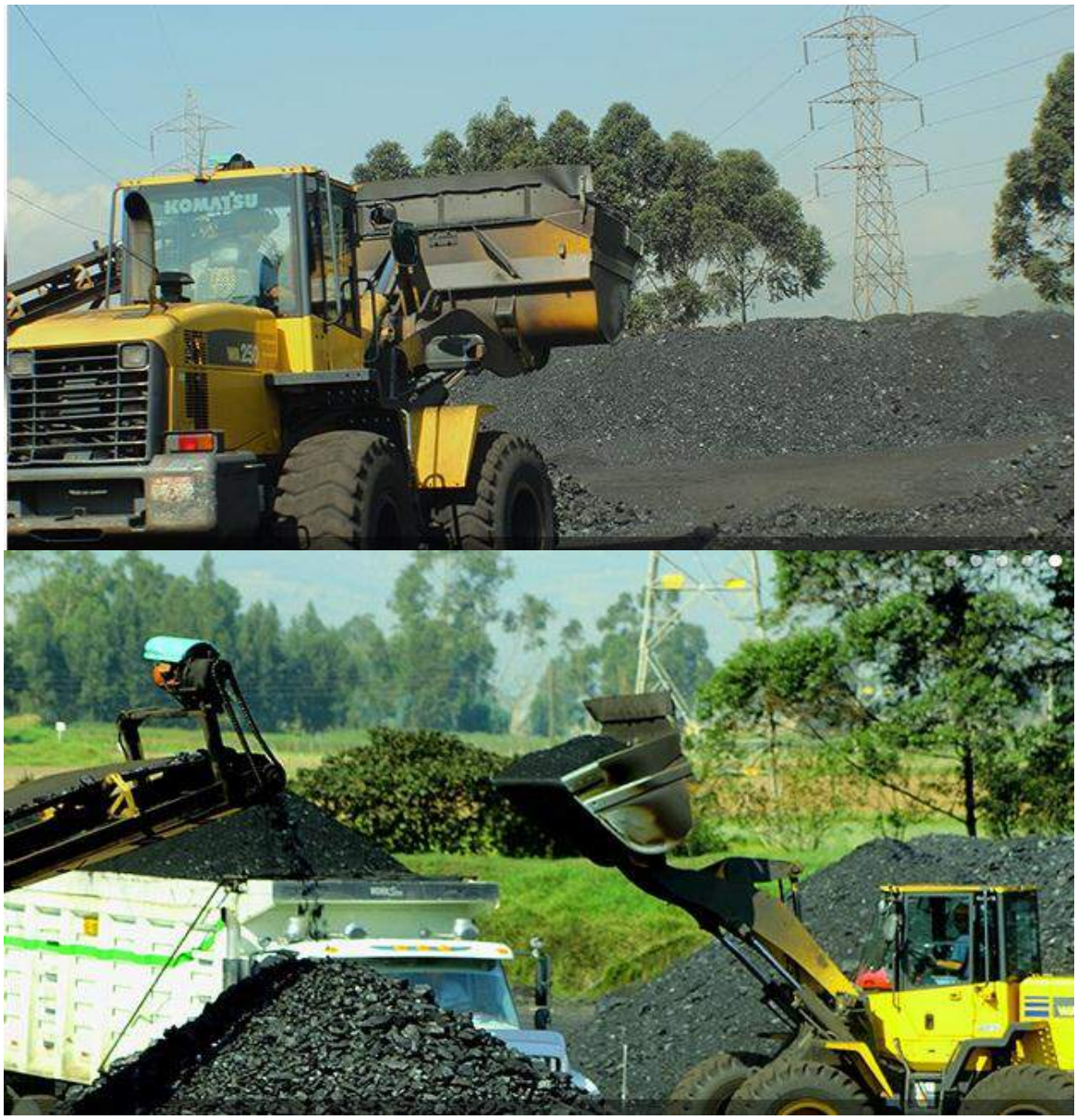


Fuente: División de sistemas Sanoha Ltda

8.3.1.3 Proceso de Remisiones

1. Empieza desde el apilado de carbón en el patio de acopio, del cual él operador de maquinaria según las características solicitadas en el pedido selecciona la pila de material y carga el vehículo como se observa en la ilustración 3.

Figura 14 Procedimiento de carga para remisión de material

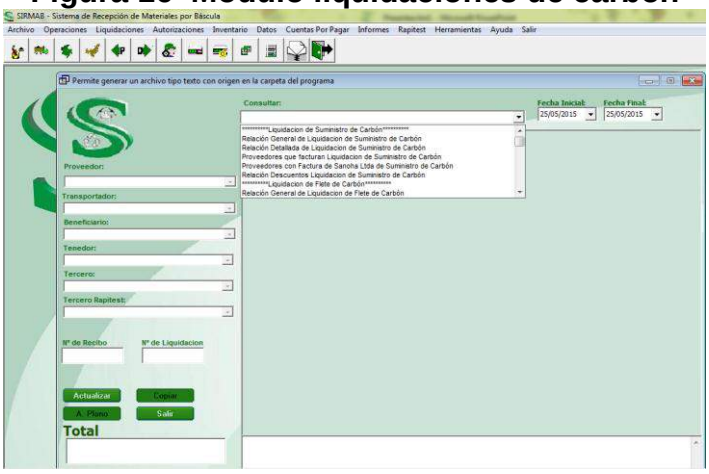


Fuente: Documentación proporcionada por Sanoha Ltda.

2. Se realiza el proceso de remisión el cual se guarda en el SIRMAB en remisiones, utilizando los siguientes atributos: peso tara, peso bruto, peso neto destino, material, tipo de carbón, numero de pedido, el número de planilla la cual hace referencia y el número de manifiesto de carga.
3. El proceso de remisiones lo que hace es esperar a que las empresas envíen los pesos de llegada para validarlos con los registrados en el SIRMAB al ingresarlos al sistema. Para hacer las facturas de acuerdo al precio que se pactó en el momento de la negociación. Ver imagen 12 y 13

Figura 15 Módulo de Remisiones

Figura 16 Modulo liquidaciones de carbón

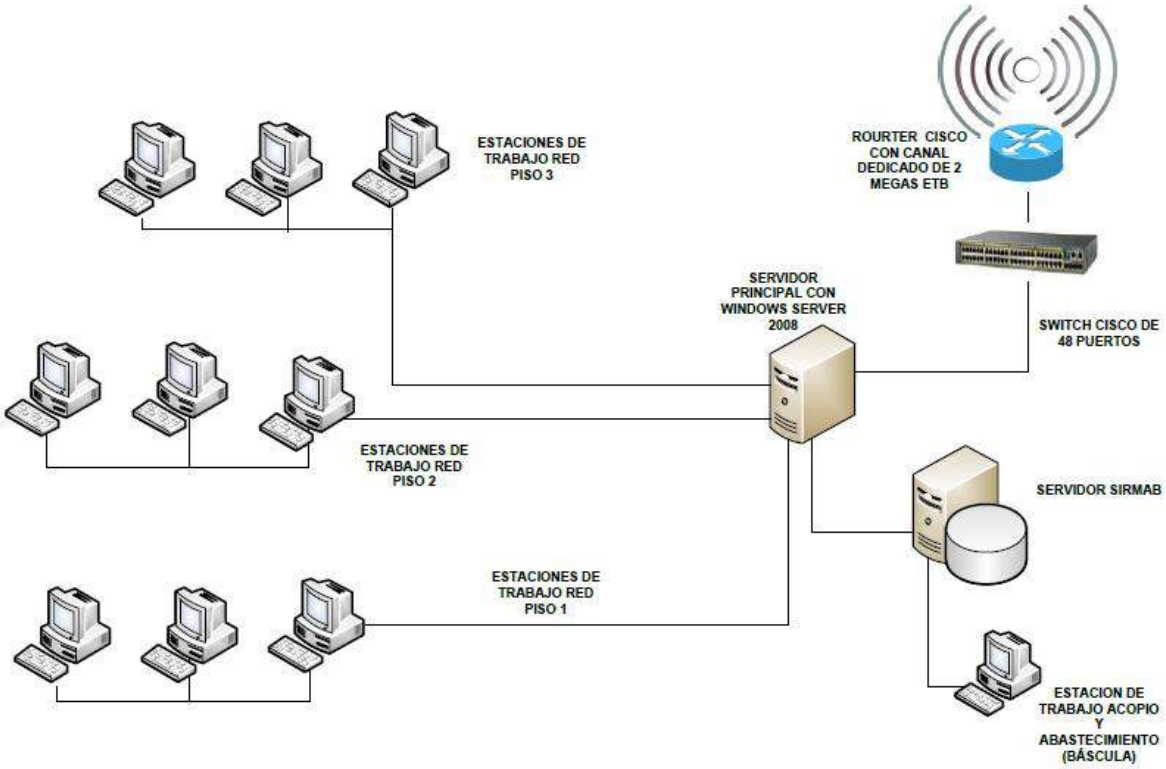


Fuente: División de sistemas Sanoha Ltda

Es decir de acuerdo a los 3 procesos anteriormente mencionados, las tareas que se efectúan en el área de automatización SIRMAB son: Registró en báscula, Control de ingresos y salidas (Vehículos, Suministro y Portería), Proveeduría de carbón , Perdidas de material por humedad, movimiento de transporte, cenizas, otros factores, Flete de carbón, Remisiones o salidas de carbón, Liquidación de carbón, Liquidación de fletes, Liquidación de causaciones, Inventario del acopio de carbón (según pilas clasificadas por propiedades físico-químicas), Servicios de báscula para empresas o personas independientes y Registro de resultados de laboratorio según las muestras proporcionadas por los proveedores.

8.5 SISTEMA INFORMÁTICO ACTUAL

Figura 17 Esquema de red actual de Sanoha Ltda



Fuente: Autor

Descripción

1. Modelos estándares si los tienen (certificaciones, normas internacionales)

- Cuentan con una red estructurada y certificada en categoría 6A, velocidad de trasferencia de una giga. Cumple los requisitos de certificación TIA-568-C e ISO 11801:2002 y tiene validado los servicios PoE de acuerdo con los estándares TIA/EIA.

2. Inventarios de sistemas de información y tecnología y tipos de redes utilizadas

- Red LAN topología en estrella velocidad de 1000 cable panduit
- Red Inalámbrica
- 1 ROUTER CISCO con canal dedicado de 2 megas PROVEEDOR DE INTERNET ETB
- 1 cuarto de comunicaciones

- Gabinete de 11 RMS, con su respectivo patch panel (AMP), organizador (DEXON) y multitoma.
- 1 ROURTER, para la distribución del internet CISCO con canal dedicado de 2 megas
- 1 PROVEEDOR DE INTERNET ETB
- 1 SWITCH CISCO DE 48 PUERTOS 10/100/1000 para la distribución de la red
- 1 servidor principal con sistema operativo WINDOWS SERVER 2003
- 1 servidor para el SIRMAB SORT equipo de sistemas operativos WINDOWS 7 64 bits memoria de 8 GB (POSTGRESQL)

3. Número de estaciones de trabajo del sistema total de Sanoha Ltda.

- 45 estaciones de trabajo con sistema operativo Windows 7, distribuidos en una edificación de 3 pisos.

4. Número de bases de datos, lenguaje en los que fueron creados, función, procesos que hacen cada uno, entre otras características.

- **Base de datos** LLAMADA **SIRMAB SORT** desarrollada en POSTGRESQL función automatización del proceso de compra de carbones liquidaciones facturación de suministros remisiones y servicios. Además tiene la función control del proceso de compra de materias primas, cotización, compra, inventarios, remisiones.

9 IDENTIFICACIÓN Y VALORACIÓN LAS AMENAZAS y VULNERABILIDADES SOBRE LOS ACTIVOS DEL PROCESO DE ACOPIO, ABASTECIMIENTO Y REMISIÓN DE CARBÓN EN EL ÁREA DE AUTOMATIZACIÓN DE BÁSCULA

9.1 VULNERABILIDADES Y AMENAZAS DE LOS ACTIVOS INFORMÁTICOS

En este punto se realiza una evaluación de los activos de información en el proceso de procesos seleccionados, considerando las dependencias entre éstos y realizando una valoración.

9.1.1 Descripción de activos

Tabla 3 Generalización de activos

Inventario de Activos	Descripción
Instalaciones	Localización de equipos informáticos y de comunicaciones
Hardware	Computadores y servidores que alojan datos, aplicaciones y servicios
Software	Programas que permiten manipular los datos.
Datos	Recurso fundamental el área de automatización de Báscula
Red	Equipos que permite intercambiar datos.
Servicios	Estos se efectúan de acuerdo a los datos que se ingresan, procesan y transmiten y que se necesitan para gestionar otros procesos dentro del sistema.
Equipamiento Auxiliar	Equipos de apoyo necesarios para complementar el funcionamiento de los demás equipos informáticos.
Soportes de Información	Medios y dispositivos que permiten almacenar la información.
Personal	Individuos que interaccionan y operan en los procesos y áreas informáticas.

9.1.2 Activos del proceso de acopio, abastecimiento y remisión de carbón en el área de automatización de báscula

Tabla 4 Activos del área de automatización de báscula

ÁMBITO	ACTIVO
Datos	Información de proveedores
	Información de pesajes en bascula
	Información de vehículos
	Información de transportadores
	Información de tipo de material
	Información de inventarios de material
	Información de liquidación de material
Servicios	Pesaje
	Análisis de muestras
	Facturación
	Acceso a la red
	Acceso a internet
SW	SIRMAB (Bases de datos)
	Sistema operativo
	Aplicaciones ofimáticas
HW	Router Cisco
	Servidor BBDD
	Servidor principal
	Terminal de Usuario en báscula
	Switch Cisco
	Discos Duros Removibles
	Unidades de Backup
Redes y comunicaciones	Red LAN
Soporte de Información	Formatos
	Comprobantes
Instalaciones	Oficina de acopio, abastecimiento y remisión de carbón
	Oficina de departamento operativo y de sistemas
Personal	Director de acopio
	Asistente de dirección de acopio
	Operadores de báscula
	Jefe de laboratorio
	Supervisor de operador de maquinaria
	muestreador
	Auxiliar de acopio
	Transportadores

9.1.2 Valoración de los activos de información

Teniendo definidos los activos se procede a establecer la escala a utilizar y los criterios. Para realizar la valoración de los activos de información se emplea una escala para cada criterio. Los criterios serán: disponibilidad, integridad, confidencialidad.

Tabla 5 valoración de los activos según criterio

CRITERIO	VALOR DEL ACTIVO SEGÚN CRITERIO		CLASE	DESCRIPCIÓN
DISPONIBILIDAD	Muy bajo	0	No es relevante	Soporta que el activo no esté disponible
	Bajo	1	Baja disponibilidad	Resiste que el activo no esté disponible por más de un día
	Medio	2	Disponibilidad mediana	Resiste que el activo no esté disponible por máximo medio o un día
	Alto	3	Alta disponibilidad	No acepta que el activo no esté en funcionamiento.
INTEGRIDAD	Muy bajo	0	No es relevante	La pérdida de exactitud y estado completo del activo no impacta negativamente al proceso.
	Bajo	1	Baja Integridad	La pérdida de exactitud y estado completo del activo impacta negativamente de manera leve al proceso.
	Medio	2	Mediana Integridad	El daño o modificación no autorizada genera un impacto significativo en la empresa
	Alto	**3**	Alta Integridad	El daño o modificación no autorizada genera un impacto importante en la empresa y podría conllevar a Problema grave o total de empresa
CONFIDENCIALIDAD	Muy bajo	0	No es relevante	El conocimiento o divulgación no autorizada de la información que gestiona este activo no impacta negativamente al proceso.
	Bajo	1	Disponible al público	Activo disponible para el público en general
	Medio	2	Para uso interno solamente	Activo disponible dentro de la organización con restricciones variadas con base en las necesidades de la empresa
	Alto	3	Estrictamente confidencial	Activo disponible sólo sobre la base de la necesidad estricta del conocimiento

9.1.3 Identificación de vulnerabilidades y amenazas

Tabla 6 vulnerabilidades y amenazas

CATEGORÍA	ACTIVO	VULNERABILIDAD	AMENAZAS	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	VALOR DEL ACTIVO SEGÚN CRITERIO
Datos	Información de proveedores Información de pesajes en bascula Información de vehículos Información de transportadores Información de tipo de material Información de inventarios de material Información de liquidación de material	• Los Backup son generados por SIRMAB cada viernes a las 6 am, es un lapso muy largo porque en el transcurso de la semana puede versen afectados los datos generados en los diferentes procesos de acopio, abastecimiento y remisión de carbón por cualquier incidencia no esperada haciendo que queden en riesgo, de la información no son debidamente etiquetados. • La asignación de perfiles de usuario no promueve la asignación de contraseñas seguras. • Los directivos permiten que jóvenes practicantes de sistemas, tengan contacto directo con los datos y del sistema de automatización sin ningún tipo de restricción. • No hay una herramienta para realizar imágenes de discos duros que garanticen la disponibilidad e integridad del sistema. • Falta de procedimientos para el manejo de información clasificada	• Cambios de electricidad drásticos que comprometan la integridad de la información. • Daño de discos duros y por ende perdida de datos. • Extracción de información por terceros. • Perdida de los Backup con información confidencial porque no hay un debido o ordenamiento, etiquetado y almacenamiento. • Fuga de información para la competencia. Infección de archivos. • Fraude.	ALTA	ALTA	ALTA	3
Servicios	Pesaje Análisis de muestras	• El sistema de automatización cuando no tiene energía los operadores hacen el proceso manualmente de los promedios de pesos de los vehículos que ingresan con carga e ingresan los valores posteriormente al sistema, prestándose para manipulación de datos. • La red no tiene un nivel de restricción para los	• Alteración de los datos por parte de los operarios cuando se realiza el proceso manualmente en báscula. • Saturación de servicios de red. • Escucha de los mensajes	MEDIA	MEDIA	MEDIA	2

	Facturación **Acceso a la red** **Acceso a internet**	servicios de internet porque los usuarios pueden recibir y enviar correos personales, descargar información, ingresar a cualquier página e instalar programas. • No hay una configuración adecuada del antivirus existente. • No hay mecanismos de encriptado de información.	transmitidos por la red. • Intrusiones de personas ajenas con fines delictivos. • Alteración de la continuidad del negocio en el área de servicios. • Problema de equipos de comunicación. • Problemas en el software de Acceso a Internet. • Perdida de comunicación con proveedores de Internet				
SW	**SIRMAB** **Sistema operativo** **Aplicaciones ofimáticas** **Router Cisco** **Servidor BBDD**	• No hay imágenes del disco del servidor de la base de datos que sirvan de respaldo en caso de pérdida total del programa de automatización. • No hay firewall que permita filtrar agentes externos que alteren el funcionamiento de los sistemas operativos. • No está configurado el software del router para que efectué su función de firewall (MAC de equipos). • Las contraseñas de los perfiles de administrador y de usuarios son fáciles de obtener a través de software que instalan los practicantes de sistemas. • Problemas en respaldo de la información. Pérdida de información. • Deficientes controles de seguridad en la base de datos • Fallos en restricciones en la base de datos. • Solo cuenta con la asignación de perfil de usuario • En los portátiles de los practicantes de sistemas cuentan con software pirata y además se conectan de la señal wifi de la empresa.	• Intrusión al sistema por hacker que altere la estructura de la base de datos SIRMAB. • Códigos maliciosos • Ataques de denegación de servicio, keyloggers. Infección y pérdida de archivos. • Eliminación, Modificación de información. • Errores de usuario. • Instalación de programas espía, de explotación de claves y de escaneo de red. • Alteración de la disponibilidad de la información primordial para el funcionamiento de Báscula. • Error de operación en el manejo del software. • Error en interno del SIRMAB. • Daño en alguno de los módulos de procesos del SIRMAB.	**ALTA**	**ALTA**	**ALTA**	3
HW	**Servidor principal** **Terminal de Usuario en báscula**	• No hay sistema de electricidad alterno. • No existe mantenimiento eléctrico y de los sistemas informáticos. • No hay sistemas de control, ni de prevención	• Robo y perdida de contenidos digitales que estén dentro de los equipos informáticos.	**MEDIA**	**MEDIA**	**MEDIA**	**2**

	Switch Cisco **Discos Duros Removibles** **Unidades de Backup**	que Implementen planes de contingencia en caso de robo, daño o desastre natural. • Problemas en el esquema de seguridad (Robos de Equipos), Incendios, Terremotos. • Falta de encriptación de los datos y mensajes trasmitidos en la red. • Además se hacen necesarios dispositivos y software que brinden mejor seguridad, filtrado y restricción a los sistemas informáticos.	• Colapso de comunicaciones. Alteración de la continuidad del negocio. • Errores en dispositivos. • Problemas en el servicio de internet de los puntos remotos. • Caída del servidor de archivos por Problema de software de red. • Problema en el suministro de energía eléctrica por mal funcionamiento del UPS. • Bajar incorrectamente el servidor de archivos. • Problemas causados usualmente por un error de chequeo de inconsistencia física. • Problemas de Componentes de Hardware del servidor. Virus. Sobrepasar el límite de almacenamiento del Disco				
Redes y comunicaciones	**Red LAN**	• La red solo cumple la función de compartir recursos y efectuar la comunicación sin seguir ninguna restricción. • No existe gestión de incidentes • Existe Manipulación de la configuración de red por personas ajenas al área de comunicaciones..	• Omisión de puertas traseras • Permitir el acceso de software malicioso y no emplear los filtros necesarios para evitar el acceso de posibles intrusos a los sistemas informáticos. • Sniffing, scanning, Denegación del servicio, enumeración, rootkit, interceptación de mensajes confidenciales etc. • Interceptación de paquetes transmitidos por red. • Problemas en el Cable UTP, Tarjeta de Red, IP, Switch, Patch Panel, Problemas en el servicio de internet de los puntos remotos. • Caída del servidor de archivos por Problema de	**MEDIA**	**MEDIA**	**MEDIA**	2

			software de red. • Falta de suministro de energía eléctrica por mal funcionamiento del UPS. • Caída de la Red LAN: Servidores Windows 7 y server 2008, equipos de comunicación. • Interrupción de las comunicaciones Internas y Externas. • Inactividad de los sistemas que soportan las funciones de la empresa. • Inactividad de operaciones de Informáticas • Acceso no autorizado e Interceptación de información • Modificación de la Información • Introducción de falsa información. • Fuerza bruta, suplantación, Phising, software malicioso, denegación del servicio. • Corrupción, Destrucción y Divulgación de la información • Perdidas económicas. • Inestabilidad de los procesos. • Fuga de información				
Soporte de Información	**Formatos** **Comprobantes**	• No existen formatos que registren los incidentes, ni las personas que los atienden. • No hay un manual de incidentes y tampoco de los equipos que se dan de baja. • No hay plan de contingencia que definan los procedimientos a efectuar y quienes serían los responsables..	• Manipulación de información para fines personales y económicos que permitan extraer datos confidenciales o equipos informática.	**BAJO**	**BAJO**	**BAJO**	**1**

Instalaciones	**Oficina de acopio, abastecimiento y remisión de carbón** **Oficina de departamento operativo y de sistemas**	• No hay sistemas de control, ni de prevención que Implementen planes de contingencia en caso de robo, daño o desastre natural.. • No existen cámaras de seguridad en el área e bascula. • No hay sistemas alternos de electricidad.	• Alteración de la continuidad del negocio • Perdida, daños, manipulación, robos en la infraestructura tecnológica. • Incendios y terremotos.	**BAJO**	**BAJO**	**BAJO**	**1**
Personal	**Director de acopio** **Asistente de dirección de acopio** **Operadores de báscula** **Jefe de laboratorio** **Supervisor de operador de maquinaria** **muestreador** **Auxiliar de acopio** **Transportadores**	• No hay funciones, ni responsabilidades asignadas en caso de haber una incidencia en la seguridad o ausencia del cargo. • No hay investigación de antecedentes del personal contratado, ni tampoco hacen firmar cláusula de confidencialidad. • No hay supervisión efectiva para monitorear los operadores de báscula en especial cuando por falta de energía deben hacer el proceso de promedios de pesos manualmente, que brinda un escenario para alteración y manipulación de datos. • Falta de conocimientos en estándares, herramientas, normas y protocolos de seguridad informática. • Ausencia de planes de seguridad para la prevención y mitigación de incidentes. • Falta de capacitación en prevención de los riesgos informáticos y sobre el buen manejo y confidencialidad de la información. • Ausencia de liderazgo en procesos de SGSI. • Falta de capacitación en prevención de los riesgos informáticos y sobre el buen manejo y confidencialidad de la información. • Manipulación incorrecta del SIRMAB. • No cuentan con personal indicado en caso que haya ausencia de uno de los operativos. • Procedimientos inadecuados de contratación • Entrenamiento insuficiente en seguridad • Uso incorrecto de software y hardware • Falta de conciencia acerca de la seguridad • Falta de mecanismos de monitoreo • Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	• Negligencia dentro de los procesos de automatización de báscula. • Errores de operación del SIRMAB • Ingeniería social • Sabotaje, Manipulación • Robo o pérdida de información confidencial de la empresa. • Exponer al sistema de automatización de báscula a negligencias informáticas que conllevan a la perdida de integridad, disponibilidad y confidencialidad de la información. • Errores de comunicación entre los departamentos. • Ingreso de datos erróneos o falsos al SIRMAB. • Omisiones de incidencias informáticas que conllevan a la pérdida de integridad, disponibilidad y confidencialidad de la información. • Desorganización e inoperatividad.	**MEDIA**	**MEDIA**	**MEDIA**	**2**

10 EVALUACIÓN DE RIESGOS

10.1 IDENTIFICACIÓN DE RIESGOS POR PROCESO

En esta identificación de riesgos se toma los tres procesos principales que influyen en el área de automatización de báscula: **Suministros, Pesaje y Remisiones** con el objetivo de segmentar el análisis de los riesgos y hallar de forma más detallada las causas y consecuencias de los mismos.

10.1.1 Riesgos proceso de Suministros

Este proceso se detalla en el numeral 8.3.1.1 y hace parte del funcionamiento del proceso del área de automatización de báscula (SIRMAB) Ver tabla 5.

Tabla 7 Riesgos proceso de Suministros

RIESGOS PROCESO DE SUMINISTROS DE MATERIAL EN BASCULA				
Objetivo General: Administrar la información sobre proveedores, vehículos de carga, conductores, muestras de material, procedencia del material o minas que procede para determinar el valor del material, realización de descuentos				
CÓDIGO DE RIESGO	**RIESGO**	**DESCRIPCIÓN**	**CAUSAS**	**CONSECUENCIAS**
1	**Error de Operación del SIRMAB en el proceso de suministro.**	Es primordial ingresar adecuadamente los datos de los proveedores, procedencia de material, placas de vehículos de carga entre otra información relacionada con el suministro.	• Personal sin la debida capacitación del proceso de suministro. • Omisión de alguno de los procedimientos de registro de información.	• Alteración de la integridad de los datos. • Reporte de información incorrecta.
2	**Perdida o alteración en las muestras de material proporcionada por el proveedor para análisis.**	La muestra proporcionada para suministro es fundamental para determinar su calidad y precio.	• Manipulación y almacenamiento inadecuado de las muestras. • Falta detalle en el etiquetado. • Sobrecarga de trabajo porque solo hay una persona encargada de realizar el análisis en el laboratorio.	• Perdida de material a analizar restringiendo el suministro. • Resultados erróneos • Retrasos de entrega de resultados de análisis.

3	**Error de comunicación entre procesos de muestreo en laboratorio y el proceso de suministros.**	Es fundamental que la comunicación y transmisión de datos deba darse en forma eficaz y oportuna.	• Error de red. • Fallo de sistema. • Fallo de electricidad	• Procesos manuales que se prestan para manipulación de datos. • Registro de información inexacta.
4	**Manipulación de resultados de muestreo en el laboratorio que pueden influir en el precio del material suministrado.**	Los resultados del laboratorio con respecto a las muestras de suministro son fundamentales para la liquidación a los proveedores.	• Falta de supervisión y auditoria interna de los procedimientos de muestreo.	• Liquidación errónea de proveedores. • Corrupción de los procesos de muestreo en laboratorio.
5	**Omitir la entrega de los comprobantes de ingreso de los vehículos de carga.**	Los comprobantes son la evidencia de los conductores han realizado la entrega del material y que han hecho el proceso de suministro.	• Error de operación. • No imprimir el comprobante. • Olvidar la entrega del comprobante.	• Inconformidad de los proveedores por omisión de procedimiento de entrega de comprobantes. • Perdida de comprobantes.
6	**Obstaculización de los procedimientos de suministro**	Los procedimientos de suministro deben cumplirse ordenadamente y siguiendo los lineamientos de la empresa.	• No cumplir con las funciones asignadas. • Desorden operativo. Personal conflictivo. • Falta de liderazgo. • Error de comunicación. • Error del SIRMAB.	• Limitar el funcionamiento del proceso de suministros. • Retraso en los tiempos de registro.
7	**Ausencia de personal operativo para la realización de los procedimientos de suministros.**	El proceso de suministros de material es la fase inicial que permite continuar con los procesos de pesaje y remisiones.	• No hay planificación en caso de ausencia de personal operativo. • No hay plan de contingencia.	• Asignar personal sin experiencia en el proceso. • Provocar errores en el sistema de automatización. • Omisión de ingreso de información fundamental para el proceso de suministros.

10.1.2 Riesgos proceso de Pesaje

Este proceso se detalla en el numeral 8.3.1.2 y hace parte esencial del funcionamiento del proceso del área de automatización de báscula (SIRMAB) porque de este depende la actividad de los procesos de suministros de acopio de material de proveedores y remisiones de material para el cumplimiento de pedidos

a clientes a nivel regional, nacional e internacional. Además influye directamente para el normal servicio de pesaje que ofrece a empresas independientes que también le genera ingresos importantes a Sanoha Ltda.

Tabla 8 Riesgos Proceso de Pesaje

RIESGOS PROCESO DE PESAJE EN BASCULA				
Objetivo General: Administrar la información capturada de la interfaz del indicador de peso electrónico y la báscula con respecto al peso bruto, peso tara y pesos netos de los diferentes vehículos de carga que suministran material de proveedores y que realizan las remisiones a clientes. Además de brindar el servicio de pesaje de otros vehículos y cargas a empresas independientes.				
CÓDIGO DE RIESGO	**RIESGO**	**DESCRIPCIÓN**	**CAUSAS**	**CONSECUENCIAS**
8	**Parar el sistema de automatización de pesaje en báscula.**	El proceso automático de pesaje en báscula funciona con electricidad y de esto depende una gran de la continuidad del negocio.	• Fallo de eléctrico. • Falta de suministro energía por causas externas. • No existe una fuente alterna de energía. • Fallo en la interfaz de la base de datos y el indicador de peso electrónico. • Daño del indicador de peso electrónico.	• Se ven obligados a realizar los pesajes de forma manual exponiendo a que se realicen promedios de peso según el criterio del operador de báscula. • Alteración de los datos por parte de los operarios cuando se realiza el proceso manualmente en báscula. • Limitar la eficacia de los procesos de pesaje en cuanto a tiempo y dinero.
9	**Error en la calibración del indicador electrónico de peso.**	El proceso de pesaje depende de los valores exactos de calibración en el indicador de peso electrónico de báscula.	• Falta de mantenimiento. • Fallo electrónico del indicador. • Cambios del entorno como movimiento del terreno donde está ubicada la báscula.	• Registro de pesajes erróneos. • Liquidación de materiales y proveedores incorrectos. • Remisión de material con pesaje de carga incompleta o con excedentes. • Costos de operación elevados.

10	**Error de operación del SIRMAB en el proceso de pesaje.**	La persona encargada debe manejar, registrar y velar que el proceso de pesaje sea efectuado correctamente.	• Falta de capacitación. • Omisión de alguno de los procedimientos. • Ingresar información en módulos no correspondientes. • Distractores que influyen en la concentración del operador (Lectura de correos personales, redes sociales , descarga de música, videos entre otros) • Oprimir incorrectamente las teclas F5 y F9 teclas función que cargar el peso bruto y tara en el proceso de pesaje.	• Alteración de la veracidad y disponibilidad de la información. • Demora en los tiempos de pesaje. • Realizar de forma invertida el pesaje de suministros y remisiones. • Registrar pesos invertidos al sistema. • Dejar pasar un vehículo con sobrecarga. • Invertir los procesos de suministros y remisiones en cuanto a la forma de pesaje.
11	**Ausencia del operador de su área de trabajo en el proceso de pesaje.**	El proceso de pesaje es continuo y debe estar disponible personal operativo listo para realizar cada procedimiento.	• Solo hay 2 operadores contratados, uno para cada jornada, hace falta de un operador suplente en caso de ausencia de alguno de ellos. • Asignar a cualquier otro empleado no competente para este proceso.	• Limitar el servicio de pesaje. • Retraso en los procesos de suministros y remisiones de material. Indisponer a los proveedores y clientes por posibles incumplimientos o retrasos. • Generará errores por omisión de procedimientos que afecten los registros de pesaje.
12	**Fallo de sistema en la comunicación y procesamiento en la red que proporciona el acceso a la base de datos del SIRMAB.**	Debe existir una constante conexión entre las estaciones de trabajo del área de bascula y el servidor donde reside el SIRMAB para que el cargue de los pesos brutos, tara y netos sean registrados y calculados correctamente.	• No existe gestión de incidentes. • No hay mantenimiento periódico de la red. • Daño en la Ups del rack de comunicaciones. • Daño en la Ups del servidor de la base de datos. • Cable UTP defectuoso.	• Inconvenientes en los registros de pesos. • Demoras en los procedimientos que dependen de la captura de pesaje bruto y tara. • Caída del sistema de automatización. • No poder realizar actividades de suministros y remisiones.
13	**Interrupción del Proceso de pesaje por desastre natural**	La báscula está en la entrada del acopio de Sanoha a cielo abierto.	• No existe plan de contingencia en caso de terremoto o rayos que pueden alterar la estructura física y electrónica de la báscula.	• Daño grave en la estructura física de báscula. • Inactividad de báscula. • Costos elevados por parar la continuidad de suministros, pesaje y remisiones.

14	**Corrosión de las vigas y soldaduras de distribución de carga por efecto del medio ambiente de la báscula.**	La báscula debe tener un mantenimiento al menos cada año que eviten inconvenientes de funcionamiento.	• Omitir el mantenimiento periódico de báscula.	• Daño grave en la estructura física de báscula. • Inactividad de báscula. • Costos elevados por parar la continuidad de suministros, pesaje y remisiones. Alteración en los valores de calibración.
15	**Error en el puerto 5432 que permite la interfaz y conexión entre báscula, el indicador de peso electrónico y el SIRMAB.**	El área de automatización de báscula depende del buen funcionamiento de todas sus partes.	• Variación inesperada de los voltajes eléctricos. • Cortos circuitos. • Des-configuración del puerto 5432 en el SIRMAB. • Código malicioso	• Inactividad de báscula • Costos elevados por parar la continuidad de suministros, pesaje y remisiones. •

10.1.3 Riesgos proceso de Remisiones

Este proceso se detalla en el numeral 8.3.1.3 y hace parte del funcionamiento del proceso del área de automatización de báscula (SIRMAB) maneja todo los pedidos de los clientes y despacha la carga de carbón según el destino. Ver tabla 7.

Tabla 9 Riesgos Proceso de Remisiones

RIESGOS PROCESO DE REMISIONES EN BASCULA				
Objetivo General: Administrar la información de los pedidos de clientes según las características solicitadas , cargue de material en vehículos de carga teniendo en cuenta la pilas de carbón existentes, peso neto destino, tipo de carbón, numero de pedido, el número de planilla la cual hace referencia y el número de manifiesto de carga.				
CÓDIGO DE RIESGO	**RIESGO**	**DESCRIPCIÓN**	**CAUSAS**	**CONSECUENCIAS**
16	**Retrasos en envíos de cargas de remisión. .**	Los pedidos son específicos en cuanto a características del material, tiempos de entrega y cantidades.	• Escasez de material solicitado en el acopio. • No tener parque automotor suficiente para entrega de remisiones de material. • Factores externos de la empresa (daños mecánicos, cierres de vías, ataques terroristas, accidentes viales etc.) • Fallos en bascula	• Incumplimiento de compromisos pactados con los clientes. • Sobrecostos para cumplir pedidos. • Pérdida de credibilidad • Pérdida de clientes

17	**Carga equivocada de material.**	Los pedidos deben cumplir con las características del carbón	• Falta de supervisión en el procedimiento de carga y verificación de material. • Omisión de características de material solicitado. • Confusión de pedidos por parte del supervisor. • Reporte equivocado de pedidos.	• Retrasos de entrega de pedidos. • Devolución de pedidos. • Cancelación de pedidos. • Costos de operación adicionales.
18	**Error de captura de pesos netos de remisiones**	Es importante que los pesos netos sean calculados correctamente para que coincidan con los pesos netos de los clientes.	• El operador de báscula puede realizar mal el procedimiento de pesaje que influye considerablemente en la liquidación del carbón. • Manipulación de pesos cuando se hace de forma manual el ingreso de los pesos. • Fallo en la automatización de bascula(SIRMAB)	• Conflicto entre empresa-clientes por no coincidir en los pesos netos. • Confusión en los procesos de remisión. • Exponer al SIRMAB a corrupción de datos.

10.2 ANÁLISIS DE RIESGOS

10.2.1 Niveles de Riesgo

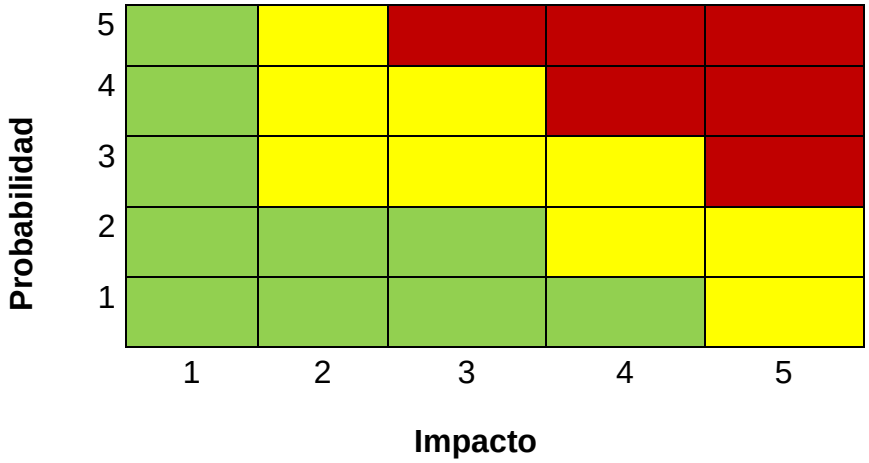
El análisis de riesgos tiene como fin valorar la probabilidad que suceda el riesgo y que tanto puede impactar los activos y la continuidad de los diferentes procesos que se desarrollan en el área de Automatización de Bascula. Para este análisis se emplean rangos de riesgos que se describen en la tabla 10 y la ponderación del impacto se explica en la tabla 11.

Tabla 10 Descripción de rangos de riesgos

RANGO	PROBABILIDAD RIESGO
1	**INSIGNIFICANTE**
2	**BAJO**
3	**MEDIO**
4	**ALTO**
5	**MUY ALTO**

Tabla 11 Descripción de ponderación respecto a probabilidad e impacto de riesgos

Color Rango	Impacto
	Leve
	Moderado
	Catastrófico



Teniendo en cuenta la identificación de los riesgos y el código de cada uno, se efectúa el análisis de los mismos según la probabilidad que sucedan y el impacto que pueden tener sobre los activos y el normal funcionamiento del área de automatización de báscula como se puede observar en las convenciones descritas en la tabla 11.

El análisis que se realiza en la tabla 12 se crea de acuerdo a los riesgos, su probabilidad de ocurrencia, rango diferenciado por el número, color y nivel de impacto. Asimismo los resultados del análisis focalizan los riesgos que pueden afectar considerablemente el funcionamiento del área de automatización del proceso de báscula, facilitando el diseño de estrategias de gestión reales y que conlleven a un mejoramiento continuo.

Tabla 12 Análisis de riesgos

CÓDIGO DE RIESGO	RIESGO	PROBABILIDAD	VALOR RANGO	IMPACTO
1	Error de Operación del SIRMAB en el proceso de suministro.	MEDIO	3	MODERADO
2	Perdida o alteración en las muestras de material proporcionada por el proveedor para análisis.	ALTO	4	CATASTROFICO
3	Error de comunicación entre procesos de muestreo en laboratorio y el proceso de suministros.	ALTO	4	CATASTROFICO

4	Manipulación de resultados de muestreo en el laboratorio que pueden influir en el precio del material suministrado.	**ALTO**	**4**	**CATASTROFICO**
5	Omitir la entrega de los comprobantes de ingreso de los vehículos de carga.	**BAJO**	**2**	**LEVE**
6	Obstaculización de los procedimientos de suministro	**BAJO**	**2**	**LEVE**
7	Ausencia de personal operativo para la realización de los procedimientos de suministros.	**BAJO**	**2**	**LEVE**
8	Parar el sistema de automatización de pesaje en báscula.	**ALTO**	**4**	**CATASTROFICO**
9	Error en la calibración del indicador electrónico de peso.	**MEDIO**	**3**	**MODERADO**
10	Error de operación del SIRMAB en el proceso de pesaje.	**ALTO**	**4**	**CATASTROFICO**
11	Ausencia del operador de su área de trabajo en el proceso de pesaje.	**BAJO**	**2**	**LEVE**
12	Fallo de sistema en la comunicación y procesamiento en la red que proporciona el acceso a la base de datos del SIRMAB.	**MUY ALTO**	**5**	**CATASTROFICO**
13	Interrupción del Proceso de pesaje por desastre natural	**BAJO**	**2**	**LEVE**
14	Corrosión de las vigas y de las soldaduras de distribución de carga por efecto del medio ambiente de la báscula.	**MEDIO**	**3**	**MODERADO**
15	Error en el puerto 5432 que permite la interfaz y conexión entre báscula, el indicador de peso electrónico y el SIRMAB.	**MUY ALTO**	**5**	**CATASTROFICO**
16	Retrasos en envíos de cargas de remisión. .	**MEDIO**	**3**	**MODERADO**
17	Carga equivocada de material.	**BAJO**	**2**	**LEVE**
18	Error de captura de pesos netos de remisiones	**BAJO**	**2**	**LEVE**

10.2.2 Cálculo del riesgo residual

A continuación se determina el cálculo del riesgo residual, que se obtiene de la relación entre el grado de exposición a los riesgos inherentes y la gestión de mitigación de los mismos establecida por la administración.

A partir del análisis y determinación del riesgo residual los administradores pueden tomar decisiones como la de continuar o abandonar la actividad dependiendo del nivel de riesgos; fortalecer controles o implantar nuevos controles. Ver tabla 13

Tabla 13 Escala de valoración de efectividad

CONTROL	EFECTIVIDAD
Ninguno	1
Bajo	2
Medio	3
Alto	4
Óptimo	5

(*) Promedio de los datos de efectividad
(**) Resultado de la división entre nivel de riesgo / Promedio de efectividad
(***) Promedio: Se considera un mismo peso de ponderación a los RI. (SIGWEB, 2012)

El calculo residual tiene niveles de tolerancia que de acuerdo a ellos se determinan que riesgos requieren una intervencion inmediata acompañado de acciones correctivas y cuales riesgos solo necesitan medidas de mejoramiento. Ver tabla 14 y 15.

Tabla 14 Descripción Nivel de Tolerancia del Cálculo Residual

RIESGO RESIDUAL	NIVEL DE TOLERANCIA	DESCRIPCIÓN
0.0 - 1	**ACEPTABLE**	Pueden existir oportunidades de mejora en la implementación de los controles y requieren supervisión.
1.1 - 3	**TOLERABLE**	Las actividades correctivas son requeridas y un plan debe ser diseñado para incorporar estas acciones dentro de un período de tiempo razonable.
3.1 - 5	**POR ARRIBA DE LA TOLERANCIA**	Se requiere de medidas correctivas. Un plan de acción correctivo a corto plazo o mediano plazo.

Tabla 15 Cálculo de Riesgos Residuales

código de riesgo	Riesgo	Nivel de Riesgo	CALIDAD DE GESTIÓN			RIESGO RESIDUAL (**)
			TIPO DE MEDIDAS DE CONTROL	EFECTIVIDAD	PROMEDIO (*)	
1	Error de Operación del SIRMAB en el proceso de suministro.	3	Reportar incidentes a la división de sistemas	3	**2,7**	**1,1**
			Copias de respaldo de información.	3		
			Capacitación de un día antes de contratación.	2		
2	Perdida o alteración en las muestras de material proporcionada por el proveedor para análisis.	4	Registro de muestras en el SIRMAB	3	**2,6**	**1,5**
			Etiquetado de muestras	3		
			Diligenciamiento de formatos físicos	2		
3	Error de comunicación entre procesos de muestreo en laboratorio y el proceso de suministros.	4	Avisar cualquier incidente de comunicación a la división de sistemas.	3	**3**	**1,3**
			Hay una persona encargada para el área de red.	3		
			Mantenimiento de red cada año	3		
4	Manipulación de resultados de muestreo en el laboratorio que pueden influir en el precio del material suministrado.	4	Conocer el manual de funciones.	2	**2,3**	**1,7**
			Se proporciona un laboratorio bien dotado.	2		
			Llamados de atención y memorandos en caso de errores.	3		
5	Omitir la entrega de los comprobantes de ingreso de los vehículos de carga.	2	Supervisión del jefe encargado.	4	**3,3**	**0,6**
			Letreros que recuerdan a los conductores reclamar los comprobantes.	3		
			Lamar a los conductores para que recojan sus comprobantes en caso de olvido.	3		
6	Obstaculización de los procedimientos de suministro	2	Supervisión del jefe encargado.	4	**3**	**0,7**
			Conocer el manual de convivencia y de funciones de la empresa.	2		
			Conocer y adaptarse a los procesos que tiene a cargo.	3		
7	Ausencia de personal operativo para la realización de los procedimientos de suministros.	2	Solicitud por escrito 3 días antes en caso de ausentarse del trabajo	3	**2,7**	**0,8**
			Sanciones y memorandos si se ausentan sin permiso p previo aviso.	2		
			Asignar temporalmente una persona que haga parte de departamento de Departamento de acopio y abastecimiento	3		
8	Parar el sistema de automatización de pesaje en báscula.	4	Reportar incidencia a la división de sistemas	2	**1,7**	**2,4**
			Realizar el proceso de pesaje de manera manual para no dejar de operar.	1		

			Llenar formatos físicos para registro de información sobre los pesos.	2		
9	Error en la calibración del indicador electrónico de peso.	3	Mantenimiento anual del indicador de pesos y bascula	5	**3,7**	**0,8**
			Reportar alteraciones en bascula a la División de sistemas	3		
			Supervisión del pesaje tanto en remisiones como en suministros.	3		
10	Error de operación del SIRMAB en el proceso de pesaje.	4	Supervisión de funciones y procesos	3	**3,0**	**1,3**
			Reporte de errores a la División de sistemas	3		
			Revisión por parte de alguien de sistemas	3		
11	Ausencia del operador de su área de trabajo en el proceso de pesaje.	2	Solicitar el permiso al jefe inmediato	3	**3,0**	**0,7**
			Supervisión de funciones por parte del jefe inmediato	3		
			Asignación temporal de una persona de acopio y abastecimiento	3		
12	Fallo de sistema en la comunicación y procesamiento en la red que proporciona el acceso a la base de datos del SIRMAB.	5	Reporte de fallos ala división de sistemas	3	**2,7**	**1,9**
			Revisión y determinar cuál fue el daño por parte de la persona encargada de la parte de red y base de datos	3		
			Realizar el proceso manualmente.	2		
13	Interrupción del Proceso de pesaje por desastre natural	2	Plan de contingencia por parte del departamento de salud ocupacional.	4	**4,0**	**0,5**
			Simulacros cada 6 meses	4		
			Conferencias sobre desastres naturales y salud ocupacional	4		
14	Corrosión de las vigas de distribución de carga por efecto del medio ambiente de la báscula.	3	mantenimiento preventivo cada año	3	**2,7**	**1,1**
			Seguimiento de cada una delas partes de la bascula	3		
			Reportar cualquier alteración de las partes de báscula a la división de sistemas.	2		
15	Error en el puerto 5432 que permite la interfaz y conexión entre báscula, el indicador de peso electrónico y el SIRMAB.	5	Reportar cualquier fallo a la división de sistemas	2	**2,3**	**2,17**
			Realizar el proceso manualmente.	2		
			Llamar a la empresa que brinda los servicios de mantenimiento de bascula	3		
16	Retrasos en envíos de cargas de remisión. .	3	Supervisión de funciones y responsabilidades de operadores de báscula.	3	**3,3**	**0,9**
			Verificación exhaustiva de los pedidos registrados y su especificaciones	4		
			Comunicación Continua con los clientes y confirmación de pedidos	3		
17	Carga equivocada de material.	2	Supervisión de funciones y responsabilidades de operadores de báscula.	3	**3,3**	**0,6**

			Verificación exhaustiva de los pedidos registrados y su especificaciones	4		
			Comunicación Continua con los clientes y confirmación de pedidos	3		
18	Error de captura de pesos netos de remisiones	2	Supervisión de procesos de remisión	3	**3,0**	**0,7**
			Cumplimiento de funciones por cada persona que interviene el proceso	3		
			Confirmación de procedimientos con el supervisor	3		

Los resultados del riesgo residual de acuerdo a los controles actuales de Sanoha, arrojan los siguientes niveles de tolerancia que permiten determinar en donde hay que mejorar controles y en donde hay que generar controles correctivos en un periodo adecuado.

Tabla 16 Resultados Nivel de Tolerancia a riesgos

RESULTADOS DE TOLERANCIA	CÓDIGO DE RIESGO
ACEPTABLE	5-6-7-9-11-13-16-17-18
TOLERABLE	1-2-3-4-8-10-12-14-15
POR ENCIMA DE LA TOLERANCIA	Ninguno

Los resultados de la tabla 16, muestran que No se detectan niveles de Tolerancia Altos, es decir, los riesgos detectados no exigen medidas correctivas y de urgencia. Sin embargo Sanoha en su área de automatización del proceso de bascula, cuenta con bastantes riesgos TOLERABLES correspondientes a los códigos 1-2-3-4-8-10-12-14-15 los cuales requieren controles efectivos pensando en una mejor gestión de las políticas de seguridad, porque pueden pasar a un nivel crítico e influir negativamente en la continuidad del negocio.

11. MODELO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN SGSI

11.1 Políticas y Objetivos de Seguridad de la Información

En base a la evaluación de riesgos efectuado en el capítulo 10 se diseñan las políticas de seguridad según la norma ISO/IEC 27001:2013 que establecen 14 dominios detallados en la tabla 15, con el objetivo de utilizar los controles de cada dominio como apoyo a la gestión de información para el área de automatización del proceso de báscula en Sanoha Ltda.

Tabla 17 Dominios y objetivos ISO7IEC27001:2013

ISO/IEC27001:2013
5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.2 Dispositivos para movilidad y teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.2 Durante la contratación.
7.3 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.2 Clasificación de la información.
8.3 Manejo de los soportes de almacenamiento.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.2 Gestión de acceso de usuario.
9.3 Responsabilidades del usuario.
9.4 Control de acceso a sistemas y aplicaciones.
10. CIFRADO.
10.1 Controles criptográficos.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.2 Seguridad de los equipos.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.2 Protección contra código malicioso.
12.3 Copias de seguridad.
12.4 Registro de actividad y supervisión.

12.5 Control del software en explotación.
12.6 Gestión de la vulnerabilidad técnica.
12.7 Consideraciones de las auditorías de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.2 Intercambio de información con partes externas.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.3 Datos de prueba.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.2 Gestión de la prestación del servicio por suministradores.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.2 Redundancias.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.2 Revisiones de la seguridad de la información.

Las políticas que se diseñan a continuación se crean en base a la identificación de amenazas del capítulo 9 y la evaluación de riesgos efectuada en el capítulo 10. También se tuvo en cuenta un checklist de prueba, donde se evalúa superficialmente los controles de la Norma ISO/IEC 27001:2013. Ver anexo D.

11.1.1 P5 Política de Seguridad

Se debe documentar las políticas y controles a seguir en el área de automatización del proceso de báscula, las cuales deben ser revisadas y contar con el visto bueno de la dirección.

La documentación de las políticas de seguridad debe detallar toda la normativa interna del área de automatización del proceso de báscula con el fin de que los funcionarios conozcan y cumplan las medidas de seguridad a través del sistema de gestión de seguridad. De igual manera debe especificar las buenas prácticas en cuento al acceso a la información, utilización de los activos físicos y lógicos del

proceso de báscula y las acciones en caso de incidentes que comprometen el funcionamiento del mismo.

Controles:

- Generar de forma responsable y detallada un documento de la política de seguridad de la información que permita gestionar de manera eficiente los incidentes de seguridad que puedan presentarse.
- Establecer medios e instrumentos que permitan la revisión de la política de seguridad de la información periódicamente.

11.1.2 P6 Aspectos Organizativos de la Seguridad de la Información

Debe existir compromiso de la dirección reconociendo la importancia de diseñar y posteriormente implementar un sistema de gestión de seguridad, creando un grupo de trabajo que cuente con un coordinador competente en el área de automatización del proceso de báscula en el departamento de Acopio y Abastecimiento.
También se debe tener en cuenta los aspectos externos como los riesgos que tiene que ver con el acceso a terceros, seguridad con respecto a los clientes y contratación con terceros.

Controles:
La Dirección de alta gerencia, la dirección de Acopio y Abastecimiento junto con la división de sistemas Sanoha Ltda deben estar comprometidos con el área de automatización del proceso de báscula y su sistema de gestión de seguridad en cuanto a:

- Cuidar la seguridad de los activos informáticos
- Supervisión eficaz de la administración de los sistemas informáticos y del procesamiento de la información.
- Diseño, documentación y aplicación de planes de seguridad y cumplimiento de políticas.
- Capacitación y sensibilización de usuarios que intervienen el proceso de báscula.
- Gestionar y coordinar un plan de contingencia, que apoye la gestión de incidentes solucionando en el menor tiempo los posibles problemas y que proporcione los procedimientos detallados que a su vez orienten y guíen a los empleados como actuar en una eventualidad.
- Supervisar el funcionamiento de los activos de información con el objetivo de monitorear alteraciones y factores que influyan negativamente en su seguridad.
- Designar un líder de dirección en el SGSI en el proceso de báscula junto con un equipo de trabajo donde cada uno debe tener roles específicos y funciones para poder administrar eficientemente el cumplimiento de los controles y políticas de seguridad.

11.1.3 P7 Seguridad Ligada a los Recursos Humanos

Un aspecto importante para reducir riesgos es contratar personal en primer lugar aplicando filtros que permitan establecer si realmente cuentan con las capacidades que se requieren de acuerdo a los perfiles solicitados. En segundo lugar hay que verificar antecedentes para evitar contratar personas que representen un riesgo para el área de automatización en el proceso de báscula.

Controles:

- Asignar las responsabilidades con respecto a protección de la información.
- Garantizar la seguridad y buen uso, así como mantener confidencialidad a la información que tiene acceso en su área de trabajo.
- Verificar al personal antes de ser contratado y establecer las debidas cláusulas contractuales para el cumplimiento de sus funciones, responsabilidades que tiene sobre los activos que utilizará entre otros.
- Definir los procedimientos que se deben efectuar cuando un empleado tenga cambio de funciones o cambio de cargo o haya salido de la empresa por diferentes motivos.
- Proporcional al personal contratado, toda la documentación necesaria para ejercer sus labores dentro del área de automatización del proceso de bascula.
- Aclarar que la información procesada, manipulada o almacenada por cada empleado en su área de trabajo es propiedad exclusiva de la Empresa Sanoha Ltda.
- Capacitar cada individuo contratado en aspectos de seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan.
- Generar respaldos de la información, diariamente con un horario fijo, para los activos de mayor importancia o críticos, un respaldo semanal que se utilizará en caso de fallas y un tercer respaldo efectuado semestralmente, el cual deberá ser guardado y evitar su utilización a menos que sea estrictamente necesaria.
- Las solicitudes de asistencia, efectuados por dos o más empleados o áreas de proceso, con problemas en las estaciones de trabajo, deberá dárseles solución en el menor tiempo posible.
- Documentar físicamente y digitalmente con formatos adecuados y estandarizados cualquier situación anómala y contraria a la seguridad, donde se verificara la situación y se dará una respuesta oportuna y acorde al incidente.

11.1.4 P8 Gestión de Activos

En el numeral 9.1 se detallan las vulnerabilidades y amenazas de los activos del área de automatización que permiten diseñar controles específicos para prevenir, gestionar y mitigar factores que pueden comprometer la continuidad del sistema.

Controles:

- Definir responsabilidades de acuerdo a cada proceso que intervenga en el área de automatización de bascula con el propósito de velen por el buen funcionamiento de los activos críticos.
- Supervisar a cada individuo que tenga a su cargo activos del proceso de báscula, se debe hacer responsable de los activos del área de trabajo, haciendo buen uso y manipulándolos de forma adecuada.
- Designar a la división de sistemas y apoyados con la dirección de Acopio y abastecimiento como los administradores de los sistemas y de los activos existentes en el proceso de báscula, responsabilizándose de la seguridad de la información almacenada en esos recursos.
- Tener documentado tanto en forma física y digital el Inventario de activos, los propietarios de los activos, la condición física y lógica de los activos, establecer directrices de clasificación y etiquetado aportando eficacia en el manejo de la información.

11.1.5 P9 Control de accesos

En base al análisis de riesgos realizado al área de automatización del proceso de báscula se requiere buen nivel de seguridad donde se deben implementar mecanismos y controles para asegurar un efectivo registro, identificación y autenticación de los usuarios del SIRMAB y de las áreas físicas del proceso de báscula. Asimismo, hay la necesidad de establecer mecanismos que aseguren el acceso bajo el principio del menor privilegio, requerido para realizar únicamente las tareas correspondientes a cada usuario, además de realizar una efectiva administración de usuarios y derechos de acceso.

Controles:

- El Coordinador de la división de sistemas proporcionará toda la documentación necesaria para agilizar la utilización de los sistemas, referente a formularios, guías, controles, otros, localizados en el sistema de gestión de seguridad del área de automatización del proceso de bascula de Sanoha.
- Si se necesita efectuar una petición, reporte o solicitud relacionada a la gestión de sistemas del departamento de Acopio y abastecimiento, se deberá el conducto regular formalmente establecido por la Sanoha.
- El recurso humano que intervienen el proceso de automatización del proceso de bascula deberán proteger sus equipos de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo temporal o cierre de sesión,

protegida por una contraseña, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.

- Cada una de las personas que laboran en el departamento de Acopio y abastecimiento en caso de detectar una falla de seguridad en los sistemas informáticos del área de automatización del proceso de báscula, estarán obligadas a reportarla a la división de sistemas o gestores de seguridad.
- En caso de la utilización indebida del servicio de correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema y se debe responsabilizar de la información que sea enviada con su cuenta.
- La división de sistemas deberá aplicar mecanismos que permitan monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red de Sanoha.
- Los usuarios deberán respetar la ley de derechos de autor, no instalando de forma ilegal licencias de software o reproducir información sin conocimiento del autor.
- El acceso al SIRMAB, se permitirá siempre y cuando se cumpla con los requerimientos de seguridad necesarios, y éste será permitido mediante un mecanismo de autenticación.
- Hay que restringir o deshabilitar cualquier acceso a la red sin previa autenticación o validación del usuario o el equipo implicado en el proceso de báscula.
- Se deberá supervisar cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, con el objetivo de verificar y auditar la seguridad de la misma.
- La división de sistemas está en la obligación de utilizar dispositivos de red para el bloqueo, enrutamiento, o el filtrado de tráfico evitando el acceso o flujo de información, no autorizada hacia la red interna o desde la red interna hacia el exterior.
- Es importante que la división de sistemas registren todo acceso a los dispositivos de red, mediante archivos de registro o Log, de los dispositivos que provean estos accesos.
- Cuando se finalice una sesión en cualquiera de las estaciones del departamento de Acopio y abastecimiento, los operadores o cualquier otro usuario del SIRMAB, evitara dejar encendido el equipo, pudiendo proporcionar un entorno de utilización de la estación de trabajo.
- La división de sistemas específicamente el personal del Área de Desarrollo de Sistemas de Información será la encargada del acceso a la configuración del servidor donde reside el sistema de automatización del proceso de bascula (SIRMAB).
- La división de sistemas deberá estructurar y especificar el nivel de permisos sobre las aplicaciones que ofrece SIRMAB, de acuerdo al nivel de ejecución o criticidad de las aplicaciones o archivos, y haciendo especial énfasis en

los derechos de escritura, lectura, modificación, ejecución o borrado de información.

- La división de sistemas se encargara de llevar un registro mediante Log de aplicaciones (SIRMAB), sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.
- La división de sistemas se encargara de registrar, documentar y archivar toda actividad, procedente del uso del SIRMAB, los sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.

11.1.6 P10 Cifrado

El cifrado de discos, documentos, archivos y la implementación de una infraestructura de clave pública Pki para el envío y recepción de información dentro del área de automatización del proceso de báscula, podría tomarse como opción a tener en cuenta para mejorar la seguridad de la información. La criptografía es una herramienta muy útil cuando se desea tener seguridad informática; puede ser también entendida como un medio para garantizar las propiedades de confidencialidad, integridad y disponibilidad de los recursos de un sistema. La criptografía es una herramienta de seguridad que le brindaría a Sanoha Ltda en su área de automatización en el proceso de báscula para proteger sus datos y encriptarlos donde únicamente las personas autorizadas puedan acceder a ellos por medio de llaves o firmas digitales. Sin embargo, en el caso que lleguen a ser vulnerados o extraídos del medio de transmisión, la criptografía debe garantizar que los mensajes no pueden ser leídos o desencriptados por personas ajenas o malintencionadas.

11.1.7 P11 Seguridad Física y Ambiental

Las oficinas, áreas físicas, equipos e infraestructura de red y eléctrica que hacen parte del proceso de automatización de báscula deben contar con mecanismos de seguridad que restrinjan el ingreso a personas externas que no tengan que ver con el departamento de acopio y abastecimiento. Además debe contar con las estructuras e instrumentos de contingencia en caso de desastres naturales como terremotos e incendios.

Controles:

- El cableado de red debe instalarse a una distancia adecuada de otro tipo de cables, (corriente o energía eléctrica), con el fin de prevenir interferencias.
- Supervisión y organización adecuada de los equipos o activos críticos de información y proceso (indicador electrónico de peso, estaciones de trabajo, Bascula, servidor SIRMAB, etc.) Deben ser ubicados en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por los supervisores de Acopio y abastecimiento, la división de sistemas y las personas responsables por esos activos.
- Las estaciones de trabajo que intervienen en el proceso de automatización de báscula y con la base de datos SIRMAB, cuyos procesamientos son sensibles e importantes para Sanoha, no deben de contar con medios de almacenamientos extraíbles, porque estos pueden prestarse para el robo y manipulación de la información.
- Se debe documentar y planificar los mantenimientos adecuados en forma periódica de tipo preventivo y correctivo de acuerdo a los requerimientos de cada equipo o maquinaria.
- Las oficinas o locaciones de trabajo deben poseer entre sus inventarios, elementos de prevención (extintores, alarmas contra incendios, lámpara de emergencia), requeridos para proteger los recursos tecnológicos y la información.
- El suministro de energía eléctrica debe estar debidamente polarizado y debe contar con suministros alternos de energía para garantizarla continuidad del proceso de automatización de bascula.
- Las instalaciones de las áreas de trabajo deben contar con una adecuada instalación eléctrica, y proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.
- Las salas o instalaciones físicas de procesamiento de información deberán poseer información en carteles, sobre accesos, alimentos o cualquier otra actividad contraria a la seguridad de la misma o de la información que ahí se procesa.

11.1.8 P12 Seguridad en la Operativa

Es primordial definir roles y responsabilidades en cuanto al manejo de seguridad en el proceso de automatización de bascula con el fin de tener un orden y procedimiento claro en caso de incidentes.

Controles:

- El recurso humano encargado de los diferentes procedimientos de automatización del proceso de báscula son responsables por mantener el funcionamiento óptimo de los procesos de suministros, pesaje y

remisiones, coordinando esfuerzos con el coordinador de división de sistemas, para fomentar una cultura de gestión segura.

- Los procedimientos, decisiones y reporte de incidencias deben estar coordinados con los supervisores, directores y personal de división de sistemas.
- El personal operativo de la automatización del proceso de bascula, llevará archivos de registro de fallas de seguridad del sistema, revisara, estos archivos de forma frecuente y en especial después de ocurrida una falla.
- En cuanto al manejo de software operativo y aplicativo se adquirirá y utilizará solo que este licenciado.
- El servidor donde reside la base de datos SIRMAB, al igual que las estaciones de trabajo del departamento de acopio y abastecimiento encargados del manejo de la automatización del proceso de bascula, tendrán instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.
- El mantenimiento del SIRMAB, del software operativo y de las aplicaciones será responsabilidad del personal de División de sistemas, o del personal de soporte técnico externo en caso de requerirse.
- El mantenimiento del indicador electrónico de peso y la báscula será responsabilidad de la empresa certificada proveedora de estos servicios, contactada directamente por Sanoha.
- Si es requerido algún cambio en el software o hardware en el departamento de Acopio y abastecimiento encargado del manejo de la automatización del proceso de báscula, deberá reportarse a los directores del área que a su vez los reportaran a la división de sistemas, donde será registrados para evaluarlos y determinar su prioridad .La división de sistemas llevará un registro global del mantenimientos efectuados sobre los equipos informáticos y de red, además de los cambios o novedades realizadas en ellos
- Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información del área de automatización del proceso de báscula, serán etiquetados de acuerdo a la información que almacenan u objetivo que suponga su uso, detallando su contenido.
- Los medios de almacenamiento con información sensible o copias de respaldo del SIRMAB, deberán ser manipulados exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su almacenamiento seguro.
- Todo medio de almacenamiento con información sensible (Backup del SIRMAB) será guardado bajo llave en un contenedor adecuado que brinden las condiciones físicas y ambientales al cual tendrá acceso únicamente, el gestor de seguridad o la alta gerencia.
- Se deberá detallar los medios de almacenamiento en los que se debe guardar información que se requiera en el área de automatización del proceso de báscula y su uso.

- Se deberá planificar auditorías periódicas internas que permitan supervisar los procedimientos realizados en los procesos de suministros, pesaje y remisiones que permitan detectar incidencias e irregularidades que permitan generan estrategias de mejoramiento.

11.1.9 P13 Seguridad en las Telecomunicaciones

Es importante que se apliquen mecanismos que dinamicen la Gestión de la seguridad en las redes, generando controles en los servicios de red, mensajería e intercambio de información en el área de automatización en el proceso de báscula.

Controles:

- Implementación de planes de seguridad, soporte y realización de auditorías internas y externas para hallar vulnerabilidades y hallar soluciones para las mismas.
- Implementación de Perfiles de administrador para gestionar las demás cuentas de usuario dentro de la red para restringir la instalación de programas a través de la configuración que brinda el mismo sistema operativo y con privilegios de administrador, este último actuara como responsable de la integridad del sistema de red y los archivos del mismo y establecerá un acceso controlado a los recursos de las estaciones y del servidor. De esta manera se anula la instalación de cualquier software que pueda vulnerar y dañar el funcionamiento del mismo. Además de programar que al detectar inactividad se suspenda las estaciones de trabajo automáticamente y que se requiera contraseña para volver al escritorio del sistema.
- Configurar dentro del sistema de administrador de red como Autoridad de seguridad para Controlar permisos de acceso al sistema, Gestionar servicios de autenticación, políticas de auditoria y registro de eventos auditados. También Configurar el Gestor de cuentas de usuario para mantener la DB de usuarios y grupos. También habilitar los servicios de validación de usuarios y el monitor de referencia de seguridad que facilitan el Control de acceso de usuarios a los objetos, verificando permisos, aplicando políticas de seguridad y generando eventos para registros de auditoría.
- Instalación, configuración y actualización de antivirus con el objetivo de evitar la aparición de lógica maliciosa y en caso de infección se detecte y se elimine de forma oportuna del sistema además que permita la inspección de los correos electrónicos evitando la infección de sus destinatarios.

11.1.10 P14 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Sanoha cuenta con SIRMAB (Sistema de Recepción de Materiales en Báscula) encargado de la automatización de los procesos de suministros, pesaje y remisiones, este sistema fue diseñado y programado como una base de datos a la medida para la empresa y actualmente es la base del funcionamiento de todos los procesos de la misma. De acuerdo al nivel de importancia de este sistema se hace necesaria la realización de pruebas para ajustar y mejorar las debilidades en seguridad y al mismo tiempo la validación que emplea. Asimismo es importante generar controles que vigilen todas las actividades relacionadas a la adquisición, desarrollo y mantenimiento de sistemas de información que interviene en el proceso de báscula.

Controles:

- Es función del Personal del Área de Desarrollo de Sistemas de Información debe documentar y establecer los privilegios que un usuario tiene sobre la base de datos (SIRMAB).
- El SIRMAB debe estar protegido contra desastres naturales y otras formas de destrucción. Se debe garantizar que los datos sean reconstruidos o recuperados en caso de daño, efectuando periódicamente un Backup de la información
- Los datos que se procesan en el SIRMAB deben poder ser sometidos a procesos de auditoria.
- Es recomendable que a la base de datos SIRMAB se le diseñe y programe funciones a prueba de intromisiones y que puedan verificar acciones que puedan alterar su funcionamiento en la red o supervisar cualquier acción indebida o errónea.
- Hay la necesidad de que SIRMAB implemente un mecanismo que permita demorar la respuesta de la base de datos ante claves erróneas y que limite los intentos a la misma. Además que permita registrar todas las entradas cada vez que un usuario de una estación de trabajo del departamento de Abastecimiento y acopio entra, y pueda chequear cuándo y desde dónde entró la vez anterior. De igual manera un aspecto que debe agregarse, es que se puedan realizar chequeos periódicos de claves fáciles de adivinar, procesos que llevan demasiado tiempo corriendo, permisos erróneos, actividades extrañas.

11.1.11 P15 Relaciones con Suministradores

Aquí se debe establecer los requisitos mínimos a cumplir para la contratación de terceros proveedores de material y de servicios para la realización de actividades

u operaciones de manera continua o temporal en el área de automatización del proceso de báscula.

Controles:

- Se debe definir claramente la Integración de los acuerdos de contratación, individualmente y en su totalidad, con los objetivos empresariales y estratégicos globales de la empresa de acuerdo a sus antecedentes, calidad, confianza y cumplimiento de los proveedores de material.
- Se sugiere que se establezcan cláusulas de confidencialidad y cumplimiento en los contratos de proveedores de suministros, para evitar una posible fuga de información corporativa y estratégica a la competencia o que se presente el incumplimiento de pedidos.

11.1.12 P16 Gestión de Incidentes en la Seguridad de la Información.

El área de automatización del proceso de báscula requiere apoyo de procedimientos de gestión de incidentes previamente documentados y divulgados para su conocimiento en el departamento de Abastecimiento y acopio. Las acciones especificadas en ellos serán ejecutadas respecto a los activos informáticos existentes con un orden y protocolo a seguir en el caso de presentarse un incidente de seguridad, esto con el propósito de mitigar el riesgo por las personas responsables y asignadas para tal fin.

Controles:

- Desarrollar un plan de contingencias para el sistema del área de automatización del proceso de bascula que incluye roles y responsabilidades, personal asignado con información de contacto y actividades relacionadas con el restablecimiento del sistema después de una interrupción o falla.
- Nombrar coordinadores del plan dentro del departamento de abastecimiento y acopio encargados de revisar y aprobar el plan y distribuir las copias al personal clave de contingencias.

11.1.13 P17 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

Sanoha depende del funcionamiento continuo de los procesos de suministros, pesaje y remisiones efectuados dentro del área de automatización del proceso de báscula, es por eso que se deben contemplar planes que sirvan para mantener el dinamismo de los procedimientos con respecto a los proveedores, inventarios, pedidos y clientes. Los planes diseñados tendrán en cuenta los puntos críticos de la empresa para protegerlos.

Controles:

- Los planes deben estar orientados a la seguridad de la información en el proceso de gestión de la continuidad del área de automatización del proceso de báscula.
- La gestión de continuidad del área de automatización del proceso de báscula estará planeado y diseñado en base a la evaluación de riesgos, haciendo uso de mecanismos de supervisión a través de pruebas, mantenimiento y reevaluación de planes de continuidad apoyado con auditorías internas que permitan la detección de fallos o posibles vulnerabilidades.

11.1.14 P18 Cumplimiento

Sanoha Ltda junto con su personal de división de sistemas y el departamento de abastecimiento y acopio, diseñara y autorizará el reglamento interno y externo en donde se consigne todas las normas que den cumplimiento de políticas y controles de seguridad para el área de automatización del proceso de báscula las cuales deberán ser divulgadas para su conocimiento y cumplimiento.

Controles:

- El personal del departamento de Abastecimiento y acopio y la división de sistemas utilizara software licenciado en sus estaciones de trabajo y servidores, donde bajo ninguna situación se permitirá el uso de software sin licencia, en el área de automatización del proceso de báscula.
- La división de sistemas, llevará un control exhaustivo con respecto a los inventarios de software referente a sus licencias y contratos firmados para ser usados en la infraestructura tecnológica de la red de Sanoha.
- La alta gerencia de Sanoha y dentro de sus políticas restringe totalmente que sus empleados puedan instalar software propio de la empresa en equipos informáticos externos a la misma.
- Sanoha y su personal encargado a razón de seguridad de sus activos, realizará copias de seguridad de las unidades de software que le son licenciadas con el fin proteger su información.
- El recurso humano que este contratado por Sanoha no podrá hacer uso externo de cualquier información, código u otros, producida, mediante tratamiento electrónico dentro de sus instalaciones, es propiedad irrevocable de la empresa.
- El personal de la red de Sanoha en especial el departamento de abastecimiento y acopio deberán tener total conocimiento de la documentación de seguridad, adherirse a esta para su cumplimiento.
- La ejecución de una auditoria a los sistemas informáticos del área de automatización del proceso de bascula, requiere una planificación previa y concienzuda de la misma, teniendo en claro las herramientas a utilizar,

objetivos, implicaciones legales, contractuales, requisitos y conformidad con la alta gerencia.

- El personal que se asigne para la auditoría no estará facultado para realizar cambios en los sistemas informáticos especialmente del SIRMAB, ya sea de los archivos que lo conforman o de la información que en este se procesa. Claro que si llega a presentar cualquier cambio intencional o accidental al sistema de archivos, será motivo de sanción.
- Las auditorías a los sistemas que intervienen en el departamento de abastecimiento y acopio, serán realizadas con equipos portátiles conectados a la red.

12. PLAN DE ACCION

El plan de acción se diseña de acuerdo al análisis de riesgos efectuado en el capítulo 10, tomando como base los riesgos que tienen mayor prioridad en el funcionamiento continuo del sistema y que poseen un nivel de tolerancia importante.

12.1 Operación del SIRMAB

Acciones de mejoramiento:

- SIRMAB (Sistema de Recepción de Materiales en Báscula) es el eje principal del área de automatización del proceso de báscula, lo que significa que requiere una constante supervisión por parte de la dirección del departamento de abastecimiento y acopio , la cual debe establecer responsabilidades del personal mediante una delegación y supervisión de tareas e incrementar la participación de los mismos en la toma de decisiones y en proposición de alternativas que contribuyan a mejorar la gestión de seguridad del SIRMAB.
- Contratar personal calificado y capacitado adecuadamente en el área de automatización del proceso de báscula, donde se asignan responsabilidades y funciones precisas.
- Diseñar e implementar planes de contingencia cuya estructura debe administrar incidencias usando mecanismos de notificación claramente definidos, según escenarios y estrategias que faciliten la prevención, control y mitigación junto con la designación de equipos de trabajo, funciones y responsabilidades, involucrando usuarios y administradores del departamento de abastecimiento y acopio, división de sistemas y alta gerencia..
- Deben generarse diariamente del SIRMAB, Backup de información que debe guardase en dispositivos extraíbles confiables para ser almacenados en contenedores que brinden las condiciones ambientales aptas para garantizar su integridad y disponibilidad en caso de contingencia, además hay que designar a las personas que se harán cargo de este procedimiento.

12.2 Manejo de muestras de material y análisis de resultados

Acciones de mejoramiento:

- Suministros en la parte de laboratorio debe mejorar el etiquetado de las muestras para que sean más detalladas al momento de su recepción y al momento de analizarlas para evitar confusiones o alteraciones en las mismas y en sus resultados.

- Es recomendable apoyar con otro profesional este proceso de análisis de muestras.
- Efectuar la supervisión y control por parte de la dirección del departamento de abastecimiento y acopio, que verifiquen el desarrollo de las diferentes actividades allí realizadas y se asegure que el muestreo, preservación y análisis de la muestra desde su recolección hasta el reporte de los resultados son adecuados.
- Los resultados deben corroborarse antes de ser ingresados al SIRMAB con el propósito de que estos sean confiables y que cuando sean requeridos por los procesos de pesaje y remisiones sean datos reales.
- La comunicación entre los procesos de suministros, pesaje y remisiones deben ser dinámica y sin retrasos que garantice el funcionamiento continuo del área de automatización del proceso de bascula.

12.3 Obstaculización de los procedimientos de suministro, pesaje y remisiones

Acciones de mejoramiento:

- Es importante que exista un ambiente de trabajo ameno y que las personas que allí laboran se sientan cómodas desarrollando sus atareas y funciones, pero esto debe ir de la mano de la Planeación, Organización e integración de Personal Alta gerencia y la Dirección y Control del departamento de abastecimiento y acopio, porque minimiza posibles errores por falta de concentración, alteración del carácter o sencillamente indisposición de los empleados.
- Se deben proporcionar los elementos, equipos, personal técnico y la documentación necesaria en el área de automatización del proceso de báscula, para que los procesos y procedimientos realizados sean de alta calidad.
- El acceso y operación del área de automatización del proceso de bascula, solo puede ser manipulada por recurso humano competente y no deben permitirse practicantes de sistemas que intervengan de un modo u otro con acciones que alteren la estabilidad y funcionamiento del mismo, porque la información que allí se procesa es relevante y confidencial para la continuidad del negocio. Salvo que estén monitoreadas y tengan un acompañamiento constante de una persona con experiencia y responsable que limite la intervención de los mismos.

12.4 Inactividad del sistema de automatización de pesaje en báscula.

Acciones de mejoramiento:

- El funcionamiento continuo de báscula influye directamente en la estabilidad de los procesos de operación, administración, comercialización, suministros, remisiones, pesaje, servicios entre otros.

Por tal razón se requiere que la empresa mejore su nivel de seguridad y la capacidad de contingencia en casos de fallos eléctricos o falta de energía, se aconseja adquirir fuentes alternas de energía para que no haya interrupciones o inactividad en los procedimientos de pesaje.

- Por seguridad e integridad de los datos que se ingresan al SIRMAB se recomienda que NO se haga manualmente el proceso de pesaje porque se expone a que se realicen promedios de peso según el criterio del operador de báscula y de esta manera se previene la alteración de los datos por parte de los mismos.
- Planear y efectuar revisiones y mantenimientos preventivos regularmente a las instalaciones e infraestructura eléctrica y electrónica de toda el área operativa de báscula.

12.5 Calibración del indicador electrónico de peso

Acciones de mejoramiento:

- Una calibración exacta permite garantizar que los pesos bruto, tara y neto sean correctos y que los precios del tipo de material a liquidar sean los que corresponden y que al momento de ser comparados con otras empresas se tenga la mínima o cero diferencia. Lo que hace necesario que BÁSCULAS SSAP S.A.S, empresa que provee los servicios de mantenimiento de báscula, siga realizando el mantenimiento de forma periódica tanto de indicador electrónico de pesos y báscula.
- Se debe crear mecanismos que incentiven a los operarios para que hagan un buen uso y cuiden los dispositivos eléctricos y de procesamiento vitales para el funcionamiento óptimo y continúo del área de automatización de báscula.
- El personal encargado del área de automatización deberá reportar cualquier anomalía en los elementos electrónicos que hacen parte del proceso de pesaje, en especial del indicador electrónico de pesos. Además de observar y reportar factores externos que pueden influir negativamente en estos mismos.

12.6 Proceso de comunicación, transmisión y acceso a la base de datos del SIRMAB desde la red.

Acciones de mejoramiento:

- Es importante que la división de sistemas en especial el área de redes y comunicaciones cuente con un plan y protocolo de atención de incidentes relacionados con la comunicación para que estos sean solucionados en el menor tiempo posible ,ya que debe existir una constante conexión entre las estaciones de trabajo del área de báscula y el servidor donde reside el SIRMAB, para que el cargue de los pesos bruto, tara y neto sean registrados y calculados correctamente, además de procesar los nuevos

datos y consultar información ingresada por suministros, pesaje y remisiones necesarias para su funcionamiento.

- Implementación de planes de seguridad, soporte y realización de auditorías internas frecuentes en la red específicamente en el departamento de Abastecimiento y acopio para hallar vulnerabilidades que representen riesgos al sistema. con el objetivo de contar con alternativas de solución oportunas y eficaces.
- Configuración correcta de antivirus y la administración eficiente del acceso a la red en cuanto a la asignación de perfiles de usuario, manejos de sesión y restricciones de escritura y modificación archivos de información.

CONCLUSIONES

El análisis de riesgos valoro la probabilidad que suceda el riesgo y que tanto puede impactar los activos y la continuidad de los diferentes procesos que se desarrollan en el área de Automatización de Bascula. Para este análisis se emplean rangos de riesgos que se describen en la tabla 10 y la ponderación del impacto se explica en la tabla 11.

La Identificación de riesgos se basa en los tres procesos principales que influyen en el área de automatización de báscula: Suministros, Pesaje y Remisiones con el objetivo de segmentar el análisis de los riesgos y hallar de forma más detallada las causas y consecuencias de los mismos.

El análisis de riesgos residual, muestran que No se detectan niveles de Tolerancia Altos, es decir, los riesgos detectados no exigen medidas correctivas y de urgencia. Sin embargo Sanoha en su área de automatización del proceso de bascula, cuenta con bastantes riesgos TOLERABLES correspondientes a los códigos de riesgo 1-2-3-4-8-10-12-14-15 los cuales requieren controles efectivos pensando en una mejor gestión de las políticas de seguridad, porque pueden pasar a un nivel crítico e influir negativamente en la continuidad del negocio.

En base a la evaluación de riesgos efectuado en el capítulo 10 se diseñan las políticas de seguridad según la norma ISO/IEC 27001:2013 que establecen 14 dominios detallados en la tabla 15, con el objetivo de utilizar los controles de cada dominio como apoyo a la gestión de información para el área de automatización del proceso de báscula en Sanoha Ltda.

Se diseña un plan de acción de acuerdo al análisis de riesgos efectuado en el capítulo 10, tomando como base los riesgos que tienen mayor prioridad en el funcionamiento continuo del sistema y que poseen un nivel de tolerancia importante.

RECOMENDACIONES

Es importante que exista un ambiente de trabajo ameno y que las personas que allí laboran se sientan cómodas desarrollando sus atareas y funciones, pero esto debe ir de la mano de la Planeación, Organización e integración de Personal Alta gerencia y la Dirección y Control del departamento de abastecimiento y acopio, porque minimiza posibles errores por falta de concentración, alteración del carácter o sencillamente indisposición de los empleados.

El funcionamiento continuo de báscula influye directamente en la estabilidad de los procesos de operación, administración, comercialización, suministros, remisiones, pesaje, servicios entre otros. Por tal razón se requiere que la empresa mejore su nivel de seguridad y la capacidad de contingencia en casos de fallos eléctricos o falta de energía, se aconseja adquirir fuentes alternas de energía para que no haya interrupciones o inactividad en los procedimientos de pesaje

SIRMAB (Sistema de Recepción de Materiales en Báscula) es el eje principal del área de automatización del proceso de báscula, lo que significa que requiere una constante supervisión por parte de la dirección del departamento de abastecimiento y acopio , la cual debe establecer responsabilidades del personal mediante una delegación y supervisión de tareas e incrementar la participación de los mismos en la toma de decisiones y en proposición de alternativas que contribuyan a mejorar la gestión de seguridad del SIRMAB.

Debe existir compromiso de la dirección reconociendo la importancia de diseñar y posteriormente implementar un sistema de gestión de seguridad, creando un grupo de trabajo que cuente con un coordinador competente en el área de automatización del proceso de báscula en el departamento de Acopio y Abastecimiento.

También se debe tener en cuenta los aspectos externos como los riesgos que tiene que ver con el acceso a terceros, seguridad con respecto a los clientes y contratación con terceros.

Implementación de planes de seguridad, soporte y realización de auditorías internas frecuentes en la red específicamente en el departamento de Abastecimiento y acopio para hallar vulnerabilidades que representen riesgos al sistema con el objetivo de contar con alternativas de solución oportunas y eficaces.

BIBLIOGRAFÍA

(Centro europeo de empresas de innovación CEI, 2010) SEGURIDAD DE LA INFORMACIÓN, ISO 27001

ISO/IEC 27000 “Information technology - Security techniques - Information security management systems - Overview and vocabulary”

UNIT - ISO/IEC 27001:2005. “Tecnología de la información – Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información – Requisitos”.

(Vargas, A.C &, Castro Mattei, A. 2011) Sistemas de Gestión de Seguridad de la Información Disponible en: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

ISO27000.es. “Sistema de Gestión de la Seguridad de la Información”. Disponible en: http://www.iso27000.es/doc_sgsi_all.htm (octubre de 2009)

Instituto Nacional de la Tecnología de la Comunicación de España. Centro de respuestas a incidentes de seguridad TIC. Recuperado de http://cert.inteco.es/cert/INTECOCERT/;jsessionid=8D54CF8208B2AAAA4A8AD638C109B9B0?postAction=getCertHome

Organización internacional de estándares- ISO. Sistema de Gestión de la Seguridad de la Información. Portal ISO 27001 en español. Recuperado de http://www.iso27000.es/sgsi.html

Universidad Politécnica de Madrid de España (2010). Information Security enciclopedia - Intypedia. Enciclopedia de la Seguridad de la Información. Recuperado de http://www.intypedia.com/

Jeimy J. Cano, Ph.D, CFE(2008). Seguridad Informática en Colombia. Tendencias 2008. Recuperado de http://www.acis.org.co/fileadmin/Revista_105/investigacion.pdf

Empresa de servicios virtuales para mypimes —esvem (2010). Lopez Alba, Tabare Parra, duarte. Estado de las mipymes colombianas frente al uso de las tic’s. Recuperado de http://www.gestiopolis.com/administracion-estrategia-2/uso-tecnologias-internet-comunicaciones-tics-en-mipymes-colombianas.pdf

Estudio anual 2014 de la empresa PandaLabs Disponible en: http://www.pandasecurity.com/colombia/about/why-panda/pandalabs/

Estudio sobre amenazas informáticas realizado por Viruslist Disponible en http://www.viruslist.com/sp/analysis?pubid=207271252

ANEXOS

ANEXO A: Carta de Autorización de la Empresa

SANOHA LTDA
Minería - Medio Ambiente y Forestal
NIT 800.188.412-0 REGIMEN COMÚN

Sogamoso 04 de Mayo de 2015

Por medio de la presente **SANOHA LTDA** expresa su interés de adoptar un Sistema de Gestión de Seguridad porque es una oportunidad para mejorar las políticas y procedimientos relacionados con la seguridad informática. Y por tal motivo autoriza a la Ingeniera **YENNY STELLA NUÑEZ ALVAREZ** identificada con C.C. No. 23810642 del Municipio de Nobsa para realizar el estudio y posterior diseño de un SGSI del Área de automatización del proceso de báscula bajo las siguientes condiciones:

- Deberá presentar su identificación correspondiente para el ingresar a la empresa y registrar sus entradas y salidas de la misma.
- Todas las actividades de investigación (encuestas, checklist, formatos de observación, entrevistas, etc.) deberán ser revisadas y supervisadas por la Ing. Mónica Hernández Jefe de la división de Sistemas.
- Si se realizan pruebas de seguridad deben ser con técnicas de mínimo impacto sobre la operación de la plataforma tecnológica del área de automatización del proceso de báscula, sin afectar la integridad, confidencialidad o disponibilidad de la información.

Se expide la presente solicitud a los 4 días del mes de Mayo de 2015

Cordialmente,

ING. LUIS CHIQUILLO
Gerente de SANOHA LTDA.

Nobsa. Km. 4 Vía Sogamoso-Belencito Teléfonos: (8)7729032 – 7726764 -7729033 Telefax: 7723673

ANEXO B: Formato de Observación de Procesos

FORMATO DE OBSERVACION DE PROCESOS	
Fecha:	
Departamento: ACOPIO Y ABASTECIMIENTO	
Tipo de Proceso: SUMINISTROS, PESAJE, REMISIONES	
Personas encargadas:	
NOMBRE DE PROCEDIMIENTO	**DESCRIPCIÓN**

ANEXO C: Formato de Encuesta sobre los Procesos del Área de Automatización del proceso de Bascula

ENCUESTA SOBRE LOS PROCESOS DEL AREA DE AUTOMATIZACION DEL PROCESO DE BASCULA

NOMBRE: _____

CARGO:

ESTA ENCUESTA SE REALIZA CON EL OBJETIVO DE CONOCER DE MANERA GENERAL EL FUNCIONAMIENTO DEL ÁREA DE BÁSCULA.
POR FAVOR MARQUE UNA X DE ACUERDO A LA PREGUNTA QUE SE ENUNCIA.

1. Hay extintores en caso de incendios

SI ☐ NO ☐

2. Existen planes de contingencia en caso de desastres naturales

SI ☐ NO ☐

3. Cuentan con cámaras de seguridad

SI ☐ NO ☐

4. Existe carnet de identificación para el ingreso de personas ajenas a las instalaciones de báscula

SI ☐ NO ☐

5. Existe personal de vigilancia en las entradas y salidas de bascula

SI ☐ NO ☐

6. ¿En el mes cuantas veces se presenta incidentes ya sea en el funcionamiento u operación en el área de automatización de bascula?

Ningún incidente ☐ 1-3 incidentes ☐ 4-8 incidentes ☐ Más de 9 incidentes ☐

7. ¿En el mes cuantas veces se presenta incidentes de comunicación con el sistema de automatización de bascula?

Ningún incidente ☐ 1-3 incidentes ☐ 4-8 incidentes ☐ Más de 9 incidentes ☐

8. Cuando hay la contratación de nuevo personal en el área de automatización de bascula, este recibe un inducción previa de:

1 día ☐ 1 semana ☐ 2 semanas ☐ Más de 2 semanas ☐

9. El mantenimiento de bascula y su sistema electrónico se realiza cada:

6 meses ☐ 1 año ☐ 2 años ☐ Más de 2 años ☐

10. ¿Se manejan formatos para llevar los registros de los incidentes o errores que puedan presentarse en el área de automatización del proceso de báscula?

SI ☐ NO ☐

ANEXO D: Checklist de prueba

ISO/IEC 27002:2013 SANOHA LTDA						
REFERENCIA			**EVALUACION DE CUMPLIMIENTO POR AREA**		**RESULTADOS**	
CHECKLIST		**ESTANDAR**	**SECCION**	**PUNTOS DE EVALUCION INCIAL**	**RECOMENDACIONES**	**PORCENTAJE DE CUMPLIMIENTO**
SI	**NO**					
		A.5	**POLÍTICAS DE SEGURIDAD.**			
		A.5.1	**Directrices de la Dirección en seguridad de la información.**			
	X	**A. 5.1.1**	**Conjunto de políticas para la seguridad de la información.**	¿Existen políticas de seguridad?		0 %
				¿Todas las políticas son aprobadas por la gerencia?		
				¿Las políticas son adecuadamente comunicadas a los empleados?		
X		**A. 5.1.2**	**Revisión de las políticas para la seguridad de la información.**	¿Las condiciones de seguridad son objeto de revisión?		10 %
				¿Se realiza su revisión periódicamente?		
				¿ la revisión llevada a cabo tiene en cuenta el cambio de condiciones?		
		A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION**			
		A.6.1	**Organización interna.**			
X		**A. 6.1.1**	**Asignación de responsabilidades para la seguridad de la información.**	¿ las responsabilidades para la protección de los activos individuales, y para llevar a cabo los procesos de seguridad específicas, son claramente identificadas , definidas y comunicadas a las partes interesadas?		20%
X		**A. 6.1.2**	**Segregación de tareas**	¿Los deberes y áreas de responsabilidad son separados, con el fin de reducir las oportunidades para la modificación o mal uso de la información o servicio no autorizado?		10%
	X	**A.6.1.3**	**Contacto con las autoridades.**	¿Existe la documentación donde se registre los datos de contacto de las diferentes autoridades pertinentes en caso de incidencias (aplicación de la ley, etc.)?		0%
				¿Hay un proceso que detalla cómo y cuándo se requiere del contacto de las autoridades?		
				¿Existe un proceso para determinar cuándo efectuar el contacto con las autoridades o si requiere un intercambio de información?		
	X	**A.6.1.4**	**Contacto con grupos de interés especial.**	¿Existen las personas dentro de la organización, encargadas de mantener relación con grupos de intereses especiales relevantes?		0 %
	X	**A.6.1.5**	**Seguridad de la información en la gestión de proyectos.**	¿Todos los proyectos pasan por algún tipo de evaluación de seguridad de información?		0 %
		A. 6.2	**Dispositivos para movilidad y teletrabajo.**			

ISO/IEC 27002:2013 SANOHA LTDA						
REFERENCIA			EVALUACION DE CUMPLIMIENTO POR AREA		RESULTADOS	
CHECKLIST		ESTANDAR	SECCION	PUNTOS DE EVALUCION INCIAL	RECOMENDACIONES	PORCENTAJE DE CUMPLIMIENTO
SI	NO					
	X	**A. 6.2.1**	**Política de uso de dispositivos para movilidad**	¿Existe una política de dispositivo móvil?		0 %
				¿Existe la documentación donde se mencionen riesgos y las políticas a seguir de acuerdo al uso de dispositivos móviles (por ejemplo, el robo de activos, uso de puntos de acceso inalámbricos abiertos?		
				¿Las políticas tienen aprobación de gerencia?		
	X	**A.6.2.2**	**Teletrabajo.**	¿Hay una política de teletrabajo?		0 %
				¿Las políticas tienen la aprobación de las directivas?		
				¿Hay un proceso establecido para la operatividad remota?		
				¿Los tele trabajadores cuentan con las condiciones y equipo necesario para proteger sus activos?		
		A.7.	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**			
		A.7.1	**Antes de la contratación.**			
	X	**A.7.1.1**	**Investigación de antecedentes.**	¿Existen controles de verificación de antecedentes, realizados con todos los nuevos candidatos a contratar?		0 %
				¿Los controles están previamente autorizados por la dirección administrativa?		
				¿Esta definidos los controles de cumplimiento de las leyes, reglamentos y ética?		
				¿Los controles exigidos a los candidatos sirven como apoyo de las evaluaciones de riesgos?		
	X	**A.7.1.2**	**Términos y condiciones de contratación.**	¿a todos los empleados , contratistas y terceros se les pide que firmen acuerdos de confidencialidad y no divulgación?		0 %
				¿Los contratos laborales y de servicios cuentan con las condiciones y términos necesarios para proteger la información empresarial?		
		A.7.2	**Durante la contratación.**			
	X	**A.7.2.1**	**Responsabilidades de gestión.**	¿Todos los administradores participan en la gestión de la seguridad de la empresa?		0 %
				¿La gestión de seguridad y administrativos incentivan a que se empleen las políticas de seguridad a todos los empleados, contratistas y usuarios y seguir los procedimientos establecidos?		

ISO/IEC 27002:2013 SANOHA LTDA						
REFERENCIA			EVALUACION DE CUMPLIMIENTO POR AREA		RESULTADOS	
CHECKLIST		ESTANDAR	SECCION	PUNTOS DE EVALUCION INCIAL	RECOMENDACIONES	PORCENTAJE DE CUMPLIMIENTO
SI	NO					
	X	**A.7.2.2**	**Concienciación, educación y capacitación en segur. de la información**	¿Los empleados, contratistas y usuarios son sensibilizados y capacitados periódicamente con el objetivo de comprender su papel y función dentro de la organización para la protección y seguridad informática?		0 %
	X	**A.7.2.3**	**Proceso disciplinario.**	¿Hay un proceso disciplinario formal que permite a la organización a tomar medidas contra los empleados que hayan cometido una violación de la seguridad de información?		0 %
		A.7.3	**Cese o cambio de puesto de trabajo.**			
	X	**A.7.3.1**	**Cese o cambio de puesto de trabajo.**	¿Hay un proceso documentado para la terminación o el cambio del puesto de trabajo?		0 %
				¿Están establecidos los procedimientos de protección de la información en caso de ausencia del empleado encargado?		
				¿La organización hace cumplir los procedimientos en caso de ausencia o cambio del puesto de trabajo?		
		A.8.	**GESTIÓN DE ACTIVOS.**			
		A.8.1.	**Responsabilidad sobre los activos.**			
X		**A.8.1.1**	**Inventario de activos.**	¿Se cuenta definidos e inventariados por categoría los activos den la organización?		10%
	X	**A.8.1.2**	**Propiedad de los activos.**	¿Esta documentados los activos con su respectivos propietarios?		0 %
X		**A.8.1.3**	**Uso aceptable de los activos.**	¿Se monitorea periódicamente que los activos funcionen correctamente o si hay alteraciones en su funcionamiento?		10%
	X	**A.8.1.4**	**Devolución de activos.**	¿Hay proceso para asegurar que todos los empleados y los usuarios externos en caso préstamo de activos sean devueltos a la organización en la terminación de su empleo, contrato o acuerdo?		0 %
		A.8.2	**Clasificación de la información.**			
	X	**A.8.2.1**	**Directrices de clasificación.**	¿Se cuenta con la documentación necesaria en la que se clasificación de la información?		0 %
	X	**A.8.2.2**	**Etiquetado y manipulado de la información.**	¿Existen los procedimientos que detallen los parámetros para etiquetar y clasificar la información?		0 %
	X	**A.8.2.3**	**Manipulación de activos.**	¿Se definen las personas y procedimientos para una a correcta manipulación de los activos?		0 %
		A. 8.3	**Manejo de los soportes de almacenamiento**			
	X	**A.8.3.1**	**Gestión de soportes extraíbles**	¿Se documenta como y quienes pueden gestionar los soportes extraíbles de la empresa?		0 %

ISO/IEC 27002:2013 SANOHA LTDA						
REFERENCIA			EVALUACION DE CUMPLIMIENTO POR AREA		RESULTADOS	
CHECKLIST		ESTANDAR	SECCION	PUNTOS DE EVALUCION INCIAL	RECOMENDACIONES	PORCENTAJE DE CUMPLIMIENTO
SI	NO					
	X	**A.8.3.2**	**Eliminación de soportes.**	¿Está documentado y con los debidos procedimientos para el manejo de procesos de eliminación de información, asegurando la confidencialidad de los mismos?		0 %
		A.9.	**CONTROL DE ACCESOS.**			
		A.9.1	**Requisitos de negocio para el control de accesos.**			
X		**A.9.1.1**	**Política de control de accesos.**	¿Se definen, se cumplen y están documentadas las políticas e seguridad para el control de accesos?		10%
X		**A.9.1.2**	**Control de acceso a las redes y servicios asociados.**	¿Existen el personal y los procedimientos pertinentes para la gestión de políticas de control de acceso a redes y servicios asociados?		10%
		A. 9.2	**Gestión de acceso de usuario.**			
	X	**A. 9.2.1**	**Gestión de altas/bajas en el registro de usuarios.**	¿Están documentados los procedimientos de gestión para habilitar y deshabilitar el registro o de usuarios del sistema según el control de accesos?		0 %
X		**A.9.2.2**	**Gestión de los derechos de acceso asignados a usuarios.**	¿Las políticas de seguridad tienen definidas las acciones para obtener los derechos de acceso según perfiles de usuario?		14%
	X	**A.9.2.3**	**Gestión de los derechos de acceso con privilegios especiales.**	¿Existe políticas pertinentes que especifiquen como gestionar los derechos de accesos especiales?		0 %
	X	**A.9.2.4**	**Gestión de información confidencial de autenticación de usuarios.**	¿Las políticas de seguridad están diseñadas para que se sigan procedimientos adecuados para proporcionar autenticación de usuarios según perfiles?		0 %
	X	**A.9.2.5**	**Revisión de los derechos de acceso de los usuarios.**	¿Hay planes de auditorio o revisión periódica para determinar si los derechos de acceso son los pertinentes?		0 %
	X	**A.9.2.6**	**Retirada o adaptación de los derechos de acceso**	¿Existen los procedimientos con las acciones necesarias y que hay que cumplir si hay una novedad de derechos de acceso en el sistema?		
		A.9.3	**Responsabilidades del usuario.**			
	X	**A.9.3.1**	**Uso de información confidencial para la autenticación.**	¿Los usuarios comprenden y están enterados de las responsabilidades individuales en cuanto al manejo de información confidencial y manejo adecuado de los mismos?		0 %
		A.9.4	**Control de acceso a sistemas y aplicaciones.**			
	X	**A.9.4.1**	**Restricción del acceso a la información.**	¿Las políticas existentes describen detalladamente cuales son las restricciones de acceso a la información?		0 %

ISO/IEC 27002:2013 SANOHA LTDA						
REFERENCIA			EVALUACION DE CUMPLIMIENTO POR AREA		RESULTADOS	
CHECKLIST		ESTANDAR	SECCION	PUNTOS DE EVALUCION INCIAL	RECOMENDACIONES	PORCENTAJE DE CUMPLIMIENTO
SI	NO					
	X	**A.9.4.2**	**Procedimientos seguros de inicio de sesión.**	¿Están documentados los procedimientos que deben seguir en para un adecuado inicio de sesión?		0 %
	X	**A.9.4.3**	**Gestión de contraseñas de usuario.**	¿Hay capacitación y la administración adecuada para el manejo y asignación de contraseñas?		0 %
	X	**A.9.4.4**	**Uso de herramientas de administración de sistemas.**	¿Los administradores de sistemas conocen y documentan las herramientas que se utilizan para gestionar los recursos y seguridad de los sistemas?		0 %
X		**A.9.4.5**	**Control de acceso al código fuente de los programas.**	¿Existe restricción y protocolos a seguir en el control de acceso al código fuente de los programas?		12%
		A.10.	**CIFRADO.**			
		A.10.1	**Controles criptográficos.**			
	X	**A.10.1.1**	**Política de uso de los controles criptográficos.**	¿Existen políticas y sistemas de cifrado para la protección en la transmisión de la información en la red e internet?		0 %
	X	**A.10.1.2**	**Gestión de claves.**	¿Se cuenta con infraestructura para la gestión de certificados digitales, claves públicas y privadas para el aseguramiento de la integridad y confidencialidad de los mensajes?		0 %
		A.11.	**SEGURIDAD FÍSICA Y AMBIENTAL.**			
		A.11.1	**Áreas seguras.**			
	X	**A.11.1.1**	**Perímetro de seguridad física.**	¿Hay un perímetro de seguridad designado? ¿Las áreas de información sensible o crítica son identificadas y adecuadamente controladas?		
X		**A.11.1.2**	**Controles físicos de entrada.**	¿Existen controles adecuados que filtren la entrada de personas ajenas a las instalaciones?		60%
	X	**A.11.1.3**	**Seguridad de oficinas, despachos y recursos.**	¿Tienen sistemas de control de entrada adecuadas para garantizar que sólo el personal autorizado tenga acceso?		0 %
	X	**A.11.1.4**	**Protección contra las amenazas externas y ambientales.**	¿Existen planes de contingencia que permitan saber los procedimientos y controles a seguir en caso de amenazas externas o ambientales?		0 %
	X	**A.11.1.5**	**El trabajo en áreas seguras.**	¿Existen planes de seguridad interna y externa que permitan saber los procedimientos y controles a seguir en caso de amenazas externas?		0 %
X		**A.11.1.6**	**Áreas de acceso público, carga y descarga.**	¿Existen zonas seguras? ¿Las áreas seguras cuentan con políticas y procesos adecuados? ¿Las políticas y procesos de seguridad existentes son monitoreados y controlados?		30%
		A.11.2	**Seguridad de los equipos.**			

ISO/IEC 27002:2013 SANOHA LTDA						
REFERENCIA			EVALUACION DE CUMPLIMIENTO POR AREA		RESULTADOS	
CHECKLIST		ESTANDAR	SECCION	PUNTOS DE EVALUCION INCIAL	RECOMENDACIONES	PORCENTAJE DE CUMPLIMIENTO
SI	NO					
	X	**A.11.2.1**	**Emplazamiento y protección de equipos.**	¿los procedimientos utilizados documentan y controlan pertinentemente el emplazamiento y protección de los equipos'		0 %
X		**A.11.2.2**	**Instalaciones de suministro.**	¿El ambiente y las condiciones físicas de las instalaciones son adecuados?		50%
X		**A.11.2.3**	**Seguridad del cableado.**	¿Hay un mantenimiento y monitoreo periódico de los sistemas de cableado de datos y eléctricos para garantizar el funcionamiento de los mismos?		50%
X		**A.11.2.4**	**Mantenimiento de los equipos.**	¿Hay un plan de mantenimiento periódico de los equipos?		50%
	X	**A.11.2.5**	**Salida de activos fuera de las dependencias de la empresa.**	¿Existen y se utilizan formatos de registro que controlen Salida de activos fuera de las dependencias de la empresa?		0 %
	X	**A.11.2.6**	**Seguridad de los equipos y activos fuera de las instalaciones.**	¿Existen las políticas y la utilización de formatos de registro que controlen la Seguridad de los equipos y activos fuera de las instalaciones?		0 %
	X	**A.11.2.7 R**	**Reutilización o retirada segura de dispositivos de almacenamiento.**	¿Existen las políticas, procedimientos y la utilización de formatos de registro que controlen reutilización o retirada segura de dispositivos de almacenamiento?		0 %
	X	**A.11.2.8**	**Equipo informático de usuario desatendido.**	¿Tiene la organización una política en torno a cómo el equipo sin supervisión deben ser protegido? ¿Se aplican controles técnicos en el lugar para asegurar el equipo desatendido?		0 %
	X	**A.11.2.9**	**Política de puesto de trabajo despejado y bloqueo de pantalla.**	¿Los usuarios cumplen con la Política de puesto de trabajo despejado y bloqueo de pantalla?		0 %
		A12.	**SEGURIDAD EN LA OPERATIVA.**			
		A.12.1	**Responsabilidades y procedimientos de operación.**			
	X	**A.12.1.1**	**Documentación de procedimientos de operación.**	¿El sistema de gestión de seguridad cuenta con la documentación de cada una de las políticas, controles y planes de contingencia pertinentes para el manejo de incidencias?		0 %
	X	**A.12.1.2**	**Gestión de cambios.**	¿Está documentada de formas organizadas y pertinentes las acciones necesarias para la gestión de cambios?		0 %
	X	**A.12.1.3**	**Gestión de capacidades.**	¿S establece controles sobre los conocimientos que deben tener las personas que gestionan los sistemas de información?		0 %
	X	**A.12.1.4**	**Separación de entornos de desarrollo, prueba y producción.**	¿Se cuentan con áreas específicas con los entornos adecuados para el desarrollo de las políticas de seguridad implantadas?		0 %
		A.12.2	**Protección contra código malicioso.**			

ISO/IEC 27002:2013 SANOHA LTDA						
REFERENCIA			EVALUACION DE CUMPLIMIENTO POR AREA		RESULTADOS	
CHECKLIST		ESTANDAR	SECCION	PUNTOS DE EVALUCION INCIAL	RECOMENDACIONES	PORCENTAJE DE CUMPLIMIENTO
SI	NO					
X		**A.12.2.1**	**Controles contra el código malicioso.**	¿Se cuenta con firewall y software especializado para filtran posibles códigos maliciosos y acciones de riesgo?		30%
		A.12.3	**Copias de seguridad.**			
X		**A.12.3.1**	**Copias de seguridad de la información.**	¿Se programa tiempos y formas para la ejecución de copias de seguridad de la información?		40%
		A.12.4	**Registro de actividad y supervisión.**			
	X	**A.12.4.1**	**Registro y gestión de eventos de actividad.**	¿Se cuenta con el registro puntual y detallado de cada actividad y se supervisa la gestión de eventos de seguridad?		0 %
X		**A.12.4.2**	**Protección de los registros de información.**	¿Se protege los registros de información en instalación es adecuadas contra la manipulación y acceso no autorizado?		30%
X		**A.12.4.3**	**Registros de actividad del administrador y operador del sistema.**	¿Los registros de administrador y operador son mantenidos, protegidos y revisados con regularidad?		30%
X		**A.12.4.4**	**Sincronización de relojes.**	¿Existe controles para monitorear y sincronizar exactamente los relojes para los Backup de información?		60%
		A.12.5	**Control del software en explotación.**			
	X	**A.12.5.1**	**Instalación del software en sistemas en producción.**	¿Hay políticas que controlen y documenten Instalación del software en sistemas en producción?		0 %
		A.12.6	**Gestión de la vulnerabilidad técnica.**			
X		**A.12.6.1**	**Gestión de las vulnerabilidades técnicas.**	¿Hay apoyo y soporte informático pertinente para gestionar las vulnerabilidades técnicas que se presenten en los sistemas informáticos?		55%
	X	**A.12.6.2**	**Restricciones en la instalación de software.**	¿La gestión de seguridad es clara con las políticas de restricción para que los usuarios instalen software no autorizado?		0 %
		A.12.7	**Consideraciones de las auditorías de los sistemas de información.**			
	X	**A.12.7.1**	**Controles de auditoría de los sistemas de información.**	¿Las políticas de seguridad efectúan controles de auditoría de los sistemas de información?		0 %
		A.13.	**SEGURIDAD EN LAS TELECOMUNICACIONES.**			
		A. 13.1	**Gestión de la seguridad en las redes.**			
X		**A.13.1.1**	**Controles de red.**	¿Existe un proceso de gestión en la red?		50%
X		**A.13.1.2**	**Mecanismos de seguridad asociados a servicios en red.**	¿Hay mecanismos se seguridad pertinentes para gestión de los servicios de red?		30%
	X	**A.13.1.3**	**Segregación de redes.**	¿Existe una segregación en la red del sistema?		0 %

ISO/IEC 27002:2013 SANOHA LTDA						
REFERENCIA			EVALUACION DE CUMPLIMIENTO POR AREA		RESULTADOS	
CHECKLIST		ESTANDAR	SECCION	PUNTOS DE EVALUCION INCIAL	RECOMENDACIONES	PORCENTAJE DE CUMPLIMIENTO
SI	NO					
		A.13.2	**Intercambio de información con partes externas.**			
	X	**A.13.2.1**	**Políticas y procedimientos de intercambio de información.**	¿La organización tiene definidos y cumple Políticas y con los procedimientos de intercambio de información?		0 %
	X	**A.13.2.2**	**Acuerdos de intercambio.**	¿Hay establecidos procedimientos para contratación de acuerdos de intercambio con otras entidades?		0 %
	X	**A.13.2.3**	**Mensajería electrónica.**	¿Los controles son efectivos en cuanto a la gestión de mensajería electrónica que aseguran la confidencialidad de transacciones y gestión de mensajes?		0 %
	X	**A.13.2.4**	**Acuerdos**	¿Previamente hay compromisos de confidencialidad de empleados y personal en general dentro las políticas de seguridad de la empresa?		0 %
		A.14.	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**			
		A.14.1	**Requisitos de seguridad de los sistemas de información.**			
	X	**A.14.1.1**	**Análisis y especificación de los requisitos de seguridad.**	¿Están documentados los procesos de Análisis y especificación de los requisitos de seguridad?		0 %
	X	**A.14.1.2**	**Seguridad de las comunicaciones en servicios accesibles por redes públicas.**	¿Existen controles que gestionen los recursos y la seguridad de las comunicaciones en servicios accesibles por redes públicas?		0 %
	X	**A.14.1.3**	**Protección de las transacciones por redes telemáticas.**	¿Existen los mecanismos suficientes apoyados en software y hardware para la Protección de las transacciones por redes telemáticas?		0 %
		A.14.2	**Seguridad en los procesos de desarrollo y soporte.**			
	X	**A.14.2.1**	**Política de desarrollo seguro de software.**	¿Existen y se estipulan las condiciones para desarrollo seguro de software?		0 %
	X	**A.14.2.2**	**Procedimientos de control de cambios en los sistemas.**	¿Existen los Procedimientos de control de cambios en los sistemas informáticos de la empresa?		0 %
	X	**A.14.2.3**	**Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.**	¿Se realiza un seguimiento efectivo sobre las aplicaciones tras efectuar cambios en el sistema operativo?		0 %
	X	**A.14.2.4**	**Restricciones a los cambios en los paquetes de software.**	¿Existen políticas que permitan efectuar Restricciones a los cambios en los paquetes de software?		0 %

ISO/IEC 27002:2013 SANOHA LTDA						
REFERENCIA			EVALUACION DE CUMPLIMIENTO POR AREA		RESULTADOS	
CHECKLIST		ESTANDAR	SECCION	PUNTOS DE EVALUCION INCIAL	RECOMENDACIONES	PORCENTAJE DE CUMPLIMIENTO
SI	NO					
	X	**A.14.2.5**	**Uso de principios de ingeniería en protección de sistemas.**	¿el diseño de seguridad de la organización, está debidamente documentado con los principios y elementos que garantizan procedimientos y técnicas para la seguridad ?		0 %
	X	**A.14.2.6**	**Seguridad en entornos de desarrollo.**	¿Se proporciona una gestión de los sistemas informáticos proactiva para que los entornos de desarrollo sean seguros y confiables?		0 %
	X	**A.14.2.7**	**Externalización del desarrollo de software.**	¿Se brindan las políticas necesarias para lograr Externalización del desarrollo de software segura?		0 %
	X	**A.14.2.8**	**Pruebas de funcionalidad durante el desarrollo de los sistemas.**	¿Existen los procedimientos adecuados para la realización Pruebas de funcionalidad durante el desarrollo de los sistemas?		0 %
	X	**A.14.2.9**	**Pruebas de aceptación.**	¿Las políticas y controles determinan los procesos adecuados para la realización de Pruebas de aceptación?		0 %
		A.14.3	**Datos de prueba.**			
	X	**A.14.3.1**	**Protección de los datos utilizados en pruebas.**	¿Existen protocolos de seguridad documentados y que permiten conocer los pasos a seguir para la protección de los datos utilizados en pruebas?		0 %
		A.15.	**RELACIONES CON SUMINISTRADORES.**			
		A.15.1	**Seguridad de la información en las relaciones con suministradores.**			
	X	**A.15.1.1**	**Política de seguridad de la información para suministradores.**	¿Están establecidos y documentados los procedimientos para Política de seguridad de la información para suministradores?		0 %
	X	**A.15.1.2**	**Tratamiento del riesgo dentro de acuerdos de suministradores.**	¿Se registran y monitorean el Tratamiento de riesgos dentro de acuerdos de suministradores?		0 %
	X	**A.15.1.3**	**Cadena de suministro en tecnologías de la información y comunicaciones.**	¿Se conoce y esta documentados los procesos a realizar en una Cadena de suministro en tecnologías de la información y comunicaciones?		0 %
		A.15.2	**Gestión de la prestación del servicio por suministradores.**			
X		**A.15.2.1**	**Supervisión y revisión de los servicios prestados por terceros.**	¿Hay una actualización y Supervisión y revisión de los servicios prestados por terceros?		40%
X		**A.15.2.2**	**Gestión de cambios en los servicios prestados por terceros.**	¿Se registran las diferentes novedades en cuanto a la Gestión de cambios en los servicios prestados por terceros?		40%
		A.16.	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**			

ISO/IEC 27002:2013 SANOHA LTDA						
REFERENCIA			EVALUACION DE CUMPLIMIENTO POR AREA		RESULTADOS	
CHECKLIST		ESTANDAR	SECCION	PUNTOS DE EVALUCION INCIAL	RECOMENDACIONES	PORCENTAJE DE CUMPLIMIENTO
SI	NO					
		A.16.1	**Gestión de incidentes de seguridad de la información y mejoras.**			
	X	**A.16.1.1**	**Responsabilidades y procedimientos.**	¿Están definidos y es de conocimiento del todo el recurso humano las Responsabilidades y procedimientos?		0 %
	X	**A.16.1.2**	**Notificación de los eventos de seguridad de la información.**	¿Hay una adecuada comunicación sobre los eventos de seguridad de la información?		0 %
	X	**A.16.1.3**	**Notificación de puntos débiles de la seguridad.**	¿Dentro de los procedimientos de seguridad se registran y documentan de puntos débiles de la seguridad de la organización?		0 %
X		**A.16.1.4**	**Valoración de eventos de seguridad de la información y toma de decisiones.**	¿El equipo informático y los directivos encargados de la gestión de la seguridad realizan una Valoración de eventos de seguridad de la información y toma de decisiones?		10 %
	X	**A.16.1.5**	**Respuesta a los incidentes de seguridad.**	¿Hay una efectiva Respuesta a los incidentes de seguridad?		0 %
	X	**A.16.1.6**	**Aprendizaje de los incidentes de seguridad de la información.**	¿Los procedimientos de seguridad están diseñados para que haya un Aprendizaje de los incidentes de seguridad de la información para la retroalimentación y mejora de las políticas de seguridad?		0 %
	X	**A.16.1.7**	**Recopilación de evidencias.**	¿Se recopilan las evidencias de cada incidente siguiendo los procedimientos definidos en las políticas de seguridad?		0 %
		A.17.	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DELA CONTINUIDAD DEL NEGOCIO.**			
		A.17.1	**Continuidad de la seguridad de la información.**			
	X	**A.17.1.1**	**Planificación de la continuidad de la seguridad de la información.**	¿Existen planes de contingencia que permitan acciones inmediatas que no impacten profundamente la continuidad de la seguridad de la información?		0 %
	X	**A.17.1.2**	**Implantación de la continuidad de la seguridad de la información.**	¿Hay una efectiva auditoria sobre los procesos encargados Implantación de la continuidad de la seguridad de la información?		0 %
	X	**A.17.1.3**	**Verificación, revisión y evaluación de la continuidad de la seguridad de la información.**	¿Hay una efectiva auditoria sobre los procesos encargados Verificación, revisión y evaluación de la continuidad de la seguridad de la información?		0 %
		A.17.2	**Redundancias.**			
X		**A.17.2.1**	**Disponibilidad de instalaciones para el procesamiento de la información.**	¿Existe la infraestructura suficiente para que haya Disponibilidad de instalaciones para el procesamiento de la información?		30%

ISO/IEC 27002:2013 SANOHA LTDA						
REFERENCIA			EVALUACION DE CUMPLIMIENTO POR AREA		RESULTADOS	
CHECKLIST		ESTANDAR	SECCION	PUNTOS DE EVALUCION INCIAL	RECOMENDACIONES	PORCENTAJE DE CUMPLIMIENTO
SI	NO					
		A.18.	**CUMPLIMIENTO.**			
		A.18.1	**Cumplimiento de los requisitos legales y contractuales.**			
	X	**A.18.1.1**	**Identificación de la legislación aplicable.**	¿ cuenta con políticas diseñadas en base a una legislación aplicable?.		0 %
	X	**A.18.1.2**	**Derechos de propiedad intelectual (DPI).**	¿Las políticas están diseñadas para respetar los derechos de propiedad intelectual en cuanto al uso de información y desarrollo de software?		0 %
	X	**A.18.1.3**	**Protección de los registros de la organización.**	¿Se tiene documentado los procedimientos a seguir para asegurar Protección de los registros de la organización?		0 %
	X	**A.18.1.4**	**Protección de datos y privacidad de la información personal.**	¿Existen cláusulas de seguridad que permiten Protección de datos y privacidad de la información personal?		0 %
	X	**A.18.1.5**	**Regulación de los controles criptográficos.**	¿Se supervisan los controles criptográficos efectuados en los procesos de comunicación y transporte de información en la red e internet?		0 %
		A.18.2	**Revisiones de la seguridad de la información.**			
	X	**A.18.2.1**	**Revisión independiente de la seguridad de la información.**	¿Se programa diferentes revisiones o auditorías internas para la verificación de las políticas y controles de seguridad?		0 %
	X	**A.18.2.2**	**Cumplimiento de las políticas y normas de seguridad.**	¿Se cumplen las políticas de seguridad y normas de forma efectiva?		0 %
	X	**A.18.2.3**	**Comprobación del cumplimiento.**	¿Los grupos de trabajo encargados dela gestión de la seguridad informática supervisan el cumplimento de las mismas?		0 %

ANEXO E: Carta de entrega de diseño SGSI

SANOHA LTDA
Minería - Medio Ambiente y Forestal
NIT 800.188.412-0 REGIMEN COMÚN

Sogamoso 30 de junio de 2015

Ingeniera
MÓNICA ISABEL HERNÁNDEZ BÁEZ
Jefe de la división de sistemas
SANOHA LTDA

Apreciada ingeniera

Por medio de la presente se hace entrega de los resultados del diseño del Sistema de Gestión de Seguridad de Información correspondiente al Área de automatización del proceso de báscula, que fue elaborado con el fin proporcionar un conjunto de actividades de gestión que deben realizarse mediante procesos sistemáticos enfocados en el proceso de automatización de báscula, proceso que influye en la continuidad negocio y del funcionamiento de los demás procesos dentro de la empresa. Su objetivo no está orientado a garantizar la seguridad sino a generar políticas y controles para que los riesgos de la seguridad de la información para que sean conocidos, asumidos, gestionados y minimizados por la empresa Sanoha Ltda, de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la misma, los riesgos, el entorno y las tecnologías.

La estructura del Diseño se desarrolla en primer lugar el capítulo 5 con un marco de referencia que describe teóricamente un SGSI, la normatividad que especifica los estándares de implementación del mismo, hace un paralelo entre la norma ISO/IEC 27001:2005 y la ISO/IEC 27001:2013 y los conceptos necesarios para comprender el contexto del proyecto. El capítulo 6 y 7 se explican los mecanismos de recolección de información y la metodología empleada y sus ventajas. El capítulo 8 abarca análisis y recopilación exhaustiva de los procesos del área de automatización de báscula, haciendo una breve reseña de la empresa, el sistema organizativo enfatizando en la división de sistemas y el departamento de Acopio y Abastecimiento, este último responsable del manejo del área de automatización del proceso de báscula que está basado en la utilización del software a medida denominado SIRMAB(Base de datos que registra todos los proceso efectuados en bascula y es compartido en la red según perfiles de usuario). También se describen los procesos que intervienen en esta área y su funcionamiento. Además de mencionar el sistema informático actual de Sanoha Ltda. El capítulo 9 se identifica y valora las vulnerabilidades y amenazas de acuerdo a los activos identificados. El capítulo 10 se evalúa los riesgos. El capítulo 11 se genera un modelo

Nobsa. Km. 4 Vía Sogamoso-Belencito Teléfonos: (8)7729032 – 7726764 -7729033 Telefax: 7723673

SANOHA LTDA
Minería - Medio Ambiente y Forestal
NIT 800.188.412-0 REGIMEN COMÚN

de gestión según la norma y por último en el capítulo 12 se recomienda un plan de acción según los riesgos más relevantes y que tienen un mayor nivel de prioridad.

Todo el diseño genera estrategias informáticas y de gestión que dan la oportunidad de mejorar y percibir los procesos que están en un nivel mayor de riesgo, proporcionando controles basados en la norma ISO/IEC 27001:2013, lo que facilitaría en un futuro implementar un SGSI y solicitar una certificación lo que diferenciaría a Sanoha Ltda con respecto a otras empresas del sector productivo.

El informe con todos los resultados se adjunta junto con el presente documento.

Cordialmente,

ING. YENNY STELLA NUÑEZ
Responsable del diseño SGSI

Nobsa. Km. 4 Vía Sogamoso-Belencito Teléfonos: (8)7729032 – 7726764 -7729033 Telefax: 7723673