UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
Documento: FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	Código: F-AC-DBL-007	Fecha: 10-04-2012	Revisión: A
Dependencia: DIVISIÓN DE BIBLIOTECA	Aprobado: SUBDIRECTOR ACADEMICO		Pág.: 1(1)

RESUMEN – TRABAJO DE GRADO

AUTORES	YAIRA MARCELA ESCOBAR VÉLEZ WILDER ANDRÉS DUARTE NEIRA FABIÁN ALEXIS VERGEL CONTRERAS
FACULTAD	DE INGENIERIAS
PLAN DE ESTUDIOS	ESPECIALIZACION EN AUDITORIA DE SISTEMAS
DIRECTOR	MSG. ANDRÉS MAURICIO PUENTES
TÍTULO DE LA TESIS	EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SISTEMAS DE LA EMPRESA GRUPO NAGALTEC S.A.S. SEGÚN LA ISO 27001

RESUMEN

(70 palabras aproximadamente)

EL ASEGURAMIENTO Y LA PROTECCIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LAS ORGANIZACIONES Y DE LOS DATOS DE CARÁCTER PERSONAL DE LOS USUARIOS, REPRESENTAN UN RETO AL MOMENTO DE PRETENDER GARANTIZAR SU CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y PRIVACIDAD, RAZÓN POR LA CUAL, LA SEGURIDAD DE LA INFORMACIÓN SE HA CONVERTIDO EN UNO DE LOS ASPECTOS DE MAYOR PREOCUPACIÓN A NIVEL MUNDIAL.

CARACTERÍSTICAS

PÁGINAS: 84	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SISTEMAS DE LA EMPRESA GRUPO NAGALTEC S.A.S. SEGÚN LA ISO 27001

AUTORES:

YAIRA MARCELA ESCOBAR VÉLEZ

WILDER ANDRÉS DUARTE NEIRA

FABIÁN ALEXIS VERGEL CONTRERAS

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

Ocaña, Colombia **Julio de 2017**

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Ocaña, 26 de Julio de 2017

DEDICATORIA

Los autores de este proyecto exponemos la siguiente dedicatoria:

A Dios, por iluminar nuestras vidas y permitirnos adquirir los conocimientos necesarios para ayudar a construir una sociedad mejor.

A nuestras familias, por su apoyo incondicional que hicieron posible el sueño de ser Ingenieros de sistemas.

Al grupo NAGALTEC S.A.S, por permitir desarrollar esta investigación en sus instalaciones y aplicar el resultado de la misma como una acción de mejora para los procesos de seguridad de su organización.

AGRADECIMIENTOS

Los autores de este proyecto exponen los siguientes agradecimientos:

A la Universidad Francisco de Paula Santander, alma mater y escenario de debate, academia, calidad y amor por formar grandes profesionales.

A los profesores de la facultad de Ingenierías, por sus aportes, paciencia y compromiso en Enseñar el infinito mundo de la tecnología e informática.

Al Director de tesis, por su apoyo permanente, su recomendación acertada y la orientación rigurosa y especializada que permitieron la construcción teórica y metodológica del proyecto de grado.

INDICE

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCION

Hoy en día, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, la cual, sólo tiene sentido cuando está disponible y es utilizada de forma adecuada, integra, oportuna, responsable y segura, lo que implica, que es necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio. Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones.

Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, contantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada.

En la medida que las organizaciones tenga una visión general de los riesgos que pueden afectar la seguridad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la integridad, disponibilidad y confidencialidad tanto de la información del negocio como los datos de carácter personal de sus empleados y usuarios.

El presente trabajo de grado busca realizar una Evaluación al Sistema de Seguridad de la Información para un grupo empresarial de soluciones tecnológicas, teniendo en cuenta para esto el marco de referencia de la norma ISO 27001:2013 que proporciona un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de Gestión de Seguridad de la Información en cualquier tipo de organización, lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo.

CAPITULO 1.

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SISTEMAS DE LA EMPRESA GRUPO NAGALTEC S.A.S. SEGÚN LA ISO 27001

1.1. Descripción General

Nagaltec S.A. es una empresa del medio de desarrollo tecnológico que crea soluciones confiables y seguras conforme a las necesidades de los clientes, su portafolio de servicios está orientado a la creación de páginas web, plantillas web, Dominios, Alojamiento de Información, sistemas de Información, y APPs.

El grupo Nagaltec es una sociedad por acciones simplificada vigilada por la superintendencia de sociedades y su objeto son las actividades de consultoría informática y actividades de administración de instalaciones informáticas.

La empresa cuenta con la infraestructura tecnológica adecuada y tiene implementado una serie de mecanismos de seguridad, tanto físicos como lógicos, con el propósito de proteger la confidencialidad, integridad y disponibilidad de la información del negocio y la privacidad de los datos de los clientes que residen en sus bases de datos.

A pesar de contar con estos recursos tecnológicos y tener implementadas medidas de seguridad, la empresa no cuenta con los mecanismos adecuados y expeditos que le permitan conocer el estado real de su seguridad en cuanto a personas, procesos y tecnología ni el nivel de efectividad de las medidas de seguridad que tiene implementadas, lo que dificulta o impide

identificar y por ende gestionar de manera efectiva los riesgos asociados a la seguridad de sus activos de información y las amenazas que puedan llegar a comprometer la integridad, disponibilidad y confidencialidad de su información.

1.1.1. Estado de la seguridad de la Información en NAGALTEC S.A.

La Gerencia de Nagaltec, con el fin de evaluar el estado de la seguridad de la Infraestructura tecnológica y con ello, poder identificar su nivel de exposición ante posibles ataques externos, realizo un análisis a fin de identificar su nivel de vulnerabilidad, encontrando que a la fecha no se han realizado pruebas que permitan medir el nivel de exposición de la plataforma tecnológica de la empresa ante ataques informáticos. Por lo que identifica la necesidad de realizar una auditoría a fin de identificar las necesidades de seguridad y control para la empresa con el objetivo que la misma cuente con un modelo de seguridad de la información.

1.2. Planteamiento del problema

Para Beekman (1996) la seguridad es un tema muy importante para cualquier empresa, este o no conectada a una red pública. No solamente es importante, sino que también puede llegar a ser compleja. Los niveles de seguridad que se pueden implementar son muchos y dependerá del usuario hasta donde quiera llegar; La seguridad informática y de datos dista mucho de simplemente tener un Firewall. Se aborda un proceso de seguridad recomendado.

En este sentido debido a los múltiples riesgos y amenazas que se generan por el cambio constante y dinámico que enmarca la evolución de la tecnología de la información, es necesario que las organizaciones cuenten con una estrategia de seguridad basado en los riesgos y a su vez

alineada con las necesidades del negocio, con el objetivo de contar con un modelo de seguridad de la información que apoye y apalanque los objetivos estratégicos de la organización.

Tomando como referencia la situación actual de la empresa se requiere realizar una Evaluación al sistema de seguridad de la información con el objetivo de fortalecer integralmente los pilares fundamentales de la seguridad correspondiente a la integridad, confidencialidad y disponibilidad de la información y garantizar con eso la debida protección de la información del negocio y la privacidad de la información de sus partes interesadas.

De acuerdo a lo anterior, se puede establecer que el problema está relacionado con un ineficiente modelo de seguridad de la información, lo que significa que es necesario Evaluar el sistema de gestión de seguridad de la información para la empresa basado en un estándar de seguridad reconocido a nivel mundial con el propósito de garantizar su debida permanencia y evolución en el tiempo.

1.3. Formulación del problema

¿Una Evaluación al sistema de seguridad de la información le proveerá a Nagaltec S.A. los elementos, mecanismos y lineamientos adecuados para mejorar la seguridad de la información de la empresa y tratamiento de los riesgos asociados al uso de la información?

1.4. OBJETIVOS

1.4.1. Objetivo General.

Evaluar el sistema de seguridad de la información de la empresa Nagaltec S.A., tomando como referencia la norma NTC-ISO-IEC 27001:2013.

1.4.2. Objetivos Específicos.

Analizar la situación actual de la empresa, con relación a la gestión de seguridad de la información.

Establecer las necesidades y requerimientos con relación al sistema de seguridad de la Información.

Definir la política, control y mecanismo de seguridad frente a los riegos encontrados en el sistema de seguridad de la información de la empresa.

1.5. Justificación

La evaluación al sistema de seguridad de la información basado en un modelo de buenas prácticas de seguridad conocido a nivel mundial como es la norma ISO/IEC 27001:2013, proveerá las condiciones de oportunidad y viabilidad necesarias para que la seguridad de la información apoye y extienda los objetivos estratégicos del negocio, mediante la protección y aseguramiento de su información que es fundamental para garantizar la debida gestión operativa de la empresa y con ello asegurar el cumplimiento de su Misión.

Al evaluar el sistema de seguridad de la información, demuestra el compromiso de la empresa hacia la seguridad de la información y provee los elementos requeridos para gestionar de manera eficiente los riesgos que puedan atentar con la seguridad de su información, lo cual

genera confianza en sus clientes que es fundamental para el crecimiento y sostenibilidad del grupo empresarial.

1.6. Delimitación del problema de investigación

1.6.1. Geográfica.

El área de sistemas de la empresa Grupo Nagaltec S.A.S. es el lugar donde se llevará a cabo la realización de todo el análisis respecto a la seguridad de la información, los controles y políticas se desarrollan con el propósito de mantener los servidores, equipos de cómputo y demás aparatos tecnológicos de manera segura con el fin de preservar la información.

1.6.2. Temporal.

El tiempo estimado para la realización de esta auditoría está comprendido por 8 semanas, es decir 2 meses de ejecución para lograr todas las actividades planteadas. Inicia el 5 de Enero y finaliza el 5 de Abril.

1.6.3. Conceptual.

Para el desarrollo del presente proyecto es necesario tener en cuenta el concepto de los siguientes términos: Seguridad de la información, Gestión de seguridad de la información, sistema de gestión de seguridad de la información, y glosario de términos inherentes a la norma objeto de estudio.

1.6.4. Operativa.

El desarrollo del trabajo se realizará con base en los parámetros establecidos; sin embargo se podrán presentar inconvenientes en la obtención de cierta información necesaria por lo que se buscará la asesoría del director del proyecto para dar respuestas a los interrogantes presentados.

CAPITULO 2. MARCO REFERENCIAL

2.1. ANTECEDENTES

2.1.1 Implementación de un Sistema de Gestión de Seguridad de la Información basada en la norma ISO 27001. Para la Intranet de la Corporación Metropolitana de Salud. Flor María Álvarez Zurita y Pamela Anabel García Guzmán. Quito, Ecuador.2007.

El objetivo principal de este proyecto de investigación es la implementación de un Sistema de Gestión de Seguridad de la Información para la Intranet de la Corporación Metropolitana de Salud con base a la Norma ISO 27001 con el fin de lograr una gestión de la red de manera organizada, adecuada y garantizando que los riesgos de seguridad de la red sean minimizados a través de los procedimientos para el tratamiento de los mismos.

2.1.2 Centro de investigaciones económicas, administrativas y sociales. Gestión de la Seguridad de la Información en la Empresa. Oscar Raúl Ortega Pacheco. México, D.F. 2010.

El presente documento presenta una serie de acciones aplicadas a un modelo de gestión de la seguridad de la información que permite alinear los objetivos de una empresa con las metas que se requieren para la protección de la información. Para lo cual se parte de la construcción de un modelo de gestión de la información que permite explicar el flujo completo que sufren los datos dentro de una empresa. Posteriormente se describen los diferentes modelos de gestión de riesgo informático donde se analizan sus principales ventajas y desventajas. Finalmente, partiendo de la base del modelo propuesto por Kiely y Benzel (2009) se establecen diferentes medidas que una empresa puede aplicar desde sus políticas, gobierno corporativo, elementos técnicos y de cultura para minimizar el riesgo informático. Así mismo se sugiere trabajar a futuro en la construcción de indicadores de seguridad, evaluar la validez del modelo

presentado ante nuevos retos tecnológicos y desarrollar estudios de trayectoria tecnológica en cuanto a delitos electrónicos como innovación en elementos de seguridad

2.2. MARCO CONCEPTUAL

2.2.1. Seguridad de la Información

La seguridad de la información de acuerdo a la norma ISO 27000:2014, SE define como la preservación de la confidencialidad, integridad y disponibilidad de la información.

De acuerdo a la Asociación Española para la calidad (2017) la Seguridad de la Información tiene como propósito la protección de la información y de los sistemas de la información contra las amenazas y eventos que atenten con el acceso, uso, divulgación, interrupción y destrucción de forma no autorizada.

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

La seguridad de la información en una organización, es un proceso de mejora continua que demanda la participación activa de toda la organización y busca preservar, entre otros, los siguientes principios de la información:

• La **confidencialidad,** asegurando que solo las personas debidamente autorizadas tengan acceso a la información.

• La **disponibilidad**, asegurando que la información esté totalmente disponible para las personas debidamente autorizadas cuando ellos la requieran.

La **integridad**, asegurando que la información no sea modificada sin la debida autorización.

La **autenticidad,** con el propósito de garantizar la identidad de la persona que genera la información. La autenticidad de la información, es la capacidad de asegurar que el emisor de la información es quien dice ser y no un tercero que esté intentando suplantarlo.

El **no repudio,** con el propósito de conocer exactamente quienes son los actores que participan en una transacción o una comunicación y no puedan negarlo en ningún momento. El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje.

La **trazabilidad,** con el objetivo de poder monitorear o rastrear cualquier operación que se realiza sobre la información desde su mismo origen.

La seguridad de la información dentro de las organizaciones, depende del nivel de protección y seguridad de sus activos de información, por lo tanto es fundamental la implementación de medidas y controles de seguridad adecuados, y el permanente monitoreo, revisión y mejora de los mismos de manera proactiva con el objetivo de garantizar su efectividad. (ISO ISO/IEC 27000:2014, Pág. 4)

2.2.2. Gestión de Seguridad de la Información.

Muchas organizaciones tienen dentro de sus objetivos mejorar de manera continua sus procesos, para esto gestionan y miden cada parámetro, lo que les permite poder determinar

cuándo una variación puede afectar la producción o los servicios que brindan. Esto mismo se debe hacer con la seguridad de la información.

Uno de los parámetros fundamentales a medir y analizar en la seguridad de la información son los incidentes, es decir, los eventos no deseados que se detectan en la red o en los servicios y que pueden poner en riesgo la disponibilidad, la confidencialidad o la integridad de la información. Cada evento debe ser registrado y calificado para así poder determinar cómo reaccionar ante cada incidente. (Espitia 2015. Art. Digital)

Los incidentes de seguridad siempre van a existir sin importar los controles que implementen las organizaciones. Sin embargo poder tener claro cuáles son los incidentes más comunes en la empresa, permite orientar las inversiones en seguridad hacia las brechas que mayor impacto pueden generar en caso que un incidente se materialice.

Todos los sistemas de gestión de seguridad de la información que empresarialmente se usan, priorizan la gestión de incidentes, con el objeto de poder detectarlo en el menor tiempo posible y así poder actuar según la criticidad del mismo en su mitigación y control. (Espitia 2015. Art. Digital)

2.2.3. Sistema de gestión de Seguridad de la Información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, 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 tecnologías. (SGSI 2013, pag.2).

2.2.4. Glosario de Términos

Las definiciones del presente glosario son tomadas de: NTC-ISO-IEC 27001:2013, Pág. 11-12

Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

Amenaza: Es la causa potencial de un daño a un activo de información.

Anexo SL: Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

Causa: Razón por la cual el riesgo sucede.

Ciclo de Deming: Modelo mejora continua para la implementación de un sistema de mejora continua.

Colaborador: Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.

Confidencialidad: Propiedad que determina que la información no esté disponible a personas no autorizados

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Disponibilidad: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.

Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

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

Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.

Responsables del Activo: Personas responsables del activo de información.

Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

SARO: Siglas del Sistema de Administración de Riesgos Operativos.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

2.3. MARCO TEÓRICO

2.3.1. Normas ISO/IEC 27000

La familia de las normas ISO/IEC 27000, son un marco de referencia de seguridad a nivel mundial desarrollado por la International Organization for Standardization -ISO e International Electrotechnical Commission – IEC, que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización.

Estas normas especifican los requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

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

Las siguientes son algunas de las normas que componen la familia ISO/IEC 27000, las cuales serán el marco teórico que se tendrá en cuenta para efectos del presente trabajo:

ISO/IEC 27000. Esta norma proporciona una visión general de los sistemas de gestión de seguridad de la información y contiene los términos y definiciones que se utilizan en las diferentes normas de la 27000.

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

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

Los dominios de la norma ISO/IEC 27001:2013 corresponde a los diferentes capítulos que establecen los requerimientos que las organizaciones deben cumplir para el establecimiento de un Sistema de Gestión de Seguridad de la Información, los cuales se resumen a continuación:

Tabla 1. Dominios de la norma ISO/IEC 27001:2013

0. INTRODUCCION
1. OBJETO Y CAMPO DE APLICACION
2. REFERENCIAS NORMATIVAS
3. TERMINOS Y DEFINICIONES
4. CONTEXTO DE LA ORGANIZACION
5. LIDERAZGO
6. PLANIFICACION
7. SOPORTE
8. OPERACION
9. EVALUACION DE DESEMPEÑO
10. MEJORA

Fuente: Adaptación autores del proyecto con base NTC-ISO-IEC 27001:2013

El Anexo A de la norma ISO 27001, contiene los diferentes objetivos de control y controles que las organizaciones deberían tener en cuenta para la planeación e implementación de su Sistema de Gestión de Seguridad de la Información, los cuales se describen con más detalle en la norma ISO 27002.

ISO/IEC 27002. Guía de buenas prácticas en seguridad de la información que describe de forma detallada las acciones que se deben tener en cuenta para el establecimiento e implementación de los objetivos de control y controles descritos de una forma general en el Anexo A de la norma ISO 27001.

ISO/IEC 27003. Guía que contiene aspectos necesarios para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información de acuerdo a los requerimientos establecidos en la norma ISO/IEC 27001, donde se describe el proceso desde la planeación hasta la puesta en marcha de planes de implementación.

ISO/IEC 27004. Guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un Sistema de Gestión de Seguridad de la Información y de los objetivos de control y controles implementados de acuerdo al Anexo A de la norma ISO 27001

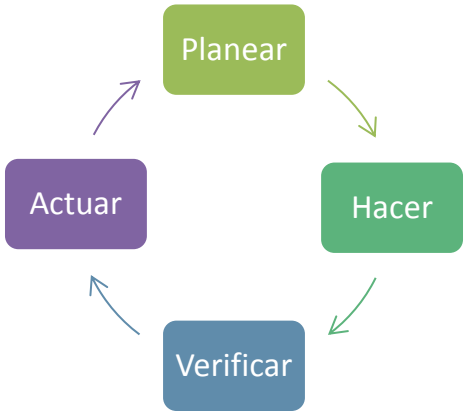
ISO/IEC 27005. Esta norma establece los lineamientos para la gestión de riesgos de seguridad de la información y está diseñada para ayudar a las organizaciones en la implementación de un Sistema de Gestión de Seguridad de la Información basada es un enfoque de gestión de riesgos. Entre otros aspectos, establecer lo requerimiento que se deben tener en cuenta para el proceso de valoración de riesgos, relacionados con la identificación, análisis, evaluación y tratamiento de los riesgos en la seguridad de la información.

ISO/IEC 27006. Establece los requisitos relacionados en la norma ISO 27001 que deben cumplir las organizaciones para la acreditación de entidades de auditoría y certificación de Sistemas de Gestión de Seguridad de la Información.

ISO/IEC 27035. Proporciona una guía sobre la gestión de incidentes de seguridad en la información

2.3.2. Ciclo de mejora continua vs norma ISO/IEC 270012013

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



Fuente: Adaptación Autores de proyecto

Figura 1. Ciclo de mejora continúa

Fase Planificar: En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

Pase Hacer: En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

Fase Verificar: Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

Fase Actuar: Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

En la versión 2013 de la norma ISO/IEC 27001, no aparece la sección de "Enfoque basado en procesos" que existía en la versión 2005, lo cual brinda una mayor flexibilidad en el momento de seleccionar o definir un modelo para la mejora continua del Sistema de Gestión de Seguridad de la Información. Aunque en la versión 2013, no se determina el modelo PHVA como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:

Fuente: Elaborada por los autores del proyecto con base en la información de la norma 27000:2013

Figura 2. Ciclo de mejora continua alineado a la norma ISO 27001:2013

El siguiente cuadro muestra la relación entre las fases del ciclo de mejora continua 'PHVA' (planear, hacer, verificar y actuar) y la estructura de capítulos y numerales de la norma ISO 27001:2013.

Tabla 2. Fases PHVA VS Estructura ISO 27001: 2013

Fase PHVA	Capitulo ISO 27001:2013
PLANEAR	4. Contexto de la organización 5. Liderazgo 6. Planificación 7. Soporte
HACER	8. Operación
VERIFICAR	9. Evaluación de desempeño
ACTUAR	10. Mejora

Fuente: Autores del Proyecto

Fase PLANEAR en la norma ISO 27001:2013

En el **capítulo 4 - Contexto de la organización** de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestiones externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del SGSI. (NTC-ISO-IEC 27001:2013, Pág. 1-2)

En el **capítulo 5 – Liderazgo**, se establece las responsabilidades y compromisos de la Alta dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización, aseguren la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen. (NTC-ISO-IEC 27001:2013, Pág. 3)

En el **capítulo 6 – Planeación**, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento. (NTC-ISO-IEC 27001:2013, Pág. 4)

En el **capítulo 7 – Soporte** se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua Sistema de Gestión de Seguridad de la Información. (NTC-ISO-IEC 27001:2013, Pág. 5)

Fase HACER en la norma ISO 27001:2013. En el **capítulo 8 – Operación** de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información. (NTC-ISO-IEC 27001:2013, Pág. 6)

Fase VERIFICAR en la norma ISO 27001:2013. En el **capítulo 9 - Evaluación del desempeño,** se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información. (NTC-ISO-IEC 27001:2013, Pág. 8)

Fase ACTUAR en la norma ISO 27001:2013. En el **capítulo 10 – Mejora ,** se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan. (NTC-ISO-IEC 27001:2013, Pág. 9)

2.4. MARCO LEGAL

2.4.1 Constitución Política de 1991. En los artículos 209 y 269 se fundamenta el sistema de control interno en el Estado Colombiano, el primero establece: "La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley" y en el 269, se soporta el diseño del sistema: "En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas".

2.4.2 Leyes en Colombia relacionadas con Información

Ley estatutaria 1266 del 31 de diciembre de 2008. Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 del 5 de enero de 2009. Delitos informáticos. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 de 2009. Se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro.

Ley Estatutaria 1581 de 2012. Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Ley 603 de 2000. Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

Ley 72 del 20 de diciembre de 1989. El Gobierno Nacional, por medio del Ministerio de Comunicaciones, adoptará la política general del sector de comunicaciones y ejercerá las funciones de planeación, regulación y control de todos los servicios de dicho sector, que comprende, entre otros:

Los servicios de telecomunicaciones.

Los servicios informáticos y de telemática.

Los servicios especializados de telecomunicaciones o servicios de valor agregado.

Los servicios postales.

Ley 555 del 2 de febrero de 2000 en la ley no. 1341 del 30 de julio de 2009.

Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la

Agencia Nacional de Espectro y se dictan otras disposiciones.”, muestra el esfuerzo que ha tenido el gobierno colombiano por brindar un marco normativo para el desarrollo de tecnologías de la información y la comunicación.

Artículo 2o. Principios orientadores.

Las Tecnologías de la Información y las Comunicaciones deben servir al interés general y es deber del Estado promover su acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional.

Artículo 3o. Sociedad de la Información y del Conocimiento.

El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

Norma ISO/IEC 27001 Familia de estándares donde especifica claramente los parámetros sobre seguridad de la información, para desarrollar, implementar y mantener los sistemas de gestión de seguridad de la información, entre ellos:

Norma ISO/IEC 27001: Define los requisitos para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información).

Norma ISO/IEC 27002: (anterior ISO 17799). Es una guía de buenas prácticas, describe los controles a seguir dentro del marco de la seguridad de la información; enmarcados en 11 dominios, 39 objetivos de control y 133 controles.

Norma ISO/IEC 27003: Proporciona ayuda y orientación sobre la implementación de un SGSI, incluye el método PHVA (planear, hacer verificar y actuar) contribuyendo con revisiones y mejora continua.

Norma ISO/IEC 27004: Especificará las métricas y técnicas de medición para determinar la eficacia de un SGSI y de sus controles. Aplicable específicamente en la fase del hacer (Do); de acuerdo con el método PHVA.

Norma ISO/IEC 27005: Suministra directrices para la gestión del riesgo en la seguridad de la información.

Ley 1273 de 2009: sobre los delitos informáticos y la protección de la información y de datos en Colombia.

CAPITULO 3. DISEÑO METODOLOGICO

El diseño es el medio de aplicación donde después de formular la hipótesis y de definir los objetivos del estudio, el investigador selecciona el tipo de estudio idóneo para responder a la interrogante que motiva la investigación.

3.1. Tipo de investigación

Tiendo en cuenta la características del proyecto, se empleará en el desarrollo del mismo el método investigación de tipo factible, que de acuerdo al "Manual de Tesis de Grado y Especialización y Maestría y Tesis Doctorales" (2006) de la Universidad Pedagógica Experimental Libertador, consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos.

Con base en la anterior definición, el presente trabajo corresponde al análisis y desarrollo de una propuesta para la evaluación del Sistema de Seguridad de la Información para el grupo NAGALTEC S.A, de acuerdo al alcance definido, las necesidades de la empresa y tomando para ello el modelo de referencia de seguridad de la norma ISO/IEC 27001:2013.

También, durante el desarrollo del proyecto se utilizara el método de investigación de campo, que permite el análisis sistemático del problema en la realidad, con el fin de describirlo, interpretarlo, entender su naturaleza y explicar sus causas y efectos. En este tipo de investigación, la información de interés es recogida de forma directa de la fuente, mediante encuestas, cuestionario entrevista o reuniones.

3.2. Muestra

Se determinó para la presente investigación que la población sujeta a la realización de muestras son los trabajadores que forman parte y tienen acceso a la información y manejo del área de sistemas, al jefe encargado de dicha área y el gerente de la empresa.

3.3. Técnicas e Instrumentos de recolección de la Información

Para el desarrollo del presente trabajo de grado, se utilizaron los siguientes mecanismos e instrumentos para la recolección de información:

Cuestionario.

Observaciones.

Entrevistas con el personal de la empresa.

Documentación existente en la empresa.

Evaluación con base en la experiencia de los autores.

También, se usó de diferentes fuentes de información, tales como tesis, libros, textos, revistas, normas, etc., existentes tanto en medios físicos, electrónicos y publicados en Internet.

3.4. Procesamiento y Análisis de la información

La información recolectada, fue analizada cuantitativamente mediante el respectivo conteo, registro y frecuencia de los datos y presentada a través de una tabla donde se agrupo los resultados de la encuesta. A sí mismo la información se interpretó cualitativamente con el objeto de determinar los aspectos relevantes orientados a la Evaluación de la seguridad de la información en el área de sistemas de la empresa grupo NAGALTEC S.A.S. según la ISO 27001.

3.5. Sistema de Categoria

Objetivo General: Evaluar el sistema de seguridad de la información de la empresa Nagaltec S.A., tomando como referencia la norma NTC-ISO-IEC 27001:2013.				
Objetivos Específicos	**Técnica**	**Instrumentos**	**Indicador**	**Actividades**
Analizar la situación actual de la empresa, con relación a la gestión de seguridad de la información.	Encuesta	Encuesta con preguntas cerradas. Formato de encuesta	Todos los empleados de la empresa tendrán conocimiento de la importancia del sistema de gestión de seguridad de la información en un 30% respecto a la situación inicial.	Aplicar encuesta a los empleados de la empresa
Establecer las necesidades y requerimientos con relación al sistema de seguridad de la Información.	Observación	Lista de verificación	Las necesidades de la empresa se establecerán en 40% teniendo en cuenta los requerimientos del sistema de seguridad de la información.	Realizar trabajo de campo. Interpretar la información cualitativamente orientado a la evaluación de la información.
Definir la política, control y mecanismo de seguridad frente a los riegos encontrados en el sistema de seguridad de la información de la empresa.	Plan de auditoria	Documentación existente en la empresa	Al finalizar el proyecto la empresa tendrá un informe de auditoría frente a los riesgos encontrados.	Realizar Pla de auditoria. Evaluación documentación existente.

CAPITULO 4. RESULTADOS

4.1. OBE1: Analizar la situación actual de la empresa, con relación a la gestión de seguridad de la información.

Para el cumplimiento de este objetivo se aplicó una encuesta y una entrevista a cada uno de los integrantes del personal que conforman el grupo NAGALTEC S.A. El modelo de la encuesta aplicado se puede ver en: (Anexo 1) de este documento.

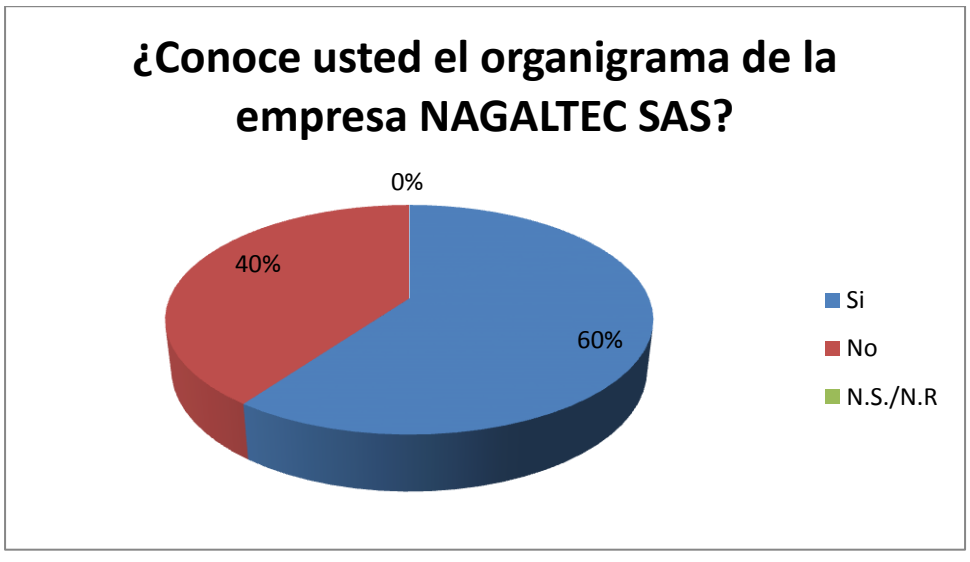
A continuación se presenta el análisis de los resultados obtenidos:

1. ¿Conoce usted el organigrama de la empresa NAGALTEC SAS?}

Tabla 3 Conocimiento Organigrama de la Empresa

Ítems	Frecuencia	Porcentaje
Si	3	
No	2	
N.S./N.R	0	
Total	5	

Fuente: Autores del Proyecto



Fuente: Autores del Proyecto

Figura 3. Conocimiento organigrama de la empresa

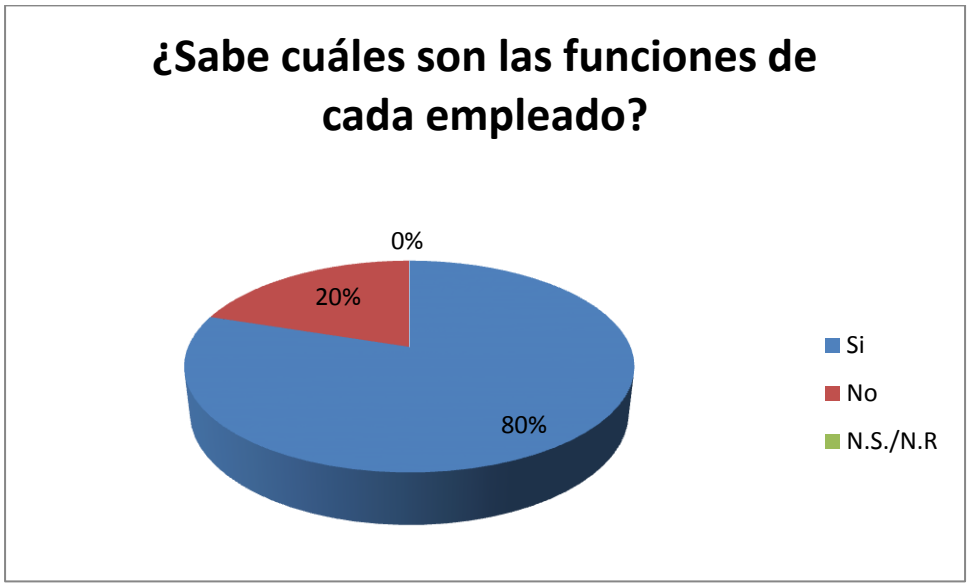
El sistema de empalme y conocimiento del funcionamiento de la empresa presenta deficiencias en un 40%, que corresponde a los empleados que no tienen claro el funcionamiento de la empresa respecto al 60% que están involucrados con el tema.

2. ¿Sabe cuáles son las funciones de cada empleado?

Tabla 4Conocimiento funciones de los empleados

Ítems	Frecuencia	Porcentaje
Si	4	
No	1	
N.S./N.R	0	
Total	5	

Fuente: Autores del Proyecto



Fuente: Autores del Proyecto

Figura 4 Conocimiento funciones de los empleados

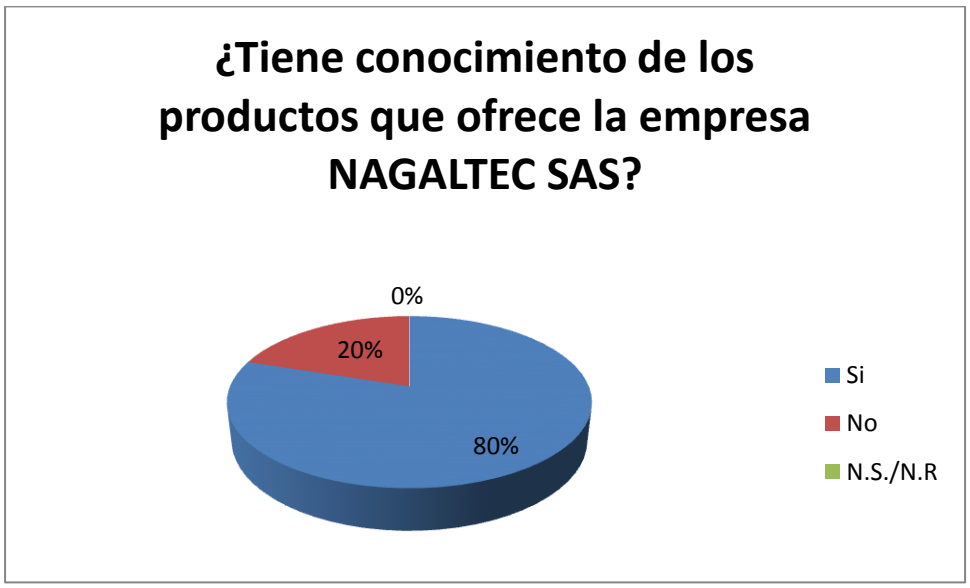
El conocimiento de las funciones de cada empleado es vital para el buen desarrollo de una empresa, en este caso la empresa tiene un nivel aceptable debido que el 80% conoce cuáles son sus funciones y actividades dentro de la organización.

3. ¿Tiene conocimiento de los productos que ofrece la empresa NAGALTEC SAS?

Tabla 5 Conocimiento productos ofertados

Ítems	Frecuencia	Porcentaje
Si	4	
No	1	
N.S./N.R	0	
Total	5	

Fuente: Autores del Proyecto



Fuente: Autores del Proyecto

Figura 5 Conocimiento productos ofertados

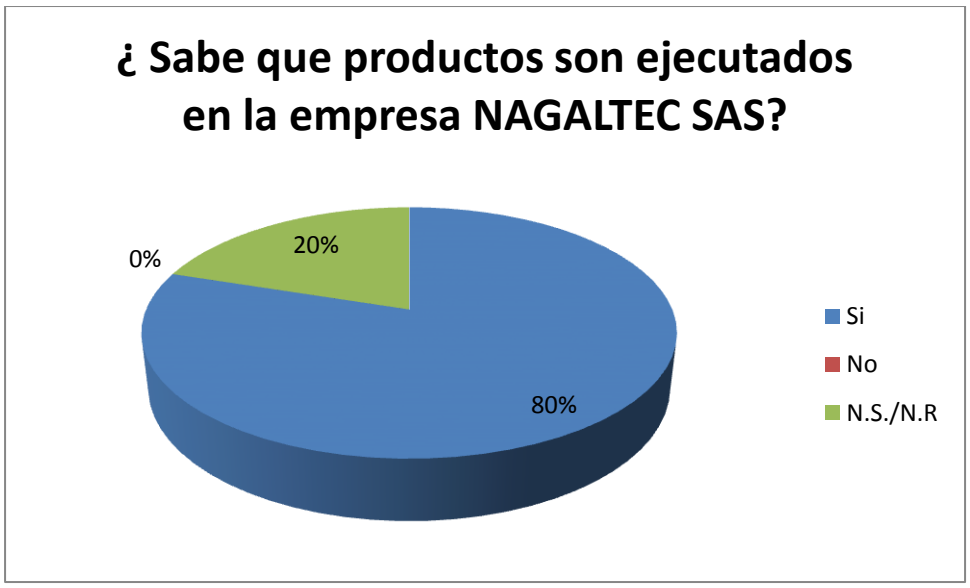
En este caso es importante reforzar el 20% de los empleados que no tiene claridad respecto al portafolio de productos que maneja la empresa, ya que estas fallas podrían generar fuga de información y pérdida de clientes.

4. ¿Sabe que productos son ejecutados en la empresa NAGALTEC SAS?

Tabla 6 Conocimiento productos ejecutados

Ítems	Frecuencia	Porcentaje
Si	4	
No	0	
N.S./N.R	1	
Total	5	

Fuente: Autores del Proyecto



Fuente: Autores del Proyecto

Figura 6Conocimiento productos ejecutados

El nivel de conocimiento respecto a los productos ejecutados en NAGALTEC SAS, es relativamente alto, se refleja en el 80% de sus empleados que responden afirmativamente frente a este tema, sin embargo es importante llegar a la totalidad de conocimiento por parte de la planta de personal, por lo tanto es necesario revisar el 20% que tiene debilidades en este aspecto.

5. ¿Se da importancia a los requerimientos y sugerencias de los clientes?

Tabla 7 Importancia Requerimientos Clientes

Ítems	Frecuencia	Porcentaje
Si	4	
No	1	
N.S./N.R	0	
Total	5	

Fuente: Autores del Proyecto

Fuente: Autores del Proyecto

Figura 7 Importancia requerimientos clientes

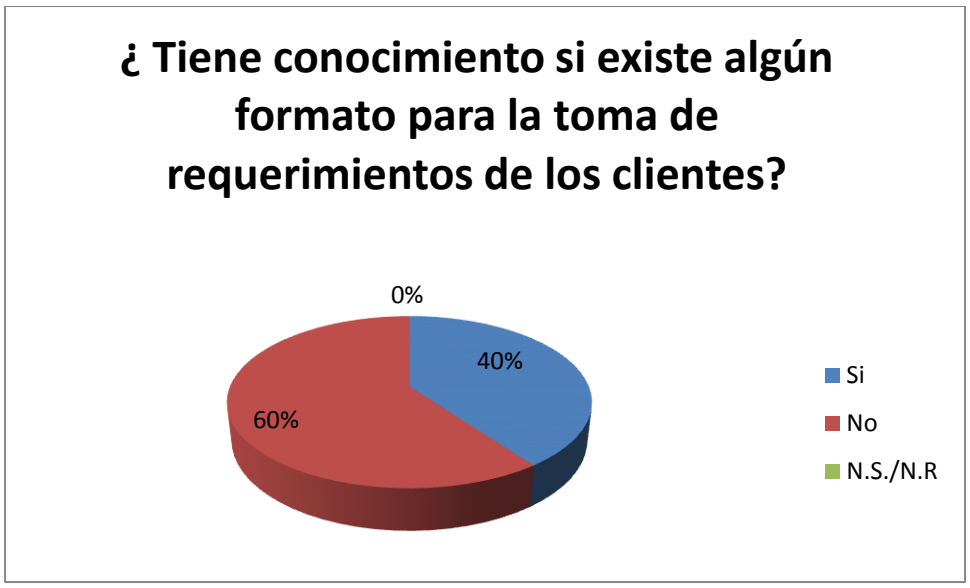
En NAGALTEC SAS, tienen claro la importancia de los clientes para la empresa, y el 80% atiende los requerimientos y sugerencias de los mismos, estando aun en el proceso de mejora del 20% restante de los empleados, que no consideran tan importante esta gestión del servicio al cliente.

6.¿ Tiene conocimiento si existe algún formato para la toma de requerimientos de los clientes?

Tabla 8 Conocimiento formato requerimiento Clientes

Ítems	Frecuencia	Porcentaje
Si	2	
No	3	
N.S./N.R	0	
Total	5	

Fuente: Autores del Proyecto



Fuente: Autores del Proyecto

Figura 8 Conocimiento Requerimiento Formato Clientes

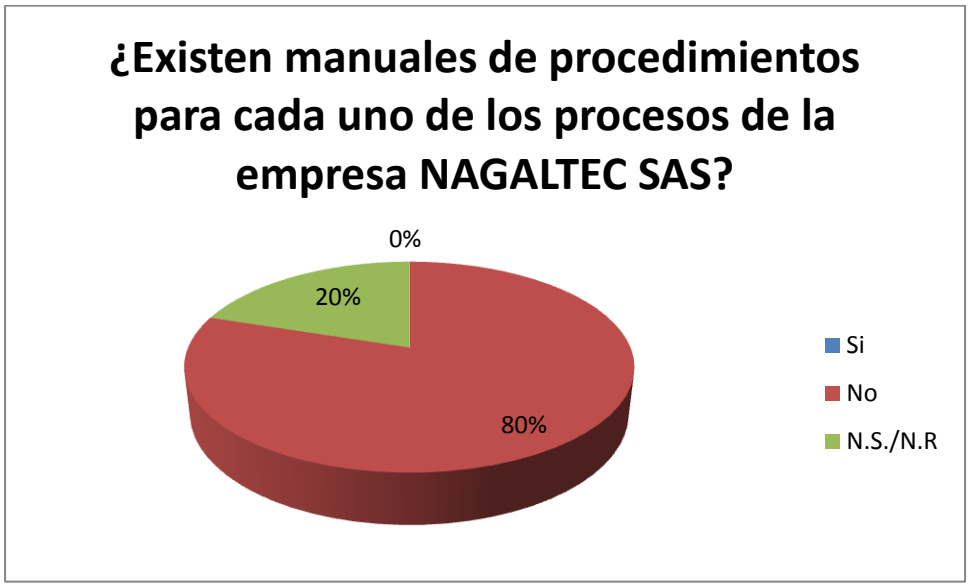
A pesar que se da la importancia de las sugerencias del cliente estas no se sistematizan, como se refleja en el 60% que desconoce la existencia de un formato que permita registrar la información, darle solución en el corto tiempo y realizar acciones de mejora al interior de la organización.

7. ¿Existen manuales de procedimientos para cada uno de los procesos de la empresa NAGALTEC SAS?

Tabla 9 Conocimiento Manual de Procedimientos

Ítems	Frecuencia	Porcentaje
Si	0	
No	4	
N.S./N.R	1	
Total	5	

Fuente: Autores del Proyecto



Fuente: Autores del Proyecto

Figura 9 Conocimiento manual de procedimientos

De acuerdo a los resultados la empresa no posee manuales de procedimientos, para cada uno de los procesos, como lo manifiesta el 80% de los encuestados respecto al 20% que tiene conocimiento del mismo.

8. ¿Existen técnicas de gestión de riesgos para medir y evaluar la vulnerabilidad de la empresa?

Tabla 10 Existencia Técnicas de gestión de riesgos

Ítems	Frecuencia	Porcentaje
Si	0	
No	5	
N.S./N.R	0	
Total	5	

Fuente: Autores del Proyecto

Fuente: Autores del Proyecto

Figura 10 Existencia técnicas de gestión de riesgos

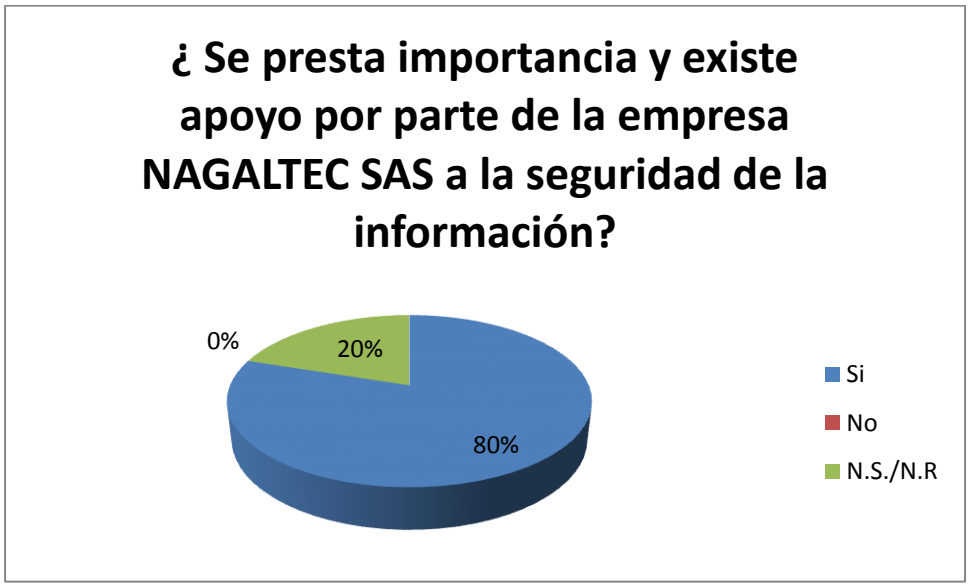
En este apartado se encuentra una falencia de la empresa, ya que no posee gestión de riesgos para medir la vulnerabilidad de la organización, como lo refleja el 100% de los encuestados.

9. ¿Se presta importancia y existe apoyo por parte de la empresa NAGALTEC SAS a la seguridad de la información?

Tabla 11 Apoyo en la seguridad de la Información

Ítems	Frecuencia	Porcentaje
Si	4	
No	0	
N.S./N.R	1	
Total	5	

Fuente: Autores del Proyecto



Fuente: Autores del Proyecto

Figura 11 Apoyo en la seguridad de la información.

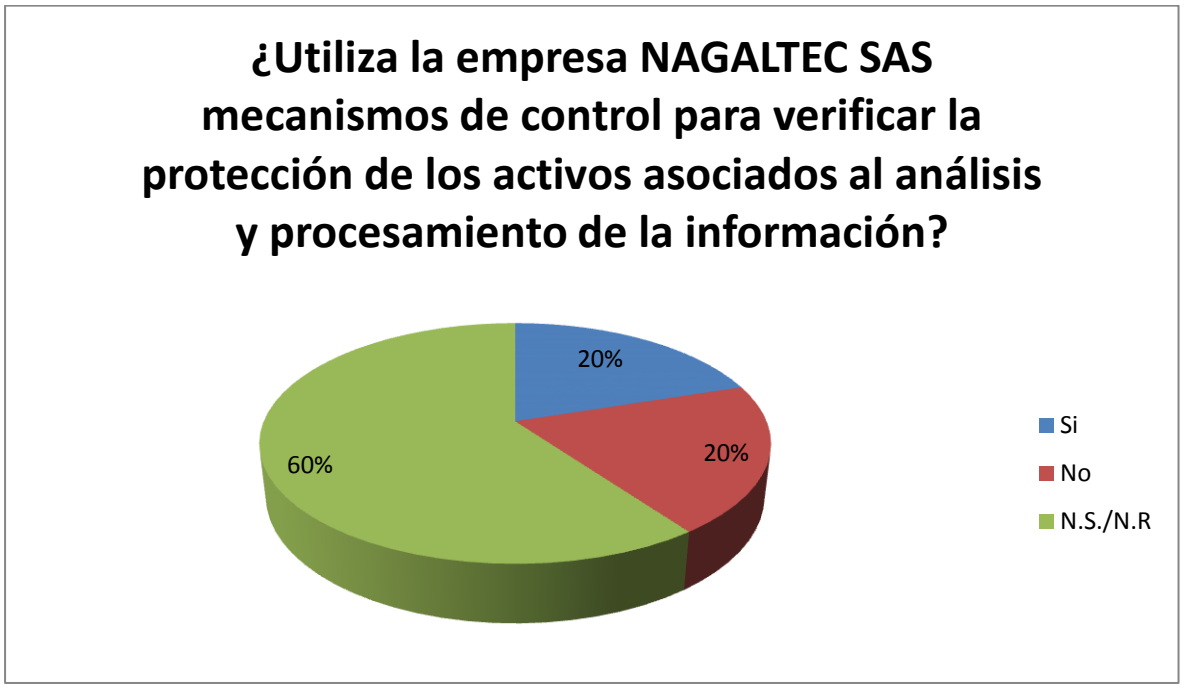
El 80% de los encuestados encuentra apoyo por parte del a organización, referente a la seguridad de la información, lo que se convierte en una fortaleza para la empresa ya que salvaguardan el activo más importante que tiene NAGALTEC SAS.

10. ¿Utiliza la empresa NAGALTEC SAS mecanismos de control para verificar la protección de los activos asociados al análisis y procesamiento de la información?

Tabla 12 utilización mecanismos de control

Ítems	Frecuencia	Porcentaje
Si	1	
No	1	
N.S./N.R	3	
Total	5	

Fuente: Autores del Proyecto



Fuente: Autores del Proyecto

Figura 12 Utilización Mecanismos de control

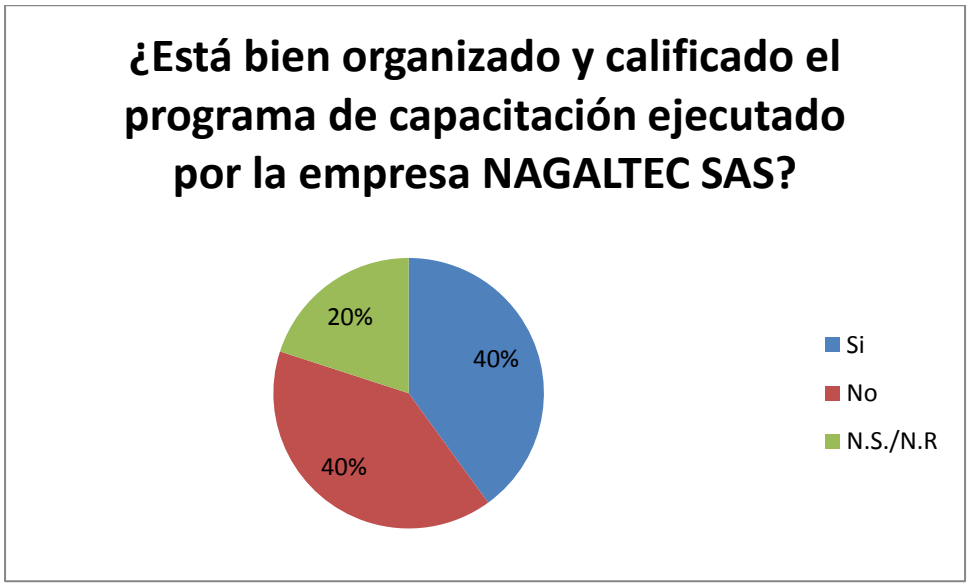
En este apartado si la empresa utiliza mecanismos de control para verificar los activos asociados al análisis y procesamientos de la información, el 60% de los encuestados no tiene conocimiento de esta información, lo que se convierte en una falencia importante en la cual debe trabajar NAGALTEC SAS.

11. ¿Está bien organizado y calificado el programa de capacitación ejecutado por la empresa NAGALTEC SAS?

Tabla 13 calificación programa de capacitación

Ítems	Frecuencia	Porcentaje
Si	2	
No	2	
N.S./N.R	1	
Total	5	

Fuente: Autores del Proyecto



Fuente: Autores del Proyecto

Figura 13. Calificación Programa de Capacitación.

Analizando los porcentajes de las respuestas, el 20% no tiene conocimiento al respecto, mientras que el 40% considera que el programa de capacitación de la empresa no se ajusta a los parámetros de una organización de este tipo, lo que indica una falencia importante que la empresa debe revisar y mejorar.

12. ¿Se manejan políticas de seguridad para conservar la integridad de la información?

Tabla 14. Manejo políticas de seguridad

Ítems	Frecuencia	Porcentaje
Si	3	
No	1	
N.S./N.R	1	

Fuente: Autores del Proyecto

Fuente: Autores del Proyecto

Figura 14. Manejo Políticas de seguridad.

El 60% considera que la empresa tiene políticas de seguridad adecuadas para conservar la integridad de la información, sin embargo en importante realizar una evaluación frente al 40% que considera que dichas políticas no son tan eficientes o en son desconocidas por parte de la planta de personal.

13. ¿Existe una bitácora o un registro del acceso de personal a las diferentes areas de la empresa?

Tabla 15. Existencia registro acceso de personal

Ítems	Frecuencia	Porcentaje
Si	0	
No	3	
N.S./N.R	2	
Total	5	

Fuente: Autores del Proyecto

Fuente: Autores del Proyecto

Figura 15. Existencia registro acceso de personal

La empresa no cuenta con una bitácora del acceso de personal a las diferentes areas de la empresa, de acuerdo al 60% de los encuestados esto se convierte en un riesgo importante ya que al no documentar los desplazamientos del personal, se puede presentar fuga de información o procedimientos indebidos.

14. ¿Se cuenta con un inventario de todos los equipos de cómputo que existen en NAGALTEC SAS?.

Tabla 16. Inventario equipos de computo

Ítems	Frecuencia	Porcentaje
Si	3	
No	1	
N.S./N.R	1	
Total	5	

Fuente: Autores del Proyecto

Fuente: Autores del Proyecto

Figura 16. Inventario equipos de cómputo.

El inventario de equipos de cómputo existente de NAGALTEC SAS. Solo es conocido por el 60% de los encuestados, lo que indica que pueden existir falencias en los procesos de inducción del personal a la empresa, ya que el 40% manifiesta que no conoce o no existe este inventario.

4.1.1. Hallazgos Encontrados de acuerdo a la norma NTC-ISO/IEC 27001 en el Anexo A.

Los objetivos de control y los controles enumerados en la Tabla A.1 se han obtenido directamente de los de la NTC-ISO/IEC 17799:2005, numerales 5 a 15, y están alineados con ellos. Las listas de estas tablas no son exhaustivas, y la organización puede considerar que se necesitan objetivos de control y controles adicionales (NTC-ISO/IEC 27001, 2013. Pág.15)

El informe entregado al representante legal de la empresa se encuentra en el anexo 2 de este documento. (Ver anexo 2).

A.5. Política de Seguridad:

A.5.1 Política de seguridad de la información

Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes

NO SE CUMPLE

De acuerdo a los resultados de la encuesta la totalidad de los consultados manifiesta que en la empresa no existen técnicas de gestión de riesgos para medir y evaluar la vulnerabilidad de la empresa.

A. 10. Gestión de Comunicaciones y Operaciones:

A.10.1 Procedimientos operacionales y responsabilidades

Objetivo: asegurar la operación correcta y segura de los servicios de procesamiento de información

NO SE CUMPLE

De acuerdo a los resultados de la encuesta la totalidad de los consultados manifiesta que en la empresa no existen manuales de procedimientos para cada uno de los procesos de la empresa NAGALTEC S.A.

A.7 Gestión de Activos

A.7.2 Clasificación de la información

Objetivo: asegurar que la información recibe el nivel de protección adecuado.

NO SE CUMPLE

De acuerdo a los resultados de la encuesta la totalidad de los consultados manifiesta que en la empresa no se utilizan mecanismos de control para verificar la protección de los activos asociados al análisis y procesamiento de la información.

4.2. OBE2: Establecer las necesidades y requerimientos con relación al sistema de seguridad de la Información.

En este sentido se realizó un plan de auditoria y se aplicó una lista de verificación que se encuentran en el anexo 3 de este documento. (ver anexo 3).

4.2.1. Contexto de la organización

La norma ISO/IEC 27001:2013 reitera la importación de conocer y comprender los factores externos e internos de la organización, que pueden afectar o ser afectados de manera positiva o negativa por el establecimiento del Sistema de Gestión de Seguridad de la Información.

Para tal efecto, la norma ISO/IEC 27001:2013 incluye el capítulo “4. CONTEXTO DE LA ORGANIZACIÓN”, donde se establece que la entidad debe determinar las situaciones y factores externos e internos que la rodean y que son pertinentes para establecer al Sistema de Gestión de Seguridad de la Información.

4.2.1.1. Conocimiento de la Organización

Naturaleza de la Entidad.

El grupo Nagaltec es una sociedad por acciones simplificada vigilada por la superintendencia de sociedades y su objeto son las actividades de consultoría informática y actividades de administración de instalaciones informáticas. En el anexo 4 de este documento se encuentran las imágenes de las instalaciones donde funciona la empresa.(Ver anexo 4).

Misión

Brindar soluciones integradas en Tecnología de la Información que apoyen a las empresas de producción y servicio en la consecución de sus metas críticas. Para ello entregamos productos y servicios informáticos con valor agregado que superen las expectativas y necesidades de nuestros clientes.

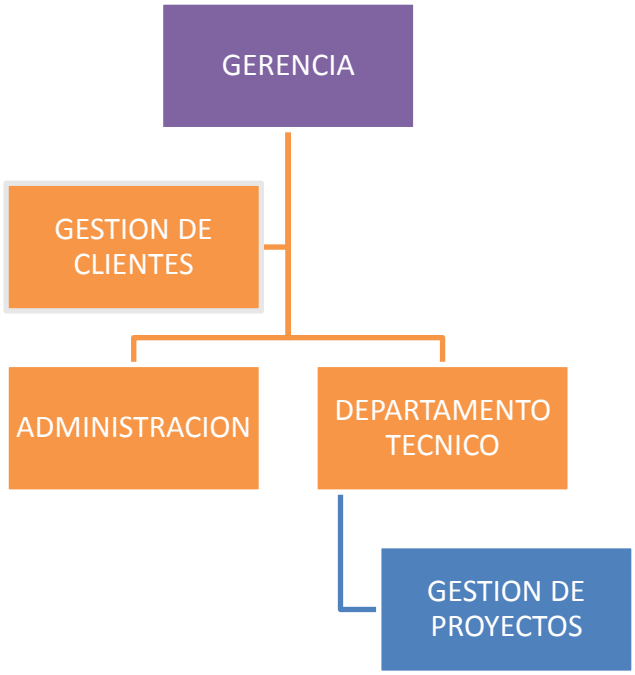
Visión

Ser la compañía más innovadora y referente en nuestro sector, líder en soluciones, servicios informáticos y generación de valor para la completa gestión de las pequeñas y medianas empresas.

Actividades que Desarrolla la Entidad

Nagaltec S.A. es una empresa del medio de desarrollo tecnológico que crea soluciones confiables y seguras conforme a las necesidades de los clientes, su portafolio de servicios está orientado a la creación de páginas web, plantillas web, Dominios, Alojamiento de Información, sistemas de Información, y APPs.

Estructura Organizacional



Fuente: Organigrama NAGALTEC S.A.S

Figura 17. Organigrama de la Empresa

Areas críticas de la Empresa

Las siguientes son las áreas críticas de la empresa, donde se deben establecer las mayores medidas y controles de seguridad con el objetivo de proteger y garantizar la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y no repudio de la información que en ellas se maneja:

Administración: Tiene por función principal garantizar la disponibilidad, continuidad, confiabilidad y seguridad de la infraestructura tecnológica y de telecomunicaciones que soportan los sistemas de información y recursos tecnológicos necesarios para la operación del negocio. Así mismo, su responsabilidad es garantizar la seguridad informática en la entidad e implementar las

medidas y controles tecnológicos orientados a evitar, prevenir o mitigar las amenazas informáticas que puede atentar contra la disponibilidad, integridad y confidencialidad de la información de la entidad.

Gestión de Clientes: Encarga de la recepción de correspondencia y documentos tanto internos como externos, y de la radicación e inclusión de los mismos en el sistema de gestión documental de la entidad, para su respectiva clasificación, asignación, distribución y entrega digital o en medio físico a los usuarios destinarios de la información. Debido que esta área está expuesta al público para la recepción de documentación, paquetes y otros elementos, y al volumen y tipo de información que maneja de carácter confidencial, público o de uso interno, en zona cuenta con las medidas de seguridad orientas a evitar accesos no autorizados.

4.2.2. ALCANCE DEL SGSI

El alcance permite determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información de la empresa.

El alcance del Sistema de Gestión de la Seguridad de la información de NAGALTEC S.A, abarca solo para el proceso de Gestión de Tecnología de la Entidad, que involucra la gestión de la infraestructura y plataforma de procesamiento, gestión de aplicaciones, gestión de proveedores de TI, gestión de Incidentes y requerimiento y gestión de cambios de TI.

4.2.3. POLITICA DEL SGSI

La política del Sistema de Gestión de Seguridad de la información corresponde a la declaración general que representa la posición de la gerencia de la empresa con relación a la seguridad de la información.

La norma ISO/IEC 27001:2013 en su numeral 5.2 Política, indica que la Alta Dirección de la empresa debe establecer una política de seguridad de la información adecuado al propósito de la organización, que incluya los objetivo de seguridad de la información, los requerimientos normativos vigentes relacionados con seguridad de la información y el compromiso de la mejora continua

La siguiente es la política general del Sistema de Gestión de Seguridad que se definió:

- Cumplir con los requerimientos legales y reglamentarios aplicables a la entidad y al Sistema de Gestión de Seguridad de la Información.
- Entregar resultados de excelencia, con sentido de pertenencia, actitud proactiva y comunicación continua y oportuna.
- Gestionar los riesgos de la entidad a través de la aplicación de estándares y controles orientados a preservar la seguridad de nuestra información.
- Mantener buenas prácticas de seguridad de la información que garantizan la Disponibilidad, Integridad y Confidencialidad de la información, proporcionando confianza en nuestras partes interesadas
- Implementar el sistema de gestión de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los colaboradores de la Entidad.
- Garantizar la continuidad de los servicios y la seguridad de la información.

4.2.4. ESTRUCTURA ORGANIZACIONAL DE LA SEGURIDAD

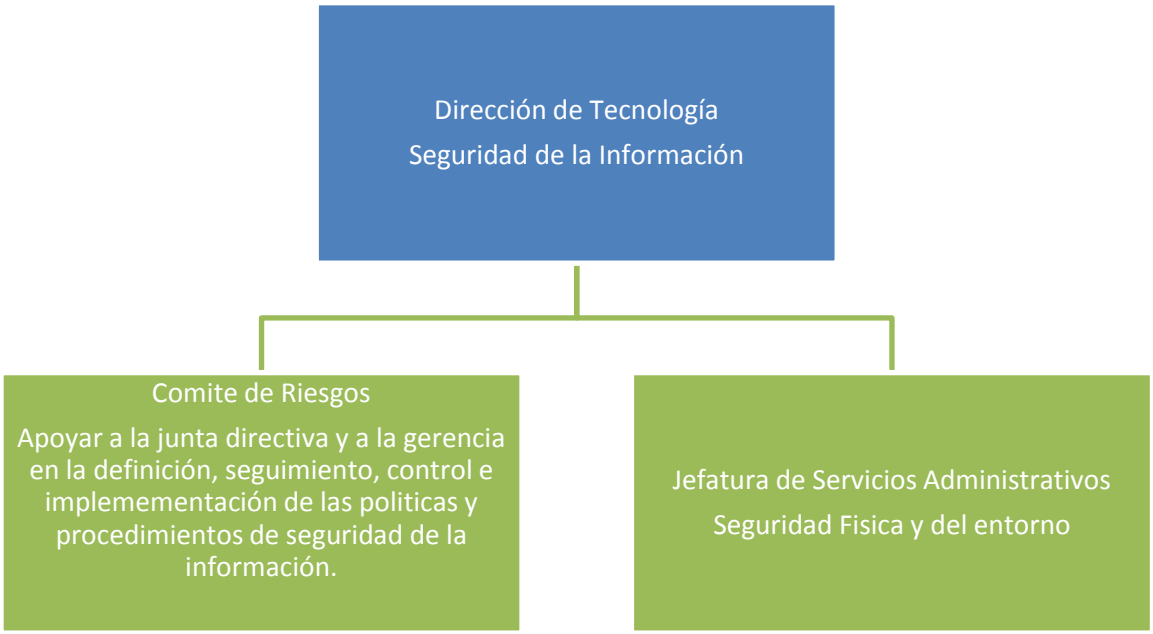
De acuerdo al numeral '5.3 Roles, Responsabilidades y autorizadas en la organización' de la norma ISO/IEC 27001:2013, la alta directiva debe asegurar que se asignen las responsabilidad y autoridades para los roles pertinentes a la seguridad de la información. Con base en este requerimiento de la norma, como primero medida se identificaron las áreas dentro de la entidad cuyas funciones están relacionadas con la seguridad de la información, para lo cual se tuvo en cuenta los siguientes aspectos:

Responsable de la seguridad de la información

Responsable de la seguridad informática

Responsable de la seguridad física

De acuerdo a lo anterior, se identificó el siguiente organigrama que permite identificar las dependencias de la entidad cuyas funciones son pertinentes a la seguridad de la información:



.

Fuente: Autores del proyecto

Figura 18. Organización de la seguridad de la Información

Una vez identificadas las áreas que cumplen funciones de seguridad de la información, se procedió a establecer las siguientes responsabilidades de la seguridad de la información para los roles pertinentes:

Comité de riesgos:

- Establecer los mecanismos adecuados para la gestión y administración de riesgos, seguridad de la información, continuidad del negocio, velar por la capacitación del personal de la entidad en lo referente a estos temas.
- Informar a la Junta Directiva sobre aspectos relacionados con la gestión de riesgos, seguridad de la información y continuidad de negocio.
- Diseñar y aprobar la estrategia de gestión de riesgos, seguridad de la información y continuidad de negocio de la Entidad y liderar su ejecución.
- Asegurar la existencia de metodologías, políticas y sistemas para riesgos, seguridad de la información y continuidad de negocio.
- Asegurar la implementación en la entidad, de la normatividad o requerimientos que sobre los temas de riesgos, seguridad de la información y continuidad del negocio que impartan o solicite el ente regulador o los entes de control.

.

Dirección de Tecnología:

- Asegurar el cumplimiento de las políticas y requerimientos de seguridad establecidos para la adquisición, diseño, desarrollo, operación, administración y mantenimiento de los

sistemas operativos, bases de datos, recursos, plataforma tecnológica y servicios de telecomunicaciones de la entidad.

- Asegurar el cumplimiento de las políticas y requerimientos de seguridad establecidos para la adquisición, diseño, desarrollo, operación, administración y mantenimiento de los Sistemas de Información de la entidad.
- Asignar las funciones, roles y responsabilidades de Seguridad, a sus funcionarios para la operación y administración de la plataforma tecnológica de la entidad. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.
- Implementar los controles y medidas de seguridad

Jefatura de servicios Administrativos

- Implementar las medidas de seguridad física adecuadas con el objetivo de proteger a la entidad antes situaciones generadas por eventos naturales, alteraciones del entorno, acciones humanes y accesos no autorizadas, que pueden comprometer la seguridad de la información de la entidad y la continuidad del negocio.
- Implementar las medidas de seguridad física con el objetivo de control el acceso a las instalaciones de la entidad de acuerdo a nivel de criticidad.

CONCLUSIONES

El análisis de la de la empresa con relación a la gestión de seguridad de la información basado en un modelo de mejoras, prácticas y lineamientos de seguridad, como es la norma ISO/IEC 27001:2013, permitió identificar para la empresa un diagnostico con el objeto de establecer un modelo de seguridad de la información a fin que la organización logre cumplir a futuro al pie de la letra lo establecido en la norma en mención.

A través de la alta directiva de NAGALTEC SAS, se establecieron las necesidades y requerimientos con relación al sistema de seguridad de la información, y se identificó El nivel de cumplimiento de la entidad frente de los requerimientos del Anexo A de la norma ISO/IEC 27001:2013, es del 46%, lo que significa que la implementación del Sistema de Gestión de Seguridad de la información le implicará a la empresa un refuerzo considerable debido a la ausencia de controles o al bajo grado de cumplimiento de muchos de ellos.

Resultado de tratar de aplicar los diferentes requerimientos de la norma ISO27001:2013, se logró obtener una serie de diagnósticos que permitieron establecer el nivel de madures de la entidad frente a la gestión de la seguridad de la información. Es necesario el establecimiento de unas políticas de seguridad aprobadas por la Alta Dirección, para garantizar su debida implementación, actualización y cumplimiento.

RECOMENDACIONES

La empresa requiere implementar una serie de controles con el objetivo de fortalecer su seguridad y poder dar cumplimiento a los requerimientos establecidos en la norma ISO 27001:2013, por eso es fundamental que lleven a cabo los diferentes planes de acciones que se definieron en el presente trabajo de grado.

Es necesario que la Dirección de Tecnología de la entidad revise su capacidad con el objetivo de garantizar la debida implementación de los controles y planes de acciones que se requieren llevar a cabo para cerrar las brechas encontradas producto de los diagnósticos realizados, ya que la mayoría de estos planes de acción requiere un componente tecnológico.

Realizar campañas de seguridad de la información, con el propósito de poder generar un sentido de pertenencia y apropiación en temas de seguridad en cada uno de los funcionarios de la entidad, y concientizar sobre los riesgos que pueden afectar la seguridad de la información.

4.3 OBE3: Definir la política, control y mecanismo de seguridad frente a los riegos encontrados en el sistema de seguridad de la información de la empresa.

A.5. Política de Seguridad:

A.5.1 Política de seguridad de la información

Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes

Riesgo encontrado: no se existen técnicas de gestión de riesgos para medir y evaluar la vulnerabilidad de la empresa.

Mecanismo de control:

- La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.
- La dirección debe apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información.
- Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información.

A. 10. Gestión de Comunicaciones y Operaciones:

A.10.1 Procedimientos operacionales y responsabilidades

Objetivo: asegurar la operación correcta y segura de los servicios de procesamiento de información

Riesgo encontrado: no existen manuales de procedimientos para cada uno de los procesos de la empresa NAGALTEC S.A.

Mecanismo de control:

- Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.
- Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información

A.7 Gestión de Activos

A.7.2 Clasificación de la información

Objetivo: asegurar que la información recibe el nivel de protección adecuado.

Riesgo encontrado: no se utilizan mecanismos de control para verificar la protección de los activos asociados al análisis y procesamiento de la información.

Mecanismo de control:

- La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.
- Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.

REFERENCIAS

ÁLVAREZ ZURITA, Flor M y GARCÍA GUZMÁN, Pamela A. Implementación de un Sistema de Gestión de Seguridad de la Información basada en la norma ISO 27001. Para la Intranet de la Corporación Metropolitana de Salud. Quito, Ecuador.. 2007. 298 h. Escuela Politécnica Nacional. [en línea]. http://bibdigital.epn.edu.ec/handle/15000/565

Asociación Española para la calidad . Articulo. 2017 recuperado de Internet: https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

Constitución Política de 1991 Recuperado de Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125

ESPITIA DIEGO SAMUEL Fecha: Feb 10, 2015 Categoría/s: Seguridad Articulo Los beneficios y la importancia de gestionar la seguridad de la información, Recuperado de Internet: http://reportedigital.com/seguridad/importancia-gestionar-seguridad-informacion/

George Beekman (1996) recuperado de internet http://problema.blogcindario.com/2008/10/00014-marco-teorico.html

ISO ISO/IEC 27000:2014, Pág. 4 Recuperado de internet: http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO/IEC 27002 Recuperado de Internet: http://www.iso27000.es/iso27002.html

ISO/IEC 27003**.** http://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

ISO/IEC 27004. https://orff.uc3m.es/bitstream/handle/10016/10564/PFC_agustin_Larrondo_Quiros.pdf?sequence=1

ISO/IEC 27005: Recuperado de internet: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27005.pdf

ISO/IEC 27006. Recuperado de internet: http://www.pmg-ssi.com/2014/02/isoiec-27006-guia-para-la-certificacion-del-sgsi/

Ley 1273 del 5 de enero de 2009. Delitos informáticos. Recuperado de internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Ley 1341 de 2009. Recuperado de internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

Ley estatutaria 1266 del 31 de diciembre de 2008 . Recuperado de internet : http://www.redipd.org/legislacion/common/legislacion/Colombia/LEY_1266_31_12_2008_HabeasData_COLOMBIA.pdf

Ley Estatutaria 1581 de 2012. Recuperado de internet: https://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf

Manual de Tesis de Grado y Especialización y Maestría y Tesis Doctorales de la UniversidadPedagógica Libertador, Pág.13. 2006 recuperado de internet http://neutron.ing.ucv.ve/NormasUPEL2006.pdf

ORTEGA PACHECO, Oscar R. Centro de investigaciones económicas, administrativas y sociales, Gestión de la Seguridad de la Información en la Empresa. México D.F. 2010. 90h. Instituto Politécnico Nacional. [en línea]. http://www.repositoriodigital.ipn.mx/handle/123456789/6564

Sistema de seguridad de la Información Recuperado de internet: http://www.iso27000.es/download/doc_sgsi_all.pdf

ANEXOS

Anexo 1. Modelo encuesta aplicado a los empleados de la empresa.

FYW AUDITORES

ENCUESTA APLICADA A EMPLEADOS DE NAGALTEC S.A.S

Objetivo: Analizar la situación actual de la empresa, con relación a la gestión de seguridad de la información.

PREGUNTA	SI	NO	N.S./N.R
1) ¿Conoce usted el organigrama de la empresa NAGALTEC SAS?			
2) ¿Sabe cuáles son las funciones de cada empleado?			
3) ¿Tiene conocimiento de los productos que ofrece la empresa NAGALTEC SAS?			
4) ¿Sabe que productos son ejecutados en la empresa NAGALTEC SAS?			
5) ¿Se da importancia a los requerimientos y sugerencias de los clientes?			
6) ¿Tiene conocimiento si existe algún formato para la toma de requerimientos de los clientes?			
7) ¿Existen manuales de procedimientos para cada uno de los procesos de la empresa NAGALTEC SAS?			
8) ¿Existen técnicas de gestión de riesgos para medir y evaluar la vulnerabilidad de la empresa?			
9) ¿Se presta importancia y existe apoyo por parte de la empresa NAGALTEC a la seguridad de la información?			
10) ¿Utiliza la empresa NAGALTEC SAS mecanismos de control para verificar la protección de los activos asociados al análisis y procesamiento de la información?			
11) ¿Está bien organizado y calificado el programa de capacitación ejecutado por la empresa NAGALTEC SAS?			
12) ¿Se manejan políticas de seguridad para conservar la integridad de la información?			
13) ¿Existe una bitácora o un registro del acceso de personal a las diferentes áreas de la empresa?			
14) ¿Se cuenta con un inventario de todos los equipos de cómputo que existen en NAGALTEC SAS?			

320-910-0058
YARAMARCELA@HOTMAIL.ES
CRA 10 # 12 - 54 CARRETERA CENTRAL

Anexo 2. Informe de auditoría entregado al representante legal de NAGALTEC SAS.

FYW AUDITORES

Señor
Representante legal
NAGALTEC SAS

De acuerdo a las instrucciones giradas por la empresa a su digno cargo, nos permitimos remitir a usted el informe de auditoría practicada al área de sistemas de la empresa NAGALTE SAS, con especial énfasis en la seguridad informática la cual se llevó a cabo desde el

De los resultados obtenidos durante la evaluación, se obtuvieron las siguientes observaciones:

1. De acuerdo a los resultados de la encuesta la totalidad de los consultados manifiesta que en la empresa no se existen técnicas de gestión de riesgos para medir y evaluar la vulnerabilidad de la empresa.
2. En la empresa no existen manuales de procedimientos para cada uno de los procesos de la empresa NAGALTEC S.A.S
3. en la empresa no se utilizan mecanismos de control para verificar la protección de los activos asociados al análisis y procesamiento de la información.
4. No se cuenta con un mecanismo de respuesta automática que permita verificar él envió de la información al final de la jornada de trabajo.
5. Los equipos no cuentan con protección por contraseña que restrinja el acceso de personal no autorizado a las herramientas de la empresa.
6. Los equipos del área de desarrollo no cuentan con un mecanismo que permita regular la sustracción de información no autorizada.
7. No se encontraron extintores en ningún área de la empresa.
8. Los equipos del área de sistemas usan tecnología inalámbrica para conectarse a la red local, esto implica que la red quede expuesta a ataques que tengan como finalidad obtener la contraseña y acceder a ella.
9. Los equipos del personal reciben direccionamiento IP por DHCP, lo cual facilita el acceso a la red en caso de ser vulnerada su seguridad por parte de un visitante no autorizado.
10. Los cambios de password no cuentan con una auditoría de soporte para registrar los movimientos internos y constantes cambios de seguridad.
11. No se lleva un registro de los cambios en los privilegios para el acceso de los usuarios al sistema

320-910-0058
YARAMARCELA@HOTMAIL.ES
CRA 10 # 12 - 54 CARRETERA CENTRAL

FYW AUDITORES

12. No existe un sistema de apoyo eléctrico capaz de mantener encendidos temporalmente los equipos del personal de desarrollo en caso de ocurrir un corte de energía inesperado.
13. Se encontró que el área de sistemas y sus equipos correspondientes no cuentan con el inventario de software y hardware.
14. No existe ninguna política implementada que defina qué tipo de software debe ser utilizado en el área de sistemas.
15. No se encontró un mecanismo de control que regule la descarga de software potencialmente peligroso.
16. Se encontró instalados en los equipos del área de sistemas, software sin sus licencias correspondientes.
17. No se cuenta con un mecanismo de respuesta automática que permita verificar él envió de la información al final de la jornada de trabajo.
18. Los equipos del área de desarrollo no cuentan con un mecanismo que permita regular la sustracción de información no autorizada.

Las siguientes son las áreas críticas de la empresa, donde se deben establecer las mayores medidas y controles de seguridad con el objetivo de proteger y garantizar la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y no repudio de la información que en ellas se maneja:

Administración: Tiene por función principal garantizar la disponibilidad, continuidad, confiabilidad y seguridad de la infraestructura tecnológica y de telecomunicaciones que soportan los sistemas de información y recursos tecnológicos necesarios para la operación del negocio. Así mismo, su responsabilidad es garantizar la seguridad informática en la entidad e implementar las medidas y controles tecnológicos orientados a evitar, prevenir o mitigar las amenazas informáticas que puede atentar contra la disponibilidad, integridad y confidencialidad de la información de la entidad.

- Gestión de Clientes: Encarga de la recepción de correspondencia y documentos tanto internos como externos, y de la radicación e inclusión de los mismos en el sistema de gestión documental de la entidad, para su respectiva clasificación, asignación, distribución y entrega digital o en medio físico a los usuarios destinarios de la información. Debido que esta área está expuesta al público para la recepción de documentación, paquetes y otros elementos, y al volumen y tipo de información que maneja de carácter confidencial, público o de uso interno, en zona cuenta con las medidas de seguridad orientas a evitar accesos no autorizados.

FYW AUDITORES

Por último me permito recomendarle la implementación de las soluciones propuestas según el criterio del equipo evaluador.

- Implementar un sistema de control que permita verificar si el usuario hace la actualización de sus archivos en el repositorio al final de la jornada laboral
- Implementar un software que permita detectar la extracción de archivos de los equipos en tiempo real
- Instalar un sistema de aire acondicionado que permita mantener la refrigerado el cuarto
- Instalar medidores de temperatura y humedad
- Instalar una cerradura electrónica que permita llevar el registro de los empleados que acceden al cuarto de servidores
- Implementar una alarma contra incendios complementado con extintores de tipo Novec 1230 o FM200 / FE-13
- Usar uno de las topologías (Estrella, anillo, mixta etc...) de cableado estructurado para llevar conexión a los equipos del personal de área de sistemas
- Deshabilitar la asignación de direcciones IP por el método DHCP y comenzar a usar un método manual
- Generar un inventario de equipos donde se lleve el registro de la dirección ip y el computador el cual la tiene asignada identificándolo por la dirección MAC
- Realizar ataques de seguridad constantes provocados por la empresa para chequear constancia y robustez en los servidores que contienen la información.
- Desarrollar e implementar un sistema de seguridad confiable para el mantenimiento de las contraseñas de seguridad.
- Implementar un sistema de seguridad confiable para los equipos de forma local.
- Instalar UPS (Uninterruptible Power Supply) fuente de poder interrumpible que permita el almacenamiento de la información manipulada y desarrollada en los diferentes equipos que lo requieran.
- Generar un inventario de software que permita establecer con que herramientas cuenta la empresa.
- Definir políticas claras que establezcan el tipo de software que se debe utilizar.
- Hacer una revisión periódica de los equipos para verificar el software instalado en los mismos.

320-910-0056
YARAMARCELA@HOTMAIL.ES
CRA 10 # 12 - 54 CARRETERA CENTRAL

FYW
AUDITORES

Esperamos haber cumplido las expectativas de su empresa y quedamos atentos a sus inquietudes.

320-910-0056
YARAMARCELA@HOTMAIL.ES
CRA 10 # 12 - 54 CARRETERA CENTRAL

Anexo 3. Plan de auditoria y lista de chequeo

FYW AUDITORES

PLAN DE AUDITORIA

EMPRESA	NAGALTEC S.A.S		
DIRECCION	CLL 9ª #9-75 BARRIO LA COSTA		
REPRESENTANTE LEGAL	Olger Navarro Guerrero		
CARGO	Representante legal	**CORREO**	info@gruponagaltec.com
		TELEFONO	3174045199
ALCANCE: Inicia con el conocimiento de las actividades propias de la empresa , verificando el estado de la protección de los activos asociados al análisis de la información mediante la elaboración del programa y las herramientas de auditoria, con el fin de establecer políticas y controles en pro del mejoramiento continuo de la organización.			
CRITERIO DE AUDITORIA: Requisitos legales, requisitos internos de la empresa Nagaltec S.A.S documentos asociados a los procesos o áreas, procedimientos o manuales.			
TIPO DE AUDITORIA	OTORGAMIENTO	SEGUIMIENTO **X**	RENOVACION
	AMPLIACIÓN	CUMPLIMIENTO	EXTRAORDINARIA
REUNION DE APERTURA: 09-01-2017		**HORA:** 09:00 AM	
Cordial saludo, me dirijo a usted para remitir el plan de auditoria que se ha planificado junto con todo el equipo auditor y su equipo de trabajo, esto con el fin de poder evidenciar todas las prácticas establecidas por la empresa para el ben manejo de la información y de esta manera establecer políticas que permitan mejorar los procesos internos y que generen impacto para los usuarios externos. Se permite establecer como objetivos principales, los siguientes: Auditoria al estado del protección de los activos asociados l análisis y procesamiento de la información. Definir políticas, controles y mecanismos de seguridad que ayuden a gestionar los riesgos que se puedan presentar. Coordinar la implementación de controles específicos para la información.			
AUDITOR LIDER	Yaira Marcela Escobar Vélez	**CORREO**	ymescobarv@ufpso.edu.co
AUDITOR 1	Wilder Andrés Duarte Neira		
AUDITOR 2	Fabián Alexis Vergel Contreras		

FECHA	**HORA**	**PROCESO / ACTIVIDAD**	**AUDITOR**
09-01-2017	09:00 am	Reunión de apertura	Todo el equipo auditor
09-01-2017	10:30 am	Planificación de las actividades a realizar en el proceso de auditoria	Todo el equipo auditor
09-01-2017	09:00 am	Realización de la entrevista al gerente de la empresa como también la encuesta para los empleados	Todo el equipo auditor

320-910-0068
YAIRAMARCELA@HOTMAIL.ES
CRA 10 # 12 - 64 CARRETERA CENTRAL

FYW AUDITORES

LISTA DE VERIFICACION	EMPRESA: Grupo Nagaltec S.A.S

OBJETIVO: Establecer el conocimiento de las políticas y actividades que se realizan en el área de sistemas.

FECHA DE ELABORACION:

AREA AUDITADA: Sistemas Desarrollo y Soporte

RESPONSABLE DEL AREA: Olger Navarro Guerrero

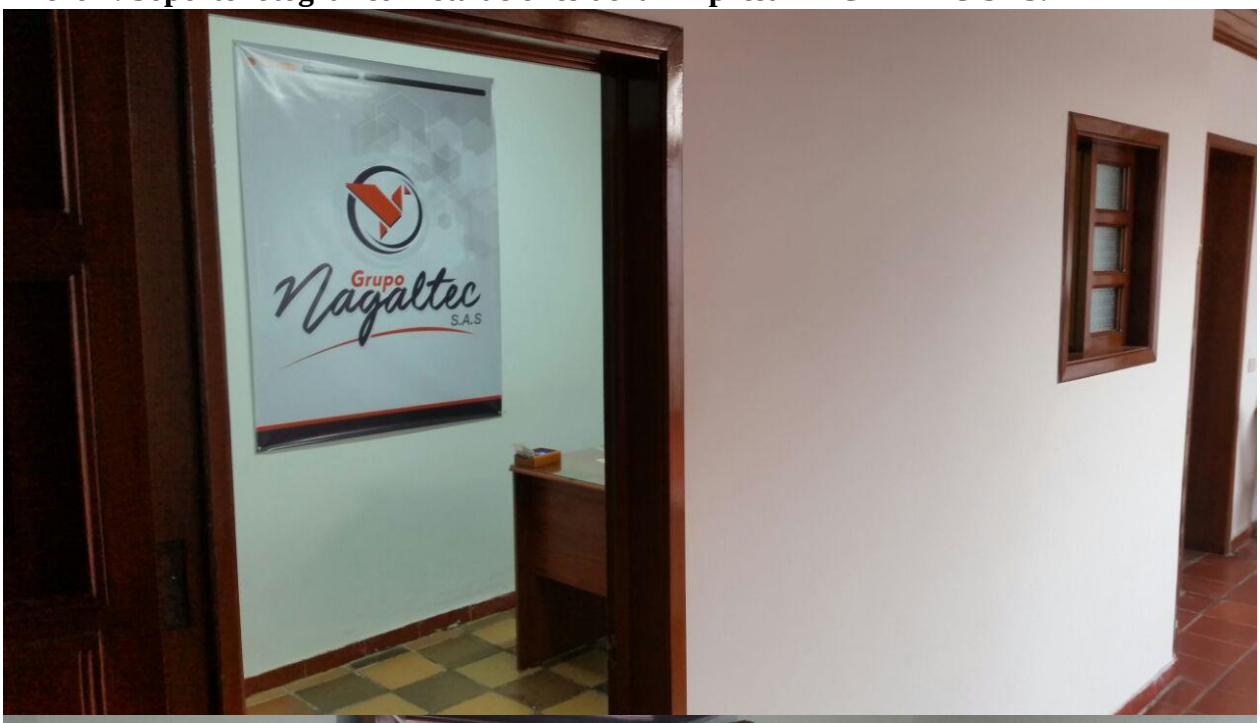
CARGO: Jefe del área de sistemas

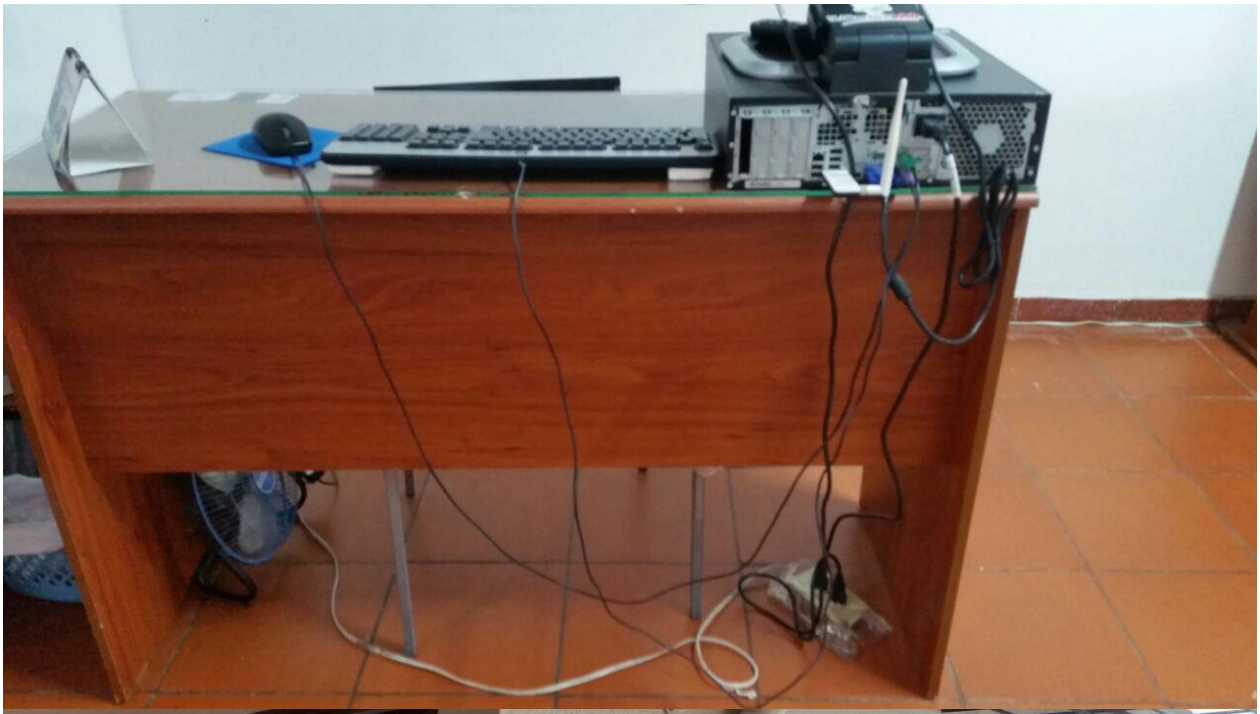
AUDITORES:
Yaira Marcela Escobar Vélez
Fabián Alexis Vergel Contreras
Wilder Andrés Duarte Neira

VERIFICACION	SE REALIZA VERIFICACION
Las características físicas del área de sistemas son seguras	✓
Conexión de los equipos del área de sistemas	✓
Coordinación dentro del área sobre los lineamientos implementados para la seguridad de la información	✓
Implementación de manuales procedimentales	✓
Evaluación de la existencia y uso de normas, resolución de base legal para el diseño del área de sistema	✓
Conoce quién coordina dentro de proceso los lineamientos implementados para la seguridad de la información	✓
Requerimientos de seguridad del área de sistemas	✓
Manual e instructivos para capacitación en el área de sistemas	✓
Planes en caso de contingencia	✓
Contraseñas de ingreso	✓
Bitácora de acceso al área de sistemas	✓
Monitoreo de accesos al sistema	✓
Niveles de acceso y seguridad en la red	✓

320-910-0068
YAIRAMARCELA@HOTMAIL.ES
CRA 10 # 12 - 64, CARRETERA CENTRAL

Anexo 4. Soporte fotográfico Instalaciones de la Empresa NAGALTEC SAS.






DKA 84C