DISEÑO DE LA FASE DE PLANEACIÓN PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN A PARTIR DE LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA GRUPO CONFECCIONISTAS.

JOHN EDWIN SUÁREZ CASTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

DISEÑO DE LA FASE DE PLANEACIÓN PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN A PARTIR DE LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA GRUPO CONFECCIONISTAS.

JOHN EDWIN SUÁREZ CASTRO

Proyecto de Grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Luis Fernando Zambrano
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

DEDICATORIA

A mi familia, quienes en su constante apoyo me brindaron el ánimo, la paciencia y su acompañamiento en los momentos difíciles para concluir una etapa en mi vida que será de gran satisfacción y enriquecimiento a título personal.

AGRADECIMIENTOS

La realización y presentación del siguiente proyecto aplicado, se basa en los conocimientos adquiridos a través del desarrollo del programa académico, también a la dedicación de cada una de las actividades realizadas y por el apoyo constante de los docentes de la universidad, que con sus continuas enseñanzas lograron trasmitir el suficiente conocimiento para conseguir y optar por mi título postgrado.

TABLA DE CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

Pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

GLOSARIO

Términos de marcos de gestión basados en Williams[1]

ACTIVO DE INFORMACIÓN: Activo de información, que hace parte de los elementos a los que se les debe brindar seguridad para evitar suplantación y captura no deseada.

AMENAZAS: Situación que pone en peligro un Activo de información.

CICLO DE VIDA: Consecución de un determinado proceso desde su etapa inicial hasta la final.

CONTINUIDAD: Consecución de una determinada acción sin interferir en las actividades por riesgos relacionados con la seguridad de la información.

CONTAINER: Elemento que agrupa en categorías los activos de información.

CONFIABILIDAD: Prestación oportuna y óptima de un dispositivo para determinada función.

CONFIDENCIALIDAD: Tratamiento que se le da a la seguridad para evitar divulgación y transferencias a personal no autorizado.

CUSTODIO: Responsable de un bien, elemento o activo que pone a disposición la empresa para sus labores.

DISPONBILIDAD: Consulta continua de la información sin afectar las actividades de las organizaciones cuando se requiere.

ESTANDAR: Referente que sirve como punto de partida para adaptar a una determinada función.

IEC: Comisión Electrónica Internacional. Organización de normalización en los campos eléctrico, electrónico y de tecnologías relacionadas.

INCIDENTES: Suceso que no se espera que ocurra y puede afectar las condiciones de seguridad o actividades en las organizaciones.

INTEGRIDAD: Almacenamiento de la información sin temor a ser manipulada por individuos no autorizados para tal fin.

[1] WILLIAMS, Lea. AXELOS. GLOBAL BEST PRACTICE. ITIL 4 Foundation. [Sitio web]. 2019. [Consulta: 15 septiembre de 2021]. Disponible en: https://www.axelos.com/welcome-to-itil-4

INFORMACIÓN: Información que se generar al interior de una entidad para ser compartida o divulgada teniendo en cuenta lo permisos de acceso y modificación.

INTRUSIÓN: Acceso no autorizado en que pone en riesgo la continuidad del negocio.

INVENTARIO: Recopilación de información acerca de activos, dispositivos o cualquier elemento que haga parte de los bienes de una organización.

ISO: Organización Internacional de Estandarización. Sistema de normalización internacional para productos de áreas diversas.

ITIL: Guía sobre mejores prácticas para la gestión de servicios TI.

MEDIO DE ALMACENAMIENTO: Medio o mecanismo en donde se resguarda la información fuera de su ubicación inicial.

NORMA: medio que se imparte para la correcta realización de una acción o actividad.

ORGANIZACIÓN: Cualquier entidad, institución o agrupación, que haga uso de sistemas informáticos para alcanzar sus objetivos trazados.

PRÁCTICA: Herramientas que sirven de guía para cumplir objetivos.

REGISTRO: Acontecimientos documentados sobre resultados de las actividades realizadas.

RIESGO: Situación que pone en alerta dependiendo de su consecuencia a un activo de la información.

SEGURIDAD: Garantía de que se protege con eficacia la información.

SERVICIO: Realización de una determinada actividad apoyada en recursos y personas.

SoA: Declaración de aplicabilidad usualmente para seleccionar los controles que están presentes o se pueden aplicar en una organización.

SGSI: Sistema de gestión de seguridad de la información, para monitorear, gestionar o administrar los objetivos propuestos de la organización evitando el riesgo de la información y sus activos.

SISTEMA INOFORMACIÓN: Sistema de información que permite realizar consultas

o acceso dependiendo el rol y permisos del usuario.

POLÍTICAS: Lineamientos que permiten establecer las condiciones que se deben tener en cuenta en el tratamiento de la información.

PYME: Pequeña y mediana empresa.

PROCESOS: Serie de pasos o actividades que se realizan para cumplir un objetivo determinado.

RESUMEN

La empresa Grupo Confeccionistas, fundada en el año 1991, desde sus inicios se ha enfocado a la confección de prendas para los almacenes ONLY, entres sus diseños más destacados, se encuentran las prendas para bebe, diseños de camisetas, ropa interior de dama y hombre, y adicionalmente la elaboración por campañas y temporadas en el área estudiantil para la elaboración de uniformes de colegio.

En la actualidad la empresa no tiene un análisis de los procesos que administra destacándose los aplicativos de SIIGO, PCP, AKKUMARK. No ha definido un alcance en la gestión de TI (Tecnologías de la Información), las políticas de seguridad son escasas y no proporcionan confiabilidad en la seguridad y análisis de la información, el inventario de activos se encuentra incompleto, desactualizado y carece de una asignación, no se ha identificado y realizado plenamente una gestión de riesgos que están presentes en la empresa.

Adicionalmente no se rigen por ningún marco ni estándar que permita una articulación entre el Gobierno Corporativo y la Gobernanza TI (Tecnologías de la Información).

Al diseñar un SGSI (Sistema de Gestión de Seguridad de la Información) se logró una gestión y administración de los objetivos propuestos de la empresa, de modo que se evitaron los riesgos en los activos de información que se presentaban en la empresa Grupo Confeccionistas, se identificaron las amenazas a partir de los objetivos propuestos, principalmente a través del análisis de riesgos y la respectiva evaluación para fomentar la integridad, disponibilidad y confiabilidad por medio del ciclo de gestión PHVA, donde se analizó el contexto de la organización que permitieron determinar los requisitos tanto internos como externos para el diseño de la fase planear del SGSI, a partir de las políticas y controles que se establecieron para dar continuidad a posteriores fases del diseño, de acuerdo con el interés de la gerencia para optimizar los procesos y establecer mecanismos de seguridad y protección en el tratamiento de los activos de información.

ABSTRACT

The Grupo Confeccionistas company, founded in 1991, since its inception has focused on making garments for ONLY stores, among its most outstanding designs are baby clothes, t-shit designs, women´s, and men´s underwear, and additionally the elaboration by campaigns and seasons in the student's area for the elaboration of school uniforms.

Currently the company does not have an analysis of the process it manages, highlighting the applications of SIIGO, PCP, AKKUMARK. It has not defined a scope in IT management, the security policies are scarce and do not provide reliability in the security and analysis of the information, the asset inventory is incomplete, out of date and lacks an allocation, it has not been identified and fully performed risk management that are present in the company.

Additionally, they are not governed by any framework or standard that allows an articulation between Corporate Governance and IT Governance.

When designing an ISMS (Information Security Management System), monitoring, management, and administration of the proposed objectives of the company was achieved, so that risks in the information assets that were presented in the company Grupo Confeccionistas were avoided, threats were identified based on the proposed objectives, mainly through risk analysis and the identification of information assets, an evaluation of risks and processes was carried out to promote integrity, availability and reliability through the cycle of PHVA management, where the context of the organization was analyzed that allowed determining both internal and external requirements for the design of the planning phase of the ISMS, based on the policies and controls that were established to give continuity to subsequent phases of the design, in accordance with the interest of management to optimize process and establish security and protection mechanisms in and I treatment of information assets.

INTRODUCCIÓN

Para elaborar el presente proyecto aplicado se toma y evalúa exhaustivamente la conformación y el estado en que se encuentra la seguridad en la compañía Grupo Confeccionistas, con la finalidad de establecer y gestionar eficazmente los activos de información garantizando que los procesos internos se ejecuten con la suficiente confianza en cada una de sus actividades por parte de los funcionarios.

Según Fernández[2], en América Latina se presentan brechas de seguridad específicamente en la pérdida de información, debido a que un 38% de las organizaciones no cuenta con unas políticas de seguridad definidas o si las hay los empleados las desconocen, este caso se presenta principalmente en la PYMES (pequeñas y medianas empresas), de acuerdo con datos revelados por Kaspersky.

Hoy es necesario que las entidades sin que interfiera su tamaño se protejan de posibles ataques siendo necesario y esencial que se alineen con sus colaboradores, proveedores y las partes interesadas, para generar conciencia por medio de capacitación y el continuo tratamiento de riesgos, vulnerabilidades y actividades.

Existen ciertas medidas que las PYMES pueden implementar a bajo costo para que eviten ser víctima de la ciberdelincuencia, donde se debe tener en cuenta que la solución que se elija sea eficiente, de fácil configuración y que no signifiquen grandes conocimientos técnicos por parte de los usuarios finales.

Al diseñar e implementar un SGSI en la empresa, se busca la mitigación de los riesgos, amenazas y vulnerabilidades que afectan las PYMES en el país, y que ocasionan un cierre parcial o total de sus actividades debido a los impactos que generan un ataque o intrusión cuando no es subsanada a tiempo.

La empresa se creó en el año de 1991, por emprendedores que quería hacer de la confección en Colombia una nueva tendencia y generar empleos para contribuir al desarrollo económico del país a través del sector privado.

En sus inicios la empresa carecía de una estandarización y la ejecución de una metodología que ofreciera una gestión integral en sus procesos de información y seguridad en cada una de las áreas de la empresa, produciéndose pérdida de información, incumplimiento en temas legales concernientes a la tics, sin embargo a raíz de estos sucesos se plantea a la dirección y gerencia de la empresa, la

[2] FERNÁNDEZ, Andrea. Pymes y ciberseguridad: ¿por qué instruir a los empleados es la inversión menos costosa? [Sitio web]. Revista Economía. 2020. [Consulta 2 de octubre de 2021]. Disponible en: https://www.revistaeconomia.com/pymes-y-ciberseguridad-por-que-instruir-a-los-empleados-es-la-inversion-menos-costosa-2/

elaboración de un SGSI que sea de utilidad para la empresa y que permita su gestión, partiendo de la documentación actual y en base a ella crear mejoría en el ámbito de la seguridad definiendo controles y políticas acertados que subsanen los riesgos presentes y que garanticen que la información se encuentre alineada con los pilares de la seguridad en cuanto integridad, disponibilidad y confiabilidad.

Para llevar a cabo este planteamiento se identificará el estado y evaluación de los activos de la empresa y de esta manera tener un inventario actualizado reconociendo los riesgos a los que están expuestos, para posteriormente diseñar a través del SGSI las políticas, controles y procesos en base a la norma ISO/IEC 27001:2013, donde se tendrán en cuentas las debilidades encontradas en el análisis que se realizará.

Finalmente se establecen las medidas y responsabilidades frente a la seguridad de la información donde se prioriza el compromiso de cada uno de los funcionarios, proveedores, colaboradores, gerencia y cada una de las personas que interna o externamente se involucre con la empresa para ofrecer las recomendaciones necesarios para el manejo adecuado de la información y su seguridad.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Grupo Confecciones, ubicado en Bogotá, en la localidad de Engativá, actualmente no cuenta con una estandarización, marco de referencia o sistema de gestión que brinde ciberseguridad y organización en la ejecución de sus actividades y procesos, por lo que no garantiza una fiabilidad a posibles intrusiones, daños informáticos, extravío de información y accesos remotos.

La empresa se ha enfocado en sus actividades propias del negocio y no en los procesos internos y la generación de un plan para tratar los riesgos, que permita la confidencialidad para que no se presente fugas de información y alteración de sus procedimientos de negocio, previniendo la afectación de sus labores por eventuales fallas en los activos y dispositivos de la organización y la integridad para reducir los incidentes que se puedan ocasionar por filtraciones y errores.

No cuenta con la debida documentación sobre sus procesos que defina las normas, políticas y procedimientos de seguridad que se deben regir y una adecuada formación y concientización por parte del personal implicado en la empresa donde se establezca la importancia de los objetivos trazados de acuerdo con su perfil ocupacional dentro de la empresa.

La dirección de la empresa no está alineada con la Gobernanza TI, no existe comunicación fluida para que se desarrollen estrategias, planes y prácticas para la gestionar la seguridad y los procesos.

Finalmente, no hay definido un documento de declaración de aplicabilidad (SoA[3]), para seleccionar los respectivos controles para la mitigación de riesgos que se han identificado al interior de la empresa.

Estas falencias en cuanto a seguridad y poca organización se toma desde la experiencia de laborar en la empresa como parte del área de sistemas donde se han identificado amenazas, vulnerabilidades, escasos modelos y políticas de seguridad para la protección en la información y procesos.

Al presentarse el SGSI a la empresa Grupo confeccionistas se pretende brindar a la gerencia disponer de una herramienta para dirigir y controlar la seguridad de la

[3] "Documento que enlista los controles establecidos en el anexo A del estándar ISO/IEC 27001:2013 (conjunto de 114 controles agrupados en 35 objetivos de control)". WELIVESECURITY. ¿Qué es una declaración de aplicabilidad (SoA) y para qué sirve? [sitio web]. 2015. [consulta: 2 de octubre de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

información, donde se podrán incluir normas internacionales como la ISO/IEC27001:2013, que hace énfasis en la protección de la información a través del ciclo de Deming Plan-Do-Check-Act, donde se pretende una mejora continua sobre los procesos y seguridad dentro de las organizaciones, PYMES o entidades.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo un Sistema de Gestión de Seguridad de la Información - SGSI permite fortalecer la seguridad de la información a partir de la fase planear al interior de la empresa grupo confeccionistas?

2 JUSTIFICACIÓN

El auge de la tecnología y la era digital han desencadenado nuevos retos para las organizaciones en la protección de sus activos, procesos e información que pueden ser vulneradas por delincuentes informáticos y afectar la información, afirma Gómez[4], a través de mecanismos de intrusión como lo pueden ser el Phishing, Ransonware, Virus maliciosos, Ingeniería Social, entre otros.

Según semic[5], contar con un sistema que permita controlar los riesgos y vulnerabilidades de la información, garantiza proteger efectivamente los activos de información de la entidad, al implementarse un SGSI se detectan los ataques y se tiene una respuesta oportuna, rápida y eficaz que minimicen los efectos ocasionados por la alteración de la seguridad.

Al no contar con un SGSI de acuerdo con ISO27000[6] se pueden presentar los siguientes inconvenientes:

- Afectación en áreas contables y financieras de una empresa.
- La productividad disminuirá circunstancialmente.
- La imagen de la empresa puede verse comprometida seriamente.
- Se perderían potenciales oportunidades de nuevas líneas de negocio.
- Se pueden presentar problemas legales.

El CCIT[7], aclara que cuando una PYME es objeto de un ciberataque importante el 60% de las PYMES no puede sostener su negocio pasados seis meses, debido a las afectaciones que conlleva y el impacto negativo en su productividad, asuntos legales y cumplimiento.

Intenco[8], menciona que las compañías que no dispongan de un SGSI se encuentran más vulnerables a ser víctimas de este tipo de ataques, como ocurre en la empresa

---

[4] GÓMEZ VIEITES Álvaro. Seguridad en equipos informáticos [En Línea]. Madrid: RA-MA Editorial, 2015. p.p 13-14. [consultado 16 abril 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/62466?page=13

[5] SEMIC. Effective IT Solutions. ¿Por qué necesitamos un SGSI? [Sitio web]. Madrid. [Consulta el 27 de mayo de 2021]. Disponible en: https://www.semic.es/es/content/por-que-necesitamos-un-sgsi

[6] ISO27000.es. SGSI. [sitio web]. 2020. [consulta: 02 octubre de 2021]. Disponible en: https://www.iso27000.es/sgsi.html

[7] Ibid., p. 31.

[8] INTENCO. Instituto Nacional de Tecnologías de la Comunicación. Implantación de un SGSI en la empresa. [En Línea]. 2020. [Consulta: 10 de agosto de 2021]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

Grupo Confeccionistas por no contar gestionar la protección de la información asegurando la integridad, confidencialidad y disponibilidad, aunque existen otras normas, Frameworks y Estándares, lo que busca el SGSI es una simplificación a través de un diseño, implantación y el mantenimiento de los procesos para disminuir los riesgos.

Se empleará como marco normativo, UNE-EN ISO/IEC 27001:2013[9] que permite la identificación, control y tratamiento de riesgos y vulnerabilidades a partir de buenas prácticas estandarizadas y confiabilidad en un sistema reconocido para fomentar diferentes estrategias para la evaluación y administración de los activos de información.

[9] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información. NTC-ISO-IEC 27001:2013. Bogotá D.C.: El Instituto, 2015. 33 p.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar un Sistema de Gestión de Seguridad de la información – SGSI en su fase de planear a partir de la norma ISO/IEC 27001:2013, que optimice la protección de los activos y la información de la empresa grupo confeccionistas.

3.2 OBJETIVOS ESPECÍFICOS

- Evaluar los activos de información mediante la aplicación de una metodología para el análisis y gestión de riesgos de la empresa grupo confeccionistas, que permita identificar vulnerabilidades y amenazas presentes.
- Proponer un documento de declaración de aplicabilidad a partir del informe de análisis de riesgos para establecer los dominios y controles de seguridad que se deben aplicar en la empresa.
- Diseñar las políticas y controles de seguridad mediante la adopción de buenas prácticas que permitan reducir los riesgos en los activos de información.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Seguridad Digital**.** De acuerdo con Escrivá[10], cuando se habla de Ciberseguridad se reconoce que es el área específica que se encarga de gestionar procesos, políticas, lineamientos, parámetros entre otros para proteger la infraestructura tanto a nivel del hardware como el software de una organización incluyendo los usuarios que hacen parte de esta.

Arroyo, Gayoso y Hernández[11], afirman que la también llamada ciberseguridad es el área específica que se encarga de gestionar procesos, políticas, lineamientos, parámetros entre otros para proteger la infraestructura tanto a nivel de hardware como de software de una organización incluyendo los usuarios que hacen parte de esta, se deben tener en cuenta los tres pilares de la seguridad integridad, confiabilidad y disponibilidad, con estas tres bases se puede establecer los aspectos y las mejores prácticas para el resguardo de la información así como emplear metodologías nacionales e internacionales con el propósito de mantener, crear y administrar un entorno digital seguro.

4.1.2 Seguridad Informática**.** Según Gómez[12], son todos aquellos aspectos, fases, técnicas y normas que son utilizadas para prohibir el acceso a redes de datos, sistemas de cómputo y cualquier dispositivo que se relacione con las tics (Tecnologías de la Información y la comunicación), donde también se desarrollen esquemas que empleen estándares y auditorias, para evitar que sean vulneradas y que el personal no autorizado pueda ocasionar fallas e interrupciones., también Gómez[13], afirma que la seguridad es la protección de datos evitando así que delincuentes informáticos se apropien de ella, realicen modificaciones y generen cambios en ella, a través de técnicas y estudios de pentest e ingeniería social para su consulta y posterior afectación.

---

[10] ESCRIVÁ-GASCO, Gema. Unidad 1 -Introducción a la Seguridad Informática. En: Seguridad Informática. España: 2016. p. 8. Consultado el 17 de abril de 2021 a las 06:20 p.m. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edselb&AN=edselb.3217398&lang=es&site=eds-live&scope=site

[11] ARROYO GUARDEÑO, David; GOYOSO MARTÍNEZ, Víctor y HERNÁNDEZ ENCIMAS, Luis. Ciberseguridad. [En Línea]. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas, 2020 [consultado 04 Oct 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/172144?page=137

[12] GÓMEZ VIEITES Álvaro. Seguridad en equipos informáticos [En Línea]. Madrid: RA-MA Editorial, 2015. p.p 13-14. [consultado 16 abril 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/62466?page=13

[13] Ibid., p. 14.

4.1.2 Norma ISO/IEC 27001-2013**.** GB[14], afirma que los estándares de seguridad ISO, COBIT e ITIL permiten emplear las mejores prácticas en cuanto a la seguridad de la información para la Gestión de la Información (SGSI), el estándar ISO/IEC 27000 es el principal y el que contiene una visión general de los términos y definiciones del ciclo PDVA logrando así una mejora continua.

La norma se encarga de implantar los SGSI, conllevando así la mejora continua, es una certificación que las organizaciones deben adquirir para demostrar que la seguridad de la información es un tema confiable GB[15] y que ha adoptado una serie de prácticas donde los riesgos son mínimos ofreciendo así a sus clientes confiabilidad y continuidad del negocio.

4.1.3 Norma ISO/IEC 27002:2013**.** A través de principios y directrices permite mejorar, crear e implementar la gestión de seguridad en una entidad, por medio de buenas prácticas llevar a cabo una serie de controles, para fomentar el análisis y valoración de los riesgos de la organización.

4.1.4 COBIT. De acuerdo con Rojas[16], es una herramienta de Gobierno TI, que gestiona los recursos tecnológicos a través de procesos para lograr la continuidad del negocio y que aspectos se deben seguir con la finalidad de una adecuada prestación de servicios, donde los usuarios son el eje fundamental y se compone de la gerencia, usuarios finales, auditores, personal TI.

4.1.5 ITIL**.** Según GB[17], es una biblioteca que proporcionas diferentes componentes estandarizados para la ejecución de prácticas y la prestación de servicios TI, se abordan diferentes temáticas con el objetivo principal de centrarse en elegir el mejor camino en la gestión de servicios y como aprovechar los recursos tecnológicos de manera eficaz, siguiendo una serie de pautas, en los modelos de operación de las organizaciones para la creación y entrega de los servicios de cada organización. Sus bases fundamentales son el SVS (Sistema de Valor del Servicio) y el modelo de las cuatro dimensiones las cuales a través de la organización y personas, información y tecnología, socios y proveedores, procesos y flujo de valor se produzca un equilibrio.

---

[14] GB Advisors. ISO, COBIT e ITIL: ¿Cuál de estas normas y estándares internacionales te conviene más para potenciar tu empresa? Madrid. 6 de abril de 2018. [consultado el 16 de abril de 2021]. Disponible en: https://www.gb-advisors.com/es/normas-y-estandares-internacionales/

[15] Ibid., p. 1.

[16] ROJAS CÓRSICO Ivana Soledad. Trabajo de auditoría normas COBIT [En Línea]. Santa Fe, Argentina: El Cid Editor | apuntes, 2009. p.5. [consultado el 16 abril de 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/28995?page=5

[17] GB Advisors. Op. Cit, p. 10.

4.1.6 NIST**.** Afirma NIST[18], A través de varios aportes y contribuciones desde diferentes sectores, este marco se encarga de proporcionar a las (IC) infraestructuras críticas, sin interesar su actividad principal, que adopten un modelo de ciberseguridad tanto a propietarios como operadores que voluntariamente quiere seguir este modelo de recomendaciones de cómo identificar, evaluar los riesgos cibernéticos expuestos en las organizaciones a través de unos principios y buenas prácticas de gestión de riesgos que impiden alcanzar de manera adecuada la prestación de sus servicios, esto sin imponer medidas o requisitos adicionales a las empresas. A través de un perfil actual se evalúan las condiciones actuales y si se está alcanzando las categorías o subcategorías del marco de la seguridad cibernética de la organización y a partir de esta evaluación se determinan un perfil objetivo que reemplace los mecanismos implementados para incorporar nuevas medidas que permitan el aseguramiento de la información y que contribuyan al mejoramiento de los procesos de seguridad y reducir los riesgos.

El marco del NIST[19] se compone de tres ejes fundamentales:

1. Núcleo: Conjunto de actividades relacionadas directamente con la Seguridad Informática, resultado y referencias, que son aplicables y que se presentan en similitud en las organizaciones y sus IC. Consta de 4 elementos:
   Funciones, Categorías, Subcategorías y Referencias Informativas. Según NIST[20] se describen de la siguiente manera:

- Funciones: A través Identificar (ID= Desarrollar comprensión organizacional), Proteger (PR= Desarrollar e implementar medidas), Detectar (DE= Desarrollar e implementar actividades), Responder (RS= Tomar medidas) Recuperar (RC= Mantener y restablecer), se logra una planificación de las actividades de seguridad cibernéticas para un menor impacto y una mayor prestación en los servicios, que alineadas ofrecen un alto nivel de ciclo de vida para el tratamiento de riesgos que se especifican en el apartado definidos por el NIST[21]
- Categorías: Subdivisiones de una función ligados a las actividades particulares.
- Subcategorías: Desglose de una categoría en función de resultados trazados.

[18] INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍAS. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. [En línea]. En NIST. (2018). p.p 1-44. Consultado el 26 de abril de 2021. Disponible en: https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

[19] Ibid. p. 15.
[20] Ibid. p. 15.
[21] Ibid., p. 15.

- Referencias Informativas: Resultados de cada Subcategoría en conjunto de las actividades trazadas.

2. Perfil del Marco NIST[22]: En este ítem se relacionan los perfiles Individuales en las Organizaciones, alineando su misión y prestación de servicios en base a la seguridad Cibernética, permite realizar autoevaluaciones y la comunicación en la organización o con otras. Además, permite describir el estado actual de las actividades de la seguridad cibernética o el que se pretende alcanzar.

3. Niveles de Implementación NIST[23]: Sistema a través del cual las organizaciones enfocan su visión para el tratamiento del riesgo de la seguridad cibernética, consiente de los riegos y amenazas, repetibles y adaptables. Apoyan las determinaciones que la organización acoge acerca de los riesgos y en qué área se debe centrar por su prioridad.

4.1.7 Sistema de Gestión de Seguridad de la Información**.** De acuerdo con Fernández[24], gestión hace referencia a lograr los objetivos por medio de los recursos de los que dispone una organización, al implementarse un Sistema de Gestión se debe tener claridad sobre lo que se pretende, cual es la finalidad, la consecución de los objetivos en cuanto a seguridad que se quiere alcanzar, teniendo en cuenta los riesgos asumibles para su cometido.

Al implementarse el SGSI se pude realizar en base a estándares reconocidos o de forma personalizada, aunque funciona no puede ser verificable, mientras que una implementación en base a un estándar debe cumplir una serie de requisitos que por ende sean verificables como es el caso de ISO/IEC 27001:2013.

4.1.8 Pasos para implementar el SGSI**.** Basándonos en la norma ISO 27001, y Fernández[25], a través del PHVA, se debe considerar:

[22] Ibid., p. 15.
[23] Ibid., p. 15.
[24] GÓMEZ FERNÁNDEZ Luis. y FERNÁNDEZ RIVERO Pedro. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. [En Línea]. Madrid: AENOR - Asociación Española de Normalización y Certificación, 2018 [consultado 20 May 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624?page=89

[25] Ibid., p. 96.

Tabla 1. Fases PHVA SGSI

Fase	Descripción
Plan	• Política, alcance y objetivos SGSI. • Administración del riesgo (analizar, estimar, evaluar, aceptar). • Acogimiento por parte de las directivas.
Do	• Implementación de políticas y controles. • Actividades formativas. • Medir eficacia y gestión de incidencias.
Check	• Ejecutar medición y eficacia de los controles. • Gestionar incidencias. • Auditoría Interna. • Revisión del SGSI por las directivas.
Act	• Mejora. • Actividades preventivas y correctivas.

Fuente: Autoría propia basado en GÓMEZ FERNÁNDEZ. Ibid., p. 96.

4.1.9 Desarrollo de las fases

4.1.9.1 Diagnóstico. Se toma en consideración el estado actual de la empresa, a través de la identificación de los activos, documentación y estrategias previamente planteadas que permiten llevar a cabo tareas y actividades de la empresa alcanzando los objetivos estratégicos planteados por la dirección y previendo los riesgos que se asocian a los activos diagnosticados.

4.1.9.2 Planificación. Para la fase de planificación se tendrán en cuenta los siguientes apartes:

- Grupo de trabajo. Donde se involucren funcionarios que conozcan y entiendan los procesos de la empresa, áreas específicas y tareas ejecutadas.
- Plan de trabajo. Elaboración de una metodología que permita involucrar un equipo de trabajo para conseguir en el tiempo determinado la identificación de actividades propias de la empresa.

4.1.9.3 Implementación. Se verifica que los objetivos planteados se hayan realizado y se compara lo que se proyectó y lo que se alcanzó generando de esta manera las brechas existentes.

4.1.9.4 Monitoreo. Evaluar el diseño del SGSI, donde se debe tener en cuenta los resultados y las posibles mejoras para su ejecución.

4.1.10 Metodología**.** Implementar una metodología que permita identificar y clasificar los peligros para estimar los riesgos, para el proyecto actual, se tomará como base la metodología Magerit 3.0 que contempla un análisis de las amenazas físicas y lógicas.

4.1.10.1 Objetivos Magerit[26]

- Concientizar sobre la existencia de riesgos a los directamente implicados con los sistemas de información para su oportuno tratamiento y análisis.
- Emplear un método eficaz para la mitigación de riesgos.
- Recomendar estrategias para que los riegos sean controlables.
- Encaminar a la entidad para el proceso de certificación y prevención según sus necesidades y condiciones.
- Un punto a favor de Magerit es que después de realizado un análisis de riesgos y de presentarse a la dirección se pude justificar las decisiones a tomar con fundamento.

4.2 METODOLOGÍA MAGERIT 3[27]

4.2.1 Elementos que intervienen en el análisis. El personal encargado de ejecutar la metodología debe considerar los siguientes seis elementos básicos para su correcto uso.

Ilustración 1. Elementos análisis de riesgos.

Fuente: MAGERIT – versión 3.0. Ibid., p.22.

[26] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. 2012. [en línea]. Madrid. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. [Consulta: 23 de junio de 2021]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[27] Ibíd., p.22.

- Activos

Define Magerit[28], que son todos aquellos recursos que se hacen parte de un sistema cuya finalidad es proporcionar las acciones para ejecutar actividades y tareas sobre el sistema y los objetivos enmarcados por la dirección y que son susceptibles a los ataques generados por su utilización.

También hacen parte de los activos:

- Datos
- Servicios
- Software
- Hardware
- Soporte de información
- Equipamiento auxiliar
- Redes
- Instalaciones
- Personas

- Amenazas

MAGERIT[29], afirma que se relacionan directamente con las afectaciones o indisponibilidad que se presentan en los activos que causan su daño o interrupción del servicio. A través de la degradación se establece si es perjudicial y la frecuencia de ocurrencia de la amenaza que determina la vulnerabilidad del activo.

- Vulnerabilidades.

Posibilidad de que se presente una amenaza a un activo determinado.

- Impactos

Se genera el daño recibido sobre el activo que presentan una determinada amenaza y al conocer el valor del activo calcular su impacto no generaría mayor inconveniente.

- Riesgo

Probabilidad de ocurrencia de una potencial amenaza, al conocer el riesgo la frecuencia se calcula sin inconveniente.

[28] Ibíd., p.22.
[29] Ibid., p. 24

4.2.2 Ejecución de la Metodología. Por medio de la metodología Magerit[30], se lleva a cabo el análisis de riesgos siguiendo esta aserie de pasos.

- Identificación

Se realiza una clasificación de los activos de la organización para su descripción y los servicios que permite desarrollar.

- Valor

De acuerdo con la descripción de los activos y su importancia en la organización se evalúan teniendo en cuenta los pilares que hacen referencia a la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad.

- Considerar las vulnerabilidades del sistema de orden:

    - Natural
    - Hardware y software
    - Medios o dispositivos
    - Factor humano

- Considerar las amenazas del sistema de origen:

    - Natural
    - Del entorno
    - Fallas de aplicaciones
    - Causas por personas
    - Sistemas de información y comunicación

- Valoración del riesgo

En el libro1 de Magerit[31], indican que el riesgo se trata a partir de:

    - Ocurrencia de que suceda o sea probable.
    - Se origina en base a la probabilidad y el impacto.

Zonas de ocurrencia de riesgos por colores:

    - Zona 1 – Rojo. Muy probables y de alto impacto.
    - Zona 2 –Naranja. Improbables y de impacto medio, situaciones muy probables, pero con bajo impacto.

[30] Ibid., p. 27
[31] Ibid., p. 30.

- Zona 3 – Amarillo. Improbables de bajo impacto.
- Zona 4 – Verde. Improbables de muy alto impacto.

4.2.3 Identificación. Valoración de activos en base a su importancia en los procesos y actividades de la empresa.

En la tabla 2, se describen los diferentes parámetros que se emplearon para la identificación de cada uno de los activos presentes en la empresa Grupo Confeccionistas.

Tabla 2. Identificación y clasificación de activos

DETALLES	DESCRIPCIÓN
Ref. ACTIVO	Identificación
ÁREA	Ubicación del activo.
PRODUCTO	Servicio prestado.
ACTIVO DE INFORMACIÓN	Detalle del activo.
DESCRIPCIÓN	Descripción del activo.
TIPO	Digital o Física
TIPO DE CONTAINER	Descripción del contenedor.
CONTAINER	Ubicación de la información.
RESPONSABLE	Encargado del activo.
CUSTODIO	Poseedor del activo.
USERS	Individuo que emplea el activo.
CLASIFICACIÓN ACTIVOS	
CLASIFICACIÓN ACTIVO	Descripción y parametrización del activo, teniendo en cuenta las siguientes connotaciones. (Secreta, Confidencial, Uso Interno, Público)

Fuente: Autoría propia. Basado en: JARA PEREZ, Ibid., p.30.

La tabla 3, explica los criterios de clasificación, de acuerdo con Jara[32], en base a los tres pilares de la seguridad informática: disponibilidad, integridad y confidencialidad, para evaluar el impacto y afectación en cada uno de los activos

[32] Autoría propia. Basado en: JARA PEREZ, Diana Fernanda. Valoración y plan de tratamiento de riesgos de seguridad de la información para los procesos incluidos en el alcance del SGSI del cliente TGE de la empresa Assurance Controltech. [en línea]. Proyecto de pasantía. Universidad Distrital Francisco José de Caldas. 2017. [Consultado el 28 de mayo de 2021]. Disponible en: https://repository.udistrital.edu.co/bitstream/handle/11349/6492/JaraPerezDianaFernanda2017.pdf?sequence=1&isAllowed=y

Tabla 3. Criterios de clasificación.

DIMENSIONES	VALOR	DESCRIPCIÓN
DISPONIBILIDAD	3	• Información muy sensible, causaría un muy alto impacto en la compañía. • Riesgo de continuidad del negocio • Solo un grupo mínimo autorizado y muy específico.
INTEGRIDAD	2	• Información sensible, causaría un leve impacto en la compañía. • Solo personal autorizado y especifico.
CONFIDENCIALIDAD	1	• Información para los procesos internos. • Solo de conocimiento interno si se va a exteriorizar contar con la justificación necesaria. • No causaría ningún impacto en la compañía
No aplicable	0	• Información para terceros. • No hay restricciones.

Fuente: Autoría propia. Basado en: JARA PEREZ, Ibid., p.30.

4.3 MARCO CONCEPTUAL

4.3.1 Principios de la Seguridad Informática. Son los principios básicos que se deben tener en cuenta para determinar si un sistema es seguro o no lo es. Estos tres pilares son: Integridad, confidencialidad y disponibilidad. Según define Escrivá[33] se encuentra que:

4.3.1.1 Integridad. Este pilar consiste en que el acceso, manipulación y configuraciones a los sistemas informáticos solo debe ser realizados por el personal autorizado, es decir no contempla que personas fuera de los admitidos ocasionen algún cambio porque ya se vería una afectación en el sistema, un ejemplo es cuando un integrante del grupo comercial de una organización modifica las bases de datos de producción sin ser este su rol y funciones y genera un impacto en el servicio.

4.3.1.2 Confidencialidad. Es el manejo y tratamiento que se le da a la información, consiste en que personas no autorizadas realicen consultas de diferentes temas sin estar autorizados, por ejemplo, en una organización cuando algún funcionario por descuido deja su correo abierto y otra persona empieza a indagar sobre los mensajes e información que es privada y no es de su interés.

[33] ESCRIVÁ-GASCO. Op. cit., p. 14.

4.3.1.3 Disponibilidad. El tercer pilar consiste en que la información de un sistema siempre este cuando se necesite consultar, por ejemplo, cuando el área tesorería de una organización necesita acceder a través de la Internet a realzar pagos y la red se encuentra sin acceso, esto es una afectación y una indisponibilidad que puede provocar retrasos en el desarrollo de los servicios de la entidad.

4.3.2 UIT-T X.800. De acuerdo con ITU[34], es una recomendación del (CCITT), hace parte del ITU. Aprobada mediante resolución N° 2 el 22 de marzo de 1991 en Ginebra. Cuya finalidad es la interconexión entre distintos dispositivos que conforman una red, asegurando la información intercambiada, la protección de las comunicaciones, adoptando una serie de medidas y recomendaciones para la interconexión de sistemas abiertos seguros sin exponer la integridad de la información.

Los servicios de seguridad básicos que se enmarcan en esta recomendación satisfacen las políticas de seguridad y las exigencias de los usuarios.

4.3.3 Autenticación. Se presenta cuando se corrobora la validez de un usuario, proceso o sistema origen con la entidad destino. Se presentan las siguientes autenticaciones a partir de cada entidad.

Autenticación de entidad cuando se transfieren datos de una conexión y se confirma que el solicitante este autorizado y que no está tratando de acceder sin permisos comprobando en tiempo real su identidad.

4.3.4 Autenticación del origen de datos. Como su nombre lo indica confirma la fuente inicial desde donde se transfiere la información, aunque no es un mecanismo que proporciono un sistema de seguridad confiable.

4.3.5 Control de acceso. Se presenta cuando en los Sistemas de Información Seguras (ISA), los recursos no están autorizados para su acceso encontrándose cualquier elemento, sistema o recurso que haga parte de la red para la transferencia de información.

4.3.6 Confidencialidad de datos. Este servicio se encarga de proporcionar protección a los datos de accesos no autorizados, presentando las siguientes connotaciones:

[34] X.800: Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT. [En línea]. Ginebra, 1991: ITU Unión Internacional de Telecomunicaciones. [Fecha de consulta: 12 de mayo de 2005]. Disponible en: https://www.itu.int/rec/T-REC-X.800-199103-I/es

4.3.6.1 Confidencialidad de los datos en modo con conexión: Protege a todos los datos de todas las peticiones, ocasionando muchas veces denegación de una fuente autorizada.

4.3.6.2 Confidencialidad de los datos en modo sin conexión: Protege a todos los datos de todas las peticiones, inclusive sin encontrarse accesibles a nivel de red.

4.3.6.3 Confidencialidad de Campos seleccionados: Protege datos específicos de usuario en una conexión sin que la conexión este activa.

4.3.6.4 Confidencialidad del flujo de tráfico: Protege la información al encontrarse en constantes accesos, movimientos y disponibilidad.

4.3.7 Integridad de los datos. Proporciona y asegurar que los datos no sufran alteraciones al transferirse o al estar disponibles en una conexión, detectando que se produzcan y dupliquen los datos,

Encontrándose las siguientes modalidades.

4.3.7.1 Integración en modo con conexión con recuperación. Se encarga de que la información de usuario no se altere o copie, protegiéndola y recuperándola en caso de pérdida.

4.3.7.2 Integración en modo con conexión con recuperación. Se encarga de que la información de usuario no se altere o copie, protegiéndola, pero no la recupera en caso de pérdida.

4.3.7.3 Integridad de campos seleccionados en modo conexión. Protege la información que se determine y alerta sin esta ha sido transformada o alterada.

4.3.7.4 Integridad en modo sin conexión. Proporciona seguridad en sola una instancia de recuperación cuando no haya conexión y alerta limitadamente si está en riesgo.

4.3.7.5 Integridad de campos seleccionados en modo sin conexión. Proporciona seguridad en sola una instancia de recuperación cuando no haya conexión y alerta si está en riesgo.

4.3.8 No repudio. Se presenta de las siguientes maneras:

4.3.8.1 No repudio con prueba de origen. Se informa al destino sobre el origen de los datos para no generar rechazo de su contenido.

4.3.8.2 No repudio con prueba de la entrega. El origen informa sobre el destino de los datos para no generar rechazo de su contenido.

4.3.9 Matriz de control de acceso

Ilustración 2. Matriz de accesos ACM

	$Objeto_1$	$Objeto_2$	$Objeto_3$	...	$Objeto_M$
$Usuario_1$	rwx	rw	rwx	...	rw
$Usuario_2$	x	r	x	...	rw
$Usuario_3$	x	rw	rwx	...	r
...	...	...	...	...	...
$Usuario_N$	x	rw	x	...	w

Fuente: Ingeniería de la Seguridad. Controles de accesos [En línea]. 2012. [consultado el 17 de mayo de 2021]. Disponible en: http://ingenieriadelaseguridad.blogspot.com/p/control-de-accesos.html

Como se evidencia en la figura 4, las matrices ACM relacionan diferentes objetos y sujetos, siendo las operaciones de los primeros sobre los segundos las determinadas como lecturas (r), escritura (w) y ejecución (x)

4.3.10 Access Control List. De acuerdo con Escrivá[35], es una herramienta que proporciona seguridad restringiendo y controlando el acceso de la red, sistemas operativos a los usuarios, las ACL se pueden basar en IP, MAC generando políticas de acceso y bloqueo, también son aplicables a nivel básico de rede en proxy, DNS, correo electrónico, etc. A través de su implementación se puede optimizar una red, permitir o denegar accesos a los equipos, no ejecución de comandos., entre otros.

[35] ESCRIVÁ-GASCO. Op. cit., p. 14.

4.4 MARCO LEGAL

Según ISOTOOLS[36], deben existir una serie de requisitos legales, seguros y reglamentarios, que contemple para la empresa para acatar las normas jurídicas de cada país sin cometer evasiones o violaciones dispuestas por la ley:

- Ley 1273 de 2009[37], "de la protección de la información y de los datos"

Se centra en evitar que se difunda sin autorización información privada y preservar integralmente a los sistemas que empleen los tics para su manipulación.

- Ley 23 de 1982[38] sobre derechos de autor.

Su objetivo es preservar íntegramente la autoría y composición, de determinado artículo, obra, escrito, etc., con el fin de mencionar un responsable de su creación sin publicar su debida obra.

- Ley 545 de 1998[39] descrita como "Convención sobre la abolición del requisito de legalización para documentos públicos extranjeros".

Proporciona una normativa para el sector cooperativo, enmarcando su importancia para el desarrollo de la Economía Nacional.

- Ley 594 de 2000[40] - Ley General de Archivos.

Permiten establecer reglas y principios para que una entidad pública o privada regulada por la ley generar y administrar una gestión de archivo de documentos adecuada.

---

[36] ISOTOOLS. ISO 270001. Cumplimiento de los requisitos legales en Seguridad de la información. [Sitio web]. Bogotá. [Consulta: 20 de mayo de 2021]. 2014. Disponible en: https://www.isotools.org/2014/12/16/iso-27001-cumplimiento-requisitos-legales-seguridad-informacion/

[37] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (enero 5 de 2009). "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". En: Diario Oficial. Enero, 2009. p. 1 – 4.

[38] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 23. (enero 28 de 1982). "sobre derechos de autor". En: Diario Oficial. Enero, 1982. p. 1-10.

[39] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 455. (11 de agosto de 1998). "convención sobre la abolición del requisito de legalización para documentos públicos extranjeros". En: Diario Oficial. Agosto 1998.

[40] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 594. (14, julio, 2000). Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. En: Diario Oficial. Julio, 2000. Nro. 44084. p. 1-9.

- Ley 527 de 1999[41], “acceso y uso de los mensajes de datos”

Se define y reglamenta el acceso y empleabilidad de los mensajes de datos, electrónico y firmas digitales, para las entidades certificadoras y otras disposiciones.

- Ley 1581 de 2012[42], “Protección de Datos Personales”.

Prohíbe la divulgación de datos personales a países que no cuenten con mecanismo de seguridad para la protección de datos, con la salvedad de que haya sido autorizado por el titular para su transferencia de información personal.

- Ley 1341 de 2009[43]. “Tecnologías de la Información y aplicación de seguridad”.

Reconocimiento por parte del estado, para el acceso, uso y apropiación de los tics, despliegue y uso eficiente de las infraestructuras, desarrollo de contenidos, protección de usuarios.

- CONPES 3701 de 2011[44] “Ciberseguridad y Ciberdefensa”

Documento constituido para aportar y posicionar al país como líder de la región en ciberseguridad y logró mitigar de manera activa los ataques de seguridad a nivel nacional.

[41] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. En: Diario Oficial. Agosto, 1999. Nro 43.673. p. 1-10.

[42] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581. (18, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Diario Oficial. Octubre, 2012. Nro. 48.587. p. 1-185.

[43] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1341. (30, julio, 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. En: Diario Oficial. Julio, 2009. Nro. 47.426. p. 1-32.

[44] DEPARTAMENTO NACIONAL DE PLANEACIÓN. [Sitio web]. Bogotá: Alta Consejería Distrital, Lineamientos de políticas para ciberseguridad y ciberdefensa, CONPES 3701 de 2011. [Consulta: 20 de mayo de 2021]. Disponible en: https://tic.bogota.gov.co/transparencia/marco-legal/normatividad/conpes-3701-2011

5 DISEÑO METODOLÓGICO

El proyecto aplicado consiste en la presentación de la fase planear de un Sistema de Gestión de la Seguridad de la Información, donde se evaluarán los sistemas y procesos de la empresa grupo confeccionistas. Tiene una metodología basada en pruebas y experimentos porque se inspeccionará exhaustivamente los sistemas de información, se revisará la documentación existente en la empresa para determinar sobre los métodos de seguridad empleados y se definirán planes de educación cibernética para asegurar el cumplimiento de las políticas de seguridad establecidas.

5.1 TIPOS DE INVESTIGACIÓN

5.1.1 Investigación exploratoria. Según Ortiz[45], este tipo de investigación es el primer paso que se debe ejecutar antes de realizar un trabajo investigativo en profundidad, donde se obtiene información relacionada con el problema de investigación.

A través de este tipo de investigación se conoce de primera instancia las situaciones e implicaciones de un problema, para determinar los aspectos más importantes para abordarlos en una investigación.

Por medio de entrevistas y observando el comportamiento dentro de la empresa, se realizó un levantamiento de datos, donde se reconocieron los mecanismos de control y seguridad que se están ejecutando al interior de la empresa.

Al ejecutar este tipo de investigación no siempre se obtienen datos exactos por lo que es necesario un estudio posterior el cual permita corroborar las primeras instancias y deducciones donde posiblemente sea necesario abrir nuevas líneas de investigación.

Algunos aspectos a tener en cuenta en este tipo de investigación son:

- Flexibilidad metodológica.
- Delimitar el problema de investigación.
- Establecer un proceso investigativo.
- Abrir nuevas líneas de investigación.

[45] WINSTON, Kimberly. Exploratory Research: Definition, Methods & Examples." [Sitio web]. 2017. Study.com. [Consulta: 5 noviembre de 2021]. Disponible en: https://study.com/academy/lesson/exploratory-research-definition-methods-examples.html.

También se debe tener en cuenta el tipo de investigación que son común entre los investigadores: La consulta a expertos del área y la revisión documental.

5.1.2 Técnicas de recolección de información: Se emplearon diferentes fuentes bibliográficas para el diseño de un Sistema de Gestión de Seguridad de la Información SGSI y en la norma ISO/IEC 270001:2013, que sirven como apoyo para determinar y sustentar la investigación realizada.

Las técnicas seleccionadas en este proyecto son: Observación, encuesta y entrevista.

Tabla 4. Técnicas de recolección de información

TÉCNICAS DE INVESTIGACIÓN	OBJETIVOS	FUENTE DE RECOLECCIÓN
Observación A través de esta técnica y como parte del personal de apoyo en las labores de sistemas al interior de la empresa, se presentan las actividades que se ejercen desde el área.	Evaluar los activos de información mediante la aplicación de una metodología para el análisis y gestión de riesgos de la empresa grupo confeccionistas, que permita identificar vulnerabilidades y amenazas presentes.	Familia normas ISO /IEC 27000-series. ISO /IEC JTC 1 / SC 27 – Técnicas de Seguridad en tecnologías de la información. Bases de datos: E Libro
Cuestionario Se realiza a través de una serie de preguntas en base a la seguridad informática, para establecer el grado de conocimiento y la posición de las partes interesadas y los funcionarios de la empresa frente a las medidas necesaria para la seguridad de la información.	Proponer un documento de declaración de aplicabilidad a partir del informe de análisis de riesgos para establecer los dominios y controles de seguridad que se deben aplicar en la empresa.	Icontec EBSCOhost Google académico Libros
Entrevista		

El proyecto se diseña para la empresa Grupo Confeccionistas S.A.S, ubicado en la ciudad de Bogotá, localidad Engativá, donde se encuentra su sede, se desarrollan todas las actividades de las áreas de producción, diseño, administrativa, etc. Muestra Se involucran de 15 a 20 personas que laboran en la empresa y que utilizan diariamente equipos de cómputo, aplicaciones, red, recursos compartidos, etc., para aplicar el cuestionario online y reconocer diferentes aspectos, además de los procesos administrativos y operativos de la empresa.	Diseñar las políticas y controles de seguridad mediante la adopción de buenas prácticas que permitan reducir los riesgos en los activos de información.	MAGERIT – versión 3.0. Libro l – Método. 2012

Fuente: Autoría propia.

6 DESARROLLO DE LOS OBJETIVOS

6.1 DESARROLLO DEL OBJETIVO 1

- Evaluar los activos de información mediante la aplicación de una metodología para el análisis y gestión de riesgos de la empresa grupo confeccionistas, que permita identificar vulnerabilidades y amenazas presentes.

Se tomará como referencia la ISO/IEC 27001:2013, y en base a Intenco[46], donde se define para el diseño de un SGSI lo siguiente:

a) Delimitar el SGSI de acuerdo con la línea y procesos del negocio de la empresa, sus activos de información, dispositivos tecnológicos y detallar su alcance en cada aspecto organizativo.
b) Determinar una política de SGSI que sea acorde con las actividades de la empresa incluyendo sus activos de información y dispositivos tecnológicos,
c) Realizar la valoración del riesgo en términos de la estructura organizativa de la empresa.
d) Reconocer los riesgos que están presentes en la empresa Grupo Confeccionistas.
e) Analizar los riesgos presentes en la empresa Grupo Confeccionistas y Evaluarlos acertadamente.
f) Elegir los controles necesarios del anexo A si omitir los que sean necesarios para un acertado tratamiento de los riesgos.
g) Generar un SoA con los controles necesarios justificando su elección o no.
h) Indagar con las directivas de la empresa sobre su aprobación para el diseño y ejecución del SGSI.

Se tuvo en cuenta el marco NIST, donde uno de sus objetivos es reducir los riegos que se presentan en la seguridad informática, el marco se alinea con esta serie de medidas y propone que en las organizaciones tanto privadas como públicas, gubernamentales o de servicios que deseen añadir este marco en su seguridad sigan estas medidas de acuerdo con NIST[47].

1. Descripción de seguridad Cibernética.
2. Descripción del alcance del objetivo en base a la seguridad informática.

[46] INTENCO. Instituto Nacional de Tecnologías de la Comunicación. Implantación de un SGSI en la empresa. [en línea]. 2017. [Consulta: 5 noviembre de 2021]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

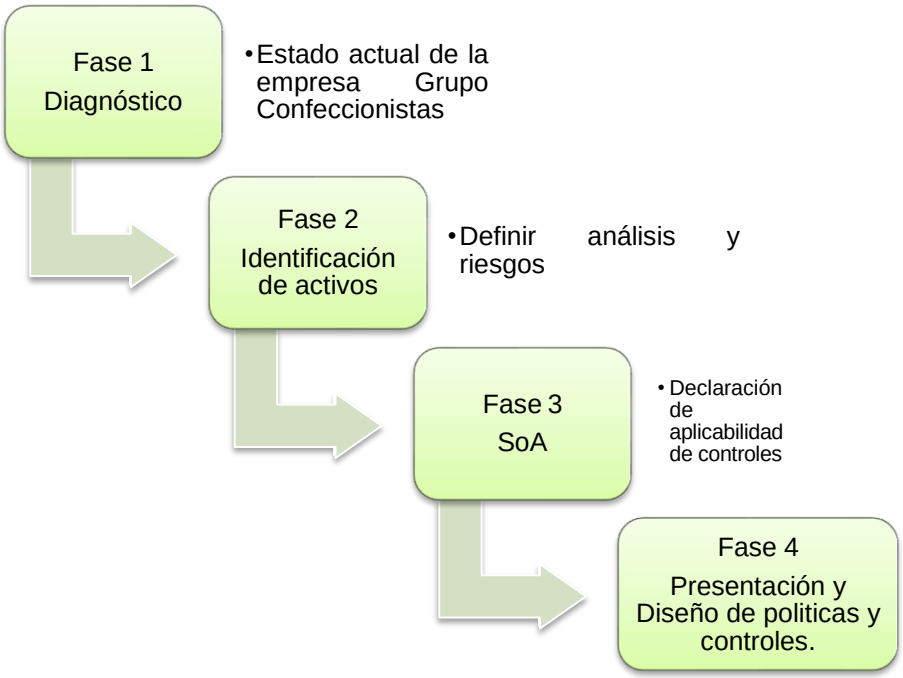
[47] NIST. Op. cit., p. 9.

3. Identificación y mejora continua en un ciclo repetible.
4. Progreso y consecución del objetivo fijado.
5. Comunicación continua con los stakeholders para socialización y conocimiento de los riesgos.

De esta manera también se realizó una metodología Hibrida que involucró tanto variables cuantitativas como cualitativas, a través de la revisión exhaustiva de documentación, informes y manuales que actualmente se encuentran en el departamento de sistemas de la empresa Grupo Confeccionistas, para la evaluación del estado actual de la seguridad.

A partir de lo mencionado se tomó como base las siguientes 4 fases que se alinean con los objetivos específicos que permitió su alcance y desarrollo en base al ciclo de Deming.

Ilustración 3. Fases Metodología SGSI



Fuente: Autoría propia. Basado en GÓMEZ FERNÁNDEZ. Op. cit, p. 96.

6.1.1 Fase 1 Diagnóstico actual. Se exploró la documentación actual que compone el manual de sistemas, inventarios, informes y cualquier medio que permita realizar un diagnóstico de la seguridad en la empresa Grupo Confeccionistas, donde se identificará los activos vinculados en las siguientes áreas de la empresa, que permitan la identificación de riesgos y amenazas que puedan comprometerlos.

- Diseño
- Estampado y bordado
- Corte
- Bodega
- Sistemas
- Subgerencia
- Recursos Humanos
- Contabilidad
- Producción
- Dpto. Técnico

Para el reconocimiento actual se seguirán la siguiente serie de pasos:

- Revisión de manuales y documentos para determinar el estado actual a partir de (misión, visión, objetivos de la empresa, procesos, políticas, estrategias).
- Analizar el manejo de la información su afectación y continuidad de actividades.

6.1.2 Fase 2 Identificación de Activos.

6.1.2.1 Inventario. Se procederá a identificar cada uno de los activos que se emplean en la ejecución de actividades de la empresa que permiten la continuidad del negocio, así como la información, aplicativos que hacen parte de las unidades organizativas de la empresa.

6.1.2.2 Análisis de Riesgos. Por medio de la metodología Magerit se identificarán los riesgos y vulnerabilidades presentes en los activos, para determinar el estado y las recomendaciones para su seguridad, integridad y confiabilidad.

6.1.3 Declaración De Aplicabilidad SoA. Se propuso el SGSI en referencia a la ISO 27001[48] y específicamente en la ISO/IEC 27006:2015[49], que permitió seleccionar las políticas, controles y procesos del anexo A más acordes con los procesos de la empresa y su aplicabilidad en cada entorno.

Al ejecutarse el diagnóstico y la identificación de activos y a su vez los riesgos asociados se seleccionarán los controles para su reducción y mitigación de las vulnerabilidades encontradas en el análisis previo.

A través de la generación de un cronograma de actividades que involucren las áreas y sus directos responsables se establecerá un plan de seguridad donde intervengan los siguientes parámetros.

- Política de seguridad.
- Objetivos estratégicos.
- Resultado del diagnóstico: Análisis de riesgos.

6.1.4 Diseño de Políticas y Controles. De acuerdo con los resultados obtenidos en las fases anteriores y según las necesidades de la empresa, se socializa el diseño del SGSI en sus fases planear y hacer ante la gerencia de la empresa Grupo Confeccionistas, para su análisis y su eventual implementación teniendo en cuenta las recomendaciones realizadas para la seguridad en los activos y actividades que desarrollan, además de seleccionar el de equipo para su diseño, asignar responsabilidades y verificar que los requisitos de la ISO/IEC 27001:2013 se alineen con la gestión de la información en base a las metodologías empleadas para cumplir los requisitos de su implementación.

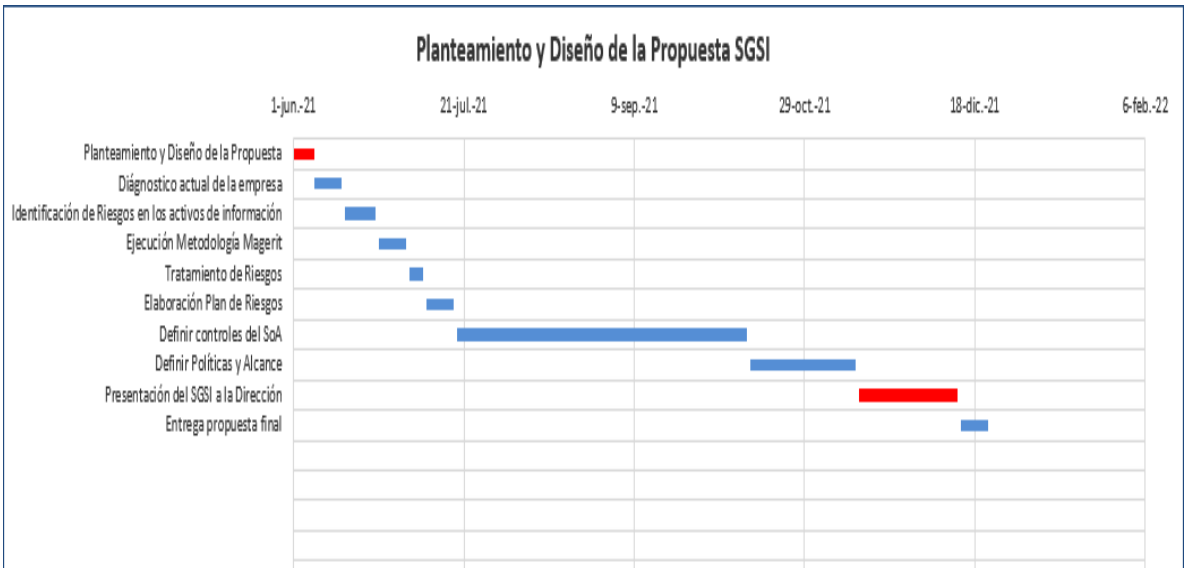
[48] NTC-ISO-IEC 27001:2013. Op. cit., p. 12.

[49] ISO / IEC 27006: 2015. Tecnología de la información – Técnicas de seguridad – Requisitos para los organismos que realizan auditorías y certificaciones de sistemas de gestión de Seguridad de la Información. [en línea]. 2015. [Sitio web]. [Consulta: 5 noviembre 2021]. Disponible en: https://www.iso.org/standard/62313.html

6.1.5 Cronograma

Ilustración 4. Cronograma SGSI

Diseño de Políticas Y Controles de las fases Planear y Hacer de un Sistema de Gestión de seguridad en base a la norma ISO/IEC 27001:2013 para el fortalecimiento de la seguridad de la información de la empresa Grupo confeccionistas.			
Actividad	**Fecha Inicio**	**Dias**	**Fecha Fin**
Planteamiento y Diseño de la Propuesta	**26-abr.-21**	42	7-jun.-21
Diágnostico actual de la empresa	**7-jun.-21**	8	15-jun.-21
Identificación de Riesgos en los activos de información	**16-jun.-21**	9	25-jun.-21
Ejecución Metodología Magerit	**26-jun.-21**	8	4-jul.-21
Tratamiento de Riesgos	**5-jul.-21**	4	9-jul.-21
Elaboración Plan de Riesgos	**10-jul.-21**	8	18-jul.-21
Definir controles del SoA	**19-jul.-21**	85	12-oct.-21
Definir Políticas y Alcance	**13-oct.-21**	31	13-nov.-21
Presentación del SGSI a la Dirección	**14-nov.-21**	29	13-dic.-21
Entrega propuesta final	**14-dic.-21**	8	22-dic.-21



Fuente: Autoría propia.

Como se mencionó anteriormente la empresa es del sector de la industria textil, se ha centrado en sus actividades y continuidad del negocio que, en proteger sus activos e información, la situación actual en cuanto a seguridad se describe a continuación:

- No se ha inculcado la gestión adecuada para garantizar la seguridad y los riesgos asociados a las vulnerabilidades presentes en la información y su tratamiento.
- No se han definido responsabilidades para el tratamiento de la información, tampoco una debida clasificación para determinar su criticidad.
- El inventario de activos se encuentra desactualizado y no se precisa el uso que representa ni el responsable de su utilización.
- No se ha delimitado para cada usuario los accesos de información y su tratamiento.
- No se presenta un continuo monitoreo en los equipos de cómputo, para reducir los riesgos que se pueden asociar con su prestación.
- No se han definido planes de remediación ante posibles a taques o vulnerabilidades a los sistemas de la empresa Grupo Confeccionistas.

En el anexo F, se detallan las condiciones y la valoración a partir de la documentación actual de la empresa grupo confeccionistas en base a su constitución (misión, visión), políticas de seguridad en el trabajo, seguridad actual de cada una de las áreas de la empresa.

6.1.6 Fase 1 PLANEAR. Evaluar los activos de información mediante la aplicación de una metodología para el análisis y gestión de riesgos de la empresa grupo confeccionistas, que permita identificar vulnerabilidades y amenazas presentes.

En primer lugar, para el desarrollo del objetivo 1 y después de analizar el estado actual de la empresa Grupo Confeccionista, se ejecutar la fase 1, del SGSI para determinar sus riesgos, vulnerabilidades e identificación de activos de información.

6.1.7 Diseño del Sistema de Gestión de Seguridad de la información, en base al marco normativo, UNEISO/IEC 27001:2013[50] .

6.1.8 Organización.

Ilustración 5. Estructura de Grupo Confeccionistas.

Fuente: Autoría propia.

6.1.9 Definir el alcance del SGSI en la empresa Grupo Confeccionistas. Se definió el alcance, a partir de lo que se va a proteger y como se va a proteger. Actualmente en la empresa, se cuenta con los siguientes activos y servicios:

- La página web como medio para dinamizar la venta por catálogo en línea con facilidad de manejo para los clientes.

- Los activos de información como eje fundamental para el desarrollo de actividades y procesos de las diferentes áreas de la empresa Grupo Confeccionistas.

[50] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información. NTC-ISO-IEC 27001:2013. Bogotá D.C.: El Instituto, 2015. 33 p.

- Gestión y aprovisionamiento de cada uno de los dispositivos de la empresa Grupo Confeccionistas.

6.1.10 Objetivos. Alcance respecto a la seguridad de la información, en base a los siguientes parámetros.

- Uso del SGSI para la empresa, para delegar funciones y tener control sobre las partes interesadas con la finalidad de que acojan los lineamientos aquí plasmados.
- Aseguramiento eficaz en los diferentes dispositivos para gestionar y el óptimo desarrollo de las actividades propias de la empresa.
- Proyección de los activos para alcanzar y contribuir con la continuidad de los procesos de la empresa.

6.1.11 Compromiso de la dirección. Daza, Ostos y Joya[51], comentan que se debe asumir por parte del Gobierno Corporativo el control y compromiso de acatamiento de los parámetros que se han establecido para evitar que la información sea alterada por parte de los miembros de la empresa ya sean internos o externos, o tengan laguna vinculo comercial que genere riesgo e integridad de la información y procesos.

Ejercer un control de cada uno de los procesos que se ejecuten, a partir de las funciones de los colaboradores para un ambiente seguro y evitando el inconvenientes que afecten la seguridad de la información.

6.1.12 Inventario de los activos. En la tabla 6 y 7, se describen e identifican los activos de información, así como los criterios de evaluación en base a la integridad, disponibilidad y confiabilidad de la información, aplicaciones y procesos que se ejecutan en la empresa para su correspondiente, en base a la tabla 2, del apartado de la metodología Magerit para detallar su información.

[51] DAZA, Alejandro, OSTOS Cristian y JOYA SANTANA, Gonzalo. Política General de Seguridad de la información. [Sitio Web]. Teveandina. 2018. [Consulta: el 22 de mayo de 2021]. Disponible en: https://canaltrece.com.co/uploads/file_uploads/POLITICA_DE_SEGURIDAD_DE_LA_INFORMACION_DE_TEVEANDINA_LTDA_V1.10_11.pdf

Tabla 5. Tipo y activos de contenedor

TIPO DE CONTENEDOR	CONTENEDOR
Servidor	Cuentas de Usuario Correo Electrónico Aplicación SIIGO Nómina Aplicación SIIGO Contabilidad Página WEB PCP Akkumark
Comunicaciones	Antivirus Router con funciones de cortafuego UPS
Equipos de Computo	Estación De trabajo
Medios de Almacenamiento	Equipos de cómputo locales Disco Externo
Espacio Físico	Oficinas Bodega Centro de Computó Personal
Transporte Documentación	Vehículo
Procesos de negocio	Confección y venta Dpto. Financiero Recursos Humanos Dpto. Técnico

Fuente: Autoría propia. Basado en: JARA PEREZ, Op. cit., p. 12.

Tabla 6. Criterios de clasificación

DIMENSIONES	VALOR	DESCRIPCIÓN
DISPONIBILIDAD	3	• Información muy sensible, causaría un muy alto impacto en la compañía. • Riesgo de continuidad del negocio • Solo un grupo mínimo autorizado y muy específico.
INTEGRIDAD	2	• Información sensible, causaría un leve impacto en la compañía. • Solo personal autorizado y especifico.
CONFIDENCIALIDAD	1	• Información para los procesos internos. • Solo de conocimiento interno si se va a exteriorizar contar con la justificación necesaria. • No causaría ningún impacto en la compañía
No aplicable	0	• Información para terceros. • No hay restricciones.

Fuente: Autoría propia. Basado en: JARA PEREZ, Op. cit., p. 12.

En el anexo B, se incluye detalladamente cada uno de los activos descritos en la tabla 6, a modo de ejemplo se presenta el siguiente activo aplicaciones identificado, con cada una de sus características y la respectiva clasificación del activo de información, de esta manera se detallado cada activo que se encuentra en la empresa Grupo Confeccionistas.

Cuadro 1. Activo de Información Aplicaciones.

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-01	**Área**	Admón., Gestión Humana, Contabilidad, Sistemas.
Activo de Información		Soportes, libros contables, documentos, memorandos, notas crédito, manuales, contratos, autorizaciones.	
Descripción			
Hacen partes los sistemas operativos WIN10 de cada estación de trabajo, el paquete ofimático para la realización de informes, documentos, etc., software libre, JAVA, PDF, Firmware de Impresoras,			
Producto	**Tipo de activo** [SW] Software	**Tipo**	Digital
TYPE CONTAINER	Servidores Equipos de Computo	**CONTAINER**	Estaciones de trabajo, red corporativa, correos electrónicos.
Responsable			
Departamento Sistemas			
Custodio	Directores, supervisores y jefes de áreas y Departamentos,	**Usuario**s	Asistentes, secretarias, ejecutivos, quien haga uso de una estación de trabajo.
CLASIFICACIÓN DE ACTIVOS DE INFO			
INTEGRIDAD	**CONFIDENCIALIDAD**	**DISPONIBILIDAD**	**TOTAL**
1	**2**	**2**	**5**

Fuente: Autoría propia.

6.1.13 Analizar los riesgos de los activos. Debido a que la empresa Grupo Confeccionistas maneja la información de sus procesos y de los clientes, se identificaron los riesgos que se generan por la degradación de una serie de eventos que pueden ser internos o externos, también señalar que, al existir el riesgo, la amenaza también se hace presente causando un daño sobre los activos, teniendo en cuenta la siguiente regla.

$$RIESGO = AMENAZA\ X\ VULNERABILIDAD$$

A continuación, se describen una serie de riesgos que podrían afectar la continuidad de las actividades en base a los siguientes parámetros.

Tabla 7. Parámetros Valoración de riesgos

Escala Probabilidad	**Escala Impacto**	**Criterios de seguridad afectados**
Alta: A	Catastrófico: C	Confidencialidad
Media: M	Moderado: M	Integridad
Baja: B	Leve: L	Disponibilidad

Fuente: Autoría propia.

Tabla 8. Valoración de riesgos.

Riesgo N°. /	Valoración	Probabilidad			Impacto		
		A	**M**	**B**	L	M	C
R1	Daños en equipos tecnológicos (Servers y PCs) y áreas por exposición al polvo.			X			X
R2	Daños en equipos tecnológicos (Servers y PCs) y áreas por exposición a temperaturas altas.			X			X
R3	Daños en equipos tecnológicos (Servers y PCs) y áreas por exposición al fuego			X			X
R4	Daños en equipos tecnológicos (Servers y PCs) y áreas por exposición a inundación.		X				X
R5	Obsolescencia de repuestos informáticos		X			X	
R6	Acceso no autorizado a personal a áreas restringidas	X			X		
R7	Falta de soporte página Web		X			X	
R8	Falta de soporte Aplicativos SIIGO, PCP, ACKKUMARK.		X			X	
R9	Infección de virus por actualización del antivirus		X			X	
R10	Acceso no autorizado a los aplicativos y bases de datos	X			X		
R11	Almacenamiento no seguro de copias de seguridad y Backup del sistema	X				X	
R12	Los puertos USB no están desactivados en los PC		X				X
R13	Robo de información confidencial			X		X	
R14	Modificación de información personal			X		X	
R15	Indisponibilidad del sistema por daños ajenos		X				X
R16	Falta de competencias y aptitudes de los usuarios finales		X		X		
R17	Falla en las políticas de seguridad implementadas		X			X	
R18	Intrusión y ataques externos	X					X
R19	Ataques por ingeniería social (Phishing, Vishing,)		X			X	

Fuente: Autoría propia. Basado en: ROJAS PEÑA, Hernán Mauricio. Aplicación de la metodología Margarit para el análisis de riesgos de los sistemas de control en la estación Tenay del oleoducto. [en línea]. Trabajo de grado. Universidad Abierta y a Distancia, 2019. [Consultado el 31 de mayo

de 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/27758/1075211684.pdf?sequence=1&isAllowed=y

En el Anexo C, se detallarán los riesgos asociados a cada uno de los activos de información identificados y su respectiva valoración frente a las vulnerabilidades identificadas. A continuación, se describen en un resumen ejecutivo la clasificación general de cada uno de los activos.

Cuadro 2. Clasificación general de activos

ID RIESGO	Tipo y nombre de activo	Escala Probabilidad:			Escala Impacto: Catastrófico, moderado, leve			Criterios de seguridad afectados: Confidencialidad, Integridad, Disponibilidad.			Ubicación	
		Alto	Medio	Bajo	C	M	L	C	I	D	Digital	Físico
R14	[SW] Aplicaciones	X			X				X		X	
R7	[SW] Aplicaciones Web		X			X				X	X	
R13, R19	[S] Sistemas de correo electrónico.	X			X					X	X	
R8	**[SW]** SIIGO Dpto. Contabilidad.		X			X			X		X	
R8	[SW] Aplicativo PCP Sistemas		X			X			X		X	
R8	[SW] Aplicativo Akkumark Diseño		X			X			X		X	
R8	[SW] SIIGO Dpto. RRHH.		X			X			X		X	
R1,R2,R3,R4 ,R15	[COM] Sistemas de Red			X		X		X	X	X		X
R9, R18	[SW] Antivirus		X			X				X	X	
R17, R18, R19	[HW] Router	X				X		X		X		X

R1,R2,R3,R4,R5,R12,R15	[HW] PC Usuarios			X		X			X	X		X
R1,R2,R3,R4,R5,R12,R13,R15	**[SW]** Servidor		X		X			X	X	X		X
R15	[AUX] UPS			X	X					X		X
R11,R13	**[MEDIA]** Disco Extraíble	X				X		X	X	X		X
R1,R2,R3,R4	**[L]** Oficinas			X		X				X		X
R1,R2,R3,R4,R6	[L] Centro de Computo	X			X			X	X	X		X
R6,R16	**[P]** Personal		X			X			X			X

Fuente: Autoría propia.

Cuadro 3. Clasificación de activos según su valor.

Cantidad de activos que se deben protegerse de clientes o terceros	1
Activos de acceso a un número limitado de empleados	6
Activos de acceso a un número limitado de persona externas.	9
Activos que pueden ser alterados para fraudes.	3
Cantidad de activos que son muy críticos para el desarrollo de procesos internos.	5
Cantidad de activos que son muy críticos para la prestación de servicios a terceros.	3

Fuente: Autoría propia.

6.2 DESARROLLO DEL OBJETIVO 2

- Proponer un documento de declaración de aplicabilidad a partir del informe de análisis de riesgos para establecer los dominios y controles de seguridad que se deben aplicar en la empresa.

6.2.1 Generar un SoA – Declaración de aplicabilidad. Según Berrios y Rocha[52] , para los controles del documento de aplicabilidad se realizó una evaluación y tratamiento sobre los riesgos identificados.

En base a la norma ISO/IEC 27001:2013, se seleccionarán los controles más pertinentes para su implementación en la empresa Grupo Confeccionista.

En la identificación de controles, se tuvo en cuenta las políticas y procesos que actualmente se encuentran establecidos en la empresa.

El contenido de los controles atiende a los 14 dominios, 35 objetivos de control y 114 controles de ISO/IEC 27002:2013, a continuación, se relacionan los dominios.

- Políticas de Seguridad
- Organización de la Seguridad de la Información.
- Seguridad en los Recursos Humanos
- Gestión de Activos.
- Control de Accesos.
- Criptografía.
- Seguridad Física y del Entorno.
- Seguridad en las Operaciones.
- Seguridad en las Comunicaciones
- Adquisición, Desarrollo y Mantenimiento de Sistemas.
- Relaciones con Proveedores.
- Gestión de Incidentes de Seguridad de la Información.
- Aspectos de Seguridad de la Información
- Cumplimiento

En el anexo D, se especifican todos los controles del anexo A y cuales se implementan en la empresa, cuales no y sus respectivas políticas asociadas. que se ajustan a la empresa Grupo confeccionistas.

[52] BERRÍOS MESÍA, César Augusto y ROCHA CAM, Martín Augusto. [en línea]. Propuesta de un modelo de sistema de gestión de la seguridad de la información en una pyme basado en la norma ISO/IEC 27001. [Consultado el 9 de junio de 2021]. Disponible en: http://hdl.handle.net/10757/581891

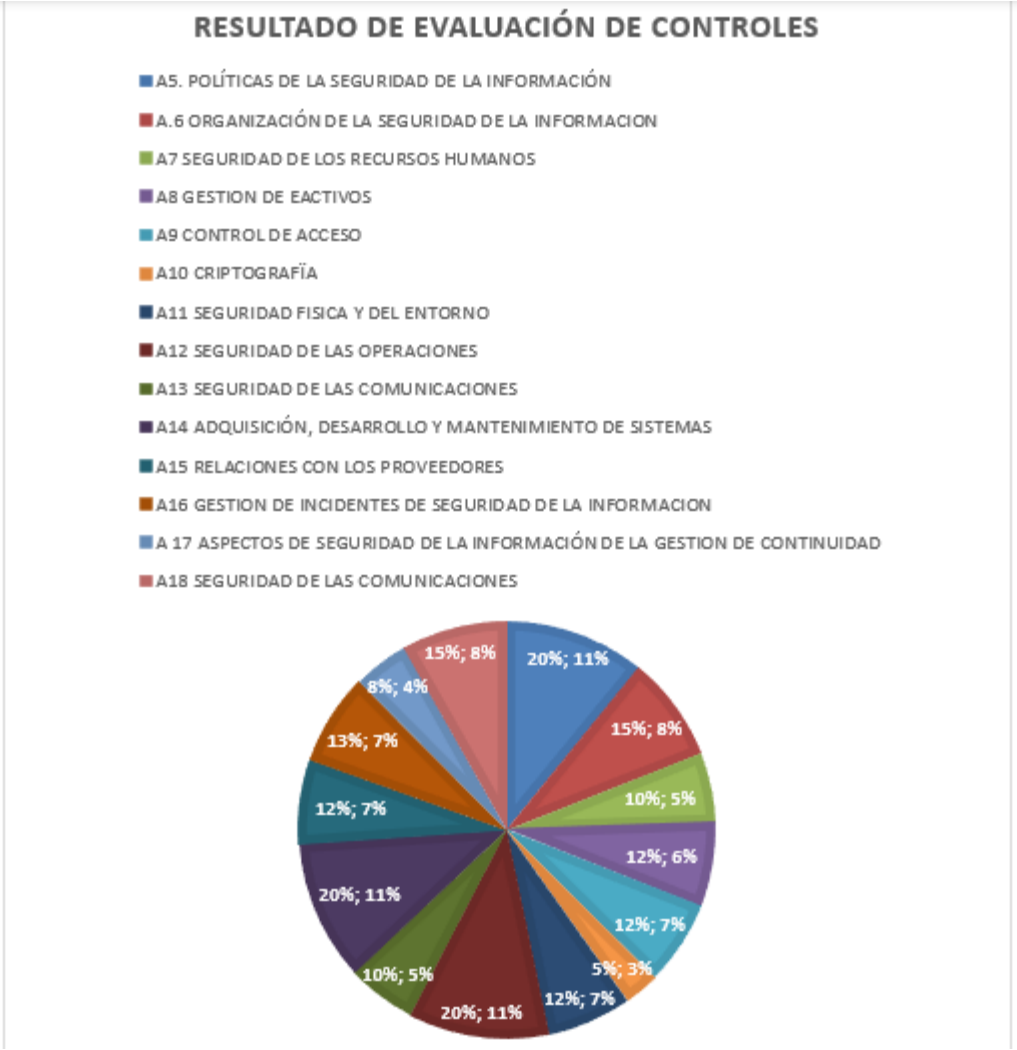
En la ilustración 6, se refleja el comportamiento actual sobre los controles, a donde se quiere llegar y cuál es el resultado óptimo, con las siguientes connotaciones:

- Línea roja representa el cumplimiento actual.
- Línea azul cumplimiento a mediano plazo.
- Línea naranja nivel de cumplimiento óptimo

Ilustración 6. Resultado de evaluación actual, esperado y óptimo de los controles del SoA

Fuente: Autoría propia en base a: INCIBE. Instituto Nacional de Ciberseguridad. Plan Director de Seguridad (PDS). Tecnología de la Información. Técnicas de Seguridad. Análisis de cumplimiento. [en línea]. 2020. [Consulta: 8 noviembre 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

Ilustración 7. Resultado de evaluación de controles actual



Fuente: Autoría propia.

En la anterior ilustración se muestra la evaluación de controles a partir de documento de declaración de aplicabilidad, donde se analizó cada control y se logró establecer cuales se están ejecutando actualmente, cuales aún no se ejecutan y cuáles son los óptimos para seleccionarlo en un futuro y realizar su implementación.

Para definir los controles que actualmente están presentes en la empresa grupo Confeccionistas, se empleó las técnicas de investigación que se detallan en el apartado 5.2, técnicas de recolección de información, donde principalmente por ser parte del área de sistemas, a través del seguimiento, observación e interacción con los activos de información, se logra su respectiva identificación y en base al anexo A de la norma ISO/IEC 27001:2013, se describen detalladamente en el anexo D.

6.3 DESARROLLO DEL OBJETIVO 3

- Diseñar las políticas y controles de seguridad mediante la adopción de buenas prácticas que permitan reducir los riesgos en los activos de información.

6.3.1 Implementar controles seleccionados. Se toma como base los controles de la norma ISO/IEC 27002:2013, para acoger los siguientes controles.

De acuerdo con Incibe[53], después de que se analizó los controles, se elaboró el siguiente documento con las medidas y controles que aplican en la empresa grupo confeccionistas, así como su respectivo grado de madurez, si están implantados y como se encuentran, en base al siguiente criterio:

- 1 control no existe.
- 2 control existe, pero no es efectivo.
- 3 control Efectivo, pero no documentado
- 4 efectivo y documento

En base al análisis realizado, en el desarrollo del objetivo 2 y en cada uno de los controles del anexo A de la norma, ISO/IEC 27001:2013, que incluyen 14 dominios, 35 objetivos de control y 114 controles, se determinó a través de la documentación existente en la empresa, que se concentra en el control de inventarios de los activos de información pertenecientes al hardware y software, licenciamiento y el contacto directo que se generan a través de los riesgos y vulnerabilidades que se presentan entorno a los activos de información, los siguientes controles seleccionados representan como generar un tratamiento efectivo para reducir los riesgos que actualmente se presentan en a empresa, cuya finalidad es la mitigación de estas vulnerabilidades que potencialmente pueden afectar las condiciones y continuidad del negocio de la empresa, generando retraso en las operaciones, desarrollo de actividades y menores brechas de seguridad para contrarrestar los ataques ocasionados por partes de delincuentes informáticos ya sean internos o externos.

[53] INCIBE. Instituto Nacional de Ciberseguridad. UNE-ISO/IEC 27002:2015. Tecnología de la Información. Técnicas de Seguridad. Código de prácticas para los controles de seguridad de la información. [en línea]. 2020. [Consulta: 8 noviembre 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

Cuadro 4. Controles seleccionados.

Identificación Controles – ISO/IEC 27001:2013							
Control	Implementado SI/NO	Descripción	Control	Estado del control			
				1 control no existe	2 existe, pero no es efectivo	3 existe es efectivo, pero no está documentado	4 existe es efectivo y está documentado
A5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN							
Orientación de la dirección para la gestión de la seguridad de la información	NO	La política de Seguridad de la Información debe ser definida	5.1.1	X			
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN							
Roles y responsabilidades para la seguridad de la información	NO	Todas las responsabilidades de la Seguridad de la Información	6.1.1	X			
A7 SEGURIDAD DE LOS RECURSOS HUMANOS							
Selección	SI	Revisar los antecedentes de todos los candidatos a empleados, contratistas.	7.1.1		X		X
Responsabilidades de la dirección	SI	La gerencia debe requerir políticas y procedimientos establecidos.	7.2.1		X		
Toma de conciencia, educación y formación en la seguridad de la información.	NO	Toma de conciencia, educación y formación en la seguridad de la información.	7.2.2	X			
A8 GESTIÓN DE ACTIVOS							
Inventario de activos	SI	Elaborar y mantener un inventario para su respectiva evaluación de vulnerabilidades.	8.1.1		X		
Clasificación de la información	NO	Clasificación en términos de su valor de la Información	8.2.1	X			

A9 CONTROL DE ACCESO							
Registro y cancelación del registro de usuarios	SI	Deshabilitar de usuarios	9.2.1			X	
Restricción de acceso a la información	SI	Denegación de acceso a la información	9.4.1			X	
Procedimiento de ingreso seguro	SI	controlados de registro de accesos.	9.4.2			X	
Sistema de gestión de contraseñas	SI	Administración de contraseñas	9.4.3			X	
A10 CRIPTOGRAFÏA							
Política sobre el uso de controles criptográficos	NO	Política de controles	10.1.1	X			
Gestión de llaves	NO	Administración de contraseñas	10.1.2	X			
A11 SEGURIDAD FISICA Y DEL ENTORNO							
Ubicación y protección de los equipos tecnológicos	SI	Protección PC	11.2.1				X
Mantenimiento de los equipos.	SI	Mantenimiento de preventivo de Equipos	11.2.4				X
A12 SEGURIDAD DE LAS OPERACIONES							
Gestión de capacidad	SI	Administración de capacidades	12.1.3		X		
Instalación de software en sistemas operativos	SI	Instalación de programas	12.5.1			X	
A13 SEGURIDAD DE LAS COMUNICACIONES							
Separación en las redes	SI	División de las redes	13.1.3			X	
Mensajería Electrónica	SI	Correos Electrónicos	13.2.3			X	
A14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS							
Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	SI	Revisión tras los cambios en el sistema	14.2.3			X	

A15 RELACIONES CON LOS PROVEEDORES							
Tratamiento de la seguridad dentro de los acuerdos con proveedores	NO	Clausulas en contratos con terceros	15.1.2	X			
Gestión del cambio en los servicios de los proveedores	NO	Requisitos de seguridad con cada proveedor que tenga acceso a la empresa	15.2.2	X			
A16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION							
Reporte de debilidades de seguridad de la información	SI	Alerta de vulnerabilidades de seguridad.	16.1.3		X		
A 17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD							
Disponibilidad de instalaciones de procesamiento de información	SI	Actualizar de plan de contingencia	17.2.1		X		
A18 SEGURIDAD DE LAS COMUNICACIONES							
Revisión independiente de la seguridad de la información	NO	Revisión dedicada a la Seguridad de la Información	18.2.1	.X			

Fuente: Autoría propia. Basado en: BERRÍOS MESÍA, César Augusto y ROCHA CAM, Martín Augusto. [en línea]. Propuesta de un modelo de sistema de gestión de la seguridad de la información en una pyme basado en la norma ISO/IEC 27001. [Consultado el 9 de junio de 2021]. Disponible en: http://hdl.handle.net/10757/581891. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información. Requisitos. NTC-ISO-IEC 27001:2013. Bogotá D.C.: ICONTEC, 2013. 35 p.

6.3.2 Diseño de políticas. Según Fernández[54] y el INCIBE[55], las políticas definen criterios específicos para la seguridad de la información que se deben acoger y aplicar por cada colaborador o personal tanto interno como externo de la empresa.

A continuación, se muestran las políticas que se propusieron de acuerdo con los controles identificados, seleccionados y reevaluados al interior de la empresa Grupo Confeccionistas.

6.3.2.1 Política de Almacenamiento Seguro de la Información. De acuerdo con Incibe[56], para gestionar un modo seguro y óptimo en cada uno de los sistemas de información de la empresa Grupo Confeccionistas, es necesario, que tanto los colaboradores, como personal externo de la empresa, adopten las siguientes reglas, criterios y procedimientos, con el fin de mitigar las vulnerabilidades que se pueden filtrar por estos medios.

- Es responsabilidad del área de sistemas y el personal técnico y de soporte de infraestructura, garantizar el acceso a los recursos de información o software que previamente haya sido autorizado para cada funcionario, de acuerdo con su rol y permisos concedidos.
- Evitar que la información sea de conocimiento común y que sea extraviada.
- Evitar que la información se deteriore en sus dispositivos de almacenamiento o donde sea conservada.
- Evitar hacer uso de dispositivos que no sean autorizados por parte del área de sistemas para el almacenamiento de la información.
- Suministrar alternativas para poder recuperar la información en caso de que se presenten sucesos inesperados de tipo técnico, natural, accidental o provocado.
- Garantizar que al ser obsoletos los dispositivos de almacenamiento, sean desechados correctamente.
- Disponer de soluciones en caso de fugas de información, contingencias o desastres relacionados con la pérdida de la información.

[54] GÓMEZ FERNÁNDEZ Y FERNÁNDEZ RIVERO. Op. cit., p. 86.

[55] INCIBE. Instituto Nacional de Ciberseguridad. Políticas de Seguridad para la Pyme. [en línea]. 2020. [Consulta: 7 noviembre 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[56] INCIBE. Instituto Nacional de Ciberseguridad. Guía de almacenamiento seguro de la información. [en línea]. 2020. [Consulta: 7 noviembre 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf

De la anterior política se desprenden las siguientes con el fin de tener un mayor control sobre las disposiciones y tratamiento para que sean de conocimiento entre los usuarios y que haya control por parte del personal especializado de sistemas.

6.3.2.2 Política de almacenamiento local en las estaciones de trabajo. La empresa Grupo Confeccionistas deberá establecer las siguientes normas de almacenamiento desde el área de sistemas y avaladas por la gerencia, para los computadores y cada uno de los dispositivos que sean utilizados para desarrollar las actividades al interior de la empresa.

- La información que se almacenará será estrictamente laboral y que haga parte de las actividades del colaborador que se encuentra ejecutando una tarea específica.
- La información que se maneja deberá permanecer por el tiempo que disponga el subgerente de servicios cuya duración no podrá exceder al año debido a que se realiza cierre y se almacena la información del transcurso del año en soportes externos para su posterior consulta.
- El tiempo que permanecerá la información en la red LAN y que es transmitida al servidor principal de la empresa no podrá superar el año para realizar una copia de seguridad general y reducir los riesgos de pérdida o cambio.
- Los documentos en red podrán contener contraseñas secretas que serán de conocimiento solo de los jefes de área que podrán compartirlas con los colaboradores que consideren necesario.
- En cada computador y sitio de trabajo, se vinculará la conexión a la red local para el almacenamiento de la información de acuerdo con el perfil, rol y permisos de usuario establecidos previamente para un área específica.
- Los funcionarios y colaboradores no podrán almacenar en sus computadores ningún tipo de información personal, más aún aquella que sea musical o imágenes con el fin de no patrocinar la falta y violación de derecho de autor que exponen las leyes regulatorias.

6.3.2.3 Política de almacenamiento en la red corporativa. En el caso de la política para la red corporativa es necesario distinguir entre la información general y la puntual de cada colaborador para el desarrollo de sus actividades y que se almacena en la red corporativa.

- El servidor principal deberá estar siempre disponible en la red para el almacenamiento y compartir los recursos para el acceso de los empleados.
- Los controles de acceso serán definidos por parte del área de sistemas y en concordancia con el gobierno corporativo para asignar y proporcionar acceso y a que contendor puede acceder el usuario para el desarrollo de sus actividades.

- La información almacenada deberá ser laboral y esta se almacenará de acuerdo con el cargo que desempeñe el usuario y el respectivo permiso que tenga sobre las carpetas, preferiblemente constantemente para que se guarde por si ocurre algún suceso inesperado.
- Las personas que actualizarán la información son aquellas que tengan el privilegio de lectura y escritura sobre el archivo, carpeta o recursos especifico.
- Para los jefes de área se dispondrá de una carpeta con su nombre donde podrá almacenar información concerniente a sus funciones pero que no es de acceso público.
- La información que se almacene deberá tener un valor justificado y que sea importante para el desarrollo de las actividades, de lo contrario será removida para no ocupar espacio innecesario.
- Para el manejo de las carpetas compartidas la responsabilidad será atribuida al colaborador con previa autorización por el área de sistemas y el Gobierno Corporativo.
- La información almacenada en la red corporativa es de propiedad de la empresa Grupo Confecciones, por lo que no está permitido su modificación sin previa autorización, así mismo se podrá auditar en cualquier momento sin la aprobación de los colaboradores.
- Las diferentes áreas de la empresa están obligadas a informas si la cuota de su almacenamiento esta por quedarse sin espacio para ampliar o verificar su contenido.

6.3.2.4 Política de manejo de dispositivos externos. Al área de sistemas y el Gobierno corporativo serán los encargados de establecer los requisitos, permisos, cambio y modificaciones sobre el uso de dispositivos externos y de almacenamiento.

- El uso de dispositivos está restringido por medio de la consola de antivirus corporativo para evitar que sea extraída la información sin previa autorización del gobierno corporativo o el personal de sistemas.
- Los colaboradores, funcionarios y personal externo no se encuentran autorizados para realizar ningún tipo de cambio en los lineamientos y permisos de la configuración del manejo de dispositivos externos que ha generalizado el área de sistemas y el Gobierno Corporativo.

6.3.2.5 Política de copias de Seguridad. Para la empresa Grupo Confeccionistas es necesario realizar un plan de contingencia con el fin de planificar adecuadamente la ejecución de copias de seguridad, debido a que la perdida de la información pude generar retrasos en las actividades cotidianas de la empresa y exponer la continuidad de la empresa.

- Realizar una previa identificación y selección de los datos que se van a resguardar, teniendo en cuenta su perjuicio en caso de pérdida para la continuad de las actividades de la empresa.
- Las copias de seguridad se realizarán con una frecuencia diaria para las carpetas y archivos frecuentes, así mismo para las aplicaciones de nómina, diseño y planeación de la producción.
- Después de realizada la copia de seguridad se resguardará en el área de sistemas bajo la supervisión del jefe de sistemas quién controlará su preservación.
- Se debe verificar periódicamente el estado del disco extraíble donde se realizan los Backup para comprobar su estado, vida útil, disponibilidad y confiabilidad para asegurar el resguardo de información.
- Se debe planificar la restauración de las copias de seguridad con el personal idóneo y capacitado para ejecutar esta acción.
- Disponer de ambientes de pruebas para comprobar la restauración de las copias de seguridad y verificar que sea exitoso el proceso.
- Contar con dispositivos de redundancia en caso de que el principal presente fallas para la recuperación en el menor tiempo posible.
- Ejecutar pruebas para comprobar la eficacia de los medios dispuestos para la ejecución de procesos de copia y restauración.
- Definir el periodo de validez de la copia de seguridad para reemplazarla por una actualizada.
- Realizar un proceso de borrado seguro en caso de desechar un dispositivo dispuesto para copias de seguridad y que ha quedado obsoleto o presenta fallas de funcionamiento.

6.3.2.6 Política de Criptografía. Para la empresa Grupo Confeccionista es importante el cifrado de la información sensible cuando se ejecute una copia de seguridad.

- El área de sistemas debe garantizar la encriptación en los aplicativos y sistemas para evitar la manipulación de la información por terceros no autorizados.
- El área de sistemas es el encarado del diseño y gestión de llaves de cifrado.
- Sistema deberá acoger sistemas y herramientas criptográficas para la aplicación de controles de seguridad de la información.
- Garantizar el acogimiento por parte del personal técnico de sistemas para ejecutar siempre estos procesos de cifrado para preservar la integridad de la información.
- Capacitar a los integrantes del área de sistemas en ejecutar los controles criptográficos establecidos.

6.3.2.7 Política de Relación con Proveedores. Para la empresa Grupo Confeccionistas es fundamental la relación estrecha con proveedores, de acuerdo con Incibe[57]donde deben existir acuerdos y contratos sobre sus servicios, alcances, que se deben contemplar durante y después de la relación contractual asegurando que se encuentren definidos en los requisitos de seguridad de la empresa.

- Definir los requisitos de ciberseguridad que deben tener los productos y servicios que se adquieren por parte de los proveedores.
- Definir cláusulas contractuales con la relación entre los proveedores y la empresa para mantener una adecuada gestión de la seguridad de la información.
- Definir las responsabilidades exclusivas a cargo de las partes interesadas, cliente-proveedor-cliente.
- Definir los Acuerdos de Nivel de Servicios (ANS), donde se contemple las responsabilidades de las partes, duración del acuerdo, detalle del nivel del servicio en atención a los horarios de disponibilidad, tiempo de respuesta y solución y personal que se encargara del servicio.
- Definir los servicios y recursos a los cuales tendrá acceso el proveedor para la ejecución y prestación de sus servicios.
- Solicitar a proveedores especiales de servicios, certificaciones de calidad en la gestión de la seguridad (ISO/IEC 27001:2013) cunado sus servicios contemplen manejo de información sensible catalogada como confidencial.
- Acordar la terminación de la relación contractual, donde se establezca la devolución de elementos empleados durante el desarrollo de las actividades, eliminar permisos provisionales y cuentas creadas, suprimir la información sensible alojada en los recursos tecnológicos del proveedor de servicios cuando ejecuto sus funciones

6.3.2.8 Política de utilización de la red Internet. Se dispone del uso Internet exclusivamente para actividades laborales y el desarrollo de sus funciones propias del cargo que así ameriten las consultas por este medio.

- Está prohibido el acceso a sitos no autorizados por la empresa y que no hacen parte de la ejecución de sus funciones como lo son: de dudosa reputación (ilegales, amenazas, estafas), uso personal (redes sociales, recreación) y ataques informáticos a través de la red empresarial.

[57] INCIBE. Instituto Nacional de Ciberseguridad. UNE-ISO/IEC 27002:2015. Tecnología de la Información. Herramientas de Ciberseguridad. Políticas de seguridad para la PYME. Relación con proveedores. [en línea]. 2020. [Consulta: 8 noviembre 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/relacion-proveedores.pdf

- Es ilegal compartir datos e información de la empresa, sin previa autorización que atente con la integridad de la misma y genere riesgo a sus cometidos.
- Evadir los controles y medidas de seguridad que permiten la navegación a página y portales con un alto nivel de riesgo que afecten directamente la seguridad de la empresa y su información.
- Los funcionarios y colaboradores de la empresa Grupo Confeccionistas acogen la política antispam de la empresa para evitar vulnerabilidades asociadas a la ingeniería social.

7 CONCLUSIONES

Se establece el alcance del diseño del SGSI para la empresa Grupo Confeccionistas, en base a ello se definen los objetivos, las normas jurídicas que debe tener en cuenta para su implementación y también los procesos que realiza la empresa desde cada departamento, identificando los aspectos principales y falencias para crear las políticas de seguridad que se ajusten con los objetivos planteados.

Se realiza el reconocimiento de cada uno de los activos de información de la empresa Grupo Confeccionistas, identificando las vulnerabilidades y amenazas existentes después de analizar los controles que se ejecutan y los que no, realizando un análisis de riesgos concreto, a partir de las dimensiones de la seguridad que permite evaluar las condiciones actuales y los procesos de la empresa en base al desarrollo y ejecución de sus actividades.

Tomando como base la ISO/IEC 27001:2013, se logró realizar una valoración de las amenazas de la empresa y aplicando la metodología Magerit se logró la respectiva identificación, para determinar las condiciones que se estaban cumpliendo dentro de la empresa y cuales no se ejecutaban, a partir de este análisis y evaluación para la continuación del trabajo.

Se propone un cambio a partir de los controles seleccionados para proporcionar de manera íntegra la seguridad en los procesos y dispositivos que forman parte de la continuidad del negocio de la empresa Grupo Confeccionistas, permitiendo el análisis por parte de los directivos y así establecer los mecanismos más adecuados que mitiguen los riesgos y las vulnerabilidades y proporcionen la debida seguridad de la información.

Se diseñan las políticas de seguridad de la información, a partir de la evaluación y selección de controles, donde se tienen en cuenta las diferentes afectaciones y procesos que no se ejecutan adecuadamente por no estar establecido un Sistema de Seguridad de la Información que establezca un control optimo, sobe el tratamiento de los activos y la información para establecer proceso efectivos y óptimos en base a la norma ISO/IEC 27001:2013 y la ISO/IEC 27002:2007

8 RECOMENDACIONES

Debido a que la empresa Grupo Confeccionistas, cuenta con un plan estandarizado para el análisis y tratamiento de riesgo a partir de la identificación de activos de información con los que se cuentan, es contemplar la ejecución del diseño presentado con la finalidad de establecer un mayor control de las actividades que suponen un riesgo en la información

Al ejecutar un Sistema de Gestión de Seguridad de la información s e contaran con las herramientas que permitan un mayor control sobre los activos, además de mantener y definir el comportamiento de los usuarios respecto con la seguridad de la información, adaptando medidas que mitiguen los riesgos y el seguimiento de buenas prácticas para el manejo de información, el levantamiento de información y asignar responsabilidades a los colaboradores.

Manejo de los dispositivos a cargo generando un acta de compromiso con su utilización, siguiendo y aplicando las recomendaciones por parte del departamento del área de sistemas de la empresa.

Finalmente, al realizar los respectivos cambios después del diseño del SGSI se presentará a la dirección para su análisis y se podrá acordar futuras modificaciones que permitan llevar a cabo una auditoría interna para la mejora continua de la seguridad.

9 BIBLIOGRAFÍA

ÁVILA, Miguel Andrés y GRANADA, María Liliana. Metodología para la identificación de caracteres de compromiso para la protección de las IC. 2018. [en línea]. Universidad de Alcalá. Disponible en: https://ebuah.uah.es/xmlui/bitstream/handle/10017/33004/TFM_Avila_Granada_2018.pdf?sequence=1&isAllowed=y

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (enero 5 de 2009). “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". En: Diario Oficial. Enero, 2009. p. 1 – 4.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 23. (enero 28 de 1982). “sobre derechos de autor”. En: Diario Oficial. Enero, 1982. p. 1-10.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 455. (11 de agosto de 1998). “convención sobre la abolición del requisito de legalización para documentos públicos extranjeros”. En: Diario Oficial. Agosto 1998.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 594. (14, julio, 2000). Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. En: Diario Oficial. Julio, 2000. Nro. 44084. p. 1-9.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. En: Diario Oficial. Agosto, 1999. Nro 43.673. p. 1-10.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581. (18, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Diario Oficial. Octubre, 2012. Nro. 48.587. p. 1-185.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1150. (16, julio, 2007). Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. En: Diario Oficial. Julio, 2007. Nro. 46.691. p. 1-18.

DAZA, Alejandro, OSTOS Cristian y JOYA SANTANA, Gonzalo. Política General de Seguridad de la información. [Sitio Web]. Teveandina. 2018. Disponible en: https://canaltrece.com.co/uploads/file_uploads/POLITICA_DE_SEGURIDAD_DE_LA_INFORMACION_DE_TEVEANDINA_LTDA_V1.10_11.pdf

DEPARTAMENTO NACIONAL DE PLANEACIÓN. [Sitio web]. Bogotá: Alta Consejería Distrital, Lineamientos de políticas para ciberseguridad y ciberdefensa, CONPES 3701 de 2011. Disponible en: https://tic.bogota.gov.co/transparencia/marco-legal/normatividad/conpes-3701-2011

ESCRIVÁ-GASCO, Gema. Unidad 1 -Introducción a la Seguridad Informática. En: Seguridad Informática. España: 2011. p. 8. Disponible en: https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edselb&AN=edselb.3217398&lang=es&site=eds-live&scope=site

FERNÁNDEZ SÁNCHEZ Carlos Mario. Modelo para el gobierno de las TIC basado en las normas ISO [En Línea]. Madrid: AENOR - Asociación Española de Normalización y Certificación, 2012. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53581?page=33

GB Advisors. ISO, COBIT e ITIL: ¿Cuál de estas normas y estándares internacionales te conviene más para potenciar tu empresa? Madrid. 6 de abril de 2018. Disponible en: https://www.gb-advisors.com/es/normas-y-estandares-internacionales/

GÓMEZ FERNÁNDEZ Luis. y FERNÁNDEZ RIVERO Pedro. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. [En Línea]. Madrid: AENOR - Asociación Española de Normalización y Certificación, 2018. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624?page=89

GÓMEZ VIEITES Álvaro. Seguridad en equipos informáticos [En Línea]. Madrid: RA-MA Editorial, 2015. p.p 13-14. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/62466?page=13

INCIBE. Instituto Nacional de Ciberseguridad. Plan Director de Seguridad (PDS). Tecnología de la Información. Técnicas de Seguridad. Análisis de cumplimiento. [en línea]. 2020. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

INCIBE. Instituto Nacional de Ciberseguridad. UNE-ISO/IEC 27002:2015. Tecnología de la Información. Técnicas de Seguridad. Código de prácticas para los controles de seguridad de la información. [en línea]. 2020. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

INCIBE. Instituto Nacional de Ciberseguridad. Guía de almacenamiento seguro de la información. [en línea]. 2020. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf

INCIBE. Instituto Nacional de Ciberseguridad. UNE-ISO/IEC 27002:2015. Tecnología de la Información. Herramientas de Ciberseguridad. Políticas de seguridad para la PYME. Relación con proveedores. [en línea]. 2020. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/relacion-proveedores.pdf

INSTITUTO DE CIBERSEGURIDAD. [sitio web]. Ciudad de México: ICS. Disponible en: https://www.iciberseguridad.io/

Ingeniería de la Seguridad. Controles de accesos [En línea]. 2012. Disponible en: http://ingenieriadelaseguridad.blogspot.com/p/control-de-accesos.html

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información. NTC-ISO-IEC 27001:2013. Bogotá D.C.: El Instituto, 2015. 33 p.

INTENCO. Instituto Nacional de Tecnologías de la Comunicación. Implantación de un SGSI en la empresa. [en línea]. 2017. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO 27001. Objeto y campo de aplicación definición del alcance del SGSI. [Sitio web]. 2021. España. Disponible en: https://normaiso27001.es/objeto-y-campo-de-aplicacion/

ISO / IEC 27006: 2015. Tecnología de la información – Técnicas de seguridad – Requisitos para los organismos que realizan auditorías y certificaciones de sistemas de gestión de Seguridad de la Información. [en línea]. 2015. [Sitio web]. Disponible en: https://www.iso.org/standard/62313.html

JARA PEREZ, Diana Fernanda. Valoración y plan de tratamiento de riesgos de seguridad de la información para los procesos incluidos en el alcance del SGSI del cliente TGE de la empresa Assurance Controltech. [en línea]. Proyecto de pasantía. Universidad Distrital Francisco José de Caldas. 2017 Disponible en: https://repository.udistrital.edu.co/bitstream/handle/11349/6492/JaraPerezDianaFernanda2017.pdf?sequence=1&isAllowed=y

KASPERSKY. Centro de recursos. Vishing. [Sitio web]. 2021. Disponible en: https://latam.kaspersky.com/resource-center/definitions/vishing

KASPERSKY. Centro de recursos. ¿Qué es una amenaza persistente APT? [Sitio web]. 2021. Disponible en: https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats

LA ROTTA, Santiago. EL ESPECTADOR. Seguridad digital: lo que debe hacer y definitivamente no. [En línea]. Tecnología. Bogotá, D.C. 2016. Disponible en web: https://www.elespectador.com/noticias/tecnologia/seguridad-digital-lo-que-debe-hacer-y-lo-que-definitivamente-no/

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro l – Método. 2012. [en línea]. Madrid. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Materia Sisoperativos. Implantación de matrices de acceso. [en línea]. Disponible en: https://sites.google.com/site/materiasisoperativo/unidad-6-proteccion-y-seguridad/6-3-implantacion-de-matrices-de-acceso

ROJAS CÓRSICO Ivana Soledad. Trabajo de auditoría normas COBIT [En Línea]. Santa Fe, Argentina: El Cid Editor | apuntes, 2009. p.5. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/28995?page=5

ROJAS PEÑA, Hernán Mauricio. Aplicación de la metodología Margarit para el análisis de riesgos de los sistemas de control en la estación Tenay del oleoducto. [en línea]. Trabajo de grado. Universidad Abierta y a Distancia, 2019. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/27758/1075211684.pdf?sequence=1&isAllowed=y

X.800: Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT. [En línea]. Ginebra, 1991: ITU Unión Internacional de Telecomunicaciones. Disponible en: https://www.itu.int/rec/T-REC-X.800-199103-I/es

WINSTON, Kimberly. Exploratory Research: Definition, Methods & Examples." [Sitio web]. 2017. Study.com. Disponible en: https://study.com/academy/lesson/exploratory-research-definition-methods-examples.html.

ANEXOS

Anexo A

A continuación, se presentan los planos del cableado estructurado en las instalaciones del grupo confeccionistas. Se usan las siguientes convenciones:

- Tubo PVC por cielo raso
- Tubo EMT por cielo raso
- Canaleta por cielo raso 
- Canaleta por muro 
- Toma de voz y datos 

- Toma de corriente regulada 

- Toma de corriente 220 L6-30 

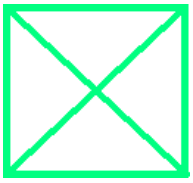
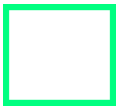
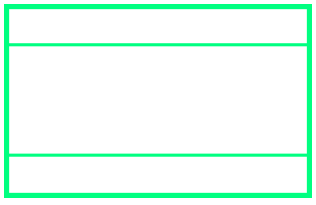
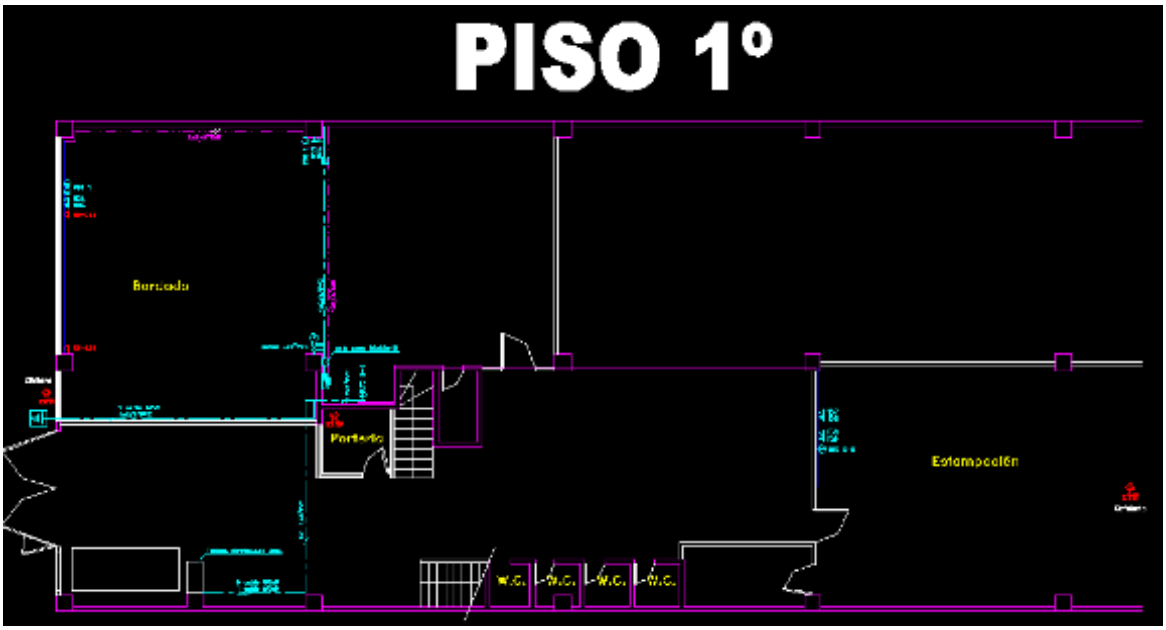
- Caja de paso. 
- Canaleta vertical en muro. 
- Gabinete. 

Ilustración 8. Plano Cableado Piso 1.

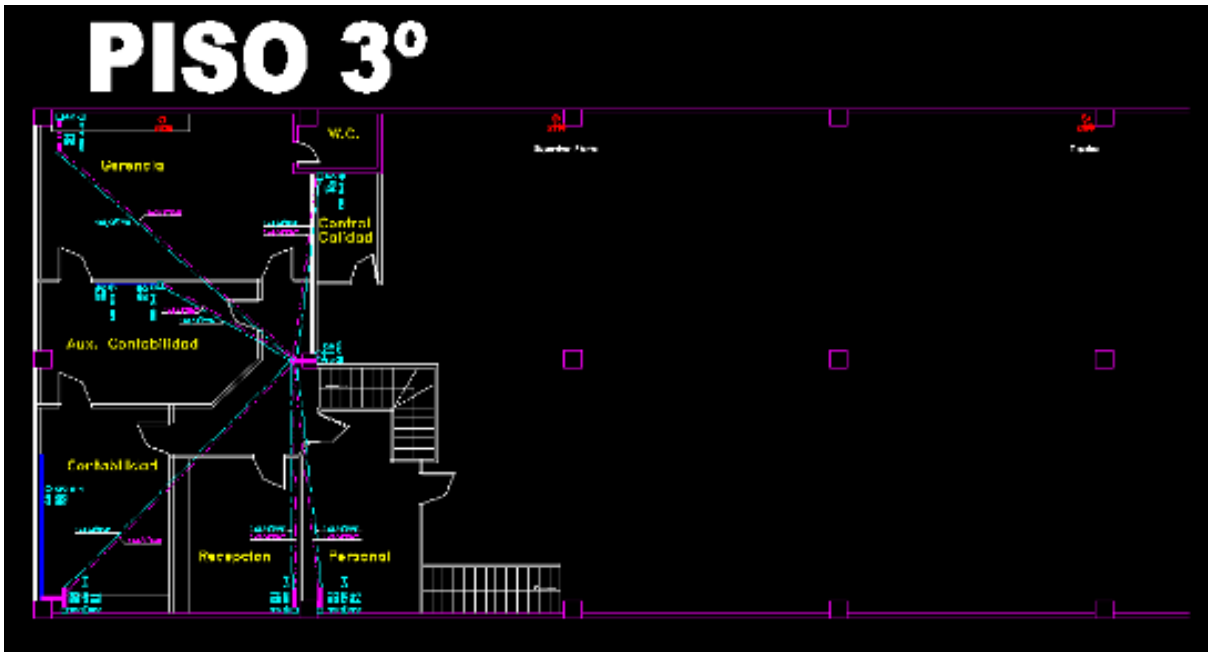


Fuente: Autoría propia.

Ilustración 9. Plano Cableado Piso 2.

Fuente: Autoría propia.

Ilustración 10. Plano Cableado Piso 3.



Fuente: Autoría Propia.

Anexo B

Cuadro 5. Activo de Información Aplicaciones.

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-01	**Área**	Admón., Gestión Humana, Contabilidad, Sistemas.
Activo de Información		Soportes, libros contables, documentos, memorandos, notas crédito, manuales, contratos, autorizaciones.	
Descripción			
Hacen partes los sistemas operativos WIN10 de cada estación de trabajo, el paquete ofimático para la realización de informes, documentos, etc., software libre, JAVA, PDF, Firmware de Impresoras,			
Producto	**Tipo de activo** [SW]Software	**Tipo**	Digital
TYPE CONTAINER	Servidores Equipos de Computo	**CONTAINER**	Estaciones de trabajo, red corporativa, correos electrónicos.
Responsable			
Departamento Sistemas			
Custodio	Directores, supervisores y jefes de áreas y Departamentos,	**Usuario**s	Asistentes, secretarias, ejecutivos, quien haga uso de una estación de trabajo.
CLASIFICACIÓN DE ACTIVOS DE INFO			
INTEGRIDAD	**CONFIDENCIALIDAD**	**DISPONIBILIDAD**	**TOTAL**
1	**2**	**2**	**5**

Fuente: Autoría propia.

Cuadro 6. Activo de Información Aplicaciones Web.

INVENTARIO DE ACTIVOS DE INFORMACIÓN			
REF. ACTIVO	GC-02	**Área**	Admón.
Activo de Información		Página Web, servicios, aplicativos, gestión	
Descripción			
A través de la página web los clientes pueden realizar compras, auto gestionando todo el procedimiento.			
Producto	**Tipo de activo** [SW] Software	**Tipo**	Digital
TYPE CONTAINER	Servidor	**CONTAINER**	Página Web
Responsable			
Admón., Departamento Sistemas			
Custodio	Jefe de área Admón. y Diseño.	**Usuarios**	Clientes Personal externo Proveedores
CLASIFICACIÓN DE ACTIVOS DE INFO			
INTEGRIDAD	**CONFIDENCIALIDAD**	**DISPONIBILIDAD**	**TOTAL**
1	**1**	**0**	**2**

Fuente: Autoría propia.

Cuadro 7. Activo de Información. Sistemas de correo electrónico.

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-03	**Área**	Gerente, Subgerente, Admón., Gestión Humana, Contabilidad, Sistemas.
Activo de Información		Correo Electrónico	
Descripción			
Envío y recepción de correos electrónicos a cada una de las áreas y usuarios que dispongan de una cuenta empresarial.			
Producto	**Tipo de activo** [S]Servicio	**Tipo**	Digital
TYPE CONTAINER	Servidor	**CONTAINER**	Correo Electrónico
Responsable			
Dpto. Sistemas			
Custodio	Jefes de áreas Admón., Gestión Humana, Contabilidad, Sistemas.	**Usuarios**	Asistentes, secretarias, ejecutivos, quien tenga asignado un correo empresarial.
CLASIFICACIÓN DE ACTIVOS DE INFO			
INTEGRIDAD	**CONFIDENCIALIDAD**	**DISPONIBILIDAD**	**TOTAL**

2	**2**	**1**	**5**

Fuente: Autoría propia.

Cuadro 8. Activo de Información. Aplicativo SIIGO Dpto. Contabilidad.

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-04	**Área**	Contabilidad
Activo de Información		Aplicación SIIGO	
Descripción			
A través de esta aplicación se lleva a cabo la contabilidad de la empresa y las obligaciones fiscales y societarias.			
Producto	**Tipo de activo** [SW] Software	**Tipo (Digital o Física)**	Digital
TYPE CONTAINER	Servidor	**CONTAINER**	Aplicación SIIGO Contabilidad
Responsable			
Jefe Dpto. Sistemas			
Custodio	Jefe Dpto. Contabilidad	**Usuarios**	Auxiliares de Contabilidad Asistentes, secretarias, ejecutivos, quien forme parte del área Financiera.
CLASIFICACIÓN DE ACTIVOS DE INFO			
INTEGRIDAD	**CONFIDENCIALIDAD**	**DISPONIBILIDAD**	**TOTAL**
2	**2**	**2**	**6**

Fuente: Autoría propia.

Cuadro 9. Activo de Información. Aplicativo PCP Sistemas

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-05	**Área**	Sistemas
Activo de Información		Aplicación PCP	
Descripción			
A través de esta aplicación se lleva a cabo la elaboración de órdenes, y planeación de trabajo de confecciones.			
Producto	**Tipo de activo** [SW] Software	**Tipo (Digital o Física)**	Digital
TYPE CONTAINER	Servidor	**CONTAINER**	Aplicación PCP
Responsable			
Jefe Dpto. Sistemas			
Custodio	Jefe Dpto. Sistemas	**Usuarios**	Auxiliares de Sistemas Asistentes, secretarias, ejecutivos, quien forme parte del área de sistemas.
CLASIFICACIÓN DE ACTIVOS DE INFO			

INTEGRIDAD	CONFIDENCIALIDAD	DISPONIBILIDAD	TOTAL
2	2	2	6

Fuente: Autoría propia.

Cuadro 10. Activo de Información. Aplicativo Akkumark Diseño

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-06	**Área**	Diseño
Activo de Información		Aplicación Akkumark	
Descripción			
A través de esta aplicación se lleva a cabo la elaboración bocetos, diseños de prendas, trazos para la elaboración de prendas			
Producto	**Tipo de activo** [SW] Software	**Tipo (Digital o Física)**	Digital
TYPE CONTAINER	Servidor	**CONTAINER**	Aplicación Akkumark
Responsable			
Jefe Dpto. Sistemas			
Custodio	Jefe Dpto. Diseño	**Usuarios**	Auxiliares de Diseño Asistentes, secretarias, ejecutivos, quien forme parte del área de diseño.
CLASIFICACIÓN DE ACTIVOS DE INFO			
INTEGRIDAD	**CONFIDENCIALIDAD**	**DISPONIBILIDAD**	**TOTAL**
2	**2**	**2**	**6**

Fuente: Autoría propia.

Cuadro 11. Activo de Información. Aplicativo SIIGO Dpto. RRHH.

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-07	**Área**	Gestión Humana
Activo de Información		Aplicación SIIGO Nómina	
Descripción			
A través de esta aplicación se gestiona las nóminas y contratos del personal			
Producto	**Tipo de activo** [SW] Software	**Tipo**	Digital
TYPE CONTAINER	Servidor	**CONTAINER**	Aplicación SIIGO RRHH
Responsable			
Jefe Dpto. Sistemas			
Custodio	Jefe Dpto. Gestión Humana	**Usuarios**	Auxiliares de Nómina Asistentes, secretarias, ejecutivos, quien forme parte del área RRHH.
CLASIFICACIÓN DE ACTIVOS DE INFO			
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONBILIDAD**	**TOTAL**
1	**1**	**2**	**4**

Fuente: Autoría propia.

Cuadro 12. Activo de Información. Sistemas de Red.

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-08	**Área**	Dpto. Sistemas
Activo de Información		Sistemas de red (LAN, Por parte del proveedor ISP Fibra óptica de 50mb, para la red local cable de cobre, topología en estrella simple, tipo de transmisión mixta, 100mbps, full dúplex)	
Descripción			
Hacen parte todos los recursos de infraestructura de la empresa destacando el cableado estructurado, puntos de red, dispositivos de comunicaciones			
Producto	**Tipo de activo** [COM]Redes de Comunicaciones	**Tipo (Digital o Física)**	Física
TYPE CONTAINER	Espacio Físico	**CONTAINER**	Oficinas, bodegas, centros de Computó
Responsable			
Jefe Dpto. Sistemas			
Custodio	Gerente, Subgerente, Admón., Gestión Humana, Contabilidad, Sistemas.	**Usuarios**	Asistentes, secretarias, ejecutivos, quien haga usos de las comunicaciones y el entorno empresarial.
CLASIFICACIÓN DE ACTIVOS DE INFO			
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONBILIDAD**	**TOTAL**
2	**2**	**3**	**7**

Fuente: Autoría propia.

Cuadro 13. Activo de Información. Antivirus.

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-09	**Área**	Equipos de Computó
Activo de Información		Antivirus	
Descripción			
Todos los equipos disponen de un sistema antivirus que se actualiza periódicamente de manera automática.			
Producto	**Tipo de activo** [SW] Software	**Tipo**	Digital
TYPE CONTAINER	Comunicaciones	**CONTAINER**	Antivirus
Responsable			
Jefe Dpto. Sistemas			
Custodio	Gerente, Subgerente, Admón., Gestión Humana, Contabilidad, Sistemas.	**Usuarios**	Asistentes, secretarias, ejecutivos, quien haga usos de las comunicaciones y el entorno empresarial.

CLASIFICACIÓN DE ACTIVOS DE INFO			
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONBILIDAD**	**TOTAL**
1	**1**	**2**	**4**

Fuente: Autoría propia.

Cuadro 14. Activo de Información. Router.

INVENTARIO DE ACTIVOS			
REF. ACTIVO	**GC-10**	**Área**	Equipos de Computó
Activo de Información		Router	
Descripción			
Conexión ADSL con un Router que realiza y ejecuta funciones de un Firewall.			
Producto	**Tipo de activo** [HW] Hardware	**Tipo**	Físico
TYPE CONTAINER	Comunicaciones	**CONTAINER**	Router
Responsable			
Jefe Dpto. Técnico			
Custodio	Gerente, Subgerente, Admón., Gestión Humana, Contabilidad, Sistemas.	**Usuarios**	Asistentes, secretarias, ejecutivos, quien haga usos de las comunicaciones y el entorno empresarial.
CLASIFICACIÓN DE ACTIVOS DE INFO			
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONBILIDAD**	**TOTAL**
1	**1**	**2**	**4**

Fuente: Autoría propia.

Cuadro 15. Activo de Información. PC Usuarios

INVENTARIO DE ACTIVOS			
REF. ACTIVO	**GC-11**	**Área**	Equipos de Computó
Activo de Información		Estaciones de Trabajo	
Descripción			
La red local está conformada por 25 ordenadores personales de usuario, los que permiten la ejecución de tareas, informes, manejo de aplicativos, programaciones, entre otros.			
Producto	**Tipo de activo** [HW] Hardware	**Tipo**	Digital y Físico
TYPE CONTAINER	Equipos de computo	**CONTAINER**	Estaciones de trabajo
Responsable			
Jefe Dpto. Sistemas			
Custodio	Gerente, Subgerente, Admón., Gestión Humana, Contabilidad, Sistemas.	**Usuarios**	Asistentes, secretarias, ejecutivos, quien haga usos de ordenadores personales en el entorno empresarial.
CLASIFICACIÓN DE ACTIVOS DE INFO			
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONBILIDAD**	**TOTAL**
1	**1**	**2**	**4**

Fuente: Autoría propia.

Cuadro 16. Activo de Información. Servidor

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-12	**Área**	Página web SIIGO PCP Akkumark Gestión Sistemas Cuentas de usuario Correo electrónico Antivirus
Activo de Información		Servidor	
Descripción			
Centralización de la información, aplicaciones (PCP, SIIGO, Akkumark) para el desarrollo de actividades, accesos de red.			
Producto	**Tipo de activo** [SW] Software	**Tipo (Digital o Física)**	Digital
TYPE CONTAINER	Servidor	**CONTAINER**	Página web SIIGO PCP Akkumark Gestión Sistemas Cuentas de usuario Correo electrónico Antivirus
Responsable			
Jefe Dpto. Sistemas			
Custodio	Jefe Dpto. Sistemas	**Usuarios**	Asistentes, secretarias, ejecutivos, quien haga usos de los recursos de red y aplicaciones en el entorno empresarial.
CLASIFICACIÓN DE ACTIVOS DE INFO			
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONBILIDAD**	**TOTAL**
3	**3**	**3**	**9**

Fuente: Autoría propia.

Cuadro 17. Activo de Información.

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-13	**Área**	Función servidor
Activo de Información		UPS	
Descripción			
Sistemas de alimentación ininterrumpida			
Producto	**Tipo de activo** [AUX] Equipamiento Auxiliar	**Tipo**	Físico
TYPE CONTAINER	Equipos de computo	**CONTAINER**	UPS
Responsable			
Jefe Dpto. Sistemas			
Custodio	Jefe Dpto. Sistemas	**Usuarios**	Asistentes, secretarias, ejecutivos, quien haga usos de los recursos de red y aplicaciones en el entorno empresarial.
CLASIFICACIÓN DE ACTIVOS DE INFO			
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONBILIDAD**	**TOTAL**
1	**2**	**2**	**5**

Fuente: Autoría propia.

Cuadro 18. Activo de Información. Disco Extraíble

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-14	**Área**	Copias de seguridad semanalmente en un disco extraíble de 1 TB
Activo de Información		Cintas magnéticas	
Descripción			
Almacenamiento de los datos del servidor y aplicativos para el desarrollo de actividades que se almacenan digitalmente.			
Producto	**Tipo de activo** [Media] Soportes de información	**Tipo**	Físico
TYPE CONTAINER	Medios de almacenamiento	**CONTAINER**	Disco Extraíble
Responsable			
Jefe Dpto. Sistemas.			
Custodio	Jefe Dpto. Sistemas	**Usuarios**	Auxiliares de soporte técnico, Ingenieros de soporte, personal de tecnología.
CLASIFICACIÓN DE ACTIVOS DE INFO			
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONBILIDAD**	**TOTAL**
2	**2**	**2**	**6**

Fuente: Autoría propia.

Cuadro 19. Activo de Información. Oficinas

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-15	**Área**	Instalaciones donde se desarrollan las actividades de gestión de la empresa.
Activo de Información		Oficinas	
Descripción			
Instalaciones donde se desarrollan todas las actividades y se concentran todas las áreas de negocio.			
Producto	**Tipo de activo** [L] Instalaciones	**Tipo**	Física
TYPE CONTAINER	Espacio Físico	**CONTAINER**	Oficinas Bodegas Centro de computó
Responsable			
Gerencia			
Custodio	Gerencia	**Usuarios**	Asistentes, secretarias, ejecutivos, quien haga usos de las instalaciones en el entorno empresarial.
CLASIFICACIÓN DE ACTIVOS DE INFO			
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONBILIDAD**	**TOTAL**
1	**2**	**2**	**5**

Fuente: Autoría propia.

Cuadro 20. Activo de Información. Centro de Computo.

INVENTARIO DE ACTIVOS			
REF. ACTIVO	GC-16	**Área**	Instalaciones donde se gestionan las comunicaciones, servicios y aplicaciones de la empresa.
Activo de Información		Centro de computó	
Descripción			
Instalaciones donde se gestionan las comunicaciones, servicios y aplicaciones de la empresa. Se encuentran todos los dispositivos de comunicaciones y se administran los servidores y dispositivos.			
Producto	**Tipo de activo** [L] Instalaciones	**Tipo**	Físico
TYPE CONTAINER	Espacio físico	**CONTAINER**	Centro de computó
Responsable			
Dirección			
Custodio	Jefe Dpto. Sistemas	**Usuarios**	Auxiliares de soporte técnico, Ingenieros de soporte, personal de tecnología.
CLASIFICACIÓN DE ACTIVOS DE INFO			
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONBILIDAD**	**TOTAL**
3	**3**	**3**	**9**

Fuente: Autoría propia.

Cuadro 21. Activo de Información. Personal

INVENTARIO DE ACTIVOS			
REF. ACTIVO	RTT-17	**Área**	Personal
Activo de Información		Personal	
Descripción			
Funcionarios y directivos que hacen parte de la empresa y que desarrollan sus actividades en las instalaciones de la empresa.			
Producto	**Tipo de activo** [P] Personal	**Tipo**	Físico
TYPE CONTAINER	Espacio físico	**CONTAINER**	Personal
Responsable			
Dirección			
Custodio	Gerente, Subgerente, Admón., Gestión Humana, Contabilidad, Sistemas.	**Usuarios**	Asistentes, secretarias, ejecutivos, quien haga usos de las instalaciones en el entorno empresarial. Auxiliares de soporte técnico, Ingenieros de soporte, personal de tecnología.
CLASIFICACIÓN DE ACTIVOS DE INFO			
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONBILIDAD**	**TOTAL**

1	**1**	**1**	**3**

Fuente: Autoría propia.

Anexo C

Cuadro 22. Aplicaciones.

ANÁLISIS DE RIESGOS			
ID RIESGO	R14 Modificación de información personal	**Proceso/Subproceso**	Admón., Gestión Humana, Contabilidad, Sistemas.
Activo de Información		Soportes, libros contables, documentos, memorandos, notas crédito, manuales, contratos, autorizaciones.	
Descripción del riesgo			
Acceso no contralado a la información generando manipulación sin la debida autorización.			
Fuente del riesgo (Interno – Externo			
Interno y externo			
Propietario del riesgo			
Asistentes, secretarias, ejecutivos, quien haga uso de una estación de trabajo			
Causa del riesgo	Falta de controles de acceso establecidos, políticas de autenticación.	**Consecuencias del riesgo**	Perdida de información, alteración de estados financieros, contratos manuales.
ANÁLISIS DE RIESGOS			
Probabilidad	Alta	**Impacto**	Catastrófico
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
	X	**X**	

Fuente: Autoría propia.

Cuadro 23. Aplicaciones web.

ANÁLISIS DE RIESGOS			
ID RIESGO	R7	**Proceso/Subproceso**	Admón.
Activo de Información		Página Web, servicios, aplicativos, gestión	
Descripción del riesgo			
Falta de soporte página Web			
Fuente del riesgo (Interno – Externo			
Externo			
Propietario del riesgo			
Admón., Departamento Sistemas			
Causa del riesgo	Falta de mantenimientos programados para la página web y personal interno para su administración.	**Consecuencias del riesgo**	Afectación en el cliente porque no podría gestionar la venta, alquiler de vehículos y más procesos auto gestionables.
ANÁLISIS DE RIESGOS			
Probabilidad	**Media**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
		X	

Fuente: Autoría propia.

Cuadro 24. Sistemas de correo electrónico

ANÁLISIS DE RIESGOS			
ID RIESGO	R13 R19	**Proceso/Subproceso**	Gerente, Subgerente, Admón., Gestión Humana, Contabilidad, Sistemas.
Activo de Información		Correo Electrónico	
Descripción del riesgo			
Robo de información confidencial, Ataques por Ing., Social.			
Fuente del riesgo (Interno – Externo			
Interno, externo			
Propietario del riesgo			
Asistentes, secretarias, ejecutivos, quien tenga asignado un correo empresarial.			
Causa del riesgo	Falta de previsión y aseguramiento del servidor, control de acceso y políticas de seguridad del servidor de correo.	**Consecuencias del riesgo**	Filtración de información, expansión de virus malicioso, Ransonware, secuestre de información.
ANÁLISIS DE RIESGOS			
Probabilidad	**Alta**	**Impacto**	Catastrófico
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
X		**X**	

Fuente: Autoría propia.

Cuadro 25. Aplicativo SIIGO Dpto. Contabilidad.

ANÁLISIS DE RIESGOS			
ID RIESGO	R8	**Proceso/Subproceso**	Contabilidad
Activo de Información		Aplicación SIIGO	
Descripción del riesgo			
Falta de soporte aplicativo SIIGO			
Fuente del riesgo (Interno – Externo			
Interno			
Propietario del riesgo			
Jefe Dpto. Sistemas, Jefe Dpto. Contabilidad			
Causa del riesgo	Mantenimiento y mejoras al aplicativo SIIGO para gestión de contabilidad.	**Consecuencias del riesgo**	Parálisis en pagos y obligaciones financieras, fiscales y societarias, que repercutirían en acciones legales.
ANÁLISIS DE RIESGOS			
Probabilidad	**Media**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
	X	**X**	

Fuente: Autoría propia.

Cuadro 26. Aplicativo PCP Sistemas

ANÁLISIS DE RIESGOS			
ID RIESGO	R8	**Proceso/Subproceso**	Sistemas
Activo de Información		Aplicación PCP	
Descripción del riesgo			
Falta de soporte aplicativo PCP			
Fuente del riesgo (Interno – Externo			
Interno			
Propietario del riesgo			
Jefe Dpto. Sistemas			
Causa del riesgo	Mantenimiento y mejoras al aplicativo PCP para gestión de órdenes y planeación de producción	**Consecuencias del riesgo**	Parálisis en pedidos, ordenes de trabajo, confección de prendas.
ANÁLISIS DE RIESGOS			
Probabilidad	**Media**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
	X	**X**	

Fuente: Autoría propia.

Cuadro 27. Aplicativo Akkumark Diseño

ANÁLISIS DE RIESGOS			
ID RIESGO	R8	**Proceso/Subproceso**	Recursos Humanos
Activo de Información		Aplicación Akkumark	
Descripción del riesgo			
Falta de soporte aplicativo Akkumark			
Fuente del riesgo (Interno – Externo			
Interno			
Propietario del riesgo			
Jefe Dpto. Sistemas, Jefe Dpto. Diseño			
Causa del riesgo	Mantenimiento y mejoras al aplicativo Akkumark para gestión de contratos y nóminas	**Consecuencias del riesgo**	Atraso en diseños, trazos y patronaje de prendas.
ANÁLISIS DE RIESGOS			
Probabilidad	**Media**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
	X	**X**	

Fuente: Autoría propia.

Cuadro 28. Aplicativo SIIGO Dpto. RRHH.

ANÁLISIS DE RIESGOS			
ID RIESGO	R8	**Proceso/Subproceso**	Gestión Humana
Activo de Información		Aplicación SIIGO	
Descripción del riesgo			
Falta de soporte aplicativo SIIGO			
Fuente del riesgo (Interno – Externo			
Interno			
Propietario del riesgo			
Jefe Dpto. Sistemas, Jefe Dpto. Gestión Humana			
Causa del riesgo	Mantenimiento y mejoras al aplicativo SIIGO para Gestión Humana.	**Consecuencias del riesgo**	Parálisis en nóminas, contratos, afiliaciones, parafiscales.
ANÁLISIS DE RIESGOS			
Probabilidad	**Media**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
	X	**X**	

Fuente: Autoría propia.

Cuadro 29. Sistemas de Red.

ANÁLISIS DE RIESGOS			
ID RIESGO	R1, R2, R3, R4, R15	**Proceso/Subproceso**	Dpto. Sistemas
Activo de Información		Sistemas de red	
Descripción del riesgo			
Daños en equipos informáticos (servidores y estaciones de trabajo) y áreas comunes por exposición al polvo, temperaturas altas, fuego, inundación y por indisponibilidad del sistema por daños ajenos.			
Fuente del riesgo (Interno – Externo			
Interno y externo			
Propietario del riesgo			
Gerente, Subgerente, Admón., Gestión Humana, Contabilidad, Sistemas.			
Causa del riesgo	Exposición frecuente a eventos locativos y de ambiente que ocasionen daños en las áreas y equipos informáticos.	**Consecuencias del riesgo**	Indisponibilidad de la red local, estaciones de trabajo y aplicativos que permitan la ejecución normal de las labores.
ANÁLISIS DE RIESGOS			
Probabilidad	**Baja**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
X	**X**	**X**	

Fuente: Autoría propia.

Cuadro 30. Antivirus

ANÁLISIS DE RIESGOS			
ID RIESGO	R9, R18	**Proceso/Subproceso**	Equipos de Computó
Activo de Información		Antivirus	
Descripción del riesgo			
Infección de virus por actualización del antivirus, Intrusión y ataques externos			
Fuente del riesgo (Interno – Externo			
Interno, externo			
Propietario del riesgo			
Jefe Dpto. Sistemas			
Causa del riesgo	Propagación de virus maliciosos, filtraciones de información, accesibilidad no autorizada de la información	**Consecuencias del riesgo**	Perjudicar las áreas de la empresa en la ejecución de sus actividades habituales por afectación de las estaciones de trabajo, servidor, recursos y sistemas de red.
ANÁLISIS DE RIESGOS			
Probabilidad	**Media**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
		X	

Fuente: Autoría propia.

Cuadro 31. ROUTER

ANÁLISIS DE RIESGOS			
ID RIESGO	R17, R18 y R19	**Proceso/Subproceso**	Equipos de Computó
Activo de Información		Router	
Descripción del riesgo			
Falla en las políticas de seguridad implementadas, intrusión y ataques externos, ataques por Ingeniería social.			
Fuente del riesgo (Interno – Externo			
Interno, externo			
Propietario del riesgo			
Jefe Dpto. Sistemas			
Causa del riesgo	Propagación de virus maliciosos, filtraciones de información, accesibilidad no autorizada de la información	Consecuencias del riesgo	Perjudicar las áreas de la empresa en la ejecución de sus actividades habituales por afectación de las estaciones de trabajo, servidor, recursos y sistemas de red.
ANÁLISIS DE RIESGOS			
Probabilidad	**Alta**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
X		**X**	

Fuente: Autoría propia.

Cuadro 32. PC usuario

ANÁLISIS DE RIESGOS			
ID RIESGO	R1, R2, R3, R4, R5, R12, R15	**Proceso/Subproceso**	Dpto. Técnico
Activo de Información		Estaciones de trabajo	
Descripción del riesgo			
Daños en equipos informáticos (servidores y estaciones de trabajo) y áreas comunes por exposición al polvo, temperaturas altas, fuego, inundación y por indisponibilidad del sistema por daños ajenos, obsolescencia de repuestos informáticos puertos USB no están desactivados.			
Fuente del riesgo (Interno – Externo			
Interno			
Propietario del riesgo			
Gerente, Subgerente, Admón., Gestión Humana, Contabilidad, Sistemas.			
Causa del riesgo	Indisponibilidad de las estaciones de trabajo para que los funcionarios realicen sus actividades habituales.	Consecuencias del riesgo	Parálisis parcial de la continuidad del negocio afectando la prestación del servicio a los clientes habituales y generales.
ANÁLISIS DE RIESGOS			
Probabilidad	**Baja**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
	X	**X**	

Fuente: Autoría propia

Cuadro 33. Servidor

ANÁLISIS DE RIESGOS			
ID RIESGO	R1, R2, R3, R4, R5, R12, R13, R15	**Proceso/Subproceso**	Dpto. Sistemas
Activo de Información		Servidor	
Descripción del riesgo			
Daños en equipos informáticos (servidores y estaciones de trabajo) y áreas comunes por exposición al polvo, temperaturas altas, fuego, inundación y por indisponibilidad del sistema por daños ajenos, obsolescencia de repuestos informáticos, robo de información confidencial, puertos USB no están desactivados			
Fuente del riesgo (Interno – Externo			
Interno y externo			
Propietario del riesgo			
Gerente, Subgerente, Admón., Gestión Humana, Contabilidad, Sistemas			
Causa del riesgo	Indisponibilidad de las aplicaciones, servicios y recursos de red para que los funcionarios realicen sus actividades habituales.	**Consecuencias del riesgo**	Parálisis total de la continuidad del negocio afectando la prestación del servicio a los clientes habituales y generales
ANÁLISIS DE RIESGOS			
Probabilidad	**Media**	**Impacto**	Catastrófico
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
X	**X**	**X**	

Fuente: Autoría propia.

Cuadro 34. UPS

ANÁLISIS DE RIESGOS			
ID RIESGO	R15	**Proceso/Subproceso**	Función servidor
Activo de Información		Sistemas de alimentación ininterrumpida	
Descripción del riesgo			
Indisponibilidad del sistema por daños ajenos			
Fuente del riesgo (Interno – Externo			
Interno			
Propietario del riesgo			
Jefe Dpto. Sistemas			
Causa del riesgo	Detección del servidor por falla eléctricas o cortes de energía ocasionado su apagado.	**Consecuencias del riesgo**	No realizar mantenimiento adecuado a las UPS genera apagado del servidor por no existir un canal de energía redundante para su normal apagado
ANÁLISIS DE RIESGOS			
Probabilidad	**Bajo**	**Impacto**	Catastrófico
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
		X	

Fuente: Autoría propia.

Cuadro 35. Análisis de Riesgos

ANÁLISIS DE RIESGOS			
ID RIESGO	R11, R13	**Proceso/Subproceso**	Copias de seguridad diariamente en disco externo
Activo de Información		Disco Externo	
Descripción del riesgo			
Almacenamiento no seguro de copias de seguridad y Backup del sistema			
Fuente del riesgo (Interno – Externo			
Interno			
Propietario del riesgo			
Jefe Dpto. Sistemas			
Causa del riesgo	Sistemas sin protección para realizar las copias de seguridad.	**Consecuencias del riesgo**	Alteración de las copias de seguridad, daño o perdida de información, destrucción natural del medio digital.
ANÁLISIS DE RIESGOS			
Probabilidad	**Alta**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
X	**X**	**X**	

Fuente: Autoría propia.

Cuadro 36. Oficinas

ANÁLISIS DE RIESGOS			
ID RIESGO	R1, R2, R3, R4	**Proceso/Subproceso**	Instalaciones donde se prestan los servicios de alquiler y venta de vehículos
Activo de Información		Oficinas	
Descripción del riesgo			
Daños en áreas comunes por exposición al polvo, temperaturas altas, fuego e inundaciones			
Fuente del riesgo (Interno – Externo			
Interno			
Propietario del riesgo			
Gerencia			
Causa del riesgo	Eventos naturales o provocados por la interacción con el funcionario	Consecuencias del riesgo	Destrucción total o parcial de las instalaciones de la empresa.
ANÁLISIS DE RIESGOS			
Probabilidad	**Baja**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
		X	

Fuente: Autoría propia.

Cuadro 37. Centro de computó

ANÁLISIS DE RIESGOS			
ID RIESGO	R1, R2, R3, R4, R6,	**Proceso/Subproceso**	Instalaciones donde se gestionan las comunicaciones, servicios y aplicaciones de la empresa
Activo de Información		Centro de computó	
Descripción del riesgo			
Daños en equipos informáticos (servidores y estaciones de trabajo) y áreas comunes por exposición al polvo, temperaturas altas, fuego, inundaciones, acceso no autorizado a personal a áreas restringidas			
Fuente del riesgo (Interno – Externo			
Interno			
Propietario del riesgo			
Jefe Dpto. Sistemas			
Causa del riesgo	Exposición sin protección de los dispositivos informáticos, sistemas de control de acceso inexistentes, políticas de riesgos no definidas.	Consecuencias del riesgo	Daños en dispositivos de comunicación, alteración de la configuración del sistema por personal no autorizado, robo y secuestre de información
ANÁLISIS DE RIESGOS			
Probabilidad	**Alta**	**Impacto**	Catastrófico
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
X	**X**	**X**	

Fuente: Autoría propia.

Cuadro 38. Personal

ANÁLISIS DE RIESGOS			
ID RIESGO	R6, R16	**Proceso/Subproceso**	Personal
Activo de Información		Personal	
Descripción del riesgo			
Acceso no autorizado a personal a áreas restringidas, falta de competencias y aptitudes de los usuarios finales.			
Fuente del riesgo (Interno – Externo			
Interno			
Propietario del riesgo			
Gerente, Subgerente, Admón., Gestión Humana, Contabilidad, Sistemas.			
Causa del riesgo	Errores de usuario en la manipulación de estaciones de trabajo e ingreso a zonas prohibidas.	**Consecuencias del riesgo**	Daño total, parcial o des configuración en equipos de cómputo e intrusiones de virus malicioso o ingeniería social por falta de capacitaciones y orientaciones tecnológicas a los usuarios de la empresa.
ANÁLISIS DE RIESGOS			
Probabilidad	**Media**	**Impacto**	Moderado
Criterios de Seguridad afectados			
Confidencialidad	**Integridad**	**Disponibilidad**	
	X		

Fuente: Autoría propia.

La clasificación de riesgos una efectuada se presenta de la siguiente forma:

Tabla 9. Matriz clasificación

	Leve	Moderado	Catastrófico
Alto	R16,R17,R18	R10,R12,R13,R14,R15	R5,R16,R19
Medio	R14	R6,R7,R11	R13
Bajo	R8,R9,R10		R1,R2,R3,R4

Fuente: Autoría propia. Basado en: ROJAS PEÑA, Hernán Mauricio. Aplicación de la metodología Margarit para el análisis de riesgos de los sistemas de control en la estación Tenay del oleoducto. [en línea]. Trabajo de grado. Universidad Abierta y a Distancia, 2019. [Consultado el 31 de mayo de 2021]. Disponible en:

https://repository.unad.edu.co/bitstream/handle/10596/27758/1075211684.pdf?sequence=1&isAllowed=y

Anexo D

Cuadro 39. Identificación de controles ISO 27001

Identificación Controles - ISO 27001:2013					Sistema de control interno informático		Niveles de aceptación del riesgo				
Control	Descripción		Control	Justificación	Tipo de requerimiento		Requerimiento legal	Obligación contractual	Requerimiento de negocio	Análisis de riesgo	Exclusión
	Aplica SI/NO	Política Tratada			Control Implementado	Control para implementar					
A5. POLÍTICAS D SEGURIDAD DE INFORMACIÓN		Orientación de la dirección para la gestión de la seguridad de la información	5.1								
	SI	Políticas para la seguridad de la información	5.1.1	La política de Seguridad de Información debe ser definida	Política de Seguridad de la información	Actualizar la política en base a la NTC-ISO 27001:2013			X		
	SI	Revisión de las políticas para la seguridad de la información.	5.1.2	La política de seguridad de la. Información debe ser revisada.	Política de Seguridad da la información	Actualizar la política en base a la NTC-ISO 27001:2013			X		

	A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION											
A.6 Gestión de un marco interno de Seguridad de la información	SI	Roles y responsabilidades para la seguridad de la información	6.1.1	Todas las responsabilidades de la Seguridad de la Información.	Roles y responsabilidades	Verificación de responsabilidades y roles				X		
	SI	Separación de deberes	6.1.2	Asignación de tareas	Roles y responsabilidades	Verificación de responsabilidades y roles				X		
	NO	Contacto con las autoridades	6.1.3	Acudir a la autoridad	No es viable porque no contribuye a mitigar los riesgos de los activos analizados anteriormente.	No es viable					X	
	SI	Contacto con grupos de interés especial	6.1.4	Acudir a grupos especiales	Contactos especiales en foros, correo, folletos.	Crear plan de contingencias				X		
	SI	Seguridad de la información en la gestión de proyectos.	6.1.5	Tratamiento independiente del tipo de proyectos	Buscar en los proyectos los riesgos.	Crear el PETI				X		
A.6.2 La empresa utiliza móviles o de teletrabajo	NO	Política para dispositivos móviles	6.2.1	política para gestionar dispositivos móviles.	No se emplean para la continuidad del negocio y el manejo de la Inf. segura.	No es viable					X	

	NO	Teletrabajo	6.2.2	Procesa o almacena en los lugares de teletrabajo.	No se presta a través de teletrabajos servicios en Grupo Confeccionistas						X
A7 SEGURIDAD DE LOS RECURSOS HUMANOS											
A7.1 Antes de asumir el trabajo Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	SI	Selección	7.1.1	Revisar los antecedentes de todos los candidatos a empleados, contratistas.	De acuerdo con las normas nacionales se hace la consulta de habeas data y confirmaciones.			X			
	SI	Términos y condiciones del empleo	7.1.2	Aceptar y firmar los términos y condiciones del contrato.	Se elaboran las cláusulas del contrato.		X				
A7.2 Durante la ejecución del empleo	SI	Responsabilidades de la dirección	7.2.1	La gerencia debe requerir políticas y procedimientos establecidos.	Se aclaran las funciones antes de las capacitaciones al nuevo personal.			X			
	SI	Toma de conciencia, educación y formación en la seguridad de la información.	7.2.2	los empleados reciben el apropiado conocimiento, capacitación sobre S. I	Se educa sobre Seguridad de la Información a los empleados para mitigar	Campañas de Seguridad de la Información	X				

					las vulnerabilidades frecuentes de usuario.						
	SI	Proceso Disciplinario	7.2.3	Disciplina con respecto a la política de Seguridad de la Información.	Se informa acerca del incumplimiento de las políticas.	Política de la empresa				X	
A7.3 Terminación o cambio de trabajo	SI	Terminación o cambio de responsabilidades de empleo	7.3.1	Las responsabilidades de cambio de empleo se deben definir y comunicar.	Al finalizar el trabajo se aclara que la S. I no se puede ver comprometida.	Obligaciones contractuales		X			
A8 GESTIÓN DE ACTIVOS											
A8.1 Responsabilidad por los activos	SI	Inventario de activos	8.1.1	Inventario de Activos	Elaborar y mantener un inventario para su respectiva evaluación de vulnerabilidades.	Actualizar activos de T.I				X	
	SI	Propiedad de los activos	8.1.2	Propiedad de los Activos	Asignación e identificación a encargado para la Seguridad de la. Información	Actualizar activos de T.I					
	SI	Uso aceptable de los activos	8.1.3	Empleo de los Activos	Parámetros de utilización	Actualizar activos de T.I				X	
	SI	Devolución de activos	8.1.4	Entrega de Activos	Al retirarse el funcionario entrega los activos a su cargo.	Crear formulario de paz y salvo.			X		

A8.2 Clasificación de la información	SI	Clasificación de la información	8.2.1	Clasificación en términos de su valor de la Inf.	Criticidad de la Inf para su tratamiento.					X	
	SI	Etiquetado de la información	8.2.2	Etiquetar y manejar la Inf.	Protección a los Activos identificados.	Actualizar activos de T.I				X	
	NO	Manejo de activos	8.2.3	Manejo de la Inf.	Seguridad en función de su estado.	Política de salvaguarda de la información				X	
A8.3 Manejo de medios	SI	Gestión de medio removibles	8.3.1	Administración de medios removibles.	Extracción adecuada de USB				X		
	SI	Disposición de los medios	8.3.2	Suprimir soportes	Destrucción física de medios.		X				
	NO	Transferencia de medios físicos	8.3.3	Protección de medios de accesos no autorizados,	Verificar que no almacene información interna de los procesos y sean divulgados exteriormente.					X	
A9 CONTROL DE ACCESO											
A9.1 Requisitos del negocio para el control de acceso	NO	Política de control de acceso	9.1.1	Política de accesos y control.	A cada usuario se le asignan los permisos necesarios para el ingreso determinadas secciones.	Actualizar y socialización de la política de seguridad			X		
	SI	Acceso a redes y a servicios en red	9.1.2	Accesos a los servicios interconectados.	Se asignan determinados accesos en red	Actualizar y socialización de la política de seguridad				X	

					dependiendo de la actividad a realizar.						
A9.2 Gestión de acceso de usuarios	SI	Registro y cancelación del registro de usuarios	9.2.1	Des habilitación de usuarios	Alta o baja de usuarios para un control ordenado y dinámico	Actualizar y socialización de la política de seguridad				X	
	SI	Suministro de acceso de usuarios	9.2.2	Aprovisionamiento de acceso	Control y restricción de permisos de usuario de acuerdo con su función.	Actualizar y socialización de la política de seguridad				X	
	SI	Gestión de derechos de acceso privilegiado	9.2.3	Proceso de gestión formal.	Permisos y roles en O.S	Actualizar y socialización de la política de seguridad				X	
	SI	Gestión de información de autenticación secreta de usuarios	9.2.4	Administración y login de usuario para la Seguridad de la Información	Según el riesgo evaluado se determina ejecutar el control.	Actualizar y socialización de la política de seguridad				X	
	SI	Revisión de los derechos de acceso de usuarios	9.2.5	Derechos de acceso de usuario	Se gestiona directamente con el encargado del usuario.	Actualizar y socialización de la política de seguridad				X	
	SI	Retiro o ajuste de los derechos de acceso	9.2.6	Modificación de acceso de usuario	Desactivación y reasignación de accesos según el estado de usuario.	Actualizar y socialización de la política de seguridad				X	

A9.3 Responsabilidades de los usuarios	SI	Uso de información de autenticación secreta	9.3.1	Uso Información privada	Primordial para proteger la Seguridad de la Información					X	
A9.4 Control de acceso a sistemas y aplicaciones	SI	Restricción de acceso a la información	9.4.1	Denegación de acceso de información	Solo se asignan los permisos a determinada Información. Según la función del usuario					X	
	SI	Procedimiento de ingreso seguro	9.4.2	controlados de registro de accesos.	Es necesario establecer un login y password de usuario para inicio de sesión.	Reforzar la autenticación en los dispositivos				X	
	SI	Sistema de gestión de contraseñas	9.4.3	Administración de contraseñas	Reforzar el establecimiento de contraseñas para que no se presenten vulnerabilidades en este sentido.	Actualizar el controlador de dominio que existe actualmente.				X	
	SI	Uso de programas utilitarios privilegiados	9.4.4	Privilegios del sistema	Los usuarios estándar tienen restricciones evitando para evitar incidentes.					X	

	NO	Control de acceso a códigos fuente de programas	9.4.5	El acceso al código	La empresa Grupo Confeccionistas tiene el servicio tercerizado para la administración y mantenimiento de la página web.			X			
A10 CRIPTOGRAFÍA												
A10.1 Controles criptográficos.	NO	Política sobre el uso de controles criptográficos	10.1.1	Política de controles	No están presentes ningún tipo de herramienta o software que genere un cifrado de la Inf.	Crear política donde se incluyan controles criptográficos				X	
	NO	Gestión de llaves	10.1.2	Administración de contraseñas	No están presentes ningún tipo de herramienta o software que genere un cifrado de la Inf.	Crear política donde se incluyan controles criptográficos				X	
A11 SEGURIDAD FISICA Y DEL ENTORNO												
A11.1 Áreas seguras	SI	Perímetro de seguridad física	11.1.1	perímetros seguros (paredes, puertas, etc.)	Restricción de usuarios a áreas restringidas				X		
	SI	Controles de acceso físicos	11.1.2	Controles físicos.	Se gestionan cambios en orden de los	Implementar control de acceso mediante			X		

					ambientes empresariales.	autenticación, como tarjetas de acceso o huellas.					
	NO	Seguridad de oficinas, recintos e instalaciones	11.1.3	Seguridad en áreas comunes.	aplicar seguridad física en las áreas comunes.				X		
	NO	Protección contra amenazas externas y ambientales.	11.1.4	Protección de eventos naturales	No aplica para disminución de los riesgos evaluados.	Diseñar control de impactos ambientales					X
	NO	Trabajo en áreas seguras	11.1.5	Trabajo en áreas comunes	Los equipos y dispositivos no cuentan con la suficiente protección que minimice los riesgos a los que están expuestos						
	NO	Áreas de carga, despacho y acceso público	11.1.6	Controlar puntos de acceso	Controlar puntos de acceso	Revisión de ingreso y salida de elementos.			X		
	SI	Ubicación y protección de los equipos tecnológicos	11.2.1	Protección PC	Deben estar resguardados y solo accesibles a las personas autorizadas.	Actualizar plan de emergencias y contingencias de la empresa			X		
A11.2 Equipos	SI	Seguridad en el suministro de electricidad y servicios	11.2.2	Fuentes de suministro	Se cuenta con una UPS para el Servidor	Actualizar los mantenimiento s de la UPS				X	

	SI	Seguridad en el cableado	11.2.3	.Cableado seguro	Los servicios de Información deben ser protegidos ante eventuales fallas y vulnerabilidades.	Revisar equipos activos en red.						
	SI	Mantenimiento de los equipos.	11.2.4	Mantenimiento de preventivo de Equipos	Se realiza limpieza preventiva y correctiva de los sistemas de computo				X			
	SI	Retiro de activos	11.2.5	Expulsión de residuos electrónicos de empresas	Al retirarse el activo no se deja almacenada información sensible.				X			
	SI	Seguridad de equipos y activos fuera de las instalaciones	11.2.6	Seguridad externa de los equipos.	Se retira adecuadamente de las oficinas los desechos electrónicos.						X	
	SI	Disposición segura o reutilización de equipos	11.2.7	Reempleo y desecho de equipos	Se reinstala los equipos para entrar nuevamente en operación.	Implementar política de borrado seguro					X	
	SI	Equipos de usuario desatendido	11.2.8	Equipos sin administración	Es fundamental para alteraciones en los equipos.	Sistema de bloqueo seguro					X	

	SI	Política de escritorio y pantalla limpios	11.2.9	Puesto y pantalla limpia	Se procura tergiversación de la Información	Falta bloqueo de sesiones				X	
A12 SEGURIDAD DE LAS OPERACIONES												
A12.1 Procedimientos operacionales y responsabilidades	SI	Procedimientos de operación documentados	12.1.1	Documentación	Documentar los procedimientos de operación,	Documentar con copias de seguridad, infraestructura y conectividad				X	
	SI	Gestión de cambios	12.1.2	Administración de cambios	Controlar los cambios para sistemas Información	Registro y manejo de eventos logs				X	
	NO	Gestión de capacidad	12.1.3	Administración de capacidades	Coste = Beneficio X aplicación de control						X
	NO	Separación de los ambientes de desarrollo, pruebas y operación	12.1.4	Segmentación de unidades de trabajo, programación, testing y operación.	La empresa en sus unidades de trabajo n cuenta con un equipo desarrollador.						X
A12.2 Protección contra códigos maliciosos	SI	Controles contra códigos maliciosos	12.2.1	Controles de virus malicioso.	Se cuenta con un sistema antivirus que se actualiza frecuentemente ofreciendo protección continua los equipos de cómputo.	Verificar consola de antivirus				X	
A12.3 Backup de protección	NO	Respaldo de la información	12.3.1	Almacenamiento seguro de la Información.	Gestión de copias en disco extraíble.	Realizar prueba de restauración				X	

A12.4 Registro y seguimiento actividades sin autorización de procesamiento de información	SI	Registro de eventos	12.4.1	Informe de sucesos	Permite verificar el cumplimiento de seguridad de la Información por los colaboradores.	Implementar herramientas para manejos de eventos.				X	
	SI	Protección de la información de registro	12.4.2	Seguridad de la Información registrada	Controles para accesos detallados protegiendo su integridad.	Implementar herramientas para manejos de eventos				X	
	NO	Registros del administrador y del operador	12.4.3	Informes de Admón. y operación	Al ser Grupo Confeccionistas una PYME no es necesario ejecutar este control.	Implementar herramientas para manejos de eventos				X	
	SI	Sincronización de relojes	12.4.4	Sincronía del reloj	Deben estar sincronizados exactamente para que los registros sean íntegros.	Implementar herramientas para manejos de eventos				X	
A12.5 Control de software operacional	SI	Instalación de software en sistemas operativos	12.5.1	Instalación de programas	Previa autorización para instalación de programas por expertos en los PC.					X	
A12.6 Gestión de la vulnerabilidad técnica.	SI	Gestión de las vulnerabilidades técnicas	12.6.1	Vulnerabilidad en aspectos técnicos.	Instalación oportuna de actualizaciones en equipos informáticos	Plan de remediación de vulnerabilidades.				X	

	SI	Restricciones sobre la instalación de software	12.6.2	Denegación en la instalación de programas	Los usuarios estándar no cuentan con privilegios de administrador para realizar instalaciones.	Implementar herramientas de monitorio y administración de software				X	
A12.7 Consideraciones sobre auditorias de sistemas de información	SI	Controles de auditorías de sistemas de información	12.7.1	Auditorias en los Sistemas de información	No aplica para disminución de los riesgos evaluados.	Auditorías SGSI		X			
A13 SEGURIDAD DE LAS COMUNICACIONES											
A13.1 Gestión de la seguridad de las redes.	SI	Controles de redes	13.1.1	Operatividad de la red	La empresa entre sus dispositivos de comunicación cuenta con un firewall que tiene funciones de Router para las comunicaciones.	Reforzar los controles de seguridad				X	
	SI	Seguridad de los servicios de red	13.1.2	Protección de la red	Se incluyen los parámetros en cualquier contrato con externos de los niveles de servicio.	Reforzar los controles de seguridad				X	
	SI	Separación en las redes	13.1.3	División de las redes	Separación de los servicios a nivel de servidor para que no causen	Reforzar los controles de seguridad				X	

					afectación a la red.						
A13.2 Transferencia de información	NO	Políticas y procedimientos de transferencia de información	13.2.1	Políticas y procedimientos de alteración de la Información	Políticas de Seguridad de la Información	Implementar procedimientos del SGSI				X	
	SI	Acuerdos sobre transferencia de información	13.2.2	Lineamientos de intercambio de Información	Entre la empresa Grupo Confeccionistas T y los proveedores se establecen acuerdos de confidencialidad.	Establecer procedimientos para asegurar trazabilidad y no repudio.		X			
	SI	Mensajería Electrónica	13.2.3	Correos Electrónicos	Los aplicativos y dispositivos de seguridad proporcionan una adecuada seguridad en los correos electrónicos.						
	SI	Acuerdos de confidencialidad o de no divulgación	13.2.4	Lineamientos de no divulgación	Se establecen acuerdos de privacidad con los proveedores.			X			
A14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS											
A14.1 Requisitos de seguridad de los sistemas de información	SI	Análisis y especificación de requisitos de seguridad de la información	14.1.1	Requisitos y análisis de los Seguridad de la Información	Especificar controles de seguridad. Por parte de los proveedores en el software realizado.					X	

	SI	Seguridad de servicios de las aplicaciones en redes públicas	14.1.2	Protección de servicios en redes	Especificar controles de seguridad. Por parte de los proveedores en la página realizada.					X	
	SI	Protección de transacciones de los servicios de las aplicaciones.	14.1.3	Protección de servicios de aplicaciones.	Especificar controles de seguridad. Por parte de los proveedores en los ataques web.					X	
A14.2 Seguridad en los procesos de Desarrollo y de Soporte	NO	Política de desarrollo seguro	14.2.1	Política de diseño protegido	La empresa Grupo Confeccionistas no dispone de un equipo desarrollador						X
	SI	Procedimientos de control de cambios en sistemas	14.2.2	Cambios de control en el sistema	Se ha acordado con los proveedores políticas de cambio.			X			
	SI	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	14.2.3	Revisión tras los cambios en el sistema	Revisión continua de las aplicaciones para que no afecte tras el cambio al sistema O.	Pruebas después de cambios o actualizaciones.				X	
	NO	Restricciones en los cambios o los paquetes de software	14.2.4	Bloqueo a los cambios de software	Las modificaciones son nulas en					X	

					los paquetes instalados						
	NO	Principio de Construcción de los Sistemas Seguros	14.2.5	Principios de Ing., en S. Seguros	La empresa Grupo Confeccionistas no dispone de un equipo desarrollador						X
	NO	Ambiente de desarrollo seguro	14.2.6	Entorno seguro	La empresa Grupo Confeccionistas no dispone de un equipo desarrollador						X
	SI	Desarrollo contratado externamente	14.2.7	Tercerización del software	Proveedor externo que se encarga de efectuar el desarrollo de aplicaciones.			X			
	NO	Pruebas de seguridad de sistemas	14.2.8	Prueba de seguridad de sistemas	La empresa Grupo Confeccionistas no dispone de un equipo desarrollador, el proveedor se encarga de hacer las pruebas.						X
	SI	Prueba de aceptación de sistemas	14.2.9	Prueba de aceptación	Se verifica el producto de acuerdo con los parámetros definidos para su aceptación.					X	

A15 RELACIONES CON LOS PROVEEDORES											
A15.1 Gestión de la seguridad de las redes	NO	Política de seguridad de la información para las relaciones con proveedores	15.1.1	Política de relación con proveedores.	El coste de implementación excedería el beneficio obtenido.	Verificar que los proveedores tengan en cuenta los riesgos de SI asociados a la cadena de suministro,		X			
	SI	Tratamiento de la seguridad dentro de los acuerdos con proveedores	15.1.2	Clausulas en contratos con terceros	Se establecen los controles de aseguramiento de la Información.			X			
	NO	Cadena de suministro de tecnología de información y comunicación	15.1.3	Suministro de TICS	El coste de implementación excedería el beneficio obtenido.			X			
A15.2 Gestión de la prestación de servicios de proveedores	SI	Seguimiento y revisión de los servicios de los proveedores	15.2.1	Mitigación de riesgo con el acceso de proveedores a los activos de información				X			
	SI	Gestión del cambio en los servicios de los proveedores	15.2.2	Requisitos de seguridad con cada proveedor que tenga acceso a la empresa		Crear política de seguridad relacionada con el tratamiento de los proveedores de servicios.		X			

A16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION											
A16 Gestión de incidentes y mejoras en la seguridad de la información	SI	Responsabilidades y procedimientos	16.1.1	Responsa, y Procede,	Involucrar a los colaboradores en las incidencias que se puedan generar.	Plan y procedimientos de gestión de incidentes de seguridad de la información				X	
	SI	Reporte de eventos de seguridad de la información	16.1.2	Alerta en los eventos de la Seguridad de la Información	Conveniente para iniciar la administración del evento.	Plan y procedimientos de gestión de incidentes de seguridad de la información				X	
	SI	Reporte de debilidades de seguridad de la información	16.1.3	Alerta de vulnerabilidades de seguridad.	Prevención ante posibles ataques que pongan en riesgo la seguridad.	Plan y procedimientos de gestión de incidentes de seguridad de la información				X	
	SI	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	16.1.4	Selección de eventos de Seguridad de la Información	Definición de términos en cada acción que involucre un evento.	Plan y procedimientos de gestión de incidentes de seguridad de la información				X	
	SI	Respuesta a incidentes de seguridad de la información	16.1.5	Resultado a incidentes de la Seguridad de la Información	Es recomendable para la oportuna resolución de incidencias.	Plan y procedimientos de gestión de incidentes de seguridad de la información				X	
	SI	Aprendizaje obtenido de los	16.1.6	Conocimiento de los	Revisión regularmente	Plan y procedimiento				X	

		incidentes de seguridad de la información		incidentes de Seguridad de la Información	para anticipar consecuencias generadas por los eventos.	s de gestión de incidentes de seguridad de la información						
	SI	Recolección de evidencia	16.1.7	Resumen de evidencias	Se efectúa el respectivo registro a causa de las evidencias presentadas en las actividades.	Plan y procedimiento s de gestión de incidentes de seguridad de la información				X		
A 17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD												
A17.1 Continuidad de Seguridad de la información	SI	Planificación de la continuidad de la seguridad de la información	17.1.1	Preparación de la continuidad de la Seguridad de la Información	Primordial para detectar vulnerabilidad es en las operaciones.	Actualizar de plan de contingencia				X		
	SI	Implementación de la continuidad de la seguridad de la información	17.1.2	Ejecución de la continuidad de la Seguridad de la Información	Primordial para mantener la continuidad de las actividades.	Actualizar de plan de contingencia				X		
	SI	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	17.1.3	Comprobació n, identificación y evaluación de la continuidad de la Seguridad de la Información	Primordial para identificar la continuidad de las actividades	Actualizar de plan de contingencia				X		
A17.2 Continuidad de Seguridad de la información	NO	Disponibilidad de instalaciones de procesamiento de información	17.2.1	Disponibilidad de recursos	El coste de implementació n excedería el	Actualizar de plan de contingencia				X		

					beneficio obtenido.						
A18 SEGURIDAD DE LAS COMUNICACIONES											
A18.1 Gestión de la seguridad de las redes	SI	Identificación de la legislación aplicable	18.1.1	Identificación de la legislación	Se identifican las leyes que son consideradas en la empresa.		X				
	SI	Derechos propiedad intelectual (DPI)	18.1.2	Procedimientos adecuados para el cumplimiento de requisitos legislativos.	Licencias y acuerdos de las aplicaciones.		X				
	SI	Protección de registros	18.1.3	Aseguramiento de los registros.	Protección a nivel físico y lógico para mantener seguros los registros.		X				
	SI	Privacidad y protección de información de datos personales	18.1.4	Aseguramiento y privacidad de contacto personal	Se rigen las leyes actuales en concordancia con la protección de información personal.		X				
	NO	Reglamentación de controles criptográficos	18.1.5	Inspección de los controles criptográficos	La empresa no cuenta con herramientas o software para generar encriptación de la información.		X				
	SI	Revisión independiente de	18.2.1	Revisión dedica a la	Práctica de auditorías	Personal experto en				X	

A18.2 Continuidad de Seguridad de la información		la seguridad de la información		Seguridad de la Información	internas para encontrar vulnerabilidades.	auditorias, norma ISO/IEC 27001:2013 para SGSI						
	SI	Cumplimiento con las políticas y normas de seguridad	18.2.2	Culminación de las políticas y normas	Cuando se realizan las auditorias se verifica que se cumpla las respectivas políticas y normas	Personal experto en auditorias, norma ISO/IEC 27001:2013 para SGSI				X		
	SI	Revisión del cumplimiento técnico	18.2.3	Afirmación del cumplimiento técnico	Revisión periódica para verificar el cumplimiento de políticas y normas de seguridad de información.					X		

Fuente: Autor de la propuesta. Basado en: BERRÍOS MESÍA, César Augusto y ROCHA CAM, Martín Augusto. [en línea]. Propuesta de un modelo de sistema de gestión de la seguridad de la información en una pyme basado en la norma ISO/IEC 27001. [Consultado el 9 de junio de 2021]. Disponible en: http://hdl.handle.net/10757/581891, y INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Código de prácticas para controles de seguridad de la información. GTC-ISO-IEC 27002:2015. Bogotá D.C.: ICONTEC, 2015. 107 p

Anexo E

QUIENES SOMOS

Empresa colombiana dedicada a la confección de ropa para bebe, ropa infantil y ropa para dama en TEJIDO DE PUNTO. Contamos con 20 años de experiencia en la confección de alta calidad para satisfacer las necesidades del mercado nacional. La producción diaria de Grupo Confeccionistas es de 8.000 prendas (con capacidad de producir un total de 18.000 prendas diarias), las cuales son elaboradas y supervisadas por personal altamente calificado –alrededor de 120 personas- en un turno de trabajo.

MISIÓN

Ser una organización que satisfaga oportunamente los gustos y necesidades y expectativas de comodidad y bienestar de los consumidores, a través de las acciones de eficiencia, calidad, innovación de diseño, servicio y con responsabilidad frente a los accionistas y colaboradores.

VISIÓN

Ser una empresa reconocida por su competitividad, tecnología e innovación llegando a consolidarse como una de las más rentables y eficientes d
el sector, cuyas confecciones sean unas de las opciones preferidas por el consumidor colombiano y participando destacadamente en los mercados internacionales.

Adicionalmente la empresa cuenta con políticas de seguridad y salud en el trabajo, destacando el talento humano, la protección del medio ambiente y las pautas para un buen clima laboral.

Ilustración 11. Políticas SGS

POLITICA DE SEGURIDAD Y SALUD EN EL TRABAJO

GICO LTDA CONFECCIONES S.A.S., en sus actividades diarias reconoce la importancia del capital humano, técnico, financiero y se compromete a nivel gerencial con el diseño, planificación, implementación y mejora continua del Sistema de Gestión de Seguridad y Salud en el Trabajo. El cual va encaminado a promover y mantener el bienestar físico, mental y social de los trabajadores, contratistas, subcontratistas y demás partes interesadas ofreciendo lugares de trabajo seguros y adecuados.

En concordancia con lo anterior, contempla los siguientes objetivos:

- Cumplir la normatividad Nacional vigente aplicable en materia de riesgos laborales.
- Identificar los peligros, evaluar y valorar los riesgos y establecer los respectivos controles.
- Proteger la seguridad y salud de todos los trabajadores, mediante la mejora continua del SG SST.
- Responder oportunamente las inquietudes que provengan de las partes interesadas.
- Prevenir los accidentes de trabajo y las enfermedades laborales
- Destinar los recursos humanos, físicos y financieros necesarios para el Sg-SST

La presente política será divulgada a todos los niveles jerárquicos de la Empresa y deberá ser actualizada, de acuerdo a los requerimientos o cambios en materia de seguridad y salud en el trabajo, mínimo se revisará una vez al año y el cumplimiento es obligatorio, para todos los trabajadores, contratistas, subcontratistas, visitantes y demás partes interesadas.

Comuníquese, publíquese y cúmplase.

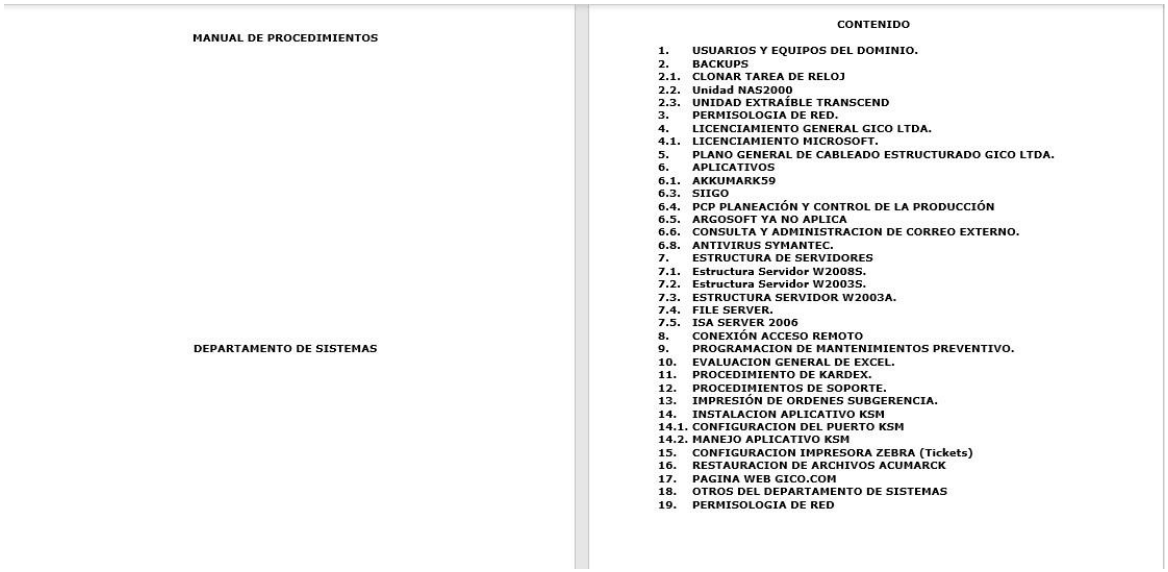
Bogotá, Agosto 17 de 2018

POLITICA	OBJETIVO DE SST	DESPLIEGUE DEL PLAN	INDICADOR / DEFINICION	META	PERIODICIDAD DE LA MEDICION
GICO LTDA CONFECCIONES S.A.S., en sus actividades diarias reconoce la importancia del capital humano, técnico, financiero y se compromete a nivel gerencial con el diseño, planificación, implementación y mejora continua del Sistema de Gestión de Seguridad y Salud en el trabajo. El cual va encaminado a promover y mantener el bienestar físico, mental y social de los trabajadores, contratistas, subcontratistas y demás partes interesadas ofreciendo lugares de trabajo seguros y adecuados.	Cumplir efectivamente con los requisitos de ley establecidos y demas disposiciones del SG-SST	Plan Anual	No Conformidades en Auditoria del SGSST: No de NC/No de Items del SGSST *100	100%	x Ciclo de Auditoria
	Identificar, mitigar, controlar y prevenir los riesgos existentes.	Matriz de Peligros	Indicador de accidentalidad	0,50%	Mensual
	Identificar, evaluar e intervenir los riesgos presentes en las actividades laborales, que puedan generar accidentes de trabajo	Matriz de Peligros	Cumplimiento del Plan de Trabajo: No de Actividades Ejecutadas/No de Actividades Programadas	90,00%	Mensual
	Garantizar condiciones optimas de salud de los colaboradores en el ambito laboral	Plan Anual			
	Proteger la integridad de los clientes, colaboradoradores, contratistas y visitantes durante las situaciones de emergencia	Plan de Emergencias	Cumplimiento a las actividades del Plan de Emergencias No de Actividades Ejecutadas/No de Actividades Programadas	90,00%	Mensual

Fuente: Autoría propia.

En cuanto a la GSI, se presenta un manual del área de sistemas del año 2018 que esta desactualizado, donde algunas aplicaciones y procedimientos ya no se ejecutan, el inventario de equipos se realizó por última en el año 2016 y no se han tenido en cuenta nueva incorporaciones y actualizaciones, tampoco se ha definido una estandarización o SGSI que permita un mayor control sobre los riesgos ligados a los activos e información presentes.

Ilustración 12. Manual de Sistemas 2018 empresa Grupo Confeccionistas.



MANUAL DE PROCEDIMIENTOS

DEPARTAMENTO DE SISTEMAS

CONTENIDO

Fuente: Autoría propia.

Seguridad en instalaciones.

La empresa tiene un sistema de cámaras CCVT para vigilancia, donde el DVR principal se encuentra en la oficina de gerencia donde se pueden observar las diferentes áreas de la empresa como lo son:

- Cámara de vigilancia área de parqueaderos.
- Cámara de vigilancia área de bordado.
- Cámara de vigilancia área de bodega pasillo.
- Cámara de vigilancia área diseño.
- Cámara de vigilancia área de producción.
- Cámara de vigilancia área externa de la empresa control vehicular y puerta de ingreso.

Ilustración 13. Cámara de vigilancia área de parqueadero.

Fuente: Autoría propia.

Para ingresar a las instalaciones de la empresa, se realiza de la siguiente manera:

- A través de citófono donde se anuncia la llegada a la recepcionista.
- Inmediatamente verifica que el visitante tenga acceso o haga parte de los operadores y funcionarios de la empresa.
- Anuncia la vigilante para que realice apertura de la puerta principal y permita su ingreso.
- Al ingresar se debe autenticar con la tarjeta asignada de ingreso para marca su entrada.
- Para visitas técnicas o proveedores, se debe programar con antelación para disponer de los recursos y personal para su atención.

Ilustración 14. Puerta principal y sistema Biométrico.

Fuente: Autoría propia.

Seguridad activos tecnológicos.

- Seguridad empresarial.

Teniendo en cuenta que no se dispone de una política definida ni un SGSI para formalizar la seguridad en los activos al ingresar un funcionario, Recursos Humanos informa al área de sistemas la incorporación y se realiza el siguiente procedimiento:

- Se realiza una breve inducción al usuario sobre el manejo de la red, impresoras y equipo de cómputo asignado.
- Se asigna un usuario y contraseña con el respectivo rol de acuerdo con sus funciones y accesos a la red que se entrega impresa para su conocimiento y la cual debe firmar para ser archivada.
- Se le indica al usuario donde quedan las impresoras y áreas comunes, también en caso de presentar fallas la extensión de sistemas o la ubicación de la oficina para que se acerque personalmente e informe los inconvenientes.
- Se le asigna un usuario de correo que se gestiona a través del navegador web, se le indica como ingresar y su contraseña, que generalmente es la misma del usuario para iniciar sesión en su computador.
- Al retirarse el funcionario Recursos Humanos informa al área de sistemas y desde allí se da de baja al usuario y se cambia su contraseña, también se verifica que los elementos informáticos se encuentren completos y en buen estado.

- Seguridad en áreas de trabajo

Grupo Confeccionista su mayor parte de gestión en sus sistemas son de Windows por lo que a través del server Windows 2008 R2, establece políticas locales a nivel de red y por dominio en cada estación de trabajo teniendo en cuenta:

- Incluir las máquinas en el dominio gicoltda.com.
- Sincronizar el reloj de manera automática.
- Gestión de contraseñas a través del Directorio Activo.
- Bloquear las cuentas de usuario desde el servidor.
- Establecimiento de tiempo para bloqueos de sesión automáticos.
- Registro de eventos en los logs del servidor.
- Servicios de red y recursos compartidos.
- Autorización de una cuenta administradora para instalación y cambios del sistema.
- Comunicación entre cliente y server.

Para el caso de la seguridad en el Datacenter es mínima, su acceso no está restringido y establecido un control de acceso, por lo que existe un riesgo de manipulación por personal a parte del área de sistemas.

El rack de sistemas su chapa se encuentra averiada, los servidores están en un mueble que no posee seguridad.

Las demás estaciones de trabajo tampoco cuentan con un sistema de seguridad adecuada, no poseen guayas o algún mecanismo de protección ante eventuales pérdidas, solo se monitorea esporádicamente a través de las cámaras de vigilancia y en las áreas donde estén presentes.

Ilustración 15. Seguridad en Datacenter.

Fuente: Autoría propia.

Ilustración 16. Seguridad en estaciones de trabajo.

Fuente: Autoría propia.

- Entradas o salidas de equipos

En el caso de requerirse enviar un equipo a soporte especializado se realiza a través de un acta sencilla para su salida en portería y conocimiento de la administradora de la empresa, donde se informa el serial del equipo, su modelo y la descripción de la falla, igual a donde requiere enviarse.

- Seguridad de las estaciones de energía

- Se cuenta con una UPS que garantiza que, al ocasionarse fallas de luz, se disponga del tiempo necesario para apagar correctamente los equipos de cómputo y servidores.
- Se verifica continua por parte del personal del área de mecánica de la empresa los servicios de electricidad, tomas corrientes, tensión eléctrica.

- Seguridad del cableado.

La empresa cuenta con un sistema distribuido de canaletas aéreas y de pared, algunos sitios no cuentan con la debida protección, al estar expuesto el cableado.

- Mantenimiento de equipos.

La empresa tiene contratado por prestación de servicios al Ing. John Suárez que el realiza el mantenimiento preventivo y correctivo en los computadores de la siguiente manera:

- Computadores de escritorio cada 4 meses.
- Servidores cada 6 meses.
- Impresoras se envían a proveedor externo para mantenimiento y reparación.

Al finalizar se registrar en un archivo cual fue le procedimiento realizado, la fecha de ejecución y la próxima fecha de mantenimiento.

- Dispositivos extraíbles

No hay política definida para su tratamiento, solamente a través del servidor de correo Symantec, se controla el bloqueo de los dispositivos en algunas áreas y computadores por solicitud de los funcionarios.

- Sistemas de información

La empresa grupo confeccionistas cuenta con los siguientes aplicativos para la ejecución de actividades de producción:

- PCP. Planeación y Control, tiene usuarios predefinidos y con una única contraseña, no se cuenta con soporte por parte del fabricante debido a que el programa es de una versión muy anterior (año 2002).
- SIIGO: Se empela en contabilidad y Gestión Humana para registros financieros e información de pedidos y proveedores y gestionar la nómina, tienen asignados tres usuarios para la contadora, auxiliar contable y jefe de recursos humanos, su versión es actual y en caso de inconvenientes y falla se contacta a soporte de SIIGO y a través de team viewer se conecta y resuelven las incidencias y requerimientos.
- Akkumark: Es un aplicativo con el que se realizan los diseños de las prendas que confecciona Grupo Confeccionistas. En el Aplicativo Akkumark se cuenta con llaves únicas de registro para cada computador, se disponen de tres licencias y en caso de fallas o soporte se contacta con el proveedor para que solucionen a través de línea telefónica o presencialmente.
- Página web: Anteriormente se realizaban ventas por internet, pero ha estado sin administración y tampoco se realizan ventas por medio de ellas, se encuentra desactualizada y sin ningún tipo de soporte.
- Correo electrónico: Se gestiona a través de un hosting del proveedor GoDaddy, donde están alojadas las cuentas de correo, desde allí se administran los usuarios se crean, eliminan y se amplían los buzones de correo.

- Seguridad en redes y comunicaciones.

La empresa no cuenta un equipo de desarrollo de aplicaciones, por ende, la red solo está configurada a nivel básico para operar con recursos compartidos de archivos, impresoras y usuarios.

Algunas opciones de seguridad con las que cuenta son:

- Los roles de usuarios se encuentran agrupados por áreas.
- Se asignan permisos a las carpetas dependiendo del usuario.
- Los Backup se almacenan es un disco extraíble que se conecta al servidor principal, se ejecuta todos los días y no cuenta con protección ni resguardo.
- Las claves de usuario se cambian manualmente desde el directorio activo y se realiza cuando el jefe de recursos humanos lo cree conveniente.

En el anexo A se presentan los planos del cableado estructurado en las instalaciones de Grupo Confeccionistas.

Cuadro 40. RAE

Fecha de Realización:	15/10/2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Gestión de Sistemas
Título:	Diseño de la fase de planeación para el Sistema de Gestión de Seguridad de la Información a partir de la norma ISO/IEC 27001:2013 para la empresa Grupo Confeccionistas.
Autor(es):	SUAREZ CASTRO, John Edwin
Palabras Claves:	Activos de información, Sistema de Gestión de Seguridad de la información, Riesgos, Vulnerabilidades
Descripción:	En la actualidad la empresa Grupo confeccionistas no tiene un análisis de los procesos que administra destacándose los aplicativos de SIIGO, PCP, AKKUMARK. No ha definido un alcance en la gestión de TI, las políticas de seguridad son escasas y no proporcionan confiabilidad en la seguridad y análisis de la información, el inventario de activos se encuentra incompleto, desactualizado y carece de una asignación, no se ha identificado y realizado plenamente una gestión de riesgos que están presentes en la empresa. Al diseñar un SGSI (Sistemas de Gestión de Seguridad de la Información) se pretende un monitoreo, gestión y administración de los objetivos propuestos de la empresa, de modo que se evitaron los riesgos en los activos de información que se presentan en la empresa Grupo Confeccionistas. Por medio del ciclo de gestión PHVA, se analiza el contexto de la organización que permita determinar los requisitos tanto internos como externos para el diseño de la fase planear del SGSI, a partir de las políticas y controles que se establecen para dar continuidad a posteriores fases del diseño.
Fuentes bibliográficas destacadas: Se referencian 50 fuentes bibliográficas, entre las cuales destacan: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro l – Método. 2012. [en línea]. Madrid. Dirección	

General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html
ROJAS PEÑA, Hernán Mauricio. Aplicación de la metodología Margarit para el análisis de riesgos de los sistemas de control en la estación Tenay del oleoducto. [en línea]. Trabajo de grado. Universidad Abierta y a Distancia, 2019. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/27758/1075211684.pdf?sequence=1&isAllowed=y
ISO 27001. Objeto y campo de aplicación definición del alcance del SGSI. [Sitio web]. 2021. España. Disponible en: https://normaiso27001.es/objeto-y-campo-de-aplicacion/

DEPARTAMENTO NACIONAL DE PLANEACIÓN. [Sitio web]. Bogotá: Alta Consejería Distrital, Lineamientos de políticas para ciberseguridad y ciberdefensa, CONPES 3701 de 2011. Disponible en: https://tic.bogota.gov.co/transparencia/marco-legal/normatividad/conpes-3701-2011

Contenido del documento:	
Marco Metodológico:	El proyecto aplicado que consiste en la presentación de un Sistema de Gestión de la Seguridad de la Información, donde se evaluarán los sistemas y procesos de la empresa grupo confeccionistas. Tiene una metodología basada en pruebas y experimentos porque se inspeccionará exhaustivamente los sistemas de información, se revisará la documentación existente en la empresa para determinar sobre los métodos de seguridad empleados y se definirán planes de educación cibernética para asegurar el cumplimiento de las políticas de seguridad establecidas. TIPOS DE INVESTIGACIÓN Investigación Exploratoria Por medio de entrevistas y observando el comportamiento dentro de la empresa, se realizará un levantamiento de datos. TÉCNICAS E INSTRUMENTOS DEREOLCECCIÓN DEINFORMACIÓN Las técnicas seleccionadas en este proyecto son: Observación, cuestionario. POBLACIÓN Y MUESTRA

	Población: El proyecto se diseña para la empresa Grupo Confeccionistas S.A.S, ubicado en la ciudad de Bogotá, localidad Engativá, donde se encuentra su sede, se desarrollan todas las actividades de las áreas de producción, diseño, administrativa, etc. Muestra: Se involucran de 15 a 20 personas que laboran en la empresa y que utilizan diariamente equipos de cómputo, aplicaciones, red, recursos compartidos, etc., para aplicar el cuestionario online y reconocer diferentes aspectos, además de los procesos administrativos y operativos de la empresa.
Conceptos adquiridos :	Al realizar una adecuada gestión para evaluar e identificar los activos que hacen parte de la empresa Grupo Confeccionistas, también se puede encontrar los riegos que se asocian a cada activo y como su afectación supondría un alto en las actividades. Levantamiento de información y relacionar los activos con sus directamente responsables, esto con el fin de crear políticas de seguridad para el adecuado uso y manejo de los dispositivos a cargo generando un compromiso con su utilización. Finalmente, al realizar los respectivos cambios después del diseño del SGSI se presentará a la dirección para su análisis y se podrá acordar futuras modificaciones que permitan llevar a cabo una auditoría interna para la mejora continua de la seguridad.
Conclusiones:	• Se establece el alcance del diseño del SGSI para la empresa Grupo Confeccionistas, en base a ello se definen los objetivos, las normas jurídicas que debe tener en cuenta para su implementación y también los procesos que realiza la empresa desde cada departamento, identificando los aspectos principales y falencias para crear las políticas de seguridad que se ajusten con los objetivos planteados. • Se realiza el reconocimiento de cada uno de los activos de información de la empresa Grupo Confeccionistas, identificando las vulnerabilidades y amenazas existentes después de analizar los controles que se ejecutan y los que no, realizando un análisis de riesgos concreto, a partir de las dimensiones de la seguridad que permite evaluar las condiciones actuales y los procesos de la

	empresa en base al desarrollo y ejecución de sus actividades. • Tomando como base la ISO/IEC 27001:2013, se logró realizar una valoración de las amenazas de la empresa y aplicando la metodología Magerit se logró la respectiva identificación, para determinar las condiciones que se estaban cumpliendo dentro de la empresa y cuales no se ejecutaban, a partir de este análisis y evaluación para la continuación del trabajo. • Se propone un cambio a partir de los controles seleccionados para proporcionar de manera íntegra la seguridad en los procesos y dispositivos que forman parte de la continuidad del negocio de la empresa Grupo Confeccionistas, permitiendo el análisis por parte de los directivos y así establecer los mecanismos más adecuados que mitiguen los riesgos y las vulnerabilidades y proporcionen la debida seguridad de la información. • Se diseñan las políticas de seguridad de la información, a partir de la evaluación y selección de controles, donde se tienen en cuenta las diferentes afectaciones y procesos que no se ejecutan adecuadamente por no estar establecido un Sistema de Seguridad de la Información que establezca un control optimo, sobe el tratamiento de los activos y la información para establecer proceso efectivos y óptimos en base a la norma ISO/IEC 27001:2013 y la ISO/IEC 27002:2007

10 AUTORIZACIONES EMPRESA GICO LTDA

10.1 AUTORIZACIÓN JEFE INMEDIATO

Bogotá, 26 de Julio de 2021

Señor(a):
Beyanire Sánchez Espejo
Administradora en jefe

Asunto: Autorización para la ejecución del proyecto titulado: Diseño de Políticas y Controles de las fases Planear y Hacer de un sistema de Gestión de Seguridad en base a la norma ISO/IEC 27001:2013 para el fortalecimiento de la seguridad de la información de la empresa GICO LTDA Confecciones S.A.S

Cordial saludo estimado Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia “UNAD”. Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a nombre de GICO LTDA Confecciones S.A.S, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: Diseño de Políticas y Controles de las fases Planear y Hacer de un sistema de Gestión de Seguridad en base a la norma ISO/IEC 27001:2013 para el fortalecimiento de la seguridad de la información de la empresa GICO LTDA Confecciones S.A.S el cual se encuentra avalado por parte la Institución de educación superior “UNAD”.

El proyecto en su objetivo general describe lo siguiente: Diseñar un Sistema de Gestión de Seguridad en sus fases planear y hacer en base a la norma ISO/IEC 27001:2013, que garantice la protección de los activos y la información de la empresa GICO LTDA Confecciones S.A.S"; al mismo tiempo será apoyado por los objetivos específicos:

- Valorar el estado actual de la empresa grupo confeccionistas a partir de informes y lectura de documentos para conocer la integridad, disponibilidad y confiabilidad de la información.
- Evaluar los activos de información mediante la aplicación de una metodología que permita el análisis y gestión de riesgos de la empresa grupo confeccionistas.
- Proponer un documento de declaración de aplicabilidad a partir del informe de análisis de riesgos para establecer los dominios y controles de seguridad que se deben aplicar en la empresa.
- Diseñar las políticas y controles de seguridad mediante la adopción de buenas prácticas que permitan reducir los riesgos en los activos de información.

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transaparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por GICO LTDA Confecciones S.A.S
- La empresa GICO LTDA Confecciones S.A.S deberá establecer qué tipo de información es privada y cuál es pública para delimintar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de pruebas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.

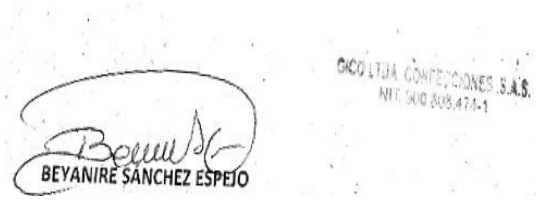
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia “UNAD”. El documento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrera profesional.

Firman en Bogotá D.C., a los (26) días del mes de (julio) de 2021

Cordialmente,

John Edwin Suárez
Estudiante UNAD



Beyanire Sánchez Espejo
Administradora

10.2 ACUERDO DE CONFIDENCIALIDAD ENTRE EMPRESA Y ESTUDIANTE.

ACUERDO DE CONFIDENCIALIDAD ENTRE John Edwin Suárez Castro y Gico LTDA Confecciones S.A.S

Por la **parte reveladora**
Nombre: GICO LTDA Confecciones S.A.S
Dirección: Calle 71ª N°. 73ª - 53
Teléfono: 390 29 37
E-mail: bsanchez@gicoltda.com

Por la parte **receptora de la información**
Nombre: John Edwin Suárez Castro
Dirección: Carrera 95 J Bis # 91 A - 56
Teléfono: 300 717 67 99
E-mail: john.suarez49@gmail.com

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a la GICO LTDA Confecciones S.A.S**,** y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto *aplicado* Diseño de un Sistema de Gestión de la Seguridad de la Información, donde se evaluarán y se tratarán los riesgos de los sistemas y procesos de la empresa *GICO* LTDA Confecciones S.A.S

2. Que la información de propiedad de *GICO* LTDA Confecciones S.A.S ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera

   único y confidencial, o que es objeto de protección a título de secreto industrial.

   Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de investigación Diseño de Políticas Y Controles de las Fases Planear Y Hacer de un Sistema de Gestión de seguridad en base a la norma ISO/IEC 27001:2013 para el fortalecimiento de la seguridad de la información de la empresa *GICO* LTDA Confecciones S.A.S.

3. *GICO* LTDA Confecciones S.A.S*, John Edwin Suárez* que para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de *GICO* LTDA Confecciones S.A.S.

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente al *GICO* LTDA Confecciones S.A.S**,** así como también a no utilizar dicha

información en beneficio propio ni de terceros, sólo con fines estadísticos y de mejoramiento de la *GICO* LTDA Confecciones S.A.S**.**

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto Diseño de Políticas Y Controles de las Fases Planear Y Hacer de un Sistema de Gestión de seguridad en base a la norma ISO/IEC 27001:2013 para el fortalecimiento de la seguridad de la información de la empresa *GICO* LTDA Confecciones S.A.S. lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de esta o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma *GICO* LTDA Confecciones S.A.S**,** restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de *la empresa GICO* LTDA Confecciones S.A.S**.**

9. La **parte receptora** se compromete a establecer que los datos a utilizar son: *Topología de la red, sistemas actuales de información, pool de direcciones IP para simulaciones.*

10. La información capturada por la **parte receptora** se observará como *cifras para estudio estadístico, comparativo, información cualitativa…*, no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad toda la persona *GICO* LTDA Confecciones S.A.S**.** no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de *GICO* LTDA Confecciones S.A.S**,** ni violentará la ley de delitos informáticos Colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. El estudiante *John Edwin Suárez Castro* se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa *GICO* LTDA Confecciones S.A.S para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el repositorio institucional y de acceso público.

14. El título del proyecto no podrá contener el nombre de la empresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de esta para la determinación de sus alcances, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en

desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

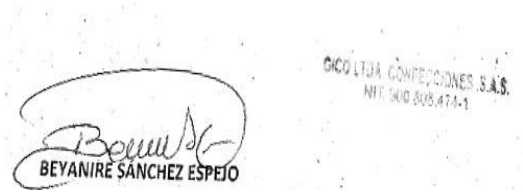
Octava. Solución de controversias: Las partes *(John Edwin Suárez Castro – GICO* LTDA Confecciones S.A.S*)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las cláusulas del presente acuerdo de confidencialidad por parte de *John Edwin Suárez Castro*.

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bogotá D.C., a los (8) días del mes de (julio) de 2021

Como Parte Receptora: **Por la parte reveladora:**



John Edwin Suárez Castro
Estudiante UNAD.
C.C. No.1.026.255.575 de Bogotá

Beyanire Sánchez Espejo
GICO LTDA Confecciones S.A.S
NIT: 900.808.474-1