UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

SUBLÍNEA DE INVESTIGACIÓN: Normas y Estándares

AUTOR: Tigse Moposita Jorge Luis

TUTOR: Ing. Franklin Mayorga Mg.

Ambato - Ecuador

Enero, 2020

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.", del señor Tigse Moposita Jorge Luis, estudiante dela Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe final reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato, enero de 2020

EL TUTOR

Ing. Franklin Mayorga, Mg.

AUTORÍA DEL TRABAJO

El presente Proyecto de Investigación titulado: "PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.", es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, enero de 2020

Jorge Luis Tigse Moposita

CC. 1804766796

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los Derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, enero de 2020

Jorge Luis Tigse Moposita

CC. 1804766796

APROBACIÓN DEL TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Félix Fernández PhD. y Dr. Víctor Guachimbosa PhD., revisó y aprobó el Informe Final del Proyecto de Investigación titulado "PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.", presentado por el señor Jorge Luis Tigse Moposita de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. Elsa Pilar Urrutia, Mg.
PRESIDENTA ENCARGADA DEL TRIBUNAL

Ing. Félix Fernández PhD.
DOCENTE CALIFICADOR

Dr. Víctor Guachimbosa PhD.
DOCENTE CALIFICADOR

DEDICATORIA

En primer lugar lo quiero dedicar a Dios, quien me brindó sabiduría y constancia a lo largo de mi carrera universitaria.

En segundo lugar a mi familia ya que con amor, paciencia y fortaleza guiaron cada momento de mi vida, pero de manera especial a mi madre Gladys, pilar fundamental en mi formación tanto personal como académica, y a mi padre Jorge que siempre ha estado en mi pensamiento que es y será mi ángel en cielo.

De igual manera a mis amigos y compañeros quienes me brindaron su apoyo incondicional en todo momento y con quienes compartimos momentos inolvidables.

Además quiero dedicarle a una persona muy especial en mi vida Shirley ❤, que por su apoyo y cariño incondicional en el ámbito personal y académico siempre motivándome a mejorar y cumplir mis objetivos.

Jorge Luis Tigse Moposita

AGRADECIMIENTO

Un sincero agradecimiento a la Universidad Técnica de Ambato y en especial a la Facultad de Ingeniería en Sistemas, Electrónica e Industrial la cual me brindó la oportunidad de formarme profesionalmente.

A todos los docentes de la carrera de Ingeniería en Sistemas Computacionales e Informáticos, que con su sabiduría y apoyo que me brindaron pude terminar mi formación académica.

A Plasticaucho Industrial, por permitirme realizar mi proyecto de investigación y que me ayudaron a desarrollar en el campo profesional.

De manera especial a mi tutor de tesis el Ing. Franklin Mayorga por su apoyo y asesoramiento durante el desarrollo mi proyecto de investigación.

Jorge Luis Tigse Moposita

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICO

RESUMEN EJECUTIVO

La empresa “Plasticaucho Industrial S.A.” dedicada a la producción de calzado en varias líneas como: casual, escolar, deportivo, industrial, entre otras, tiene su matriz en la ciudad de Ambato, se encuentra en constante crecimiento tanto a nivel del Ecuador como a nivel internacional en Colombia y Perú, de esta manera requiere contar con personal ampliamente capacitado y recursos que permitan ofrecer productos de calidad de manera eficiente y segura.

La tecnología se encuentra en constante desarrollo por lo que es importante mantener actualizado los procesos de seguridad dentro de la empresa, verificando y corrigiendo errores que puedan poner en peligro la información relevante de la entidad, por lo cual existe la necesidad de adaptarse a un modelo de gestión de la información de acuerdo a Normas Internacionales que permitan el control y manejo de datos con total integridad.

Plasticaucho Industrial S.A. cuenta con políticas de gestión de la información, pero las mismas deben ser analizadas para su control y si se da cumplimiento por parte de los usuarios, además determinar una metodología que pueda ser adaptado a la Norma Internacional ISO 27001 para gestionar la seguridad de los datos, de esta manera obtener una Certificación Internacional para la empresa que le dará más fortaleza y seguridad ante sus competencias.

El diseño de un Plan de Gestión de Seguridad Informática basado en la Norma ISO 27001 que se plantea en el presente proyecto permitirá analizar las fortalezas, debilidades y determinar un plan de acción ante un problema que pueda tener a futuro la empresa en la cual puede quedar expuesta la integridad de sus datos.

ABSTRACT

The company "Plasticaucho Industrial SA" faces the production of footwear in several lines such as: casual, school, sports, industrial, among others, has its headquarters in the city of Ambato, is constantly growing both at the level of Ecuador and at an international level in Colombia and Peru, this way requires trained personnel and resources that can offer quality products efficiently and safely.

The technology is in constant development, so it is important to keep the security processes within the company updated, verifying and correcting errors that may jeopardize the relevant information of the entity, so there is a need to need a model of Information management according to International Standards that control the control and management of data with complete integrity.

Plasticaucho Industrial SA has information management policies, but they must be analyzed for control and if it is complied with by users, it will also determine a methodology that can be adapted to the International Standard ISO 27001 to manage security of the data, in this way obtain an International Certification for the company that will receive more strength and security before their competences.

The design of a Computer Security Management Plan based on the ISO 27001 Standard that is presented in this project that analyzes the strengths, weaknesses and determine an action plan for a problem that the company may have a future in which it can remain Exposed the integrity of your data.

INTRODUCCIÓN

El presente trabajo tiene como principal objetivo realizar un Plan de Gestión de Seguridad Informática para el departamento de Tecnología dela Información en la empresa Plasticaucho Industrial, se lo efectúo mediante la aplicación de la norma ISO 27001 que permite el aseguramiento, la confidencialidad e integridad de los datos, así como de los sistemas que lo procesan dentro de la organización; en esta empresa anteriormente se realizó un proyecto de tesis para crear un plan de riesgos y contingencias informáticas, la cual sirvió de apoyo para continuar con la investigación propuesta.

La importancia de este proyecto radica es que se pudo realizar una valoración de los controles y las políticas que se aplican en el departamento de TI de la empresa, esto se llevó a cabo mediante la recolección de información con técnicas como la observación, entrevista y encuesta a las personas que intervienen en el proceso del departamento de Tecnología de la información. Con el análisis realizado se procedió a la aplicación de la Norma ISO 27001 con sus respectivos controles, teniendo como resultado un Plan de Gestión de Seguridad Informática en donde se describen políticas de seguridad de la información y tener un mejor uso de las Tecnologías de la información y Comunicación (TIC) que la empresa maneja internamente.

El presente proyecto cuyo nombre está denominado "PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.", está estructurado por 5 capítulos que se detallan a continuación:

Capítulo I. "El Problema", se expone el problema a investigar y su contextualización a nivel maso, meso, micro, además la justificación del origen de la investigación y en donde se establece los objetivos a cumplir durante el desarrollo del proyecto.

Capítulo II. "Marco teórico", se recopila los antecedentes investigativos relacionados al proyecto, también se encuentra fundamentación teórica.

Capítulo III. "Metodología", se describe las modalidades que son aplicadas en la investigación, así como los procedimientos para la recolección y procesamiento de la

información que servirán para cumplir con los objetivos definidos, y el proceso de desarrollo del proyecto.

Capítulo IV. "Desarrollo de la Propuesta", constituye las actividades llevadas a cabo durante el desarrollo e implementación de la propuesta de solución, su discusión, así como los resultados y su interpretación.

Capítulo V. "Conclusiones y Recomendaciones", se plantean las respectivas conclusiones y recomendaciones a la que el investigador llegó posterior al desarrollo del proyecto y obtención de resultados.

Al final, se incluyen referencias bibliográficas consultadas, anexos de entrevistas y encuestas que se realizaron en el transcurso de desarrollo del proyecto de investigación para la empresa Plasticaucho Industrial S.A.

CAPÍTULO I

EL PROBLEMA

1.1 Tema de investigación

"PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A."

1.2 Planteamiento del problema

Un plan de gestión de seguridad informática en base a reglas establecidas es de real relevancia en una empresa, ganando seguridad en sus datos. Es así que surgen a nivel internacional normas estandarizadas que se pueden adaptar para el manejo de grandes y pequeñas cantidades de información, las mismas que son importantes para que una empresa pueda llevar a cabo sus actividades.

En Europa por ejemplo posterior a tener problemas de robo de datos a empresas como Uber, debido a anticuadas directrices que desde años atrás no se actualizan dando como resultado la pérdida de control de información. Al no tener un plan de normas de seguridad, la UE (Unión Europea) analiza la regulación de leyes que protejan y conlleven sanciones a implicados en acciones ilícitas en contra de empresas a nivel internacional [1].

Un estudio denominado "State of the Internet/Security Report Q3 2017", realizado por la empresa SeachDataCenter en Español donde se determinó un aumento de los ataques a la seguridad de la información en un 69% en ese período. Los ataques de este tipo se originan principalmente en Estados Unidos (38,7%) y Rusia (6,9%),

seguidos de Países Bajos, Ucrania, Brasil, China e India. En América, la mayor parte del tráfico de los ataques fue detectado en Estados Unidos, Brasil, Canadá, México y Perú. Cecilia Pastorino, especialista en seguridad informática de ESET Latinoamérica, destaca que la principal medida que se debe tomar en una empresa al pensar en la seguridad de su información es en un buen sistema que gestione la seguridad. Hoy en día ya no basta con solo aplicar controles de seguridad, sino que resulta necesario trabajar en la gestión de la seguridad. [2]

En Ecuador, por ejemplo el organismo gubernamental CNE (Consejo Nacional Electoral), para los comicios electorales del año 2019 encontró puntos críticos de control de información en el proceso de transmisión de datos correspondientes a resultados de actas y parte que se realiza también en el sistema de escrutinio, el problema se ve reflejado al no aplicar ningún plan de seguridad tecnológico que garantice y permita a los ciudadanos tener una transparente integridad de datos, así también tener en cuentas las fases del sufragio. Además, el CNE al tener acceso a la información personal de todos los ciudadanos en la base de datos del Registro Civil deben mostrar un plan de protección de datos críticos como es el padrón electoral de acuerdo a técnicas que lo permitan mantener en cadena de custodia, así también mediante fases de control poder identificar inconsistencias y sean depuradas a tiempo evitando problemas en comicios futuros [3].

Actualmente la empresa Plasticaucho Industrial, ubicada su matriz en la ciudad de Ambato maneja varios procesos que hace que la información crezca a diario, la misma que se vuelve susceptible a vulnerabilidades. Además de constatar que las TIC y las políticas que disponen no son explotadas en su totalidad ya que no existe una correcta aplicación de los usuarios y administradores del departamento de Tecnología de la información, que posteriormente afectarán tanto a empleados de la empresa como a sus propios clientes con los que interactúan diariamente.

En la empresa Plasticaucho Industrial en anteriores proyectos de investigación, se ha realizado un Plan de riesgos y contingencia informática enfocada en detectar amenazas a los cuales están expuestos los sistemas informáticos para posterior elaborar un plan de contingencia informática [4], además otro proyecto se basó en prácticas de Hacking Ético con el objetivo de evaluar la seguridad informática en la infraestructura de la organización [5], los cuales han sido de gran aporte para la empresa pero los mismos

que necesitan ser reforzados con la aplicación de un Plan de Gestión Informática en donde se especifiquen las políticas de seguridad de la información al que se deban regir los usuarios de la empresa.

Por lo tanto, el problema que radica en la empresa es la carencia de políticas que estén basadas al régimen de las normas estandarizadas internacionalmente para la seguridad de la información, por lo tanto, no se garantiza la confidencialidad, disponibilidad e integridad de los datos que es propiedad de la organización.

1.3 Delimitación

1.3.1 Delimitación de Contenido

Área Académica: Administrativas Informáticas

Línea de Investigación: Normas y Estándares

Sublíneas de investigación: Seguridad de Unidades Informáticas

1.3.2 Delimitación Espacial

La presente investigación se realizará en la empresa PLASTICAUCHO INDUSTRIAL S.A. de la ciudad de Ambato.

1.3.3 Delimitación Temporal

La presente investigación se desarrollará en el periodo septiembre 2018 – febrero 2019.

1.4 Justificación

La investigación se realizó dentro del departamento de TI en la empresa PLASTICAUCHO INDUSTRIAL, en el que se pudo revisar principalmente la carencia y/o reestructuración de normas establecidas para la seguridad de datos. Además, en este estudio se obtuvo información actualizada de procesos de la empresa y así se conoció los problemas que tienen al no contar con un plan de contingencia ante el robo de información. También el desconocimiento de aplicar normas estandarizadas a nivel internacional ha ocasionado tener al personal desactualizado a las nuevas formas de controlar información importante en la empresa.

Al conocer los procesos que manejan en cada planta dentro de la empresa y la importancia de los datos, se estableció el personal que tiene acceso, la cantidad de

información que maneja, la integridad que tiene los datos al momento de ser modificada por el personal; lo que contribuyó al objetivo de la investigación. Se analizó la seguridad del reglamento establecido para autorizar a los usuarios el ingreso a documentos, sea de lectura o escritura que refieren a la productividad de una planta, actividades que son generadas por el personal mediante tickets y son resueltos por parte del departamento de TI.

Con el presente estudio se quiere contribuir en las labores diarias del personal dentro del departamento de TI en la empresa PLASTICAUCHO INSUTRIAL, con la implementación de un Plan de Gestión Informática basado en la Norma ISO 27001 la que permitirá mejorar la seguridad de información combinando los procesos de negocio con la tecnología, considerando las ventajas que tiene esta norma, la cual se puede adaptar a la empresa al ser una entidad que maneja grandes cantidades de información de todas sus plantas ubicadas en el Parque Industrial, Catiglata y además que se maneja datos a nivel internacional de sus sucursales en los países de Colombia y Perú.

El beneficiario principal al implementar el modelo de gestión informática será la empresa con sus respectivos departamentos, integrando políticas y/o normas de seguridad sobre su información y sus activos informáticos, de esta manera poder cumplir con los requerimientos legales que le permitirán a la organización empresarial obtener una ventaja comercial ante sus competidores.

1.5 Objetivos

1.5.1 General

Implementar un plan de gestión de seguridad informática basado en la Norma ISO 27001 para mejorar la seguridad de la información en la empresa PLASTICAUCHO INDUSTRIAL S.A.

1.5.2 Específicos

- Analizar las políticas ya establecidas dentro del departamento de TI para el control de información y la seguridad integrada en cada sistema contratado por la empresa.
- Estudiar la metodología para la aplicación de la Norma Estándar ISO 27001.

- Elaborar un plan de gestión de seguridad informática, integrando los beneficios de la Norma Estándar ISO 27001 aplicable en la empresa PLASTICAUCHO INDUSTRIAL S.A.
- Presentar el Plan de Gestión de Seguridad Informática en el Departamento de TI.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes Investigativos

Para el desarrollo de la propuesta se ha consultado en varios proyectos de investigación enfocados a la implementación de un plan de gestión de seguridad informática basándose en la ISO Estándar 27001.

Joseph Alexander Guamán Seis de la Escuela Superior Politécnica del Litoral ha desarrollado un proyecto de investigación titulado "Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., Utilizando la norma ISO 27001:2013", en el documento analiza el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) estableciendo políticas de seguridad estandarizados a nivel internacional que se ajusten al campo militar y el avance tecnológico, implementando metodologías para evaluar y minimizar riesgos evitando la fuga de información [6].

En la Universidad Central del Ecuador, Diego Alejandro Romero Quevedo ha desarrollado un proyecto de investigación titulado "Implementación de un esquema de seguridad para la red de la Unidad Educativa Particular Cardenal Spellman Femenino", en la que realiza un diagnóstico para la implementación de un esquema de seguridad en la red mediante búsqueda de fallos, técnicas de Hacking Ético y configuraciones de dispositivos de la infraestructura informática basándose en el Esquema Gubernamental

de Seguridad Informática (EGSI) y estableciendo Políticas de Seguridad con Normativas Estándar ISO 27001 [7].

Roberto Lema y Diego Donoso de la Universidad de las Fuerzas Armadas Escuela Politécnica del Ejercito (ESPE), han realizado un proyecto de investigación titulado "Implementación de un Sistema de Gestión de Seguridad de Información basado en la Norma ISO 27001:2013 para el Control Físico y Digital de documentos aplicado a la Empresa Lockers S.A.", en el documento establecen una metodología para la implementación de un SGSI aplicando los requisitos y procedimientos que están establecidos por la Norma ISO 27001:2013 para empresas con el objetivo principal de crear un proceso de negocios que permitan el control físico y digital de documentos. Además de esta manera desarrollar una cultura organizacional de seguridad de información identificando y corrigiendo los riesgos que puedan tener durante las actividades del personal de la empresa [8].

En Colombia, Benjamín José Ramírez Montealegre de la Universidad Nacional de Colombia ha desarrollado un proyecto de investigación titulado "Medición de madurez de Ciberseguridad en MiPymes colombianas" en la cual explica la influencia que tiene al no invertir en seguridad de datos hace que una empresa sea vulnerable a cualquier ataque de personas propias o ajenas a la empresa. MiPymes en Colombia representa al 95% de las empresas en Colombia, el objetivo fundamental que tuvo la investigación fue analizar la situación en relación a la ciberseguridad y las prácticas que tiene el personal ante un ataque sobre su información. Los modelos de madurez son analizados para poder establecer capacidades y nivel de conocimiento en temas de seguridad, también se establece los beneficios de implementar un SGSI evitando tener personal desactualizado con actitudes de organización informal [9].

En España, Jorge Cástulo Guerrón Eras de la Universidad Autónoma de Barcelona (UAB), desarrolló un proyecto de investigación titulado "Plan para la implementación de un Sistema de Gestión de Seguridad de la Información", en el cual se realizó un diagnóstico del ambiente de Seguridad de la información que disponen en sus sistemas, medios de enlace, infraestructura física, y funcionarios del Banco de Loja para posterior establecer controles en base a la norma ISO 27002, los cuales formaran parte de los pilares fundamentales de la seguridad de la información en los activos y los procesos [10].

Iván Alfaro y Edwin Vargas de la Universidad Piloto de Colombia, han realizado un trabajo de investigación titulado “Plan de Seguridad Informática del Sistema de Información Misional de la Procuraduría General de la Nación”, en el documento establecen una metodología para diseñar un plan de seguridad informática mediante la aplicación de buenas prácticas de seguridad para la preservación de confidencialidad, integridad y disponibilidad. Además se realiza la identificación de riesgos asociados al sistema de información misional y establecer controles efectivos que permitan mantener segura la información de la entidad. [11]

2.2 Fundamentación Filosófica

La presente investigación está relacionada en el paradigma Crítico Propositivo, relacionado a lo crítico porque se realiza un análisis de la actual situación del proceso de seguridad de la información de las diferentes áreas que tiene la empresa y establecidas dentro departamento de TI. Propositivo porque se busca plantear una solución, implantado normas y/o políticas para guardar la integridad de los datos dentro de la empresa.

2.3 Fundamentación Legal

La Norma ISO 27001, su origen fue la BS 7799-1, publicada en 1995 de la entidad normalizadora británica British Standards Institution (BSI) con carácter internacional publica normas con el prefijo “BS” con el objetivo de ayudar a las empresas británicas a administrar la Seguridad de la Información [12].

La Norma Estándar ISO/IEC 27001 se basa tanto en el cumplimiento de requisitos legales en seguridad desde el funcionamiento como en el diseño de un SGSI (Sistemas de Gestión de Seguridad de la Información), los cuales deben mantenerse actualizados con un control específico y definidos en documentos que garanticen el cumplimiento total de los requisitos de seguridad. Durante el procedimiento de la investigación se debe establecer el cumplimiento de las siguientes leyes originarias de Europa:

Ley de Protección Intelectual (LPI) que establece la prohibición de copiar, duplicar, transformar parte de los documentos sin permiso de autor. Si se usa software, se los debe adquirir mediante fuentes confiables manteniendo pruebas de propiedad con licencias.

Ley Orgánica de Protección de Datos (LOPD) referida a todos los archivos que contengan datos personales aplicando una protección que corresponda y elaborando documentos de seguridad que establezcan medidas de organización para mantener integridad en los datos.

Ley de Servicios de la Sociedad de la Información (LSSI), en este caso aplicado a empresas que utilicen comercio electrónico las cuales deben ser comunicadas el dominio en el Registro Mercantil y en la página web mostrar datos completos de la empresa como de los productos. [13]

En ecuador, las leyes mencionadas anteriormente son requeridas con el propósito de generar una garantía de que los Planes de Gestión de Seguridad de la Información satisfacen todas las políticas y normas de seguridad de la organización, y el objetivo primordial que se persigue es eludir los incumplimientos de toda obligación legal o contractual en las organizaciones que requieran obtener una certificación ISO 27001.

Además, la Asamblea Nacional de Ecuador aprobó un proyecto realizado por la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación, el cual fue denominado como Código Ingenios en octubre del año 2016, como Nuevo régimen de Propiedad Intelectual, fue la primera normativa que se socializó por medios digitales y que tiene como objetivo promover la investigación responsable, innovación, ciencia y tecnología, saberes ancestrales y tradicionales, talento humano y otros, en el contexto de la protección de los derechos de propiedad intelectual como las marcas, derechos de autor de software, patentes, variedades vegetales y acciones legales [14].

2.4 Fundamentación teórica

2.4.1 Seguridad Informática

La seguridad informática garantiza la integridad, disponibilidad y acceso a la información perteneciente a una entidad, el objetivo principal es mantener el mínimo riesgo sobre los recursos informáticos para garantizar la continuidad de las operaciones de la organización reduciendo costos con una administración estructurada por técnicas administrativas de seguridad, además permite la preservación de documentos, registros y archivos informáticos de la empresa para mantener siempre confiabilidad total.

Las cuatro áreas principales que cubre la seguridad informática:

1. **Confidencialidad**: Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
2. **Integridad**: Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.
3. **Disponibilidad**: Los datos deben estar disponibles para los usuarios cuando sea necesario.
4. **Autenticación**: Estás realmente comunicándote con los que piensas que te estás comunicando.

La seguridad informática es importante para prevenir el robo de datos tales como números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos, etc., que es algo esencial durante las comunicaciones de hoy en día [15].

2.4.2 Amenazas a la Seguridad de la Información

Amenaza se refiere a todo tipo de elemento o acción ocasionada para atentar contra la seguridad de la información, las mismas que surgen al detectar la existencia de vulnerabilidades que pueden ser utilizadas para diversas situaciones sean para perjudicar o robar información. El aumento de vulnerabilidades se da desde el usuario con el uso incorrecto de la tecnología, dado también por diferentes técnicas como ingeniería social, falta de capacitaciones a personal, y el aumento de rentabilidad en ataques

Para conseguir un sistema de información seguro y confiable se establecen una serie de estándares, protocolos, métodos, reglas y técnicas. Sin embargo, existen amenazas que deben tenerse en cuenta:

- **Usuarios**: Se considera la causa del mayor problema ligado a la seguridad de un sistema informático, es así porque con sus acciones podrían ocasionar graves consecuencias.
- **Programas maliciosos**: Conocidos como malware que son destinados a perjudicar un ordenador cuando se instala o hacer uso ilícito de datos.
- **Errores de programación**: Se trata de un mal desarrollo, pero también se tiene que ver como un riesgo evitando que los sistemas operativos y aplicaciones estén sin actualizar.

- **Intrusos**: Cuando personas que no están autorizadas acceden a programas o datos que no deberían.
- **Siniestro**: También se puede perder o deteriorar material informático por una mala manipulación o mala intención, tales situaciones como robo, incendio o inundación.
- **Fallos electrónicos**: Un sistema informático en general puede verse afectado por problemas del suministro eléctrico o por errores lógicos como cualquier otro dispositivo que no es perfecto.
- **Catástrofes naturales**: Rayos, terremotos, inundaciones.
- **Copias de seguridad**: Para proteger de forma eficiente los datos son imprescindibles las copias de seguridad o backups. [16].

2.4.3 Vulnerabilidades

Las vulnerabilidades siendo explícitamente debilidades de un sistema informático y el lugar donde trabajan; la presencia exclusiva de una o varias vulnerabilidades no causan daño por sí mismas, es necesario que exista una amenaza para ser explotada y ocasionar problemas dentro de una organización empresarial, de esta manera se puede considerar que si una vulnerabilidad no tiene ninguna amenaza no será necesario aplicar un control.

Las áreas que se pueden identificar vulnerabilidades son:

- **Organización**: es afectado por ser el lugar físico donde trabajan un conjunto de personas tanto internas como externas.
- **Procesos y procedimientos**: los procesos y procedimientos se verán afectados por su participación en el manejo de la información.
- **Personal**: es el principal responsable de que las vulnerabilidades afecten a la organización por ser el que trabaja y manipula la información sean físicos o lógicos.
- **Ambiente**: se verá afectado el ambiente cuando no se siga lineamientos para mantener un espacio estable y libre de amenazas.
- **Configuraciones de los sistemas de información**: al no existir una correcta configuración de los sistemas de información, se deja abierto una brecha para posibles vulnerabilidades que sean explotadas por personas mal intencionadas.

- **Hardware y Software**: el escoger el tipo de tecnología que se vaya a utilizar para las labores de la empresa, debe ser tomando en cuenta la seguridad que ofrece y los beneficios que se obtiene al utilizarlos.
- **Equipos de comunicación:** es importante considerar la seguridad de los medios de comunicación, ya que en una organización siempre se mantendrá interacción con varios usuarios internos y externos. [17]

2.4.4 Administración de Riesgos

Proceso interactivo e iterativo que se basa en conocer, evaluar y manejar los riesgos con sus respectivos impactos, con la finalidad de mejorar la toma de decisiones dentro de la organización. La administración de riesgos es aplicable en cualquier situación que represente oportunidades de mejora a la empresa, se debe considerar dentro de TI los principales factores que son: seguridades, controles (Preventivos, Detectivos y Correctivos), manuales de usuario y políticas implementadas, para evitar afectaciones a nivel de toda la organización empresarial sobre sus planes comerciales, financieros, administrativos y sistemas.

La aplicación de la norma ISO 27001 en materia de seguridad, la administración de riesgos es uno de los trabajos más importantes cuando queremos definir un proyecto y las iniciativas con las que vamos a mejorar la seguridad de la información en nuestra organización. El objetivo después del análisis de riesgos es poder reducirlos a los que se encuentra expuesta la empresa hasta niveles aceptables a partir de un análisis de la situación inicial. [18]

2.4.5 Plan de Gestión de Seguridad Informática

Un plan de gestión de Seguridad Informática es un conjunto de medios administrativos, medios técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados. El plan de gestión de seguridad informática es el documento básico en donde se establecen los principios organizativos y funcionales de la actividad de seguridad informática para las entidades y aglomera todas la políticas de seguridad y las responsabilidades de los participantes en el proceso informático, y las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo. [11]

2.4.6 Sistemas de Gestión de la Seguridad de la Información (SGSI)

Un SGSI tiene un enfoque sistemático, que es utilizada para la administración de información confidencial de una organización empresarial para mantener la integridad y la seguridad de la misma. Este modelo de gestión de riesgos incluye a todo el personal, procesos internos, procesos externos y los sistemas manejados por el departamento de TI.

Al implementar un SGSI ayuda a las empresas pequeñas, medianas y grandes a mantener seguros los activos de información que permitirá crecer a la empresa en confiabilidad ante sus competidores. [19]

2.4.7 International Organization for Standardization (ISO)

La Organización Internacional de Normalización conocida por la abreviatura ISO es una organización independiente y no gubernamental a nivel internacional que posee varias membresías, su trabajo a través de sus miembros es reunir conocimientos y desarrollar estándares basados en el consenso y relevantes para el mercado, que ayudan en soluciones e innovación para empresas enfrentar desafíos globales [20].

2.4.8 ISO 27001

La Norma Estándar ISO 27001 establecida por La Organización Internacional de Estandarización para la certificación de los sistemas de gestión de seguridad de la información pertenecientes a organizaciones empresariales, al obtener la certificación la empresa puede demostrar la integridad de los datos a sus clientes, accionistas y personal que pertenece a la entidad; de igual manera permite reforzar la seguridad de la información y disminuir los peligros actuales como fraude, pérdida o filtración de datos importantes para una empresa.

Al verificar que una empresa cumple con los requisitos para certificarse con la Norma ISO 27001, será emitido por un organismo de certificación independiente y autorizada la certificación con la cual quedara demostrado que la organización empresarial ha establecido políticas de precaución para proteger la información. [21]

Funcionalidades

- **Evaluación de Seguridad de la Información:** Evaluación de riesgos de los activos de la organización utilizando la metodología designada por la empresa.

- **Controles 27002:** Autoevaluación de los controles mencionados en la norma ISO 27002, para ver en qué estado se encuentra la empresa.
- **Salvaguardas:** Establecimiento de salvaguarda para realizar el Plan de tratamiento de riesgos, estableciendo fechas de puesta en marcha de las mismas y responsabilidades.
- **Métricas e Indicadores:** Seguimiento y medición que permite ver el camino por el que se alcanza a comprobar el estado en el que se encuentra nuestro sistema de gestión.
- **Cuadro de Mando:** Gracias al tratamiento de la información, seremos capaces de poder analizar los datos desde distintos puntos de vista, pudiendo relacionar los distintos indicadores entre sí, mejorando la toma de decisiones.
- **Objetivos y Metas:** Establecimiento de programas de Gestión Laboral.
- **Gestor documental:** Revisión, aprobación, control de cambios y de versiones. Gestión de documentos en vigor/obsoletos. Distribución de documentos. Gestión de registros.
- **Recursos Humanos:** Aseguramiento de las competencias. Definición de puestos y roles. Gestión de currículums. Definición de las responsabilidades y autoridades dentro de la organización.
- **Capacitación:** Establecimiento del Plan de Formación. Evaluación de la eficacia de las acciones tomadas.
- **Procesos:** Enfoque basado en procesos. Descripción de los procesos y su interacción entre ellos. [13]

2.4.9 Implementación ISO 27001

La implementación de la ISO 27001 genera variables de confianza para la gestión en todo su entorno referente a la información, el uso de medidas tecnológicas permite el control y la facilidad de gestión del volumen de la información dentro de las organizaciones en la que se considera lo crítico de los datos dependiendo de su actividad económica. La gestión de la información debe ser analizada para ser puesta a resguardo aplicando políticas que permitan el control adecuado sobre los activos más importantes dentro de la empresa [22].

CAPÍTULO III
METODOLOGÍA

3.1 Modalidad Básica de la Investigación

3.1.1 Modalidad Bibliográfica o Documental

Con el propósito de fortalecer la investigación se recurrirá a obtener investigación teórica de diferentes autores obtenidas en fuentes obtenidas de libros, artículos científicos, tesis desarrolladas en Universidades y documentación interna y externa de la empresa.

3.1.2 Modalidad de Campo

Se considera esta modalidad ya que la investigación se requiere acudir al lugar en donde se desarrollan las actividades de control de la información, la cual se maneja dentro del departamento de Tecnología de la Información para recopilar datos relacionados con los objetivos finales del trabajo. Las técnicas a ser utilizadas serán: entrevistas, encuesta, observación y la norma ISO 27001.

3.2 Población y muestra

Para la investigación e implementación del Plan de Gestión de seguridad Informática dentro del departamento de TI de la empresa, no se requiere muestra ya que solo se trabajará con el personal encargado de los procesos de TI como población, tal como se muestra en la tabla 1.

Tabla 1: Personal de TI

Cargo	Cantidad	Porcentaje
Coordinador de Infraestructura y Soporte	1	20%
Analista de Seguridades TI	1	20%
Gestor Hardware y Software	1	20%

Personal de Soporte TI	2	40%
Total	5	100%

Fuente: Elaboración propia a partir de [23]

3.3 Recolección de Información

Para conocer la situación actual de la empresa Plasticaucho Industrial en temas de seguridad de la información, en el departamento de TI de la empresa, se realizaron entrevistas a las personas que están encargadas del Análisis de seguridades Ing. Alexander Rojas y además a la persona encargada de la Gestión de Hardware y Software Ing. Silvana Garcés, como se muestra en la tabla 2.

3.3.1 Entrevistas sobre la gestión de seguridad informática

3.3.1.1 Entrevista a Analista de Seguridades de TI

Tabla 2: Entrevista a Analista de Seguridades TI

Entrevistado: **Ing. Alexander Rojas** Cargo: **Analista de Seguridades TI**	
PREGUNTAS	**RESPUESTAS**
1. ¿Qué problemas de seguridad informática ha tenido la empresa Plasticaucho Industrial S.A.?	• Ataques en correos electrónicos. • Spam. • Borrado de información.
2. ¿Qué problema fue más perjudicial para la empresa y que aún no se pueda controlar en su totalidad?	• Pérdida de información. • Ataques de spam de dominios filtrados de listas blancas
3. ¿Para mejorar la calidad de seguridad de la información que acciones ha realizado la empresa en conjunto con el departamento de TI?	• La empresa optó por contratar el servicio de terceros para la gestión de la red Wide Area Network (WAN) para la conexión entre plantas ubicadas en Ambato, Quito, Guayaquil, Santo Domingo, Colombia y Perú.

PREGUNTAS	RESPUESTAS
	• Además, la administración de Firewall y Correo electrónico.
4. ¿La empresa cuenta con políticas de seguridad para la proteger la información?	• Existen políticas de seguridad para dar accesos a carpetas de información que se encuentran en los servidores de archivos, además de respaldo de información de usuarios y equipos críticos. • Para los usuarios existen políticas de seguridad personal, los equipos son administrados en Active Directory para la formación de contraseñas, instalación de programas, roles de usuarios, perfiles de navegación los cuales se basan en el perfil tecnológico de la empresa creado por el departamento de Gestión Humana.
5. ¿Cómo es administrada la red interna de Plasticaucho?	• La red Corporativa Plasticaucho está distribuida en VLAN por cada planta lo cual ha permitido una mayor flexibilidad de administración y mejor rendimiento. • La red interna LAN es administrada por el Coordinador de Infraestructura y el Analista de Seguridades de TI.
6. ¿Cómo se encuentra la seguridad física para acceso a los servidores en la empresa?	• El acceso a los servidores se encuentra determinados solo a usuarios autorizados, en el caso de ser personas no autorizadas se deberá llenar una bitácora con sus datos.

PREGUNTAS	RESPUESTAS
	• El espacio físico se encuentra bajo controles biométricos y vigilados por cámaras de seguridad.

Fuente: Elaboración propia

3.3.1.2 Entrevista a Gestor de Hardware y Software

Tabla 3: Entrevista a Gestor de Hardware y Software

Entrevistado: **Ing. Silvana Garcés** Cargo: **Gestor de Hardware y Software**	
PREGUNTAS	**RESPUESTAS**
1. ¿Cómo es la distribución de software y equipos informáticos para el personal de Plasticaucho?	• El personal con el cargo de Gestor de Hardware y Software (Silvana Garcés), es la persona que distribuye los equipos según su cargo y su perfil tecnológico. • En el perfil tecnológico esta descrito las características del equipo y el software que tiene que ser instalado para ejercer sus labores.
2. ¿Todo el software utilizado en la empresa posee licencia?	• Todo el software utilizado en la empresa posee una licencia para su uso. • Existen programas que se instalan cuando su licencia es libre o tienen versiones de prueba.
3. ¿Cuál es el procedimiento de un usuario final para realizar un requerimiento con el departamento de TI?	• El usuario final deberá ingresar al software instalado en el equipo llamado SysAid, el cual es un sistema de generación de tickets Helpdesk en el que se cargará automáticamente con su información (Equipo, usuario) y deberá describir

PREGUNTAS	RESPUESTAS
	su requerimiento de manera detallada que puede ser solo texto o enviar un archivo adjunto. • Posterior el envío de la solicitud se generará un numero de ticket para conocer el estado (Nuevo, en proceso, congelado, cancelado, en espera, cerrado,..) • La solicitud llegara al personal de soporte técnico los cuales se encargarán de atender la solicitud.
4. ¿Cómo se maneja el acceso a la información de los servidores de archivos (NAS) de Plasticaucho?	• La información se encuentra almacenada en carpetas con el nombre del departamento o nombre de la Planta, las mismas que cuentan con administradores que son las únicas personas habilitadas para que mediante un ticket creado en SysAid, dar la autorización de acceso a la información a uno o varios usuarios y a que carpetas. • Los permisos que se pueden otorgar son de lectura o escritura.
5. ¿La empresa cuenta con herramientas para realizar respaldo de información de cada empleado?	• La empresa cuenta con licencias de Office en la que dispone de la nube OneDrive en la que se instala el cliente en el equipo de los empleados que requieran tener respaldado su información y de esa manera se sincronice automáticamente.

Fuente: Elaboración propia

3.4 Procesamiento y Análisis de Datos

La información obtenida se organizó, representó y analizó, presentando los resultados en porcentajes y diagramas que permitieron establecer gráficamente la situación actual de la empresa, la realidad del problema planteado y la necesidad de aplicar cambios o mejoramiento de la situación existente, a través de la metodología de normalización ISO 27001 para la gestión de la seguridad informática.

3.4.1 Análisis de la entrevista

En la entrevista se evidenció información importante para la investigación, en la empresa se han presentado problemas internos como es hasta la actualidad: ataques de spam, presentándose correos con archivos adjuntos que pueden perjudicar la integridad de la información, lo que genera un aspecto negativo como es la pérdida de información, siendo un problema muy perjudicial, es por ello que la empresa opto por la contratación de terceros que gestionan la red Wide Area Network (WAN), la cual es administrada por Century Link mediante red Multi-Protocol Label Switching (MPLS) para asegurar la conexión entre plantas ubicadas en el Parque Industrial de Ambato, Catiglata, Quito, Guayaquil, Santo domingo, además Colombia y Perú.

Es importante mencionar que la administración de la red interna Local Area Network (LAN) está controlada por dos personas capacitadas en seguridades, cuyos cargos son: Coordinador de Infraestructura y Analista de Seguridad de TI.

La red corporativa de Plasticaucho se maneja con una distribución de red de área local virtual (VLAN) por cada planta lo que ha permitido una flexibilidad de administración y un óptimo rendimiento.

También para una mayor seguridad la empresa ha implementado políticas que permiten proteger la información y los equipos, la infraestructura está administrada en Active Directory (AD), para localizar, proteger, administrar y organizar los recursos del equipo y de la red, como archivos, usuarios, grupos, periféricos y dispositivos de red.

En cuanto a la seguridad física, la ubicación del Data Center ha permitido realizar un control correcto de acceso para el personal, debiéndose llenar una bitácora con los datos de la persona; el área se encuentra con controles biométricos y vigilados con las cámaras de seguridad.

La persona con el cargo de Gestor de Hardware y Software es la encargada de distribuir los equipos y el Software que debe ser instalado para ejercer las labores. En caso que el usuario tenga requerimientos adicionales la empresa cuenta con un sistema Helpdesk SysAid el cual le permite crear Tickets, los cuales llegan al personal de TI para ser revisado si es factible su pedido, lo cual denota una buena organización en el área.

El software que se encuentra instalado en los equipos, es el necesario para las labores diarias del personal y son programas que tienen licencias pagadas para su ejecución, otros son con licencia libre, así también como las versiones de pruebas.

Para respaldo de la información la empresa Plasticaucho cuenta con licencias de Office para ciertos usuarios en donde disponen de la nube Onedrive. Además se dispone de servidores *Network Attached Storage* (NAS) para el almacenamiento de archivos, organizados en carpetas con el nombre del departamento o planta, donde cada administrador es el encargado de autorizar y solicitar al departamento de Tecnología de la Información el acceso a usuarios específicos con los permisos de lectura o escritura a estos archivos, todo el proceso de solicitud es a través del sistema Helpdesk.

3.4.2 Encuesta al personal de TI

Conocimiento de Seguridad de la Información

Objetivo: Determinar el nivel de conocimiento que dispone el personal con respecto a las normas de seguridad de la información.

1. Actual conocimiento que posee con respecto a la seguridad de la información.

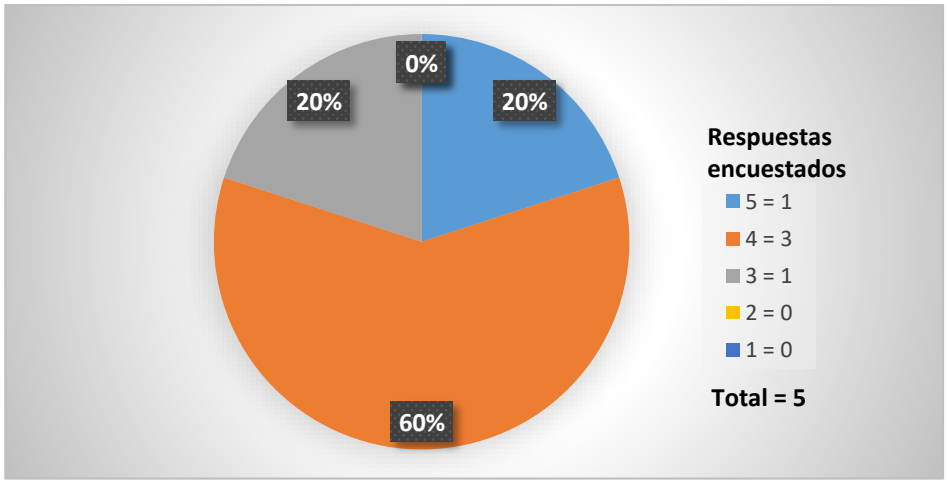

Fig. 1: Encuesta - Gráfico Pregunta 1

Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: El 20% de las respuestas obtenidas mencionan que tienen un nivel Excelente sobre el conocimiento de la seguridad de la información, el 60% con un nivel Bueno y el 20% restante indicó que disponen de un Regular conocimiento. Es decir, el personal de TI encargado de la seguridad de la información tiene un nivel aceptable sobre la seguridad de la información.

2. Que conocimientos dispone con respecto a las normas internas que establece la seguridad de información.

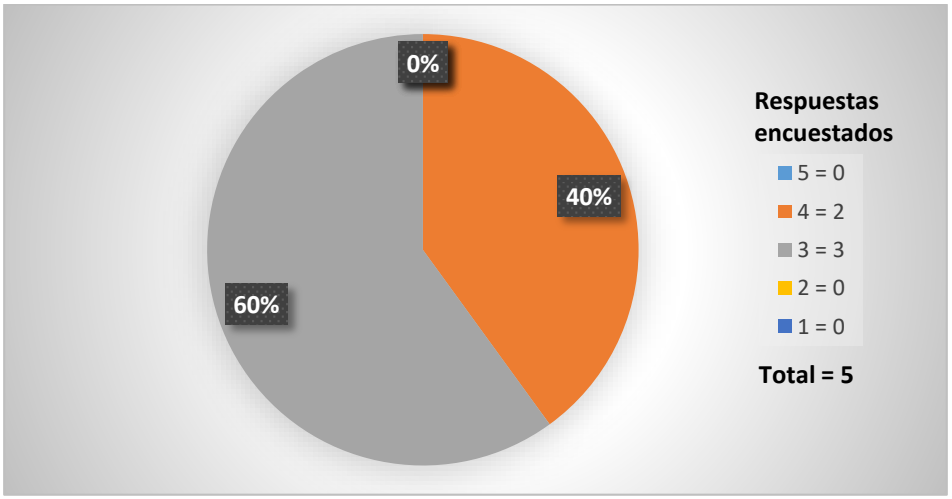

Fig. 2: Encuesta - Gráfico Pregunta 2
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: En la respuesta por el personal ante la pregunta de los conocimientos de las normas que estable la seguridad de información como se ve en el grafico es de un 60% respondió que es regular y con un 40% mencionó que es bueno. Por lo tanto, gran parte del personal del departamento TI tiene un déficit en el conocimiento de las normas de la seguridad de la información y solo una parte las conoce.

3. Qué nivel de conocimientos ha adquirido a través de las capacitaciones realizadas en seguridad de la información por parte de la empresa.

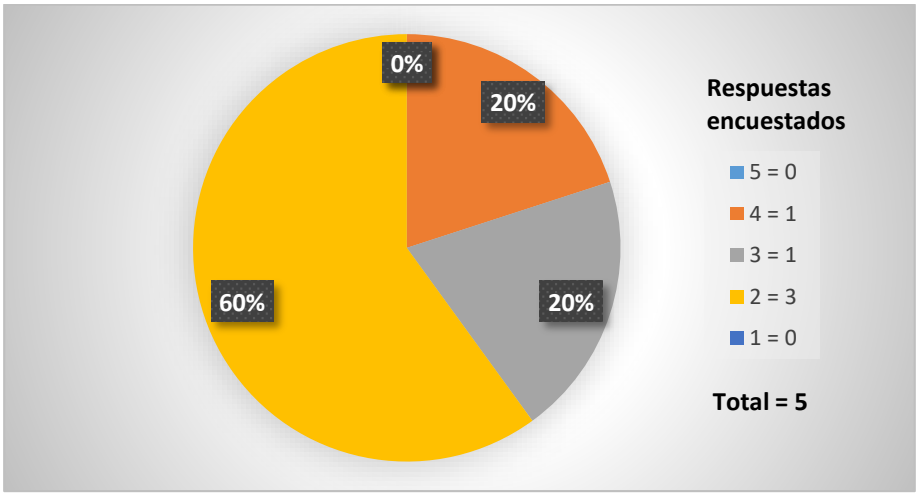

Fig. 3: Encuesta - Gráfico Pregunta 3
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: Aproximadamente un 60% contesto que los conocimientos que han adquirido en las capacitaciones realizadas por la empresa son muy deficiente, y con un 20% refirió que regular y otro 20% como bueno. Es decir, la empresa no ha dado mucha importancia a la seguridad de la información por lo cual no ha realizado capacitaciones a su personal, lo cual ha generado que se preparen por su propia cuenta ya que es importante para la empresa mantener actualizado los parámetros de seguridad según avance y se implemente nueva tecnología.

Conocimiento de la normatividad

Objetivo: Establecer el nivel de conocimiento sobre la Norma ISO 27001 y ley de protección de datos.

4. Cuál es su conocimiento actual sobre la Norma ISO 27001.

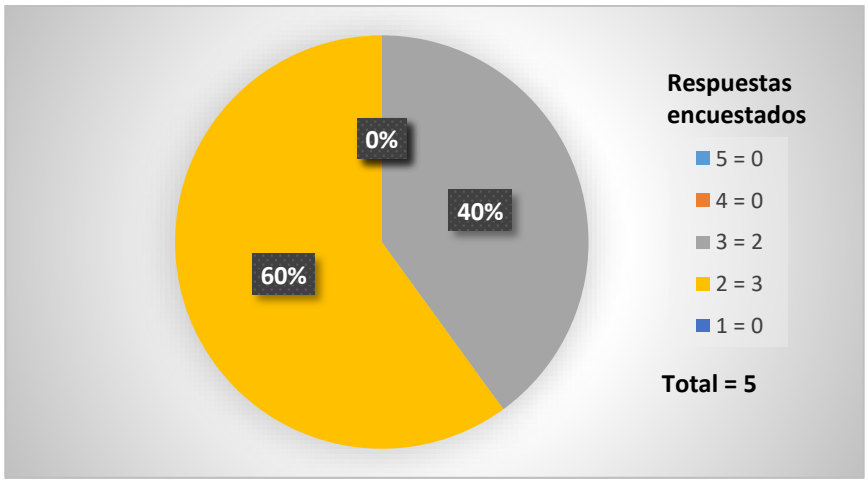

Fig. 4: Encuesta - Gráfico Pregunta 4
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: En la evaluación de la normativa ISO 27001 un 60% de la población contesto que es muy deficiente su conocimiento y un 40% es regular. Por lo tanto, se determina que existe un escaso conocimiento de la normativa ISO 27001, importante para el sistema de seguridad de información.

5. Qué conocimiento dispone sobre la ley de protección de datos.

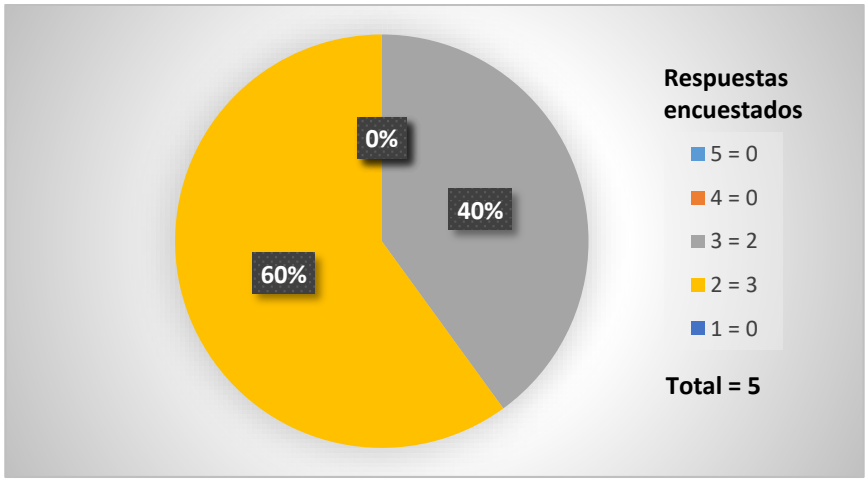

Fig. 5: Encuesta - Gráfico Pregunta 5
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: En cuanto a los conocimientos que disponen el personal del departamento de TI su respuesta fue muy deficiente representada con un 60% y un 40% refirió de regular los conocimientos acerca de ello. Entonces, se puede determinar que es necesario realizar un aporte para que puedan tener mejores y definidos conocimientos de las normativas de la ley de protección de datos.

6. En qué estado se encuentra la empresa en seguridad de la información de acuerdo a las Auditorías internas.

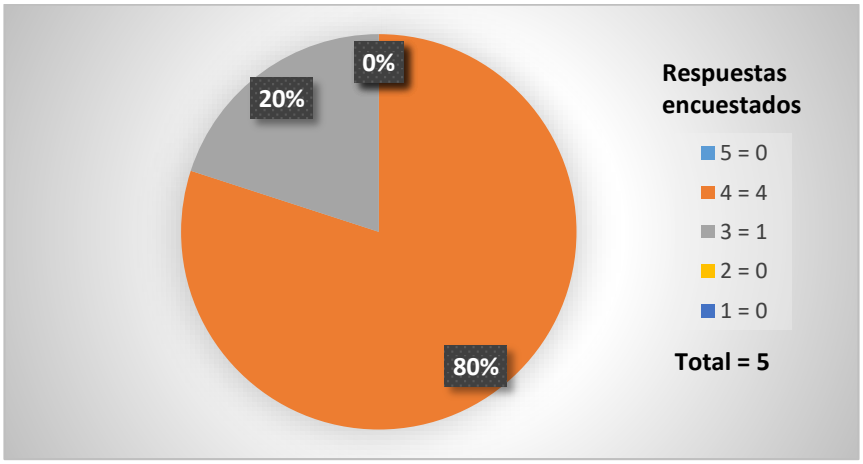

Fig. 6: Encuesta - Gráfico Pregunta 6
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: Un 80% contesto que el estado de las auditorias es bueno y que solo un 20% de regular. Es decir, por medio de auditorías que se realizan internamente en la empresa, se verifica que la seguridad de la información tiene un nivel aceptable pero los mismos se deben mejorar para llegar a un nivel excelente.

Técnicas para la protección de datos y seguridad de la información

Objetivo: Conocer el estado actual sobre la seguridad de la información, a través de los servicios que brindan el personal interno y externo para la empresa.

7. El medio donde se guardan los archivos backup (servidores). ¿En qué estado de seguridad se encuentran?

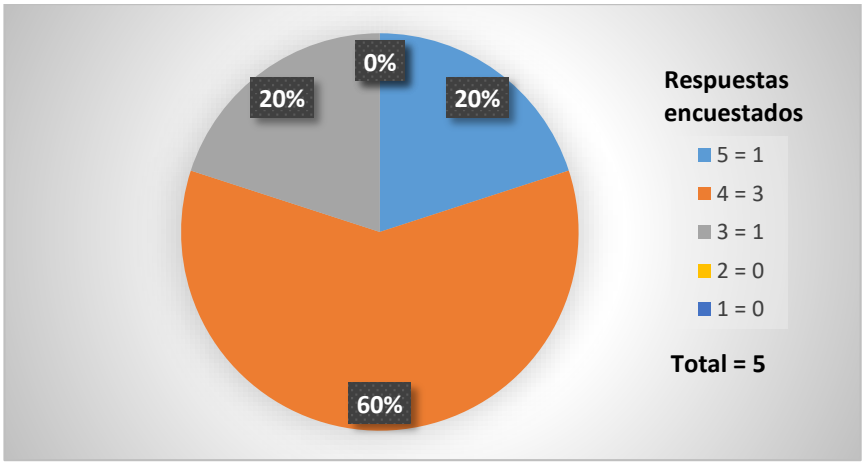

Fig. 7: Encuesta - Gráfico Pregunta 7
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: De acuerdo al estado que se encuentra los servidores de archivos Backup, el personal menciono con un 60% que es bueno,

un 20% es excelente y otro 20% revelo de regular. Por lo tanto, los servidores que son utilizados dentro de la empresa y administrados por el personal de TI se encuentran en un estado seguro pero han existido problemas que han ocasionado retrasos en el proceso para guardar los respaldos.

8. Los servicios prestados por proveedores externos en qué estado de confiabilidad se encuentran.

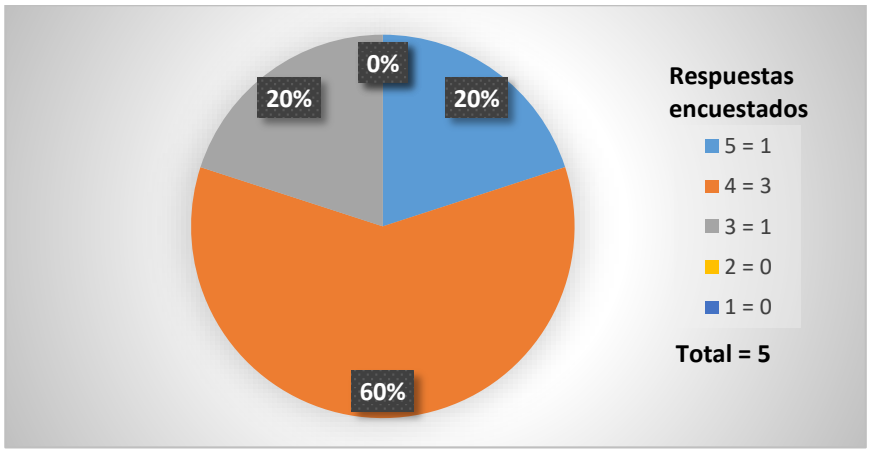

Fig. 8: Encuesta - Gráfico Pregunta 8
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: Un 60% del personal del departamento de TI respondieron que es bueno el estado de confiabilidad y un 20% refirió de regular, también otro 20% contesto de deficiente. Es decir**,** la confiabilidad de los servicios prestados por externos varía según el proceso en el que son requeridos, ya que en unos se trabajan con más datos que en otros.

9. Los servicios prestados por proveedores externos en caso de tener un fallo ¿Cómo define su accionar en tiempo de respuesta para resolver dichos problemas?

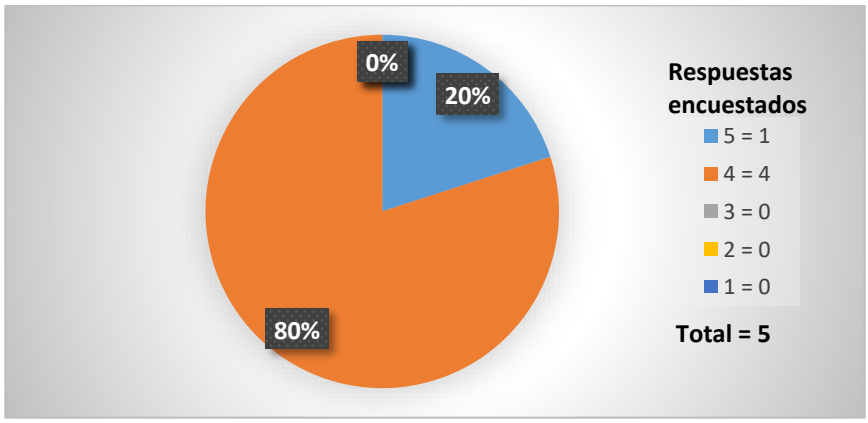

Fig. 9: Encuesta - Gráfico Pregunta 9

Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: El 80% del personal contesto que los servicios presentados por los proveedores externos en caso de tener un fallo expresaron ser buena, mientras que solo un 20% manifestaron que es excelente. Por lo tanto, el servicio que brindan los proveedores externos ha garantizado el cumplimiento y accionar ante un problema; según la complejidad dependerá el tiempo para dar solución a dichos acontecimientos.

10. Ante un fallo en uno de los servidores de la empresa y si se dispone de un servidor alterno ¿En qué estado se encuentra?

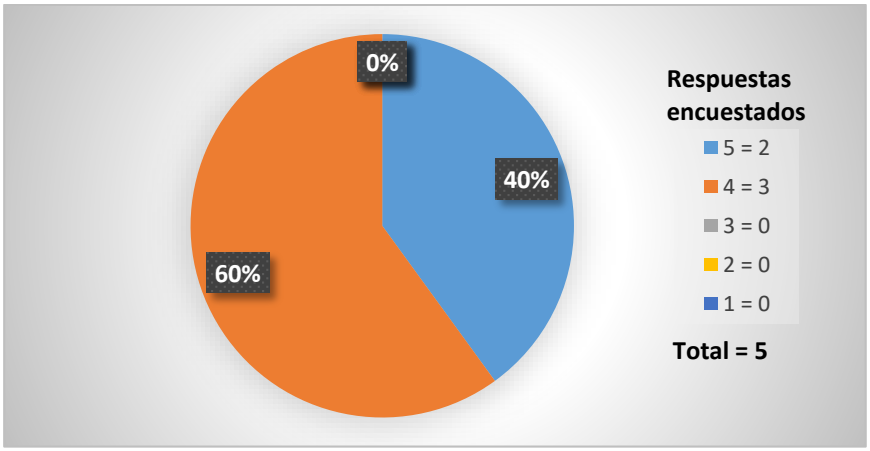

Fig. 10: Encuesta - Gráfico Pregunta 10
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: Las respuestas en cuanto al estado del servidor alterno ante un fallo, se pudo encontrar que un 60% consideran que es bueno, a su vez un 40% sostuvo que era excelente. Es decir, se evidencia que si existe un servidor alterno en caso de emergencia, el mismo que se encuentra en condiciones seguras para ser utilizado y continuar con las operaciones cotidianas de la empresa.

Acceso al área de servidores o Data Center

Objetivo: Conocer el nivel de seguridad física de acceso al área de servidores que disponga la empresa.

11. El sistema de control (registro, bitácoras, cámaras, etc.) para el ingreso a esta área está definida como

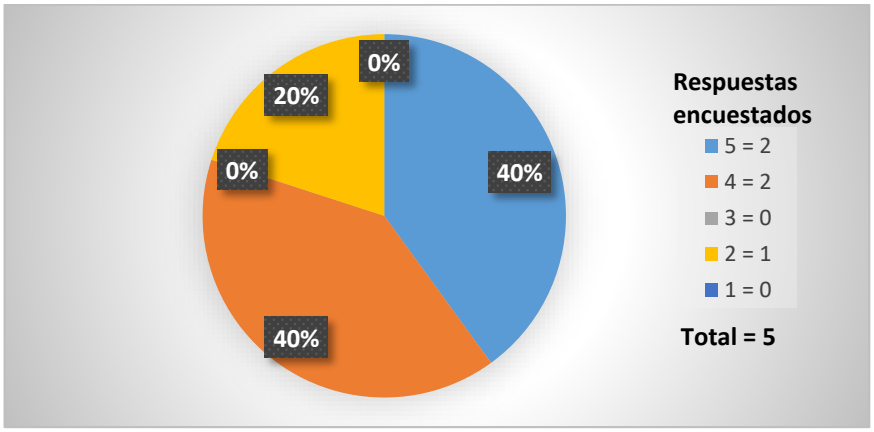

Fig. 11: Encuesta - Gráfico Pregunta 11
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: Un 40% del personal contesto que el sistema de control de esta área es bueno y otro 40% contesto que excelente y solo un 20% refirió que es muy deficiente. Por lo tanto, se verifica que el control que se ha implementado para la seguridad del Data Center cumple con las garantías para administrar el ingreso al área, además se cuenta con la persona encargada para este proceso, pero Plasticaucho al tener varias sucursales con su propia área de servidores no existe el mismo control.

12. El área de servidores de acuerdo a las normativas de seguridad de la información para el diseño y ubicación ¿En qué estado se encuentra?

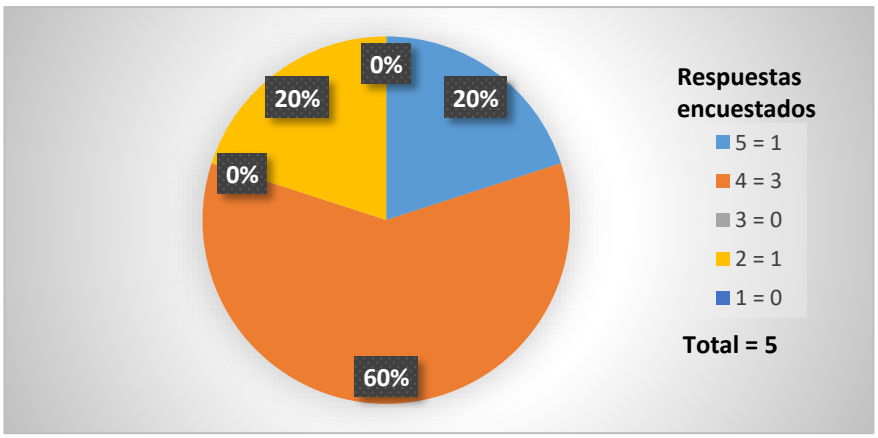

Fig. 12: Encuesta - Gráfico Pregunta 12
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: El área de los servidores se encuentran en un estado Excelente así lo pudieron manifestar un 20% del personal, un 60% refirió que es bueno y muy deficiente lo indican un 20%. Es decir, la ubicación del área de servidores se lo define por importancia y cantidad de usuarios que trabajan

en cada sucursal, en la Plantas Principales el Data Center cumple con las normativas de diseño y control; en sucursales pequeñas su administración no es completa.

13. Ante una emergencia donde se encuentre en riesgo la información y es necesario contar con un plan de contingencia ¿En qué nivel lo define?

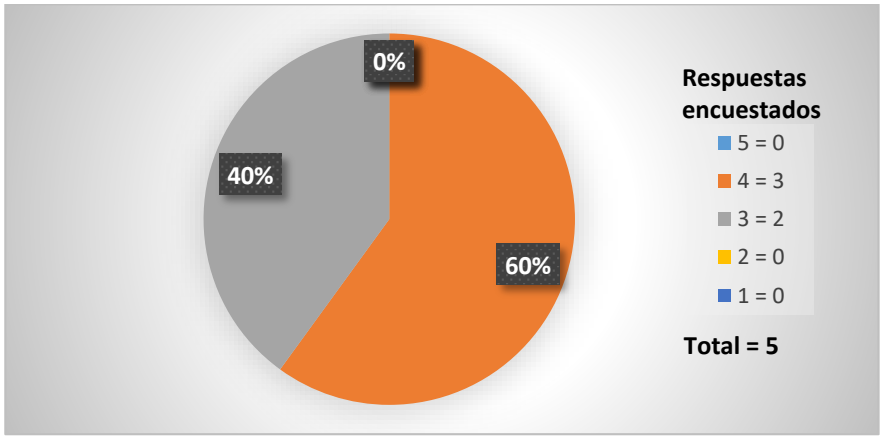

Fig. 13: Encuesta - Gráfico Pregunta 13
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: En cuanto a nivel de contingencia que presenta con un 60% en un buen estado y solo un 40% menciono que es regular. Por lo tanto, la empresa cuenta con un plan de contingencia pero es necesario verificar y actualizar periódicamente, ya que los problemas avanzan al igual que la tecnología.

Protección de datos y seguridad de la información

Objetivo: Definir el nivel de control que disponga el departamento de TI para los servicios que utiliza el personal de la empresa.

14. ¿Cómo define el control de correos electrónicos?

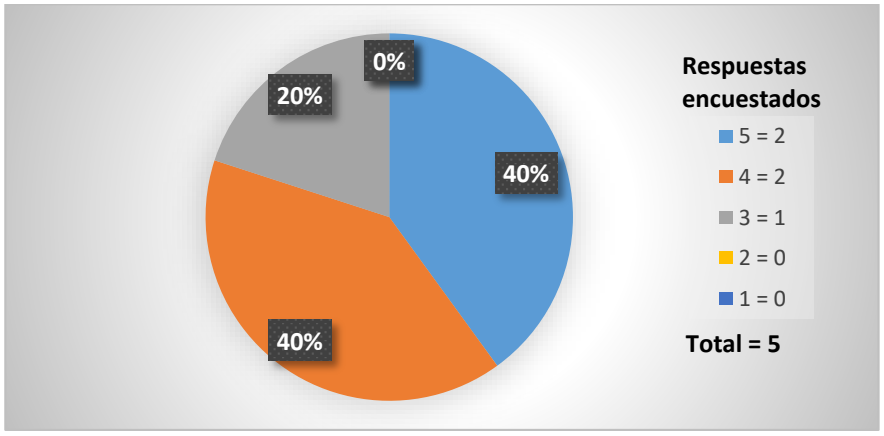

Fig. 14: Encuesta - Gráfico Pregunta 14
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: El personal encuestado definió que el control de correos de la empresa es excelente con un 40%, otro 40% indico como bueno y solo 20% que es regular. Es decir, la empresa cuenta con licencia Exchange Online Protection de Microsoft para la administración de los correos electrónicos, en la que permite controlar Lista Blancas, Listas Negras, Antispam entre otros, pero las mismas que en ocasiones son vulneradas e ingresan a la bandeja de los usuarios como correos normales.

15. ¿Cómo se define el control de antivirus en los equipos de cómputo de la empresa?

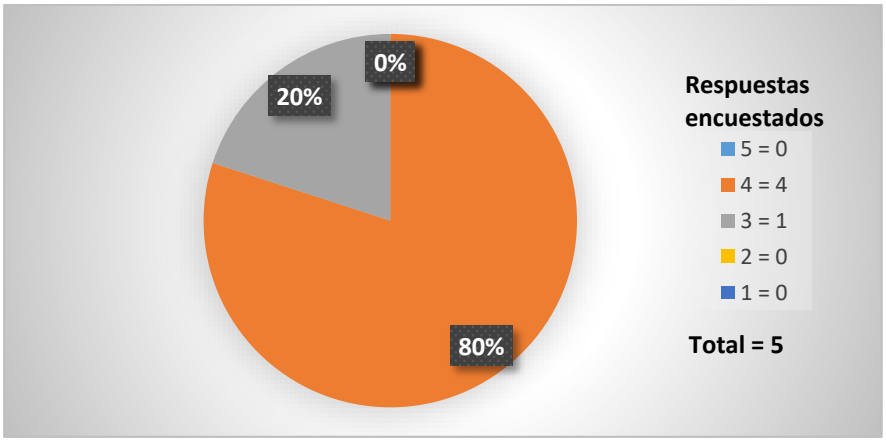

Fig. 15: Encuesta - Gráfico Pregunta 15
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: La definición de los antivirus en la empresa es buena así lo manifestó el 80% del personal a través de la encuesta y solo un 20% de regular. Por lo tanto, Windows Defender al ser el antivirus que utilizan los equipos dentro de la empresa, el nivel de seguridad que brinda es medianamente confiable, ya que dispone de un conjunto de características de protección en tiempo real, pero los ataques que en la actualidad existe puede superar todo tipo de antivirus por eso es importante tenerlo actualizado.

16. La seguridad que tienen los sistemas desarrollados por el personal dentro de la empresa ¿Qué confiabilidad brindan para el manejo de datos?

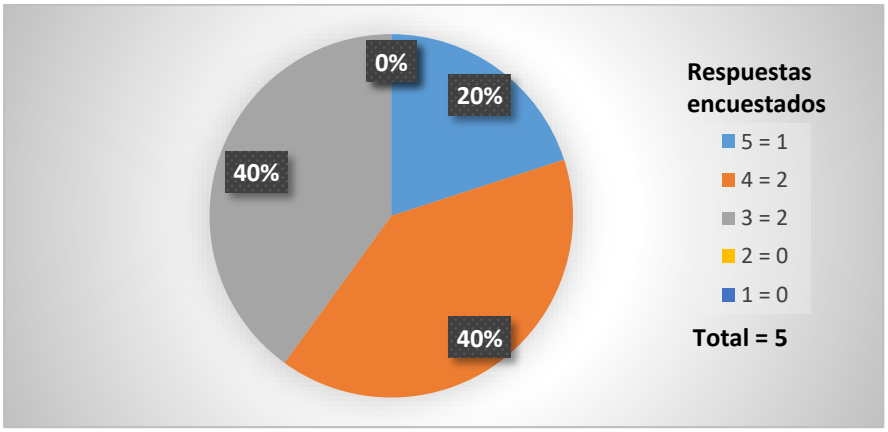

Fig. 16: Encuesta - Gráfico Pregunta 16
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: La confiabilidad que tienen los sistemas que son desarrollados por el personal es excelente así se puede evidenciar en el gráfico con un 20%, un 40% como bueno y el otro 40% lo catalogaron de regular. Es decir, los sistemas que han sido desarrollados por el personal interno de la empresa han ido evolucionado en cuanto a su seguridad, pero los mismos que deben ser revisados en cada versión para no comprometer los datos.

17. La seguridad que tienen los sistemas contratados por la empresa ¿Qué confiabilidad brindan para el manejo de datos?

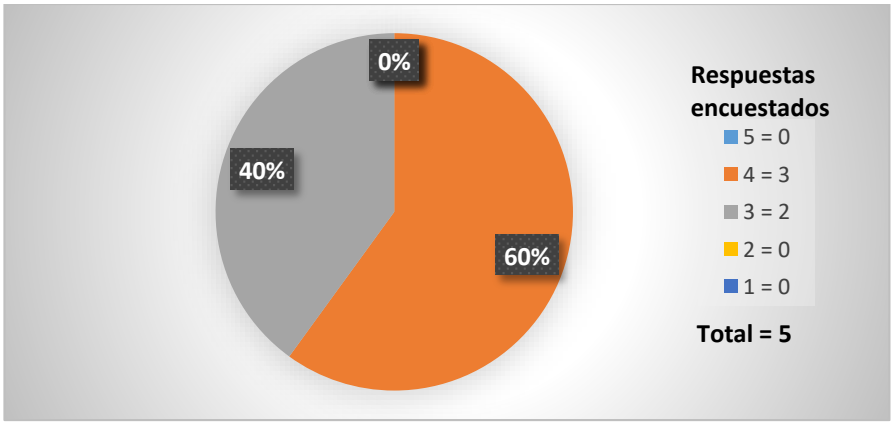

Fig. 17: Encuesta - Gráfico Pregunta 17
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: La confiabilidad del manejo de datos por el sistema contratado por la empresa es bueno, así se evidencia en el gráfico con un 60% y un 40% de regular. Por los tanto, el personal de TI para cada sistema que se requiera, antes de proceder al contrato es analizado la seguridad que tenga para la manipulación de datos, además del soporte técnico que el sistema brinde.

18. Cómo definen el acceso y restricción a la red para los usuarios, sea a páginas de navegación como acceso a carpetas compartidas dentro de la red de Plasticaucho.

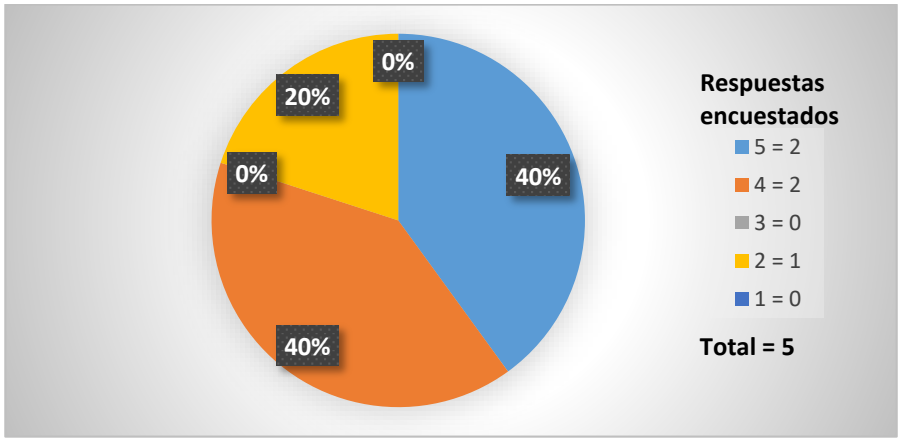

Fig. 18: Encuesta - Gráfico Pregunta 18
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: Un 40% define el acceso a la red de los usuarios es excelente, otro 40% lo refiere de bueno y solo un 20% como muy deficiente. Es decir, el control es administrado mediante perfiles de navegación para cada usuario, así también como el acceso a carpetas compartidas; en casos de páginas web explícitas que requieran apertura de puertos, lo administra un proveedor externo por lo que se tiene que esperar un tiempo de respuesta para este tipo de escalamiento de servicio.

19. El software utilizado dentro de la empresa definidos con licenciamiento pagado ¿Qué seguridad la evalúa?

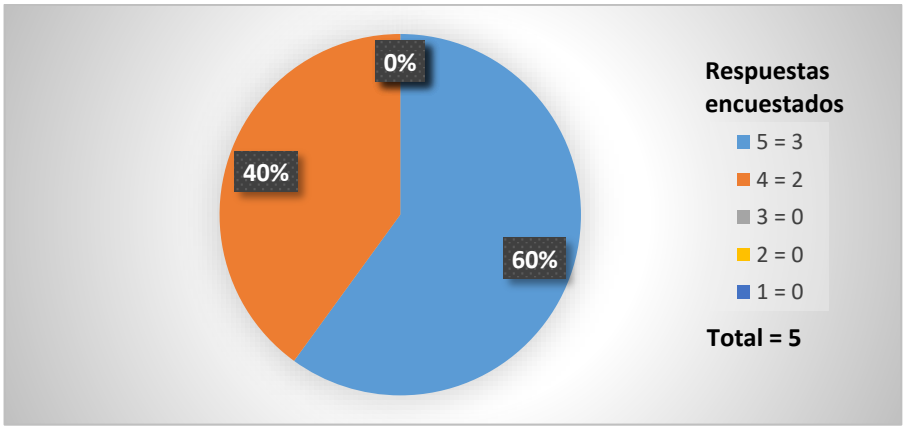

Fig. 19: Encuesta - Gráfico Pregunta 19
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: En cuanto al software utilizado dentro de la empresa es definido como excelente destacando su seguridad con un 60% y solo un 40% mencionó que es bueno. Por lo tanto, es importante indicar que dentro de la empresa se maneja mediante licencias para cada programa que se utilice, de esta manera evitando instalaciones de software malicioso y asegurar los datos del usuario.

20. El software utilizado dentro de la empresa definidos con licenciamiento libre ¿Qué seguridad la evalúa?

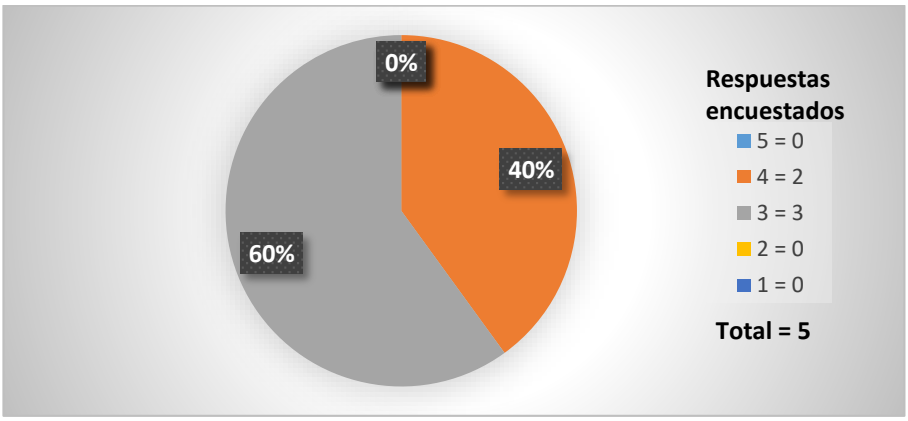

Fig. 20: Encuesta - Gráfico Pregunta 20
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: Con respecto al licenciamiento libre el personal mencionó que es regular con un 60% y un 40% como bueno. Es decir, el software libre que vaya a ser utilizado para actividades ocasionales o permanentes es analizado antes de ser instalado, se verifica el tiempo de uso que se dará y si es realmente necesario.

Estrategia para la protección de información

Objetivo: Establecer el nivel de protección que disponen para el uso de los sistemas cotidianos en la empresa.

21. Cómo define los parámetros para creación de contraseñas que son utilizadas para ingreso a sistemas de trabajo en la empresa

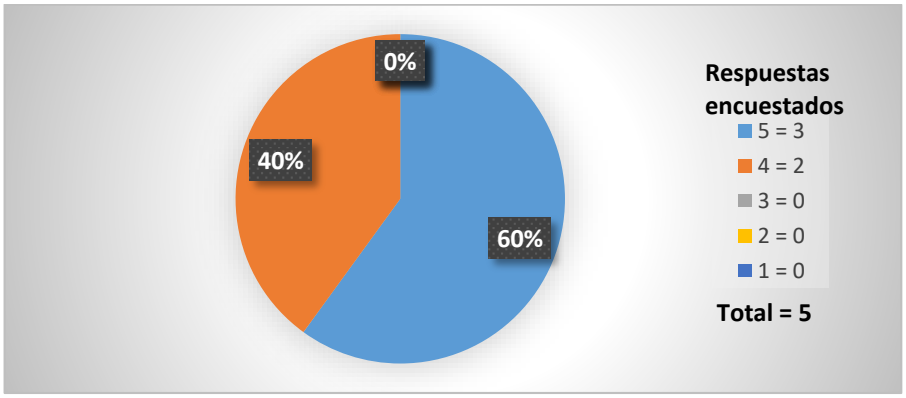

Fig. 21: Encuesta - Gráfico Pregunta 21
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: Los parámetros utilizados para la creación de las contraseñas con un 60% indican que es excelente y solo un 40% refirió de ser bueno. Por lo tanto, el nivel de seguridad que se implementa para la creación de contraseñas cumple con los parámetros para ser segura, la misma que se pide obligatoriamente actualizar cada mes por parte del usuario.

22. El nivel de seguridad para ingreso a los sistemas propios o contratados por la empresa cumple con los parámetros de seguridad

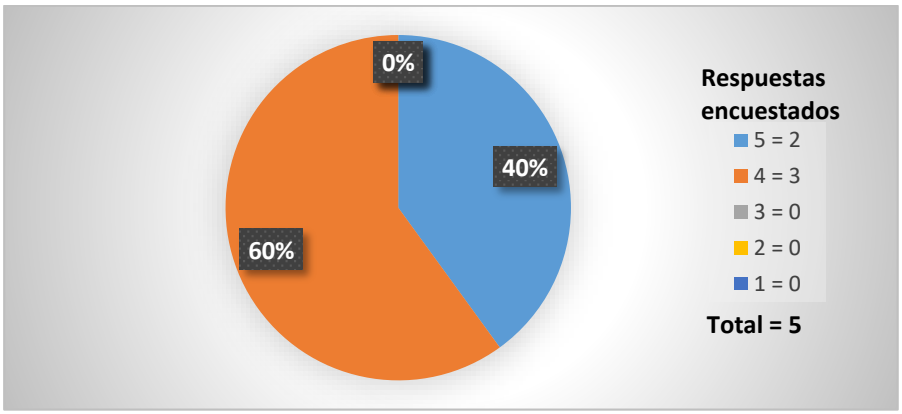

Fig. 22: Encuesta - Gráfico Pregunta 22
Fuente: Elaboración propia a partir de la encuesta

Análisis e Interpretación: Los parámetros de seguridad en sistemas propios o contratados por la empresa, el personal mencionó que son excelentes con un 40% y el restante 60% los catalogó de bueno. Es decir, la mayoría de los sistemas que son desarrollados y contratados por la empresa, están implementados con los parámetros de seguridad que los hacen confiable, y que ha permitido la manipulación de datos.

3.5 Desarrollo del Proyecto

En el desarrollo del presente proyecto se emplearon los siguientes pasos:

- Análisis de la situación actual de la empresa.
- Análisis de los sistemas y aplicaciones existentes en la empresa.
- Descripción de las políticas ya establecidas para la gestión de seguridad informática.
- Aplicación de la Norma Estándar ISO 27001.
- Plantear las etapas para la elaboración del Plan de Gestión de Seguridad Informática.
- Definición del alcance del Plan de Gestión de Seguridad Informática.
- Análisis de riesgos y selección de controles de la ISO 27001.
- Declaración de aplicabilidad.
- Nivel de cumplimiento y aplicabilidad.
- Presentación del Plan de Gestión de Seguridad Informática.
- Monitorización e implementación del Plan de Gestión de Seguridad Informática.

CAPÍTULO IV

DESARROLLO DE LA PROPUESTA

4.1 Análisis de la situación actual del departamento de Tecnología de la Información

4.1.1 Información de la Empresa

- **Beneficiario**

Plasticaucho Industrial S.A.

- **Ubicación**

Ecuador

Catiglata: Panamericana Norte Km 2 ½

Parque Industrial: Panamericana Norte Km 10 - Parque Industrial 4ta. Etapa Ambato

- **Introducción a la empresa**

La empresa Plasticaucho Industrial es una sociedad anónima, constituida bajo las leyes ecuatorianas, dedicada a la elaboración y comercialización de calzado de cuero, lona y plástico, sus actividades se desarrollan con su sede principal en Ambato Ecuador y con filiales en Colombia y Perú.

Plasticaucho Industrial S.A. realiza la comercialización de su producto en Ecuador y se extiende bajo importaciones a Colombia y Perú de productos específicos que son producidos únicamente en el país. Es una empresa en la que prima la innovación de su proceso y a su vez pone énfasis en la constante mejora tecnológica.

- **Misión**

Lideramos el sector calzado en el Ecuador con procesos ágiles, eficiente e innovadoras.

- **Visión**

Todo ecuatoriano usará un par de zapatos de una de las marcas comercializadas por la empresa.

4.2 Sistemas y aplicaciones existentes en la empresa

La empresa Plasticaucho Industrial S.A., conocida a nivel nacional e internacional por la producción de calzado de calidad, y lo que le ha permitido escalar ante sus competidores, se maneja bajo estrictos controles de seguridad de la información que es propia de la empresa, clientes y personal en general.

Para la seguridad de la información en la empresa, se la administra bajo políticas de seguridad en la que están involucrados todos los sistemas que se adquieren y/o desarrollan. Además, el personal que ingresa a laborar está bajo estrictos cumplimientos establecidos en contratos para mantener la información a buen recaudo.

Los sistemas y aplicaciones de mayor importancia, las mismas que manejan información sensible son detallados a continuación en la tabla 4.

Tabla 4: Sistemas y aplicaciones utilizados en Plasticaucho Industrial

Sistema	Logo	Definición	Características
Active Directory (AD)	 **Fig. 23:** Active Directory **Fuente:** [24]	Active Directory o Directorio Activo es una implementación de servicio de directorio en la red distribuida de computadores de la organización Plasticaucho, el cual se encuentra establecido en un servidor central el cual permite organizar y gestionar todos los elementos de la red informática como ordenadores, grupos, usuarios, dominios, políticas de seguridad. [24]	• Control de recursos de informáticos. • Organización de grupos de trabajo con los usuarios que pertenecen a un mismo departamento. • Autenticación a cada usuario, identificando dentro de la red mediante credenciales. • Integración con aplicaciones de terceros para facilitar la autenticación. • Control para otorgar o denegar accesos a recursos compartidos de la red. • Creación de políticas para las directivas de grupo, limitando el comportamiento de los usuarios para acceder a recursos de la red. • Políticas de grupo para establecer contraseñas seguras y caducidad. • Clasificación de usuarios normales y administradores. [24]

Sistema	Logo	Definición	Características
SAP ERP	 **Fig. 24:** Software SAP **Fuente:** [25]	El sistema SAP representan las siglas en alemán Systeme Anwendungen und Produkte que significa en español "sistemas, aplicaciones y productos", este sistema ERP (Enterprise Resource Planning o planificación de los recursos empresariales) consta de módulos que van desde la Gestión de Recursos Humanos hasta Finanzas que están integrados entre sí para manejo de información inmediata. [25]	• Mínimos requerimientos de programación adicionales. • Procesos organizativos y de negocio son reflejados en el sistema. • Adaptación del sistema al modelo de la empresa mediante parametrizaciones. • Optimización en el manejo de inventarios con el control de entrada y salida de mercancía. • Cadenas de suministros más eficientes. • Control de seguridad de acceso a usuarios normales y administradores. [25]
Squarenet	 **Fig. 25:** Software SquareNet **Fuente:** [26]	Software para la gestión de información personal de la empresa, mediante esta aplicación se administra los datos personales de empleados de la organización. [26]	• Control de personal activo de la empresa. • Seguridad de la información personal de cada empleado. • Administración de personal autorizado para ingresar a las instalaciones. • Registro de la hora de entrada y salida de las instalaciones. • Administración de usuarios y perfiles de permisos por departamento. [26]
Papercut	 **Fig. 26:** Software PaperCut **Fuente:** [27]	Aplicación de software diseñada para administrar las impresiones mediante la asignación de un determinado cupo para los usuarios registrados en el sistema. Es aplicado como una política de seguridad de la información con mejores prácticas para proteger el sistema de impresión. [27]	• Reducción de costos en recursos (tóner/tinta, papel). • Seguridad de los documentos, liberación de impresión segura. • Usuarios finales mejoran su comportamiento de impresión. • Importación de usuarios de Active Directory. • Control de impresión y registros que ocurran en el sistema. • Reportes y rastreo de todas las actividades de impresión. [27]

Sistema	Logo	Definición	Características
SysAid	 **Fig. 27:** Software SysAid **Fuente:** [28]	SysAid Helpdesk es un software para la gestión de servicios de Tecnología Informática (IT) y de centro de soporte integrado que permite administrar e interactuar con el usuario final. [28]	• Gestión de tickets, automatizando los procesos y actividades de TI. • Centro de soporte para la gestión de incidentes. • Portal de servicios para interactuar con el departamento de TI. • Herramienta que guarda una base de conocimientos, consejos y soluciones para los administradores como usuarios finales. • Comunicación de estado del ticket con usuarios finales por medio de correos electrónicos. • Control de tiempo de las actividades que se realizan para solventar un incidente o solicitud. • Informes finales para revisiones de cumplimientos. [28]
Exchange Online Protection	 **Fig. 28:** Software Exchange Online Protection **Fuente:** [29]	Exchange Online Protection es un servicio de Microsoft de correos electrónicos para proteger de mensajes no deseados y de software malintencionado, es de utilidad empresarial y de gran apoyo para la mensajería de Plasticaucho Industrial. [29]	• Protección de correos no deseados y malware. • Seguridad y confiabilidad para proteger la información. • Elimina amenazas antes de que alcancen el firewall corporativo, con protección en tiempo real ante correos no deseados. • Administración desde una interfaz web. • Filtrado de contenidos activos y conexiones basados en directivas corporativas. • Control de listas blancas y negras de dominios de correos electrónicos. [29]

Sistema	Logo	Definición	Características
Red MPLS	 **Fig. 29:** Red MPLS **Fuente:** [30]	La empresa Century Link provee del servicio MPLS/IP VPN para Plasticaucho Industrial, es un servicio de red Multiprotocol Label Switching (MPLS) que permite crear trayectos privados de punto a punto, con una infraestructura segura, confiable y de alto desempeño que ha permitido mantener la disponibilidad de la red WAN de la empresa. [30]	• Conexión eficaz entre sucursales de Plasticaucho dentro y fuera del país. • Seguridad en el transporte de datos confidenciales. • Administración para la gestión y enrutamiento de tráfico de la red. • Servicio VPN. • Flexibilidad, control y rendimiento. • Administración de Firewall. [30]
PRTG	 **Fig. 30:** Software PRTG **Fuente:** [31]	Paessler Router Traffic Grapher (PRTG), es una herramienta de monitoreo de la infraestructura y red de Plasticaucho Industrial la cual permite identificar de manera rápida las anormalidades de la red, encontrar problemas y optimizar la infraestructura de TI. [31]	• Supervisión de toda la infraestructura de TI. • Herramienta para análisis de tráfico, paquetes, aplicaciones, ancho de banda, tiempo de actividad, puertos, IP, hardware y demás dispositivos de IT. • Monitorización de toda la infraestructura LAN, WAN. • Alertas en tiempo real para analizar advertencias o métricas inusuales. [31]

Fuente: Elaboración propia

4.3 Entornos de desarrollo de software

Para mantener la seguridad de los datos, el departamento de Tecnología de la Información se basa en los siguientes entornos para el proceso de desarrollo de software:

Tabla 5: Entornos de desarrollo de Software

N°	Entorno	Objetivo	Responsables
1	Desarrollo	Ambiente utilizado para la elaboración de software.	• Área de desarrollo
2	Pruebas	Establecido como un ambiente similar al de producción, utilizado para controlar la calidad y pruebas del sistema	• Área de desarrollo • Área de calidad
3	Producción	Ambiente utilizado para la puesta en marcha la operación de los sistemas	• Área de desarrollo • Área de Base de datos • Área de Operaciones

Fuente: Elaboración propia

La información que se encuentra almacenada en el entorno de producción no es utilizada, ni visible a los entornos de prueba y desarrollo, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los datos.

4.4 Políticas de TI para la gestión de seguridad informática

Las políticas que se encuentran establecidas en el departamento de Tecnología de la Información, tienen como objetivo el buen uso de los recursos de tecnología de la empresa, y dar a los usuarios las normas necesarias para cuidar la confidencialidad, integridad y disponibilidad de la información. El documento incluye un conjunto de políticas, procedimientos y estándares que tiene como objetivo básico regular la forma como los usuarios manejan, protegen y distribuyen su información. [32]. En la tabla 6 se describen las políticas establecidas, contenido y responsables de verificar su cumplimiento.

Tabla 6: Descripción de Políticas de Seguridad TI

Política	Descripción	Contenido	Responsables
Usuarios	Políticas para las cuentas de usuario que son utilizados en los sistemas informáticos de la empresa, tienen como objetivo asegurar la autenticación, acceso, administración de recursos, etc.	• Creación y vigencia de usuarios de red. • Acciones cuando un empleado renuncia. • Acciones ante la desvinculación de un empleado. • Eliminación de cuentas de usuario. • Creación de contraseñas. • Caducidad de contraseñas. • Responsabilidad de uso de contraseñas. • Acciones durante las vacaciones de los empleados. • Usuarios/consultores externos o invitados.	• Analista de Seguridades TI • Agentes de Soporte Técnico
Software	Políticas con el propósito de establecer las guías para la administración de los programas.	• Responsables de la instalación de software. • Requerimientos esenciales de software. • Aprobaciones de adquisiciones de software. • Desarrollo o implementación de software. • Responsables de nuevas soluciones de software. • Requerimientos de automatizar o mejorar procesos de la empresa. • Soporte de desarrollo o implementación de software.	• Analista de Seguridades TI • Gestor de Hardware y Software • Agentes de Soporte Técnico

Política	Descripción	Contenido	Responsables
Hardware y accesorios periféricos	Políticas establecidas para asegurar el uso de hardware o periféricos electrónicos y accesorios que entrega la empresa al empleado para el desarrollo de su trabajo en el tratamiento de la información.	• Adquisición, asignación y configuración de hardware y software. • Actividades permitidas en el uso de hardware y software. • Responsabilidades de los equipos entregados a los empleados. • Autorización de salida de equipo fuera de la compañía. • Tiempo establecido para el cambio de equipo. • Seguridad implementada para los equipos. • Privilegios establecidos según el rol de usuario. • Responsabilidades de compra de hardware, periféricos y accesorios. • Actividades permitidas en los equipos de cómputo.	• Analista de Seguridades TI • Gestor de Hardware y Software • Agentes de Soporte Técnico
Datos y respaldos	Políticas dispuestas para la protección de toda la información almacenada en servidores, equipos de cómputo, dispositivos móviles y en general cualquier dispositivo de almacenamiento, debe ser relacionada con el negocio y propiedad intelectual de la empresa.	• Selección de la herramienta para realizar el respaldo de información. • Contenidos permitidos y prohibidos de almacenar. • Responsables de realizar el respaldo de información. • Descripción de los esquemas de respaldo (Colaborativo, Nube compartida, Nube de usuario, One Drive). • Tiempo estimado de conservar el respaldo. • Copia de seguridad de los servidores.	• Analista de Seguridades TI • Coordinador de Infraestructura

Política	Descripción	Contenido	Responsables
Impresoras	Políticas para controlar el servicio de impresión, copiado y escaneado.	• Descripción de equipos de impresión. • Control de cupos de impresión o copiado. • Prohibiciones de impresión de documentos. • Soporte técnico de los equipos de impresión. • Responsables de movimiento de equipos de impresión.	• Analista de Seguridades TI • Agentes de Soporte Técnico
Correo electrónico	Políticas consideradas para el uso aceptable y uso inaceptable de las herramientas de comunicación electrónica.	• Información prohibida para transmitir mediante el servicio de correo. • Actividades prohibidas en la creación de los mensajes. • Controles de correo SPAM. • Tamaño máximo de mensajes de entrada y salida. • Tipos de archivos no permitidos de enviar o recibir. • Descripción del filtrado de correo electrónico.	• Analista de Seguridades TI • Coordinador de Infraestructura
Internet	Políticas establecidas para controlar el acceso al servicio de Internet por parte de los usuarios de la organización.	• Descripción de los perfiles de navegación (Controlado, Restringido, Completo, Completo Plus, Completo Full). • Actividades prohibidas. • Filtrado de contenido en páginas web.	• Analista de Seguridades TI • Coordinador de Infraestructura

Política	Descripción	Contenido	Responsables
Prevención contra intrusos	Políticas dispuestas para el análisis de vulnerabilidades de acuerdo a la planificación del plan de riesgos tecnológicos.	• Análisis de vulnerabilidades. • Software antivirus. • Capacitaciones a usuarios.	• Analista de Seguridades TI • Coordinador de Infraestructura
Telefonía	Políticas establecidas para el servicio de telefonía, que incluye la recepción y generación de llamadas desde los diferentes tipos de teléfonos análogos, digitales o IP que posee la empresa.	• Descripción de perfiles de telefonía. • Responsabilidades de asignación de líneas. • Restricciones del servicio de telefonía.	• Analista de Seguridades TI • Coordinador de Infraestructura • Agentes de Soporte Técnico
Soporte Técnico	Políticas dispuestas para dar a conocer el servicio que prestará el servicio de soporte técnico.	• Descripción de los servicios de TI. • Responsables de mantenimiento de los equipos de tecnología.	• Analista de Seguridades TI • Agentes de Soporte Técnico

Fuente: Elaboración propia a partir de [32]

4.5 Matriz FODA de la gestión de Seguridad Informática

Tabla 7: Análisis Matriz FODA

FORTALEZAS	**OPORTUNIDADES**
• Personal estructurado para cada proceso de área de Tecnología de la Información. • Personal capacitado para el desenvolvimiento cotidiano en la empresa. • Licencia para Software de trabajo. • Políticas internas de seguridad para usuarios existentes. • Software apoyo para el control de la seguridad de la información. • El área de desarrollo se basa en entornos de software seguro.	• Capacitación periódica a los usuarios en la seguridad de la información. • Implementación de nuevas herramientas tecnológicas para la seguridad de información. • Aplicación de software libre para procesos dentro de la empresa • Establecer un plan de gestión de seguridad informática, para el mejoramiento de la seguridad de la información • Personal externo especializado en servicio Web, correo electrónico y firewall. • Estandarización de la empresa con la Norma Internacional ISO 27001
DEBILIDADES	**AMENAZAS**
• Políticas definidas pero no aplicadas completamente por parte del usuario. • Falta de tiempo por parte del personal para recibir capacitaciones. • Recursos económicos no suficientes para la implementación de nuevas tecnologías.	• Se debe contratar a un personal externo para realizar diferentes acciones en el área de TI. • Por el costo de licencias se debe analizar usuarios según su proceso para asignar el tipo de software. • Software libre en ocasiones no confiables en base a la seguridad de integridad de la información.

• La empresa no está al 100% con la seguridad de la información. • Personal incapaz de seguir lineamientos planteados por una norma	• Ataques a la infraestructura evidenciándose un déficit de seguridad.

Fuente: Elaboración propia

4.6 Aplicación de la Norma Estándar ISO 27001

4.4 Noma ISO 27000

La información es un activo valioso capaz de impulsar o destruir una empresa. Las organizaciones deben garantizar su seguridad en cuanto a la integridad, disponibilidad y confidencialidad de la información.

En este sentido organizaciones como ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission) han elaborado conjuntamente la familia ISO/IEC 27000. Esta, es un conjunto de normas desarrolladas para proveer un marco en gestión de la seguridad de la información que sirva de aplicación.

4.4.1 Norma ISO/ IEC 27001:2013

Los estándares internacionales hacen que las cosas funcionen bien, ofrecen especificaciones de clase mundial para productos, servicios y sistemas, para garantizar la calidad, la seguridad y la eficiencia.

ISO/ IEC 27001:2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO/ IEC 27001:2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza, la revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013, la primera revisión se publicó en 2005. [33]

4.4.2 Relación entre las normas ISO/IEC 27001 y 27002

La norma ISO/IEC: 27001:2013 es una norma que define como ejecutar un Sistema de Gestión de la Seguridad de la información (SGSI), indicando que la seguridad de la información debe ser planificada, implementada, supervisada, revisada y mejorada. De estos hitos, se extraen una serie de objetivos para su cumplimiento y que están establecidos en la norma. Por lo tanto, es una norma de certificación de cumplimiento de dichos objetivos. [34]

En cambio, la norma ISO/IEC/27002:2013 es una guía de buenas prácticas para mejorar la seguridad de la información de tal manera que ayuda a alcanzar los objetivos marcados en la ISO/IEC: 27001:2013. Estas buenas prácticas se presentan en forma de controles diferenciados por dominios relativos a la seguridad de la información. Dichos controles ya aparecen nombrados en la norma ISO/IEC: 27001:2013 en su Anexo A, pero sin ser desarrollados, y es en la 27002 donde se desarrollan. [34]

Por tanto, se puede concluir que la norma ISO/IEC 27002 ofrece las herramientas para ayudar a alcanzar los objetivos que se establecen en la norma ISO/27001.

4.4.3 Familia ISO 27000

A continuación se presenta una lista de las principales Normas ISO de la familia 27000 que están relacionadas con el Sistema de Gestión de Seguridad de la Información.

ISO 27000 es un conjunto de normas desarrolladas o en fase de desarrollo que facilitan un marco de gestión de la seguridad de la información aplicable a cualquier tipo de empresa privada o pública, pequeña o grande. [35]

ISO / IEC 27000:2018 proporciona una descripción general de los sistemas de gestión de la seguridad de la información (SGSI). Además proporciona términos y definiciones comúnmente utilizados en la familia de estándares SGSI. Este documento es aplicable a todos los tipos y tamaños de organización (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). [35]

ISO/IEC 27001:2013 Certificable. Especifica los requisitos necesarios para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO/IEC

27001:2013 son genéricos y están destinados a ser aplicables a todas las organizaciones independientemente de su tamaño, tipo o naturaleza. [35]

ISO/IEC 27002:2013, proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información incluida la selección, implementación y gestión de los controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización. [35]

ISO/IEC 27003:2017, es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. [35]

ISO/IEC 27004:2016, proporciona directrices con la finalidad de ayudar a las organizaciones a evaluar el rendimiento de la seguridad de la información y la eficacia de un sistema de gestión de seguridad de la información con el fin de cumplir con los requisitos de ISO/IEC 27001: 2013. [35]

ISO/IEC 27005:2011, proporciona directrices para la gestión de riesgos de seguridad de la información, es compatible con los conceptos generales especificados en ISO / IEC 27001 y está diseñado para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. [35]

ISO/IEC 27006:2015, especifica los requisitos y proporciona una guía para los organismos que proporcionan auditoría y certificación de un sistema de gestión de seguridad de la información (ISMS), además de los requisitos contenidos en ISO / IEC 17021-1 e ISO/IEC 27001. Está destinado principalmente para apoyar la acreditación de los organismos de certificación que proporcionan la certificación ISMS. [35]

ISO/IEC 27007:2017, proporciona orientación sobre la gestión de un programa de auditoría del sistema de gestión de seguridad de la información (ISMS), sobre la realización de auditorías y sobre la competencia de los auditores de ISMS, además de la orientación contenida en ISO 19011:2011. [35]

ISO/IEC 27008:2011, proporciona orientación sobre la revisión de la implementación y operación de controles, incluida la verificación de cumplimiento técnico de los

controles del sistema de información, de conformidad con los estándares de seguridad de la información establecidos por una organización. [35]

ISO/IEC 27009:2016, define los requisitos para el uso de ISO/IEC 27001 en cualquier sector (campo, área de aplicación o sector de mercado). Indica cómo incluir requisitos adicionales a la norma ISO/IEC 27001, cómo refinar cualquiera de los requisitos y cómo incluir controles o conjuntos de controles además de ISO/IEC 27001:2013. [35]

4.4.4 Ventajas de implantar un Sistema de Gestión de Seguridad de la Información basado en la ISO/IEC 27001:2013

- Disminuir el riesgo, y reducción de gastos asociados.
- Reducir la incertidumbre de conocer los riesgos e impactos asociados.
- Mejora constante de la gestión de seguridad de la información.
- Garantizar la continuidad del negocio.
- Aumento de competitividad mejorando la imagen corporativa.
- Incremento de confianza.
- Aumento de la rentabilidad, que derive del control de riesgos.
- Cumplir la legislación vigente relacionada a la seguridad de la información.
- Aumentar las oportunidades de negocio.
- Reducir los costos asociados a los incidentes.
- Mejorar la participación de los usuarios en la gestión de la seguridad.
- Integración con distintos sistemas de gestión como la norma ISO 9001.
- Mejorar los procesos y servicios prestados. [33]

4.5 Plan de Gestión de Seguridad Informática

En esta primera fase se presenta el Plan de Gestión de Seguridad Informática, el cual está considerado como un modelo estructurado de carácter preventivo el cual tiene como objetivo principal garantizar que los riesgos de la seguridad de la información sean analizados y mitigados por parte del Departamento de Tecnología de la Información de la empresa Plasticaucho Industrial de una forma eficiente y estructurada. El plan está propuesto de las siguientes etapas:

- Alcance
- Definir política de seguridad
- Declaración de aplicabilidad

- Implementación de procedimientos y controles

Es importante mencionar que el Plan de Gestión de Seguridad Informática será desarrollado en base a los dominios y controles de la ISO 27001 que en la actualidad está vigente, la cual es la versión del año 2013.

4.5.1 Definición de Alcance

Para definir el alcance tomamos en cuenta los aspectos importantes como activos, estructura de la organización, recursos, entre otras que forman parte de la empresa en sus labores diarias. Cuando ya se haya elaborado la definición del alcance, la responsabilidad del alcance será asumida por el personal del departamento de Tecnología de la Información encargado de procesos de seguridad.

Plasticaucho Industrial define el alcance de acuerdo a los servicios y sistemas en la que está involucrada la información, esto corresponde con los procesos diarios de la empresa en cada una de las áreas.

Los procesos que estarán considerados en el alcance, se detallan a continuación:

- Mantenimiento preventivo, se refiere a equipos físicamente como de los diferentes sistemas que se gestionan (hardware y software). Habrá una revisión periódica de ciertos aspectos del hardware y software, con el objetivo de mantener un rendimiento confiable tanto de los equipos como de los sistemas, manteniendo siempre la integridad de los datos.
- Gestión de recursos humanos, aspecto importante donde el personal debe comprometerse a salvaguardar la información. Se definirán responsabilidades de la administración, así como las pautas para garantizar la seguridad de los recursos y la información durante el período de trabajo, así como la fase posterior o la finalización o el cambio de empleo.
- Gestión de activos, establecido como la sección más importante es, sin duda, la gestión de activos que son propiedad de la empresa Plasticaucho Industrial. Se establecerán parámetros tales como la definición de responsabilidades y la regulación del uso apropiado, evidentemente después de que se haya llevado a cabo la gestión completa de los riesgos y vulnerabilidades potenciales.

- Control de acceso, necesario verificar la identidad de un empleado para otorgar el acceso a un recurso físico o lógico específico, de esta manera manteniendo la confidencialidad e integridad de la información.
- Gestión de operaciones y comunicaciones, con el fin de garantizar la disponibilidad de información y evitar que la empresa se exponga a detener sus actividades, para los cual se definirán procesos que permitan garantizar el correcto funcionamiento.

La definición del alcance está a cargo del departamento de Tecnología de la Información el cual brindará ayuda a todo el personal de la empresa en los diversos servicios y procesos de sus labores diarias.

4.5.2 Política de seguridad

Para la implementación del Plan de Gestión Informática se establece la siguiente política, la cual tendrá como objetivo cubrir la mayoría de las exigencias que están relacionadas con la gestión de la seguridad de la información:

"Fomentar prácticas de seguridad de la información, las mismas que permitan asegurar la continuidad de los procesos que están dentro del alcance definido para la empresa Plasticaucho Industrial S.A. a través de un Plan de Gestión de Seguridad Informática, manteniendo un nivel adecuado de integridad, confidencialidad y disponibilidad de la información."

Objetivos:

Los objetivos han sido definidos para garantizar el cumplimiento de la política establecida:

- Establecer políticas que permitan prevenir o disminuir los impactos de las amenazas relacionadas con la seguridad de la información.
- Implementar el Plan de Gestión de Seguridad Informática.
- Monitorear el Plan de Gestión de Seguridad Informática para garantizar la confidencialidad, disponibilidad e integridad de la información.

4.5.3 Análisis de riesgos y selección de objetivos de control

La siguiente fase para el desarrollo del Plan de Gestión de Seguridad Informática es enlazar los controles ya definidos por la Norma ISO 27001 con los activos de valor

más alto en términos del factor de riesgo, las mismas que se revisarán a partir del proyecto de tesis realizado con el tema "PLAN DE RIESGOS Y CONTINGENCIAS INFORMÁTICAS BASADO EN UN ACUERDO DE NIVEL DE SERVICIO APLICADA A LA EMPRESA PLASTICAUCHO INDUSTRIAL" realizado por el Ing. David Noe Cruz Ojeda en el año 2018, en la cual se realiza el análisis de riesgos utilizando la metodología MAGERIT.

A partir del análisis de riesgos, se presenta la tabla de activos más importantes para la empresa.

Tabla 8: Activos Tecnológicos de la empresa Plasticaucho

Tipo de Activo Descripción	ID	ACTIVO
Hardware [HW]	HW1	Servidor de BDD
	HW2	Servidor de Virtualización-PIA
	HW3	Servidor de Virtualización-CAT
	HW4	Servidor de Aplicación Mitrol
	HW5	Servidor de Comunicaciones Mitrol
	HW6	Servidor de Telefonía IP-CAT
	HW7	Servidor Administración Telefonía
	HW8	Servidor Telefonía IP-UIO
	HW9	Servidor de Impresión
	HW10	Servidor AD Principal
	HW11	Servidor AD Secundario
	HW12	Servidor de Aplicación SCCM
	HW13	Servidor Base SCCM
	HW14	Servidor Web Services
	HW15	Servidor AD Bogotá
	HW16	Nube Azure
Software [SW]	SW1	Squarenet
	SW2	Mitrol
	SW3	Hipath Manager
Redes de comunicaciones [COM]	COM1	Red Local
	COM2	Enlaces entre sucursales
	COM3	Red Inalámbrica
	COM4	Internet
	COM5	Telefonía IP
Servicios (S)	S1	Acceso a la Red Corporativa
	S2	SAP
	S3	Internet

	S4	Correo Electrónico
	S5	Mitrol
	S6	Impresión
	S7	Movilidad/Optimiza
	S8	BI
	S9	Sistema de Nómina
	S10	Respaldos y Restauración
Equipamiento Auxiliar [AUXI]	AUXI	UPS
		Aire Acondicionado
		Cableado LAN
		Cableado Eléctrico
		Fibra óptica
		Racks
Personal [P]	P1	Operadores
	P2	Jefe de Sistemas
	P3	Administrador infraestructura y Redes
	P4	Agente de Seguridades
	P5	Consultor Internos
	P6	Analistas Programadores
	P7	Usuarios Internos
Soportes de información [M]	M1	Equipos de Respaldo (NAS)

Fuente: [4]

La selección de controles se lo realiza a partir del tratamiento del riesgo, con el objetivo de eliminar vulnerabilidades o minimizar los impactos. Se ha tomado como referencia la norma ISO 27002 para una ampliación de las prácticas e implementar los controles. Los siguientes 14 anexos o dominios, son los cuales conforman el estándar ISO 27001:

- **Anexo 1:** Políticas de seguridad de la Información.
- **Anexo 2:** Organización de la seguridad de la información.
- **Anexo 3:** Seguridad de los Recursos Humanos.
- **Anexo 4:** Gestión de recursos.
- **Anexo 5:** Control de Acceso.
- **Anexo 6:** Criptografía.
- **Anexo 7:** Seguridad física y ambiental.
- **Anexo 8:** Seguridad Operacional.
- **Anexo 9:** Seguridad de las Comunicaciones.

- **Anexo 10:** Adquisición, desarrollo y mantenimiento de Sistemas.
- **Anexo 11:** Relaciones con los proveedores.
- **Anexo 12:** Gestión de Incidentes en Seguridad de la Información.
- **Anexo 13:** Aspectos de Seguridad de la Información para la gestión de la continuidad del negocio.
- **Anexo 14:** Cumplimiento.

Para la identificación de amenazas se trabajó con el listado propuesto por la metodología Magerit, la misma que plantea que una amenaza afecta a determinados activos. Para calificar la frecuencia con que las amenazas aparecen se utilizó la Tabla 28, nos ayudará para identificar los riesgos e impactos potenciales.

Tabla 9: Frecuencia de ocurrencia de amenazas

Frecuencia	ID	Rango
Frecuencia Extrema	FE	1 vez al día
Frecuencia Alta	FA	1 vez cada 2 semanas
Frecuencia Media	FM	1 vez cada 2 meses
Frecuencia Baja	FB	1 vez cada 6 meses
Frecuencia Muy Baja	FMB	1 vez al año

Fuente: [4]

Tomando en cuenta las frecuencias con sus respectivos rangos de ocurrencia se determinaron para cada amenaza, la frecuencia y el impacto por cada dimensión de valoración: [C] Confidencialidad, [D] Disponibilidad e [I] Integridad de los datos. El análisis se lo determinó por parte del tesista Ing. David Cruz en conjunto con el Coordinador de Infraestructura de la empresa Plasticaucho Industrial [4]. En la presente investigación se realizó la selección de controles que se muestran en la tabla 29, donde se indica en la columna "Objetivo de control" el dominio relacionado con la posible amenaza de cada activo informático.

Tabla 10: Selección de Controles

Tipo de Activo	Amenaza	Probabilidad de ocurrencia	Objetivos de Control	Controles de la norma ISO 27001
Hardware	A. Fuego	FMB	A1.1 Directrices de gestión de la seguridad de la información A4.1 Responsabilidad sobre los activos A5.2 Gestión de acceso de usuario A7.1 Áreas seguras A7.2 Seguridad de los equipos A12.1 Gestión de incidentes de seguridad de la información y mejoras	A7.1.1 Perímetro de seguridad física (A, B, C, D) A7.1.3 Protección contra las amenazas externas y ambientales (A, B, C, D) A4.1.3 Uso aceptable de los activos (E, K) A7.2.4 Mantenimiento de los equipos (E, K) A7.2.2 Instalaciones de suministro (F) A1.1.1 Políticas para la seguridad de la información (G) A4.1.2 Propiedad de los activos (H, L) A5.2.3 Gestión de privilegios de acceso (I, J) A12.1.1 Responsabilidades y procedimientos (M)
	B. Erupción Volcánica	FMB		
	C. Terremoto	FMB		
	D. Daños por Agua	FMB		
	E. Avería de origen físico o lógico	FMB		
	F. Corte de suministro eléctrico	FB		
	G. Errores de Administrador	FB		
	H. Pérdida de equipos	FMB		
	I. Abuso de privilegios de acceso	FMB		
	J. Acceso no autorizado	FMB		
	K. Manipulación de los equipos	FMB		
	L. Robo	FMB		
	M. Ataque destructivo	FMB		
Software	A. Avería de origen físico o lógico	FB	A1.1 Directrices de gestión de la seguridad de la información A4.1 Responsabilidad sobre los activos A5.2 Gestión de acceso de usuario A5.4 Control de acceso a sistemas y aplicaciones A8.2 Protección contra el software malicioso (malware) A8.6 Gestión de la vulnerabilidad técnica	A4.1.3 Uso aceptable de los activos (A) A1.1.1 Políticas para la seguridad de la información (B, C, E, N) A8.2. 1 Controles contra el código malicioso (D) A5.4.1 Restricción del acceso a la información (F, G) A8.6.1 Gestión de las vulnerabilidades técnicas (H, I, M) A5.4.2 Procedimientos seguros de inicio de sesión (J) A5.2.3 Gestión de privilegios de acceso (K, L)
	B. Errores de usuarios	FA		
	C. Errores de administrador	FB		
	D. Difusión de Software dañino	FB		
	E. Alteración accidental de la información	FMB		
	F. Destrucción de información	FMB		
	G. Fugas de información	FMB		
	H. Vulnerabilidades de los programas (software)	FMB		

	I. Errores de mantenimiento/actualización de programas (software)	FA		
	J. Suplantación de la identidad del usuario	FMB		
	K. Abuso de privilegios de acceso	FMB		
	L. Acceso no autorizado	FMB		
	M. Manipulación de programas	FMB		
	N. Divulgación de información	FMB		
Redes de comunicación	A. Erupción Volcánica	FMB	A1.1 Directrices de gestión de la seguridad de la información A5.2 Gestión de acceso de usuario A5.4 Control de acceso a sistemas y aplicaciones A7.2 Seguridad de los equipos A9.1 Gestión de la seguridad de las redes A9.2 Intercambio de información	A7.2.1 Emplazamiento y protección de equipos (A, B) A7.2.3 Seguridad del cableado (B) A1.1.1 Políticas para la seguridad de la información (D, K) A9.1.1 Controles de red (D) A5.4.1 Restricción del acceso a la información (E, F) A5.4.2 Procedimientos seguros de inicio de sesión (G) A5.2.3 Gestión de privilegios de acceso (H, I) A9.1.2 Seguridad de los servicios de red (J) A9.2.4 Acuerdos de confidencialidad o no revelación (K)
	B. Terremoto	FMB		
	C. Fallo de servicios de comunicaciones	FB		
	D. Alteración accidental de la información	FMB		
	E. Destrucción de la información	FMB		
	F. Fugas de información	FB		
	G. Suplantación de la identidad del usuario	FMB		
	H. Abuso de privilegios de acceso	FMB		
	I. Acceso no autorizado	FMB		
	J. Análisis de tráfico	FMB		
	K. Divulgación de información	FMB		
Servicios	A. Errores de los Usuarios	FM	A1.1 Directrices de gestión de la seguridad de la información A5.2 Gestión de acceso de usuario A5.4 Control de acceso a sistemas y aplicaciones	A1.1.1 Políticas para la seguridad de la información (A, B, C, I) A5.4.1 Restricción del acceso a la información (D, E) A5.4.2 Procedimientos seguros de inicio de sesión (F) A5.2.3 Gestión de privilegios de acceso (G, H)
	B. Errores del administrador	FM		
	C. Alteración accidental de la información	FB		
	D. Destrucción de la información	FMB		
	E. Fugas de información	FM		
	F. Suplantación de identidad del usuario	FB		
	G. Abuso de privilegios de acceso	FB		

	H. Acceso no autorizado	FB		
	I. Divulgación de información	FM		
Equipamiento Auxiliar	A. Fuego	FMB	A1.1 Directrices de gestión de la seguridad de la información A4.1 Responsabilidad sobre los activos A5.2 Gestión de acceso de usuario A7.1 Áreas seguras A7.2 Seguridad de los equipos A12.1 Gestión de incidentes de seguridad de la información y mejoras	A7.1.1 Perímetro de seguridad física (A, B, C, D) A7.1.3 Protección contra las amenazas externas y ambientales (A, B, C, D) A4.1.3 Uso aceptable de los activos (E, I) A7.2.4 Mantenimiento de los equipos (E, I) A7.2.2 Instalaciones de suministro (F) A4.1.2 Propiedad de los activos (G, J) A5.2.3 Gestión de privilegios de acceso (H) A12.1.1 Responsabilidades y procedimientos (K)
	B. Erupción Volcánica	FM		
	C. Terremoto	FMB		
	D. Daños por Agua	FMB		
	E. Avería de origen físico o lógico	FB		
	F. Corte de suministro eléctrico	FB		
	G. Pérdida de equipos	FMB		
	H. Acceso no autorizado	FMB		
	I. Manipulación de los equipos	FB		
	J. Robo	FMB		
	K. Ataque destructivo	FMB		
Personal	A. Fugas de información	FMB	A1.1 Directrices de gestión de la seguridad de la información A3.1 Antes del empleo A3.2 Durante el empleo	A1.1.1 Políticas para la seguridad de la información (A) A3.1.2 Términos y condiciones del empleo (B) A3.2.1 Responsabilidades de gestión (B) A3.2.3 Proceso disciplinario (C, D)
	B. Indisponibilidad del personal	FB		
	C. Extorsión	FMB		
	D. Ingeniería social (picaresca)	FMB		
Soportes de información	A. Fuego	FMB	A1.1 Directrices de gestión de la seguridad de la información A4.1 Responsabilidad sobre los activos A5.2 Gestión de acceso de usuario A5.4 Control de acceso a sistemas y aplicaciones A7.1 Áreas seguras A7.2 Seguridad de los equipos	A7.1.1 Perímetro de seguridad física (A, B) A7.1.3 Protección contra las amenazas externas y ambientales (A, B) A4.1.3 Uso aceptable de los activos (C, M) A7.2.4 Mantenimiento de los equipos (C, M) A7.2.2 Instalaciones de suministro (D) A1.1.1 Políticas para la seguridad de la información (E, F, G, L)
	B. Daños por agua	FMB		
	C. Averia de origen físico o lógico	FMB		
	D. Corte de suministro eléctrico	FB		
	E. Errores de los usuarios	FMB		
	F. Errores del administrador	FMB		
	G. Alteración accidental de la información	FMB		

	H. Destrucción de información	FMB	A12.1 Gestión de incidentes de seguridad de la información y mejoras	A5.4.1 Restricción del acceso a la información (H, I) A4.1.2 Propiedad de los activos (J, N) A5.2.3 Gestión de privilegios de acceso (K) A12.1.1 Responsabilidades y procedimientos (O)
	I. Fugas de información	FMB		
	J. Pérdida de equipos	FMB		
	K. Acceso no autorizado	FMB		
	L. Divulgación de información	FMB		
	M. Manipulación de los equipos	FMB		
	N. Robo	FMB		
	O. Ataque Destructivo	FMB		

Fuente: Elaboración propia a partir de [4]

4.5.4 Declaración de Aplicabilidad

Se desarrolló la declaración de aplicabilidad (SoA por las siglas en inglés de Statement of Applicability), el cual es denominado como un documento que si bien es un requisito en el estándar ISO 27001, puede ser utilizado por cualquier organización, como una manera de mantener el registro y control de las medidas de seguridad que son aplicadas. Los controles relevantes se detallan y se verifican su aplicabilidad a la situación actual de la empresa Plasticaucho Industrial S.A., respaldada por la norma ISO/IEC 27002, la misma es la versión mejorada en términos de controles que la norma ISO 27001.

El proceso consiste en enumerar los controles de seguridad que son factibles de implementar en la empresa, así como la justificación de aquellos que no lo son. La declaración de aplicabilidad incluye:

- El dominio o control de la norma ISO 27001.
- Los objetivos de control así como los controles que se llevan a cabo o se implementan.
- Los objetivos de control seleccionados y su justificación.
- Los objetivos de control que se han excluido y la justificación para tomar tal decisión.

Las personas encargadas de revisar y aprobar la declaración de aplicabilidad, son: el encargado de la Seguridad de TI y el Coordinador de Infraestructura de la empresa. Es importante mencionar que se ha utilizado el formato de SoA de la misma norma ISO.

Tabla 11: Declaración de Aplicabilidad

1 Políticas de seguridad de la información					
Objetivo: Mantener un control acerca de cómo deben ser escritas y revisadas las políticas de seguridad de la información.					
Sección	**Controles ISO 27001**	**Aplicabilidad**		**Justificación de aplicabilidad**	**Justificación de exclusión**
		Si	**No**		
1.1	Directrices de gestión de la seguridad de la información				
1.1.1	Políticas para la seguridad de la información	X		Es esencial el diseño de una política de seguridad de TI aprobada por la Gerencia que marque las líneas maestras del Plan de Gestión de Seguridad.	
1.1.2	Revisión de las políticas para la seguridad de la información	X		Es imprescindible realizar revisiones periódicas de las políticas, para garantizar el cumplimiento y evitar que no quede anticuada.	
2 Aspectos organizativos de la seguridad de la información					
Objetivo: Controlar la asignación de las responsabilidades; además de la revisión de los controles para los dispositivos móviles y el teletrabajo.					
2.1	Organización interna				
2.1.1	Roles y responsabilidades en seguridad de la información	X		Es esencial definir y documentar las diferentes responsabilidades con respecto a la seguridad de la información.	
2.1.2	Segregación de tareas	X		Es necesario separa roles del personal de acuerdo a sus capacidades en la seguridad de la información.	
2.1.3	Contacto con las autoridades	X		Las actividades llevadas a cabo deben mantener una coordinación directa con el departamento de seguridad en tecnología.	
2.1.4	Contacto con grupos de interés especial	X		Debe existir un monitoreo de interés especial, para identificar nuevos riesgos potenciales.	

2.1.5	Seguridad de la información en la gestión de proyectos	X		Es necesario agregar la seguridad como parte de la gestión de proyectos.	
2.2	Dispositivos para movilidad y teletrabajo.				
2.2.1	Política de uso de dispositivos para movilidad	X		Es necesario establecer medidas y políticas de seguridad que regulen, el uso de dispositivos para la movilidad, así como también en el caso de ser necesario trabajar desde lugares diferentes a la oficina.	
2.2.2	Teletrabajo	X			
3 Seguridad relativa a los recursos humanos					
Objetivo: Asegurar que el personal de la empresa sea el indicado; comprenda sus funciones dentro de la empresa antes, durante y después de emplear.					
3.1	Antes de la contratación				
3.1.1	Investigación de antecedentes	X		Debe ser un requisito necesario para para contratación de personal, verificar los antecedentes en concordancia con la ética y leyes relevantes.	
3.1.2	Términos y condiciones de contratación	X		Es necesario al momento de la contratación especificar las políticas y reglamentos en el cual el personal deba regirse.	
3.2	Durante la contratación				
3.2.1	Responsabilidades de gestión	X		Se debe asegurar que los empleados cumplan con las políticas de seguridad de la empresa.	
3.2.2	Concienciación, educación y capacitación en seguridad de la información	X		Es necesario la formación continua bajo capacitaciones que formen una cultura de seguridad.	
3.2.3	Proceso disciplinario	X		Definir procesos formales para el tratamiento de empleados que falten a la seguridad.	
3.3	Cese o cambio de puesto de trabajo				

3.3.1	Cese o cambio de puesto de trabajo	X		Es importante mantener políticas, que sean aclaradas durante la firma del contrato y al momento del cese de trabajo no conlleve consecuencias.	
4 Gestión de activos					
Objetivo: Controlar todo lo relacionado con el inventario de activos, su uso aceptable, clasificación de la información y además la gestión de los medios de almacenamiento.					
4.1	Responsabilidad sobre los activos				
4.1.1	Inventario de activos	X		Es fundamental conocer y mantener actualizado el listado de activos de información de la empresa.	
4.1.2	Propiedad de los activos	X		Necesario conocer el propietario o encargado de monitorear y llevar un control de activos.	
4.1.3	Uso aceptable de los activos	X		Indispensable establecer controles que promuevan la utilización adecuada de los activos.	
4.1.4	Devolución de activos	X		Debe existir un proceso formal para la devolución de los activos de información.	
4.2	Clasificación de la información				
4.2.1	Clasificación de la información	X		Necesario especificar un plan para la clasificación de la información, basándose en la confidencialidad, integridad y disponibilidad.	
4.2.2	Etiquetado de la información	X		Debe establecerse un proceso de etiquetado de información.	
4.2.3	Manipulado de la información	X		Se debe establecer medidas de control que verifiquen que solo el personal autorizado pueda manipular la información.	
4.3	Manejo de los soportes				

4.3.1	Gestión de soportes extraíbles	X		Se debe definir procedimientos para la utilización y el manejo de soportes extraíbles.	
4.3.2	Eliminación de soportes	X		Es necesario definir procedimientos para la eliminación de soportes de información.	
4.3.3	Soportes físicos en tránsito	X		Es necesario cumplir con controles de seguridad que se establezcan para soportes físicos que necesitan ser trasladados.	
5 Control de accesos					
Objetivo: Establecer y controlar las políticas de control de acceso, gestión de acceso para usuarios, control de acceso para el sistema, aplicaciones, y responsabilidades del usuario.					
5.1	Requisitos de negocio para controlar los accesos				
5.1.1	Política de control de accesos	X		Es importante mantener políticas en donde se indiquen los accesos creados, a quienes y, a que sistemas.	
5.1.2	Acceso a las redes y a los servicios de red	X		Los accesos deben ser autorizados y controlados, en sistemas y aplicaciones.	
5.2	Gestión de acceso de usuario				
5.2.1	Registro y baja de usuario	X		Debe existir un procedimiento adecuado de control de la base de datos de los usuarios.	
5.2.2	Provisión de acceso de usuario	X		Hay que disponer de una gestión centralizada de permisos para los usuarios.	
5.2.3	Gestión de privilegios de acceso	X		En requerida una monitorización periódica de quien tiene privilegios de administrador.	
5.2.4	Gestión de información confidencial de autenticación de usuarios	X		Se debe controlar para mantener la confidencialidad de información y evitar su filtración.	

5.2.5	Revisión de los derechos de acceso de los usuarios	X		Necesario revisar los derechos de acceso periódicamente para detectar permisos erróneos.	
5.2.6	Retirada o reasignación de los derechos de acceso	X		Revisión de los permisos al cese o cambio de puesto de trabajo, de igual manera con personal externo.	
5.3	Responsabilidades del usuario				
5.3.1	Uso de información confidencial para la autenticación	X		Es necesario para mantener segura la información sensible como contraseñas.	
5.4	Control de acceso a sistemas y aplicaciones				
5.4.1	Restricción del acceso a la información	X		Se debe restringir los accesos indeseados o para personas ajenas a la empresa.	
5.4.2	Procedimientos seguros de inicio de sesión	X		Importante para todo sistema y equipos sensibles se requieran autenticación, garantizando inicios de sesión seguros.	
5.4.3	Sistema de gestión de contraseñas	X		Necesario para controlar el acceso con contraseñas de calidad para todo sistema y equipo.	
5.4.4	Uso de utilidades con privilegios del sistema	X		Se debe revisar y proporcionar acceso específicamente para personas autorizadas.	
5.4.5	Control de acceso al código fuente de los programas	X		Control establecido para evitar la modificación maliciosa de programas.	
6 Criptografía					
Objetivo: Establecer controles relacionados con la gestión de cifrado y claves, para la compartición de información.					
6.1	Controles criptográficos				
6.1.1	Política de uso de los controles criptográficos	X		Es necesario desarrollar e implantar una política de uso de controles criptográficos para la protección de la información.	

6.1.2	Gestión de claves	X		Es necesario la gestión de claves, para tener en cuenta el ciclo de vida completo (generación, uso y protección, distribución, renovación o destrucción), además para determinar fechas de activación y desactivación de claves.	
7 Seguridad física y ambiental					
Objetivo: Definir controles para las áreas físicas; estableciendo controles de entrada, protección contra amenazas, y seguridad de los equipos.					
7.1	Áreas seguras				
7.1.1	Perímetro de seguridad física	X		Necesario para proteger los equipos y activos de información.	
7.1.2	Controles físicos de entrada	X		Necesario para establecer controles físicos de entrada a sitios donde se encuentren los equipos y activos de información.	
7.1.3	Seguridad de oficinas, despachos y recursos	X		Indispensable para controlar la seguridad de los lugares donde se encuentre información sensible.	
7.1.4	Protección contra las amenazas externas y ambientales	X		Es necesario para establecer un plan ante amenazas ambientales o desastres naturales, para la protección de equipos.	
7.1.5	El trabajo en áreas seguras	X		Indispensable para la protección física en áreas seguras y establecer prohibiciones.	
7.1.6	Áreas de acceso público, carga y descarga	X		Es necesario para establecer puntos sensibles para la seguridad física y los respectivos controles en las áreas de acceso público.	
7.2	Seguridad de los equipos				
7.2.1	Emplazamiento y protección de equipos	X		Necesario para establecer zonas estratégicas que permitan disminuir el riesgo de amenazas y daños	

				ambientales que afecten el estado físico de los equipos.	
7.2.2	Instalaciones de suministro	X		Es necesario mantener monitoreado periódicamente el sistema UPS que proporcione potencia adecuada, confiable y de calidad.	
7.2.3	Seguridad del cableado	X		Esencial para la protección y separación entre cableado de comunicaciones con el de suministro eléctrico, y evitar daños e interferencias.	
7.2.4	Mantenimiento de los equipos	X		Importante para realizar programaciones periódicas, para efectuar mantenimientos de los equipos.	
7.2.5	Salida de activos fuera de las dependencias de la empresa	X		Es necesario controlar los equipos fueras de las instalaciones, así también mantener un registro de los usuarios que lo puedan realizar.	
7.2.6	Seguridad de los equipos y activos fuera de las instalaciones	X		Necesario establecer el uso aceptable y compromiso del empleado en la seguridad de los equipos fuera de las instalaciones.	
7.2.7	Reutilización o eliminación segura de equipos	X		Indispensable controlar la reasignación o eliminación de equipos, y el respaldo o borrado seguro de la información.	
7.2.8	Equipo informático de usuario desatendido	X		Requerido para aplicar a todos los equipos y evitar la suplantación de identidad.	
7.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	X		Aplicable para todos los usuarios y los respectivos equipos que eviten la suplantación y robo de información.	
8 Seguridad en la operativa					
Objetivo: Revisar los controles relacionados con la gestión de la producción en las Tecnologías de la Información.					

8.1	Procedimientos y responsabilidades operacionales				
8.1.1	Documentación de procedimientos de operación	X		Debe existir en los procesos operativos la documentación con estricta gestión y seguridad, para ponerlos a disposición de los demás.	
8.1.2	Gestión de cambios	X		Debe existir un plan de control para gestionar los cambios en sistemas operacionales.	
8.1.3	Gestión de capacidades	X		Necesario para realizar monitoreos continuos del uso de los recursos, evitando interrupciones de servicio.	
8.1.4	Separación de entornos de desarrollo, prueba y producción	X		Requerido para mantener la seguridad de la información separando datos para sistemas de pruebas o de lanzamiento.	
8.2	Protección contra código malicioso (malware)				
8.2.1	Controles contra el código malicioso	X		Es necesario garantizar la protección de la información, y establecer una programación para realizar controles antimalware.	
8.3	Copias de seguridad				
8.3.1	Copias de seguridad de la información	X		Es importante que se establezcan periodos adecuados, para que se realicen copias de seguridad garantizando que la información este respaldada y disponible.	
8.4.	Registro de actividad y supervisión				
8.4.1	Registro y gestión de eventos de actividad	X		Es necesario realizar un monitoreo y registro de las eventualidades que se presenta dentro de la red corporativa.	

8.4.2	Protección de los registros de información	X		Los servicios y la información de registro de la actividad deben estar protegidos contra acciones forzadas o accesos no autorizados.	
8.4.3	Registros de administración y operación	X		Las actividades del administrador y operador del sistema deben registrarse.	
8.4.4	Sincronización de relojes	X		Los relojes de todos los sistemas de procesamiento de información dentro del dominio corporativo deben estar sincronizados con una fuente de tiempo acordada y precisa.	
8.5	Control del software en explotación				
8.5.1	Instalación del software en sistemas en producción	X		Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	
8.6	Gestión de la vulnerabilidad técnica				
8.6.1	Gestión de las vulnerabilidades técnicas	X		Se debe monitorear la red, mantener actualizado los sistemas y obtener información sobre las vulnerabilidades técnicas de los sistemas de información utilizados.	
8.6.2	Restricciones en la instalación de software	X		Indispensable para controlar que solo los administradores instalen software en los equipos.	
8.7	Consideraciones de las auditorías de los sistemas de información				
8.7.1	Controles de auditoría de los sistemas de información	X		Necesario para garantizar, el correcto respaldo y confidencialidad de la información en los sistemas evitando interrupciones.	
9 Seguridad de las comunicaciones					
Objetivo: Controlar las acciones relacionados con la seguridad de las redes en el intercambio de información siendo interna o externamente.					
9.1	Gestión de la seguridad en las redes				

9.1.1	Controles de red	X		La red debe estar controlada adecuadamente para protegerla de las amenazas y mantener la seguridad en los sistemas y aplicaciones.	
9.1.2	Seguridad de los servicios de red	X		Deben identificar e incluir, en cualquier acuerdo sobre los servicios de red, las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios.	
9.1.3	Segregación de redes	X		Necesaria para controlar la segregación de red según los grupos de servicios, usuarios y sistemas de información.	
9.2	Intercambio de información con partes externas				
9.2.1	Políticas y procedimientos de intercambio de información	X		Se debe implementar políticas, procedimientos y controles de intercambio de información sean por canales seguros.	
9.2.2	Acuerdos de intercambio	X		Necesario para establecer acuerdos que deben abordar el intercambio seguro de información entre la organización y partes externas.	
9.2.3	Mensajería electrónica	X		La información que se administra mediante la mensajería electrónica debe estar protegida.	
9.2.4	Acuerdos de confidencialidad y secreto	X		Necesario para establecer acuerdos documentados para regular la confidencialidad y "no divulgación" de información.	
10 Adquisición, desarrollo y mantenimiento de los sistemas de información					
Objetivo: Administrar los controles que definen los requerimientos de seguridad en los procesos de desarrollo y soporte de los sistemas de información.					
10.1	Requisitos de seguridad en los sistemas de información				

10.1.1	Análisis y especificación de los requisitos de seguridad	X		La seguridad de la información debe incluirse en los requisitos para nuevos sistemas o mejoras a los sistemas de información existentes.	
10.1.2	Asegurar los servicios de aplicaciones en redes públicas		X		La empresa no cuenta con servicios accesibles públicos. La web corporativa no tiene acceso a información sensible.
10.1.3	Protección de las transacciones de servicios de aplicaciones	X		Es necesario para garantizar la protección de las transacciones entre aplicaciones y garantizar las comunicaciones extremo a extremo.	
10.2	Seguridad en los procesos de desarrollo y soporte				
10.2.1	Política de desarrollo seguro de software	X		La empresa debe establecer políticas que fomenten el desarrollo seguro de software, para seguridad de la información.	
10.2.2	Procedimientos de control de cambios en los sistemas	X		Se debe realizar una documentación que identifique los procedimientos de cambio en los sistemas.	
10.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	X		Las aplicaciones de negocio deben ser revisadas y probadas posterior al cambio, para garantizar que no se hayan generado impactos adversos en las operaciones o la seguridad de información.	
10.2.4	Restricciones a los cambios en los paquetes de software	X		Se debe controlar los cambios en los paquetes de software, limitándose a los cambios que son realmente necesarios.	
10.2.5	Uso de principios de ingeniería en protección de sistemas	X		Los sistemas deben estar establecidos, documentados y revisado la seguridad en todo el diseño de software	

10.2.6	Seguridad en entornos de desarrollo	X		Se debe establecer una protección adecuada de los entornos de desarrollo e integración de sistemas, que abarque todo el ciclo de vida del desarrollo del sistema.	
10.2.7	Externalización del desarrollo de software	X		La empresa debe supervisar y monitorear las actividades de desarrollo del sistema que se han subcontratado.	
10.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	X		Las pruebas de funcionalidad deben realizarse en aspectos de seguridad durante las etapas de desarrollo.	
10.2.9	Pruebas de aceptación	X		Se debe establecer procesos de prueba y criterios para la aceptación de sistemas de información nuevos, y/o nuevas versiones.	
10.3	Datos de prueba				
10.3.1	Protección de los datos utilizados en pruebas	X		Se deben seleccionar cuidadosamente los datos de prueba, los mismos que deben ser monitoreados.	
11 Relación con proveedores					
Objetivo: Analizar los controles que están o deben incluirse en los contratos, para revisar el cumplimientos de los proveedores.					
11.1	Seguridad en las relaciones con proveedores				
11.1.1	Política de seguridad de la información en las relaciones con los proveedores	X		La empresa debe documentar las condiciones seguridad de la información en los activos, para mitigar los riesgos que se asocien al acceso por parte de los proveedores.	
11.1.2	Requisitos de seguridad en contratos con terceros	X		Los acuerdos con terceros que impliquen acceso, procesamiento, comunicación o gestión de la información de la empresa deben cubrir todos los requisitos de seguridad relevantes.	

11.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	X		Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información relacionados con la cadena de suministro de productos.	
11.2	Gestión de la prestación del servicio por suministradores				
11.2.1	Supervisión y revisión de los servicios prestados por terceros	X		La empresa debe monitorear, revisar y auditar la presentación de los servicios del proveedor regularmente.	
11.2.2	Gestión de cambios en los servicios prestados por terceros	X		Los cambios en servicios prestados por terceros deben mantenerse o mejorar las condiciones de las políticas de seguridad de la información.	
12 Gestión para incidentes en la seguridad de la información					
Objetivo: Establecer controles que permitan encontrar y archivar debilidades, para que posterior sean analizadas y garantizadas con una solución efectiva.					
12.1	Gestión de incidentes de seguridad de la información y mejoras				
12.1.1	Responsabilidades y procedimientos	X		Se deben establecer responsabilidades y procedimientos de gestión para garantizar una respuesta inmediata, eficaz y ordenada a los incidentes de seguridad de la información.	
12.1.2	Notificación de los eventos de seguridad de la información	X		Los eventos de seguridad de la información deben ser comunicados lo más pronto posible, al personal o administrador apropiado.	
12.1.3	Notificación de puntos débiles de la seguridad	X		Se debe informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios.	
12.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	X		Los eventos de seguridad de la información deben ser evaluados antes de la toma de una decisión.	

12.1.5	Respuesta a los incidentes de seguridad	X		Se debe contar con un plan de contingencia documentado los procedimientos realizados que solventen los incidentes.	
12.1.6	Aprendizaje de los incidentes de seguridad de la información	X		Se debe basar en el conocimiento obtenido del análisis y resolución de incidentes, para reducir la probabilidad de impacto en incidentes futuros.	
12.1.7	Recopilación de evidencias	X		Se debe definir y aplicar procedimientos necesarios ante cada evento negativo, crear un registro de incidentes.	
13 Aspectos para la seguridad de la información y gestión de la continuidad del negocio					
Objetivo: Establecer controles que permitan la planificación para la continuidad del negocio.					
13.1	Continuidad de la seguridad de la información				
13.1.1	Planificación de la continuidad de la seguridad de la información	X		Es necesario determinar requisitos necesarios para la seguridad de la información y su administración en situaciones adversas.	
13.1.2	Implantación de la continuidad de la seguridad de la información	X		Indispensable para que pueda ser puesto en marcha el plan de continuidad de seguridad de la información.	
13.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	X		Periódicamente se debe realizarse una revisión y evaluación de la continuidad para la seguridad de la Información.	
13.2	Redundancias				
13.2.1	Disponibilidad de instalaciones para el procesamiento de la información	X		Se debe implementar una redundancia suficiente en las instalaciones de procesamiento de información y en correspondencia con los requisitos de disponibilidad.	
14 Cumplimiento					

Objetivo: Verificar el cumplimiento tanto de los controles, políticas y normas establecidas; así como las normativas contractuales con el fin de garantizar una adecuada gestión de la seguridad de la información.					
14.1	Cumplimiento de los requisitos legales y contractuales				
14.1.1	Identificación de la legislación aplicable	X		Se debe identificar todos los requisitos legales reglamentarios y contractuales, como ley de seguros y LOPD.	
14.1.2	Derechos de propiedad intelectual (DPI)	X		Se debe implementar para garantizar el cumplimiento de requisitos legales, relacionados con los derechos de propiedad intelectual y el uso de software original.	
14.1.3	Protección de los registros de la organización	X		Es importante establecer protección de los registros importantes de la empresa, evitando perdida, destrucción, falsificación o publicación no autorizada.	
14.1.4	Protección de datos y privacidad de la información personal	X		En necesario determinar normativas para mantener un control y privacidad de los datos personales, tanto de los usuarios como de la empresa.	
14.1.5	Regulación de los controles criptográficos	X		Al aplicar mecanismos de cifrado es necesario tener en cuenta las normativas de uso de controles criptográficos vigentes, como la firma electrónica.	
14.2	Revisiones de la seguridad de la información				
14.2.1	Revisión independiente de la seguridad de la información	X		El enfoque de la compañía para la implementación y administración de la seguridad de la información debe revisarse en base a revisiones de manera independiente, en intervalos planificados o	

				cuando se producen cambios específicos en la organización.	
14.2.2	Cumplimiento de las políticas y normas de seguridad	X		Se debe revisar y evaluar periódicamente al personal el cumplimiento de las políticas de seguridad de la información.	
14.2.3	Comprobación del cumplimiento técnico.	X		Es necesario revisar regularmente el cumplimiento y que realmente funcionen.	

Fuente: Elaboración propia

4.5.5 Nivel de cumplimiento y aplicación de la norma ISO 27001

Sobre la base de la declaración de aplicabilidad realizada, se analiza su aplicación actual en la empresa y se determina el nivel de cumplimiento para elaborar posteriormente la propuesta de mejora en cada uno de los controles relevantes de la norma ISO 27001.

Después de realizar el análisis de cada control, junto con el analista de seguridad del departamento de tecnología de la información, se determina el porcentaje de cumplimiento de cada uno de ellos para obtener una representación cuantitativa del cumplimiento.

4.5.6 Control de Anexos

1. Políticas de seguridad de la información

1.1. Políticas para la seguridad de la información

La empresa Plasticaucho Industrial, mantiene una estructura administrada por políticas que cubren los riesgos relacionados con la información. Protección de activos informáticos, sistemas, servicios y control de áreas.

La comunicación de las políticas se las realiza a través del portal IsoTools, donde se mantiene el documento formalizado y aprobado, el mismo que esta disposición de todo el personal para su conocimiento.

1.2. Revisión de las políticas para la seguridad de la información

Las políticas establecidas cuentan con un formato y estilo consistente, cumpliendo las revisiones debidas. Además existe un proceso en el cual se revisa periódicamente el documento para realizar actualizaciones y, posterior su comunicación hacia el personal de la empresa.

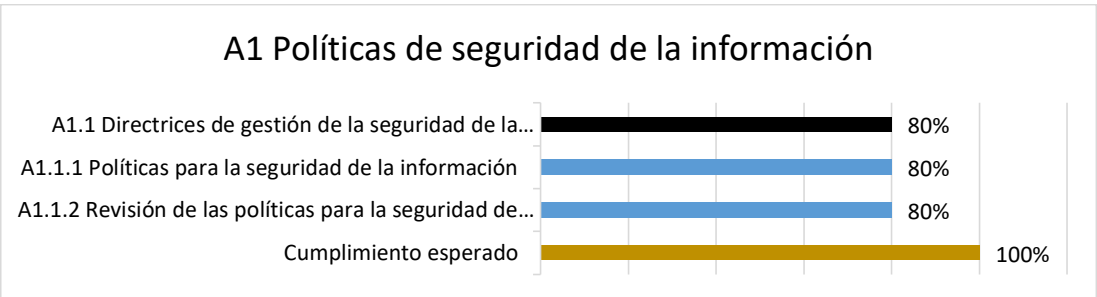

Fig. 31: Cumplimiento - Políticas de seguridad de la información
Fuente: Elaboración propia

En la figura anterior se puede observar que los controles relacionados con las Políticas de seguridad de la información se las llevan a cabo de forma óptima, pero es siempre necesario realizar revisiones periódicas y actualizaciones para que su funcionamiento sea excelente.

2. Aspectos organizativos de la seguridad de la información

2.1. Organización interna

2.1.1. Roles y responsabilidades en seguridad de la información

En el departamento de TI están establecidas actividades separadas, según el cargo y las funciones que tienen que cumplir; es así que para la seguridad de la información se cuenta con el personal capacitado en el Análisis de Seguridades, Desarrollo de Software, Infraestructura, Hardware/Software, Consultoría y Soporte Técnico.

2.1.2. Segregación de tareas

El personal que labora en la empresa Plasticaucho Industrial tiene definido su rol, proceso en el que se va a realizar sus funciones de acuerdo a sus conocimientos y competencias. De igual manera en cada proceso o área de trabajo existe una persona encargada de autorizar o para la toma de decisiones; la segregación de tareas está definido en un documento denominado Perfil Tecnológico el cual se mantiene actualizado y en el que se describe el cargo que va ocupar con su respectivo equipo tecnológico y software que va a utilizar para ejercer sus labores.

2.1.3. Contacto con las autoridades

En la empresa actualmente se cumple con este control conforme a la estructura organizacional que tiene Plasticaucho Industrial. El área de TI cumple con sus funciones, es decir salvaguardar la información que maneja la empresa; en el caso de encontrarse ante un problema grave o que comprometa la seguridad interna, el departamento de tecnología debe informar al jefe inmediato del área, quien a su vez emite la alerta al administrador interno o externo a la organización involucrado con el inconveniente, para en conjunto dar una solución inmediata.

2.1.4. Contacto con grupos de interés especial

La empresa Plasticaucho Industrial por la magnitud de información que maneja, decidió contratar los servicios de proveedores externos para la administración de la red Corporativa y mantener la seguridad de la información, es así que en conjunto con el departamento de TI mantienen un contacto especial y profesional para el tratamiento de riesgos de la información, compartición de amenazas, nuevas tecnologías de seguridad, buenas prácticas de seguridad, vulnerabilidades, entre otras, de esta manera tener controlado y mantener la integridad de la información importante de la empresa.

2.1.5. Seguridad de la información en la gestión de proyectos

El control de la seguridad de la información en proyectos se lo realiza de una manera informal, no se mantiene registros actualizados de los nuevos desarrollos, cambios o mejoras que se realicen en los sistemas y aplicaciones existen en la empresa; lo cual no permite identificar de manera oportuna los riesgos de la información además de verificar los requisitos de seguridad para cada etapa de los proyectos y los que estén relacionados con la información.

2.2. Dispositivos para movilidad y teletrabajo.

2.2.1. Política de uso de dispositivos para movilidad

No existe un documento donde se expongan las políticas que se relacionen para usuarios que utilicen dispositivos móviles y sistemas portátiles, el departamento de TI después de realizar la entrega de los dispositivos, mantiene el control de los equipos de manera remota para verificar y validar que las aplicaciones se encuentren en funcionamiento. No se mantiene un control formal para evaluar el acceso y el mantenimiento íntegro de la información.

2.2.2. Teletrabajo

Los controles de seguridad para teletrabajo se los administra conforme a un procedimiento interno de la empresa, en el cual para tener acceso a la red Corporativa desde el exterior de las instalaciones, cualquier personal que labore en la empresa debe tener autorización de su gerencia y el motivo por el cual lo requiere se lo debe informar al departamento de TI.

Realizado el procedimiento, el personal encargado de TI habilitará la conexión VPN al usuario para que pueda ejercer sus labores netamente relacionados con el cumplimiento de su trabajo y de las políticas de seguridad de la información.

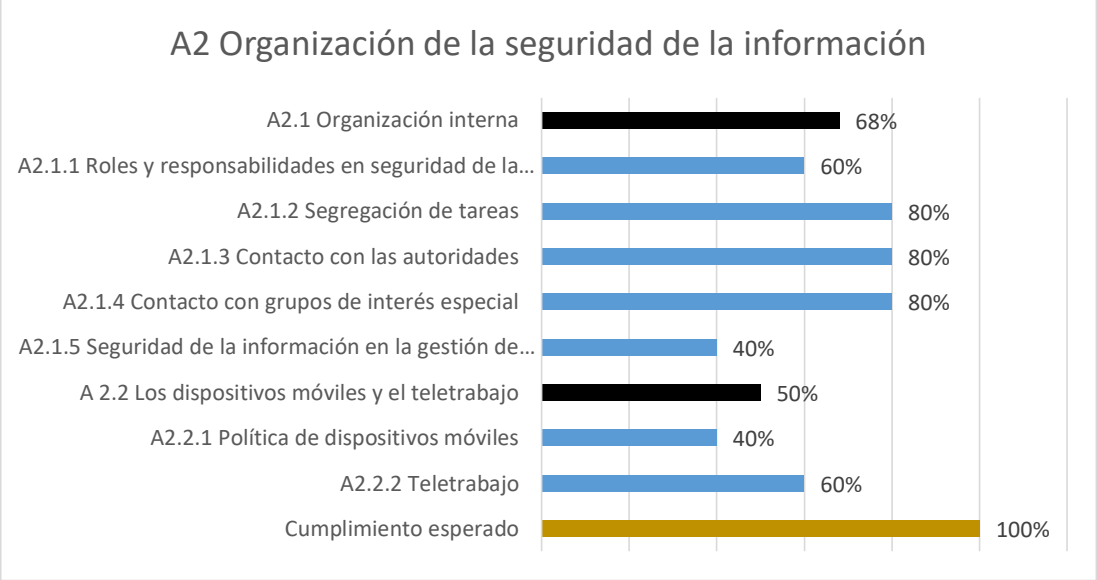

Fig. 32: Cumplimiento - Organización de la seguridad de la información
Fuente: Elaboración propia

En la figura anterior se puede apreciar que los porcentajes de cumplimiento de los controles referentes a la segregación de tareas, contacto con las autoridades y grupos de interés especial son a los que se ha puesto mayor énfasis.

Los controles donde es necesario realizar mejoras en cuanto a su aplicabilidad es la seguridad de la información en gestión de proyectos y política de dispositivos móviles.

3. Seguridad relativa a los recursos humanos

3.1. Antes de la contratación

3.1.1. Investigación de antecedentes

El control que se mantiene dentro de la empresa para la contratación del personal se basa en políticas establecidas entre el departamento de Seguridad Física, que se encargan de realizar la investigación y documentar los antecedentes de cada persona que se encuentre postulando para un cargo dentro de la empresa; y el departamento de Gestión Humana conjuntamente con el Jefe de área donde se requiera la contratación; son los que realizan un análisis al perfil laboral,

conocimientos, referencias, entre otros aspectos personales para realizar un proceso de selección adecuado y correcto en cubrir las áreas de la organización.

3.1.2. Términos y condiciones de contratación

Los términos y las condiciones ligadas con la seguridad de la información para los empleados y subcontratos son difundidos claramente antes de iniciar sus actividades en la empresa; con esto evitar la divulgación de información confidencial de la organización.

3.2. Durante la contratación

3.2.1. Responsabilidades de gestión

Los empleados al iniciar a laborar dentro de la empresa, el departamento de TI es el encargado de otorgar los equipos y claves de acceso a los sistemas que va a utilizar. En el acto de entrega se capacita al usuario sobre la seguridad de la información en el equipo, el uso adecuado del software y contraseñas; todo el proceso se registra en un acta de entrega-recepción firmada por ambas partes.

3.2.2. Concienciación, educación y capacitación en seguridad de la información

El compromiso que dispone el departamento de Tecnologías de la Información, es informar a todos los empleados la importancia de cumplir las políticas de seguridad de la información establecidas en los contratos, además de informar incidentes de seguridad, uso de contraseñas, software malicioso, entre otros.

Plasticaucho Industrial a través del departamento de TI difunde correos electrónicos informativos a todo el personal de la empresa, para concientizar e informar sobre la seguridad e integridad de la información que debe mantener la organización.

3.2.3. Proceso disciplinario

El control que se realiza esta cubierto en los contratos y acuerdos establecidos por la empresa para el personal de Plasticaucho como para personas externas a la organización, lo cual es la capacitación inicial y conocimiento continúo de los procesos que se realicen, si es el caso que involucre la seguridad de la información.

3.3. Cese o cambio de puesto de trabajo

3.3.1. Cese o cambio de puesto de trabajo

Se encuentra establecido para comunicar al empleado las responsabilidades sobre la seguridad de la información después de finalizar el contrato o cambio de puesto de trabajo, las cuales aplican en las responsabilidades legales y acuerdos de confidencialidad cuando sean necesarios.

Se establece periodos de vigencia para después de la desvinculación en los términos y condiciones del contrato como son:

- Tiempo estimado para el bloqueo o eliminación del usuario de los registros de la empresa.
- Traspaso de la información confidencial o necesaria para el personal que sustituya en el cargo.
- Deberes y responsabilidades que permanecen válidos después de la desvinculación.
- Cambiar o actualizar las responsabilidades en el contrato de empleo ante cambios de puesto de trabajo dentro de la organización.

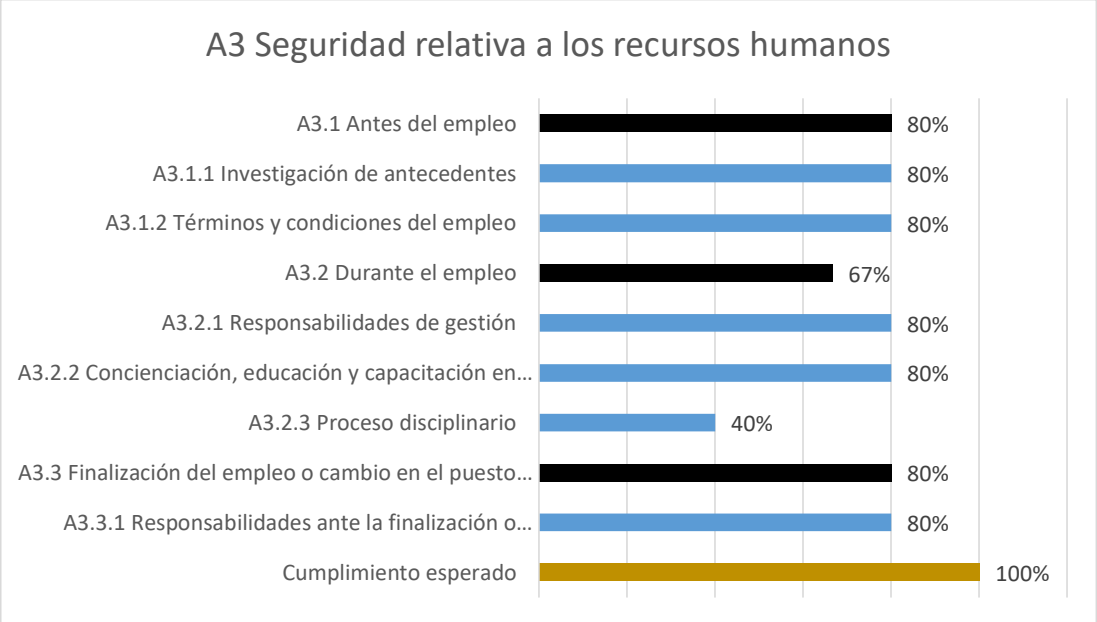

Fig. 33: Cumplimiento - Seguridad relativa a los recursos humanos
Fuente: Elaboración propia

En la figura 33 se puede observar que la mayoría de los controles cumplen una aplicabilidad óptima pero en la que se debe mejorar su índice en el proceso disciplinario de la seguridad relativa a los recursos humanos dando seguimiento los cumplimientos de contratos por parte del personal interno y externo.

4. Gestión de activos

4.1. Responsabilidad sobre los activos

4.1.1. Inventario de activos

El control de los activos dentro de la empresa es de manera óptima, en donde cada uno de los activos está correctamente identificado de acuerdo a su importancia, tipo de activo o información; adicional se encuentra asignado al área al que pertenece y su responsable. El proceso se encuentra gestionado por el personal de TI que tiene a cargo la Gestión de Hardware y Software.

4.1.2. Propiedad de los activos

Los activos son identificados de acuerdo al área y el responsable de su gestión; el inventario se encuentra documentado formalmente, en el cual se define las restricciones de acceso y las clasificaciones de activos importantes, además se garantiza el manejo adecuado cuando es eliminado o destruido.

4.1.3. Uso aceptable de los activos

La empresa cuenta con un documento formalizado, donde se explican las políticas para el uso aceptable de los recursos tecnológicos dentro de la empresa, el control de accesos dentro la red corporativa, la navegación en páginas de internet así como la monitorización del uso apropiado de la información de los activos.

4.1.4. Devolución de activos

Se controla que todos los empleados o contratistas devuelvan los activos de información una vez que haya finalizado el periodo de utilización o contrato. El proceso se formaliza mediante documentos que verifiquen el cumplimiento de las cláusulas de devolución de activos físicos y/o electrónicos, además está establecido el procedimiento para transferencia y borrado de la información de forma segura en el caso que sea pertinente.

4.2. Clasificación de la información

4.2.1. Clasificación de la información

La información sea física o digital de la empresa está clasificada según su área y el valor que tiene para la organización, de igual manera existe un proceso para que los usuarios puedan acceder a esa información. Es necesario tener autorización por el administrador principal de esa información para que el departamento de TI otorgue los permisos necesarios a la(s) persona(s) que se requiera; el nivel de protección es indispensable para lo cual se maneja permisos de lectura o lectura y escritura de esta manera evitando la divulgación o modificación no autorizada o accidental.

4.2.2. Etiquetado de la información

La información de la empresa se encuentra identificado de acuerdo con el área que la maneja sea digital o físicamente, de igual manera se toma en cuenta los activos de los sistemas que están etiquetados para tener la información clasificada como sensible o crítica y reservada su acceso.

4.2.3. Manipulado de la información

La manipulación de la información, como procedimiento consecuente de la correcta clasificación de los activos que permitirá el mejor manejo, procesamiento, almacenamiento y la comunicación de la información. Se considera los siguientes procedimientos para garantizar la seguridad de los datos de la organización.

- Se considera las restricciones de acceso de acuerdo al nivel de clasificación.
- Creación y manejo de un registro de autorizaciones de acceso o uso de los activos.
- En el intercambio de información se mantiene el etiquetado para que la interpretación sea la correcta.

4.3. Manejo de los soportes

4.3.1. Gestión de soportes extraíbles

Los soportes extraíbles son una de las brechas más importantes de la seguridad de la información, por lo cual se ha mantenido un control dentro de la empresa para gestionar este tipo de equipos; se consideró indicar al personal la necesidad que

tiene para su uso y tener autorización, así también como los controles apropiados para mantener la confidencialidad de los datos que se encuentren almacenados.

4.3.2. Eliminación de soportes

La eliminación de soportes están establecidos con procedimientos de borrado seguro cuando haya llegado la finalización de su uso, se trata de minimizar o evitar que los datos confidenciales puedan ser recuperados una vez que el dispositivo se haya dado de baja.

4.3.3. Soportes físicos en tránsito

Dentro de la empresa se trata de establecer controles para proteger la información cuando los soportes necesitan ser trasladados a otras ubicaciones. Se tiene un registro y autorización de la salida de un soporte, además se administra los controles posteriores al traslado, como es lugar de destino, transportistas, embalaje, condiciones ambientales y los recursos necesarios para su instalación en el nuevo sitio.

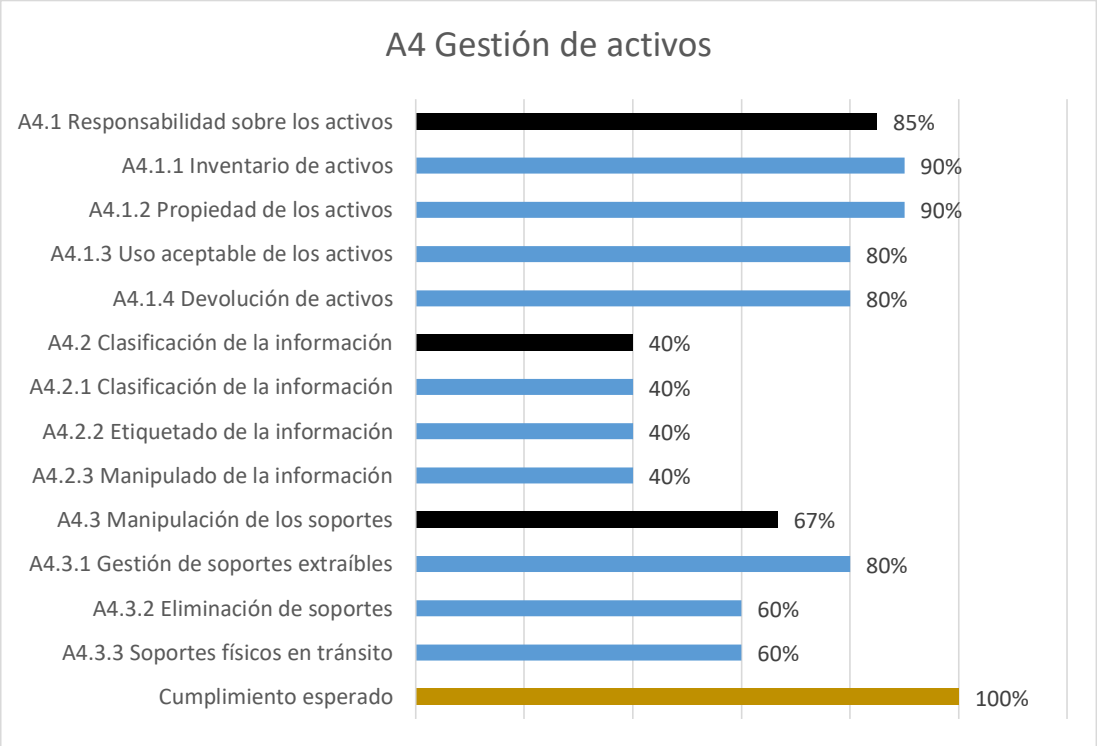

Fig. 34: Cumplimiento - Gestión de activos
Fuente: Elaboración propia

En la figura anterior se aprecia que los porcentajes de cumplimiento de los controles que refieren al inventario de activos y propiedad de los activos son los mejores preparados por el departamento de TI en cuanto a su aplicación.

Los controles que son necesario aplicar mejoras son en los controles de clasificación, etiquetado y manipulado de la información.

5. Control de accesos

5.1. Requisitos de negocio para controlar los accesos

5.1.1. Política de control de accesos

Los accesos están definidos por el área de TI por cada rol que cumpla el personal dentro de la empresa, en donde están definidas reglas de control de acceso, como son los derechos y restricciones para acceder a la información.

En la empresa se mantiene un documento establecido y verificando su cumplimiento periódicamente de las políticas de control de acceso, en la elaboración de las normas se asigna la menor cantidad de privilegios posibles para llevar una tarea dentro de un sistema de información así también se toma en cuenta el tiempo que requiera sea controlado, todo esto referido a nivel lógico, y de igual manera con los mismos principios a nivel físico.

5.1.2. Acceso a las redes y a los servicios de red

Para la empresa es de real importancia tener en cuenta la gestión para autorizar a los usuarios acceder a los recursos de la red corporativa, y consecuente elaborar políticas que controlen estas actividades. Plasticaucho Industrial por medio del área de TI mantiene un control para administrar la gestión de acceso de usuarios de red, determinando a qué información se puede ingresar, protección de la red, requisitos de autenticación, medios por los cuales se accede (VPN, Wifi) y supervisión del uso.

5.2. Gestión de acceso de usuario

5.2.1. Registro y baja de usuario

El departamento de TI mantiene un control administrado para el registro y baja de usuarios en el Directorio Activo (Active Directory), para lo cual se realizan las siguientes actividades:

- Se mantiene un registro de cuentas de usuario que identifica al personal.
- Las cuentas de usuario se deshabilitan de manera inmediata cuando el personal abandona la organización.
- Comunicación eficiente entre el personal de Administración de Seguridad de la información y el área de Gestión Humana.
- Existe una revisión periódica para identificar y deshabilitar usuarios redundantes.
- Se eliminan las cuentas de usuario después de confirmar que ya no son necesarias.

5.2.2. Provisión de acceso de usuario

En la empresa se manejan los accesos a sistemas y servicios de información de acuerdo al Perfil Tecnológico del Cargo aprobado por el Departamento de Gestión Humana, además conforme al rol que vaya cumpliendo en la organización, se garantiza que se asignen permisos conforme a las políticas de control de acceso y a sus funciones.

5.2.3. Gestión de privilegios de acceso

En el departamento de TI se controla los derechos de acceso privilegiados de manera independiente y de acuerdo al siguiente proceso:

- Se encuentran definidas políticas de acceso sea físico o lógico.
- Se identifica accesos privilegiados de cada sistema o proceso.
- Se establece una norma de caducidad de los permisos privilegiados.
- Se actualizan periódicamente de acuerdo a las competencias de los usuarios.
- Se establecen mecanismos para mantener la confidencialidad de los datos con el cambio de contraseñas periódicas, y controlando los accesos de usuarios genéricos.

5.2.4. Gestión de información confidencial de autenticación de usuarios

Para asegurar la autenticación de los usuarios dentro de la organización se mantienen controles que mantengan la confidencialidad de la información por lo cual se implementa.

- Cláusulas en contratos y condiciones de puesto de trabajo sobre el mantenimiento secreto de las contraseñas o información de autenticación.
- Obligación de cambios de contraseñas mensualmente o después de la entrega de una clave temporal para su primer uso.
- Controles técnicos para controlar el uso de contraseñas seguras, no compartidas.
- Uso de medios seguros para la comunicación.

5.2.5. Revisión de los derechos de acceso de los usuarios

Se encuentran establecidos revisiones periódicas de los permisos de acceso de los usuarios en sistemas y aplicaciones, de acuerdo a las siguientes directrices:

- Revisión de los derechos de acceso a la terminación del contrato del empleo o cambios dentro de la organización.
- Se encuentra establecido derechos de acceso con privilegios especiales solo a usuarios autorizados por jefaturas y acordado el tipo de trabajo que vaya a realizar.
- Las cuentas con privilegios especiales se revisan periódicamente y se registran los cambios que se realicen.

5.2.6. Retirada o reasignación de los derechos de acceso

Existe un proceso de modificación de derechos de acceso para todos los usuarios, de acuerdo a las siguientes actividades que se realicen:

- Empleados, proveedores y contratistas que finalizan el empleo, contrato o acuerdo.
- Cambios de puestos de trabajo dentro de la organización.
- Las modificaciones incluyen accesos físicos a las instalaciones y acceso lógico a la red corporativa.
- Las cuentas de usuario se bloquean inmediatamente cuando ocurren ceses o despidos de empleados que las usan.

5.3. Responsabilidades del usuario

5.3.1. Uso de información confidencial para la autenticación

No existe un control formalizado para asegurar la confidencialidad de las credenciales de autenticación, por lo cual el departamento de TI ha tratado de asegurar este control con mensajes informativos para todos los usuarios, en donde se indican los siguientes puntos sobre la seguridad de la información confidencial.

- Se informa que las contraseñas no se divulguen.
- Indicaciones de cambio de las contraseñas e informar cualquier amenaza.
- Cumplir las políticas de calidad de las contraseñas.
- Evitar el almacenamiento de contraseñas.

5.4. Control de acceso a sistemas y aplicaciones

5.4.1. Restricción del acceso a la información

Las aplicaciones/sistemas que la empresa dispone y que se encuentran aprobados por el departamento de TI para el manejo de la información, éstas cumplen los siguientes controles de acceso:

- Las aplicaciones cuentan con menús para controlar el acceso a las distintas funciones.
- Funciones de administración ocultadas para usuarios habituales.
- Se determinan que datos son accesibles y cuales deben estar disponibles para cada cuenta de usuario.
- La información se encuentra restringida de forma selectiva (lectura, escritura).
- Se considera accesos físicos o lógicos adicionales para sistemas o información altamente clasificada.

5.4.2. Procedimientos seguros de inicio de sesión

El control de inicio de sesión seguro corrobora la identidad del usuario, y se establecen los siguientes procedimientos que verifican el cumplimiento de este control.

- Los sistemas manejan advertencias, evitando proporcionar mensajes de ayuda a usuarios no deseados.

- Los formularios de acceso solo se validan cuando se han completado, evitando mostrar mensajes de error con información.
- Los sistemas registran los intentos fallidos.
- Las sesiones inactivas son dependientes del tiempo, son cerradas después de un cierto tiempo adaptado a la política de la empresa.
- Se limita el acceso de las aplicaciones solo dentro de la red corporativa, para el trabajo fuera de la organización se los realiza mediante conexiones remotas como VPN la misma que debe ser autorizada con anterioridad y realizada únicamente por el departamento de TI.

5.4.3. Sistema de gestión de contraseñas

Los sistemas utilizados dentro de la empresa están establecidos de acuerdo a las políticas de creación de contraseñas seguras y se verifica que cumplan los siguientes lineamientos:

- Longitud mínima de 8 caracteres de la contraseña.
- Evitar la utilización de nombres usuarios como contraseña.
- Reglas de complejidad (mayúsculas, minúsculas, números, símbolos).
- Requiere el cambio obligatorio, después de su asignación.
- Cambio de contraseñas cada 30 días, se rechazan las últimas 5 utilizas anteriormente.

5.4.4. Uso de utilidades con privilegios del sistema

El departamento de TI se encuentra segregado por tareas, en el cual existe una persona encargada de controlar los servicios privilegiados en los sistemas, los cuales son concedidos bajo condiciones y fines únicamente laborales según su rol y sus responsabilidades, autorizados por su jefatura o gerencia.

5.4.5. Control en el acceso al código fuente en programas

El código fuente de los programas se encuentran protegidos con acceso restringido mediante el uso de librerías fuente o repositorios. Se mantiene una administración del entorno, acceso adecuado, control de versiones y personal autorizado por el departamento de TI, que es el área de Desarrollo de Software para realizar las funciones de modificación, compilación, publicación del código fuente.

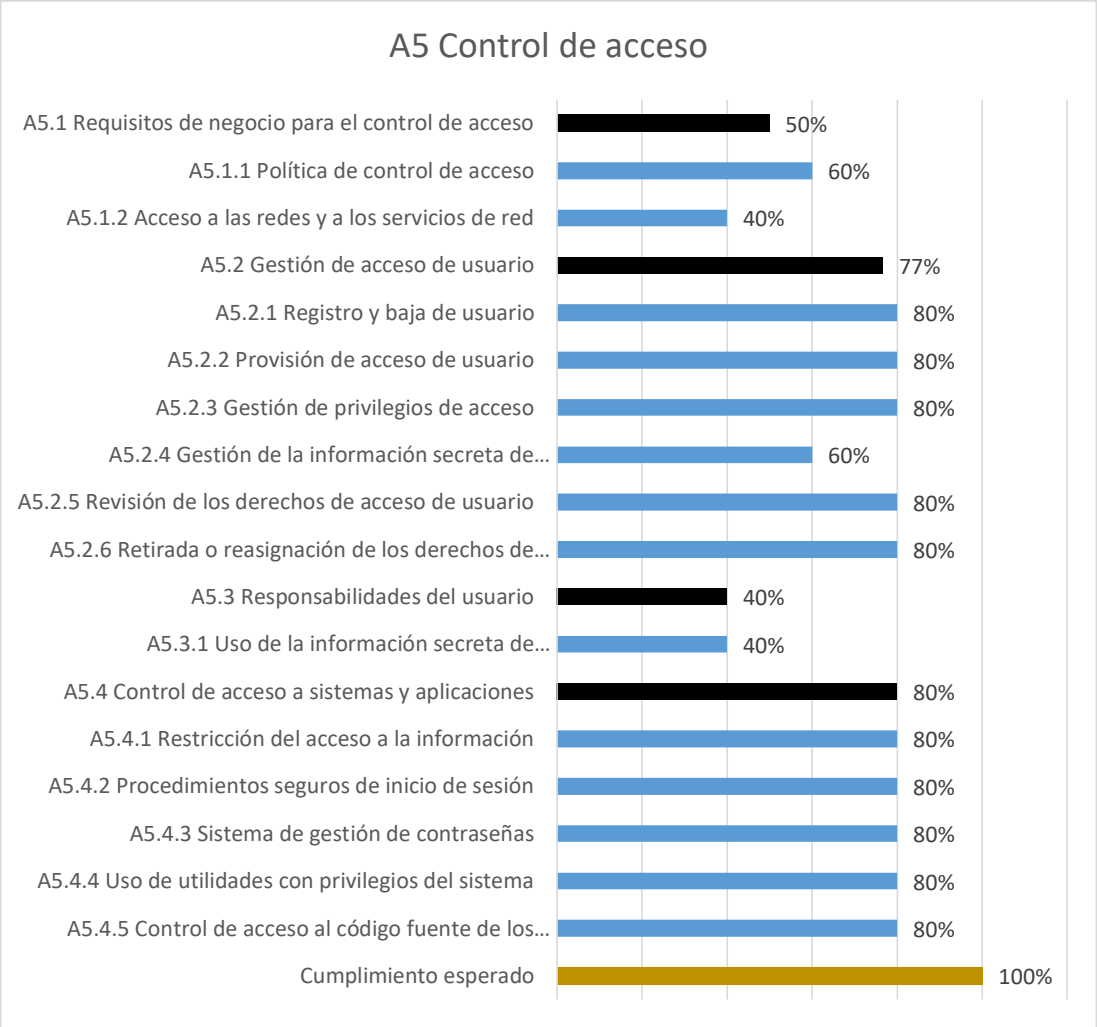

Fig. 35: Cumplimiento - Control de acceso
Fuente: Elaboración propia

En la figura 35 se puede apreciar que la mayoría de los controles cumplen con su aplicabilidad óptima pero en los cuales que hay que mejorar son en los controles de acceso a las redes y uso de información confidencial para la autenticación que parten de revisiones iniciales del departamento de TI.

6. Criptografía

6.1 Controles criptográficos

6.1.1 Política de uso de los controles criptográficos

En la empresa no se encuentra establecido políticas para el uso de controles criptográficos.

6.1.2 Gestión de claves

La gestión de claves al no contar con políticas de controles criptográficos no se puede establecer un método de gestión de claves, pero al igual que el control de gestión de contraseñas se establece mantener los mismos lineamientos para crear claves seguras pero es necesario la gestión de claves, para tener en cuenta el ciclo de vida completo (generación, uso y protección, distribución, renovación o destrucción), además para determinar fechas de activación y desactivación de claves.

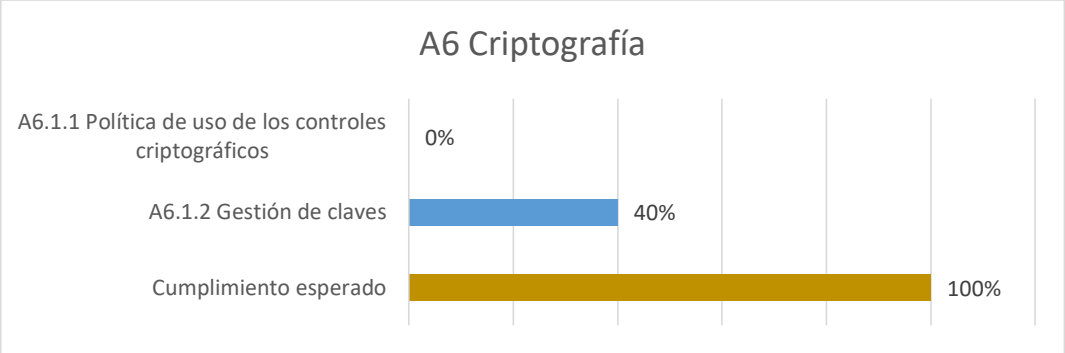

Fig. 36: Cumplimiento - Criptografía
Fuente: Elaboración propia

En la figura 36 se puede apreciar que el control de criptografía no es aplicado en la empresa, y la gestión de claves tiene los mismos lineamientos que la gestión de contraseñas, pero no está implementado totalmente en conjunto con políticas de controles criptográficos.

7. Seguridad física y ambiental

7.1. Áreas seguras

7.1.1. Perímetro de seguridad física

Las instalaciones se encuentran aseguradas físicamente y el responsable directo es el área de Seguridad Física de la empresa, además están definidos los perímetros de seguridad bajo niveles de protección de las instalaciones dependiendo la criticidad de la información a proteger. El control se lo realiza de la siguiente manera:

- Se limita el acceso para las personas a las instalaciones de la empresa.
- Se dispone de tarjeta de identificación y control biométrico para cada empleado.

- Monitoreo en tiempo real, bajo el control de cámaras en cada área de acceso, y activos de información de la empresa.
- Se establece áreas restringidas, para acceso solo de personal autorizado.

7.1.2. Controles físicos de entrada

El área de seguridad física, tiene a su cargo mantener y verificar que las personas que ingresan a las instalaciones sean identificadas y cumplan el proceso de acceso seguro, de acuerdo a los siguientes controles:

- Control de videovigilancia en tiempo real.
- Visitantes deben identificarse, registrar su fecha y hora de entrada/salida.
- Comunicación a empleados y visitantes sobre los procedimientos de seguridad y emergencia.
- Personal externo a la empresa, debe tener autorización y acompañamiento por el personal propio de la organización.
- Entrada a áreas definidas de la empresa según sus roles y responsabilidades.

7.1.3. Seguridad de oficinas, despachos y recursos

Las instalaciones están diseñadas para evitar posibles riesgos que la información confidencial sea accesible para los visitantes, para lo cual se encuentran implementados accesos bajo controles biométricos. Se tiene en cuenta la seguridad de los activos de información almacenados, procesados o utilizados en cada área de la empresa.

7.1.4. Protección contra las amenazas externas y ambientales

En la empresa existe un control establecido para recuperación ante amenazas externas y ambientales, en las que están considerados los activos de mayor importancia. Las leyes vigentes para las empresas, comprometen a tener planes de protección y emergencias, lo cual se aplica dentro de la organización.

7.1.5. El trabajo en áreas seguras

Adicional a las medidas de protección física, en áreas seguras está definido los siguientes procedimientos de trabajo:

- Está prohibido realizar trabajos sin supervisión por parte de terceros.
- Se revisa las zonas a la finalización de las visitas.

- Está prohibido el uso de móviles/cámaras o cualquier equipo de grabación, a no ser que estén expresamente autorizados.

7.1.6. Áreas de acceso público, carga y descarga

El área de carga, al ser uno de los puntos sensibles para la seguridad física se han implementado los siguientes controles:

- Se establece horarios de apertura y cierre.
- Control de apertura y cierre de puertas externas e internas.
- Control de personal que ingresa a las instalaciones.
- Inventario de los materiales entregados.
- Revisión de mercadería entregada, detectar materiales peligrosos.
- Verificar entregas entrantes y salientes.
- Información de cualquier incidente a los responsables de seguridad.

7.2.Seguridad de los equipos

7.2.1. Emplazamiento y protección de equipos

Los equipos dentro de la empresa se encuentran establecidos los siguientes controles para proteger de daños ambientales y accesos no autorizados.

- Se evita accesos no necesarios.
- Equipos protegidos de áreas sensibles como los centros de datos o salas de servidores.
- Protección para equipos que contienen información sensible.
- Medidas de protección contra daños eléctricos.
- Control medioambiental para cumplir con las especificaciones de protección para evitar daños de los equipos.

7.2.2. Instalaciones de suministro

Dentro de la empresa se encuentra establecido medidas de control para el sistema UPS necesario y potencia adecuada para mantener operativas las instalaciones y los equipos. En este control se verifica lo siguiente:

- Cumplimiento de las especificaciones de los fabricantes de los equipos en cuanto a suministros.
- Cumplimientos de requisitos legales de la empresa.

- Procesos de detección de fallos de suministros.
- Capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente.

7.2.3. Seguridad del cableado

Se encuentra establecido controles para la protección de cableado de energía y de comunicaciones que afecte a los sistemas de información, evitando el posible daño de las infraestructuras como posibles interferencias que corrompan los datos o el suministro de energía, el área encargada de esta labor es Servicios Generales que se encargan de verificar lo siguiente:

- Los cables de potencia se encuentran separados de los cables de comunicaciones.
- Los puntos de acceso del cableado a los equipos o a las salas, están asegurados, identificados y protegidos adecuadamente.
- El cableado alrededor de los centros de datos (Data center) se encuentran aislados de forma segura, evitando la conexión de dispositivos no autorizados.

7.2.4. Mantenimiento de los equipos

Los controles establecidos garantizan que los equipos se mantengan adecuados, no se deterioren y siempre estén disponibles; para esta actividad el área TI establece realizarlo anualmente, los responsables se disponen dependiendo de la complejidad y propiedad del equipo, sea de la misma empresa o en su caso del proveedor. En este control se toma en cuentas las siguientes indicaciones:

- Recomendaciones de los fabricantes.
- Solo personal autorizado está encargado del mantenimiento de los equipos críticos y registrados las actividades realizadas.
- La información sensible se respalda o se transfiere del equipo cuando sea necesario.
- Cumplimiento de los requisitos de las pólizas de seguros para los equipos.

7.2.5. Salida de activos fuera de las dependencias de la empresa

Los activos de información sean equipos, software u otros dispositivos; para tener autorización de salida de las instalaciones de la empresa, se establecen las siguientes directrices:

- Firma de acta de salida de equipo.
- Identificación y autorización de personal para retirar equipos o activos fuera de la organización.
- Fijación de límites de tiempo.
- Registro de los equipos que son retirados y registro de su retorno.

7.2.6. Seguridad de los equipos y activos fuera de las instalaciones

En la empresa no se encuentra establecido políticas de uso aceptable de los activos, dispositivos móviles o portátiles fuera de las instalaciones.

Es necesario para este control realizar un registro de los activos y activos que abandonan la organización, responsable y mediante evaluaciones de riesgo de instalaciones y uso, establecer políticas que regulen y controlen el uso adecuado.

7.2.7. Reutilización o eliminación segura de equipos

Los equipos que van a ser reutilizados o eliminados, se encuentran establecidos las siguientes normas que controlan que la información no sea revelada.

- La información que el equipo contiene, es eliminado o transferido según la importancia antes de su reutilización.
- Se garantiza que la información sea eliminada completamente del equipo.
- Evaluación de riesgos antes de proceder a una reparación de los equipos que se encuentren averiados.
- Registro de los equipos reutilizados o eliminados.

7.2.8. Equipo informático de usuario desatendido

Están establecidas reglas que permiten controlar la suspensión/finalización de sesión en los equipos informáticos, para evitar la pérdida o corrupción de datos se establece las siguientes directrices:

- Tiempo definido de inactividad (10 min), para que el equipo se establezca en estado de bloqueo o suspensión.

- Bloqueos de pantalla protegidos con contraseñas.
- Reglas establecidas para todos los equipos de trabajo como servidores, portátiles y otros dispositivos TIC.

7.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla

En este control, una de las políticas de seguridad más fácilmente reconocidas dentro de la empresa y las que más se incumple en la práctica; se establece las siguientes normas aplicado a todas las personas de la organización:

- Las pantallas no deben mostrar información cuando el equipo no se encuentre en uso.
- Clasificación de los documentos físicos y lógicos.
- Restricción clasificada a personal interno y externo para el uso de tecnologías que permitan realizar copias de información como: impresoras, fotocopiadoras, escáner y cámaras (especialmente en teléfonos).
- Equipos de impresión configurados para acceso a copias mediante un ID.

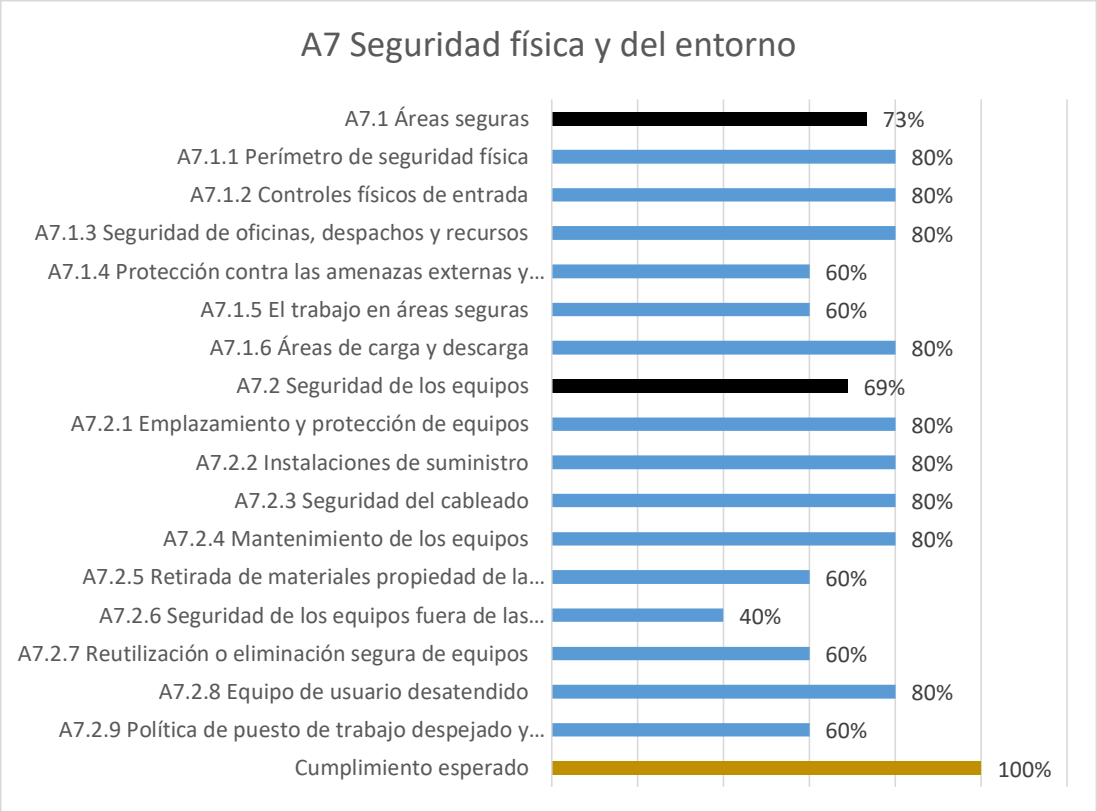

Fig. 37: Cumplimiento - Seguridad física y del entorno
Fuente: Elaboración propia

En la figura anterior se puede observar que la mayoría de los controles referentes a la seguridad física y del entorno cumplen con una aplicabilidad aceptable, pero si se requiere poner más énfasis en el control de Seguridad de los equipos fuera de las instalaciones.

8. Seguridad de las operaciones

8.1.Procedimientos y responsabilidades operacionales

8.1.1. Documentación de procedimientos de operación

Los procedimientos de operación se encuentran documentados y disponibles para los empleados de la organización. La documentación abarca las siguientes actividades, se toman en cuentas aquellas que afectan el procesamiento de la información y aquellas que la protejan.

- Procesos de verificación, instalación, configuración y administración de sistemas/aplicaciones.
- Procesamiento y manejo de información.
- Procesos de gestión de respaldo de información, pruebas y verificación de copias de seguridad.
- Procesos de gestión de registros y elementos de seguimiento de auditoria.
- Procedimientos de monitoreo de red y activos de información.

8.1.2. Gestión de cambios

No se encuentra establecido políticas de gestión de cambios, el proceso se lo realiza informalmente con medidas de precaución y verificando el control de cambios en instalaciones o infraestructuras (equipos y software), evitando que los riesgos se asocien a la seguridad de la información.

8.1.3. Gestión de capacidades

Control establecido en la empresa para evitar pérdidas de disponibilidad o rendimiento de los sistemas por falta de capacidad, permitiendo tener el control del uso de los recursos tecnológicos. Para el cumplimiento de este control se verifica lo siguiente:

- Acuerdos de nivel de servicio (SLA), entre el proveedor y el cliente.
- Medición y seguimiento de uso de recursos.

- Planificación para ampliaciones de capacidad de los recursos cuando sea necesario.
- Optimizar el uso de recursos.

8.1.4. Separación de entornos de desarrollo, prueba y producción

Los entornos de desarrollo se encuentran separados de los entornos de producción o prueba, para evitar problemas de indisponibilidad o fallos en el servicio. Para lo cual se definió lo siguiente:

- Entorno de desarrollo, código fuente y herramientas de trabajo separados del entorno de producción.
- Datos utilizados en entornos de desarrollo no son copia de los datos de producción a menos que se hay previsto controles de seguridad (acuerdos de confidencialidad).
- Controles en etapa de desarrollo para evitar introducir código malicioso.
- Planificación especial antes de una migración de código al entorno de producción.

8.2.Protección contra código malicioso (malware)

8.2.1. Controles contra el código malicioso

Los equipos tecnológicos de propiedad de la empresa Plasticaucho, se encuentran controlados para la detección de código malicioso, mediante la asignación de las siguientes actividades:

- Definir responsable específico para la tarea de detección de malware.
- Procedimientos para realizar las tareas de mantenimiento y actuar en las situaciones de emergencia.
- Actualizaciones periódicas de software antivirus en cada uno de los equipos.
- Aislamiento de equipos en caso de detección y recuperación de cualquier ataque.
- Monitoreo de software utilizado y los datos de red.
- Equipos protegidos con software antivirus.
- Software en caso de ser nuevo se verifica con el listado de software autorizado y no autorizado. Todo archivo adjunto en correo o descargado

de alguna fuente desconocida, es analizado antes de su uso, mediante la página web https://www.virustotal.com.

8.3.Copias de seguridad

8.3.1. Copias de seguridad de la información

El respaldo de la información es primordial en la empresa, por lo cual se ha definido políticas de copias de seguridad o respaldo de la información teniendo en cuenta la periodicidad para realizarlas y tomando en cuentas las siguientes indicaciones:

- Copias de seguridad de datos e información sensible.
- Verificación de la validez de las copias de seguridad.
- Ubicación segura de los respaldos, evitando posibles intentos de acceso no autorizado o desastres naturales.
- Medios de recuperación en perfecto estado de funcionamiento y disponibles cuando se los requiera.
- Como parte de un cronograma mantienen registros de las copias de seguridad.

8.4.Registro de actividad y supervisión

8.4.1. Registro y gestión de eventos de actividad

Los registros de eventos que ocurran en los sistemas de información son necesarios para determinar el problema a la hora de un incidente, en la empresa se los administra de mediante las herramientas que los mismos sistemas disponen para la revisión del historial de log o registros.

8.4.2. Protección de los registros de información

Los registros de información están protegidos en cada sistema, en el cual sólo el usuario con perfil de administrador puede verificar los eventos que ocurran. Para la protección de los registros se aplica las siguientes normas:

- Accesos restringidos para los registros de eventos.
- Protección de los registros para evitar pérdidas, corrupción o cambios no autorizados.

- Administrador del sistema no tiene el permiso de borrar o desactivar el registro de sus propias actividades.

8.4.3. Registros de administración y operación

Existen responsables identificados para la administración de los accesos privilegiados para el análisis de los eventos en los sistemas de información. El registro de las actividades se lo realiza no solo a los usuarios normales sino también a los usuarios administradores.

8.4.4. Sincronización de relojes

La sincronización de los sistemas es imprescindible para la empresa, es así que la hora establecida en los sistemas corresponde al tiempo de referencia definido como es el NTP.

8.5.Control del software en explotación

8.5.1. Instalación del software en sistemas en producción

Están establecidas políticas que cubren los procedimientos para las instalaciones de software en cualquier dispositivo dentro de la empresa. Se verifica lo siguiente:

- Software se encuentre autorizado por el departamento de TI para su instalación.
- Pruebas de funcionamiento de nuevas aplicaciones o software.
- Comprobación de las necesidades de instalación (compatibilidad del entorno).
- Valoración de la necesidad de actualización o instalación.
- Las instalaciones de software son realizadas por usuarios autorizados.
- Procedimientos de monitoreo del software para detectar cambios no autorizados.

8.6.Gestión de la vulnerabilidad técnica

8.6.1. Gestión de las vulnerabilidades técnicas

En los sistemas que la empresa dispone se analizan las vulnerabilidades técnicas de los activos de información, en la que se establecen los siguientes controles adecuados para su seguridad:

- Escaneos periódicos de vulnerabilidades técnicas.

- Evaluación del uso de software que solo sea necesario para las actividades de la empresa.
- Aplicaciones que cumplan las reglas y objetivos de seguridad de la información.

8.6.2. Restricciones en la instalación de software

Administrado en controles anteriores para la empresa, se insiste en establecer restricciones para la instalación de software por parte de los usuarios. El personal del departamento de TI es el único responsable para realizar y verificar el cumplimiento de estas actividades.

- Instalación de software es limitado solo para personal capacitado y autorizado con privilegios de administrador.
- Análisis de la instalación de software que son permitidas y las prohibidas para los usuarios finales.

8.7.Consideraciones de las auditorías de los sistemas de información

8.7.1. Controles de auditoría de los sistemas de información

Dentro de la empresa se mantiene una auditoria de los sistemas de información para evaluar el cumplimiento y la seguridad de la información. De acuerdo a la planificación anual del departamento de Tecnología de la Información se designa al personal con el cargo de Analista de Seguridades TI y el Coordinador Infraestructura para la ejecución de las siguientes actividades:

- Verificación de los usuarios que trabajen con privilegios correctos.
- Asegurar que la infraestructura tecnológica se encuentre estable y confiable.
- Verificar que los recursos de la infraestructura tecnológica cuente con la capacidad suficiente para operar.
- Efectividad de las actividades de mantenimiento y monitoreo.
- Analizar las mejoras que se puedan aplicar.

Al finalizar los controles de auditoria de los sistemas de información, se entrega un informe técnico donde se detalla los resultados obtenidos, para posterior diseñar un Plan de Mejora de los sistemas de Información.

Fig. 38: Cumplimiento - Seguridad de las operaciones
Fuente: Elaboración propia

En la figura 37 se puede apreciar que los controles referentes a la seguridad de las operaciones cumplen su aplicabilidad de manera óptima, pero si es necesario mejorar su control en la gestión de cambios, registro de eventos y la protección de la información de los registros.

9. Seguridad de las comunicaciones

9.1. Gestión de la seguridad en las redes

9.1.1. Controles de red

En la red corporativa de Plasticaucho están establecidos las siguientes políticas para su control, tanto en redes físicas como inalámbricas:

- Se establece personal independiente para la administración de la infraestructura de red.
- Monitorización de la red y los dispositivos conectados en ella.

- Sistema de autenticación para todos los accesos a la red de la empresa.
- Autenticación de usuarios en el inicio de sesión.
- Limitación de accesos de personas a aplicaciones o servicios.
- Segmentación de red adecuada con el uso de Firewall y distribuida en VLAN.
- Control de puertos y servicios utilizados para funciones de sistemas de información.

9.1.2. Seguridad de los servicios de red

La empresa dispone de servicios de red WAN administrados externamente por un proveedor e internamente la red LAN por el personal del departamento de TI, para lo cual se han establecido los requisitos siguientes.

- Definición de acuerdos de Niveles de Servicio o SLA.
- Auditorias de calidad de servicios prestados.
- Evaluación de riesgos que están expuestos con el uso de los servicios contratados.
- Monitorización de los servicios de red.
- Revisiones periódicas de configuraciones de cortafuegos.

9.1.3. Segregación de redes

La red corporativa de Plasticaucho Industrial está distribuida por VLAN dentro de la red física cableada, para lo cual se estableció lo siguiente:

- Segmentación de red lógica y física para cada proceso de la empresa.
- Identificación de equipos tecnológicos.
- Monitoreo y control de la distribución de la red.
- Segmentación de la red inalámbrica, física y red invitados.
- Seguridad evaluada periódicamente para identificar riesgos.

9.2.Intercambio de información con partes externas

9.2.1. Políticas y procedimientos de intercambio de información

No existe un procedimiento de evaluación para verificar el cumplimiento de este control, pero se lo realiza bajo la verificación de los siguientes aspectos:

- Verificación de uso de solo medios de transmisión autorizados por el departamento de TI o gerencia respectivamente.
- Integración a la red corporativa de dispositivos bajo permisos restringidos y a usuarios autorizados.
- Verificación de soportes informáticos se encuentren libres de cualquier amenaza.

9.2.2. Acuerdos de intercambio

Para la empresa no se cuenta con un Acuerdo de intercambio de información, se lo administra con procedimientos propios y la responsabilidad es individual. Se establece lo siguiente para los usuarios:

- Responsabilidades individuales para el uso, protección e intercambio de información.
- Controles de acceso a la información.

9.2.3. Mensajería electrónica

La mensajería electrónica dentro de la empresa se lo administra mediante las siguientes políticas para el control de envío y recepción de correos.

- Administración de dominios en listas blancas y negras.
- Control de mensajería anti spam.
- Prohibición de envío o recepción de archivos ejecutables.
- Aseguramiento de direccionamiento y transporte de los mensajes.
- Autorización para uso de otro tipo de mensajería instantánea o redes sociales.

9.2.4. Acuerdos de confidencialidad o no revelación

Al no tener establecidos acuerdos de intercambio de información, no se puede establecer acuerdos de confidencialidad o no revelación pero este control es administrado bajo las siguientes reglas previamente elaboradas en un contrato de servicios.

- Se establece contratos con partes externas en medida que no influyan mucho con la manipulación de la información.

- Contratos aprobados y firmados por las personas responsables de cada organización.
- Informar los cumplimientos y sanciones a las personas involucradas.
- Establecer sanciones por incumplimientos.

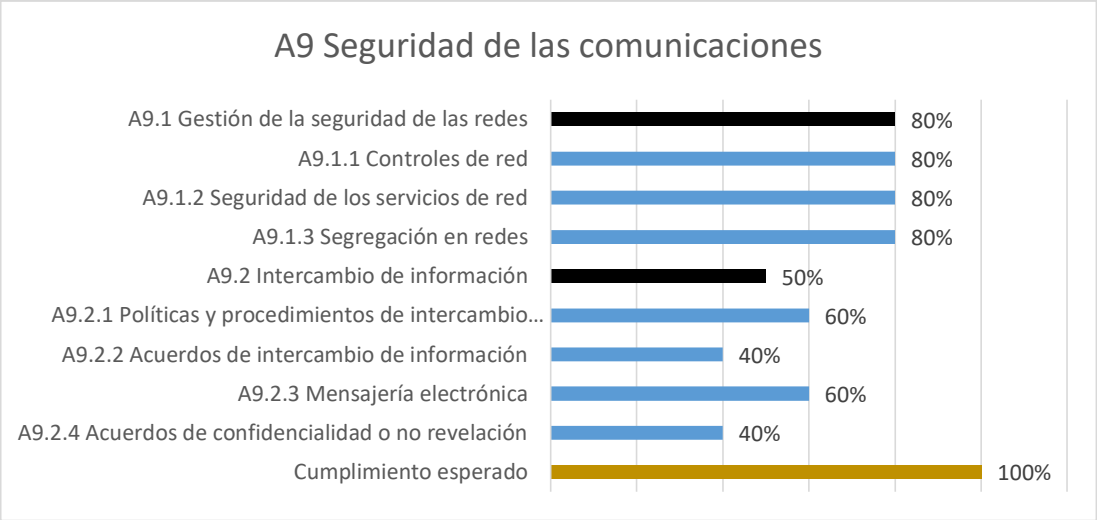

Fig. 39: Cumplimiento - Seguridad de las comunicaciones
Fuente: Elaboración propia

En la figura 38 se puede apreciar que los porcentajes de cumplimiento de los controles referentes a los controles, seguridad de los servicios y segregación de las redes son en los que más énfasis en su aplicación.

Los controles que requieren mejorar su índice de aplicabilidad son los acuerdos de intercambio de información y acuerdos de confidencialidad.

10. Adquisición, desarrollo y mantenimiento de los sistemas de información

10.1. Requisitos de seguridad en los sistemas de información

10.1.1. Análisis y especificación de los requisitos de seguridad

Se encuentra establecido requisitos para la seguridad de la información en la fase de especificación de características para sistemas de información, esto se analiza en las funcionalidades requeridas. Para este control se lo realiza de acuerdo a los siguientes lineamientos:

- Especificación de funcionalidades antes de adquirir o desarrollar un software.
- Requisitos de seguridad ante posibles fallos de seguridad.

- Verificación de requisitos de autenticación.
- Especificar la provisión de accesos para los usuarios.
- Usuarios privilegiados y responsables de mantenimiento.

10.2. Seguridad en los procesos de desarrollo y soporte

10.2.1. Política de desarrollo seguro de software

Se encuentran establecidas las siguientes reglas para mantener la información íntegra y segura, durante todas las etapas de desarrollo de software:

- Desarrollo de software separado en entornos de desarrollo, pruebas y producción.
- Repositorios seguros con control de acceso y control de cambios para el entorno de desarrollo.
- Registro de cambios y gestión de versiones aplicadas.

10.2.2. Procedimientos de control de cambios en los sistemas

No existe establecido procedimientos formales para gestionar los cambios en los sistemas, se lo realiza en base a los riesgos de información y aspectos de seguridad en el desarrollo de software. Se realiza las siguientes actividades:

- Planificación y pruebas de cambios.
- Realización de pruebas y control de funcionamiento de los cambios introducidos.
- Control de versiones.

10.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Las revisiones técnicas en sistemas que se hayan aplicado cambios son revisados y probados, garantizando su operatividad. Se cumple los siguientes lineamientos:

- Establecimiento de tiempos de prueba.
- Revisión de los cambios aplicados, que cumplan las funciones solicitadas.
- Seguimiento y registro de actividades durante/después de la aplicación de cambios.

10.2.4. Restricciones de cambios en paquetes de software

Limitar los cambios en los paquetes de software es aplicado como medida para delimitar o minimizar la posibilidad de generar incidentes. El departamento de TI establece los siguientes controles para realizar los cambios absolutamente necesarios sobre el software:

- Verificar que controles originales del software no sea comprometidos.
- Autorización y cumplimiento de precauciones indicadas por proveedores.
- Soporte de actualizaciones por parte del proveedor.
- Comprobación de compatibilidades de software.

10.2.5. Principios de ingeniería de sistemas seguros

Los principios de ingeniería para la protección de los sistemas son importantes para la seguridad de la información dentro del ciclo de vida de desarrollo, se sigue algunos procedimientos pero no cumple con totalidad este control en la empresa:

- Procesos de diseño para mecanismos de autenticación.
- Procedimientos por etapas para el diseño y codificación del sistema.

10.2.6. Seguridad en entornos de desarrollo

Para la seguridad de la información y el desarrollo de software se aplican los siguientes controles de seguridad en los entornos de desarrollo:

- Evaluar el grado de sensibilidad de los datos.
- Aplicar niveles de seguridad.
- Controles desarrollados para la seguridad de cada tipo de información.
- Confiabilidad del personal de desarrollo.
- Separación de entornos de desarrollo.
- Respaldo de información.

10.2.7. Externalización del desarrollo de software

Al igual que el control de seguridad en entornos de desarrollo se aplican las siguientes normas a desarrolladores externos, además de incluir otras condiciones en los contratos para la seguridad de la información.

- Acuerdos de cumplimiento y supervisión de los requisitos de seguridad.
- Control y gestión de aspectos relacionados de licencias y propiedades de código fuente.

- Desarrollo de prácticas seguras en el diseño, desarrollo y prueba.

10.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas

Se encuentran establecidos procedimientos de pruebas y verificación para sistemas nuevos o actualizados, teniendo en cuenta el cumplimiento de la seguridad y condiciones acordadas.

10.2.9. Pruebas de aceptación de sistemas

Para la aceptación de un software se lo verifica bajo los siguientes controles establecidos para la seguridad de la información:

- Análisis de la seguridad de los sistemas antes de ser introducidos en la red.
- Pruebas de aceptación por parte del usuario.
- Entornos de prueba separados a los de operación.

10.3. Datos de Prueba

10.3.1. Protección de los datos utilizados en pruebas

Para la protección de los datos se tiene precaución en el uso y se sigue los siguientes lineamientos:

- Etapas de desarrollo se utilizan datos no reales.
- Controles de seguridad en datos confidenciales.
- Establecer personal capacitado y confiable para la etapa de pruebas.

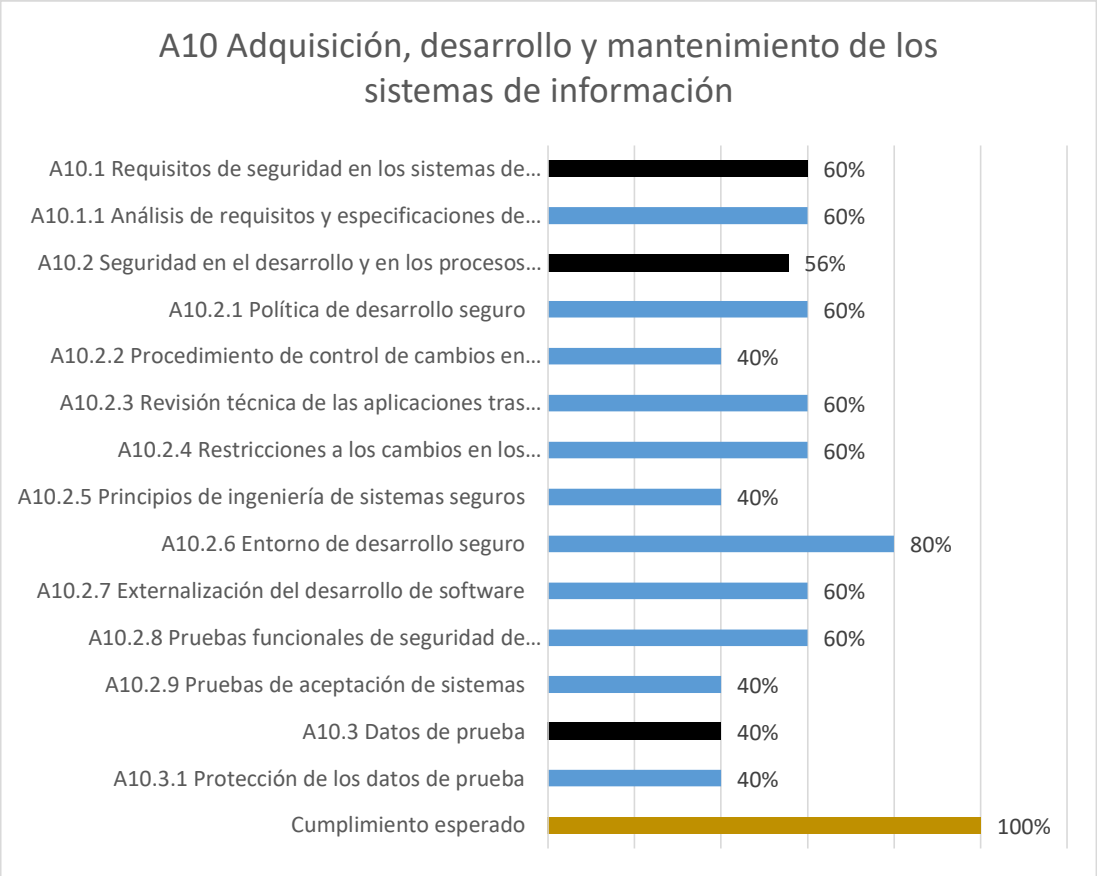

Fig. 40: Cumplimiento - Adquisición, desarrollo y mantenimiento de los sistemas de información
Fuente: Elaboración propia

En la figura anterior se puede apreciar que los controles referentes a la Adquisición, desarrollo y mantenimiento de los sistemas de información cumplen su aplicabilidad de manera aceptable, pero si es necesario mejorar en los controles de procedimientos de control de cambios en los sistemas, principios de ingeniería de sistemas seguros, pruebas de aceptación de sistemas y en la protección de los datos de prueba.

11. Relación con proveedores

11.1. Seguridad en las relaciones con proveedores

11.1.1. Política de seguridad de la información en relaciones con los proveedores

El control se aplica conforme a todo lo relacionado con la gestión de proveedores y condiciones de seguridad, se establece y se da a conocer a las partes involucradas en los contratos las siguientes directrices:

- Establecimiento de acceso a la información únicamente que sea necesaria.
- Controles físicos y lógicos para la seguridad de los activos.
- Aplicación entre las partes involucradas Acuerdos de Niveles de Servicio.
- Monitoreo de acceso a la información.
- En la finalización del servicio se controla la devolución de activos, eliminación o destrucción de datos y revocación de accesos.

11.1.2. Requisitos de seguridad en contratos con terceros

Los requisitos de seguridad de la información se encuentran reflejados en los contratos de manera explícita, los mismos que están firmados por ambas partes y verificar el cumplimiento de lo siguiente:

- Responsable de seguridad para verificar que se cumplan los controles pactados entre las partes.
- Control de personal, ante cualquier cambio se establece informar y ser revocado los permisos tanto a las instalaciones como a sistemas de información.
- Cumplimiento de los requisitos legales para la protección de los datos.
- Establecimiento de cláusulas para el uso correcto de los activos evitando el daño o revelación de la información.
- Auditorias de seguridad.

11.1.3. Cadena de suministros de tecnología de información y de comunicaciones

Los requisitos de seguridad de la información no solo se toman en cuenta al proveedor sino que se fija a toda la cadena de suministro antes de llegar a la empresa, estableciendo los siguientes controles que garanticen la fiabilidad del servicio:

- Verificación de los proveedores (recomendaciones, calidad servicio).
- Exigencia a los proveedores un control de seguridad sobre sus propios proveedores.
- Comprobación de los productos o servicios cumplan con los requisitos de la seguridad de la información.

11.2. Gestión de provisión de los servicios del proveedor

11.2.1. Control y revisión de provisiones de servicios del proveedor

La monitorización de los servicios tecnológicos prestados está a cargo del departamento de TI para verificar el cumplimiento.

- Reuniones con el proveedor para la revisión del servicio prestado.
- Informes de riesgos, incidentes, cumplimiento y auditorias.
- Informes/métricas sobre el nivel de servicio prestado.
- Cláusulas de penalización en el contrato por incumplimiento relacionadas con el riesgo de la información y con los activos.

11.2.2. Gestión de cambios en la provisión del servicio del proveedor

Los cambios que se apliquen en el servicio prestado por parte del proveedor son previamente informados entre ambas partes para aplicar los controles de riesgos necesarios y se verifica el cumplimiento de las siguientes actividades:

- Análisis de los riesgos en el nuevo escenario.
- Evaluar la necesidad de modificar o ampliar los acuerdos de nivel de servicio si es el caso para cubrir nuevas necesidades de seguridad.

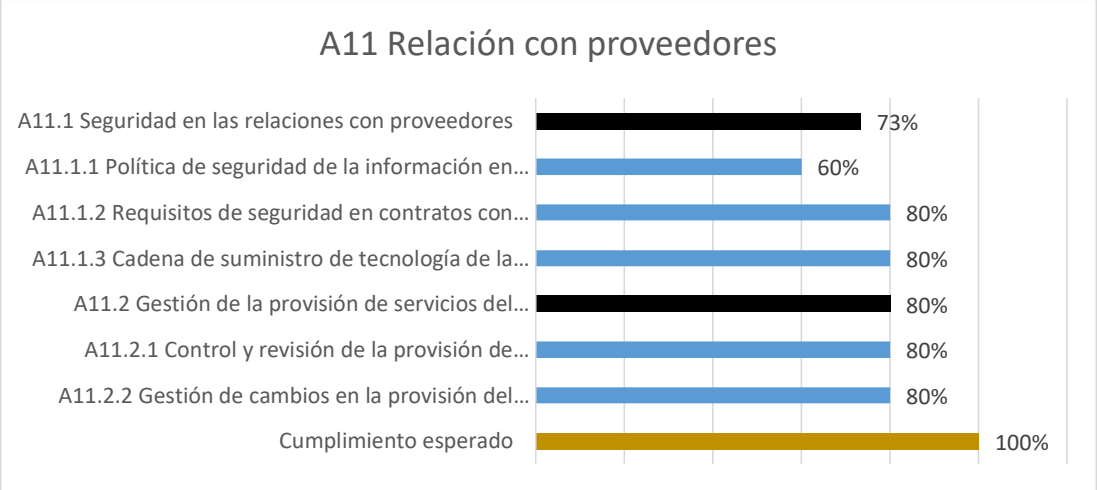

Fig. 41: Cumplimiento - Relación con proveedores
Fuente: Elaboración propia

En la figura 40 referente a la relación con proveedores los controles cumplen con su aplicabilidad de manera óptima, pero obviamente es necesario revisar los lineamientos para que su utilidad sea excelente.

12. Gestión para incidentes en la seguridad de la información

12.1. Gestión de incidentes en seguridad de la información y sus mejoras

12.1.1. Responsabilidades y procedimientos

Para la gestión de incidentes se han establecido procedimientos y responsables del área de TI para aplicar las siguientes medidas de seguridad.

- Responsables designados para la tarea de gestión de incidentes.
- Plan de respuestas ante incidentes.
- Designación de puntos de contacto para notificar incidentes, seguimiento y evaluación.
- Monitoreo para detección de eventos de seguridad.
- Comunicados dirigidas al personal para informar la detección y cómo actuar ante una amenaza.

12.1.2. Notificación de los eventos de seguridad de la información

El personal de TI al tener en cuenta los diversos eventos e incidentes que ocurren a diario, capacita a los empleados para identificar y de manera inmediata informar cualquier amenaza, para lo cual se realiza:

- Capacitaciones y mensajes informativos para el personal en general de la empresa para identificar amenazas.
- Identificación de incidentes y su probabilidad de ocurrencia.
- Seguimiento de los incidentes detectados para buscar su resolución.

12.1.3. Notificación de puntos débiles de la seguridad

Para los empleados no existe una obligación contractual que los comprometa a reportar cualquier tipo de ocurrencia inusual, pero a partir del departamento de TI se envían boletines informativos para todo el personal de la empresa. En donde se explica las amenazas que están expuestos los activos informáticos de la empresa. Para cumplir con este control se informa a los empleados lo siguiente:

- Antes de abrir cualquier mensaje o correo electrónico verificar que sea de remitentes conocidos por el personal de la empresa.
- No compartir claves en páginas web, y entre personas dentro o fuera de la empresa.

- No descargar de páginas/fuentes desconocidas archivos al equipo.

12.1.4. Evaluación y decisión sobre los eventos de seguridad de información

La evaluación de los eventos de seguridad de la información se lo realiza mediante reuniones semanales del departamento de TI, se analiza si se trata de un evento simple o ya paso a ser incidente para posterior tomar decisiones. Se verifica las actividades siguientes:

- Se asigna una escala de clasificación para seleccionar el personal indicado para solventar los eventos ocurridos.
- Se prioriza los incidentes dependiendo del sistema o servicio afectado y del usuario.
- Clasificación de incidentes de acuerdo al impacto y urgencia.
- Registro de los incidentes y actividades realizadas.

12.1.5. Respuesta a los incidentes de seguridad

El control del proceso de resolución de incidentes de la seguridad de la información se lo mantiene registrado como actividades que realiza el personal de TI en la herramienta Helpdesk SysSaid, y se realiza las siguientes actividades:

- Identificación del incidente ocurrido.
- Designar el personal específico del área de TI para solventar el incidente.
- Solución del incidente aplicando métodos seguros.
- Informes de actividades y vulnerabilidades encontradas al jefe inmediato o gerencia.
- Registro de actividades realizadas en la herramienta Helpdesk.

12.1.6. Aprendizaje de los incidentes de seguridad de la información

Los registros que se mantienen dentro del software Helpdesk de cada incidente que haya ocurrido, funcionan como una fuente de información para dar solución a incidentes futuros, para ello se realiza investigación a profundidad con el objetivo de poder evaluar el riesgo al cual haya sido expuesto los activos de información y se realiza las siguientes actividades:

- Se identifica los incidentes más recurrentes y de alto impacto, con sus respectivas actividades.

- Se establece controles y criterios de evaluación de los riesgos que han ocurrido.
- Mediante capacitaciones periódicas a los usuarios por parte del departamento de TI, sobre el correcto uso de los sistemas de información para evitar incidentes.

12.1.7. Recopilación de evidencias

La recopilación de evidencias lo hace el departamento de TI mediante las herramientas propias del software y hardware que se administra en el área, revisando los registros (log) que ocurrieron durante y después de un incidente.

- Registro de inicios y cierres de sesión.
- Estado de los dispositivos y de la red.
- Revisión del software de trabajo.

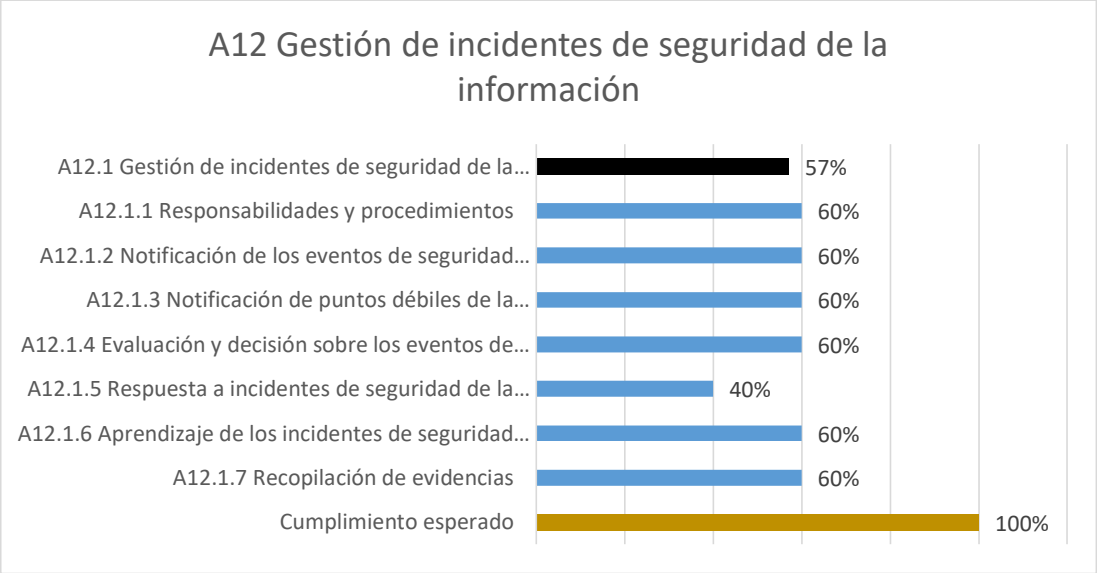

Fig. 42: Cumplimiento - Gestión de incidentes de seguridad de la información
Fuente: Elaboración propia

En la figura anterior referente a la gestión de incidentes de seguridad de la información cumplen con los controles de manera aceptable, pero si es necesario aplicar mejoras en el control de respuesta a incidentes de seguridad de la información.

13. Aspectos para la seguridad de la información y gestión de la continuidad del negocio

13.1. Continuidad de la seguridad de la información

13.1.1. Planificación para la continuidad de la seguridad de información

La planificación para la continuidad de negocio está establecida por la criticidad de los equipos tecnológicos y riesgos que puedan tener durante sus funciones, para lo cual se realiza las siguientes actividades:

- Determinación de activos tecnológicos críticos.
- Análisis de alta disponibilidad para sistemas de TI.
- Identificación de impactos potenciales de los incidentes.
- Planes de contingencia ante una situación de detenimiento de los distintos servicios como energía, comunicaciones, red o infraestructura.

13.1.2. Implantación de la continuidad de la seguridad de la información

Los planes establecidos para la continuidad del negocio están gestionadas de acuerdo al nivel de criticidad del incidente y se aplica los siguientes controles:

- Se definen tiempos para restaurar servicios tras una interrupción.
- Identificación de prioridades de restauración.
- Acuerdo de responsabilidades para aplicar procedimientos de recuperación sea para proveedores externos como internos.
- Designación de las personas adecuadas para realizar las funciones del plan de continuidad de la seguridad de la información y recuperación ante desastres.

13.1.3. Verificación, revisión y evaluación para la continuidad de la seguridad de la información

No se ha establecido procesos para pruebas de plan de continuidad pero se realiza reuniones semanales en el departamento de TI para analizar los incidentes y las acciones que fueron realizadas para solventarla.

13.2. Redundancias

13.2.1. Disponibilidad de instalaciones para el procesamiento de la información

En la empresa se ha garantizado la disponibilidad de las instalaciones de procesamiento de información mediante los siguientes controles que permiten analizar la viabilidad de sistemas redundantes:

- Identificación de los sistemas de información que por su arquitectura no garantizan siempre la disponibilidad.
- Administración de sistemas redundantes que permiten reaccionar en tiempo real a la caída de sistemas o activos de información.
- Pruebas periódicas de funcionamiento de sistemas redundantes.

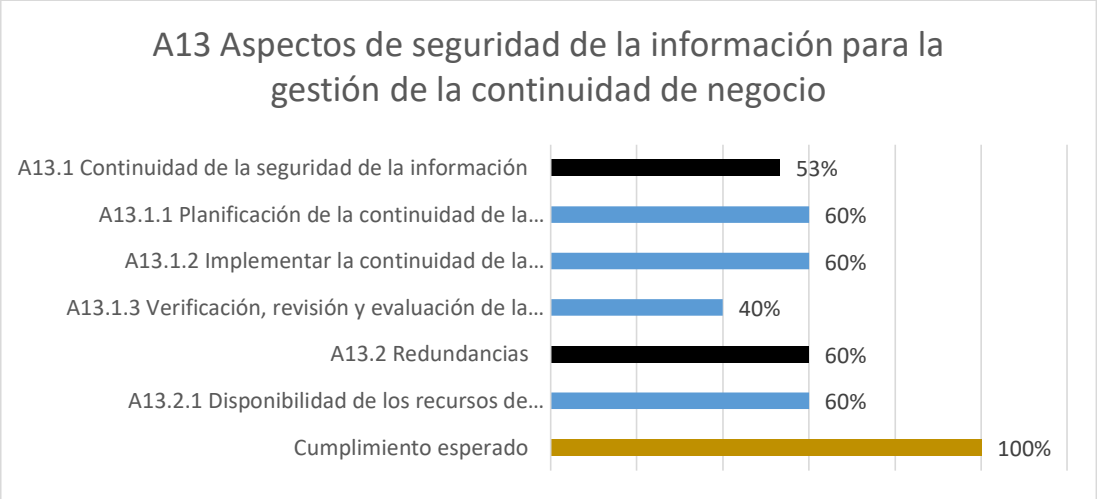

Fig. 43: Cumplimiento - Aspectos de seguridad de la información para la gestión de la continuidad de negocio
Fuente: Elaboración propia

En la figura 42 referente a los aspectos de seguridad de la información para la gestión de la continuidad de negocio cumplen con los controles de manera aceptable, pero si es necesario aplicar mejoras en el control de verificación, revisión y evaluación de la continuidad de la seguridad de la información.

14. Cumplimiento

14.1. Cumplimiento de los requisitos legales y contractuales

14.1.1. Identificación de la legislación aplicable

En nuestro país Ecuador no se ha logrado aplicar leyes de cumplimientos legales para las empresas como es la LOPD (Ley Orgánica de Protección de Datos), es así que en la empresa no tiene un apoyo legal en cual sustentar la seguridad de la información y aplicar penalizaciones cuando amerite el caso; es así que la empresa

Plasticaucho mantiene la seguridad de los datos personales de los empleados como de la organización mediante la estipulación de reglamentos dirigidos al personal interno y externo para mantener un entorno que asegure y aplique correcciones al incumplir un contrato en contra de la seguridad de los datos.

14.1.2. Derechos de propiedad intelectual (DPI)

En la empresa están establecidos acuerdos para procedimientos que garantizan el uso de software de acuerdo a los términos que indican en la Ley de Propiedad Intelectual, para lo cual se controla lo siguiente:

- Políticas de uso legal de productos software.
- Asegurar la no violación de derechos de autor.
- Registro de compra de licencias de Software.
- Control de números máximos de usuarios por licencia.
- Revisión periódica que se estén utilizando solamente productos Software con licencia.
- Comunicación con el personal de la política de uso legal de software, aclarando cuales están permitidas y cuáles no.
- Documentación y registro de justificaciones que acreditan la propiedad de las licencias.

14.1.3. Protección de los registros de la organización

En la empresa se realizan análisis de los requisitos legales y protección de los registros para evitar pérdidas, falsificaciones o acceso no autorizados. Se realizan las siguientes actividades:

- Clasificación y revisión de los registros legales de base de datos, transacciones, auditorias, procedimientos operativos, archivos físicos o lógicos.
- Revisión de los medios de almacenamiento que sean los autorizados.
- Establecimiento de directrices para la retención, almacenamiento, tratamiento y eliminación de los registros de información.

14.1.4. Protección de datos y privacidad de la información personal

El establecimiento de reglamentos para instruir y dar a conocer al personal sobre el manejo de información de carácter personal ha permitido a la empresa elevar la confianza y seguridad sobre estos datos, para lo cual se ha definido los siguientes lineamientos:

- Definir responsables para la administración de la privacidad de la información en la organización.
- Almacenamiento y procesamiento seguro de la información.
- Controles de seguridad para dar acceso a la información personal solo a personas autorizadas.
- Manejo de acceso bajo roles de personal.

14.2. Revisiones de la seguridad de la información

14.2.1. Revisión independiente de seguridad de la información

Las revisiones del cumplimiento de la seguridad de la información en la empresa se la realizan mediante auditorías realizadas por personal interno y externo a la organización, con el siguiente objetivo:

- Garantizar el cumplimiento de las políticas dispuestas para la seguridad de la información.
- Planificar auditorias anualmente para identificar y evitar riesgos.
- Definir objetivos y alcance de las auditorias que previamente están autorizados por la Gerencia General.
- Documentación de los resultados de la auditoria.
- Evaluaciones desde un punto imparcial.
- Aportaciones con experiencias de profesionales de la seguridad de la información.

14.2.2. Cumplimiento de las políticas y normas de seguridad

El cumplimiento de las políticas de seguridad está bajo los responsables de cada área en conjunto con el departamento de TI que son los encargados de supervisar el correcto uso y funcionamiento de los activos de información realizando los siguientes controles:

- Verificación del cumplimiento de los requisitos de seguridad de la información en cada área con su respectivo responsable.

- Analizar los casos de incumplimientos e identificación de las causas.
- Implementación de acciones correctivas apropiadas.
- Identificar e informar debilidades de los sistemas de información.

14.2.3. Comprobación del cumplimiento técnico

Plasticaucho Industrial por medio del departamento de TI implementa controles diarios para verificar el cumplimiento técnico de los sistemas de información, esta actividad está encargada por el analista de seguridades TI, el cual realiza las siguientes actividades.

- Escaneo de vulnerabilidades y pruebas de pestesting regularmente.
- Análisis y registro de los resultados obtenidos.
- Establecimiento de prioridades y tratamientos de riesgos bajo un análisis.
- Medidas correctivas ante fallos registrados que supongan una amenaza real para los sistemas de información.
- Prácticas de Hacking ético de manera anual.

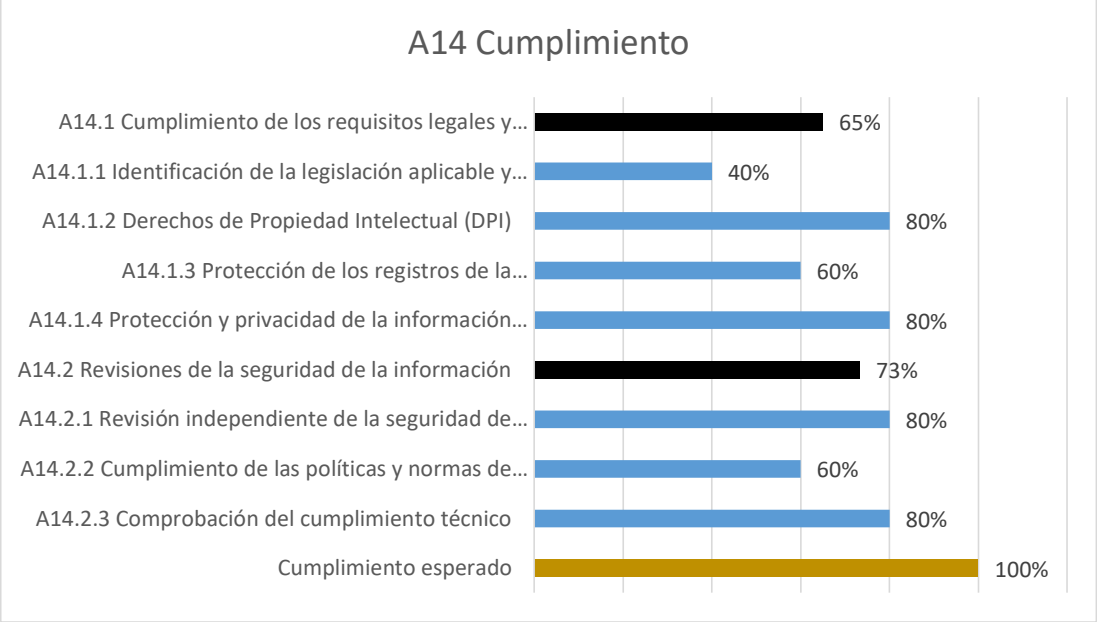

Fig. 44: Cumplimiento
Fuente: Elaboración propia

En la figura anterior referente al Anexo de cumplimiento de los controles es de manera aceptable, pero si es necesario aplicar mejoras en el control de Identificación de la legislación aplicable.

4.6 Presentación del Plan de Gestión de Seguridad Informática

En base al análisis realizado mediante la aplicación de los controles de la norma ISO 27001 y tomando en cuenta los diferentes escenarios que maneja la empresa Plasticaucho Industrial para llevar a cabo las diferentes actividades tanto administrativas como operativas se ha podido determinar que la probabilidad de ocurrencia de incidentes relacionados con la seguridad de la información es alta.

Para ello es necesario establecer políticas de seguridad coherentes y enmarcadas dentro de los límites de cumplimiento de la empresa, cuyo objetivo será apoyar y proporcionar la guía para gestionar adecuadamente la seguridad de la información.

Las políticas definidas a continuación cubren las necesidades de seguridad: Organizacional, lógica, física y legal de la empresa Plasticaucho Industrial en lo referente al manejo adecuado para salvaguardar la información, las mismas que siguen la línea de cumplimiento de los controles de la norma ISO 27001.

- Seguridad Organizacional (Gestión de activos – Recursos humanos)

  Se establecerá un marco formal a través del cual se maneje la empresa incluyendo aspectos relacionados como servicios, gestión de activos, recursos humanos, físicos, responsabilidades y actividades complementarias ante eventualidades relacionadas a la seguridad de la información.

- Seguridad Lógica (Control de acceso – gestión de las operaciones y comunicaciones)

  Se establecerán los lineamientos y normativas para la gestión de control de acceso por parte de los usuarios tanto a sistemas empresariales como a equipos para evitar alteraciones en la configuración de los mismos. Además se definen normativas para el control de vulnerabilidades por causa de software malicioso.

- Seguridad Física

  Se establecen límites en cuanto a la definición de perímetros de seguridad, además se implementarán controles relacionados con el manejo, mantenimiento y soporte técnico de los equipos.

- Seguridad Legal - Cumplimiento

Se deben integrar las políticas y normativas de seguridad establecidas bajo el régimen o reglamentación interna de la empresa Plasticaucho Industrial para verificar el cumplimiento de las mismas y a partir de ello definir sanciones al personal de la organización ante faltas cometidas y que vulneren la seguridad de la información.

4.6.1 POLÍTICAS QUE REGULAN ACTIVIDADES RELACIONADAS USO DE TECNOLOGÍAS

4.6.1.1 Finalidad

Las Políticas de Tecnología de la Información y Comunicación tienen como finalidad el proteger la información, a la empresa y buscar un aumento en la seguridad y aprovechamiento de la tecnología, lo que contribuye de manera determinante a aumentar la eficiencia en el trabajo y garantizar la continuidad de las operaciones de la empresa.

4.6.1.2 Ámbito

Las Políticas de Tecnología de la Información y Comunicación serán aplicadas de manera obligatoria por las y los empleados, servidores y trabajadores que integran Plasticaucho Industrial a nivel nacional, que utilicen el hardware, software y comunicaciones, para el cumplimiento de sus actividades diarias.

4.6.1.3 Responsable

El departamento de Tecnología de la Información será la encargada de administrar y ejecutar estas políticas a través de procedimientos, asimismo las políticas deben cumplirse a nivel nacional por las dependencias que tienen a su cargo el uso de recursos tecnológicos.

4.6.1.4 Recursos Tecnológicos

Las Políticas de Tecnología de la Información regularán y estandarizarán el uso de los recursos informáticos que Plasticaucho Industrial pone a disposición de todo el personal para desarrollar sus actividades y cumplir con la misión de la Empresa.

4.6.1.5 Términos

Se definen los siguientes términos:

- ***Tecnologías de información y comunicaciones.-*** Equipos informáticos, software y dispositivos de impresión personalizados y centralizados que se utilizarán para

almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

- ***Hardware*.-** Componente físico de un computador y dispositivos externos.
- ***Información.-*** Conjunto de datos procesados y organizados.
- ***Usuarios.-*** Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.
- ***Seguridad informática.-*** Es el área de tecnología de la información que se centra en la protección de la infraestructura informática y todo lo relacionado con ella, especialmente, la información contenida o circulante.
- ***Integridad.-*** Refiere a la corrección y complementación de los datos en una base de datos.
- ***Confidencialidad.-*** La información solo debe ser accesible únicamente para personal autorizado.
- ***Disponibilidad.-*** Debe estar disponible cuando se necesita, es decir, accesible.
- ***Amenaza*.-** Evento que puede desencadenar en un incidente en la empresa, que cause daños materiales o pérdidas inmateriales en sus activos.
- ***Impacto.-*** Medir la consecuencia al materializarse una amenaza.
- ***Vulnerabilidad.-*** Posibilidad de que ocurra mediante una exploración, se viole la seguridad del sistema.
- ***Ataque.-*** Evento exitoso o no, que atenta sobre el buen funcionamiento de un sistema.
- ***Backup.-*** Respaldo de la información.
- ***Passwords.-*** Clave que se asigna a los usuarios.
- ***Retención.-*** Tiempo de vigencia de un respaldo.
- ***Dirección MAC-*** Identificador de 48 bits (6 bloques hexadecimales) que corresponde de manera única a una tarjeta o dispositivo de red.
- ***Dirección IP-*** Es un número que identifica, lógica y jerárquicamente, una interfaz de red (elemento de comunicación / conexión) de un dispositivo (computadora, tableta, computadora portátil, teléfono inteligente) que utiliza el protocolo IP (Protocolo de Internet), que corresponde al modelo de red de nivel TCP/IP.
- ***URL.-*** Dirección web.
- ***TI.-*** Tecnologías de la Información.

- ***Shareware.-*** Modalidad de distribución de software, en la que el usuario puede evaluar el producto de forma gratuita, pero con limitaciones en tiempo de uso o en algunas formas de uso o con restricciones.
- ***Freeware.-*** Tipo de software que se distribuye sin ningún costo, disponible para su uso y por tiempo ilimitado.

4.6.2 POLITICA PARA EL USO ADECUADO DE LAS TECNOLOGIAS DE INFORMACION Y COMUNICACIONES

4.6.2.1 Responsables

Personal con el cargo de: Gestor de Hardware y Software, Analista de Seguridades TI, Soporte Técnico.

4.6.2.2 Generales

Los usuarios internos para el uso adecuado de los recursos tecnológicos tomarán en cuenta las siguientes indicaciones:

1. Para el hardware (equipos, impresoras, escáner, servidores y demás recursos tecnológicos) de propiedad Plasticaucho Industrial, el departamento de Tecnología de la Información es la única autorizada para realizar las actividades de soporte técnico, mantenimiento y cambios de configuración en el equipo de cómputo. En el caso de trabajos de mantenimiento efectuadas por terceros, éstas serán previamente autorizadas por el departamento de Tecnología de la Información.
2. En caso de equipos tecnológicos en estado de arrendamiento, la empresa proveedora es la única autorizada a realizar los trabajos de mantenimiento y cambio de hardware o en su caso autorizar dichas labores, previa coordinación con el departamento de Tecnología de la Información.
3. El acceso al área de infraestructura informática es restringido y únicamente ingresará personal autorizado.
4. Se restringirá el acceso a los equipos tecnológicos, a aquellos usuarios que no cuenten con una autorización previa de su Gerencia o Jefatura para laborar fuera de horario.
5. Las/os usuarios autorizados de los sistemas informáticos de Plasticaucho Industrial, no harán uso indebido de suministro, información empresarial, datos en general y datos considerados como confidenciales.

6. Las bases de datos de la empresa estarán centralizadas en el Data Center del departamento de Tecnología de la Información, de existir bases de datos separadas o no compatibles con la infraestructura tecnológica se implementarán proyectos de integración y/o migración de aplicativos y base de datos a cargo del departamento de Tecnología de la Información con participación de las unidades de negocio involucradas.
7. Los sistemas de información desarrollados internamente o aquellos adquiridos a terceros, estarán instalados en la infraestructura disponible en el departamento de Tecnología de la Información (licenciamiento, software, código fuente, hardware).
8. La identidad de los usuarios externos y los derechos de acceso otorgados, se mantendrán en un repositorio central, sea un documento que contenga al menos los siguientes campos como: nombres/apellidos, cédula de ciudadanía/identidad, empresa o entidad en la que labora, nombre del proyecto, responsable del proyecto, fecha de solicitud de los permisos, fecha de expiración de los permisos, sitios a los que se otorgó el acceso, dirección IP de la máquina, dirección MAC de la máquina, persona que autoriza y persona que otorga el acceso.
9. Se prohíbe a los usuarios utilizar los permisos otorgados para fines diferentes a los especificados en la solicitud de acceso, así como también se prohíbe el intercambio de direcciones IP con otros usuarios que no estén incluidos en la solicitud.
10. En caso de que el usuario tenga la sospecha que sus accesos han sido comprometidos, solicitará de manera inmediata su bloqueo al departamento de Tecnología de la Información.
11. Para el caso de conexiones inalámbricas, por defecto se otorgará acceso a la red de visitantes de la empresa. Si se especifican accesos puntuales, se otorgará acceso a la red corporativa con un perfil de navegación de acuerdo a sus necesidades.
12. Se mantendrá un inventario actualizado de los activos tecnológicos.
13. Todos los equipos de propiedad de Plasticaucho Industrial a nivel nacional, se sujetarán a la versión del software antivirus, que determine el departamento de Tecnología de la Información, el software estará bajo protección en tiempo real en el sistema operativo.
14. Bajo ninguna circunstancia las/os empleados/as de la empresa, podrán utilizar los activos informáticos para realizar actividades que están prohibidas por las políticas.

4.6.2.3 Hardware

El hardware de propiedad de Plasticaucho Industrial o arrendado, se utilizará únicamente para actividades relacionadas con los objetivos de la empresa, para lo cual se observará lo siguiente:

1. Para el correcto funcionamiento del hardware se realizará mantenimiento preventivo, de acuerdo a un plan de mantenimiento preventivo del equipo de cómputo anual, elaborado por los técnicos de soporte del departamento de Tecnología de la Información.
2. La adquisición de bienes tecnológicos se ejecuta de acuerdo al PERFIL TECNOLÓGICO DEL CARGO aprobado por Gestión Humana, en coordinación con el departamento financiero y Tecnología de la Información.
3. Cuando exista algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa al hardware de Plasticaucho Industrial, se notificará de inmediato a las autoridades competentes y al departamento de Tecnología de la información.
4. Solamente el personal de Plasticaucho Industrial autorizado por el departamento de Tecnología de la Información, está facultado para abrir los gabinetes de las computadoras personales o de cualquier otro equipo de cómputo propiedad de la empresa, que NO cuenten con la garantía técnica vigente.
5. Para los equipos cuya garantía técnica aún se encuentre vigente, lo efectuará únicamente el personal técnico calificado de la empresa proveedora.
6. Para los equipos de cómputo de arrendamiento, la empresa arrendadora es la única autorizada para abrir los gabinetes de dichos equipos o en su caso autorizará la apertura de ellos, previa coordinación con el departamento de Tecnología de la Información.

4.6.2.4 Data Center

En el Centro de Datos de Plasticaucho Industrial se alojarán los servidores y equipos de comunicaciones necesarias para la operación de las actividades informáticas de la empresa y se observará lo siguiente:

1. El acceso a los centros de datos es restringido y sólo personal autorizado por el departamento de Tecnología de la Información puede tener acceso a él.

2. El acceso a los servidores de los centros de datos, ya sea usando la consola de administración local o una consola de administración remota es restringido al personal autorizado por el departamento de Tecnología de la Información.

4.6.2.5 Propiedad de la información

Los/as usuarios de cualquier equipo de cómputo de Plasticaucho Industrial deben estar informados y conocer que los datos que ellos crean y manipulan en los sistemas, aplicaciones y cualquier medio de procesamiento electrónico, durante sus actividades laborales, son de propiedad y responsabilidad de Plasticaucho Industrial, para lo cual se respetará lo siguiente:

1. Los derechos patrimoniales de un programa de computación, hojas de cálculo, archivos de Word, macros, etc., y su documentación, creados por uno o varios empleados en el ejercicio de sus actividades laborales corresponden a Plasticaucho Industrial.
2. Los respaldos que contengan información de Plasticaucho Industrial y que fueron realizados o solicitados por el usuario del equipo de cómputo, se tendrán exclusivamente bajo resguardo, debiendo entregarlos al superior inmediato al finalizar su relación laboral con la empresa, mediante la respectiva acta de entrega recepción.

4.6.2.6 Usos inadecuados

Las siguientes actividades están prohibidas:

1. Violar los derechos de cualquier persona o empresa protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades, se incluye la distribución o instalación de software sin la licencia de uso adecuada adquirida por Plasticaucho Industrial (Políticas de Uso de Software).
2. Difundir información identificada como confidencial a través de medios que involucren el uso de equipos tecnológicos.
3. Introducir software malicioso en la red o en los servidores (virus, troyanos, ráfagas de correo electrónico no solicitado, etc.).
4. Utilizar la infraestructura de tecnología de información de Plasticaucho Industrial para conseguir o transmitir material con fines de lucro.

5. Utilizar el sistema de comunicaciones de Plasticaucho Industrial con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier actividad hostil.
6. Hacer propuestas fraudulentas de productos o servicios cuyo origen sean los recursos o servicios propios de Plasticaucho Industrial.
7. Realizar actividades que incumplan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.
8. Monitorear puertos o realizar análisis del tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad. El personal del departamento de Tecnología de la Información y encargado de la Seguridad Informática puede realizar estas actividades siempre y cuando cuente con la aprobación por parte del Jefe de área.
9. Eludir mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
10. Usar comandos o programas para el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet, Intranet).
11. Instalar cualquier tipo de software en los equipos de cómputo de Plasticaucho Industrial sin la previa autorización del departamento de Tecnología de la Información.
12. Modificar la configuración del software antivirus, firewall personales o políticas de seguridad en general implementadas en los equipos de cómputo de Plasticaucho Industrial sin consultar previamente con el departamento de Tecnología de la Información.
15. No se permite la reproducción de archivos de música, video si éstos están cualquier URL de Internet (aplicable para los usuarios que hacen uso del servicio de Internet).

4.6.2.7 Excepciones

Para propósitos de mantenimiento de la red y de seguridad, por excepción el personal debidamente autorizado, podrá estar exento de seguir algunas de las restricciones anteriores, debido a las responsabilidades bajo su cargo o a eventos programados. Estos privilegios de accesos deberán ser solicitados al departamento de Tecnología de la Información anexando la justificación respectiva, vía correo electrónico y/o de manera escrita.

4.6.3 POLITICA DE CONTRASEÑAS

4.6.3.1 Responsables

Personal con el cargo de: Analista de Seguridades TI, Soporte Técnico.

4.6.3.2 Generales

El cumplimiento de la política de contraseñas por parte de las/os usuarios internos de Plasticaucho Industrial, es extremadamente importante ya que se establecen como la primera línea de defensa para garantizar que el acceso a los aplicativos de información sólo sea realizado por personal autorizado.

4.6.3.3 Administración

Se acatará lo siguiente:

1. Todos los usuarios internos de Plasticaucho Industrial requieren de un nombre de usuario y una contraseña para utilizar el equipo de cómputo que se le haya asignado y servicios de red como correo electrónico, impresión, archivos compartidos, Intranet, Internet etc.
2. Todas las contraseñas son personales e intransferibles. Se prohíbe a los usuarios dar a conocer a terceras personas su contraseña, quien así lo hiciere debe considerar que sigue siendo el único responsable de las actividades que se realicen con su usuario y contraseña.
3. Todas las contraseñas del sistema (cuentas de administrador, cuentas de aplicaciones, etc.) se cambiarán con una periodicidad de al menos cada 30 días.
4. Todas las contraseñas del usuario (cuentas de usuario, cuentas de servicios web, etc.) se cambiarán al menos cada 30 días.
5. En caso de que el usuario detecte que su contraseña ha sido comprometida deberá cambiar su contraseña o solicitar al departamento de Tecnología de la Información.
6. En caso de olvido o bloqueo de su contraseña, el usuario debe coordinar el restablecimiento de la misma con el responsable del departamento de Tecnología de la Información.
7. Las contraseñas de los usuarios deben cumplir con ciertos requerimientos de seguridad los cuales definirá el departamento de Tecnología de la Información con el objeto de evitar que los usuarios elijan contraseñas débiles. No se utilizarán contraseñas que resulten obvias, fáciles de descubrir, o predecibles para un

atacante: (el mismo usuario, palabras de diccionario, fechas o nombres de personas cercanas, secuencias de números repetidos o consecutivos).

8. Las contraseñas para acceso al equipo informático deberán ser modificadas por el usuario la primera vez que acceda a su cuenta.
9. Las contraseñas de los sistemas internos contarán con contraseñas independientes de la utilizada para iniciar sesión en la red corporativa.
10. Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única.
11. Los derechos de acceso al correo electrónico, red corporativa, servidores de archivos y otros servicios provistos por el departamento de Tecnología de la Información, deben estar alineados con necesidades de negocio definidas, firmadas, con requerimientos de trabajo.
12. Los usuarios internos de Plasticaucho Industrial, deberán negar la opción de recordar contraseñas que se presentan en los navegadores, con el fin de evitar la autenticación automática de acceso a los sistemas informáticos que operan en la intranet como en el Internet.
13. Cuando un usuario se desvincule de la empresa o se le asigne un rol diferente, el Jefe inmediato junto con el área de Gestión Humana deberá notificar al departamento de Tecnología de la Información para suspender los usuarios de la red corporativa, sistemas especializados, etc. De la misma manera, el área de Gestión Humana, reportará de manera inmediata al departamento de Tecnología de la Información el listado de traspasos, renuncias, y otros movimientos de personal con el fin de coordinar la cancelación de los derechos de acceso a servicios e información que dispongan dichos usuarios.
14. Las/os empleados, deberán suscribir un compromiso de responsabilidad en seguridad y uso de usuario y claves de acceso a la información de recursos tecnológicos administrados por el departamento de Tecnología de la Información

4.6.3.4 Prohibiciones

Las actividades que se detallan a continuación están prohibidas:

1. Revelar o compartir su contraseña de cualquier manera.

2. Escribir la contraseña o almacenarla en archivos, comunicarla en el texto de correo electrónico, o en cualquier otro medio de comunicación electrónica.
3. Comunicar las contraseñas en conversaciones telefónicas.

4.6.4 POLITICA DE USO DE CORREO ELECTRONICO

4.6.4.1 Responsables

Personal con el cargo de: Analista de Seguridades TI.

4.6.4.2 Generales

El Correo Electrónico (email) es un recurso que la empresa pone a disposición de las/os empleados de Plasticaucho Industrial, como una herramienta de comunicación, colaboración e intercambio de información, se observará lo siguiente:

1. El acceso a estos recursos, estará limitado a la aceptación de la presente Política de Uso.
2. Las comunicaciones de la empresa efectuadas por correo electrónico, solo podrán ser realizadas por las cuentas corporativas creadas en el departamento de Tecnología de la Información.
3. Las cuentas de correo asignadas a los empleados de cada área, deberán ser utilizadas sólo para actividades laborales que estén relacionadas con los propósitos y funciones empresariales.
4. Los buzones de correo electrónico, creados para las/os empleados de Plasticaucho Industrial, y toda la información contenida en los mismos, son propiedad exclusiva de la empresa.
5. El departamento de Tecnología de la Información se reserva el derecho para modificar las condiciones de uso establecidas cuando lo considere necesario. También podrá modificar o bloquear servicios relacionados al servicio de correo electrónico cuando sea necesario, por razones administrativas, mantenimiento, causas de fuerza mayor o por necesidad empresarial.

4.6.4.3 Tipos de Cuentas

1. Cuentas Personales**:** El personal de Plasticaucho Industrial, contará con una cuenta de correo electrónico con capacidad de bandeja asignada.

2. Cuentas Temporales: Estas cuentas se crearán bajo propósitos específicos, que serán detallados al momento de crearla. Además se especificará el tiempo de validez, para que sea eliminada una vez que ya no se la requiera.
3. Cuentas Departamentales: Estas cuentas serán creadas, con el objetivo de comunicación a todos los miembros de una determinada área o lista de usuarios específica.

4.6.4.4 Responsabilidades

1. Los servicios de correo electrónico serán administrados por el departamento de Tecnología de la Información y será el responsable de vigilar el correcto funcionamiento y operación de dicho servicio.
2. El área de Gestión Humana deberá comunicar al departamento de Tecnología de la Información, sobre el personal que haya ingresado a laborar en la empresa, así como el personal que ha dejado de laborar, para la activación o desactivación de las cuentas de correo respectivas.
3. Los usuarios son los únicos responsables de todas las actividades realizadas, desde sus cuentas de acceso y buzones.
4. La información transmitida mediante el servicio de correo electrónico, es responsabilidad única y exclusiva de cada usuario.
5. La cuenta de correo es intransferible, por lo que la información que corresponde al inicio de sesión (usuario, contraseña) no se debe proporcionar a otras personas.
6. La información que se recibe de manera personal y confidencial por correo electrónico, no se puede reenviar a otra persona, sin la autorización del remitente.

4.6.4.5 Gestión del buzón de correo

1. Cuidar que la gestión de la información contenida en su cuenta de correo electrónico sea la adecuada. Para lo cual debe revisar periódicamente sus bandejas de correo, se recomienda eliminar los mensajes que no deban conservarse y archivar el resto carpetas o subcarpetas apropiadas.
2. Respaldar periódicamente la información contenida en su buzón de correo, para lo cual podrán solicitar soporte al departamento de Tecnología de la Información para la gestión de esta actividad.

3. Resguardar la seguridad del buzón de correo, el usuario deberá evitar la recepción de correo cuando se desconozca al remitente ya que en ocasiones este puede ser un mensaje con contenido potencialmente peligroso o un virus.
4. El departamento de Tecnología de la Información definirá el espacio y los servicios asignados para cada cuenta de correo electrónico, de acuerdo a las necesidades que se requiera.

4.6.4.6 Uso Inaceptable

El mal uso del correo electrónico se considera las siguientes actividades:

1. Utilizar el correo electrónico para actividades comerciales diferentes a la empresa.
2. Participar en la propagación de cadenas, esquemas piramidales y otros similares de envío con el correo empresarial.
3. Enviar o reenviar mensajes con contenido ofensivo, difamatorio, racista u obsceno.
4. Enviar mensajes anónimos, así como aquellos que consignen cargos o funciones no oficiales.
5. Utilizar mecanismos y sistemas, que traten de ocultar o suplantar la identidad del emisor del correo electrónico.
6. La saturación y falta de mantenimiento del buzón de correo por parte del usuario.
7. Apropiarse de cuenta(s) de correo diferente a la asignada a su persona.
8. Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado, considerado como "spam".

4.6.5 POLITICA DE USO DE SEGURIDAD INFORMATICA Y DE LA INFORMACION

4.6.5.1 Responsables

Personal con el cargo de: Coordinador de Infraestructura, Analista de Seguridades TI, Soporte Técnico.

4.6.5.2 Generales

Las/os usuarios internos cumplirán las siguientes recomendaciones:

1. Si no va a estar cerca de su sitio de trabajo, bloquee el equipo. Se recomienda activar el bloqueo automático de la pantalla del computador para que cuando detecte inactividad no pueda ser utilizado, sin ingresar una contraseña.

2. No modificar las configuraciones del equipo como fondo de pantalla y protector de pantalla, así como la configuración de software y hardware establecidos por el departamento de Tecnología de la Información. Si en su equipo se han realizado modificaciones, se debe notificar de manera inmediata para que se realice la re-configuración del mismo.
3. Está prohibido instalar aplicaciones, programas, utilitarios, que no sean aprobados o que difieran del software designado por el departamento de Tecnología de la Información, que no tengan licencias o que para su uso se deba corromper la seguridad de licenciamiento del mismo.
4. Para evitar pérdida de información, el usuario es responsable de respaldar su información importante periódicamente y verificar que los respaldos generados se encuentren disponibles, e íntegros para su uso cuando sea requerido.
5. No pueden moverse los equipos o reubicarlos sin permiso. En caso de que necesite movilizar un equipo propiedad de la empresa se requiere autorización del Jefe inmediato en coordinación con el departamento de Tecnología de la Información.
6. Está prohibido desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios y/o alterar o dañar los recursos informáticos.
7. Todo el personal que accede a los sistemas de información de Plasticaucho Industrial debe utilizar únicamente las versiones de software instaladas y siguiendo sus normas de uso.

4.6.5.3 Compromiso de Confidencialidad

Las/os empleados de la empresa deberán firmar compromisos de confidencialidad y de no-divulgación de información de conformidad con lo dispuesto las necesidades de protección de información de la empresa.

1. El área de Gestión Humana será encargada de controlar que los compromisos de confidencialidad de la información, documento físico o electrónico, sean firmados por todo el personal de la empresa sin excepción, custodia de los compromisos firmados, adjuntar con el contrato de cada empleado, y controlar que la firma de los compromisos de confidencialidad sean parte de los procedimientos de incorporación de nuevos integrantes a la empresa.
2. El personal de entidades externas; deberán de igual manera suscribir el compromiso de confidencialidad previo su acceso a la información.

4.6.5.4 Responsables de la seguridad

Los responsables de la seguridad informática de los activos será el departamento de Tecnología de la Información a cargo de la persona de Seguridad de la Información dispuesto en el área.

4.6.5.5 Responsables de la Información

Los responsables de la información se definen para asegurar adecuadamente la custodia, pertenencia y salvaguarda de los recursos, teniendo en cuenta una correcta distribución de funciones, que se diferencian entre:

a) Responsables Directos: Los responsables directos de la información son quienes que por la naturaleza de su posición en la empresa conocen el tipo de información que se genera o comunica o ingresen en los diversos sistemas o aplicativos, pueden ser las Gerencias, Jefaturas o aquellos designados como delegados para dicha actividad, serán responsables de:
   - La clasificación directa, de la organización y la autorización del acceso a la información.
   - Manejo, transmisión, comunicación y almacenamiento de la información.
   - Monitoreo del uso de la información por parte de personal que está a su cargo.
   - Asignar a quienes serán responsables del uso y manejo de la información.

b) Responsables Secundarios: Los responsables secundarios de la información son quienes que por la naturaleza de su cargo en la empresa deben acceder, modificar o almacenar información. Son responsables de:
   - Manejo, transmisión, comunicación y almacenamiento de la información a la que se le haya dado acceso.

c) Custodios: Los custodios de la información son quienes que por la naturaleza de su cargo en la empresa deben cuidar, respaldar o almacenar la información. Se convierten en custodios el personal que tenga acceso a la información. Entre sus responsabilidades constan:
   - El manejo, transmisión, comunicación y almacenamiento de la información a la que se le haya dado acceso.
   - Mantener la disponibilidad e integridad de la información.
   - Mantener el acceso y permisos de acceso a la información.
   - Colaborar para evaluar e identificar la información para su clasificación.

4.6.5.6 Clasificación de la Información

Los responsables directos de la información deberán clasificar adecuadamente la información que manejan y asegurarse de que se respete el acceso a la misma por parte del personal que está a su cargo.

Los activos de información de la empresa deben ser clasificados en una de las categorías definidas en el punto Niveles de Clasificación de Información de la Política de Seguridad de la Información.

Para clasificar la información dentro de uno de los niveles determinados o modificar su categoría, se deben tomar en cuenta los criterios de clasificación de información mencionados en el punto Criterios de Clasificación de la Política de Seguridad de la Información.

La información será rotulada claramente con la clasificación que le sea otorgada, la misma que debe ser clara y visible.

Toda la información generada en la empresa y que no se le dé una clasificación específica, mantendrá el nivel de PRIVADA y deberá ser considerada como tal.

1. Criterios de Clasificación.- Son:
    a) Valor: Es el principal criterio de clasificación, se basa en el valor del activo desde el punto de vista del negocio (valor propio del activo o producto del mismo).
    b) Edad: Es donde la clasificación de cierta información puede variar si el valor de la información se reduce con el tiempo.
    c) Vida útil: Es cuando la información se vuelve obsoleta en base a nueva información generada, por cambios organizacionales u otros motivos.
2. Niveles de clasificación de la Información.- Son:
    a) Pública: Es la información que por su naturaleza, puede ser visible o divulgada por el personal general de la empresa, clientes o el público en general, sin riesgo de que su contenido pueda afectar en ningún sentido la integridad o economía de la empresa.
    b) Privada: Solo para uso interno, destinada al uso exclusivo por parte de los empleados de la empresa en el desarrollo diario de los procesos de negocio.

La divulgación o visibilidad de la misma dentro de la organización es segura. Esta información debe ser mantenida dentro de la organización; su divulgación fuera de la misma puede tener un impacto leve o moderado de la privacidad del personal o causar un daño leve al negocio o la imagen de la organización.

c) Restringida: Información por su naturaleza es destinada solo para uso exclusivo de la empresa. Esta información debe ser accedida y visualizada solo por el personal de la empresa que cuente con la autorización y extenderse a las dependencias de Plasticaucho Industrial en general.

La divulgación o visualización no autorizada dentro de la organización o fuera de ella podría violar la privacidad de personas, reduciría ventaja competitiva de la organización o causar un daño significativo al negocio o la imagen de la organización.

d) Confidencial: Es la información considerada como sensible y está destinada a uso solamente interno y por parte del personal específico que debe tener permisos y autorización para su visualización y/o manejo.

La divulgación o visualización no autorizada causaría violación de la privacidad de las personas, reduciría ventaja competitiva de la organización o produciría un daño grave o irreparable al negocio o la imagen de la organización.

3. Acceso a recursos y privilegios.- Los usuarios deberán tener el nivel necesario de privilegios para acceso a las aplicaciones, o acceso a recursos para cumplir con las actividades de su cargo.
4. Gestión de Incidentes de Seguridad.- La gestión de incidentes de seguridad se debe realizar considerando los siguientes objetivos básicos:
   - Responder rápida y eficientemente.
   - Solucionar el daño causado por los incidentes.
   - Prevenir daños futuros.
5. Segregación Funcional.- Ningún proceso crítico debe ser conocido o ejecutado por una sola persona, o que un mismo usuario tenga privilegios o accesos en diferentes fases de un proceso. Los distintos procesos del negocio deben ser claramente

descritos, de tal manera que cualquier persona de la empresa pueda ser capaz de asumir los roles y responsabilidades de otra.

6. Prevención y Entrenamiento Continuo.- Las políticas, reglamentos y normas referentes a la Seguridad de la Información deberán ser conocidos por todos los miembros de la organización y para el efecto, la empresa proveerá recursos necesarios para realizar capacitaciones a los distintos usuarios de aplicaciones, personal técnico y demás personal de la empresa en general.

4.6.5.7 Almacenamiento

La información obtenida de cualquier servicio y que sea almacenada localmente en el equipo de cómputo del usuario y sea propiedad de la empresa, no podrá ser distribuida o transmitida por ningún medio de comunicación sin la autorización del inmediato superior.

Es responsabilidad del usuario solicitar de forma periódica al departamento de Tecnología de la Información, el respaldo de dicha información.

El departamento de Tecnología de la Información revisará el aprovechamiento óptimo de los recursos compartidos en la red para mantener la integridad y asegurar que los usuarios utilicen los recursos de manera responsable.

4.6.5.8 Transmisión de datos

A fin de garantizar la integridad y confidencialidad de la información obtenida de los sistemas y aplicativos informáticos de la empresa y en razón de que los dispositivos móviles, magnéticos y los soportes extraíbles generan vulnerabilidades como divulgación no autorizada, robo, datos dañados o comprometidos, por la facilidad de uso, el departamento de Tecnología de la Información, de forma programada y bajo pedido, procederá a salvaguardar la información cuando se requiera que sea transferida.

4.6.5.9 Propiedad y Derechos de contenidos

La información disponible en internet, que incluyen software, música, video, sonido, fotografía, gráficos, textos u otro material contenido, está protegida por copyright, marcas registradas, patentes u otros derechos de propiedad y leyes.

1. Se permite sólo el uso de este material bajo autorización expresa del autor.

2. El bajar, cargar, archivar, copiar, imprimir o enviar cualquier material debe ser realizado solamente bajo la autorización del autor.
3. Los usuarios no deben descargar, ni instalar ningún software de tipo comercial, shareware o freeware en las unidades de disco de los equipos de cómputo, sin la autorización del departamento de Tecnología de la Información.

4.6.5.10 Respaldo de la información tecnológica

El departamento de Tecnología de la Información, y las diferentes áreas propietarias de la información, determinarán el procedimiento de resguardo y contención de la información obtenida de los sistemas y/o aplicativos informáticos, considerando al menos los siguientes puntos:

1. Se debe establecer un cronograma donde se detallen los períodos de tiempo en los cuales se realizarán los respaldos de la información.
2. Etiquetado de las copias de respaldo, tipo de contenido, periodicidad y retención.
3. Extensión (completo/diferencial) y la frecuencia que se realice los respaldos, de acuerdo a los requisitos del negocio de la empresa.
4. Guardado de los respaldos en un sitio seguro, evitar cualquier daño debido a desastres en la empresa.
5. Grado apropiado para la protección física y ambiental.
6. Eventos regulares para verificar y restaurar los respaldos, garantizando que sean confiables para su uso en alguna emergencia.

4.6.5.11 Recursos compartidos

El uso de carpetas compartidas en los equipos informáticos de propiedad de Plasticaucho Industrial, es una práctica que tiene algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto su uso para la aplicación debe ser controlado. Por lo cual la organización define los siguientes puntos para su uso seguro:

1. Se debe evitar el uso de carpetas compartidas sin autorización del propietario de la información en equipos de cómputo.
2. Los administradores de red establecen e implementan, en las solicitudes aprobadas la configuración de acceso a la carpeta compartida, previo requerimiento formal de la misma a través de la mesa de ayuda (Helpdesk).

3. El usuario que autorice y tiene a su disposición el recurso compartido es principal el responsable de las acciones y los accesos sobre la información de dicha carpeta.
4. Se debe definir el tipo de acceso y los roles que sean estrictamente necesarios sobre la carpeta compartida (lectura, lectura y escritura).
5. Se definir el límite de tiempo durante el cual estará disponible la información y compartido el recurso en el equipo.
6. Para la información confidencial o crítica de la empresa, deben utilizarse las carpetas designadas para tal fin en el servidor de archivos, para que sean incluidos en las copias de respaldo de información o implementar herramientas para respaldar continuamente la información sobre dichos equipos.
7. El acceso a las carpetas compartidas debe delimitarse a los usuarios que las necesitan y estar protegidas con contraseñas.
8. No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con antivirus actualizado.

4.6.5.12 Registro de eventos

El registro de eventos generará trazabilidad en las operaciones realizadas en los sistemas de información y sistemas operativos, para monitorear los servicios informáticos.

1. Todos los sistemas de información, aplicaciones, sistemas operativos, bases de datos, dispositivos de seguridad, dispositivos de comunicación y servidores deben tener registros o registros de auditoría que verifiquen las actividades del usuario, excepciones, fallas y eventos de seguridad.
2. Es responsabilidad de los administradores del departamento de Tecnología de la Información, estar al tanto de la activación de los registros de auditoría.
3. La persona a cargo de las aplicaciones deben mantener un inventario de los registros de auditoría existentes por aplicación y su ubicación.
4. Los registros sobre actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información se deben preparar, mantener y revisar periódicamente.
5. Es responsabilidad de los propietarios de la información, solicitar y saber qué eventos han ocurrido en los sistemas de tratamiento de su información.

6. Es responsabilidad de los administradores de infraestructura y sistemas de información establecer un plan de respaldo de los registros de auditoría a través de la herramienta que se disponga.
7. Se debe establecer pautas para la retención, respaldo y recuperación de archivos logs y los registros de auditoría de los sistemas de información cuando corresponda, ya que constituyen evidencia para la identificación de un incidente de seguridad.
8. Garantizar que no se pierda, ni se sobre-escriba los respaldos de archivos logs de los sistemas de información.

4.6.6 POLITICAS DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.6.6.1 Responsables

Personal con el cargo de: Coordinador de Infraestructura, Analista de Seguridades TI.

4.6.6.2 Generales

Para controlar la asignación de las responsabilidades y del correcto uso de los dispositivos móviles y el teletrabajo, se tomarán en cuenta los siguientes lineamientos.

4.6.6.3 Segregación de funciones

Las tareas y responsabilidades propias de gestión de tecnología, se deben segregar para reducir e impedir las oportunidades de acceso no autorizado a la red y cualquier modificación o mal uso de los activos de los sistemas de información. Se prestará especial cuidado que una persona no pueda por si misma acceder, modificar o utilizar los activos, sin previa autorización.

4.6.6.4 Separación de Ambientes

Cuando aplique los ambientes de desarrollo, pruebas y producción deben estar separados para reducir los riesgos de acceso o cambios no autorizados, prevenir fallos e implementar controles.

4.6.6.5 Planificación y Aceptación

Se deben definir los requisitos de capacidad futura, con el fin de reducir el riesgo a una sobrecarga del sistema. Los requisitos operativos de sistemas nuevos se deben establecer, documentar y probar antes de su aceptación. Los requisitos de restitución para los servicios apoyados por diferentes aplicaciones se deben

coordinar y revisar frecuentemente. Los administradores del departamento de Tecnología de la Información deben estar alerta a los riesgos asociados a estas tecnologías, así mismo considerar la toma de medidas especiales para su prevención o detección.

4.6.6.6 Uso equipos portátiles, dispositivos móviles y teletrabajo

Los colaboradores, contratistas y terceros se comprometen hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la empresa, tales como escritorios y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros, atendiendo las siguientes directrices:

1. La asignación de los equipos se lo debe realizar mediante un procedimiento documentado, en el cual se registre las características, modelo, serie, estado en el que se encuentra el dispositivo, de esta manera mantener un inventario activo.
2. Al tratarse de dispositivos sensibles, es necesario implementar un software de localización.
3. El dispositivo móvil debe estar en el bolsillo, maletín o lugar no visible en partes públicas.
4. Los equipos deben estar configurados para bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como: contraseña, patrón huella dactilar, reconocimiento de voz, entre otras.
5. Uso de aplicación de antivirus.
6. Las conexiones a redes ajenas a la empresa, no se deben configurar como visibles a otros dispositivos de la red.

4.6.6.7 Seguridad de los equipos y activos fuera de las instalaciones

1. El empleado tendrá una identificación personal, donde se visualice la autorización de la salida de los equipos fuera de las instalaciones de Plasticaucho Industrial.
2. El empleado que no cuente con una identificación, debe solicitar al departamento de Tecnología de la Información un documento firmado que indique las características del equipo que saldrá de las instalaciones, todo esto previamente autorizado y solicitado por su gerencia o jefatura.
3. Se deben revisar los equipos que salen de la empresa y mantener un inventario actualizado con el responsable de su custodia.

4. El área de seguridad física debe revisar cada equipo que sale o ingresa a las instalaciones de la empresa con su respectiva autorización.
5. Cada empleado de la organización deberá mantener un informe detallado sobre el estado y uso de los activos informáticos hacia el departamento de Tecnología de la Información.
6. El empleado es el único responsable del equipo que se le haya facilitado para el desempeño de sus actividades fuera de las instalaciones.

4.6.6.8 Prohibiciones

Están prohibidas las siguientes actividades

1. Instalar software que ocasiones modificaciones de configuración del equipos sin autorización del departamento de Tecnología de la Información.
2. Modificar configuraciones del sistema BIOS por parte del usuario.
3. Exponer los equipos a altas temperaturas que ocasionen daños a los equipos.
4. Usar los equipos para fines personales distintos a los de la empresa.

4.6.7 POLITICA DE USO DE SOFTWARE

4.6.7.1 Responsables

Personal con el cargo de: Gestor de Hardware y Software, Analista de Seguridades TI, Soporte Técnico.

4.6.7.2 Administración

El departamento de Tecnología de la Información será el único encargado a nivel nacional, de la administración, instalación, soporte y funcionamiento del software instalado en los equipos de propiedad de Plasticaucho Industrial. Dentro de las responsabilidades de la administración e instalación de software se detallan las siguientes:

1. Mantener el resguardo de las licencias de uso de software de la empresa.
2. Mantener actualizado el catálogo de software de la empresa, y desinstalar el software de los equipos que no posean licencias o que no estén aprobadas por el departamento de Tecnología de la Información.
3. Revisar periódicamente la vigencia de uso de las licencias que se hayan adquirido.
4. Generación de estándares de software empresarial.
5. Establecer los procedimientos para el uso de software.

6. Realizar el análisis de las necesidades y los requerimientos de negocio, con la finalidad de planificar la adquisición o desarrollo de software.
7. Registrar los derechos de autor de los sistemas de Plasticaucho Industrial, desarrollados directamente o a través de terceros (contratados), en cumplimiento con las disposiciones de la Ley de Propiedad Intelectual.

4.6.7.3 Uso/Instalación de Software

Para el uso e instalación de software se regirá a lo siguiente:

1. El departamento de Tecnología de la Información es el único autorizado, así como responsable de realizar la instalación de software y proporcionar soporte técnico del mismo en los equipos de cómputo de la empresa.
2. El software utilizado por la empresa, deberá ajustarse a las especificaciones técnicas y arquitectura tecnológica disponible en el departamento de Tecnología de la Información.
3. El software que se adquiera debe cumplir con los procesos formales de recepción, validación técnica y pruebas, previos a la aceptación del producto.

4.6.7.4 Restricciones

Se prohíbe la instalación y/o uso del software en los siguientes casos:

1. Copias ilegales de cualquier sistema informático, programa o software.
2. Software que haya sido descargado de Internet.
3. Instalaciones no autorizadas o que no hayan sido solicitadas al departamento de Tecnología de la Información.
4. Software adquirido para uso personal del usuario (sin fines empresariales).
5. Software de entretenimiento o que no tenga relación con las actividades de la empresa.
6. Software sin licencia.

4.6.7.5 Requerimientos de Software

Todo usuario que requiera la instalación de un determinado software deberá solicitarlo al departamento de Tecnología de la Información de acuerdo al procedimiento y formatos que para el efecto se establezcan.

El departamento de Tecnología de la Información determinará, de acuerdo a las características del software solicitado, si existe disponibilidad de licencias para atender

la solicitud o si se cuenta con el software adecuado para atender a los requerimientos del usuario.

En caso de ser necesaria la adquisición de nuevo software el departamento de Tecnología de la Información será el encargado de remitir al usuario las especificaciones técnicas generales y específicas de dicho software. Para la continuación del trámite respectivo, el usuario deberá tener la autorización de la adquisición, para posterior realizar la instalación con su respectiva licencia.

4.6.8 POLITICA DE DESARROLLO DE SOFTWARE

4.6.8.1 Responsables

Personal con el cargo de: Analista desarrollador, Analista de Seguridades TI.

4.6.8.2 Generales

Para el desarrollo de software se requiere:

1. Toda solicitud de desarrollo, evaluación o modificación de sistemas informáticos deberá empezar con el pedido formal al departamento de Tecnología de la Información, para su análisis y aprobación.
2. El área requirente será el responsable de contar con la siguiente documentación, previa al inicio del proceso de desarrollo:
    - Proceso oficializado y aceptado por su gerencia con apoyo del departamento de Tecnología de la Información.
    - Documentación que detalle el flujo de procesos, procedimientos y actividades.
    - Formularios relacionados con el proceso.
    - Reglas y excepciones de negocio.
    - Responsables de las áreas involucradas para el seguimiento en el proceso de desarrollo.
    - Documentación adicional que se deba tener en cuenta en el proceso de desarrollo de software.
3. Los desarrollos o modificaciones de software deben estar de acuerdo a la arquitectura de aplicaciones definida por el departamento de Tecnología de la Información, deben seguir estándares y buenas prácticas de la empresa.
4. El ciclo de desarrollo de software debe contar con un proceso de aseguramiento de la calidad (QA), que garantice que el producto sea desarrollado cumpliendo con

criterios de calidad. Para lo cual, el departamento de Tecnología de la Información deberá realizar pruebas necesarias que garanticen la seguridad, rendimiento y confiabilidad de la aplicación.

5. El área requirente deberá validar que el software cumpla con las funcionalidades y requerimientos solicitados, previo a la liberación en ambiente de producción.
6. Todo software desarrollado debe garantizar el registro de rastros de auditoría, donde se evidencien los eventos realizados por los usuarios dentro de la aplicación.

4.6.8.3 Entorno de Trabajo

El departamento de Tecnología de la Información utilizará los siguientes ambientes para el proceso de desarrollo de software:

a) Desarrollo.- Ambiente utilizado para la elaboración de software. El ambiente es administrado por el área de desarrollo.
b) Pre producción (Pruebas).- Establecido como un ambiente similar al de producción, utilizado para controlar la calidad y pruebas del sistema.
c) Producción.- Ambiente utilizado para la puesta en marcha la operación de los sistemas.

La información almacenada en el ambiente de producción no debe ser utilizada, ni visible a los ambientes de pre producción y desarrollo, con el fin de asegurar la confidencialidad de los datos.

4.6.8.4 De la implantación de un sistema en ambiente de producción

1. El área de desarrollo de software y el área de operaciones, seguirán el proceso determinado y aprobado por el departamento de Tecnología de la Información para la implantación o modificación de los sistemas que se encuentran en ambiente de producción.
2. La implantación o modificación de los sistemas desarrollados por el departamento de Tecnología de la Información debe ser validada y aprobada formalmente por el área requirente, previamente a la liberación en el ambiente de producción.

4.6.8.5 Actualizaciones de parches de seguridad en los sistemas de información

1. Vigilar el estado de actualización de todos nuestros dispositivos y aplicaciones.
2. Elegir la opción de actualizaciones automáticas siempre que esté disponible.

3. Instalar las actualizaciones de seguridad tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores, antivirus y sistemas utilizados en la empresa.
4. Ser cuidadosos con las aplicaciones que instalamos, huyendo de fuentes no confiables y vigilando los privilegios que les concedemos.
5. Evitar hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad.

4.6.9 POLITICA DE USO DE INTERNET E INTRANET

4.6.9.1 Responsables

Personal con el cargo de: Coordinador de Infraestructura, Analista de Seguridades TI.

4.6.9.2 Generales

Los servicios de Internet e Intranet son recursos que la empresa pone a disposición de las/os empleados de Plasticaucho Industrial, como una herramienta para consulta de información, investigación y acceso a los sistemas de la empresa, facilitando la realización de las labores diarias, se debe tomar en cuenta lo siguiente:

1. El uso y acceso a los servicios de Internet e Intranet está limitado a la aceptación de las presentes políticas.
2. El uso del servicio de Internet e Intranet está condicionado a la realización de actividades laborales que estén relacionadas con los propósitos y funciones propuestos por la empresa.
3. El acceso a estos servicios debe ser solicitado al departamento de Tecnología de la Información, previa autorización de la gerencia de la unidad administrativa u operativa a la que pertenezca el usuario.
4. En caso de que la solicitud sea aprobada, se realizará la configuración necesaria en el equipo del usuario y se le asignará un perfil de acceso con un nivel de navegación (acceso a sitios web) determinado, de acuerdo a las actividades que el usuario vaya a desempeñar dentro de la empresa.
5. En el caso de que un usuario requiera acceder a un sitio web restringido por el nivel de navegación otorgado, deberá solicitar al departamento de Tecnología de la Información la habilitación del sitio, adjuntando las justificaciones necesarias.
6. En el caso de que un usuario externo a la empresa, requiera el acceso al servicio de Internet, se le asignará un perfil de acceso limitado, navegación básica y a través

de una conexión de red que no ponga en riesgo la seguridad de los equipos internos de la empresa.

7. El intercambio de información entre las áreas administrativas y operativas de Plasticaucho Industrial se lo realizará a través de red local, Intranet o una conexión privada virtual.

4.6.9.3 Responsabilidades

Los servicios de enlaces de datos y de Internet e Intranet son administrados por el personal del departamento de Tecnología de la Información a través del área de Infraestructura. El proveedor del servicio enlace de datos y de Internet es responsable de garantizar la disponibilidad y el ancho de banda del enlace, conforme a los acuerdos de nivel de servicio contratados, tomando en cuenta lo siguiente:

1. Los servicios de Internet contratados por la empresa Plasticaucho Industrial a nivel nacional, su uso y su administración estarán de acuerdo a las especificaciones que disponga el departamento de Tecnología de la Información; el mismo que se encargará de resolver los problemas técnicos, errores de recepción, envío y asegurar la gestión para su atención inmediata.
2. El departamento de Tecnología de la Información es responsable de monitorear periódicamente el uso de Internet e Intranet de Plasticaucho Industrial, con el fin de vigilar el cumplimiento de las presentes políticas, que mantenga la confidencialidad de la información.
3. La información y mensajes que se envíen a través de internet, serán de absoluta responsabilidad del usuario emisor. En ningún momento los mensajes podrán atentar contra la reputación e imagen de la empresa
4. El usuario será el único responsable de los sitios web visitados desde su perfil, por lo tanto, será también responsable de mantener en reserva las credenciales de su cuenta.

4.6.9.4 Prohibiciones

Se prohíbe lo siguiente:

1. Utilizar el servicio de internet como un medio para realizar cualquier actividad comercial o lucrativa individual o la participación y distribución de actividades o materiales que vayan en contra de la empresa.

2. Utilizar el servicio de internet con propósitos que puedan influir negativamente en la imagen de Plasticaucho Industrial, de sus autoridades o empleados.
3. Realizar actividades que puedan comprometer la seguridad de los servidores y recursos informáticos de la empresa.
4. Accesos a sitios web que puedan ser declarados como obscenos, que distribuyan o promocionen material pornográfico, ofensivo o con humor inapropiado; que vaya en contra de la moral y buenas costumbres.
5. Acceso a sitios web de juegos y actividades recreativas de intereses personales tales como redes sociales, chat, concursos, mensajes no solicitados, etc.
6. Transmitir amenazas, material indecente o de hostigamiento. Así como intimidar, difamar, insultar, acosar, ofender a otras personas o interferir en las labores de otros usuarios.
7. Distribuir por internet material que ocasione daños, específicamente la distribución de software malicioso.
8. Descargar e instalar programas o archivos vía el servicio de internet. Únicamente se podrá llevar a cabo estas actividades en situaciones previamente coordinadas con el departamento de Tecnología de la Información.
9. Congestionar, interferir o paralizar el uso del servicio de internet e intranet.
10. Descargar música, fotos, videos, u otro material que no esté relacionado con las actividades o propósitos laborales.

4.6.10 POLITICA DE CRIPTOGRAFÍA

4.6.10.1 Responsables

Personal con el cargo de: Analista de Seguridades TI, Coordinador de Infraestructura.

4.6.10.2 Generales

Definir métodos criptográficos de protección de la información crítica o sensible, para reducir los riesgos de confidencialidad, disponibilidad o integridad de la información mediante la ayuda de técnicas criptográficas, para lo cual se debe tomar en cuenta lo siguiente:

1. Las normativas de desarrollo de esta política deben indicar la aplicación de criptografía en cada caso y escenario concretos:
    - Firma electrónica
    - Autenticación electrónica

- Cifrado

2. La empresa Plasticaucho Industrial, velará por la implementación y proponer una postura institucional que regule el uso de controles criptográficos para la protección de la información, sobre su uso, su protección y el ciclo de vida de las claves criptográficas.
3. El departamento de TI en conjunto con el Analista de Seguridad de la información, deben definir el mejor método de cifrado y la herramienta que se adapte a las especificaciones requeridas.
4. Las claves criptográficas deben estar disponibles operativamente tanto en tiempo como lo requiera el servicio criptográfico correspondiente.
5. Las claves pueden mantenerse en un equipamiento criptográfico mientras se utilizan, o pueden almacenarse de manera externa con las medidas de seguridad adecuadas y recuperarlas cuando sea necesario.
6. Una clave se utilizará durante un plazo concreto, o período criptográfico.
7. Para los nuevos sistemas de información o en su defecto, nuevas versiones de estos, exista una identificación de datos sensibles, y se determinará los requerimientos de resguardo y mecanismos de encriptación tanto para su almacenamiento, transporte, validación y control de acceso.
8. Para la protección de claves criptográficas, en caso de requerirse encriptación, se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar sus claves privadas, considerándolo crítico o de alto riesgo.
9. Protección y uso de firmas digitales avanzadas, los certificados digitales avanzados se deberán almacenar en equipamiento especializado del tipo HSM (Hardware Security Module).
10. El acceso físico y lógico al equipo HSM, el enrolamiento de firmas en el mismo y la definición de las entidades firmadoras y su correspondiente firma digital en el módulo firmador, se encuentra resguardado por el Coordinador de Infraestructura.
11. Para la evaluación de cumplimiento, la revisión de esta Política se efectuará anualmente por el encargado de Seguridad de la Información de TI.

4.6.10.3 Excepciones

Frente a casos especiales, el analista de Seguridad de la Información podrá establecer condiciones puntuales de excepción en el cumplimiento de las directrices de esta Política, siempre que no infrinja la legislación vigente ni afecte directrices de otras

políticas. Toda excepción debe ser documentada y se le debe efectuar seguimiento, generando un proceso de revisión de la misma, para determinar si amerita una nueva directriz particular o un cambio en otra ya existente.

4.6.11 SANCIONES

4.6.11.1 Responsables

Departamento de TI.

4.6.11.2 Incumplimiento de las Políticas

Ante el incumplimiento de las obligaciones establecidas en este instrumento, dependiendo de la gravedad de la infracción cometida, se iniciarán las respectivas acciones y procedimientos administrativos, de conformidad a las normas que las regulan, con el fin de que se determine la responsabilidad administrativa y penal, a que haya lugar, en contra de las personas imputables. La empresa Plasticaucho Industrial S.A. podrá iniciar las acciones de oficio o a petición de parte, a través de los órganos competentes.

Además de las acciones y procedimientos que se ejerzan en contra de los sujetos responsables de la violación de este instrumento, el Jefe del departamento de Tecnología de la Información, dependiendo de la gravedad del incumplimiento y luego de seguir el debido proceso de acuerdo a la normativa legal vigente (Contrato), calificará motivadamente la falta e impondrá las siguientes acciones:

1. Ante un incumplimiento leve de las Políticas, se notificará por escrito recordándole la vigencia de las Políticas al usuario responsable de la falta, así como se pondrá en conocimiento del Titular del área a la que pertenezca el usuario y al departamento de Gestión Humana para su seguimiento y control.
2. En el evento de presentarse un incumplimiento moderado en las Políticas, o una reincidencia en un incumplimiento leve, se notificará por escrito al Titular del área a la que pertenezca el usuario y al departamento de Gestión Humana, así como de considerarlo necesario se podrá disponer la suspensión temporal del servicio al usuario responsable hasta que el Titular del área apruebe por escrito la restauración del servicio.

3. En caso de presentarse un incumplimiento grave de las Políticas, causará el retiro de los equipos, bienes, servicios y herramientas informáticas, como la desvinculación total de la empresa.

4.7 Resultados de la aplicación del Plan de Gestión de Seguridad Informática

Para la evaluación de los resultados obtenidos al implementar el Plan de Gestión de Seguridad Informática basado en ISO 27001, se realizó una encuesta (véase el Anexo D) en el departamento de Tecnología de Información de la empresa Plasticaucho Industrial, la evaluación se lo realizó en base tres objetivos fundamentales de la seguridad de la información que son:

- Disponibilidad
- Integridad
- Confidencialidad

El presente proyecto de investigación hace uso del paradigma Crítico-Positivo, debido al diagnóstico y el análisis de la situación actual de la empresa descrito en el capítulo 4, sección 4.1, a partir de ello se plantea una solución alternativa para la seguridad de los activos que posee la entidad.

Población encuestada

Se toma como referencia la población detallada en el capítulo 3, tabla 1.

Número de encuestados = 5

- **Disponibilidad**

Tabla 12: Análisis de preguntas sobre Disponibilidad

Preguntas Disponibilidad	Numero encuestados	Total
9	5	45

Fuente: Elaboración propia a partir de la encuesta

- **Integridad**

Tabla 13: Análisis de preguntas sobre Integridad

Preguntas Integridad	Numero encuestados	Total
9	5	45

Fuente: Elaboración propia a partir de la encuesta

- **Confidencialidad**

Tabla 14: Análisis de preguntas sobre Confidencialidad

Preguntas Confidencialidad	Numero encuestados	Total
7	5	35

Fuente: Elaboración propia a partir de la encuesta

A continuación, se presenta las siguientes tablas en valores numéricos y porcentuales basados en la encuesta aplicada Post implementación del Plan de Gestión de Seguridad Informática.

Tabla 15: Resultados de la encuesta sobre Disponibilidad

Indicador	Pregunta	POST IMPLEMENTACION			
		Si	No	Parcial	Encuestados
Disponibilidad	P1	4	0	1	5
	P3	4	0	1	
	P7	3	1	1	
	P8	4	0	1	
	P11	4	0	1	
	P12	4	0	1	
	P13	5	0	0	
	P14	4	0	1	
	P15	4	0	1	
Total Disponibilidad		36	1	8	45
Porcentaje Disponibilidad		80,00	2,22	17,78	100%

Fuente: Elaboración propia a partir de la encuesta

Tabla 16: Resultados de la encuesta sobre Disponibilidad

Indicador	Pregunta	POST IMPLEMENTACION			
		Si	No	Parcial	Encuestados
Integridad	P4	5	0	0	5
	P5	4	1	0	
	P6	3	1	1	
	P7	3	1	1	
	P9	5	0	0	
	P11	4	0	1	
	P12	4	0	1	
	P14	4	0	1	
	P15	4	0	1	
Total Integridad		36	3	6	45
Porcentaje Integridad		80	6,67	13,33	100%

Fuente: Elaboración propia a partir de la encuesta

Tabla 17: Resultados de la encuesta sobre Disponibilidad

Indicador	Pregunta	POST IMPLEMENTACION			Encuestados
		Si	No	Parcial	
Confidencialidad	P2	5	0	0	5
	P7	3	1	1	
	P10	3	1	1	
	P12	4	0	1	

	P13	5	0	0	
	P14	4	0	1	
	P15	4	0	1	
Total Confidencialidad		28	2	5	35
Porcentaje Confidencialidad		80,00	5,71	14,29	100

Fuente: Elaboración propia a partir de la encuesta

4.7.1 Análisis de los resultados en base a la encuesta aplicada Post Implementación

4.7.1.1 Disponibilidad

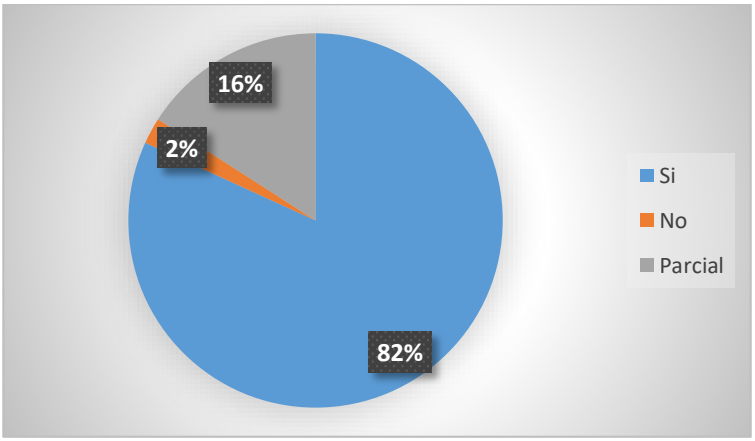

Fig. 45: Resultado post implementación sobre disponibilidad
Fuente: Elaboración propia a partir de la encuesta

Interpretación: En el figura 44 de acuerdo al indicador de disponibilidad, se puede observar que existe un alto porcentaje de incremento, en donde el 76% de los encuestados afirma que la disponibilidad de la información es satisfactoria.

4.7.1.2 Integridad

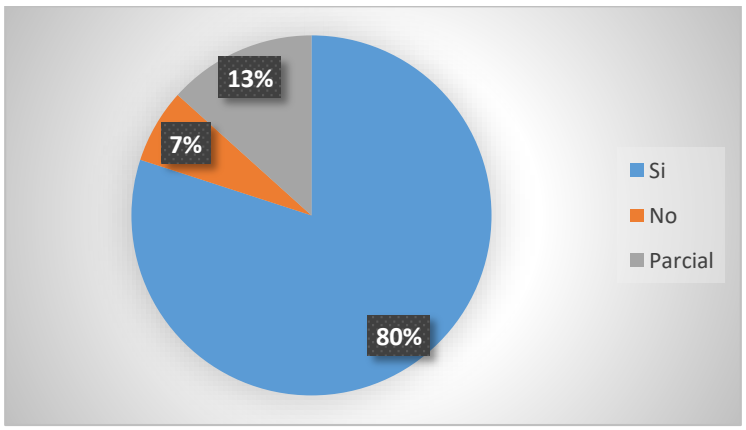

Fig. 46: Resultado post implementación sobre integridad
Fuente: Elaboración propia a partir de la encuesta

Interpretación: En el figura 45 de acuerdo al indicador de integridad, se puede observar que existe un alto porcentaje de incremento, en donde el 80% de los encuestados afirma que la integridad de la información es satisfactoria.

4.7.1.3 Confidencialidad

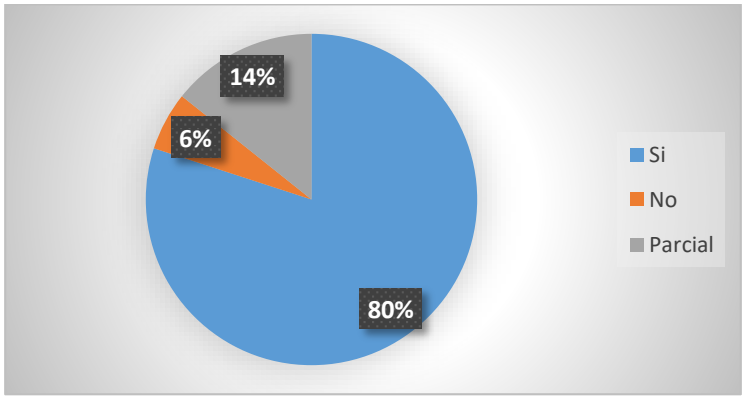

Fig. 47: Resultado post implementación sobre confidencialidad
Fuente: Elaboración propia a partir de la encuesta

Interpretación: En el figura 45 de acuerdo al indicador de confidencialidad, se puede observar que existe un alto porcentaje de incremento, en donde el 80% de los encuestados afirma que la confidencialidad de la información es satisfactoria.

Con la obtención de los resultados mediante la encuesta aplicada post implementación, se pudo verificar que el Plan de Gestión de Seguridad Informática que se basa en la norma ISO 27001, ha logrado obtener un favorable resultado de mejora para mantener la confidencialidad, integridad y disponibilidad de los datos de la empresa.

4.8 Monitorización e implementación de mejoras

Una vez ya implementado el Plan de Gestión de Seguridad Informática, la empresa debe llevar actividades de monitorización periódicamente para verificar el cumplimiento de los controles, con el fin de mantener un nivel de seguridad que garantice la integridad, confidencialidad y disponibilidad de la información. A partir de las actividades de monitoreo la empresa Plasticaucho Industrial por medio del departamento de Tecnología de la información tiene la obligación de aplicar mejoras constantemente sobre la eficacia y productividad en cuanto a los resultados obtenidos.

El plan de mejoramiento será anualmente, donde cada inicio de año se procederá con la apertura del mismo y estará distribuido con las siguientes actividades.

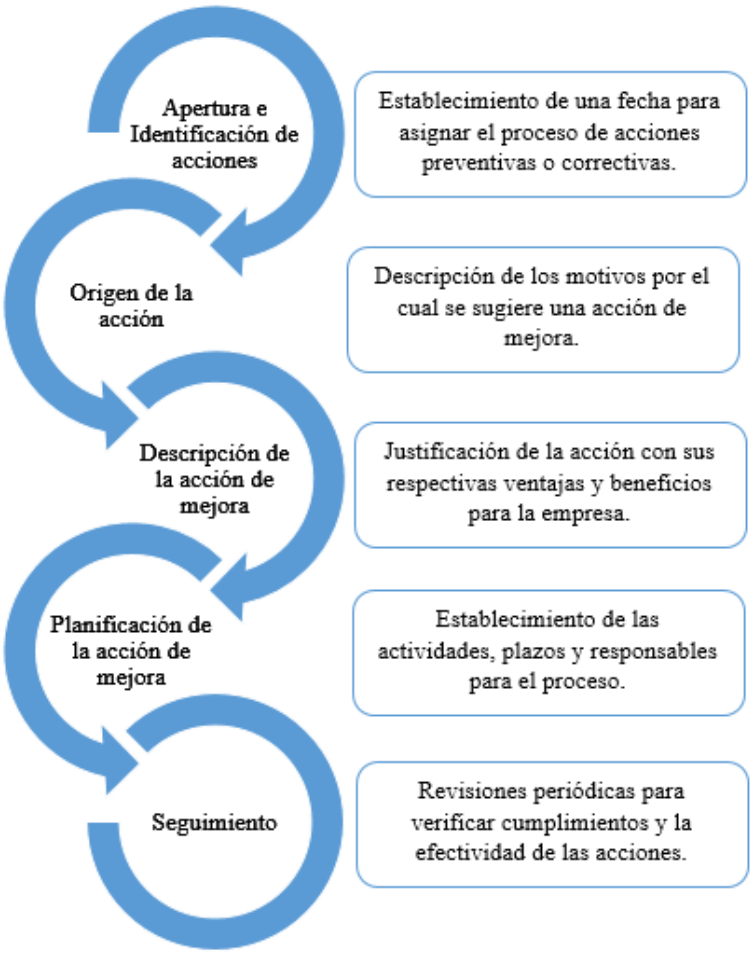

Fig. 48: Plan de Mejoramiento
Elaborado por: Jorge Tigse

Los procesos de mejoramiento deberán ser propuestos por el departamento de Tecnología de la Información de la empresa Plasticaucho Industrial y de ser el caso con la gerencia respectiva y el personal involucrado en dichos procesos de seguridad de la información para las aprobaciones respectivas.

Para dar el seguimiento se pone a disposición la gestión de indicadores (véase el anexo E) a partir de los principales controles y períodos en el cual se debe evaluar.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Al concluir el presente trabajo de investigación se concluyó lo siguiente:

- La empresa Plasticaucho Industrial S.A. actualmente cuenta con procedimientos definidos por el departamento de Tecnología de la Información para asegurar la información. Los procesos dirigidos desde esta área están establecidos en base a políticas que permiten controlar las actividades del personal, software, hardware y activos en general de información.
- La segregación de tareas dentro del departamento de Tecnología de la Información ha permitido mejorar la calidad de servicio, en el cual cada uno de los miembros del área tienen actividades designadas para el monitoreo y detección de actividades anormales, para aplicar procedimientos de solución.
- Al contar con el Directorio Activo se ha logrado identificar los usuarios, computadores, equipos tecnológicos y de comunicación que se encuentran dentro del dominio corporativo, y mediante la aplicación de directivas de grupo han permitido limitar el comportamiento de los accesos a los recursos de la red.
- Plasticaucho Industrial al tener contratado los servicios de red de proveedores externos han logrado disminuir las responsabilidades de actividades que conllevan asegurar la integridad, disponibilidad y confidencialidad de la información a nivel de conexiones WAN, y así poner más énfasis en las labores de seguridad interna de la red LAN en la empresa.

- A pesar de que el personal del departamento de Tecnología de la Información no conoce a fondo los lineamientos de la Norma ISO 27001 para la seguridad de la información, el diseño del Plan de Gestión Informática que se basa en esta norma es el paso inicial para la implementación total y posterior obtener la certificación internacional.

Recomendaciones

- Implementar el Plan de Gestión Informática el cual sea supervisado periódicamente con el fin de aplicar límites a toda actividad que esté relacionada con la seguridad de la información.
- Concientizar a todo el personal interno y de igual manera a externos que estén inmersos en la manipulación de la información dentro de las instalaciones de Plasticaucho Industrial, sobre la importancia de salvaguardar la información, con el fin de cumplir con las políticas de seguridad y contratos firmados, y no tener eventos que comprometan la continuidad de la organización.
- Plasticaucho Industrial deberá trabajar con el apoyo del departamento de Tecnología de la Información en los temas relacionados de la seguridad de la información para mantener la garantía de la misma en confidencialidad, integridad y disponibilidad.
- Seguir con los lineamientos establecidos para los proveedores externos en asegurar la continuidad del negocio y mantener la información segura, siempre monitoreando el cumplimiento de los Acuerdos de Niveles de Servicio (SLA) y actualizarlos si es necesario.
- Aprobar, y poner en funcionalidad el cumplimiento de las políticas de seguridad que se implementan en el presente proyecto de investigación.
- Realizar un monitoreo periódicamente de las políticas de seguridad y evaluar su funcionamiento, para proponer mejoras de acuerdo a las necesidades que se requieran en la empresa.

Bibliografía

[1] Diario El Pais, «Europeos estrenan hoy nuevas normas para proteger sus datos - Vida Actual - Últimas noticias de Uruguay y el Mundo actualizadas - Diario EL PAIS Uruguay,» 2018. [En línea]. Available: https://www.elpais.com.uy/vida-actual/europeos-estrenan-hoy-nuevas-normas-proteger-datos.html.

[2] Searchdatacenter en Español, 19 Febrero 2018. [En línea]. Available: https://searchdatacenter.techtarget.com/es/cronica/Gestion-de-seguridad-debe-ser-integral-y-reforzar-la-capacitacion.

[3] EL TELÉGRAFO, «CNE implementará plan de seguridad informática: Ecuadorinmediato,» 2018. [En línea]. Available: http://ecuadorinmediato.com/index.php?module=Noticias&func=news_user_view&id=2818842774&umt=el_telegrafo_guayaquil_cne_implementara_plan_seguridad_informatica.

[4] D. N. Ojeda Cruz, *PLAN DE RIESGOS Y CONTINGENCIAS INFORMÁTICAS BASADO EN UN ACUERDO DE NIVEL DE SERVICIO APLICADA A LA EMPRESA PLASTICAUCHO INDUSTRIAL*, Ambato, 2018.

[5] A. I. Rojas Buenaño, *HACKING ÉTICO PARA ANALIZAR Y EVALUAR LA SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA DE LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.,* Ambato, 2018.

[6] J. A. Seis Guaman, «Diseño de un Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Dirección de Tecnologías de la Información y Comunicaciones del Comando Conjunto de las FF.AA., Utilizando la norma ISO 27001:2013,» 2017.

[7] D. A. Quevedo Romero, «Implementación de un esquema de seguridad para la red de la Unidad Educativa Particular Cardenal Spellman Femenino,» 2017.

[8] R. C. Lema Vinlasaca y D. F. Donoso Gallo, «Implementación de un Sistema de Gestión de Seguridad de Información basado en la Norma ISO 27001:2013 para el Control Físico y Digital de documentos aplicado a la Empresa Lockers S.A.,» 2018.

[9] B. José y R. Montealegre, «Medición de madurez de CiberSeguridad en MiPymes colombianas,» 2016.

[10] J. C. G. Eras, *PLAN PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*, Loja, España, 2015.

[11] I. A. Alfaro Viana y E. Vargas León, *DISEÑO DEL PLAN DE SEGURIDAD INFORMÁTICA DEL SISTEMA DE INFORMACIÓN MISIONAL DELA PROCURADURÍA GENERAL DE LA NACIÓN*, Bogotá, 2016.

[12] ISOTools Excellence, «Blog especializado en Sistemas de Gestión, La NCh ISO 27001. Origen y evolución.,» Agosto 2017. [En línea]. Available: https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/.

[13] ISOTools, «ISO 27001: Cumplimiento de los requisitos legales en Seguridad de la Información,» 2014. [En línea]. Available: https://www.isotools.org/2014/12/16/iso-27001-cumplimiento-requisitos-legales-seguridad-informacion.

[14] L. M. Tobar, «Código Ingenios: Nuevo régimen de Propiedad Intelectual en Ecuador,» 5 diciembre 2016. [En línea]. Available: https://www.pbplaw.com/es/codigo-ingenios-nuevo-regimen-de-propiedad-intelectual-en-ecuador/.

[15] S. M. Quiroz Zambrano y D. G. Macías Valencia, Seguridad Informática, 3 ed., vol. 3, Polo de Capacitación, Investigación y Publicación (POCAIP), 2017.

[16] Departamento de Seguridad Informática, «Amenazas a la Seguridad de la Información | Departamento de Seguridad Informática,» 2016. [En línea]. Available: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12. .

[17] MINTIC, «Guía de gestión de riesgos,» 2016.

[18] G. S. Cedeño Canessa, «Plan de gestión de riesgo informático para el Gobierno Autónomo descentralizado de la Provincia de Esmeraldas,» 2017.

[19] ISO, «ISO / IEC 27001 Gestión de la seguridad de la información,» [En línea]. Available: https://www.iso.org/isoiec-27001-information-security.html.

[20] ISO, «About ISO,» [En línea]. Available: https://www.iso.org/about-us.html.

[21] DNV-GL, «¿Qué es y para qué sirve la Norma ISO 27001? | Tecnología | Apuntes empresariales | ESAN,» 2016. [En línea]. Available: https://www.esan.edu.pe/apuntes-empresariales/2016/05/que-es-y-para-que-sirve-la-norma-iso-27001/.

[22] H. Vite Cevallos, B. Molina Montero y J. Dávila Cuesta, Gestión de la Información en las Instituciones de Educación Superior (IES) con base a la norma ISO 27001, vol. 2, 2018.

[23] PLASTICAUCHO INDUSTRIAL, «PERFIL TECNOLÓGICO,» AMBATO, 2018.

[24] Microsoft, «Descripción general de los servicios de dominio de Active Directory,» 2017. [En línea]. Available: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview.

[25] SAP LATINOAMERICA, «SAP ERP,» [En línea]. Available: https://www.sap.com/latinamerica/index.html.

[26] SquareNet, «Plataforma SquareNet,» 2019. [En línea]. Available: http://www.squarenet.com.ec/plataforma.html.

[27] PaperCut, «PaperCut MF,» 2019. [En línea]. Available: https://www.papercut.com/products/mf/.

[28] SysAid, «Software de Help Desk,» 2019. [En línea]. Available: https://www.sysaid.com/es/help-desk-software.

[29] Microsoft, «Exchange Online Protection,» 2019. [En línea]. Available: https://products.office.com/es/exchange/exchange-email-security-spam-protection.

[30] Century Link, «Una red global en la que puede confiar,» 2019. [En línea]. Available: https://www.centurylink.com.ar/redes/aczq/mpls-ipvpn.html?rid=lvltmigration.

[31] Paessler AG, «Seguridad de red,» 2019. [En línea]. Available: https://www.es.paessler.com/network-security-monitoring.

[32] William Velastegui - Plasticaucho Industrial, *POLITICAS DE SEGURIDAD TI*, Ambato, 2017.

[33] ITService, «ISO 27001,» 2019. [En línea]. Available: https://itservice.com.co/iso-27001-una-breve-historia-de-la-norma/.

[34] C. De la Torre, M. De la Torre, M. De la Torre y A. De la Torre, «Normas ISO 27001 - ISO 27002,» Agosto 2017. [En línea]. Available: https://www.scprogress.com/NOTICIAS/CyberNoticia47-20170824.pdf.

[35] ISOTools, «La familia de normas ISO 27000,» 21 Enero 2015. [En línea]. Available: https://www.isotools.org/2015/01/21/familia-normas-iso-27000/.

[36] GlobalSTD, «ISO Survey 2018,» Septiembre 2019. [En línea]. Available: https://www.globalstd.com/networks/blog/iso-survey-2018.

[37] ISO 27001, «Normativa de gestion de seguridad de la informacion,» 2013.

[38] Lopez, F, «Grupo trevenque,» 2018. [En línea]. Available: https://www.trevenque.es/seguridad/sgsi/.

[39] Borragan, F, «ADAPTACIÓN DE LAS NORMAS ISO 27001 E HIPPA PARA LA,» Riobamba, 2017.

ANEXOS

Anexo A

FORMATO DE ENTREVISTA APLICADO AL PERSONAL ENCARGADO DE LAS SEGURIDADES TI

1. ¿Qué problemas de seguridad informática ha tenido la empresa Plasticaucho Industrial S.A.?

   ……
   …….

2. ¿Qué problema fue más perjudicial para la empresa y que aún no se pueda controlar en su totalidad?

   ……
   …….

3. ¿Para mejorar la calidad de seguridad de la información que ha realizado la empresa en conjunto con el departamento de TI?

   ……
   …….

4. ¿La empresa cuenta con políticas de seguridad para la proteger la información?

   ……
   …….

5. ¿Cómo es administrada la red interna de Plasticaucho?

   ……
   …….

6. ¿Cómo se encuentra la seguridad física para acceso a los servidores en la empresa?

   ……
   …….

Anexo B

FORMATO DE ENTREVISTA APLICADO AL PERSONAL ENCARGADO DE HARDWARE Y SOFTWARE

1. ¿Cómo es la administración de software y equipos informáticos para el personal de Plasticaucho?

   ……
   …….

2. ¿Todo el software utilizado en la empresa posee licencia?

   ……
   …….

3. ¿Cuál es el procedimiento de un usuario final para realizar un requerimiento con el departamento de TI?

   ……
   …….

4. ¿Cómo se maneja el acceso a la información de los servidores de archivos (NAS) de Plasticaucho?

   ……
   …….

5. ¿La empresa cuenta con herramientas para realizar respaldo de información de cada empleado?

   ……
   …….

Anexo C

FORMATO DE ENCUESTA APLICADO AL PERSONAL DEL DEPARTAMENTO DE TECNOLOGIA DE LA INFORMACIÓN (PRE IMPLEMENTACIÓN)

Nombre: …….

Cargo: ……

Según las preguntas planteadas a continuación, seleccione la opción que usted considere apropiada en base a sus conocimientos, de acuerdo a la escala siguiente:

Excelente (5), Bueno (4), Regular (3), Muy Deficiente (2), No Tiene Conocimientos (1)

Conocimiento de Seguridad de la Información

Objetivo: Determinar el nivel de conocimiento que dispone el personal con respecto a las normas de seguridad de la información.

1. Actual conocimiento que posee con respecto a la seguridad de la información

   5( ) 4( ) 3( ) 2( ) 1( )

2. ¿Qué conocimientos dispone con respecto a las normas que establece la seguridad de información?

   5( ) 4( ) 3( ) 2( ) 1( )

3. ¿Qué nivel de conocimientos ha adquirido a través de las capacitaciones realizadas en seguridad de la información por parte de la empresa?

   5( ) 4( ) 3( ) 2( ) 1( )

Conocimiento de la normatividad

Objetivo: Establecer el nivel de conocimiento sobre la Norma ISO 27001 y ley de protección de datos.

4. ¿Cuál es su conocimiento actual sobre la Norma ISO 27001?

   5( ) 4( ) 3( ) 2( ) 1( )

5. ¿Qué conocimiento dispone sobre la ley de protección de datos?

   5( ) 4( ) 3( ) 2( ) 1( )

6. En qué estado se encuentra la empresa de acuerdo a las Auditorías internas sobre la seguridad de la información

   5( ) 4( ) 3( ) 2( ) 1( )

Técnicas para la protección de datos y seguridad de la información

Objetivo: Conocer el estado actual sobre la seguridad de la información, a través de los servicios que brindan el personal interno y externo para la empresa.

7. El medio donde se guardan los archivos backup (servidores) ¿En qué estado de seguridad se encuentran?

   5( ) 4( ) 3( ) 2( ) 1( )

8. Los servicios prestados por proveedores externos en ¿qué estado de confiabilidad se encuentran?

   5( ) 4( ) 3( ) 2( ) 1( )

9. Los servicios prestados por proveedores externos en caso de tener un fallo ¿Cómo define su accionar en tiempo de respuesta para resolver dichos problemas?

   5( ) 4( ) 3( ) 2( ) 1( )

10. Ante un fallo en uno de los servidores de la empresa y si se dispone de un servidor alterno ¿En qué estado se encuentra?

    5( ) 4( ) 3( ) 2( ) 1( )

Acceso al área de servidores o Data Center

Objetivo: Conocer el nivel de seguridad física de acceso al área de servidores que disponga la empresa.

11. El sistema de control (registro, bitácoras, cámaras, etc.) para el ingreso a esta área está definida como.

    5( ) 4( ) 3( ) 2( ) 1( )

12. El área de servidores de acuerdo a las normativas de seguridad de la información para el diseño y ubicación ¿En qué estado se encuentra?

    5( ) 4( ) 3( ) 2( ) 1( )

13. Ante una emergencia donde se encuentre en riesgo la información y es necesario contar con un plan de contingencia ¿En qué nivel lo define?

    5( ) 4( ) 3( ) 2( ) 1( )

Protección de datos y seguridad de la información

Objetivo: Definir el nivel de control que disponga el departamento de TI para los servicios que utiliza el personal de la empresa.

14. ¿Cómo define el control de correos electrónicos?

    5( ) 4( ) 3( ) 2( ) 1( )

15. ¿Cómo se define el control de antivirus en los equipos de cómputo de la empresa?

5( ) 4( ) 3( ) 2( ) 1( )

16. La seguridad que tienen los sistemas desarrollados por el personal dentro de la empresa ¿Qué confiabilidad brindan para el manejo de datos?

    5( ) 4( ) 3( ) 2( ) 1( )

17. La seguridad que tienen los sistemas contratados por la empresa ¿Qué confiabilidad brindan para el manejo de datos?

    5( ) 4( ) 3( ) 2( ) 1( )

18. Cómo definen el acceso y restricción a la red para los usuarios, sea a páginas de navegación como acceso a carpetas compartidas dentro de la red de Plasticaucho.

    5( ) 4( ) 3( ) 2( ) 1( )

19. El software utilizado dentro de la empresa definidos con licenciamiento pagado ¿Qué seguridad la evalúa?

    5( ) 4( ) 3( ) 2( ) 1( )

20. El software utilizado dentro de la empresa definidos con licenciamiento libre ¿Qué seguridad la evalúa?

    5( ) 4( ) 3( ) 2( ) 1( )

Estrategia para la protección de información

Objetivo: Establecer el nivel de protección que disponen para el uso de los sistemas cotidianos en la empresa.

21. Cómo define los parámetros para creación de contraseñas que son utilizadas para ingreso a sistemas de trabajo en la empresa

    5( ) 4( ) 3( ) 2( ) 1( )

22. El nivel de seguridad para ingreso a los sistemas propios o contratados por la empresa cumple con los parámetros de seguridad

    5( ) 4( ) 3( ) 2( ) 1( )

Anexo D

FORMATO DE ENCUESTA APLICADO AL PERSONAL DEL DEPARTAMENTO DE TECNOLOGIA DE LA INFORMACIÓN (POST IMPLEMENTACIÓN)

Nombre: …….

Cargo: ……

Objetivo

Determinar la preservación de la seguridad de la información en la empresa Plasticaucho Industrial S.A., y que permitan el incremento de la seguridad con ayuda de la implementación del Plan de Gestión de Seguridad Informática.

Seleccione con una (X) la opción que usted mejor considere:

Preguntas

1. ¿Actualmente, los procesos tienen una documentación formal detallada y disponible en cualquier ámbito?

   SI ( ) NO ( ) PARCIAL ( )

2. ¿Existe información que se filtra hacia fuera del departamento?

   SI ( ) NO ( ) PARCIAL ( )

3. ¿Para los usuarios en los sistemas autorizados, se encuentra disponible toda información necesaria?

   SI ( ) NO ( ) PARCIAL ( )

4. ¿Existen seguridades de ingreso a los sistemas, que manejan los usuarios?

   SI ( ) NO ( ) PARCIAL ( )

5. ¿Se tiene planificado el monitoreo periódico de la información almacenada en los sistemas?

   SI ( ) NO ( ) PARCIAL ( )

6. ¿Se garantiza el uso adecuado de los dispositivos móviles?

   SI ( ) NO ( ) PARCIAL ( )

7. ¿Existen políticas que den respuesta a los incidentes que se presenten?

   SI ( ) NO ( ) PARCIAL ( )

8. ¿Existe una persona responsable de realizar backups de la información?

   SI ( ) NO ( ) PARCIAL ( )

9. ¿El usuario que necesita instalar un software en su ordenador, presenta autorización por parte de una autoridad?

   SI ( ) NO ( ) PARCIAL ( )

10. ¿Existen mecanismos de control para la relación con personal externo que le proveen bienes o servicios?

    SI ( ) NO ( ) PARCIAL ( )

11. ¿Los activos fijos se manejan bajo directrices de bloqueo, protección, seguridad, entre otros?

    SI ( ) NO ( ) PARCIAL ( )

12. ¿Existen controles ante amenazas que pueden ocasionar interrupciones de los procesos o actividades que afecten el servicio de la empresa?

    SI ( ) NO ( ) PARCIAL ( )

13. ¿Existe controles sobre el código malicioso para los equipos de cómputo?

    SI ( ) NO ( ) PARCIAL ( )

14. ¿Se aplican actualmente políticas de seguridad para gestionar la información?

    SI ( ) NO ( ) PARCIAL ( )

15. ¿Se tiene conocimiento si el departamento de TI posee una política de seguridad de la información?

    SI ( ) NO ( ) PARCIAL ( )

Anexo E

GESTIÓN DE INDICADORES

Tabla 18: Gestión de Indicadores

ID	CONTROL	INDICADOR	OBJETIVO /DESCRIPCIÓN	TOLERANCIA	FRECUENCIA	RESPONSABLE
1	1.1.2	Política de Seguridad	Verificar la revisión por parte del departamento	Mínimo 1 vez por año.	Anual	• Analista de Seguridades TI
2	2.1.1 2.1.2 2.1.5	Organización Interna	Verificar que se apliquen los controles adecuadamente.	No debe superar 1 (>1). Es el número de NO conformidades que sean detectadas en las auditorias.	Depende del plan de auditorías.	• Analista de Seguridades TI • Coordinador de Infraestructura
3	2.1.3	Contacto con las autoridades.	Mantenerse informado con las autoridades pertinentes, cambios normativos o legislativos referente a seguros.	Número de contactos anuales y de ser por lo menos una vez al año.	Anual	• Analista de Seguridades TI • Coordinador de Infraestructura
4	2.1.4	Contacto con grupos de interés especial.	Mantenerse actualizado ante nuevas amenazas o riesgos.	Mínimo un contacto al año.	Anual.	• Analista de Seguridades TI • Coordinador de Infraestructura
5	2.2.1	Dispositivos móviles	Controlar el número de dispositivos y aceptaciones de las políticas.	Número de conexiones móviles seguras a los sistemas.	Anual	• Analista de Seguridades TI • Coordinador de Infraestructura
6	3.2.2	Capacitación en seguridad de la información	Asegurar que existan capacitaciones constantes en temas de seguridad.	>1 Número de capacitaciones por año.	Anual	• Analista de Seguridades TI • Coordinador de Infraestructura
7	3.2.3 3.3.1	RRHH	Comprobar la existencia de estos procedimientos en el área de RRHH.	Deben existir obligatoriamente.	Anual	• Analista de Seguridades TI • Gestión Humana
8	4.1.3	Uso de activos	Número de incidencias en equipos o periféricos por mal uso.	<3 Número de incidencias.	Anual	• Analista de Seguridades TI • Gestor de Hardware y Software
9	4.3.1	Devolución de equipos	Número de equipos, susceptibles con información sensible, pendientes de ser borrados correctamente.	Debe ser 0. Se debe controlar efectivamente que ningún equipo este expuesto su información.	Anual	• Analista de Seguridades TI • Gestor de Hardware y Software
10	5.2.3	Privilegios de acceso	Control de la restricción de número de usuarios que dispongan de permisos de administrador.	Se puede obtener consultando en el AD.	Diario	• Analista de Seguridades TI • Coordinador de Infraestructura
11	5.4.1	Restricción de acceso	Número de accesos denegados a recursos compartidos, aplicaciones o login en SO.	<5 Calculado mediante los logs del servidor y aplicaciones.	Mensual	• Analista de Seguridades TI • Coordinador de Infraestructura

12	7.1.4	Amenazas externas y ambientales	Revisión de la existencia de extintores para equipos informáticos.	Debe existir una revisión anual obligatoria registrada y documentada.	Anual	• Analista de Seguridades TI • Coordinador de Infraestructura • Seguridad Física
13	7.2.2	Suministros	Asegurar la continuidad del negocio. Este indicador debe encontrar equipos sin protección UPS.	<3 Número de equipos sensibles sin protección.	Mensual	• Analista de Seguridades TI • Coordinador de Infraestructura • Área de servicios generales
14	8.1.3	Capacidad	Asegurar que los servidores tienen espacio libre tanto para el SO como para los datos.	>30% libre en la partición de SO. >25% libre en la partición de datos.	Mensual.	• Analista de Seguridades TI • Coordinador de Infraestructura
15	8.2.1	Código malicioso	Número de equipos en peligro (tanto de equipos por no tener antivirus como por tenerlo desactualizado)	No se permite ninguno. La información se obtiene del inventario de software por equipo y consola del antivirus.	Mensual.	• Analista de Seguridades TI • Coordinador de Infraestructura
16	8.3.1	Copias de seguridad	Número de días desde el último backup total correcto.	<3 días Se obtiene del registro del propio programa de backup.	Diario.	• Analista de Seguridades TI • Coordinador de Infraestructura
17	8.6.1	Vulnerabilidades técnicas	Numero de actualizaciones que se encuentren pendientes en los sistemas.	<5 Se obtiene de los eventos en sistemas operativos y de las aplicaciones.	Mensual.	• Analista de Seguridades TI • Coordinador de Infraestructura • Agente de Soporte Técnico
18	12.1.3	Puntos débiles de seguridad	Numero de debilidades detectadas	<3 Se obtiene en base a los registros de usuarios, personal externo y auditorías internas.	Mensual.	• Analista de Seguridades TI • Coordinador de Infraestructura
19	12.1.5	Respuestas a incidentes	Número de incidencias de seguridad pendientes de ser resueltas.	<3 Estas incidencias nunca pueden perdurar en el tiempo por más de 3 meses.	Mensual.	• Analista de Seguridades TI • Coordinador de Infraestructura • Agente de Soporte Técnico
20	13.1.2	Continuidad de la seguridad	Indica la operatividad de los equipos que conforman el plan de contingencia.	1 (SI) o 0 (NO) Se procedería a comprobar que el servidor alterno esté operativo y listo realizando chequeos automáticos en él.	Diario.	• Analista de Seguridades TI • Coordinador de Infraestructura
21	13.2.1	Redundancia	Indica la disponibilidad de los elementos redundantes (RAID, fuentes, red,..)	1(SI) o 0 (NO) Análisis de eventos en el SO.	Diario.	• Analista de Seguridades TI • Coordinador de Infraestructura
22	14.1.1	Legislación aplicable	Control de revisión de requerimientos legales y contractuales.	1 por año. Se debe albergar estas revisiones.	Anual.	• Analista de Seguridades TI • Coordinador de

						Infraestructura
23	14.1.2	Derechos de Propiedad Intelectual	Control que indica el número de licencias ilegales en producción.	0. Se obtiene del inventario.	Anual	• Analista de Seguridades TI • Coordinador de Infraestructura • Gestor de Hardware y Software
24	14.2.1	Auditorias de seguridad de la información	Indicador del número de auditorías realizadas.	>=1 al año Se obtiene la información del registro documental.	Anual.	• Analista de Seguridades TI

Fuente: Elaboración propia

Anexo F

ESTADÍSTICA DE CERTIFICACIONES ISO 27001 EMITIDOS EN EL 2018

Fig. 49: Estadística de Certificaciones ISO en 2018
Fuente: [36]