UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACION

TEMA: "Modelo de gestión de la seguridad de la información para pequeñas empresas"

Trabajo de investigación, previo a la obtención del grado académico de Magister gerencia de sistemas de información

AUTOR: Ing. David Israel Chicaiza Cazar**.**

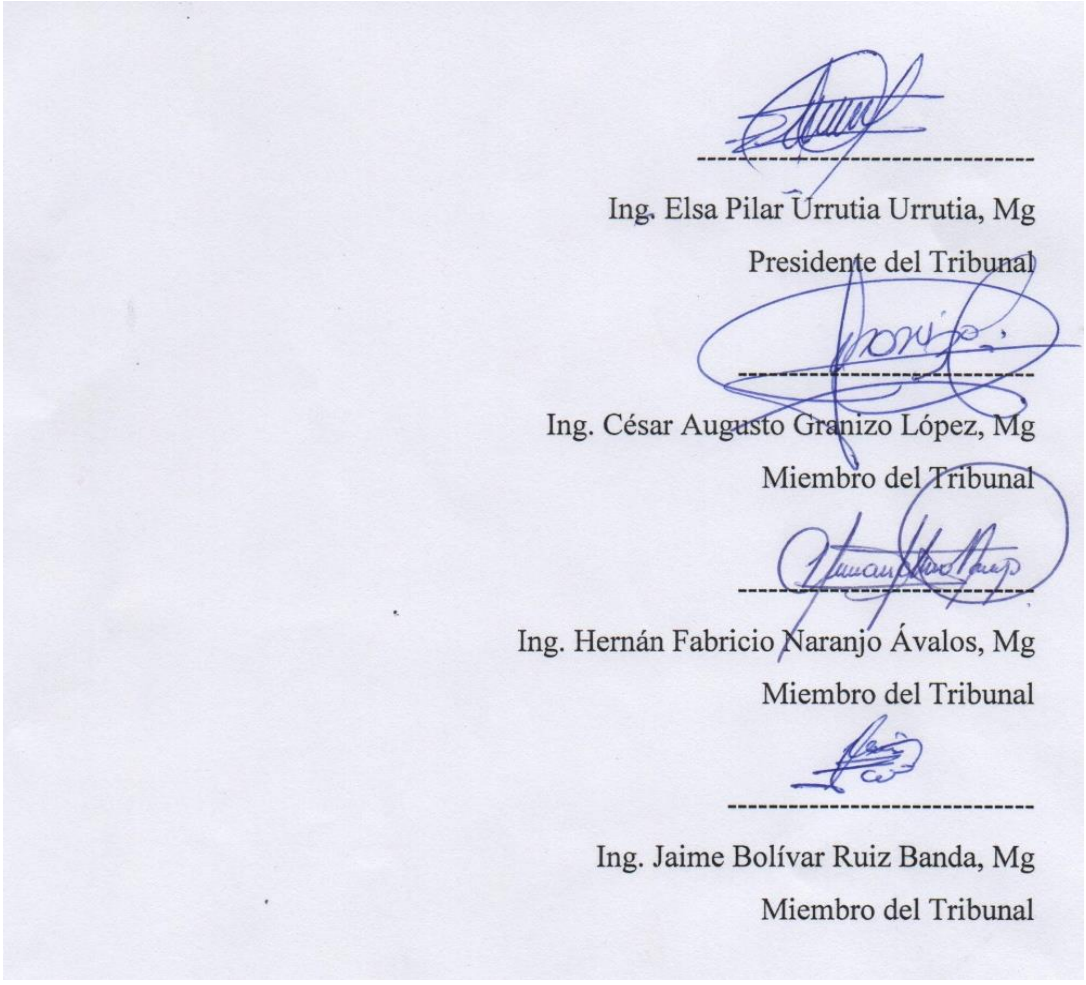
DIRECTOR: Ing. Félix Oscar Fernández Peña. Dr.

Ambato – Ecuador

2019

A la Unidad Académica de Titulación de la Facultad de la facultad de ingeniería en sistemas electrónica e industrial.

El Tribunal receptor del Trabajo de Investigación presidido por Ingeniera Elsa Pilar Urrutia Urrutia Magister, e integrado por los señores: Ingeniero César Augusto Granizo López Magister, Ingeniero Hernán Fabricio Naranjo Ávalos Magister, Ingeniero Jaime Bolívar Ruiz Banda Magister, designados por la unidad académica de titulación de posgrado de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "***Modelo de gestión de la seguridad de la información para pequeñas empresas***", elaborado y presentado por el(la) señor(a) Ingeniero David Israel Chicaiza Cazar para optar por el Grado Académico de Magister en Gerencia de Sistemas de Información; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.



Ing. Elsa Pilar Urrutia Urrutia, Mg

Presidente del Tribunal

Ing. César Augusto Granizo López, Mg

Miembro del Tribunal

Ing. Hernán Fabricio Naranjo Ávalos, Mg

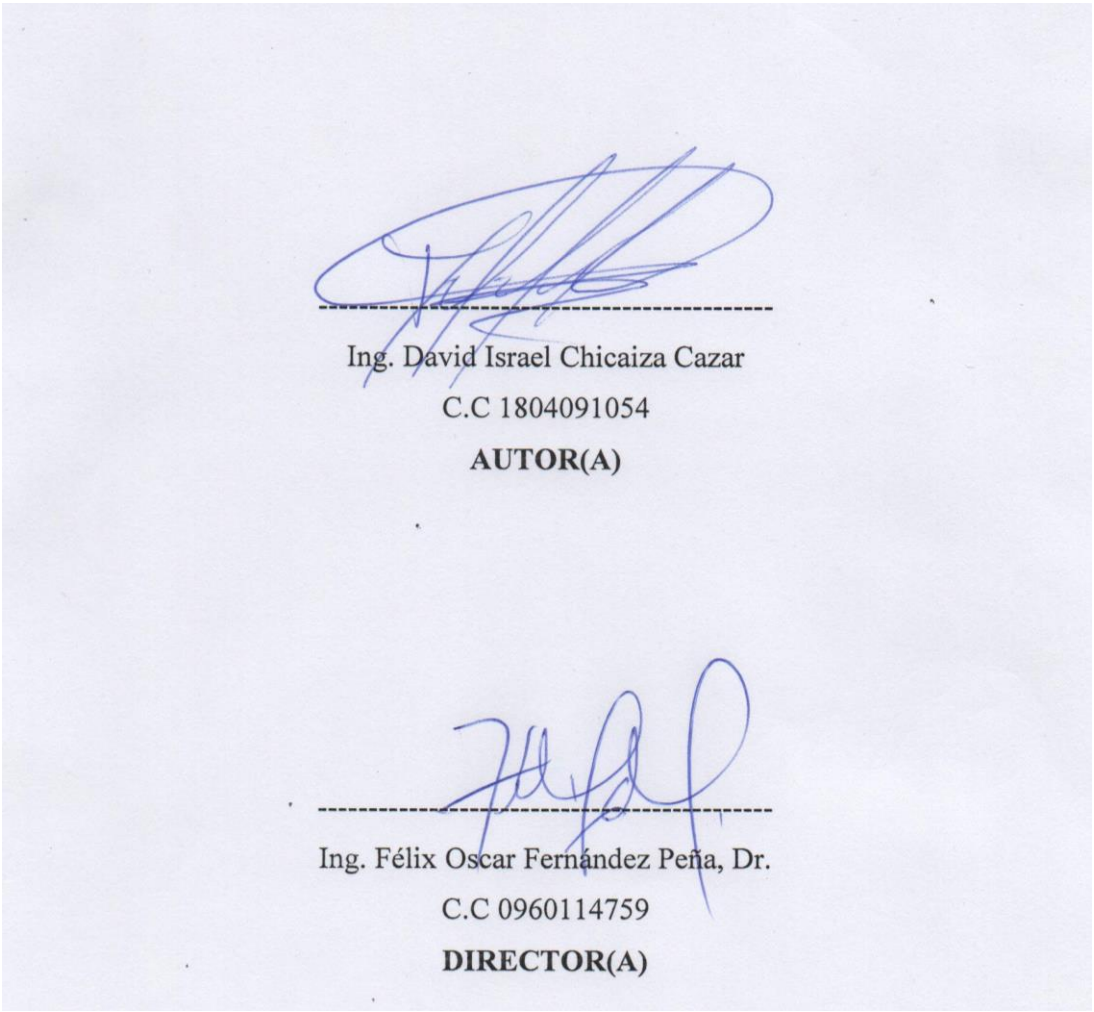
Miembro del Tribunal

Ing. Jaime Bolívar Ruiz Banda, Mg

Miembro del Tribunal

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: Modelo de gestión de seguridad de la información para pequeñas empresas, le corresponde exclusivamente a: Ing. David Israel Chicaiza Cazar, Autor(a) bajo la Dirección de Dr. Félix Oscar Fernández Peña, Director(a) del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.



Ing. David Israel Chicaiza Cazar

C.C 1804091054

AUTOR(A)

Ing. Félix Oscar Fernández Peña, Dr.

C.C 0960114759

DIRECTOR(A)

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ing. David Israel Chicaiza Cazar

C.C 1804091054

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

AGRADECIMIENTO

Agradecemos a Dios por las bendiciones de la vida, por guiarme a lo largo de mi existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

A mis padres, por ser los principales promotores de mis sueños, por confiar y creer en mis expectativas, por los consejos, valores y principios que me han inculcado.

En especial al Dr. Félix Fernández quien me ha guiado con su paciencia, y su rectitud como docente. También un eterno agradecimiento a Pasteurizadora el Ranchito. Por abrirme sus puertas y su confianza.

David Chicaiza

DEDICATORIA

El presente trabajo está dedicado a mis padres Luis y Sandra quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre.

A mí querida hermana Evelyn por su cariño y apoyo incondicional, durante todo este proceso y todos los días de mi vida, por estar conmigo en todo momento gracias.

A mi amada esposa Geovanna, por su apoyo y ánimo que me brinda día con día para alcanzar nuevas metas, tanto profesionales como personales.

Finalmente deseo acotar mi gratitud eterna a mi Dios quien con sus bendiciones me ha dado fuerzas y me ha protegido de todo mal para que este sueño sea hoy una realidad.

David Chicaiza

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMA DE INFORMACIÓN

TEMA

"MODELO DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA PEQUEÑAS EMPRESAS"

AUTOR: Ing. David Israel Chicaiza Cazar

DIRECTOR: Ing. Félix Oscar Fernández Peña, Dr.

FECHA: 26 de Noviembre del 2018

RESUMEN EJECUTIVO

El uso de las tecnologías de la información en todos los aspectos de la cotidianidad, ha conducido a que la seguridad informática no sea sólo una preocupación de las grandes compañías, sino también de las pequeñas empresas, las cuales inconscientemente en gran parte quedan vulnerables ante la falta de controles que les permitan estar protegidas de acceso no deseado. El modelo que aquí se propone basa una metodología de implementación en la norma ISO 27001 para que sea aplicable en las pequeñas empresas del Ecuador. Este modelo busca facilitar las tareas que en este tipo de empresas se dificultan, debido a los recursos limitados con los que cuenta en presupuesto, personal y conocimiento; marcando lineamientos que sirvan como guía para las organizaciones que no cuenten con una maduración de seguridad, bien sea por su estructura reducida y escases de recursos económicos o humanos.

Descriptores: Tecnologías, información, seguridad, informática, metodología, modelo de gestión, norma ISO 27001, pequeñas empresas, tareas, recursos.

UNIVERSIDAD TECNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
MAESTRÍA EN GERENCIA DE SISTEMA DE INFORMACIÓN

THEME:
"MODELO DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA PEQUEÑAS EMPRESAS"

AUTHOR: Ing. David Israel Chicaiza Cazar
DIRECTED BY: Ing. Félix Oscar Fernández Peña, Dr.
DATE: 26 de Noviembre de 2018

EXECUTIVE SUMMARY

The use of information technology in all aspects of everyday life has led to the purpose of computer security; it is not only a concern of large companies, but also of small businesses, which unconsciously are largely vulnerable to lack of controls that allow them to be protected from unwanted access. The model proposed is based in a methodological implementation in ISO 27001 standards in order to be applied in small companies in Ecuador. This model seeks to facilitate the tasks of this type of companies, which show difficulty during their process due to the limited resources of budget, stuff and knowledge. Setting guidelines that serve as lead for many organizations that do not have sophisticated security access because of their reduced structure and lack of economical or human resources .

.

Descriptors: Technogy, information technology, security, computing, methodology, management model, ISO 27001 standards, small companies, tasks, resources.

INTRODUCCIÓN

En la actualidad el desarrollo de la gestión administrativa ha recobrado impulso, ya que las pequeñas empresas se encuentran en búsqueda de calidad y excelencia en sus procesos administrativos, con la finalidad de desarrollarse y evolucionar para lograr así la eficiencia en cada uno de sus procesos.

La información en cualquier organización constituye actualmente en un recurso clave. La tecnología juega un rol clave en la creación, uso, retención, divulgación, y destrucción dela información que se genera. Es por ello que la tecnología es ahora parte integral de todos los aspectos de la organización.

Las empresas se esfuerzan para lograr que la tecnología brinde un soporte para apoyar las decisiones y lograr metas estratégicas, minimizando el riesgo que se pueda generar con ella; para ello se requiere contar con políticas de seguridad que permitan regular el adecuado manejo de los BackUp de Base de Datos, información contable, datos gerenciales, respaldos de correos electrónicos e información de cada uno de los usuarios.

Es un requisito fundamental para las instituciones lograr una buena coordinación en el área de tecnología y alinearla con la estrategia institucional a través del gobierno de TI y del afinamiento de procesos que impidan que la información se encuentre vulnerable debido a la falta de políticas que regulen las buenas prácticas relacionada con el manejo de la información, para esto es indispensable realizar un análisis de riesgos de seguridad , lo cual permitirá minimizar la posibilidad de ser víctima de delitos informáticos que impidan el normal funcionamiento de la Empresa.

El CAPÍTULO I, EL PROBLEMA contiene: el tema de investigación, el planteamiento del problema, su contexto, análisis crítico, prognosis, formulación del problema, interrogantes, delimitación, justificación y objetivos.

El CAPÍTULO II MARCO TEÓRICO contiene: antecedentes de la investigación, fundamentación filosófica, fundamentación legal, categorías fundamentales, hipótesis y señalamiento de variables.

El CAPÍTULO III METODOLOGÍA contiene: el enfoque de investigación, modalidad básica de la investigación, nivel o tipo de investigación, población y muestra, operacionalización de variables, plan de recolección de información y plan de procesamiento de la información.

El CAPÍTULO IV MARCO ADMINISTRATIVO contiene: Los recursos requeridos, cronograma, bibliografía y los respectivos Anexos.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema de Investigación

Modelo de gestión orientado a la seguridad de la información para pequeñas empresas.

1.2 Planteamiento del Problema

1.2.1 Contextualización

La información es clave para el crecimiento y éxito de una organización, para ello las pequeñas empresas deben poner mayor atención al aseguramiento de su información asignando los recursos necesarios para implementar políticas de seguridad que permitan estar preparados frente a eventuales ciber ataques.

Según la revista ED economía digital (Capital, 2015) los ciberataques han aumentado un 130% en el 2016 siendo las pequeñas empresas los objetivos más vulnerables. Según este medio las cifras son preocupantes y es posible que en realidad se escondan números grandes, ya que no todos los ataques que sufren las empresas se denuncian debido a que un ciberataque puede poner en riesgo su marca.

En el Ecuador particularmente el tema no es nuevo, ya que según diario el comercio (Bravo, 2015) indica que "Ecuador se muestra vulnerable a ciberataques", el mismo indica que en el país se descubrió que hay vulnerabilidades en los sitios web oficiales de empresas privadas ; por tal motivo el gobierno conjuntamente con las empresas privadas, deberían tomar parte en el asunto aplicando medidas de prevención para evitar en algo este tipo de ataques, permitiendo así proteger los activos de información de las organizaciones.

Este es el caso de las Pequeñas empresas en el Ecuador, ya que por sus limitaciones no se encuentran en capacidad de implementar políticas de seguridad así como medidas de prevención que les permitan resguardar sus activos de información, razón por la cual es prudente que este tipo de empresas apliquen medidas de seguridad que permitan mantener su información resguardada ante posibles ataques se seguridad.

Según el Instituto nacional de estadísticas y censos (INEC) (Ecuadorencifras, 2018), existen registradas 63814 pequeñas empresas en Ecuador, debido a que el universo es demasiado grande para el estudio, el estudio se centrara en realizar un análisis de riesgos de seguridad en Pasteurizadora El Ranchito ya que esta institución se encuentra en el rango de clasificación que señala el INEC como pequeña empresa en la cual se validarán los resultados a obtener.

1.2.2 Análisis Crítico

A continuación se realizará un análisis crítico al problema planteado, partiendo de las causas que promueven el desarrollo del presente tema de investigación.

La complejidad de los nuevos sistemas informáticos así como los datos que en ellos se maneja sumada al desconocimiento de los mecanismos tecnológicos que permiten resguardar la información y de las tendencias tecnologías para protegerse, contra amenazas y ataques tanto internos como externos, ha llevado a la necesidad de mejorar el área de seguridad en las pequeñas empresas, para así mantener su información resguardada.

Debido a que el aumento de amenazas en contra de la información que circula en los sistemas de información de las pequeñas empresas se multiplica, la utilización de un modelo para realizar la gestión de seguridad de la información, facilitará un cambio socio-cultural con responsabilidad y eficiencia en las pequeñas empresas.

Existen estándares de seguridad informática implementadas por grandes empresas pero que dificulta su implementación en pequeñas empresas, es por esto que se ha visto necesario generar un modelo de gestión que sea aplicable a pequeñas y medianas empresas.

1.2.3 Prognosis

El no implementar un modelo de gestión para la seguridad de los activos de información contribuirá que las pequeñas empresas corran el riesgo de sufrir ataques tanto internos como externos con el riesgo eventual de perder información, esto traducido a pérdidas económicas.

1.2.4 Formulación del Problema

¿Un Modelo de Gestión de Seguridad de la Información concebido para pequeñas empresas garantizará la seguridad de los activos de información?

1.2.5 Interrogantes (Subproblemas)

- ¿Cuáles son las vulnerabilidades web más comunes para pequeñas empresas en Ecuador?
- Simplificación de la ISO 27001 para pequeñas empresas.
- ¿Cómo medir el nivel de seguridad de la información en una auditoria a pequeñas empresas en Ecuador?

1.2.6 Delimitación del objeto de investigación

Campo: Pequeña Empresa
Área: Seguridad de la información
Aspecto: Factibilidad de uso del modelo de gestión.

1.3 Justificación

En mayor parte las pequeñas empresas tienen infraestructura tecnológica en crecimiento, de la cual dependen muchos de sus procesos productivos y administrativos. Gran parte de la información (sistemas de información, buzones de correo, doc, pdf, etc) que generan no se encuentran resguardados de manera adecuada; evidenciando una carencia de políticas de control que puedan proveer un adecuado tratamiento de la información.

En la empresa del caso de estudio la Coordinación de sistemas realiza algunas funciones de seguridad, lo cual va en contravía con las mejores prácticas definidas en modelos y estándares de seguridad (ISO 27001:2005, 2005). Por tanto, se considera prudente implementar estándares de seguridad de la información que se ajusten al tamaño y funcionamiento de este tipo de instituciones para garantizar que la información sea accesible por aquellas personas que estén debidamente autorizadas.

Factibilidad Técnica:

Es factible técnicamente ya que se cuenta con los recursos tecnológicos requeridos, haciendo referencia a la infraestructura, herramientas tecnológicas o software, acceso a datos e información requerida.

- **Factibilidad Operativa:**

  El presente proyecto es factible operativamente porque cuenta con el apoyo de quienes están al frente de la institución, así como de la gerencia financiera y jefatura de sistemas, lo cual permitirá tener la apertura necesaria para reunir la información necesaria y asegurar que los resultados del presente proyecto por su beneficio y utilidad sean aplicados.

- **Factibilidad Económica:**

  Podemos mencionar que económicamente el presente proyecto es factible ya que los costos que implican el análisis, estudio, tiempo empleado en estos temas son asumidos por el investigador, mientras que los tiempos del personal de la institución involucrados son asumidos por Pequeñas empresas.

1.4 Objetivos

1.4.1 Objetivo General

Diseñar un modelo de Gestión de Seguridad de la Información para pequeñas empresas.

1.4.2 Objetivos Específicos:

- Caracterizar el problema de la gestión de seguridad de la información en pequeñas empresas del Ecuador.
- Definir un modelo de gestión de seguridad de la información para pequeñas empresas del Ecuador.
- Validar el modelo propuesto en el ámbito del caso de estudio seleccionado.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes de Investigativos

Un modelo de gestión de seguridad de la información aplicable a pequeñas empresas de la manera en la que se quiere desarrollar, constituye un proyecto prometedor, pero hay que recalcar que luego de realizar una exhaustiva investigación en los portales de las Universidades de Ambato, en la biblioteca de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato sobre proyectos o temas de investigación relacionados al presente trabajo de investigación, se ha encontrado que:

Realizando una investigación de campo se logró constatar que en el repositorio de la Universidad Central del Ecuador se encontró que en la Facultad de Ingeniería, ciencias Físicas y Matemáticas existe un trabajo relacionado pero desde un enfoque diferente al planteado, el cual citamos a continuación:

Según Francisco Xavier Freire Zapata (Zapata, 2014) para su tesis de maestría con el tema "IMPLEMENTACIÓN DEL MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN APLICANDO ISO 27000 EN LA EMPRESA COKA TOURS, AMBATO – ECUADOR" En el año 2014 en la que trata sobre la importancia de aplicar normas ISO al proceso de gestión de seguridad de la información como un modelo a seguir lo que permitirá mantener una serie de políticas que regulen las buenas prácticas para el manejo adecuado de la información. En dicha investigación entre sus principales conclusiones indica que:

- Con el Modelo de Gestión de la Seguridad de la Información implementado por la empresa Coka Tours, el personal que labora en dicha institución podrán acceder a la información con la respectiva autorización; lo que permite considerar a la información como un activo más, minimizando el riesgo de fuga y/o pérdida de información.
- Al no implementar un modelo de gestión de seguridad de la información la detección de pérdidas o fugas de la información por parte de las pequeñas empresas, puede requerir de varias semanas o meses, con la implementación del modelo permita reducir de manera significativa el tiempo en prevención de este tipo de riesgos, lo que permitirá detectar de forma oportuna las vulnerabilidades y riesgos de la institución.
- Todos los controles establecidos dentro de la normativa de la empresa permite mejorar los niveles de seguridad ya sea en su parte física, estructural, tecnológica; donde se podrán ir identificando cada uno de los problemas presentados, los mismos que podrán ser tomados como casos de análisis para poder identificar mecanismos y falencias en controles y políticas de seguridad de la información. Fundamentación Filosófica.
- Esta propuesta es generalizable a cualquier entidad del tipo Coka Tours ya que está concebida para ser aplicada en pequeñas empresas, a comparación con la propuesta de Francisco Freire Zapata la cual está limitada a una empresa (Coka Tours).
- Guevara Tucta Ramiro Alejandro (Alejandro, 2017), en su proyecto de investigación "Sistema de Gestión de Seguridad de la información basado en la Norma Iso/Iec 27001 para el departamento de tecnologías de la información y comunicación del distrito 18d01 de Educación", defendido en la Universidad Técnica de Ambato, propone políticas de seguridad para apoyar, proporcionar y gestionar adecuadamente la seguridad de la información en el distrito 18d01 de educación.

En la tesis de Luis Fernando Sánchez (Sánchez, 2009) , ha realizado una síntesis de otras metodologías que se han buscado resolver el problema de la implementación de los SGSI en las pequeñas empresas. Se va a comentar rápidamente a manera de resumen, los aspectos relevantes tomados de la misma tesis, ya que Luis Fernando

realiza fuertes críticas a cada una, justificando la creación de su metodología, como solución a las falencias que presentan las demás metodologías.

Fernando Gómez y Andrés Alvares en su publicación (Alvares, 2012) pretende facilitar a las pequeñas empresas, la comprensión de los diversos conceptos involucrados en un sistema de gestión normalizado y ofrece recomendaciones generales para la implementación de un SGSI, tanto para la norma UNE-ISO/IEC 27001, UNE-ISO/IEC 27002. Dicho artículo empieza por definir conceptos importantes, realizando una explicación de cada uno de los puntos de la norma, sus requisitos de documentación y su implementación. Ejemplifica con un caso práctico, la implementación de los apartados y documentos explicados, que pretende sumar los esfuerzos de los antecesores, para encontrar una alternativa que facilite el trabajo de las pequeñas empresas y que minimice los costos de implementación de las buenas prácticas que conduzcan a contar con un SGSI normalizado, bajo la norma ISO/IEC 27001.

2.2 Fundamentación Filosófica

La presente investigación se enmarca en el paradigma Critico Propositivo, es crítico porque realiza un análisis crítico del problema, y es propositivo porque busca proponer una solución factible al problema.

2.3 Fundamentación Legal

El presente trabajo de investigación se sustenta en las siguientes leyes:

LA CONSTITUCIÓN

Sección tercera

Comunicación e información

Art. 16.-Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.

2. El acceso universal a las tecnologías de información y comunicación.
3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.
4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.
5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación.

Art. 18.-Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley.
En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Sección novena
Personas usuarias y consumidoras
Art. 52.- Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características.

La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de estos derechos, la reparación e indemnización por deficiencias, daños o mala

calidad de bienes y servicios, y por la interrupción de los servicios públicos que no fuera ocasionada por caso fortuito o fuerza mayor.

Capítulo octavo
Derechos de protección

Art. 76.- En todo proceso en el que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas:

3. Nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley. Sólo se podrá juzgar a una persona ante un juez o autoridad competente y con observancia del trámite propio de cada procedimiento.

4. Las pruebas obtenidas o actuadas con violación de la Constitución o la ley no tendrán validez alguna y carecerán de eficacia probatoria.

5. En caso de conflicto entre dos leyes de la misma materia que contemplen sanciones diferentes para un mismo hecho, se aplicará la menos rigurosa, aun cuando su promulgación sea posterior a la infracción. En caso de duda sobre una norma que contenga sanciones, se la aplicará en el sentido más favorable a la persona infractora.

2.4 Categorías Fundamentales

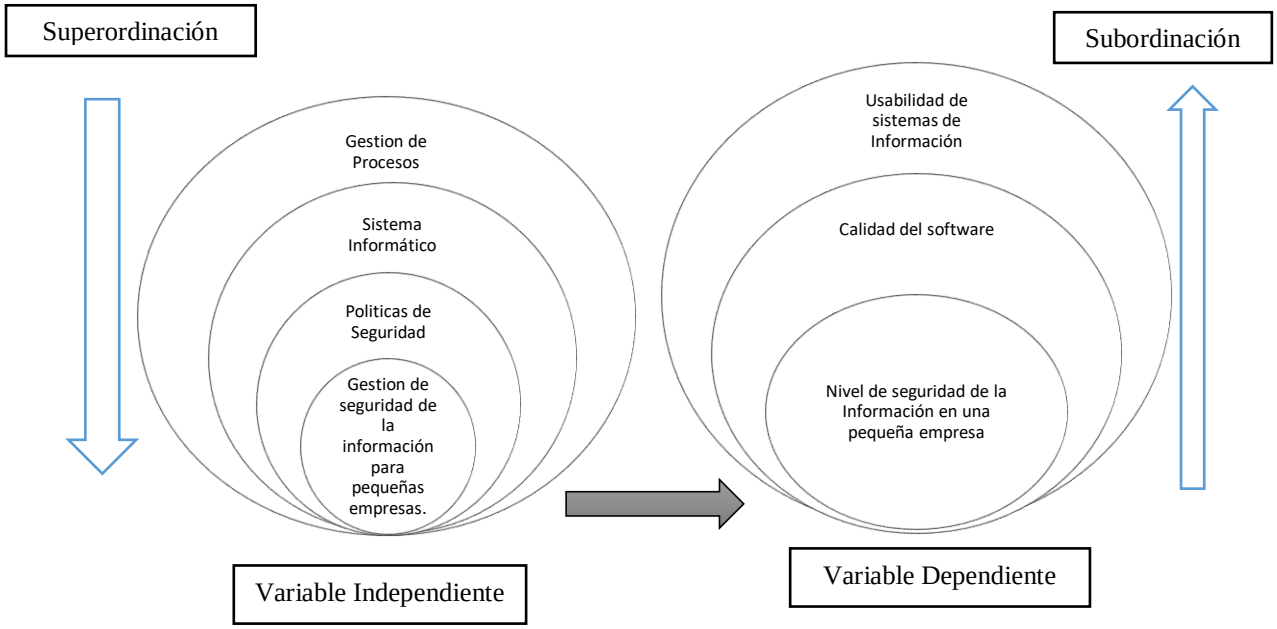


Ilustración 2-1: Inclusiones Conceptuales

Elaborado por: Investigador

Constelación de Ideas, Variable Independiente.

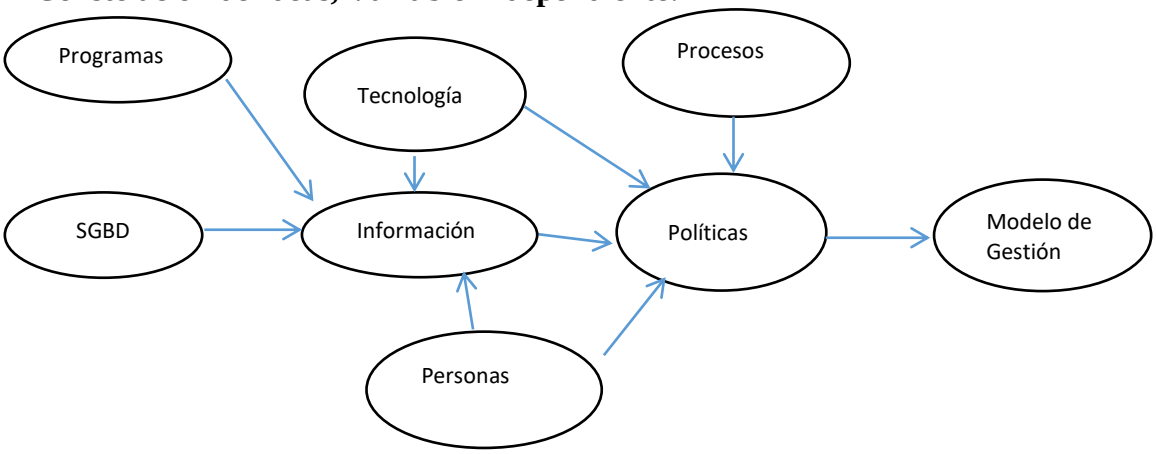


Ilustración 2-2: Constelación de Ideas de la Variable Independiente

Elaborado por: Investigador

Constelación de Ideas, Variable Dependiente.

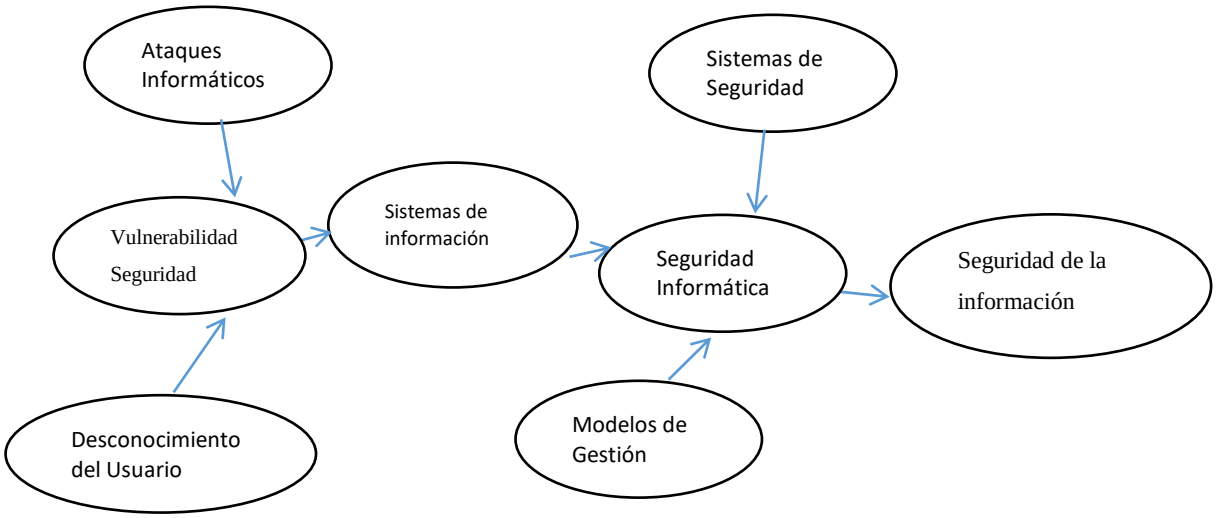


Ilustración 2-3: Constelación de Ideas de la Variable Dependiente

Elaborado por: Investigador

2.5 Hipótesis

La definición de un modelo de Gestión de Seguridad de la Información garantizará la seguridad de los activos de información en pequeñas empresas del Ecuador.

2.6 Señalamiento de Variables

Variable Independiente: Gestión de seguridad de la información para pequeñas empresas.

Variable Dependiente: Nivel de seguridad de la información en pequeñas empresas.

CAPITULO III

METODOLOGÍA

3.1 Modalidad básica de la investigación

Investigación Bibliográfica

La investigación será bibliográfica porque nos apoyaremos en libros, documentos técnicos, tesis del área financiera e informática, revistas, artículos y leyes existentes para la elaboración del marco teórico sobre modelos de gestión así como también de la seguridad de la Información.

Investigación de Campo

Se ha considerado esta modalidad ya que el investigador irá a recoger la información primaria directamente de los involucrados a través de una encuesta o entrevista.

3.2 Nivel o tipo de investigación

Se ha realizado la investigación exploratoria ya que permitió plantear el problema de la investigación Modelo de gestión de la seguridad de la información para pequeñas empresas. Como de la misma manera ayudo a plantear la hipótesis Modelo de Gestión de Seguridad de la Información concebido para la pequeña empresa garantizara la seguridad de los activos de información.

Se ha considerado la investigación descriptiva porque permitió analizar el problema en sus partes como delimitar en tiempo y en espacio construyendo el análisis crítico, la contextualización y los antecedentes investigativos.

Por otro lado se ha tomado la investigación correlacional ya que ha permitido medir la compatibilidad de la variable independiente.

3.3 Población y Muestra

Es importante resaltar que este trabajo trata un tema asociado a la realidad actual de las pequeñas empresas, el cual servirá como guía para otras que quieran tener una participación más activa en el sector productivo del país. El modelo propuesto brindará aportes en forma recomendaciones, acciones correctivas y preventivas que servirán para comprender y mejorar la gestión de riesgos de seguridad de la información para las pequeñas empresas, lo cual les permitirá contar con un modelo de gestión de seguridad de la información con niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información considerados relevantes para este tipo de instituciones, de manera tal que se asegure la continuidad operacional de los procesos y la entrega de productos y servicios a los usuarios, clientes o beneficiarios.

De acuerdo al directorio de empresas y establecimientos 2017 (Ecuadorencifras, 2018), ejecutada por el INEC se define a una pequeña empresa de acuerdo con el volumen de ventas anuales y el número de personas afiliadas.

	Ventas anuales	**Número de personas afiliadas**
Grande	$5´000.001 en adelante	200 en adelante
Mediana "B"	$2´000.001 a $5´000.000	100 a 199
Mediana "A"	$1´000.001 a $2´000.000	50 a 99
Pequeña	$100.001 a $1´000.000	10 a 49
Microempresa	menor o igual a $100.000	1 a 9

Tabla 3-0-1: Clasificación, Tamaño de empresa

Elaborado por: Investigador

Tomando en cuenta lo expuesto en la tabla 3-1, **Pasteurizadora el Ranchito** clasifica como pequeña empresa, por tal motivo para facilitar la implementación del modelo de Gestión de Seguridad de la Información el proyecto se valida en esta institución que se utilizó como caso de estudio.

Para ello se trabajará con una población total de grupo de expertos encargados de la admiración de empresas del sector.

De esta manera se podrá comprobar que el modelo de seguridad de la información propuesto será aplicable en las pequeñas empresas del Ecuador.

Población	Número	Porcentaje
Pasteurizadora el Ranchito	1	10%
Calzado Rexell	1	10%
Instal com	1	10%
Unidad educativa CEBI	2	20%
Pasteurizadora Agua Santa	1	10%
Pasteurizadora el Ordeño	2	20%
Pasteurizadora "Leches Zuu"	2	20%
Total	10	100%

Tabla 3-0-2: Población de Estudio

Elaborado por: Investigador

En vista que la población 10 expertos de la administración de sistemas se trabajarán con la totalidad del universo sin que sea necesario sacar muestras representativas.

3.4 Operacionalización de Variables

3.4.1 **Variable Independiente:** Gestión de la seguridad de la información para pequeñas empresas

Conceptualización o Descripción	**Dimensiones**	**Indicadores**	**Ítems Básicos**	**Técnicas e Instrumentos**
Es un esquema o marco de referencia para la administración de una entidad o área determinada en la que se desarrollan políticas y acciones, y con el cual se pretende alcanzar los objetivos	- Administración - Control. - Objetivos.	- Tipos de sistemas: Autenticación, manual. -Personalizado/General -Sistema Integral/Medular.	- Políticas de seguridad de la información. - Infraestructura. - Personal Involucrado.	- Modelo de Gestión de seguridad de la información - Auditoria informática - Socialización.

Tabla 3-0-3: Variable Independiente: Modelo de Gestión

Elaborado por: Investigador.

3.4.2 **Variable Dependiente:** Nivel de seguridad de la información en pequeñas empresas.

Conceptualización o Descripción	**Dimensiones**	**Indicadores**	**Ítems Básicos**	**Técnicas e Instrumentos**
Un modelo de gestión de seguridad de la información abarca un conjunto de medidas que permiten resguardar y proteger la información ante eventuales perdidas de información.	- Autenticación. - No repudio. - Integridad de información. - Confidencialidad - Disponibilidad. - Integridad	- Seguridad de la plataforma y red - Seguridad de Aplicaciones.	- Ha sido víctima de algún tipo de ataque en el cual haya perdido información. - Aplicar medidas preventivas permitirán minimizar el riesgo de un ataque. - Tiene conocimiento sobre los riesgos de un ataque informático.	Encuesta Cuestionario

Tabla 3-0-4: Variable Dependiente: Seguridad de la información

Elaborado por: Investigador

3.5 Plan de recolección de Información

La técnica a emplearse será la encuesta dirigida para lo que es necesario utilizar como instrumento el cuestionario a través de preguntas cerradas, lo que ayudará a la obtención más concreta de la información que queremos obtener.

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Para qué?	Para alcanzar los objetivos de la investigación
¿De qué personas u objetos?	Gerente General Jefe Contabilidad Responsables de Áreas Coordinador de Sistemas
¿Sobre qué aspectos?	Vulnerabilidades de seguridad de la información.
¿Quién, Quiénes?	Investigador: Ing. David Israel Chicaiza Cazar.
¿Cuándo?	Primer trimestre del 2018
¿Dónde?	Pequeñas empresas Cía. Ltda.
¿Cuántas veces?	Una
¿Qué técnicas de recolección?	Encuesta Entrevista Datos Estadísticos
¿Con qué?	Cuestionario Cuestionario Inspecciones
¿En qué situación?	Dentro del horario de trabajo con profesionalismo investigativo y absoluta confidencialidad y reserva.

Tabla 3-0-5: Recolección de la Información

Elaborado por: Investigador

3.6 Plan de procesamiento y Análisis

- Revisión crítica de la información recogida; es decir limpieza de información defectuosa, contradictoria, incompleta, no pertinente y otras fallas.
- Repetición de la recolección, en ciertos casos individuales para corregir errores de contestación.

- Tabulación o cuadros variables de la hipótesis y objetivos:
- Manejo de información (reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente que no influyen significativamente en los análisis).
- Estudio estadístico de datos para presentación de resultados.

Análisis de Resultados

- Análisis de los resultados estadísticos, destacando tendencias o relaciones fundamentales de acuerdo con los objetivos e hipótesis.
- Interpretación de los resultados con apoyo del marco teórico en el aspecto pertinente.
- Comprobación de hipótesis para la verificación estadística.
- Establecimiento de conclusiones y recomendaciones.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de los resultados.

Para el análisis de los datos, se ha procedido a considerar el criterio de 10 expertos de la administración de sistemas.

MATRIZ Nº 1 DE RESULTADOS DE ENCUESTA A EXPERTOS.

<table>
<tr><td></td><td>PREGUNTA</td><td>Resultados</td></tr>
<tr><td>1</td><td>El computador que utiliza tiene instalado antivirus y se encuentra actualizado?</td><td>
<table>
<tr><th>Opción</th><th>Cant. respuestas</th><th>Porcentaje %</th></tr>
<tr><td>SI</td><td>20</td><td>83.3 %</td></tr>
<tr><td>NO</td><td>4</td><td>16.7 %</td></tr>
</table>
</td></tr>
<tr><td>2</td><td>Ha firmado algún acuerdo de confidencialidad antes de ingresar a laborar en la institución ..?</td><td>
<table>
<tr><th>Opción</th><th>Cant. respuestas</th><th>Porcentaje %</th></tr>
<tr><td>SI</td><td>3</td><td>12.5 %</td></tr>
<tr><td>NO</td><td>21</td><td>87.5 %</td></tr>
</table>
</td></tr>
<tr><td>3</td><td>¿La información que usted maneja es respaldada periódicamente según sus necesidades..?</td><td>
<table>
<tr><th>Opción</th><th>Cant. respuestas</th><th>Porcentaje %</th></tr>
<tr><td>SI</td><td>4</td><td>16.7 %</td></tr>
<tr><td>NO</td><td>20</td><td>83.3 %</td></tr>
</table>
</td></tr>
<tr><td>4</td><td>¿Ha recibido capacitación sobre temas</td><td>
<table>
<tr><th>Opción</th><th>Cant. respuestas</th><th>Porcentaje %</th></tr>
<tr><td>SI</td><td>8</td><td>33.3 %</td></tr>
</table>
</td></tr>
</table>

	de seguridad de la información..?	NO	16	66.7 %

Tabla 4-4-1: Matriz Nº 1 de Encuesta a expertos

Elaborado por: Investigador

MATRIZ Nº 2 DE RESULTADOS DE ENCUESTA A EXPERTOS

	PREGUNTA	Resultados		
1	Poseen requisitos de seguridad para conceder acceso a la información a personal ajeno a la institución..?	**Opción**	**Cant. respuestas**	**Porcentaje %**
		SI	0	0 %
		NO	5	100 %
2	¿Mantienen inventario actualizado del hardware y software de la institución?	**Opción**	**Cant. respuestas**	**Porcentaje %**
		SI	3	60 %
		NO	2	40 %
3	¿Los derechos de acceso a la información son retirados después de la culminación del contrato con el empleado..?	**Opción**	**Cant. respuestas**	**Porcentaje %**
		SI	3	60 %
		NO	2	40 %
4	El área de servidores estará protegido por controles apropiados de entrada para asegurar que sólo el personal autorizado se les permite el acceso..?	**Opción**	**Cant. respuestas**	**Porcentaje %**
		SI	2	40 %
		NO	3	60 %
6	Disponen de políticas para asegurar el mantenimiento de	**Opción**	**Cant. respuestas**	**Porcentaje %**
		SI	0	0 %
		NO	5	100 %

<table>
<tr><td></td><td>hardware lo que permitirá mantener la disponibilidad e integridad continua de las TIC..?</td><td></td></tr>
<tr><td>7</td><td>Disponen de políticas para el manejo de contraseñas..?</td><td><table><tr><th>Opción</th><th>Cant. respuestas</th><th>Porcentaje %</th></tr><tr><td>SI</td><td>1</td><td>20 %</td></tr><tr><td>NO</td><td>4</td><td>80 %</td></tr></table></td></tr>
<tr><td>8</td><td>¿Se realiza copia de seguridad de la información que genera la empresa?</td><td><table><tr><th>Opción</th><th>Cant. respuestas</th><th>Porcentaje %</th></tr><tr><td>SI</td><td>4</td><td>80 %</td></tr><tr><td>NO</td><td>1</td><td>20 %</td></tr></table></td></tr>
<tr><td>9</td><td>La información sensible que genera la organización se encuentra protegida contra pérdida, destrucción y falsificación..?</td><td><table><tr><th>Opción</th><th>Cant. respuestas</th><th>Porcentaje %</th></tr><tr><td>SI</td><td>4</td><td>80 %</td></tr><tr><td>NO</td><td>1</td><td>20 %</td></tr></table></td></tr>
</table>

Tabla 4-4-2: Matriz Nº 2 de Encuesta a expertos

Elaborado por: Investigador

Análisis a encuesta Nº 1 de realizada a usuarios expertos

Análisis Pregunta N. 1

De las respuestas obtenidas, es posible evidenciar que un porcentaje de encuestados indica que sus equipos no poseen antivirus y mucho menos actualizado, confirmando que no todas las áreas se encuentran cubiertas por un antivirus con licencia.

Interpretación.

Al existir un porcentaje de usuarios encuestados indicando que su computador no se encuentra protegido con un antivirus actualizado, se puede demostrar que los equipos de la organización se encuentran en potencial riesgo de seguridad.

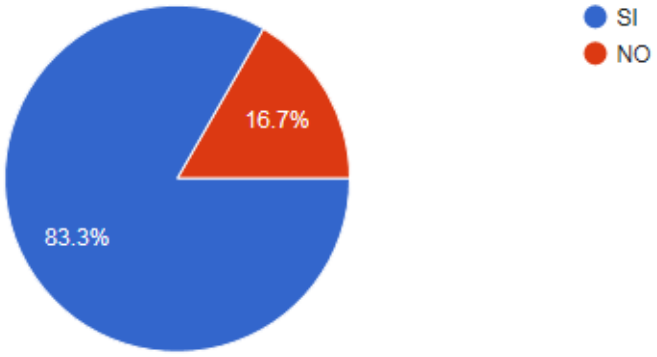


Ilustración 4-1: Usuarios expertos análisis Pregunta N. 1

Elaborado por: Investigador

Análisis Pregunta N. 2

Por las respuestas indicadas, se consiguió identificar que el mayor porcentaje de encuestados, no han firmado acuerdos de confidencialidad alguno al momento de ingresar a la institución.

Interpretación.

Por el porcentaje de respuestas negativas, podemos interpretar que los ex empleados de la organización podrían filtrar información de la misma. Lo cual podría dar lugar a que la institución no pueda judicializarlos a empleados que incurran con el acto ya que no se ha firmado acuerdos de confidencialidad alguna.

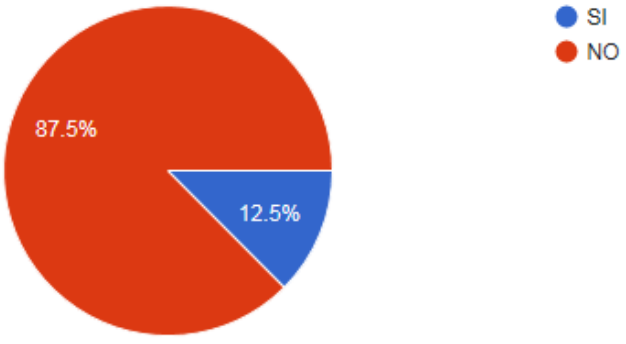


Ilustración 4-2: Usuarios expertos análisis Pregunta N. 2

Elaborado por: Investigador

Análisis Pregunta N. 3

De acuerdo a los resultados queda claro que no existe un proceso definido para respaldar la información que genera cada empleado en el cargo que desempeña.

Interpretación.

Existe la necesidad de definir un proceso para administrar de manera organizada los respaldos de información que generan los empleados administrativos, de manera que se la información se encuentre protegida contra pérdida, destrucción y falsificación.

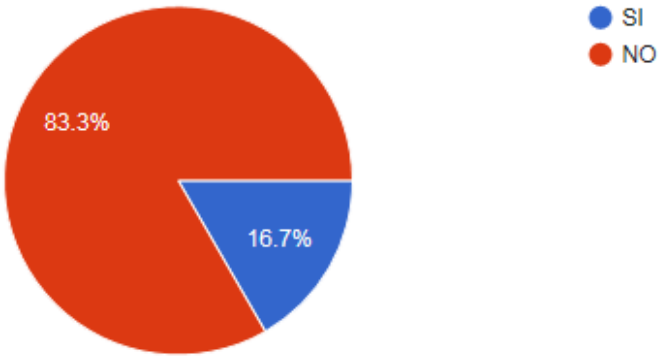


Ilustración 4-3: Usuarios expertos análisis Pregunta N. 3

Elaborado por: Investigador

Análisis Pregunta N. 4

Tomando en cuenta el gráfico anterior, se considera que la toma de decisiones se realiza con datos no muy confiables. Un buen porcentaje lleva solo apuntes manuales lo que aún agrava más la problemática.

Interpretación

Al disponer de un sistema de información gerencial y una vez almacenado los datos necesarios para la toma de decisiones, la plataforma ayudará a que la misma sea en base a información confiable y con datos que reflejen la realidad de los productos.

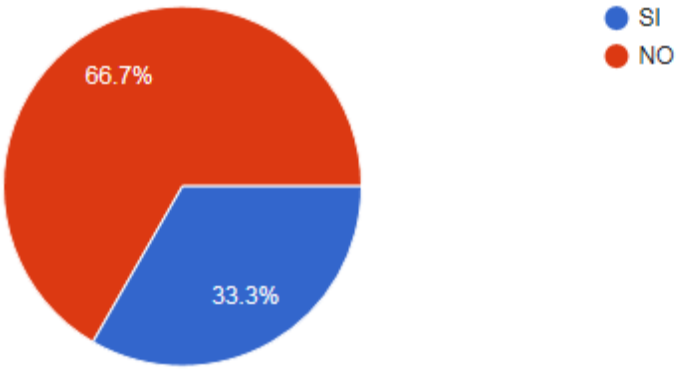


Ilustración 4-4: Usuarios expertos análisis Pregunta N. 4

Elaborado por: Investigador

Análisis a encuesta Nº 2 de realizada a usuarios expertos

Análisis Pregunta N.1

De las respuestas obtenidas en esta pregunta, queda evidenciado una falla de seguridad muy grave, ya que al no poseer requisitos de seguridad para que los invitados accedan a la red institucional la empresa se encuentra frente un potencial riesgo de seguridad, por lo que mucha de la información sensible se encuentra desprotegida.

Interpretación

Con la implementación de medidas de seguridad para el acceso a la red institucional, la empresa podrá gestionar su información de manera segura sin riesgos en el momento que desee.

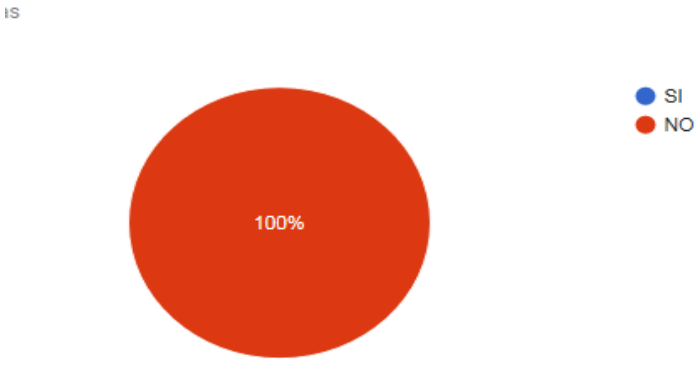


Ilustración 4-5: Usuarios expertos análisis Pregunta N. 1

Elaborado por: Investigador

Análisis Pregunta N. 2

Con las respuestas obtenidas, queda en evidencia que hay un campo amplio de mejora en cuanto al mantenimiento del inventario de hardware y software de la institución ya que el proceso no se está llevando de manera adecuada.

Interpretación

Es necesario implementar un proceso que permita mantener de manera continua actualizado el inventario de hardware y software de la institución.

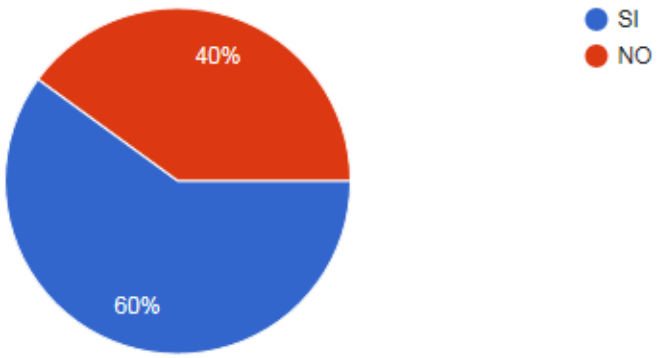


Ilustración 4-6: Usuarios expertos análisis Pregunta N. 2

Elaborado por: Investigador

Análisis Pregunta N. 3

El gráfico anterior muestra la falta de un proceso adecuado para retirar los derechos de acceso al a información cuando un empleado deja de laborar en la institución, ya sea por poca coordinación entre departamentos o por la escasez de normativas que permitan llevar el proceso de una manera organizada.

Interpretación

El modelo de gestión para la seguridad de la información que se implementara permitirá retirar los derechos de acceso a la información del empleado apenas culmine su relación laboral con la institución de esta manera se podrá evitar la fuga de información.

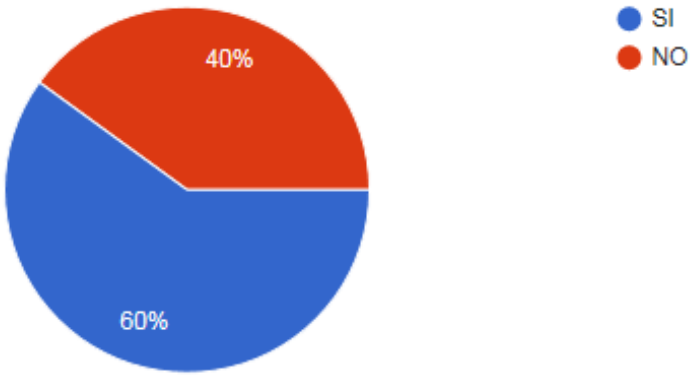


Ilustración 4-7: Usuarios expertos análisis Pregunta N. 3

Elaborado por: Investigador

Análisis Pregunta N. 4

El gráfico de la pregunta evidencia que el área de servidores no cumple con las normativas de seguridad mínimos, lo que demuestra una clara necesidad de usar todas las herramientas tecnológicas disponibles para asegurar y resguardar la zona tangible de información que posee la institución.

Interpretación

Al implementar medidas de seguridad físicas para el acceso a los servidores se asegurara que el acceso sea concedido únicamente al personal autorizado, lo que permitirá asegurar el área tangible de procesamiento de información dela organización.

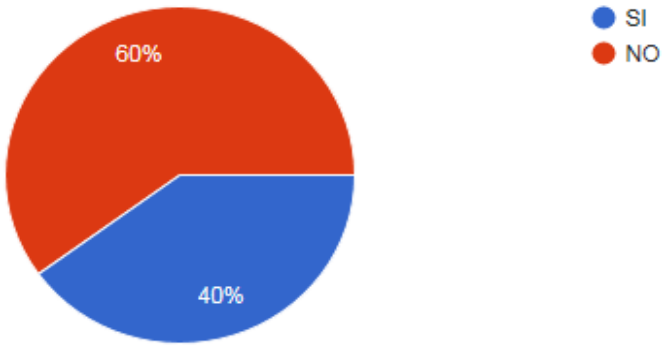


Ilustración 4-8: Usuarios expertos análisis Pregunta N. 4

Elaborado por: Investigador

Análisis Pregunta N. 5

De las respuestas obtenidas en esta pregunta, queda claro que es una necesidad importante contar con una adecuada política que reúna las características necesarias para para asegurar el mantenimiento del hardware de la institución.

Interpretación

Al incorporar políticas para el aseguramiento del mantenimiento del hardware de la institución mantener la disponibilidad e integridad continua de las TIC consiguiendo así una toma de decisiones más sustentada en datos reales.

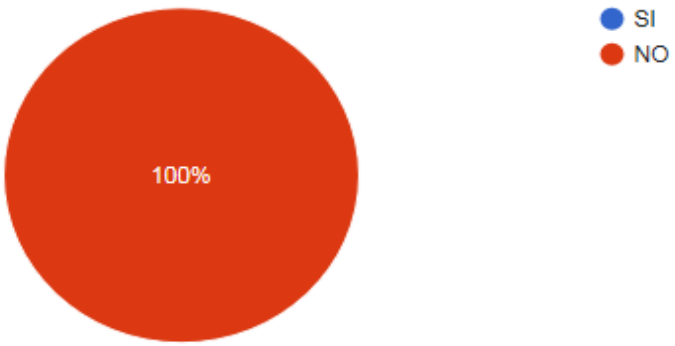


Ilustración 4-9: Usuarios expertos análisis Pregunta N. 5

Elaborado por: Investigador

Análisis Pregunta N. 6

Al momento, la institución carece de políticas para la administración y manejo contraseñas lo que podría desencadenar en fuga de información sensible para el usuario y la organización. Las consecuencias son diversas y varían según el valor que cada usuario haya establecido para la información.

Interpretación

Para gestionar correctamente la seguridad de las contraseñas, es recomendable establecer políticas para la administración y manejo de contraseñas.

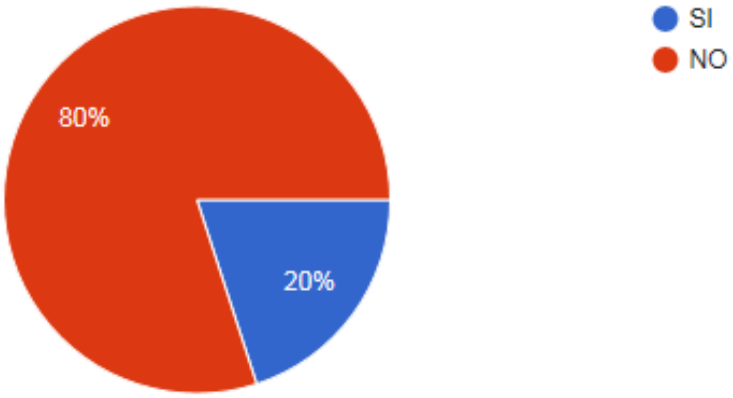


Ilustración 4-10: Usuarios Directivos análisis Pregunta N. 6

Elaborado por: Investigador

Análisis Pregunta N. 7

El proceso para respaldos de información se lo realiza sin seguir un proceso estandarizado ya que dichos respaldos se los almacena en el mismo esquipo donde se realizan los respaldos lo cual genera una baja confianza en la integridad de los mismos.

Interpretación

Con la implementación de un proceso estandarizado se podrá garantizar la integridad y disponibilidad de los respaldos de información, ya que al ser almacenados de una manera íntegra, la información que dispondrán y generarán estará de acuerdo a los procesos que la institución identificara como críticos.

El resguardar o respaldar la información es muy importante ya que se cuenta con un valioso elemento como lo es una o varias copias de archivos con información importante o personal y no solo respaldar sino también para asegurar que dicho contenido sea robado, dañado por un virus.

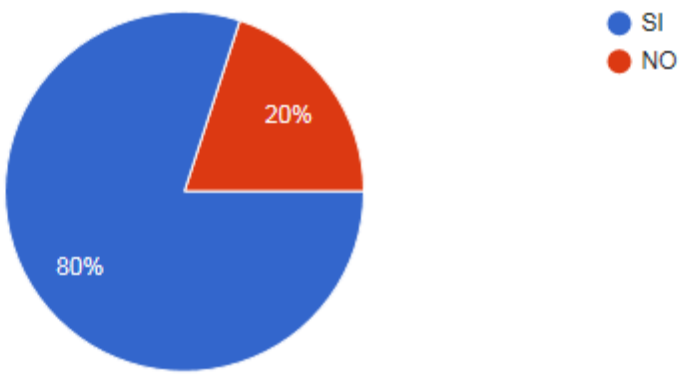


Ilustración 4-11: Usuarios expertos análisis Pregunta N. 7

Elaborado por: Investigador

Análisis Pregunta N. 8

El área directiva mantiene un escepticismo sobre la forma en la que se manejan los respaldos debido a que en ocasiones cuando ha sido necesario utilizarlos estos se encontraban inconsistentes obligando a utilizar respaldos de días anteriores.

Interpretación

Con la implementación del modelo propuesto, las empresas del sector podrán asegurar que su información se encuentre siempre disponible y protegida contra pérdida, destrucción y falsificación.

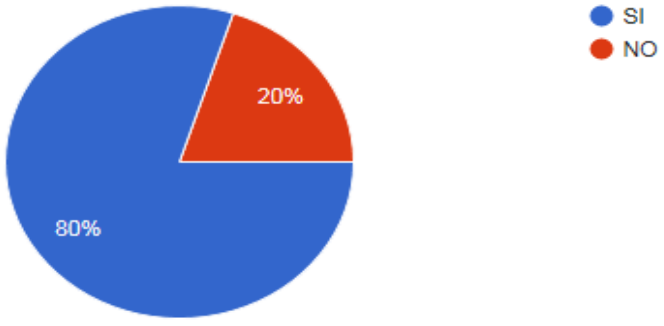


Ilustración 4-12: Usuarios expertos análisis Pregunta N. 8

Elaborado por: Investigador

4.2 Interpretación de datos.

De acuerdo a los datos recabados en las encuestas realizadas los usuarios expertos de las distintas instituciones, el modelo de gestión de seguridad de la información tiene como objeto planificar y crear procedimientos adecuados, para luego implementar controles de seguridad basados en una evaluación de riesgos y consiguiendo mediciones de eficiencia de los mismos.

Al establecer las políticas de seguridad y los procedimientos en relación a los objetivos del negocio, teniendo como objeto el mantener un nivel de riesgo menor al que la institución decida asumir, se empieza a hablar de un Modelo de gestión de seguridad de la información.

4.3 Verificación de Hipótesis

Para la verificación de la hipótesis se ha utilizado el método Chi Cuadrado, que para (Carranza, 2010), no es más que analizar, determinar y evaluar si existe una relación entre dos variables categóricas.

Ahora, según (Carranza, 2010), para evaluar se calculan los valores que indicarían la independencia absoluta, lo que se denomina frecuencias esperadas, comparándolos con las frecuencias de la muestra.

Para proceder con el cálculo se ha elegido de la encuesta dos preguntas del tema de investigación, considerando las dos variables.

Pregunta N. 4: ¿Ha recibido capacitación sobre temas de seguridad de la información..?

Opción	**Cant. respuestas**	**Porcentaje %**
SI	8	33.3 %
NO	16	66.7 %

Tabla 4-3: Verificación de la hipótesis Pregunta 4

Elaborado por: Investigador

Pregunta N. 4: ¿ El área de servidores estará protegido por controles apropiados de entrada para asegurar que sólo el personal autorizado se les permite el acceso..?

Opción	Cant. respuestas	Porcentaje %
SI	2	40 %
NO	3	60 %

Tabla 4-4: Verificación de la hipótesis Pregunta 4

Elaborado por: Investigador

4.3.1 Planteamiento de la hipótesis

La definición de un modelo de Gestión de Seguridad de la Información garantizará la seguridad de los activos de información en pequeñas empresas.

Modelo lógico

H_0: La definición de un modelo de Gestión de Seguridad de la Información NO garantizará la seguridad de los activos de información en pequeñas empresas.

H_1: La definición de un modelo de Gestión de Seguridad de la Información SI garantizará la seguridad de los activos de información en pequeñas empresas.

Modelo Matemático

$H_0 : O = E \qquad O - E = 0$

$H_1 : O \neq E \qquad O \neq E = 0$

Modelo Estadístico

Por la información obtenida a través de la encuesta propuesta y realizada, al personal administrativo de Pequeñas empresas, se procede a verificar la hipótesis planteada, con el uso de la prueba Chi-Cuadrado, con la siguiente fórmula:

$$X^2 = \sum_i \frac{(O_i - E_i)^2}{E_i}$$

En donde:

X^2 = Chi-cuadrado

∑ = Sumatoria

O = Frecuencia observada

E = Frecuencia esperada o teórica

4.3.2 Cálculo del Chi-cuadrado X^2

Propiedades	**Si**	**No**	**Total**
Falta de capacitación en temas de seguridad de la información	8	16	24
Poca seguridad en el área de servidores	2	3	5
TOTAL	10	19	29

Tabla 4-4-5: Valores para Cálculo de Chi-Cuadrado 4-6

Elaborado por: Investigador

Frecuencias observadas (O)	**Frecuencias esperadas (E)**	**(O-E) ² / E**
8	E = (8*24) /29 = 6.62	0.29
16	E = (16 * 24) / 29 = 13.24	0.58
2	E = (2 * 5) / 29 =0.34	8.10
3	E = (3 * 5) / 29 = 0.51	12.16
∑		21.13

Tabla 4-4-7: Cálculo de Chi-Cuadrado

Elaborado por: Investigador

Resultado: $X^2 = 21.13$

4.3.3 Nivel de significación

El nivel de significación es del 5% en donde $\alpha = 0.05$.

4.3.4 Grado de libertad

Para obtener este dato, utilizamos la siguiente fórmula

Donde

GL = Grado de libertad.

c = Columnas de la tabla.

h = Hileras de la tabla.

GL = (c-1) (h-1)

GL = (2-1) (2-1)

GL = 1

4.3.5 Grado de significancia

$\alpha = 0.05$

$X^2t = 0.00393$

Tabla de distribución del CHI CUADRADO

v	0,005	0,01	0,025	0,05	0,95	0,975	0,99	0,995
1	0,00003935	0,000157	0,000982	0,00393	3,841	5,024	6,635	7,879
2	0,010	0,020	0,051	0,103	5,991	7,378	9,210	10,597
3	0,072	0,115	0,216	0,352	7,815	9,348	11,345	12,838
4	0,207	0,297	0,484	0,711	9,488	11,143	13,277	14,860
5	0,412	0,554	0,831	1,145	11,070	12,832	15,086	16,750
6	0,676	0,872	1,237	1,635	12,592	14,449	16,812	18,548
7	0,989	1,239	1,690	2,167	14,067	16,013	18,475	20,278
8	1,344	1,647	2,180	2,733	15,507	17,535	20,090	21,955

Tabla 4-4-8: Tabla de distribución del CHI cuadrado

Elaborado por: Investigador

4.3.6 Decisión estadística

$X^2c = 21.13$ Valor obtenido del cálculo del Chi-cuadrado.

$X^2t = 0.00393$ Valor obtenido de la tabla de distribución del Chi – Cuadrado

Conclusión:

Como $X^2c = 21.13 > X^2t = 0.00393$, el valor que se obtuvo del calculó es mayor al valor de la distribución, se considera que las variables no son independientes y se RECHAZA la hipótesis nula con un nivel de significancia del 99%, por ende se ACEPTA la hipótesis alterna, es decir: “La definición de un modelo de Gestión de Seguridad de la Información SI garantizará la seguridad de los activos de información en pequeñas empresas”.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones.

La pequeña empresa caso de estudio en este trabajo, no realiza una Gestión formal de la seguridad de la Información, y no dispone de un Sistema de Gestión de Seguridad de la Información, debido más a la falta de interés y básicamente por un desconocimiento de su utilidad.

El modelo de sistema de gestión de seguridad de la información propuesto será de uso genérico y permitirá que las pequeñas empresas, se vuelvan más formales y sobre todo documentadas, optimizando por tanto el funcionamiento de la Seguridad de la Información.

En este como en todos los proyectos de implementación, un aspecto importante es que deben ser socializados, antes durante y después; si se quiere realmente resultados de calidad.

5.2 Recomendaciones.

Se recomienda que las pequeñas empresas inviertan recursos en la gestión de riesgos en seguridad de la información ya que esto le permitirá mantener su información de forma íntegra, disponible y manteniendo un grado aceptable de confidencialidad.

Es importante que en todo momento y principalmente en la planificación de la Gestión de la Seguridad de la Información se considere el tratamiento de los Riesgos, como una área más de conocimiento, es decir una gerencia de riesgos, no solo para para evitarlos o minimizar su efecto, sino que se constituya un proceso iterativo de saber qué hacer, y como hacerlo con la oportunidad del caso, característica única de una gestión de calidad.

Es responsabilidad del alta dirección de las pequeñas empresas formalizar una adecuada inducción a la utilización de un Sistema de Gestión de Seguridad de la Información.

CAPITULO VI

PROPUESTA

6.1 Datos Informativos.

6.1.1 Título

"Modelo de gestión de la seguridad de la información para pequeñas empresas."

6.1.2 Institución

Esta propuesta se la realiza para que sea aplicable a pequeñas empresas. Se valida su uso en Pasteurizadora el Ranchito, institución que se utilizó como caso de estudio.

6.1.3 Beneficiarios

Con el desarrollo del presente proyecto, los principales beneficiarios son los gerentes o representantes de las pequeñas empresas.

6.1.4 Ubicación.

- Provincia: Cotopaxi
- Cantón: Salcedo.

6.1.5 Técnico responsable

- Investigador: David Israel Chicaiza Cazar
- Coordinador del proyecto: Dr. Félix Oscar Fernández Peña
- Personal designado por pasteurizadora el Ranchito.

6.2 Antecedentes de la propuesta.

Guevara Tucta Ramiro Alejandro (Alejandro, 2017), en su proyecto de investigación "Sistema de Gestión de Seguridad de la información basado en la Norma Iso/Iec 27001 para el departamento de tecnologías de la información y comunicación del distrito 18d01

de Educación", defendido en la Universidad Técnica de Ambato, propone políticas de seguridad para apoyar, proporcionar y gestionar adecuadamente la seguridad de la información en el distrito 18d01 de educación.

En la tesis de Luis Fernando Sánchez (Sánchez, 2009) , ha realizado una síntesis de otras metodologías, buscado resolver el problema de la implementación de los SGSI en las pequeñas empresas. Luis Fernando Sánchez (Sánchez, 2009) realiza fuertes críticas a cada metodología, como solución a las falencias que presentan las estudiadas en su tesis. Fernando Gómez y Andrés Álvares en su publicación (Alvares, 2012) pretende facilitar a las pequeñas empresas, la comprensión de los diversos conceptos involucrados en un sistema de gestión normalizado y ofrece recomendaciones generales para la implementación de un SGSI, tanto para la norma UNE-ISO/IEC 27001, UNE-ISO/IEC 27002. Dicho artículo empieza por definir conceptos importantes, realizando una explicación de cada uno de los puntos de la norma, sus requisitos de documentación y su implementación. Ejemplifica con un caso práctico, la implementación de los apartados y documentos explicados, que pretende sumar los esfuerzos de los antecesores, para encontrar una alternativa que facilite el trabajo de las pequeñas empresas y que minimice los costos de implementación de las buenas prácticas que conduzcan a contar con un SGSI normalizado, bajo la norma ISO/IEC 27001.

Además se realizó hizo una búsqueda en Scopus utilizando como palabras clave "Cyber" y "Security", de la cual se obtuvieron 15,398 registros con fecha de publicación entre 2015 al 2019, lo que demuestra la pertinencia actual del tema.

Sin embargo al agregar "pequeña empresa" entre las palabras clave la búsqueda en Scopus no devolvió ningún resultado quedando claro que la investigación en Cyber seguridad para la solución del problema en pequeñas y medianas empresas es un área de investigación que no está ampliamente tratada aun cuando para el caso del Ecuador, las pequeñas y medianas empresas constituyen alrededor del 40% del total de empresas registradas en el país (Media, 2017), resulta fundamental atender las necesidades de cyber-seguridad de las empresas que tienen la mayor participación económica en el sector manufacturero siendo las de mayor participación económica las empresas del sector de la industria manufacturera (telégrafo, 2017).

En el proceso de investigación se han encontrado referencias de intentos por resolver el problema de implementación de sistemas de información de seguridad de la información. Estos trabajos analizados se aproximan a lo que se pretende proponer, sin embargo a la final, no se enfocan específicamente en las pequeñas empresas. El modelo propuesto desarrolla un conjunto de directrices, que permitirán mantener y gestionar la seguridad de los sistemas de información de las pequeñas empresas.

6.3 Justificación.

El manejo y administración de la información que generan las pequeñas empresas del sector industrial de la zona centro del país, manifiesta poco interés por parte de los directivos de las empresas de dicho sector, ya sea por desconocimiento o falta de recursos en invertir en temas de seguridad de la información. Por tanto se ve la necesidad de definir, basados en estándares internacionales, políticas de seguridad que se acoplen a este tipo de empresas mismas que permitirán gestionar los activos de información de una manera ordenada y segura.

Es importante mencionar que se cuenta con el apoyo y respaldo de la pequeña empresa Pasteurizadora "El Ranchito", empresa del sector industrial de la zona centro del país, y también por parte del equipo del proyecto que pertenece a la Universidad Técnica de Ambato, por lo que es factible implementar el proyecto propuesto, con lo que se va a conseguir validar la propuesta actual para gestionar de manera adecuada los activos de información que generan este tipo de instituciones.

En su artículo "Análisis de la Productividad de la Industria Manufacturera del Ecuador" Juan López y Rafael Quintana (Vera & Quintana, 2017), señalan que el Ecuador tiene un problema fuerte de competitividad en el sector industrial, influenciado por los bajos niveles de innovación, conocimiento y cooperación. Por tal motivo se reconoce como aplicable la propuesta planteada; debido que está orientando a que las pequeñas empresas hagan un uso responsable de los recursos que poseen.

6.4 Objetivos.

6.4.1 Objetivo General

Definir un modelo de gestión de la seguridad de la información para pequeñas empresas

6.4.2 Objetivos Específicos

- Realizar un análisis crítico de los estándares de seguridad y propuestas de otros autores, como base para la construcción del modelo.
- Definir políticas de seguridad de la información en las que se basará el modelo de gestión para pequeñas empresas en el Ecuador.
- Validar el modelo propuesto en el ámbito del caso de estudio seleccionado.

6.5 Análisis de Factibilidad.

El proyecto realizado para el sector industrial de las pequeñas empresas, cuenta con el presupuesto necesario para proceder con el desarrollo de modelo de gestión planteado, posibilitando gestionar de mejor manera la inversión individual o conjunta, mismas que influyen de manera directa en el crecimiento empresarial.

6.5.1 Factibilidad Económica

Al tratarse de un proyecto para el sector industrial de las pequeñas empresas, se cuenta con el presupuesto adecuado para implementar el modelo propuesto.

6.5.2 Factibilidad Técnica

Es factible técnicamente ya que se cuenta con los recursos tecnológicos requeridos, así como el acceso a la infraestructura, brindando las herramientas tecnológicas, acceso a datos e información necesaria.

6.6 Fundamentación.

Considerando que el proyecto ayudará a las pequeñas empresas del sector industrial, se tomó como caso de estudio a Pasteurizadora el "Ranchito". Sus directivos han brindado la apertura necesaria para que se evalúe la propuesta en su entorno empresarial, siendo importante el apoyo del coordinador de sistemas de la institución, quien posee el

conocimiento adecuado sobre el estado en materia de seguridad de la información en la institución. Por tal motivo se concluye que es factible desarrollar el modelo de gestión de la seguridad de la información para pequeñas empresas que se propone.

6.6.1 Serie ISO 27000

La familia de normas ISO 27000 consta de una serie de normas, misma que consta de un rango de numeración reservado por ISO; van de 27000 a 27019 y de 27030 a 27044.

ISO 27001 (ISO 27001:2005, 2005)**,** Publicada el 15 de octubre de 2005, es una norma fundamental de esta serie ya que contiene los requisitos para los sistemas de gestión de seguridad de la información que establecen condiciones para aquellas empresas que deseen certificarse bajo esta norma. En el anexo A, se describe en forma de resumen los objetivos que deben tener en cuenta aquellas instituciones para desarrollar sus modelos de gestión de seguridad de la información. La implementación de todos los controles enumerados en dicho anexo no es obligatoria pero las instituciones deberán justificar con base en la norma la no aplicabilidad de los controles no implementados.

ISO 27002 (ISO 27002:2005, 2005)**,** Desde el 1 de julio de 2007, es el nuevo nombre de la ISO 17799:2005, manteniendo 2005 como año de edición. Constituye una orientación de buenas prácticas que cuenta con objetivos de control recomendables para la seguridad de la información. Consta de 39 objetivos de control y 133 controles, organizados en 11 dominios. Sin embargo, no es certificable.

ISO 27003 (ISO 27003, 2010)**,** Consta de normas para la implementación de modelos de seguridad de la información sobre el uso del modelo PDCA (modelo de mejora continua) y de las obligaciones de sus diferentes fases. Su origen se basa en el anexo B de la norma BS7799-2 y la documentación publicada por BSI (British Standards Institution), el cual es un organismo colaborador de ISO y proveedor de estas normas, son destacables la ISO 9001, ISO 14001, ISO 13485 e ISO 27001.

ISO 27004 (ISO 27004, 2009)**,** Este estándar especifica cómo estructurar el sistema de medición, cuáles son los parámetros a medir, cuándo y cómo medirlos. Además, ayuda a las empresas al establecimiento de objetivos relacionados con el rendimiento y los criterios de éxito.
Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo de mejora continua.

ISO 27005 (ISO 27005, 2018)**,** Esta norma determina los lineamientos para gestionar los riesgos en temas de seguridad de la información. Reemplaza a la norma ISO 13335-2 "Gestión de Seguridad de la Información y la tecnología de las comunicaciones" y está orientada para ayudar a la implementación favorable del SGI desde el punto de vista de la gestión de riesgos. La norma es aplicable a todo tipo de instituciones (por ejemplo, empresas comerciales, agencias gubernamentales, etc.) interesadas en gestionar los riesgos que puedan comprometerlas en el ámbito de seguridad de la información.

ISO 27006 (ISO 27006, 2015)**,** Especifica los requisitos para la acreditación de entidades de auditoria y certificación de sistemas de gestión de seguridad de la información, está pensada para apoyar la acreditación de organismos de certificación que ofrecen la certificación del Sistema de Gestión de Seguridad de la Información. Se encarga de especificar los requisitos y suministrar una guía para la auditoría y la certificación del sistema, pero no es una norma de acreditación por sí misma.

ISO 27011 (ISO 27011, 2008)**,** Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

ISO 27031 (ISO 2731, 2011)**,** Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones, proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos para mejorar la preparación de las TIC de una empresa para asegurar la continuidad de negocio.

ISO 27032 (ISO 27032, 2012)**,** Consiste en una guía relativa a la ciberseguridad. La cual facilita la colaboración segura y fiable para proteger la privacidad de las personas. De esta manera, puede ayudar a prepararse, detectar, monitorizar y luchar contra ataques de ingeniería social, hackers, malware, spyware y otros tipos de software no deseado.

ISO 27033 (ISO 2733-5, 2013)**,** Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes.

ISO 27034 (ISO 27034-1, 2011)**,** Consiste en una guía de seguridad en aplicaciones la cual está dirigida a aquellas personas que llevan a cabo el diseño, programación, adquisición y uso de los sistemas de aplicación. La finalidad de dicha norma es asegurar que las aplicaciones informáticas conceden el nivel necesario o deseado de la seguridad en apoyo del Sistema de Gestión de Seguridad de la Información de las empresas.

ISO 27799 (ISO 27799, 2016)**,** Es un estándar de gestión de seguridad de la información en el sector sanitario. Define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos e imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo),

ya que la información siempre debe estar adecuadamente protegida. El original se encuentra en inglés.

Aplicación de la norma ISO 270001

Las medidas de seguridad deberán estar adaptadas a la estructura administrativa, al personal y al entorno tecnológico de cada pequeña empresa. El esfuerzo financiero y tecnológico deberá ser proporcional a los riesgos reales existentes.

Los primeros acercamientos en la institución de caso de estudio, complementadas con las encuestas que se encuentran referenciadas en el anexo 1 y 2 de la propuesta, las cuales permiten indagar los niveles de gestión de la seguridad de la información de la institución, permitieron observar limitaciones de aplicación de algunas políticas de seguridad que fueron establecidas de manera empírica, y otras políticas que no han sido implementadas por razones principalmente culturales, falta de conocimiento y una mala planificación para el establecimiento de sus necesidades en cuanto a seguridad de la información.

La falta de gestión ocasiona que no se realicen auditorías de las aplicaciones a donde ingresan los usuarios y la información a la cual acceden, con el fin de hacer evaluaciones e imponer correctivos si el análisis así lo determina. En conclusión, se ha observado que no es prioridad el operativizar la seguridad de la información. Por tal motivo, las políticas de seguridad que deben estar documentadas no existen. A esto se suma la falta de apoyo económico del área gerencial en pequeñas empresas para atender el tema de la seguridad informática.

Las políticas, procedimientos y guías de seguridad son elementos dinámicos que deben modificarse de acuerdo con los cambios organizacionales de las pequeñas empresas y a las innovaciones tecnológicas en seguridad de la información, al igual que atendiendo a los cambios del entorno político, social y económico del país.

Los planteamientos de gestión de seguridad de la información, resumidos por medio de políticas, serán válidos por un determinado periodo de tiempo. Los enunciados de las políticas cumplen una permanencia limitada, luego de lo cual será necesario actualizarlas y por tanto se crearán nuevas adaptaciones. Por lo expuesto es pertinente contar con un modelo que estructure, organice y defina adecuadamente estos procesos de cambio.

Un certificado ISO 27001 implica que un Sistema de Gestión de Seguridad de la Información ha sido certificado bajo una norma de acuerdo con las buenas prácticas que esta norma establece. Cuando una entidad de certificación ha expedido el certificado demuestra que la entidad evaluada ha tomado suficientes precauciones para proteger la información confidencial contra el acceso no autorizado y los cambios.

La norma se encuentra orientada a establecer una guía que permita implantar, poner en marcha, analizar y mantener un modelo de Gestión Seguridad de la Información para ser aplicable a compañías, relativamente pequeñas.

El modelo planteado sigue un rumbo preciso orientado a la seguridad de la información. Que necesite un entorno de protección comenzando por la información digital, activos físicos, equipos de cómputo y redes, entre otros activos.

ISO/IEC 27001 pretende que se proteja la información en términos de:

- Asegurar la confidencialidad: que la información está accesible solo para aquellas personas autorizadas a tener acceso.
- Garantizar la integridad de la información, asegurando que los datos continúen inalterados excepto cuando sean modificados por personal autorizado.
- Consolidar la disponibilidad; esto garantizará que los usuarios autorizados tengan acceso a la información y los activos relacionados cuando sea necesario.

La meta es llegar a un completo modelo de gestión que abarque los aspectos necesarios para ser aplicado en pequeñas empresas, desarrollando un proceso de mejora continua.

6.6.2 Aspectos tomados en cuenta en el desarrollo del modelo propuesto.

Se propone seguir los pasos que se enumeran a continuación, y que se refieren en la serie ISO 27000, para medir y reportar el estado de la seguridad de la información en la forma en que se especifica.

6.6.2.1 Involucramiento de la alta dirección

El apoyo permanente del área directiva de las pequeñas empresas, se constituye en uno de los principales requerimientos para su implantación; su participación en el proyecto es de vital importancia, ya que el entendimiento claro y apoyo a la gestión del director o persona que se encuentre implementando este Sistema marcará la ruta por la cual se encamine el proceso de implementación. Además implica que el cumplimiento posterior de las políticas establecidas se traduzca en disposiciones para todos los niveles de este tipo de organizaciones.

Su participación también definida en la Planificación Estratégica Institucional, incluirá el desarrollo de las TIC en la competitividad de la institución; ya que hoy en día, las TIC deben responder a las necesidades del negocio.

6.6.2.2 Reglamentaciones o disposición legales

Según Patricio Chacón (Chacón Mejía), una buena gestión no es posible sin una buena reglamentación. Dicho de otra manera, es la legislación interna y externa lo que determina que la aplicabilidad del sistema tenga sustento para su fiel cumplimiento en la fase de implementación.

Se dice, en términos comunes, que el personal no hace lo que se dice que haga, sino lo que se le controla y supervisa. Por tanto, se requiere un mecanismo a través del cual se pueda garantizar la existencia de reglamentaciones y/o disposiciones que cuenten con la firma y aval de los altos mandos de la institución, que establezcan, de forma concreta, un plan de medidas de seguridad informática en la institución.

El aspecto del control legal a tomar en consideración es la revisión del cumplimiento de la legislación vigente sobre la base de criterios a continuación definidos, en función del alcance que se pretenda dar a la revisión de los aspectos legales.

En particular, de los aspectos jurídicos comunes a todo tipo de organización, la ISO/IEC 27001 identifica, de modo meramente enunciativo, los siguientes criterios:

- Propiedad intelectual.
- Protección de datos de carácter personal.

- Uso de las herramientas tecnológicas por parte de los usuarios de los sistemas de información de la organización.
- Registros de información de la organización.
- Reglamentación de los controles de cifrado y uso de firma electrónica.

6.6.2.3 Plan de acción

Los aspectos que se tomaran en cuenta para desarrollar el modelo propuesto abarcan las siguientes especificaciones:

- Se identificarán y clasificarán los activos de información que poseen las pequeñas empresas para establecer mecanismos de protección necesarios.
- Se determinarán e implantarán medidas para proteger los datos contra accesos no autorizados, infracciones de autenticidad y pérdida de integridad, que garanticen la disponibilidad necesaria para que los clientes y usuarios de los servicios puedan acceder a una información íntegra de manera segura.
- Todos los funcionarios y/o contratistas, serán responsables de proteger la información la cual accedan y procesen (ver anexo 4), para evitar su pérdida, alteración, destrucción o uso indebido.
- Se admitirá únicamente el uso de software que haya sido legalmente adquirido por la institución.
- Los empleados y contratistas asumirán la responsabilidad de reportar incidencias de seguridad, sucesos sospechosos y el uso inadecuado de recursos que identifiquen.
- Las violaciones a las políticas y controles de seguridad de la información serán reportadas y se tratarán según las disposiciones contractuales y legales.
- La entidad contará con un plan de contingencia (anexo 5) proyecto para mantener la continuidad del negocio y sus operaciones, ante el acontecimiento de sucesos no previstos como desastres naturales y ciberataques.
- El modelo propuesto recomendará controles destinados a impedir infracciones y violaciones de las leyes del derecho civil y penal de las obligaciones establecidas

por las leyes, estatutos, normas, reglamentos o contratos, y de los requisitos de seguridad.

6.6.3 Modelo de gestión orientado a la seguridad de la información para pequeñas empresas

La información es un activo importante para la organización, el cuál debe ser protegido adecuadamente; este activo vé cada vez más amenazado, e independientemente de su forma, se expone a una gran variedad de amenazas y vulnerabilidades.
Para asegurar la continuidad de los sistemas de información el modelo propuesto sugerirá políticas, procesos y procedimientos para minimizar los riesgos que enfrenta el funcionamiento de la entidad.

A los efectos de la presente metodología se entienden por:

- **Amenaza:** Es una situación o acontecimiento que pueda causar daño a los bienes informáticos; puede ser una persona, un programa malicioso o un suceso natural o de otra índole y representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema.
- **Política:** Es un conjunto de reglas para el mantenimiento de cierto nivel de seguridad. Pueden cubrir cualquier cosa desde buenas prácticas para la seguridad de un solo ordenador, reglas de una empresa o edificio, hasta las directrices de seguridad de un país entero
- **Procedimiento:** es un conjunto de acciones u operaciones que tienen que realizarse de la misma forma, para obtener siempre el mismo resultado bajo las mismas circunstancias.
- **Análisis de riesgo:** el proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar
- **Bienes informáticos:** Los elementos componentes del sistema informático que deben ser protegidos en evitación de que como resultado de la materialización

de una amenaza sufran algún tipo de daño.

- **Impacto:** Es el daño producido por la materialización de una amenaza.
- **Riesgo:** Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en la organización.
- **Seguridad:** Es usado en el sentido de minimizar los riesgos a que están sometidos los bienes informáticos hasta llevarlos a niveles adecuados.
- **Sistema informático:** Es el conjunto de bienes informáticos de que dispone una entidad para su correcto funcionamiento y la consecución de los objetivos.
- **Vulnerabilidad:** En un sistema informático es un punto o aspecto susceptible de ser atacado o de dañar su seguridad; representan las debilidades o aspectos falibles o atacables en el sistema informático y califican el nivel de riesgo del mismo.

Ya que en el modelo de gestión planteado está basado en la normativa ISO 27001, cubre los aspectos que se muestran en la Ilustración 6-1:

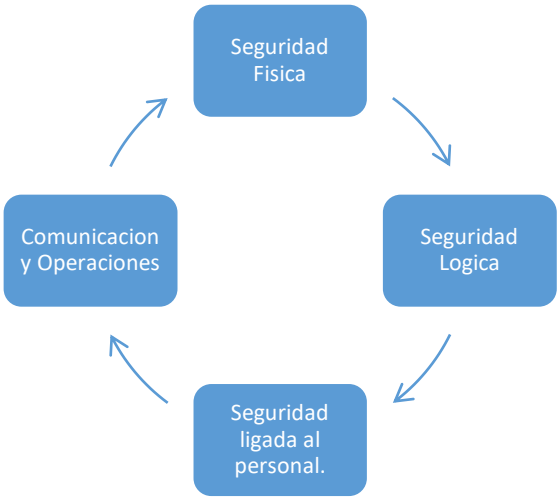


Ilustración 6-1: Barreras de Seguridad.

Elaborado por: Investigador

En aras de generar los controles necesarios, el modelo propuesto incluye políticas, procesos y procedimientos específicos, las cuales incluyen procedimientos, lineamientos

y directrices con el fin de que el modelo de gestión de la seguridad quede claro para todo el personal de la organización , tal y como se muestra en la tabla 6-1:

Modelo Propuesto

Estado de situación inicial	• Inventario de activos de información • Análisis de riesgos.
Seguridad Física	• Uso adecuado de los activos • Implementación o actualización de recursos tecnológicos • Control de acceso físico • Protección y ubicación de los equipos • Gestión de medios removibles • Riesgos relacionados con terceros
Seguridad Lógica.	• Control de acceso a los sistemas de información • Definición de roles de usuario • Protección contra software malicioso • Copias de respaldo • Seguridad para el intercambio de información • Gestión de contraseñas de usuario • Escritorio y pantalla limpia
Seguridad ligada al personal	• Acuerdos de confidencialidad • Gestión del Talento Humano • Culminación o cambio de contrato laboral
Comunicación y Operaciones	• Acceso a Internet • Correo electrónico • Segregación de redes

Tabla 6-1: Modelo propuesto seguridad de la información

Elaborado por: Investigador

Ilustración 6-2: Resumen modelo de seguridad propuesto.

Elaborado por: Investigador

6.6.3.1 Estado de situación inicial.

A. Inventario de activos de información [ISO/IEC 27001:2005 A.7.1.1]

Mediante el inventario de activos de información se específica y se reconoce cuáles son los activos de información más importantes para la institución y de esta forma darles el tratamiento que se requiere para una protección adecuada, para el cumplimiento de la misión y los objetivos institucionales.

El inventario permite identificar los activos de información a los que se les debe brindar mayor protección y que se pueden requerir para servir a otros propósitos de la empresa por ejemplo: controles de seguridad física, lógica, de acceso, entre otros.

El flujo de las actividades que se surten para la identificación, elaboración, mantenimiento y actualización del inventario de activos se relaciona a continuación:

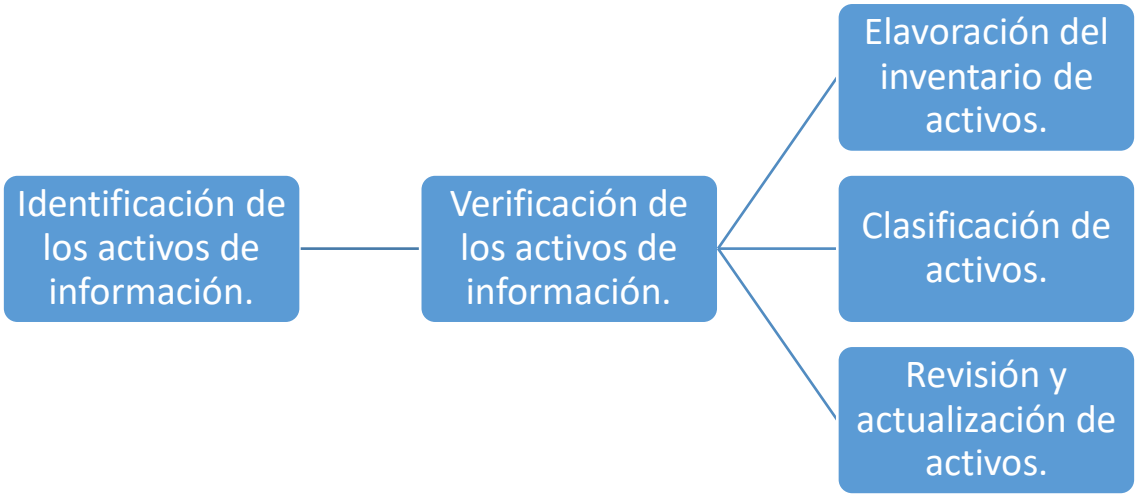


Ilustración 6-3: Flujo de actividades; activos de información

Elaborado por: Investigador

La coordinación de sistemas será la responsable de realizar el levantamiento de los activos de información, así como de liderar la ejecución y mantenimiento del Inventario de Activos, de acuerdo a lo anterior se define las siguientes actividades:

Identificar los activos de información

En esta actividad, se deberán identificar cuáles y cuantos activos son los activos de información a ser inventariados.

Definir los activos de información

En esta actividad se establecen los procesos para la inclusión de los activos en la matriz de inventarios de activos, de acuerdo con las variables establecidas para lograr identificar cuales activos son de mayor criticidad e impacto para la institución.

Periodicidad revisión de los activos de información

Para la realización del levantamiento, revisión y/o actualización del inventario de activos de Información se establecerá como periodicidad anual, sin embargo, esta podrá cambiar de acuerdo a las necesidades de cada institución.

Consolidación de los activos de información

La consolidación del inventario y su actualización se deberá llevar a cabo con una periodicidad anual o cada vez que la Agencia lo crean necesario.

CAMPOS MATRIZ INVENTARIO ACTIVOS DE INFORMACIÓN

A continuación se detallan los campos que se establecen en el instrumento para realizar el levantamiento de activos de información:

Sección Registro de Activos

- **Número:** Digitar el consecutivo con el cual se puede llevar el conteo de los activos de información.
- **Dependencia/Ubicación:** Identificar la ubicación exacta en donde se encuentra el activo de información.
- **Nombre del activo de información:** El activo de información se define como el elemento de información que la empresa recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes. Los Tipos de activos de Información de la institución son de: Información Física, Información Digital, Software, Hardware y Servicios. Se debe indicar entonces el nombre específico del activo de información, es decir, la palabra o frase con la que se da a conocer el asunto de la información. Se deben evitar abreviaciones o el uso excesivo de siglas.
- **Dispositivo:** se debe incluir una breve descripción del contenido del activo de información. Responder la pregunta: ¿de qué se trata la información?. Cuando se

trate de activos de información consistentes en información física o información digital, se deberán tener en cuenta las definiciones del banco de términos de la entidad.

- **Marca y Modelo:** En este apartado se deberá describir la marca y modelo del activo.
- **Serie:** Si el activo posee número de identificación deberá ser colocado en este apartado.
- **Características:** En este ítem se deberá identificar algún rasgo o señal que identifique al activo de información.
- **Estado:** Señala en que si el estado se encuentra el activo de información (Bueno/Malo).
- **Custodio:** En este campo se define a cargo de que empleado de la institución se encuentra el activo de información.
- **Observaciones:** Este campo identifica algún rasgo adicional que tiene el activo de información.

B. Análisis de riesgos [ISO/IEC 27001:2005 A.6.2.1]

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y las consecuencias (impacto) de ellos, calificándolos y evaluándolos para establecer el nivel de riesgo y las acciones que conformarán el plan de tratamiento a implementar.

Se deben establecer dos aspectos a tener en cuenta en el momento de evaluar o analizar los riesgos: la *Probabilidad* e *Impacto*.

La **Probabilidad** puede ser medida con criterios de Frecuencia, si se ha materializado, por ejemplo: N° de veces que un riesgo ha sucedido en un tiempo determinado, o de *Factibilidad* teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

El **Impacto** se mide según el grado en que las consecuencias o efectos pueden perjudicar a la institución si se materializa el riesgo.

- **Clasificación de los riesgos**

Los riesgos pueden clasificarse en las siguientes categorías:

a) **Riesgos de cumplimiento:** Situaciones o eventos que atentan contra el cumplimiento de requisitos internos o externos de la Institución.

b) **Riesgos estratégicos:** Situaciones o eventos que atentan contra el cumplimiento de la misión y los objetivos estratégicos, en función de sus políticas o directrices institucionales.

c) **Riesgos financieros:** Situaciones o eventos que atentan contra la sostenibilidad financiera. Se relacionan con el manejo de los recursos de la Institución, la eficiencia y transparencia en el manejo de los recursos, así como con la reducción de los flujos de ingresos y/o aumento de los flujos de gastos.

d) **Riesgos de imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

e) **Riesgos operativos:** Comprende los riesgos relacionados tanto con la parte operativa como técnica de la Institución relacionados con su función.

f) **Riesgos de tecnología:** Se asocian con la capacidad de la Institución para que la tecnología disponible satisfaga las necesidades actuales y futuras de la Institución y soporten el cumplimiento de su misión.

g) **Riesgos de afectación del producto y/o servicio:** Están asociados a la calidad en la prestación de los servicios de la institución.

h) **Riesgos en la gestión de activos:** Pérdida, daño, destrucción, indisponibilidad de edificios, instalaciones, equipos e inventarios propios o de terceros.

La calificación del riesgo: se logra a través de la evaluación de la probabilidad de ocurrencia y el impacto de la materialización del riesgo. Los criterios para la calificación

son subjetivos, depende de la particularidad del riesgo y los antecedentes en cada uno de los procesos y los equipos de gestión.

- **Criterios para la calificación de la probabilidad:**

Valor de la Probabilidad	Nivel de la Probabilidad	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
3	Posible	El evento podría ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos 1 vez en los últimos año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año

Tabla 6-2: Criterios para la clasificación de probabilidad

Elaborado por: Investigador

- **Criterios para la calificación de impacto:**

Valor de Impacto	Nivel de Impacto	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.

5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Tabla 6-3: Criterios para la clasificación de impacto

Elaborado por: Investigador

- **Evaluación de los riesgos**

Teniendo en cuenta los parámetros previamente descritos de probabilidad y de impacto, se deben identificar los criterios que apliquen al riesgo identificado y realizar la calificación acorde con la Matriz de Calificación, Evaluación y Respuesta a los Riesgos. Este primer análisis de denomina riesgo inherente, donde no se tienen en cuenta los controles.

- **Matriz de calificación, evaluación y respuesta a los riesgos.**

		Consecuencia				
Probabilidad		1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastróficos
5	Casi seguro	5 Alto	10 Alto	15 Extremo	20 Extremo	25 Extremo
4	Probable	4 Moderado	8 Alto	12 Alto	16 Extremo	20 Extremo
3	Posible	3 Bajo	6 Moderado	9 Alto	12 Alto	15 Extremo
2	Improbable	2 Bajo	4 Bajo	6 Moderado	8 Alto	10 Alto
1	Raro	1 Bajo	2 Bajo	3 Bajo	4 Moderado	5 Alto

Zona no admisible del riesgo	Extremo	Requiere la atención inmediata y ser objeto de seguimiento continuo. **Tipo de Respuesta al Riesgo:** reducir o evitar el riesgo.
	Alto	Requiere la atención necesaria y recibir seguimiento periódico. **Tipo de Respuesta al Riesgo:** reducir o evitar el riesgo.
Zona admisible del riesgo	Moderado	Debe ser objeto de seguimiento semestral por parte del dueño de proceso **Tipo de Respuesta al Riesgo:** asumir el riesgo, reducir el riesgo.
	Bajo	Debe ser objeto de seguimiento por parte del dueño de proceso **Tipo de Respuesta al Riesgo:** asumir el riesgo

Tabla 6-4: Matriz de riesgo

Elaborado por: Investigador

Se cruza la calificación de probabilidad e impacto y la zona que de cómo resultado, implica identificar qué tipo de riesgo es, acorde con la siguiente clasificación:

- **Riesgos inaceptables o no admisibles: zona extrema y de riesgo alto (rojo y amarillo)** Se debe dar tratamiento a las causas que generan el riesgo. Es decir, se deben implementar controles de prevención para reducir la Probabilidad del riesgo o disminuir el impacto de los efectos; medidas de Protección para compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles, las acciones que se definan como tratamiento se deben establecer a corto plazo.
- **Riesgos importantes: (amarillo**) se deben tomar medidas para llevar los riesgos a la zona baja, fortaleciendo los controles existentes.
- **Riesgos moderados: zona moderada (verde)** se deben tomar medidas para llevar los riesgos a la zona baja, fortaleciendo los controles existentes.
- **Riesgos aceptables: zona baja (azul)** el riesgo se encuentra en un nivel que puede aceptarse sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

6.6.3.2 Seguridad física.

La seguridad física es uno de los entes clave en el modelo propuesto ya que cubre aspectos sensibles para el correcto funcionamiento de los sistemas de información.

A. Uso adecuado de los activos [ISO/IEC 27001:2005 A.7.1.3]

Todos los empleados, contratistas y usuarios por tercera parte deberían seguir las reglas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información, incluyendo:

a) Reglas para el uso del correo electrónico y de Internet (véase numeral 6.6.3.4 literal B).

b) Directrices para el uso de los dispositivos móviles, especialmente para su utilización fuera de las instalaciones de la organización (véase numeral 6.6.3.4 literal E).
c) Firmar un "**acuerdo de confidencialidad de la información**", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información (véase anexo 7).

Los empleados, contratistas y usuarios de tercera parte que utilizan o tienen acceso a los activos de la organización deberían estar conscientes de los límites que existen para el uso de la información y de los activos de la organización asociados con los servicios de procesamiento de información, así como de los recursos. Deberían ser responsables del uso que hagan de los recursos de procesamiento de información y de cualquier uso efectuado bajo su responsabilidad.

B. Implementación o actualización de recursos tecnológicos [ISO/IEC 27001:2005 A.7.1.3]

Considerando los recursos con los que cuentan las pequeñas empresas, se propone un modelo de referencia para implementar lo especificado en la ISO 27001 en pequeñas empresas. Esto no significa que los demás controles de la norma no se consideren, pero como se trata de pequeñas empresas que cuentan con recursos limitados, lo que se propone es que los demás controles se vayan implementando como plan de mejora continua de manera progresiva. La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad de la coordinación de sistemas. Así mismo, los medios de instalación de software deben ser los proporcionados por el coordinador de sistemas.

Según (Mantulak, Hernández Pérez, & Michalus, 2016), el uso apropiado de los recursos tecnológicos concedidos a los empleados y/o terceros se establece bajo los siguientes lineamientos:

a) La instalación y configuración del hardware y software en los equipos de cómputo es tarea de la coordinación de sistemas. Por lo tanto, esta coordinaciones el único ente autorizado para realizar esta tarea.

b) Los usuarios de ninguna manera estarán autorizados a modificar la configuración de las estaciones de trabajo asignadas, tales como conexiones de red, modificación de usuarios locales, cambiar el protector de pantalla corporativo, entre otros. El único ente autorizado para realizar estas modificaciones es la Coordinación de Sistemas.
c) La Coordinación de Sistemas es la encargada de definir y actualizar, periódicamente, el inventario de software y aplicaciones (ver anexo 9) permitidas para ser instaladas en los equipos de cómputo de los usuarios. De igual manera, realizar el registro y verificación del licenciamiento del respectivo software utilizado en la institución.
d) Únicamente los empleados y terceros autorizados por la Coordinación de Sistemas, previa solicitud de la dependencia que lo requiera debidamente escrita y autorizada por Gerencia General, pueden conectarse a la red inalámbrica de la institución.
e) La coordinación de sistemas es el único ente autorizado para ejecutar actividades de administración remota de equipos, servidores (véase numeral 6.6.3.4 literal C) y dispositivos de la infraestructura de procesamiento de información de pequeñas empresas.
f) La sincronización de dispositivos móviles, tales como smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la organización, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con la coordinación de sistemas y podrá llevarse a cabo sólo en dispositivos provistos por la organización, para tal fin.

C. Control de acceso físico [ISO/IEC 27001:2005 A.9.1]

Los servicios de procesamiento de información sensible o crítica deberían estar ubicados en áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad y controles de entrada adecuados. Dichas áreas deberían estar protegidas físicamente contra acceso no autorizado, daño e interferencia.

Se utilizaran perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información.
Se deberían considerar e implementar las siguientes directrices:

a) Se recomienda definir claramente los perímetros de seguridad y la ubicación dependiendo de los requisitos de seguridad de los activos dentro del perímetro.
b) Los perímetros de una edificación o un lugar que contenga servicios de procesamiento de información deberán ser robustos físicamente (es decir, no deberían existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir una intrusión); las paredes externas del sitio tendrán una construcción sólida y todas las puertas externas deberían tener protección adecuada contra el acceso no autorizado con mecanismos de control tales como barras, alarmas, relojes, etc., las puertas y ventanas deberían estar cerradas con llave cuando no están atendidas y se tendrá presente la protección externa para las ventanas, particularmente a nivel del suelo;
c) Establecer un área de recepción con personal u otros medios para controlar el acceso físico al lugar o edificación; el acceso a los sitios y edificaciones estará restringido únicamente al personal autorizado.
d) Es recomendable la instalación de sistemas adecuados de detección de intrusos y someterlos a pruebas regularmente para verificar todas las puertas externas y ventanas accesibles.
e) Los servicios de procesamiento de información dirigidos por la organización deberían estar físicamente separados de aquellos dirigidos por terceras partes.
f) Registrar la fecha y la hora de entrada y salida de todos los visitantes.
g) Controlar el acceso a áreas en donde se procesa o almacena información sensible y restringir el acceso únicamente a personas autorizadas; se deberían utilizar controles de autenticación como las tarjetas de control de acceso más el número de identificación personal (PIN) para autorizar y validar el acceso.

La protección física se puede lograr creando una o más barreras físicas alrededor de las instalaciones y los servicios de procesamiento de información de la organización. El empleo de barreras múltiples proporciona protección adicional, cuando la falla de una sola barrera no implica que la seguridad se vea comprometida inmediatamente.

D. Protección y ubicación de los equipos [ISO/IEC 27001:2005 A.9.2]

Los equipos que forman parte de la infraestructura tecnológica de las pequeñas empresas así como equipos de procesamiento y almacenamiento de datos, comunicaciones, seguridad lógica, UPS (Sistema de alimentación ininterrumpida), central telefónica, equipos de cómputo y comunicación móvil que brinden servicios de soporte de información crítica de los distintos departamentos, deben ser situados de manera adecuada para evitar daño, pérdida o robo. De la misma manera, es necesario incorporar medidas para mantener los equipos apartados de lugares que puedan ser de potencial riesgo o amenaza, como fuego, agua, polvo, vibraciones, obstrucción electromagnética, vandalismo, entre otros.

El personal que tenga acceso a los equipos que componen la infraestructura tecnológica de pequeñas empresas no puede fumar, beber o consumir algún tipo de alimento cerca de los equipos.

E. Gestión de medios removibles [ISO/IEC 27001:2005 A.10.7]

La utilización de dispositivos de almacenamiento móviles (ejem: CDs, DVDs, Flash Memory, discos duros removibles, celulares,etc), en la infraestructura de procesamiento de información, será autorizado por los usuarios cuyo perfil del cargo y funciones establecidos en el manual de funciones de la institución lo demande. La coordinación de sistemas será la responsable de establecer las medidas para garantizar que únicamente los usuarios facultados puedan hacer uso de los medios de almacenamiento removibles. De igual manera, el funcionario se responsabiliza de resguardar física y lógicamente el dispositivo con la finalidad de no exponer los datos de que éste contiene.

F. Riesgos relacionados con terceros [ISO/IEC 27001:2005 A.6.2.1]

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, es recomendable identificar los riesgos relacionados con el acceso de partes externas, para ello se deberán considerar los siguientes aspectos:

a) Los servicios de procesamiento de información a los cuales requiere acceso la parte externa;
b) El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información, por ejemplo:
    1) Acceso físico, a oficinas, recintos de computadores y gabinetes de archivos.
    2) Acceso lógico, a las bases de datos de la organización o a los sistemas de la organización.
    3) Conexión de red entre las redes de la organización y de la parte externa por ejemplo conexión permanente, acceso remoto.
    4) Si el acceso tendrá lugar en las instalaciones o fuera de ellas.
c) El valor y la sensibilidad de la información involucrada y su importancia para las operaciones del negocio.
d) Los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas.
e) El personal de la parte externa involucrado en manejar la información de la organización.
f) La forma en que se puede identificar a la organización o al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo;
g) Los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información;
h) El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a información inexacta o engañosa;
i) Las prácticas y los procedimientos para tratar los incidentes de seguridad de la información y los daños potenciales, al igual que los términos y las condiciones

para la continuación del acceso de la parte externa en el caso de un incidente de seguridad de la información;

j) Los requisitos legales y reglamentarios y otras obligaciones contractuales pertinentes a la parte externa que se deberían tener en cuenta;
k) La forma en que se podrían ver afectados los intereses de cualquier otro accionista debido a los acuerdos.

Las partes externas podrían poner en riesgo la información con una gestión inadecuada de la seguridad. Se deberían identificar y aplicar los controles para administrar el acceso de la parte externa a los servicios de procesamiento de información. Por ejemplo, si existe una necesidad especial de confidencialidad de la información, se podrían utilizar los acuerdos de no divulgación.

Las organizaciones pueden enfrentar riesgos asociados con procesos, gestión y comunicación entre las organizaciones, si se aplica un alto grado de contratación externa cuando existen varias partes externas involucradas.

6.6.3.3 Seguridad lógica

A. Control de acceso a los sistemas de información [ISO/IEC 27001:2005 A.11.1]

La coordinación de sistemas será la encargada de asignar el acceso a sistemas de información, creación o cambio/reseteo de contraseña para usuarios, y acceso a los segmentos de red en concordancia a procedimientos de autorización los cuales deben ser revisados de manera periódica por la coordinación de sistemas de la institución.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dependencia propietaria de la información (ver anexo 10), o a quien ésta defina, debiendo conceder en concordancia al grado de la información catalogada, mediante la cual se deben definir controles y privilegios de ingreso que se pueden conceder a usuarios y terceros.

Todos los usuarios ya sean internos o externos que soliciten acceso remoto a la red y a la infraestructura de la institución, sea por Internet o por otro medio, deben estar siempre autorizados.

B. Definición de roles de usuario [ISO/IEC 27001:2005 A.10.1.3]

Toda tarea en la cual los usuarios tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles establecidos en el manual de funciones de la institución así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización.
Teniendo en cuenta lo indicado en el párrafo anterior se propone el siguiente conjunto de medidas en cuanto a segregación de funciones:

- Todos los sistemas de disponibilidad crítica o media de la organización deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.
- Deben estar claramente segregadas las funciones de soporte técnico, planificadores y operadores.

C. Protección contra software malicioso [ISO/IEC 27001:2005 A.10.4]

La coordinación de sistemas de las pequeñas empresas deberán establecer medidas de prevención para que los recursos informáticos estén resguardados mediante un antivirus de licenciamiento que contenga antispam, antispyware que brinden resguardo contra código malicioso y prevención del ingreso del mismo a la red corporativa, en donde se cuente con los estándares adecuados para localizar, prevenir y recuperar eventuales fallos causados por código malicioso. Es responsabilidad de la coordinación de sistemas conceder el acceso al uso de las herramientas, así como mantenerlos permanentemente actualizados.
Teniendo en cuenta lo indicado se propone el siguiente conjunto de medidas en cuanto a protección de software malicioso:

Queda prohibido:

- Los usuarios de la organización no podrán desinstalar o inactivar aplicativos y herramientas de seguridad, de ser necesario deberán solicitar autorización al coordinador del departamento al que pertenece para que el mismo solicite a coordinación de sistemas su inhabilitación.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

D. Copias de respaldo [ISO/IEC 27001:2005 A.10.5]

La coordinación de sistemas debe garantizar que los datos especificados como sensibles por los departamentos responsables de los mismos se encuentren en la plataforma tecnológica de la institución, como servidores, dispositivos de red, equipos de trabajo, archivos de configuración de dispositivos de red y seguridad, sea protegida mediante los siguientes elementos planteados:

a) La extensión (por ejemplo respaldo completo o diferencial) y la frecuencia de los respaldos deberán reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la importancia de la operación continúan de la organización.
b) La información de respaldo tendrá un grado apropiado de protección física y consistente; los controles aplicados a los medios se deberían extender para cubrir el sitio en donde está el respaldo.
c) Es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias, cuando sea necesario.
d) Los respaldos deben estar sometidos a prueba con regularidad para garantizar que cumplen los requisitos de los planes para la continuidad del negocio. Para sistemas críticos, las disposiciones de respaldo deberían comprender toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar todo el sistema en caso de desastre.

e) Es necesario determinar el periodo de almacenamiento de la información relevante para el negocio según las necesidades del mismo, así como cualquier requisito para retener permanentemente las copias de archivos.

E. Seguridad para el intercambio de información [ISO/IEC 27001:2005 A.10.8.1]

Las pequeñas empresas han de garantizar la firma de acuerdos de confidencialidad por parte de los funcionarios, clientes y terceros que, por diferentes razones, requieran conocer o intercambiar información restringida o confidencial de la organización. En estos acuerdos quedarán especificadas las responsabilidades de cada una de las partes para el intercambio de la información. Estos acuerdos deberán firmarse antes de permitir el acceso o uso de dicha información.

Todo funcionario de la institución es responsable por proteger la confidencialidad e integridad de la información (ver anexo 11) mediante el uso de técnicas criptográficas y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad.

Los procedimientos y controles a seguir cuando se utilizan servicios de comunicación electrónica para el intercambio de información deberían considerar los siguientes elementos:

a) No dejar información sensible o crítica en los dispositivos de impresión como copiadoras, impresoras y máquinas de fácil acceso.
b) No dejar mensajes que contengan información sensible en el contestador automático ya que pueden volver a ser escuchados por personas no autorizadas,

almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación errónea;

c) Recordar al personal no registrar datos demográficos, como direcciones de correo electrónico u otra información personal, en ningún software para evitar su recolección para uso no autorizado;
d) Recordar al personal que las fotocopiadoras modernas tienen páginas de almacenamiento y caché, en caso de falla en el papel o en la transmisión, que se pueden imprimir una vez se ha solucionado la falla.
e) Además, se debería recordar al personal que no debería tener conversaciones confidenciales en lugares públicos ni oficinas abiertas, como tampoco en lugares de reunión sin paredes a prueba de sonido:

El intercambio de información se puede producir a través de la utilización de diferentes tipos de servicios de comunicación, incluyendo correo electrónico, voz y video.

El intercambio de software se puede dar a través de diferentes medios, incluyendo descargas desde Internet y adquiridas de vendedores de productos de mostrador.

Se deberá considerar las implicaciones de negocios, legales y de seguridad asociadas con el intercambio electrónico de datos, el comercio electrónico y las comunicaciones electrónicas, así como los requisitos para los controles.

La información podría verse amenazada debido a la falta de conciencia, de políticas o procedimientos sobre el uso de los servicios de intercambio de información, por ejemplo por la escucha en un teléfono móvil en un lugar público, la dirección incorrecta de un mensaje de correo electrónico, la escucha de los contestadores automáticos, el acceso no autorizado a sistemas de correo de voz de marcación.

Las operaciones del negocio podrían ser afectadas y la información podría ser comprometida si los servicios de comunicación fallan, se sobrecargan o interrumpen. La información se vería comprometida por el acceso de usuarios no autorizados.

F. Gestión de contraseñas de usuario [ISO/IEC 27001:2005 A.11.2.3]

Todos los medios de información sensible tendrán establecidos privilegios de acceso a usuarios en base a roles y perfiles de los funcionarios que así lo requieran, para el

desenvolvimiento en el desarrollo de sus actividades, determinados y aprobados por las áreas de negocio en concordancia con la coordinación de sistemas.

Todo usuario o agente externo que solicite acceso a los sistemas de información de la institución debe estar previamente autorizado; para acceder a los sistemas deberá hacer uso de un usuario y contraseña previamente asignado por la coordinación de sistemas. El personal externo debe comprometerse en hacer un buen uso de las credenciales de acceso concedidas, y garantizar que utiliza contraseñas con base a las condiciones de seguridad establecidas en forma y contenido, no usar contraseñas de fácil adivinación.

El proceso incluirá los siguientes requisitos:

a) El convenio de confidencialidad que firme el empleado deberá contener cláusulas que señalen que la seguridad de sus contraseñas es responsabilidad de cada uno de los usuarios.
b) Las contraseñas que se les otorgue a los usuarios inicialmente, será una contraseña temporal para que cuando ingresen a los sistemas de información estos les obliguen a cambiarlas inmediatamente.
c) Las contraseñas nunca se deberían ser almacenadas en el computador en un formato no protegido.
d) La coordinación de sistemas deberá cambiar las contraseñas predeterminadas por los proveedores de hardware y software inmediatamente luego de su instalación.

Según el caso, es recomendable considerar otras tecnologías disponibles para la identificación y autenticación del usuario como equipos de verificación de huella digital o firma así como el uso de tokens de autenticación, (tarjetas inteligentes).

G. Escritorio y pantalla limpia [ISO/IEC 27001:2005 A.11.2.4]

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios de las pequeñas empresas deberán mantener la información restringida o confidencial que se encuentre a su cargo bajo llave cuando sus puestos de trabajo se

encuentren desatendidos o en horas no laborales. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata.
Todos los usuarios son responsables de verificar que su estación de trabajo se bloquee al momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Al culminar el horario de labores el usuario deberá cerrar las aplicaciones abiertas e inmediatamente apagar el equipo.
Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

6.6.3.4 Seguridad ligada al personal.

A. Acuerdos de confidencialidad. [ISO/IEC 27001:2005 A.6.1.5]

Todos los funcionarios de las pequeñas empresas y/o terceros involucrados en su gestión deberán firmar los convenios de confidencialidad establecidos por la institución, mismos que se comprometen a hacer buen uso de la información suministrada (ver cláusula 2 del anexo 7) por la organización.
Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de pequeñas empresas a personas o entidades externas.
Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

- **Análisis de acuerdos de confidencialidad**

Un aspecto importante en la definición del modelo es la especificación del acuerdo de confidencialidad. A continuación se incluye el análisis realizado al respecto, el que permitió establecer una pauta para elegir la mejor opción a ser aplicada en una pequeña empresa y que fue validada en el ámbito de la empresa del caso de estudio.

Tipos de acuerdos de confidencialidad		
	Acuerdo de confidencialidad para Empleados	**Acuerdo de confidencialidad para terceros**
Partes afectadas	Personas naturales a los que afecte el contrato de confidencialidad.	Personas, naturales o jurídicas, a las cuales afecta el contrato de confidencialidad.
Definición de qué es confidencial	La definición de lo que es confidencial se encuentra claramente definido en el contrato.	La definición de "confidencial" hay que estipularlo previo la firma del contrato
Excepciones	La información es de conocimiento público; es decir, no fuera la parte receptora la causa de la divulgación de la información. Fuese divulgada masivamente sin limitación alguna por la parte contratante. Fuese creada completa e independientemente por la parte receptora, mismas que deben ser comprobadas de acuerdo a sus archivos debidamente suministrados.	Que previa a su divulgación fuese conocida por la parte receptora, libre de cualquier obligación de mantenerla confidencial, según se evidencie por documentación en su posesión; Que sea desarrollada o elaborada de manera independiente por o de parte del receptor o legalmente recibida, libre de restricciones, de otra fuente con derecho a divulgarla; Que sea o llegue a ser del dominio público, sin mediar incumplimiento de este convenio por la parte receptora; y Que se reciba de un tercero sin que esa divulgación quebrante o viole una obligación de confidencialidad.
Sanciones	Autorizara a la otra parte a solicitar por la vía legal que considere procedente, la compensación de los daños y perjuicios ocasionados.	La parte receptora será responsable por los daños y perjuicios si algún incumplimiento llegase suceder.

Plazo	Las partes pactan mantener el convenio de confidencialidad, incluso culminadas sus relaciones comerciales.	Indefinida mientras exista relación comercial entre ambas partes

Tabla 6-5: Tabla comparativa tipos de contrato de confidencialidad

Elaborado por: Investigador

El estudio comparativo de los tipos de contratos de confidencialidad ha permitido constatar la existencia de un cierto número de coincidencias y de divergencias entre ellos, lo que permitirá elegir la mejor opción que dependiendo del caso podría ser utilizada en una pequeña empresa.

B. Gestión de talento humano [ISO/IEC 27001:2005 A.8, A.8.1, A.8.2]

Antes de la contratación laboral, el personal contratado para laborar donde se tenga acceso a información sensible o confidencial, deberá ser analizado bajo los parámetros específicos de seguridad definidos para el perfil, firmar el acuerdo de confidencialidad, asegurando que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades, sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

Las funciones y responsabilidades deberían incluir los requisitos:

a) Implementar y actuar de acuerdo con las políticas de seguridad de la información de la organización.
b) Proteger los activos contra acceso, divulgación, modificación, destrucción o interferencia no autorizados.
c) Informar los eventos de seguridad, los eventos potenciales u otros riesgos de seguridad para la organización.
d) Que todos los empleados, contratistas y usuarios de terceras partes que tengan acceso a información sensible deberían firmar un acuerdo de confidencialidad o no-divulgación antes de tener acceso a los servicios de procesamiento de información;

e) Deberá dictar capacitaciones continuas en temas de seguridad de la información, con especial atención a aquellas personas que tengan acceso a datos sensibles de la organización.

C. Culminación del contrato laboral [ISO/IEC 27001:2005 A.8.3; A.8.3.1]

Para los usuarios o terceras personas que culminen sus labores o servicios para con la institución, deberán realizar el proceso cumpliendo los siguientes requisitos:

- La coordinación de Talento Humano será la responsable de realizar el proceso culminación laboral junto con el jefe inmediato de la persona, para manejar el punto de vista para seguridad de los procedimientos importantes.
- Es responsabilidad de los ex empleados, devolver los activos de la organización asignados a su cargo posterior a la culminación de su relación laboral, mediante la firma del acta de devolución de activos fijos (ver anexo 8).
- En casos que el equipo pertenezca al empleado o contratista, la coordinación de sistemas deberá garantizar la transferencia y eliminación de la información institucional que contenga el mismo, antes del retiro del empleado.
- Talento humano informara a todo el personal y contratistas los cambios de personal que existan en la empresa.
- La coordinación de sistemas deberá eliminar los derechos de acceso al ex empleado, luego de que talento humano lo comunique, para proteger la confidencialidad e integridad de la información.
- Si el empleado cambia de cargo, la coordinación de sistemas deberá hacer las configuraciones necesarias para el nuevo cargo, limitando lo que no corresponda con las nuevas funciones para garantizar la segregación de funciones.

6.6.3.5 Comunicación y Operaciones

A. Acceso a internet [ISO/IEC 27001:2005 A.7.1.3]

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de pequeñas empresas. Por tanto, el uso apropiado de este recurso debe ser monitoreado en todo momento, contemplando los siguientes lineamientos:

En concordancia a lo que estipula la cláusula 2 (anexo 7) del convenio de confidencialidad el empleado utilizara los recursos tecnológicos de la Institución, con ética, reserva y profesionalismo, por tanto queda prohibido:

a) Acceder a páginas web que presenten contenido relacionado con pornografía, alcohol, drogas, hacking, webproxys y cualquier página que vaya en contra de la ética moral, leyes vigentes y políticas establecidas en la institución.
b) El uso de youtube, spotify o similares para escuchar música en línea (ver cláusula 2 del anexo 7).
c) El uso de mensajería instantánea o servicios web como Facebook, Skype, whatsapp-web y otros afines, que tengan como objetivo la creación de agrupaciones para el intercambio información, o en otro caso para fines diferentes a las actividades asignadas.
d) Intercambiar información confidencial sin autorización previa de clientes o empleados, con personas ajenas a la institución.
e) Descargar, usar o instalar software para distracción personal como juegos, música, películas, imágenes, etc. Productos que de alguna manera atenten contra la integridad, disponibilidad y confidencialidad de la infraestructura tecnológica institucional. Si la descarga de este tipo de software es necesario para realizar actividades laborales, se deberá solicitar autorización por el Jefe inmediato a la coordinación de sistemas.
f) La coordinación de sistemas deberá implementar herramientas de seguridad perimetral (proxi, firewall) en concordancia a las capacidades de económicas de la institución, que les permita monitorear de manera permanente los períodos de navegación y acceso a páginas por parte de los

usuarios que utilicen la red institucional.

g) Los funcionarios serán responsables por dar un uso apropiado a este recurso y de ninguna manera podrán utilizarlo para realizar prácticas indebidas que atenten a terceros.
h) Los usuarios o terceros, no deberán tomar el nombre de la institución para realizar encuestas, foros o actividades similares, salvo autorización de gerencia general.

El acceso a Internet que no se encuentre estipulado dentro de las restricciones anteriores, estará autorizado siempre y cuando se utilice este recurso de forma ética, razonable, responsable, que no afecte al rendimiento productivo ni la protección de la información institucional.

B. Correo electrónico [ISO/IEC 27001:2005 A.7.1.3]

Todos los empleados que posean una cuenta de correo electrónico institucional deberán seguir las reglas para el uso aceptable del correo institucional, incluyendo:

a) El usuario al que se le asigne una cuenta de correo electrónico debe usarla únicamente para el ejercicio de las funciones asignadas en la institución.
b) La información contenida en el buzón de correo electrónico es propiedad de la institución y cada funcionario se hace responsable de la información que contiene. Así mismo, se compromete a mantener únicamente mensajes relacionados con el desarrollo de sus funciones.
c) La capacidad de almacenamiento para los buzones de correo será definida por la coordinación de sistemas en concordancia con las necesidades de los usuarios y previa autorización del Jefe de la dependencia correspondiente.
d) La capacidad para el envío y recepción de correos, su contenido y propiedades serán definidos por la coordinación de sistemas.
e) Los correos institucionales serán utilizados exclusivamente para el envío de información corporativa. Así mismo, las cuentas de correo personales no deberán ser utilizadas este fin.

f) El envío masivo de mensajes publicitarios corporativos lo realizara únicamente el departamento de marketing. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, éste debe ser canalizado a través del departamento de marketing.
g) De ser el caso, la información que requiera ser trasladada fuera de la institución, debe ser enviada usando medidas de seguridad que permitan mantener en formato no editable para garantizar la integridad de la misma, utilizando herramientas proporcionadas por la Coordinación de Sistemas.
h) Los correos institucionales enviados deben mantener el esquema de formato e imagen corporativa determinado por gerencia general.

Queda prohibido:

- Enviar cadenas de mensajes con contenido publicitario, político, religioso, racista, pornográfico, o cualquier tipo de mensajes que atenten contra la honra y el normal desempeño de las actividades del personal
- Emplear el correo corporativo como punto de contacto en web sociales, tales como *Facebook, twitter, Instagram* entre otros, o cualquier página que no tenga relación con las actividades laborales.
- Bajo ninguna circunstancia enviar correos que contengan archivos con extensiones ejecutables.
- En caso de requerir el envío de archivos de audio y video, el usuario deberá solicitar autorización a su dirección respectiva y a la Coordinación de Sistemas.
- La configuración del correo electrónico en celulares, ipad, portátiles y equipos tecnológicos en general que no sean propiedad de la empresa.

C. Segregación De Redes [ISO/IEC 27001:2005 A.11.4.5]

La plataforma de red que soporta los sistemas de Información debe quedar dividida en segmentos físicos y lógicos, por ejemplo, dominios de red internos de la organización y dominios de red

externos, cada uno protegido por un perímetro de seguridad definido. Se puede aplicar un conjunto graduado de controles en diferentes dominios lógicos de red para separar aún más los entornos de seguridad de la red, por ejemplo los sistemas de acceso público, las redes internas y los activos críticos.

Implementar un perímetro de red instalando una puerta de enlace (gateway) seguro entre las redes que se van a interconectar para controlar el acceso y el flujo de información a través de los dos dominios. Esta puerta de enlace (gateway) se debe configurar para filtrar el tráfico entre estos dominios y para bloquear el acceso no autorizado. Un ejemplo de este tipo de puerta de enlace (gateway) es lo que se conoce comúnmente como barrera de fuego(firewall).

Los criterios para separar las redes en dominios deberán tener en cuenta los costos relativos y el impacto en el desempeño por la incorporación de tecnología conveniente de puerta de enlace (gateway) o de enrutamiento de red

6.6.3.6 Mantenimiento y administración.

La política de seguridad genérica, resultante de este modelo, debe establecer períodos de revisión de su procedimiento abierto a revisiones extraordinarias motivadas por una necesidad de mejora, aplicando el Principio del Kaizen, es decir, mejorar lo mejorado.

Otro mecanismo de gran importancia por su carácter totalmente práctico, para el mantenimiento de las medidas de protección planteadas y que, sin embargo, es olvidado con frecuencia, son las pruebas de los planes de contingencia (ver anexo 5), de recuperación de copias de respaldo de datos, y de respuesta a incidentes de seguridad.

Se debe tener presente los factores de éxito para el mantenimiento del Modelo de Gestión de Seguridad de la Información propuesto: **la prevención**, que puede concretarse en acciones como: la recolección, análisis y revisión de los registros de actividad (logs), y la reconfiguración de equipos, herramientas y, en el límite, de la arquitectura de la red (ubicación de los proxys, etc.), atendiendo a los avisos de vulnerabilidades recibidos para así evitar los riesgos asociados.

6.6.3.7 Socialización del modelo

Es fundamental que todos los involucrados conozcan el qué y para qué de este modelo de gestión, la organización asegurará que el personal tiene conciencia de la necesidad e importancia de las actividades de seguridad informática que le corresponde realizar y cómo ellas contribuyen al logro de los objetivos del modelo propuesto.

Las actividades para la socialización y sensibilización incluyen:

1. Concienciar al personal de la importancia que el modelo tiene para la organización.
2. Garantizar la divulgación, el conocimiento y comprensión de las políticas de seguridad que se implementan.
3. Capacitar a los usuarios en las medidas y procedimientos que se van a implantar.
4. Lograr que el personal esté consciente de los roles a cumplir dentro del modelo.
5. Incentivos de participación y concienciación de la utilidad de este modelo.

Durante la socialización del modelo es necesario precisar la aplicación de cada uno de los controles mencionados anteriormente en las áreas que los requieren y que los mismos cubran los riesgos que para ellos fueron identificados. En este sentido, la participación de los jefes de áreas es determinante, pues corresponde a ellos refrendar que los controles que se establezcan y den plena respuesta a los requerimientos de protección de cada área en particular.

El modelo propuesto se apoya de los estándares de la norma ISO 27001 que pueden ser aplicados en una pequeña empresa, su principal aporte es ser un facilitador en la implementación y/o aplicación de la seguridad de la información para TIC en cualquier tipo de organización de este tipo.

La estructura que presenta el modelo se basa sobre la implementación práctica y concreta relacionada con las actividades que permitan dar seguridad a la información que manejan las pequeñas empresas, la cual, en base a sus propias necesidades, lineamientos y perspectivas de negocio, busca mantener su información asegurada.

Otro aspecto importante que aporta este modelo, es que, por su presentación simple puede ser implementada sin mayor dificultad en cualquier tipo de organización considerada

como pequeña empresa, de manera que ella logre asegurar la información en conformidad a la realidad de TIC que disponga.

En la implementación del modelo se debe tener conocimiento de las funciones, tareas, actividades y diseño relacionadas con cada una de las etapas, por lo cual, se enfatiza en el rol de la ISO 27001, ya que con su aporte la organización podrá estructurar de forma adecuada su seguridad.

Los estándares presentados en el modelo propuesto, pretende ser una solución y aporte en la implementación de la seguridad de la información de cualquier pequeña empresa. El modelo no entrega documentos desarrollados (procedimientos, instructivos), sino que sienta las bases para su desarrollo. Esto se justifica en que cada empresa u organización tiene sus propios entornos y realidades, por lo cual, el desarrollo acabado de este tipo de implementaciones requiere de un detalle superior que escapa al alcance de este estudio.

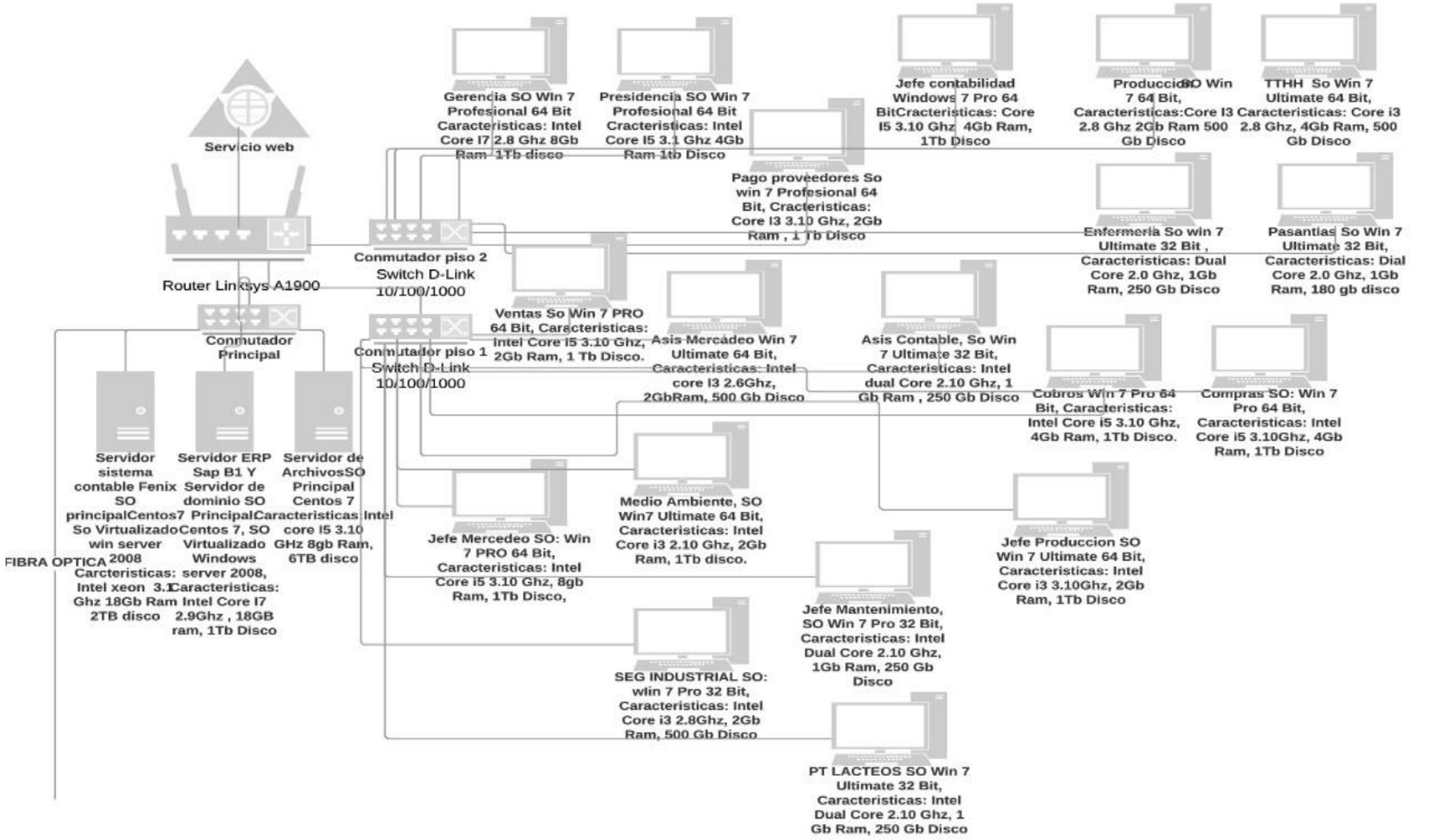
6.6.4 Metodología, Modelo Operativo.

Con el interés de dar cumplimiento al tercer objetivo de la propuesta, se incluye a continuación lo referente a la aplicación y validación del modelo propuesto en el contexto de la pequeña empresa Pasteurizadora El Ranchito, como caso de estudio que permitió validar los resultados obtenidos.

6.6.4.1 Descripción del caso de estudio

Levantamiento de la información

Pasteurizadora el Ranchito fue fundada en 1981. Desde entonces ha elaborado productos lácteos y sus derivados. La institución se encuentra ubicada en la provincia de Cotopaxi, específicamente en el Cantón Salcedo Panamericana Norte Km 2 ½ vía Salcedo Latacunga. Su estructura de red se detalla a continuación:


Servicio web
Router Linksys A1900
Conmutador Principal
FIBRA OPTICA
Servidor sistema contable Fenix SO principal So Virtualizado win server 2008 Carcteristicas: Intel xeon 3.1 Ghz 18Gb Ram 2TB disco
Servidor ERP Sap B1 Y Servidor de dominio SO principal Centos7 Centos 7, SO Virtualizado Windows server 2008, Caracteristicas: Intel Core I7 2.9Ghz , 18GB ram, 1Tb Disco
Servidor de Archivos SO Principal Centos 7 Caracteristicas Intel core I5 3.10 GHz 8gb Ram, 6TB disco
Conmutador piso 2 Switch D-Link 10/100/1000
Conmutador piso 1 Switch D-Link 10/100/1000
Gerencia SO Win 7 Profesional 64 Bit Caracteristicas: Intel Core I7 2.8 Ghz 8Gb Ram 1Tb disco
Presidencia SO Win 7 Profesional 64 Bit Cracteristicas: Intel Core I5 3.1 Ghz 4Gb Ram 1tb Disco
Jefe contabilidad Windows 7 Pro 64 BitCracteristicas: Core I5 3.10 Ghz 4Gb Ram, 1Tb Disco
Produccion SO Win 7 64 Bit, Caracteristicas:Core I3 2.8 Ghz 2Gb Ram 500 Gb Disco
TTHH So Win 7 Ultimate 64 Bit, Caracteristicas: Core i3 2.8 Ghz, 4Gb Ram, 500 Gb Disco
Pago proveedores So win 7 Profesional 64 Bit, Cracteristicas: Core I3 3.10 Ghz, 2Gb Ram , 1 Tb Disco
Enfermeria So win 7 Ultimate 32 Bit , Caracteristicas: Dual Core 2.0 Ghz, 1Gb Ram, 250 Gb Disco
Pasantias So Win 7 Ultimate 32 Bit, Caracteristicas: Dial Core 2.0 Ghz, 1Gb Ram, 180 gb disco
Ventas So Win 7 PRO 64 Bit, Caracteristicas: Intel Core I5 3.10 Ghz, 2Gb Ram, 1 Tb Disco.
Asis Mercadeo Win 7 Ultimate 64 Bit, Caracteristicas: Intel core I3 2.6Ghz, 2GbRam, 500 Gb Disco
Asis Contable, So Win 7 Ultimate 32 Bit, Caracteristicas: Intel dual Core 2.10 Ghz, 1 Gb Ram , 250 Gb Disco
Cobros Win 7 Pro 64 Bit, Caracteristicas: Intel Core i5 3.10 Ghz, 4Gb Ram, 1Tb Disco.
Compras SO: Win 7 Pro 64 Bit, Caracteristicas: Intel Core i5 3.10Ghz, 4Gb Ram, 1Tb Disco
Jefe Mercedeo SO: Win 7 PRO 64 Bit, Caracteristicas: Intel Core i5 3.10 Ghz, 8gb Ram, 1Tb Disco,
Medio Ambiente, SO Win7 Ultimate 64 Bit, Caracteristicas: Intel Core i3 2.10 Ghz, 2Gb Ram, 1Tb disco.
Jefe Produccion SO Win 7 Ultimate 64 Bit, Caracteristicas: Intel Core i3 3.10Ghz, 2Gb Ram, 1Tb Disco
Jefe Mantenimiento, SO Win 7 Pro 32 Bit, Caracteristicas: Intel Dual Core 2.10 Ghz, 1Gb Ram, 250 Gb Disco
SEG INDUSTRIAL SO: wlin 7 Pro 32 Bit, Caracteristicas: Intel Core i3 2.8Ghz, 2Gb Ram, 500 Gb Disco
PT LACTEOS SO Win 7 Ultimate 32 Bit, Caracteristicas: Intel Dual Core 2.10 Ghz, 1 Gb Ram, 250 Gb Disco

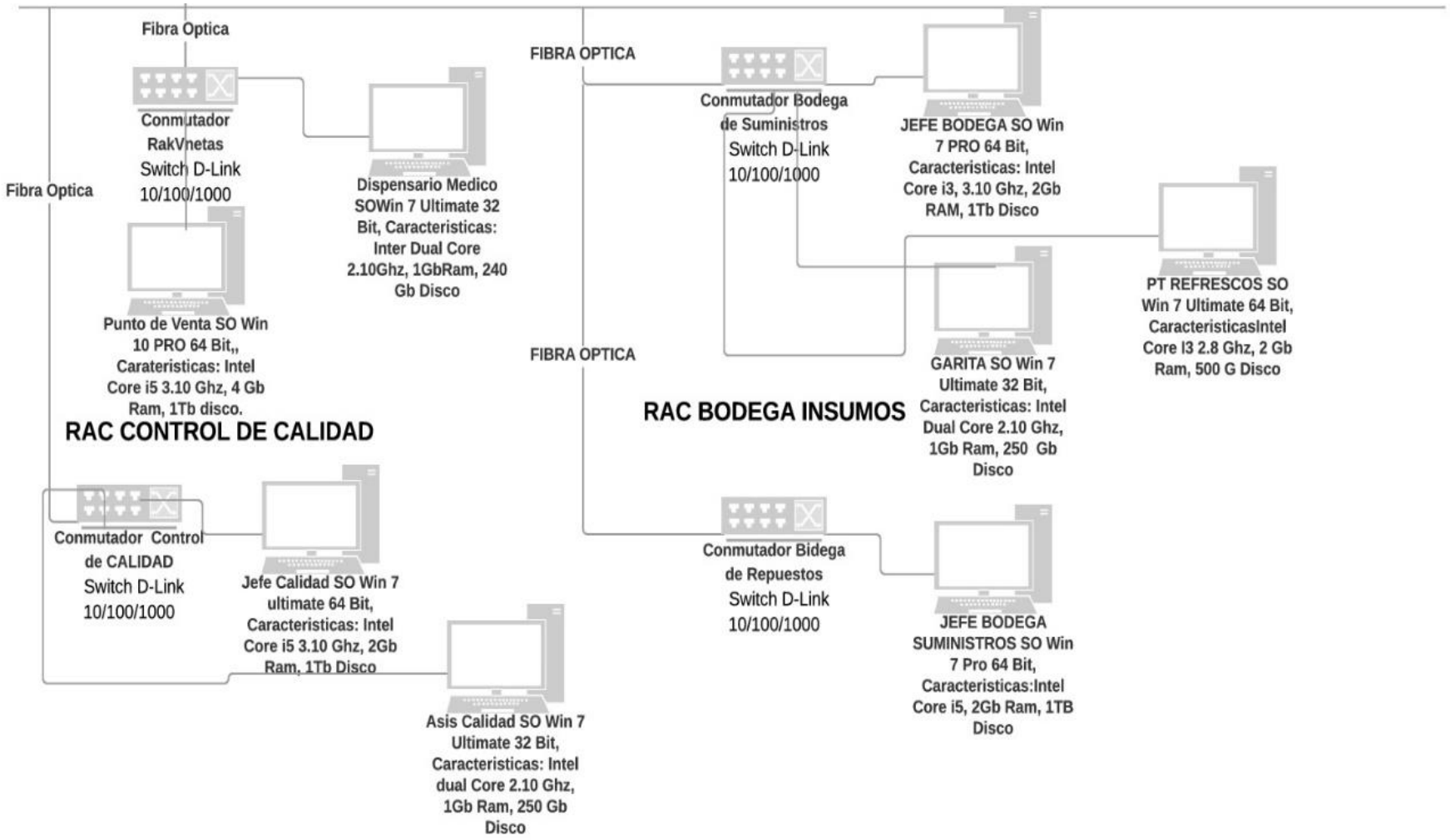


Ilustración 6-4:Diagrama de Red

Elaborado por: Investigador

Según lo descrito en el diagrama anterior, del total de equipos se puede identificar los equipos según el SO que maneja.

Sistema Operativo	**Num equipos**
Centos 7	3
Windows server 2008	2
Windows 7 Profesional 64 Bit	12
Windows 7 Profesional 32 Bit	2
Windows 7 Ultimate 64 Bit	7
Windows 7 Ultimate 32 Bit	4
Total	**30**

Tabla 6-6: Equipos según SO

Elaborado por: Investigador

El Software contable y de escritorio que es utilizado en la organización.

Software contable:

- Fenix Pro
- ERP SAP B1

Software utilitario:

- Office 2010, 2013
- Eset Nod32
- Skype
- Dropbox
- Open VPN
- Software Para el control de pesas

Según el Hardware:

Hardware	**Num equipos**
Intel Xeon	1
Intel Core i7	2
Intel Core I5	10
Intel Core I3	9
Intel Dual Core	8
Total	30

Tabla 6-7: Equipos según hardware

Elaborado por: Investigador

Plano Distribución de la empresa.

Este plano es una ilustración para graficar la empresa y sus procesos de negocio:

- **Gerencia:** Es el Representante Legal de la Sociedad y tendrá a su cargo la dirección y la administración de los negocios sociales, deberá velar por el cumplimiento de todos los requisitos legales que afecten los negocios y operaciones de ésta.
- **Contabilidad:** Encargada de la administración y control de los recursos financieros que de la Institución.
- **Marketing:** Posee la importante función de manejar y coordinar estrategias de venta. Además está encargado de satisfacer los requerimientos y necesidades del cliente.
- **Control de calidad:** Se ocupa de asegurar el cumplimiento de la política de calidad de la institución. Es decir, verifica que el proceso de producción así como el producto final se cumpla dentro de los plazos previstos, con los recursos que han sido asignados y la calidad e inocuidad del producto terminado.
- **Seguridad Industrial:** Garantiza y protege la salud de las personas, controlando las condiciones ambientales de trabajo que puedan producir enferme dades y lesiones temporales o permanentes, sobrevenidas en el curso con ocasión del trabajo. Asimismo, garantizar las operaciones y las medidas adecuadas en el uso de las maquinarias, instrumentos y materiales de trabajo para controlar el riesgo. Igualmente
- **Medio Ambiente:** Encargado de administrar las herramientas y metodológicas para las empresas en términos de evitar conflictos socio – ambientales “licencia social de la empresa”, así como brindar una imagen respetuosa del ambiente.
- **Producción:** Es el área que tiene como función principal transformar los recursos o insumos en el producto final que llegará al cliente.

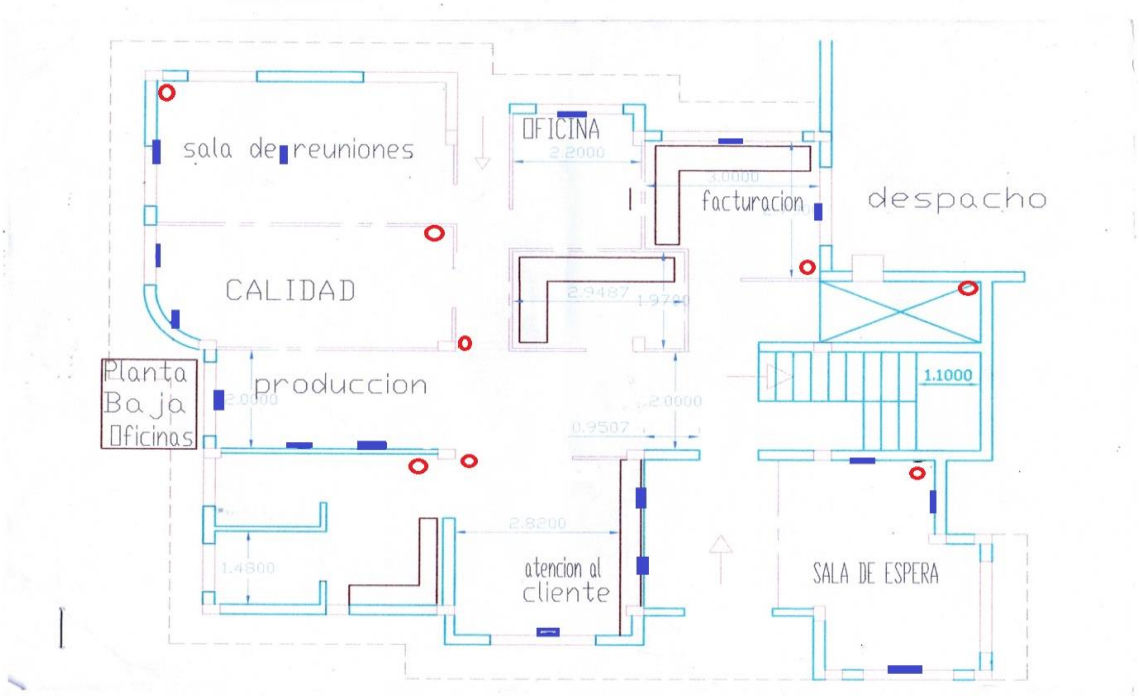


Ilustración 6-5: Plano Distribución de la empresa piso 1

Elaborado por: Investigador

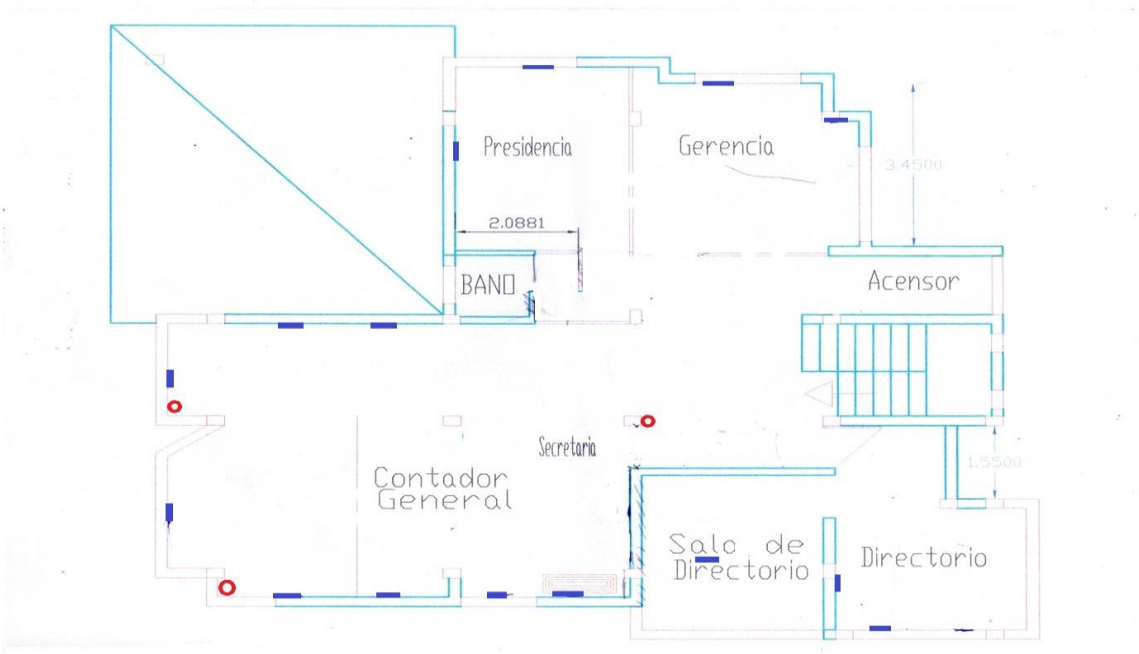


Ilustración 6--6 Plano Distribución de la empresa piso 2

Elaborado por: Investigador

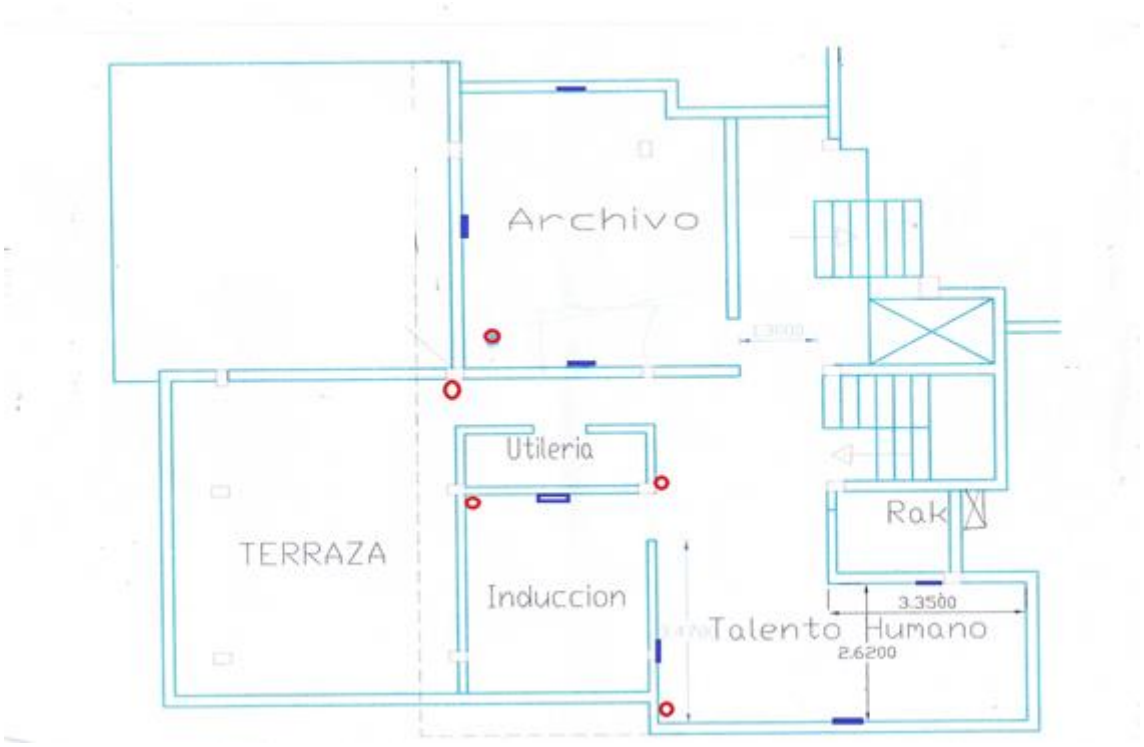


Ilustración 6-7: Plano Distribución de la empresa piso 3

Elaborado por: Investigador

Diagrama de Procesos

Ilustración 6--8: Diagrama de procesos

Elaborado por: Investigador

Organigrama

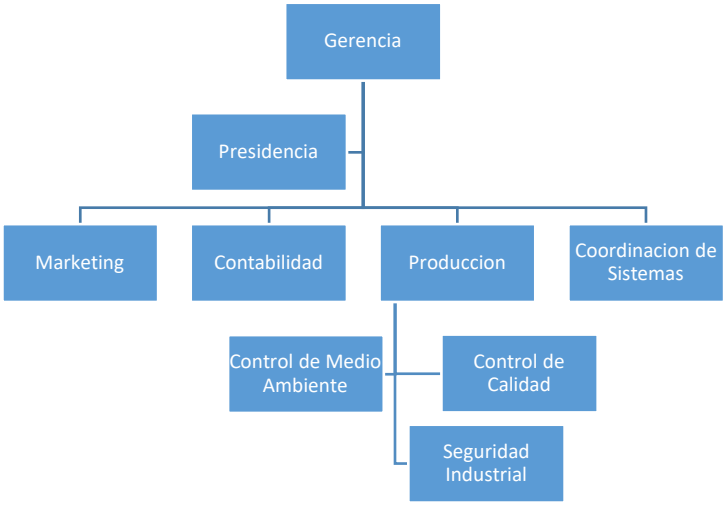


Ilustración 6-9: Organigrama Institucional

Elaborado por: Investigador

Responsabilidades

La gerencia general de Pasteurizadora el Ranchito tuvo el compromiso de implementar el presente modelo de gestión de seguridad de la información, dentro de su infraestructura tecnológica, así como de velar por ejecución de dicha política por parte de su equipo de trabajo.

El modelo de Seguridad de la Información, se aplicó (y aplica) de manera obligatoria para todo el personal de la institución, de todos los departamentos y en todos los niveles de tareas que se desempeñan.

La Coordinación de Sistemas propuso a la alta dirección de Pasteurizadora El Ranchito, la presente metodología, la cual está enfocada en la seguridad de la información para las pequeñas empresas, para ello conjuga, por una parte, las necesidades de cumplimiento y desarrollo de un modelo de gestión de la seguridad de la información, según estándares internacionales y por otra, la obtención de resultados a corto plazo para disminuir el riesgo

alto inicial que estas organizaciones están asumiendo, proporcionando resultados rápidos a la alta dirección. Para su respectiva aprobación,

- El coordinador de Sistemas será el encargado de promover la implementación y cumplimiento de la presente Política, así como de realizar actividades relativas a la seguridad de los sistemas informáticos de la institución, incluyendo la supervisión y llevar a cabo los aspectos a los temas tratados en la presente Política. Deberá implementar y supervisar el cumplimiento de las políticas, procedimientos y prácticas definidas en el marco de ésta política.

- Los Propietarios de la Información (desde el punto de vista técnico no jurídico)**,** son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
- El Responsable del Talento Humano, será el encargado de difundir al personal que ingresa a la institución, las obligaciones que debe cumplir respecto a las normas establecidas en la Política de Seguridad de la Información, así como procedimientos y prácticas que de ella surjan. Así mismo, tendrá a su cago la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de Confidencialidad y las tareas de capacitación continua en materia de seguridad.
- El Responsable del Área Legal verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la organización con sus empleados y con terceros. Así mismo, asesorará en materia legal a la organización, en lo que se refiere a la seguridad de la información.
- Los usuarios de la información y de los sistemas utilizados para su procesamiento, son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de la Seguridad de la Información vigente.
- El responsable de gestión de calidad, es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y

medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

6.6.5 Aplicación del modelo propuesto en el ámbito del caso de estudio

Estos procedimientos están diseñados para la empresa de estudio, misma que tendrá que tener el formato del encabezado, con la codificación definida y la hoja de control de distribución y cambios definidos en el procedimiento de control de documentos.

A. Procedimiento para realizar inventario de activos de información.

Objetivo

Establecer los lineamientos para la adecuada identificación y clasificación de activos de información que genere, obtenga, adquiera, transforme o controle Pasteurizadora el Ranchito

Responsables

- **Jefe de Área:** encargado de determinar y clasificar los activos de información relevantes para ser resguardados.
- **Coordinador de sistemas:** encargado ejecutar el proceso de inventario de información.

Contenido.

El registro de activos de información de los procesos de pasteurizadora el Ranchito se realiza mediante el formato del anexo 9 (registro de Activos de Información).

Etapas para la identificación de activos de información:

Las etapas descritas a continuación hacen referencia a la metodología utilizada para el registro de activos de información en la entidad:

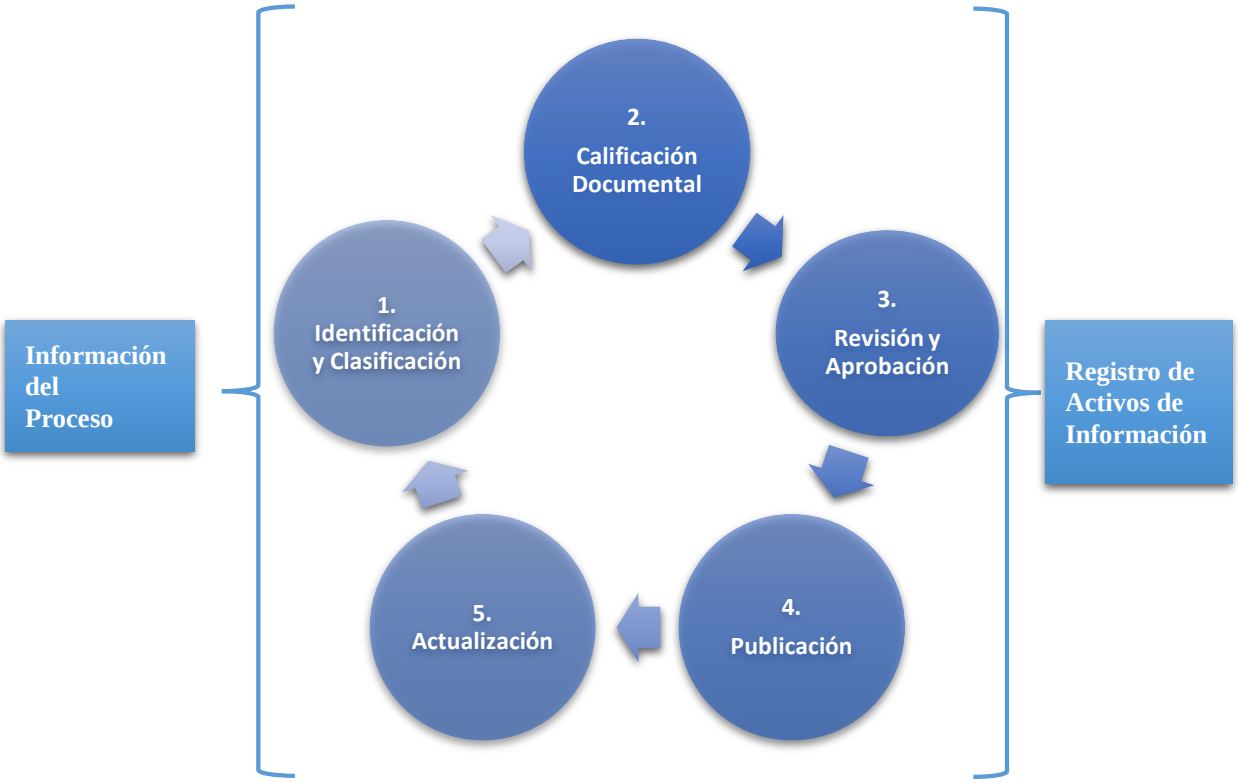


Ilustración 6-10: Etapas para la identificación de Activos de Información

Elaborado por: Investigador

1.- Identificación y Clasificación: la coordinación de sistemas realiza la identificación y clasificación de los activos de información de la entidad conjuntamente con los jefes de área a quien ellos designen, con el fin de valorarlos y protegerlos adecuadamente teniendo en cuenta los cambios en la normatividad vigente, en el mapa de procesos o en la estructura organizacional de Pasteurizadora el Ranchito.

2.- Calificación Documental: la calificación documental de los activos de información busca la adecuada custodia de los mismos

3.- Revisión y Aprobación: una vez se finaliza el ejercicio de identificación y clasificación de activos de información según el formato estipulado en el anexo 9, la coordinación de sistemas, mediante memorando envía a los líderes de procesos el registro de activos de información de los procesos que tiene a cargo para su respectiva revisión y aprobación.

4.- Publicación: Una vez aprobados los activos de información, la coordinación de sistemas, consolida los activos de información y los envía mediante memorando a los líderes de proceso respectivo.

5.- Actualización: anualmente la coordinación de sistemas actualizara el registro de activos de información conjuntamente con un representante del departamento contable.

B. Procedimiento para realizar análisis de riesgos.

Objetivo

Definir la metodología para la identificación de riesgos de Seguridad de la Información en los procesos de la entidad, con el propósito de identificar y documentar los factores que pueden afectar la confidencialidad, integridad y disponibilidad de la información de pasteurizadora el ranchito

Responsables

Todos los empleados de la institución, deben conocer sus procesos para que puedan identificar y sus riesgos.

Contenido.

La información de pasteurizadora el ranchito es crucial para el desarrollo de su objeto institucional. Es por ello que debe ser protegida de cualquier posibilidad de ocurrencia de eventos de riesgo de seguridad de la información y que pudiese significar un impacto indeseado generando una consecuencia negativa para el normal progreso de las actividades de la institución.

Para la identificación, análisis y valoración de los riesgos de Seguridad de la Información, es necesario identificar a los líderes del proceso sobre el cual se vaya a realizar el análisis de riesgos, quienes son definidos por los responsables de la información con base en la oficina o dependencia productora, quienes a su vez son los responsables del tratamiento de los riesgos de seguridad identificados.

Los líderes del proceso, con el acompañamiento y apoyo de la coordinación de sistemas de la Entidad, realizan la identificación de riesgos de Seguridad de la Información, los cuales quedan registrados en el formato del anexo 13 **Matriz de Riesgos y oportunidades**, el formato contiene las siguientes secciones:

- **Proceso:** Hace relación al proceso al cual se le administrará los riesgos.
- **Riesgo:** posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la Institución y le impidan el logro de sus objetivos.
- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Probabilidad:** entendida como la posibilidad de ocurrencia del riesgo; ésta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: No. de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.
- **Evaluación del Riesgo:** Resultado obtenido en la matriz de calificación, evaluación y respuesta a los riesgos teniendo en consideración la probabilidad y el impacto de estos.

- **Controles existentes:** Especificar cuál es el control que la Institución tiene implementado para combatir, minimizar o prevenir el riesgo.
- **Valoración del Riesgo:** Es el resultado de determinar la vulnerabilidad de la Institución al riesgo, luego de confrontar la evaluación del riesgo con los controles existentes.
- **Opciones de Manejo:** opciones de respuesta ante los riesgos tendientes a evitar, reducir, dispersar o transferir el riesgo; o asumir el riesgo.
- **Acciones:** es la aplicación concreta de las opciones de manejo del riesgo que entrarán a prevenir o a reducir el riesgo y harán parte del plan de tratamiento del riesgo.
- **Plan de tratamiento:** Los planes de tratamiento son el conjunto de actividades (acciones) encaminadas a prevenir y/o mitigar el riesgo, las cuales comprenden su correspondiente descripción, fechas de inicio, fechas de ejecución, seguimiento y responsables.

Monitoreo y revisión

Es necesario monitorear continuamente los riesgos, la efectividad del plan de tratamiento, las estrategias y el sistema de administración que se establece para controlar la implementación. Los riesgos y la efectividad de las medidas de control necesitan ser revisadas constantemente para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos, la aparición de riesgos remanentes. Es importante tener en cuenta que pocos riesgos permanecen estáticos.

Es esencial una revisión sobre la marcha para asegurar que el plan de administración mantiene su relevancia. Pueden cambiar los factores que podrían afectar las probabilidades y consecuencias de un resultado, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento. En consecuencia, es necesario repetir regularmente el ciclo de administración de riesgos.

El seguimiento es una parte integral del plan de tratamiento de la administración de riesgos; la periodicidad de la revisión de todos los componentes de la administración de riesgos lo determinaran al interior de cada equipo de gestión, administrador de sus riesgos.

Evaluación de la gestión de riesgos

La evaluación de la efectiva gestión del riesgo se puede evidenciar a través de:

- El aumento del número de controles existentes.
- Los resultados de la evaluación de efectividad de los controles.
- La ejecución de los planes de tratamiento determinados.
- La (in)materialización del Riesgo.
- Los resultados asociados al desempeño de los procesos.

C. Procedimiento para la gestión de activos de información

Objetivo

Establecer los lineamientos para la adecuada identificación y clasificación de activos de información que genere, obtenga, adquiera, transforme o controle en la institución.

Responsables

- **Jefe de Área:** encargado de apoyar, otorgar el tiempo y recursos necesarios para realizar la identificación, actualización, clasificación, revisión y aprobación de los activos de información de los procesos que tiene a su cargo.
- **Coordinador de sistemas:** Encargado de acompañar al líder de proceso en la identificación, clasificación y/o actualización de los activos de información de los procesos que tiene a cargo.
- **Profesional de Gestión Documental:** Encargado de acompañar jefe de área en la calificación documental de los activos de información identificados para su proceso.
- **Profesional de Planeación:** Encargado de gestionar la publicación del inventario de activos de información de la entidad en el canal dispuesto para tal fin.

Contenido.

1. **Identificación y Clasificación:** La coordinación de sistemas realiza la identificación y clasificación de los activos de información de la entidad conjuntamente con los líderes de proceso o con el funcionario designado para tal fin (gestor), con el fin de valorarlos y protegerlos adecuadamente teniendo en cuenta los cambios en la normatividad vigente, en el mapa de procesos o en la estructura organizacional.
2. **Calificación Documental**: La calificación documental de los activos de información busca la adecuada custodia de los mismos, teniendo en cuenta los tiempos de retención en el archivo de gestión y central de acuerdo con las Tablas de Retención Documental del proceso. Esta calificación se realiza con el acompañamiento del Profesional de Gestión Documental.
3. **Revisión y Aprobación:** una vez se finaliza el ejercicio de identificación y clasificación de activos de información, la coordinación de sistemas, mediante memorando envía a los líderes de procesos el registro de activos de información de los procesos que tiene a cargo para su respectiva revisión y aprobación.
4. **Publicación:** Una vez aprobados los activos de información, la coordinación de sistemas, consolida los activos de información y la entrega mediante memorando al departamento de seguridad industrial para su publicación.
5. **Actualización:** anualmente la coordinación de sistemas actualiza el registro de activos de información acorde con los cambios que se presenten al interior de la institución.

D. Procedimiento para la implementación o actualización de recursos tecnológicos.

Objetivo

Establecer las actividades y áreas responsables para planear y evaluar la adquisición y renovación de recursos tecnológicos de forma que se garantice una buena calidad, precio y que satisfagan las necesidades de la institución

Responsables

- **Jefe de Área:** encargado de apoyar, otorgar el tiempo y recursos necesarios para realizar la identificación, actualización, clasificación, revisión y aprobación de los recursos tecnológicos.
- **Coordinador de sistemas:** Encargado de gestionar la adquisición o renovación de equipos tecnológicos que solicite el líder de proceso.

Contenido.

El proceso de gestión de sistemas de información en coordinación con la gerencia de la institución, contara con un procedimiento de compra o reposición de recursos tecnológicos, que incluya la evaluación de la necesidad de la tecnología, que tenga en cuenta los requerimientos técnicos, pruebas de validación antes de su compra, la seguridad de uso tanto para usuarios, análisis de costo-efectividad y evaluación del funcionamiento de la misma.

Para ello se deberá cumplir con los siguientes requerimientos:

- Exigir garantía al proveedor por los desperfectos que se presenten al comprar, reponer, adquirir en comodato equipos, dicha garantía incluye la reposición completa del equipo cuando éste no cumpla con el objetivo para el cual fue adquirido. En todo caso la garantía que incluye el equipo es mínimo de 24 meses.
- Contar con un programa de mantenimiento preventivo de equipos, cuya periodicidad responda a las condiciones definidas por el fabricante, éste debe contener el plan de mantenimiento anual de los equipos, las condiciones para crear, actualizar y mantener las hojas de vida de los mismos, listas de chequeo a realizar en el mantenimiento y el diseño de indicaciones de uso de los equipos, que incluyan las alarmas de mal funcionamiento o desperfectos en las áreas donde están ubicados los mismos.
- Renovar la tecnología cuando esta sea obsoleta o exista una historia de fallas continuas, poca confiabilidad, se agoten los repuestos o cuando el costo de la reparación sea mayor al beneficio.

- Incorporar dentro de los criterios de compra la preferencia por el uso de tecnologías que preserven y cuiden el medio ambiente: TECNOLOGÍAS LIMPIAS.

E. Procedimiento para el control del acceso físico

La coordinación de sistemas se considera una dependencia sensible que requiere controles de acceso en concordancia con dicho estado, al igual que otras dependencias de la institución que contengan información confidencial.

Responsables

- **Jefe de área:** encargado de aprobar, definir condiciones de seguridad para todo equipamiento que tenga información clasificada como confidencial.
- **Coordinación de sistemas:** Habilitar los permisos de acceso a las diferentes dependencias, así como generar nómina de personal autorizado a ingresar a las diferentes dependencias. Además es el autorizar traslado de equipos de computación o de comunicaciones.

Contenido.

Personal: El personal la institución y terceros autorizados, deben portar siempre su identificación en un lugar visible.

Visitas: A las visitas autorizadas a ingresar a la institución, se les debe exigir su identificación y firma en el registro de ingreso. Se les debe entregar una tarjeta de visita que señale el área a la que se le autoriza, la que se debe portar en un lugar visible.

Áreas que contienen Información Sensible

- El acceso a oficinas, o áreas de trabajo que contengan información sensible debe estar físicamente restringido.
- El jefe de área debe definir los niveles de seguridad asociados a sus departamentos, así como los controles adecuados en cada nivel.

Registro del Acceso

El ingreso a los sectores restringidos por parte de los funcionarios autorizados, requiere el uso de su tarjeta de identificación personal a fin de registrar su ingreso y egreso.
El acceso de personal interno o externo a una dependencia restringida, debe quedar registrado, detallando nombre, motivo del ingreso, fecha y hora del ingreso y egreso. Durante su permanencia debe estar siempre acompañado por personal de la coordinación de sistemas.

Accesos Revocados

Cuando un trabajador termina su relación laboral, sus permisos de acceso a dependencias deben ser revocados. Por lo mismo, la lista de personas y permisos debe ser actualizada periódicamente, de acuerdo a Política de T.T.H.H.

Salas de Computadores y Comunicaciones

Todo equipamiento que tenga información confidencial, debe estar configurado y aprobado por la coordinación de sistemas.
Las dependencias que contengan computadores multi-usuario y equipos de comunicaciones (switches, PBX, routers, firewalls) y consolas de administración, deben tener acceso restringido.

Personal Autorizado

El coordinador de sistemas o a quien él delegue debe generar un listado del personal autorizado a ingresar a las diferentes dependencias de procesamiento de información.
La coordinación de sistemas, será responsable de habilitar los permisos de acceso correspondientes.

Registro del Acceso de Personal Interno o Personal Externo

El acceso de personal interno o personal externo, autorizados a ingresar a una dependencia restringida, debe quedar registrado, detallando nombre, empresa, motivo del ingreso, fecha y hora del ingreso y egreso.

Señalización

La ubicación del área de servidores, no debe ser anunciada mediante signos o señales en áreas de acceso público.

Acceso al área de servidores

Todo equipo de computación o de comunicaciones debe ser rotulado para su identificación. No se debe permitir el acceso a cualquier equipo que no esté claramente identificado.

Todo traslado de equipos de computación o de comunicaciones debe estar autorizado por el coordinador de sistemas o en quien éste delegue, al mismo tiempo se debe actualizar el inventario, dicho evento, debe identificar al menos, la persona, el equipo trasladado y los lugares de origen y destino.

Los equipos ingresados en forma temporal por terceros deben ser anotados en un registro para su control de entrada, salida, tiempo y usuario.

Antes de que un equipo computacional sea vendido, donado o dado de baja, debe ser examinado por la coordinación de sistemas y proceder a la eliminación de toda información.

F. Procedimiento para la gestión de medios removibles

Brindar los lineamientos para la adecuada gestión de los medios removibles, a fin de propender por la disponibilidad, integridad y confidencialidad de la información que maneja la Entidad.

Responsables

Todos los empleados de la institución, deben conocer y poner en práctica las disposiciones dadas por el presente procedimiento.

Contenido

Éste procedimiento está orientado para la correcta gestión de los medios removibles, los usuarios deben conocer la criticidad de los riesgos de seguridad de la información que pueden llegar a materializarse en caso de utilizar medios removibles no autorizados.

Actividades de la Gestión de Medios Removibles:

Nº	**Actividad**	**Descripción**	**Responsable**
1	Solicitar la activación de los puertos USB o la unidad de CD/DVD	El funcionario o tercero que tiene la necesidad de utilizar el recurso USB o la unidad CD/DVD debe hacer la solicitud mediante atención al cliente, o delegado indicando la justificación de la necesidad.	Jefe atención al cliente o delegado.
3	Verificar si la justificación es viable	El Oficial de la seguridad de la información o quien haga sus veces, analiza el mensaje recibido y autoriza o no el acceso a los recursos solicitados.	Oficial de Seguridad de la Información
4	Solicitar la apertura del recurso	En caso de que la solicitud sea autorizada, el Oficial de Seguridad de la Información comunica al funcionario encargado del grupo de Administración y Seguridad de la Información para que proceda a establecer el acceso. En caso que No sea autorizada la solicitud se procederá a informar al	Oficial de Seguridad de la Información

		área correspondiente las razones de la negación.	
5	Conceder permisos	El encargado de la apertura del acceso debe informar a través de la herramienta de gestión de TI que el acceso ha sido asignado y el tiempo que está disponible el recurso y cerrar la solicitud en la herramienta de gestión.	Oficial de Seguridad de la Información
6	Desactivación de acceso a recursos	Una vez transcurrido el tiempo asignado se debe cerrar el acceso a los recursos previamente asignados. Si es de carácter permanente se debe incluir en los controles pertinentes.	Oficial de Seguridad de la Información

Tabla 6-8: Actividades de la Gestión de Medios Removibles
Elaborado por investigador.

- La información que es almacenada en medios removibles y que debe estar disponible por largo tiempo, es protegida y controlada adecuadamente para evitar que ésta se vea afectada por el tiempo de vida útil del medio.
- La responsabilidad de la información contenida en los medios removibles es del usuario que está a cargo del mismo.

G. Procedimiento para el control de acceso a los sistemas de información

Establecer las actividades necesarias para la asignación de equipos y creación de cuentas de acceso a los Sistemas de Información, así como también para la devolución de activos y cierre de las cuentas.

Responsables

Usuarios de Sistemas de Información

Todos los usuarios de los Sistemas de Información, ya sean de planta, contro, honorarios y externos deben regirse bajo lo establecido en este procedimiento.

Unidades Administrativas

A las Unidades Administrativa les corresponderán las siguientes responsabilidades:

- Notificar sobre las vinculaciones y desvinculaciones del personal de su área, con la debida antelación para que sea factible realizar las actividades descritas en este procedimiento.
- Solicitar el acceso a Sistemas de Información para el personal de su área.
- Administrar el uso de los Sistemas de Información relacionados con su cargo.
- Capacitar a su personal en el uso de los Sistemas de Información relacionados con el cargo.

Coordinación de TTHH

Es responsable de notificar de forma consolidada la coordinación de sistemas, sobre las vinculaciones y desvinculaciones del personal, con la debida antelación para que sea factible realizar las actividades descritas en este procedimiento.

Coordinación de sistemas.

Corresponderá las siguientes responsabilidades:

Velar por el cumplimiento de este procedimiento y de los tres principios básicos de la Seguridad de la Información, de la siguiente forma:

- **Integridad:** tomar resguardos e implementar herramientas para que la información se mantenga completa, actualizada y veraz, sin modificaciones inapropiadas o corruptas.
- **Confidencialidad:** tomar resguardos e implementar herramientas para que la información esté protegida de personas/usuarios no autorizados.

- **Disponibilidad:** to mar resguardos e implementar herramientas para que todos los usuarios autorizados puedan acceder a los Sistemas de Información cuando lo requieran, con objeto de desempeñar sus funciones.
- Responder a las notificaciones enviadas por TTHH, sobre vinculaciones y desvinculaciones de funcionarios o colaboradores.
- Proporcionar la información que requiera TTHH, con objeto de mantener actualizado el inventario de activos fijos, respecto a equipos informáticos.
- Mantener actualizado los siguientes registros:
    - Inventario de los activos informáticos (licencias y equipos), incluyendo los asignados a usuarios y aquellos en bodega, junto a los formularios de asignación y devolución de equipos.
    - Usuarios activos y no activos en la red.
    - Usuarios con permisos para acceder a cada sistema de información.

Contenido

Inventario de activo fijo tecnológico

Según (Chile, 2016) es indispensable mantener un inventario actualizado de activos fijos tecnológicos, durante todas los ciclos correspondientes, hasta que la vida útil haya terminado.

Para ello, es necesario cumplir con los siguientes requerimientos:

1) Al receptar el activo fijo, se deberá actualizar el registro de activos con los siguientes datos: ubicación, tipo, marca/modelo, serie, fecha de compra, estado, custodio y observaciones
2) Al asignar un equipo a un usuario, la coordinación de sistemas será la responsable de registrar la información relevante a la asignación en el registro de activos fijos, el cual deberá incluir el nombre del usuario en el registro pertinente.
3) Una vez al año, el coordinador de sistemas y un representante del depto. Contable, verificaran físicamente el inventario de hardware y software de la institución.

Asignación de equipos y creación de cuentas

La asignación de equipos informáticos y la creación de cuentas para acceder a la red institucional son actividades que realizará la coordinación de sistemas, de acuerdo a las notificaciones consolidadas que enviará la coordinación de TTHH. Es responsabilidad de cada área de la institución informar con la debida antelación a la coordinación de talento humano, para que ésta pueda recopilar todos los antecedentes necesarios y luego notifique al coordinador de sistemas, el cual deberá proceder con las acciones indicadas a continuación:

- Habilitar estaciones de trabajo de nuevos colaboradores, con respecto a aspectos de tecnologías de información, configurando los equipos que correspondan (computador, teléfono, etc.). Al momento de recibir los equipos o insumos computacionales (incluyendo cambios), el usuario deberá firmar el formulario de asignación de activos, que proporcionará la coordinación de talento humano.
- Crear credenciales de acceso (usuario y contraseña) en el servicio de directorio para acceder a la red y al correo electrónico institucional.

Acceso a sistemas de información

Según procedimiento de seguridad de la información realizado por la superintendencia del medio ambiente del gobierno de Chile (Chile, 2016), los requerimientos de acceso específico a sistemas de información para nuevos colaboradores, deberá ser gestionada por las jefaturas de área y comunicada pertinentemente a la coordinación de sistemas para que sean habilitados los accesos solicitados.

Esta solicitud de acceso se deberá indicar:

- Datos del usuario que solicita permisos de acceso.
- Especificar fecha de la solicitud.
- Especificar el o los sistemas a los cuales el usuario deberá tener acceso.
- Detallar el perfil con el que debe contar el usuario para cada uno de los sistemas a los cuales se solicitó acceso.

Devolución de activos y des habilitación de cuentas

Desacuerdo con el procedimiento de seguridad de la información realizado por la superintendencia del medio ambiente del gobierno de Chile (Chile, 2016), la recuperación de activos y la des-habilitación de cuentas de usuarios para acceder a la red institucional son actividades que realizará la coordinación de sistemas de acuerdo al informe que debe ser enviado por la coordinación de TTHH.

La coordinación de TTHH deberá recopilar todos los antecedentes necesarios y luego notificar inmediatamente a la coordinación de sistemas la desvinculación del usuario, el cual deberá proceder con las acciones indicadas a continuación:

- El usuario deberá firmar un formulario de devolución de activos tecnológicos, el cual proporcionará la coordinación de TTHH. En caso de que el usuario no se encuentre al momento de retirar los equipos, el formulario deberá ser firmado por el jefe de área.
- Inmediatamente se deberá deshabilitar las credenciales de acceso (usuario y contraseña) a los sistemas de información de la institución, con el objeto de impedir el acceso a datos sensibles.
- Respaldar la información del computador del usuario desvinculado, de acuerdo a lo establecido en el procedimiento de respaldo de información.
- Notificar a la coordinación de TTHH, si los equipos tecnológicos asignados devueltos se encuentren con desperfectos, para que se tomen las medidas que correspondan.

H. Definición de roles de usuario.

Objetivo

Establecer las directrices para controlar el acceso de usuarios a los sistemas que la institución disponga para ellos, para prevenir la intromisión de personas no autorizadas, que pudiesen modificar la información registrada.

Alcance

Este procedimiento considera todas las solicitudes de usuarios para acceder a la plataforma tecnológica de la institución, es aplicable a todos los usuarios (planta, reemplazos y suplencia), personal a honorarios y terceros, que presten servicios a la institución.

Responsabilidades

Para cumplir los objetivos del presente procedimiento, se establecen los siguientes roles y responsabilidades.

Coordinación de TTHH

Le corresponderán las siguientes responsabilidades:

- Gestionar solicitudes de creación de cuentas por parte de los usuarios.
- Mantener registros de las solicitudes.

Coordinación de sistemas

Atenderá las solicitudes de acceso a los sistemas de información que TTHH requiera.

Contenido

La solicitud de acceso específico a sistemas de información para nuevos funcionarios o colaboradores se debe gestionar con TTHH el acceso a los sistemas específicos, de acuerdo a las funciones que establezca su rol. En particular, deberán remitir, al menos, los siguientes antecedentes:

- Usuario que requiere permisos de acceso.
- Detallar el o los sistemas a los cuales el usuario deberá tener acceso.
- Detalle del perfil de usuario con el que debe contar el funcionario para cada uno de los sistemas a los cuales se solicita acceso.

I. Procedimiento para la protección contra software malicioso.

Objetivo

Contar con una plataforma de hardware y software que proteja la integridad y disponibilidad de la información y del software que la procesa. La red local institucional de malware, troyanos, y demás virus que atenten contra la integridad y disponibilidad

de la información almacenada tanto en servidores como en estaciones de trabajo y cualquier otro medio magnético.

Alcance

Aplica a todos los procesos contemplados dentro del alcance del Sistema de Administración de la Seguridad de la Información.

Lineamientos

Se deberán tomar las precauciones necesarias para proteger la red institucional previniendo (Smith & Galleguillos, 2011), detectando y recuperándose de la introducción de software malicioso como son virus en las PC´S y Servidores. Se capacitara periódicamente a los usuarios en cuanto a controles contra software malicioso, los apropiados accesos a sistemas y el control de cambios.

Deberán cumplirse los siguientes puntos:

a) No se puede instalar ni descargar software de ningún tipo sin previa autorización de jefe de área, en caso de requerirlo se debe hacer debe ser bajo la supervisión de la coordinación de sistemas.
b) Los equipos de la institución servidores y computadores tendrán instalado software de antivirus (se recomienda Eset Nod32) para evitar la propagación de virus a través de la red institucional.
c) La plataforma de Antivirus deberá cumplir con los siguientes requerimientos:
   Consola centralizada de administración.
   - Actualización centralizada y permanente de la base de datos de virus.
   - Actualización automática de la BD de virus en las estaciones de trabajo.
   - Panel de control principal para realizar monitoreo centralizado.
   - Correr en las distintas plataformas (Windows, Linux).
   - Resumen de información de cada equipo (dirección ip, procesador, sist. Operativo, disco, ram, etc).
   - Facilidad de ejecutar una revisión silenciosa de virus en los equipos informáticos, para evitar la propagación de los mismos, como medida preventiva.

d) La coordinación de sistemas deberá estar suscrita a los boletines de alerta tanto del fabricante como del proveedor de antivirus, así como de los principales fabricantes de antivirus en el mercado, para determinar y seguir las recomendaciones de terceros en caso de ataques o vulnerabilidades, también para diferenciar y determinar los diversos riesgos o falsos virus.
e) La herramienta de Antivirus que se implemente en la institución tendrá carácter de corporativo y por ende será obligatoria su instalación y uso en todo el equipamiento computacional sean estos servidores, estaciones de trabajo.

J. Procedimiento para copias de respaldo

Objetivo

Realizar actividades de respaldo de la información, que permitan garantizar la disponibilidad e integridad de la misma, en caso de sufrir algún incidente de seguridad que implique un proceso de recuperación.

Responsables

- **Coordinador de Sistemas**: Para los backups del software administrativo e información de usuarios.

Contenido.

Para la creación de backups se realizarán copias de la información (ver anexo 4) de la siguiente manera:

Para el software administrativo: Este software permite las actividades de facturación administración contable y de la producción, en su programación original; el software está configurado para realizar una copia automática, cada día a las 23:00h. Esta copia está configurada para realizarse en otra partición del disco duro del equipo donde el software está instalado, luego de esto otra tarea programada a las 02:00am copiara a un disco duro externo de respaldos.

Los días Sábados a las 05:00am se realizará una copia incremental del último backup, y se almacenará fuera de la institución en un outsourcing llamado **Paradox**, el proveedor brindara todas las seguridades para que la información permanezca integra,
Para llevar el registro del backup, se utilizara un formato, que contenga, la fecha de en la que se ha realizado el respaldo, el nombre del archivo, el lugar de almacenamiento que le corresponde y firma de la persona que realiza el backup.

Para los archivos de usuarios. Los archivos de todos los usuarios, así como los respaldos del software comercial son de alta relevancia debido a que son el insumo inicial de creación que da origen al todo el proceso productivo de la empresa, los archivos creados se guardan en el disco duro del equipo en que fueron creados, pero adicional a esto se guardan al final del mes una copia de los archivos más relevantes en un disco duro externo y de este disco duro se hará respaldos en un servidor de archivos que contiene un disco duro adicional para almacenar estos respaldos. Adicional a esto realizara un backup del mismo, quemándolo en un DVD y almacenándolo en la Gerencia.
Igualmente para llevar el registro del backup, se llevará un formato, que contenga, la fecha de backup, el nombre del archivo y, el lugar de almacenamiento que le corresponde y firma de la persona que realiza el backup.

K. Procedimiento para mantener la seguridad en el intercambio de información

Objetivo.
Definir los lineamientos, políticas, procedimientos de transferencia de información, mitigando el riesgo de fuga o pérdida de información restringida.

Alcance.
La reglamentación dispuesta en esta guía aplica para todos los funcionarios de la institución.

Responsable.

Todos los funcionarios de la institución son responsables de asegurar el debido tratamiento y cumplimiento a esta guía, de los niveles de seguridad y de la adecuada transferencia de información.

Definiciones:

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** Propiedad de que la información se accesible y utilizable por solicitud de una entidad autorizada.
- **Incidente de Seguridad de la Información:** Un evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

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

Contenido

El intercambio de información de la empresa, entre organizaciones o terceras partes debe estar controlado y se deben cumplir todas las legislaciones y normas que correspondan. Para mantener una adecuada protección de la información, establece procedimientos y controles de intercambio por medio de la utilización de todo tipo de servicios de comunicación.

1. **Acuerdos de transferencia de Información.**

Toda información que necesariamente deba ser transportada en medios físicos, debe estar protegida contra acceso no autorizado y uso inadecuado. Para ello se deben aplicar los siguientes controles:

- Usar medios de traslado de confiabilidad certificada.
- Los medios informáticos que sean transportados físicamente deberán cumplir con medidas preventivas para su traslado como: ser embalado y protegido correctamente con cajas de cartón y protectores de icopor para el caso de PC o servidores críticos.
- Los empleados no deben mantener conversaciones confidenciales en lugares públicos y oficinas abiertas.
- Si la información tiene que ser movilizada en una memoria USB o disco duro externo, el transporte de información se debe realizar mediante contenedores o espacios cifrados.

2. **Responsabilidad legal y consecuencias**

   Debido a que el uso inadecuado en la transferencia de información puede causar fuga de información restringida, los empleados pueden ser sujeto de sanciones que podrán llegar hasta la terminación del contrato de trabajo, sin perjuicio de las acciones legales a que haya lugar, según las leyes aplicables vigentes.

L. Procedimiento para la gestión de contraseñas de usuario.

Objetivos

Establecer, difundir y verificar el cumplimiento de buenas prácticas en el uso de contraseñas.

Responsables.

Todos los funcionarios de la institución son responsables de hacer uso del procedimiento para el uso adecuado de contraseñas.

Contenido

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a las contraseñas.

Los puntos clave de esta política son:

Gestión de contraseñas.

La gestión de contraseñas es uno de los aspectos más delicados para asegurar el acceso a los sistemas de información. Se ocupa de registrar:

- Motivo por el que se genera una clave;
- Fecha de creación;
- Responsable de la custodia;
- Periodo de validez;
- Posibles observaciones, incidentes, etc.

Herramientas para garantizar la seguridad de tus contraseñas.

Para garantizar que las contraseñas asignadas a los usuarios sean modificadas de manera frecuente la coordinación de sistemas se puede ayudar de herramientas como directorio activo o servicios externos que obliguen al cumplimiento de los requisitos de seguridad implementados.

En todos los casos se contemplaran los aspectos más relevantes como:

1) Las contraseñas tendrán un periodo de validez definido por gerencia general.
2) Sera imposible re utilizar contraseñas usadas anteriormente.
3) El formato de contraseña deberá tener un mínimo de 9 caracteres, por lo menos una letra mayúscula, como mínimo un carácter numérico y al menos un carácter especial.
4) Ningún usuario tendrá la posibilidad de modificar su contraseña, de ser necesario el usuario deberá solicitar a la coordinación de sistemas el reseteo de contraseña.
5) La coordinación de sistemas configurara un número límite de intentos.
6) No compartir las contraseñas con nadie.
7) No apuntarlas en papeles o post-it.
8) Bajo ninguna circunstancia almacenarlas en correos electrónicos ni en formularios web cuyo origen no sea confiable.
9) No utilizar la misma contraseña para servicios diferentes.
10) No hacer uso del recordatorio de contraseñas. Esto es especialmente frecuente en el uso de navegadores web.

M. Procedimiento para mantener escritorio y pantalla limpia.

Objetivo.

Establecer las reglas para reducir los riesgos de acceso no autorizado, daño o pérdida de la información en cada uno de los puestos de trabajo, así como en el resto de las instalaciones.

Alcance

Este procedimiento, es aplicable y debe ser conocido y cumplido por todas y todos los funcionarios y funcionarias de la institución, a los que se les haya asignado un escritorio de trabajo, un equipo de computación, manejo de documentos físicos y/o digitales, así como terceros que presten servicios a la institución.

Roles y Responsabilidades

- **Coordinador de sistemas.** Estará a cargo de definir las normas y procedimientos para la correcta aplicación de esta política.
- **Usuarios de la información.** Ellos deberán dar cumplimiento a los procedimientos que deriven de esta Política, lo que incluye el resguardo de sus artículos personales.

Desarrollo

1) Está prohibido pegar adhesivos y figuras en las pantallas de los equipos asignados.
2) Los usuarios son responsables de mantener su equipo en buenas condiciones de limpieza externa.
3) La información con la que se genera dentro de la institución es de propiedad de la empresa y para uso de la misma.
4) En caso de ausencias prolongadas el usuario tiene la responsabilidad de asegurar que su información se encuentre fuera del alcance de terceras personas.
5) Si un equipo se encuentra dentro de una zona de tránsito de usuarios o público ajeno la institución, se lo ubicara de manera tal, que terceras personas no puedan tener acceso a la información de pantalla.
6) Está prohibido tener sustancias o líquidos en el escritorio, mismos que pueden afectar los equipos.

7) Eta prohibido utilizar dispositivos de respaldo de información como USB, CD, etc.
8) El usuario es responsable de cerrar su sesión de trabajo y dejar el equipo en suspensión, cuando deje de usarlo por tiempo prolongado.
9) Desde el momento de la firma del acta de asignación de un equipo, la responsabilidad sobre el estado del mismo, es totalmente del usuario.
10) Las estaciones de trabajo están adecuadas para que el usuario realice sus labores cotidianas con normalidad, el mismo no está dispuesto para trabajos de índole personal.
11) Está prohibido que el usuario pueda realizar cualquier tipo de configuración en sus estaciones de trabajo asignadas.
12) La estación de trabajo asignado al usuario es un bien institucional, por lo mismo el usuario no es dueño del mismo.
13) La coordinación de sistemas configurara en cada estación de trabajo, un descanso de pantalla de tipo institucional.

Sanciones

El incumplimiento de este procedimiento, podrá tener como resultado la aplicación de sanciones, conforme a la magnitud y característica del aspecto no cumplido o vulnerado.

N. Procedimiento para la configuración del computador.

Objetivo

Generar un estándar de configuración de los equipos, que facilite la reconfiguración, la comunicación y la administración de la red.

Responsables

Coordinador de Sistemas: Personal técnico encargado de la configuración de los equipos.

Contenido.

Para la configuración de los computadores de la institución, se seguirán los siguientes estándares:

Configuración de equipos.

Nombres de los equipos definidos de la siguiente manera:

- **XXXYYY###** donde
- **XXX**: iniciales que identifiquen la organización.
- **YYY**: Caracteres que identifiquen el área de proceso que utiliza el equipo.
- **###**: Número del último byte de la dirección ip del equipo.

Las direcciones ip de los equipos de red, se configurarán, teniendo en cuenta los siguientes estándares, **###** dónde ### hará referencia según la siguiente denominación:

- **101:** Gerencia: Si hubiera más equipos de personas asistentes a gerencia irían consecutivamente entre 101 y 106.
- **107:** Presidencia. Si hubiera más equipos de personas asistentes a gerencia irían consecutivamente entre 107 y 115.
- **116: Contabilidad**: La numeración sería consecutivamente entre 116 y 135
- **136: Márqueting:** Inicia entre 136 y 155.
- **156: Ambiente y Seg. Industrial:** Inicia entre 156 y 175
- **176: Producción y Calidad:** Inicia entre 176 y 200
- **201: TTHH:** Inicia entre 201 y 210
- **210: Seguridad Física:** Inicia entre 210 y 220
- **221: Invitados:** Inicia entre 220 y 250

Ejemplo del Nombre y dirección IP de un equipo:

- **Nombre Equipo:** RANCON116
- **Dirección IP:** 192.168.1.116

El Usuario administrador del equipo, tendrá un nombre compuesto por:

- adminXXX dónde XXX serán las iniciales definidas para identificar la organización en los nombres de los equipos.

  Ejemplo: adminran

Y la contraseña del administrador será la composición del nombre de la empresa + punto + sistemas el símbolo @ y el año actual.

Ejemplo: ranchito.sistemas@2018

El usuario administrador, no es el usuario de trabajo normal de cada computador, ya que tendría demasiados privilegios y es una condición insegura.

Se debe crear un usuario estándar, sin características de administrador para que sea el usuario de uso del equipo.

El coordinador de sistemas y la alta dirección serán los únicos en conocer la nomenclatura de las contraseñas de administrador, en caso de que sea necesario su uso.

O. Procedimiento para uso de antivirus

Los computadores tendrán el antivirus Eset nod32 de licenciamiento instalado.

Firewall de Windows y Actualizaciones Automáticas

Se realizará un proceso de legalización del sistema operativo, con el fin de que estas características como Firewall de Windows, Windows Defender y las Actualizaciones, estén activadas para que se realicen periódicamente.

Programas de archivos comprimidos

Los computadores de la alta dirección, Contador General, y el coordinador de sistemas, estará instalado el software Winrar, con el fin de filtrar la información que se permite ser descomprimida en los equipos, debido a que esta es una frecuente modalidad de contagio de virus.

Ejecución Automática de USB y discos externos

Se debe deshabilitar la ejecución automática de dispositivos de almacenamiento externo.

P. Procedimiento para la descarga de archivos de correo Electrónico

Objetivo

Generar hábitos preventivos en los usuarios, que permitan ejercer un control en las principales fuentes de contagio de virus informáticos.

Responsables

- Usuarios de los equipos
- Coordinación de sistemas

Contenido

El uso del correo electrónico institucional es necesario debido que es el contacto directo entre el cliente y la institución para realizar el intercambio de archivos e información, por lo tanto es muy importante, prevenir el contagio de virus, a través de ciertas prácticas al usar este medio, por ende es necesario que los usuarios sigan las siguientes instrucciones:

1. Evitar la abrir archivos que le parezcan llamativos, generalmente esto es lo que busca un archivo malicioso para atraer a su víctima.
2. Jamás descargar archivos que contengan extensión (.exe.pdf, zip, rar) pueden contener archivos maliciosos en su interior.
3. Si el usuario descubre que ha sido contagiado por algún tipo de virus, deberá reportarlo inmediatamente a la coordinación de sistemas, de ser posible el usuario deberá desconectar el equipo de la red para evitar el contagio de otros equipos.
4. Si presenta dudas sobre la dirección de correo electrónico del remitente, el usuario deberá contáctese con la coordinación de sistemas para que le brinde soporte y le ayude a verificar la autenticidad del mismo.
5. Verifique la ortografía del correo electrónico del remitente, muchas veces simulan direcciones electrónicas similares, por ejemplo, para suplantar a www.pichincha.com pueden usar www.pichimcha.com que puede pasar desapercibido en un usuario que no tome precauciones.
6. Si un remitente envía un link indicando que de click, deberá colocar el puntero sobre el enlace sin presionarlo, verificando que la ayuda de contexto que sale indique la misma dirección que dice el link, de lo contrario es un link falso, que puede llevar a un lugar malicioso.

6.6.6 Validación del modelo. (Resultado del hacking ético que demuestra que hay un nivel de seguridad adecuado y hace referencia al aval emitido por los directivos de la entidad)

A. Análisis.

El sitio web de la institución (www.elranchito.com.ec) se encuentra alojado con un proveedor de hosting externo, por tanto en la red interna no existe un servidor web ni un servidor de correo electrónico.

Se obtuvo el listado de hosts activos, tanto servidores resultantes del escaneo con NMAP como hosts clientes proporcionados por la coordinación de sistemas.

Análisis de Equipos Windows Servers y GNU/Linux

Se procedió con un análisis de los hosts resultantes del escaneo con NMAP; en la tabla 6-9 se indica la proporción de hosts por sistema operativo.

Resumen de equipos resultantes de escaneo NMAP

Sistema Operativo	Porcentaje
Windows	88%
GNU/Linux	9%
Mac OS	3%

Tabla 6-9: Resumen de SO escaneo NMAP

Elaborado por: Investigador

En el resultado del escaneo de la red (tabla 6-9) se evidencio que en mayor medida existen equipos con sistemas operativos Windows y GNU/Linux. El análisis se enfoca en el servidor principal el cual abarca los sistemas de información y es el que da la cara al internet.

A continuación se resume el reporte de hosts activos bajo las plataformas Windows Server y GNU/Linux con el número de puertos abiertos para cada equipo:

Equipos Windows server (Virtualizados)

Equipos	Puertos abiertos
192.168.1.97	**5**
192.168.1.98	**3**

Tabla 6-10: Equipos Windows Server

Elaborado por: Investigador

Equipo GNU/Linux

Equipos	Puertos abiertos
192.168.1.96/186.42.163.142	**10**

Tabla 6-11: Equipos GNU/Linux

Elaborado por: Investigador

B. Análisis de Vulnerabilidades

El análisis de vulnerabilidades se enfocó al servidor (**GNU/Linux**) principal que es el que contiene los Windows server (virtualizados) así como la IP publica; para esto se usara dos herramientas: OpenVAS, Nessus y Acunetix.

- **Análisis de vulnerabilidades con NESSUS**

Para la investigación se utilizó la versión 7.2.1 home de Nessus, el cual tiene limitantes como:

- No permitir un análisis de más de 16 IP´s por scaner.
- No posee soporte.
- No admite usar el dispositivo virtual de Nessus.

No obstante los módulos de análisis de la versión utilizada son válidos para llevar a cabo el análisis de verificación de vulnerabilidades propuesto sin incurrir en costos por pago

de licencia de software.

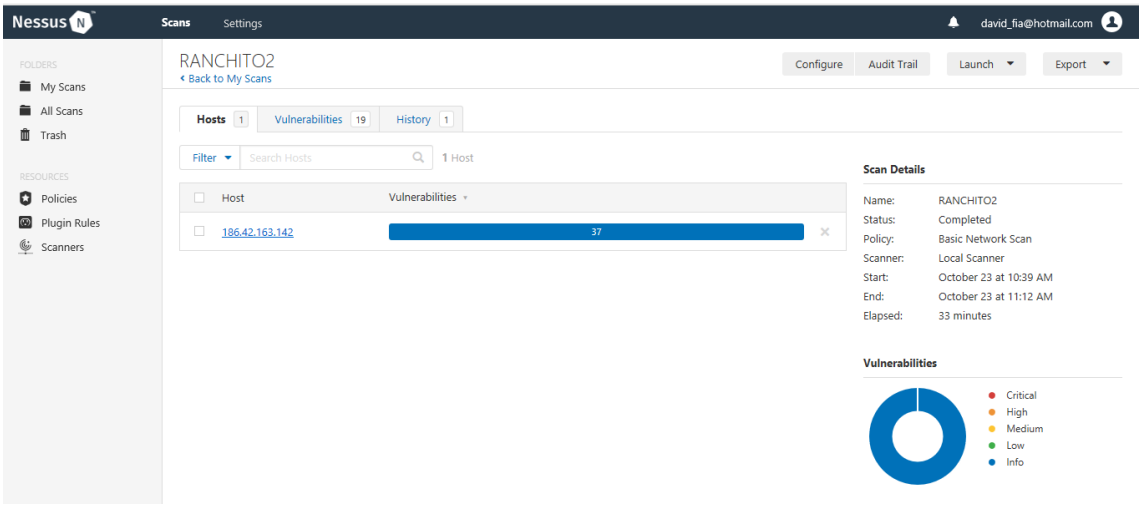


Ilustración 6-11: Tablero de Instrumentos Nessus

Elaborado por: Investigador

Nessus proporciona varios tipos de escaneo. Para el caso en cuestión se seleccionó un escaneo de tipo avanzado, tal y como se ilustra en la Ilustración 6-12.

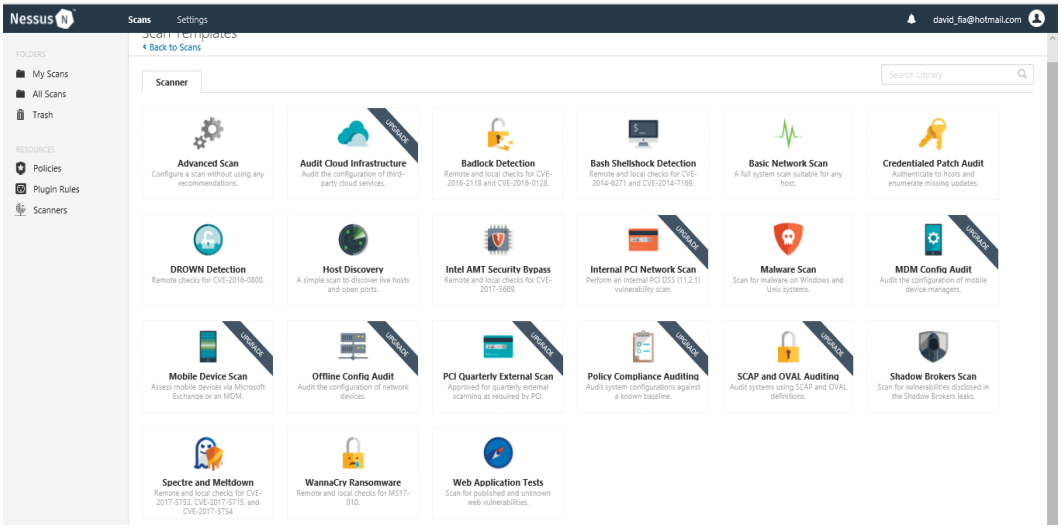


Ilustración 6-12: Tipos de escaneos en Nessus

Elaborado por: Investigador

Completado el escaneo, se creó la siguiente tabla resumen que permite analizar la cantidad de vulnerabilidades en dependencia de su criticidad (tabla 6-12).

Host	Critical	High	Medium	Low	Info
186.42.163.142	0	0	0	0	19
Total	**0**	**0**	**0**	**0**	**19**

Tabla 6-12: Escaneo Nessus host

Elaborado por: Investigador

El escaneo de vulnerabilidades reveló que el host no presenta vulnerabilidades, solo de nivel informativo.

Al desplegar el reporte de Nessus correspondiente al equipo 186.42.163.142, se pudo identificar que este no presenta vulnerabilidades evidenciando que el aplicar las políticas de seguridad propuesta mejoro la seguridad del servidor principal (ver ilustración 6-13).

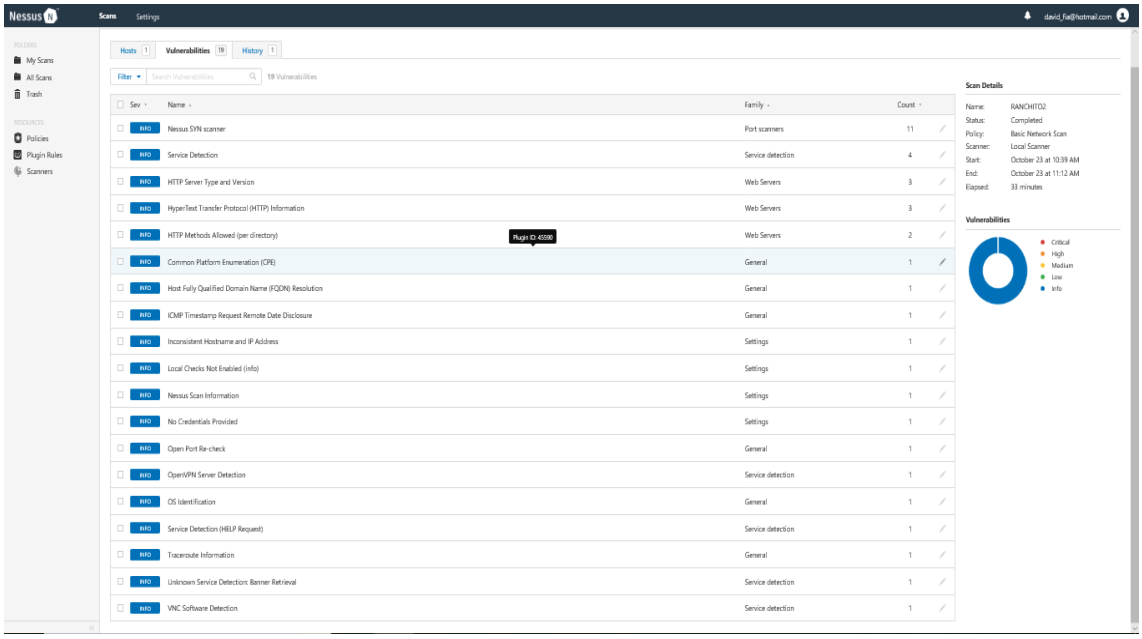


Ilustración6-13: Vulnerabilidades Nessus

Elaborado por: Investigador

Análisis de vulnerabilidades con OpenVAS

Como primer paso se creó el objetivo (186.42.163.142), tal y como se ilustra en la Ilustración 6-14.

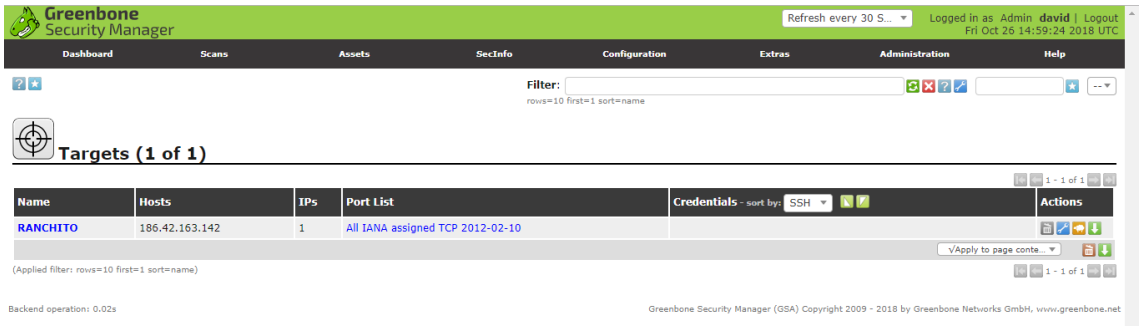


Ilustración 6-14: Targets OpenVAS

Elaborado por: Investigador

De manera seguida, se creó y ejecuto tareas de escaneo hacia el objetivo previamente establecido, tal y como se muestra la Ilustración 6-15.

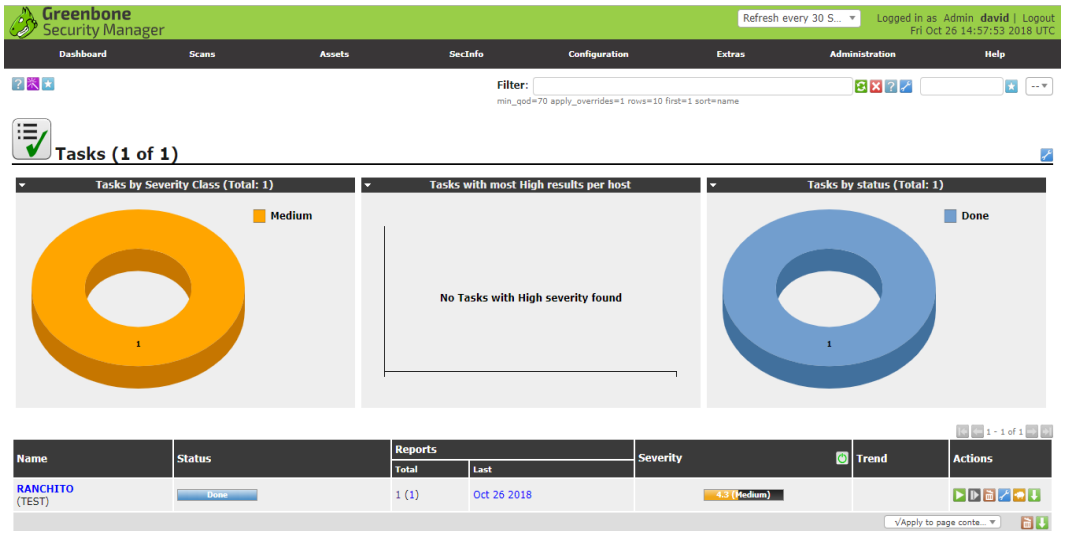


Ilustración 6-15: Tasks OpenVAS

Elaborado por: Investigador

Una vez finalizado el proceso de escaneo, los resultados se pudo evidenciar que se posee una sola amenaza de categoría media y dos de tipo baja (Ilustración 6-16) comprobando nuevamente que las políticas aplicadas han sido de utilidad. Así mismo los resultados arrojados fueron agrupados en la tabla (6-12):

Ilustración 6-16: Resumen de vulnerabilidades OpenVas

Elaborado por: Investigador

Host	High	Medium	Low
186.42.163.142	0	1	2
Total	**0**	**1**	**2**

Tabla 6-13: Escaneo OpenVAS hosts GNU/Linux

Elaborado por: Investigador

Vulnerabilidad de categoría Media

La vulnerabilidad con calificación media indica que el algoritmo de encriptación compatibles con SSH es débil.

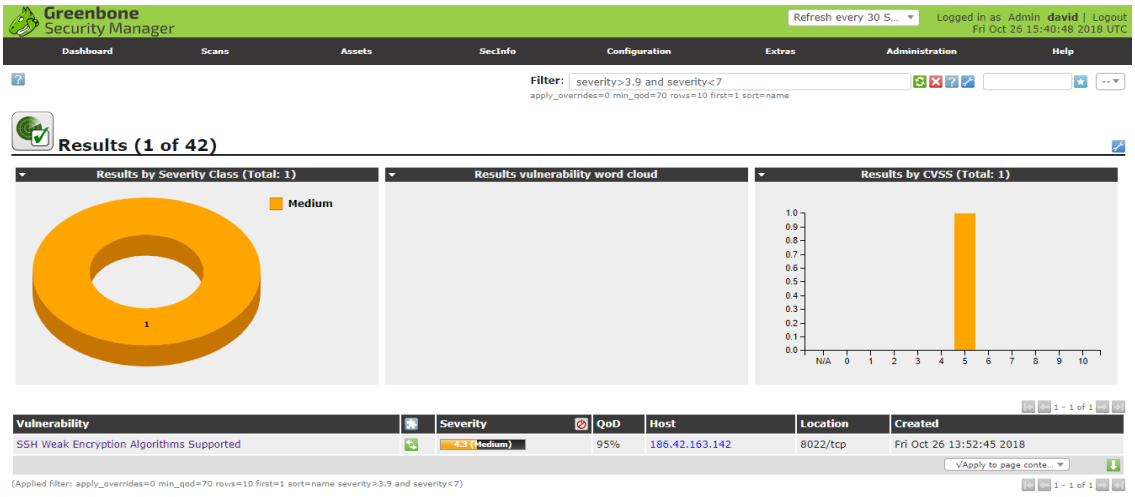


Ilustración 6-17: Vulnerabilidad media OpenVAS

Elaborado por: Investigador

La vulnerabilidad corresponde a que los mensajes SSH que emplean el modo CBC (Cifrado de bloque de encadenamiento) pueden permitir que un atacante recupere texto sin formato de un bloque de texto cifrado.

La solución es inhabilitar el cifrado en modo CBC con el siguiente procedimiento:

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption custom "aes128-ctr:aes192-ctr:aes256-ctr"
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

Vulnerabilidades de categoría Baja

Las vulnerabilidades de categoría baja que nos despliega OpenVas corresponden a que el algoritmo de cifrado SSH remoto está configurado para permitir algoritmos débiles de MD5 y / o MAC de 96 bits. La otra vulnerabilidad contempla que el host remoto implementa marcas de tiempo TCP y, por lo tanto, es posible calcular el tiempo de actividad.

Mismas que se solucionan ejecutando el procedimiento para inhabilitar el cifrado de modo CBC y deshabilitar las marcas de tiempo TCP **timestamps** a un valor=0 respectivamente.

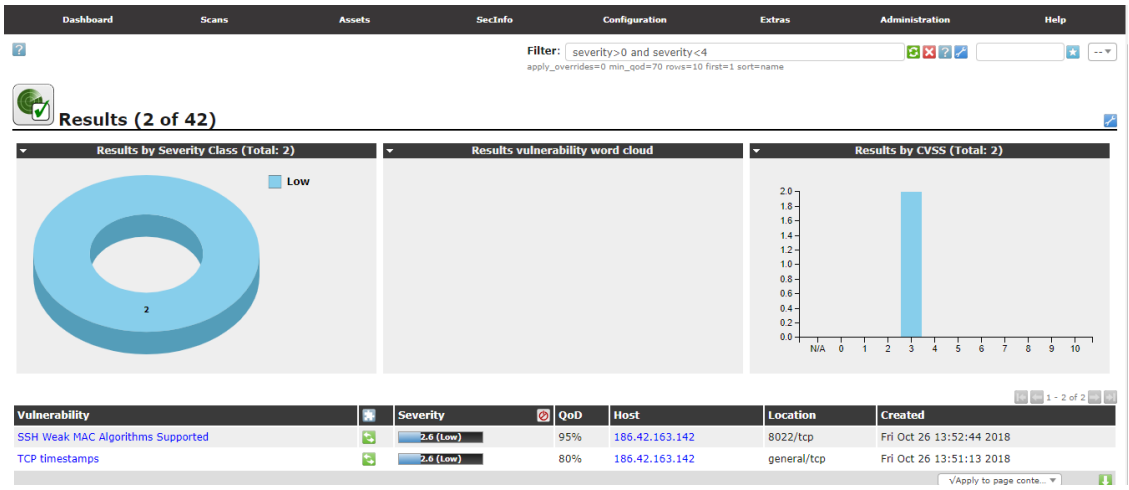


Ilustración 6-18: Vulnerabilidades Baja

Elaborado por: Investigador

Análisis de vulnerabilidades con ACUNETIX

Para finalizar se procedió con un análisis de vulnerabilidades a la página web (www.elranchito.com.ec) de la institución que se encuentra alojada con un proveedor de hosting externo, ya que la herramienta utilizada (Acunetix) versión Demo permite analizar sitios web únicamente.

Cumplido el escaneo, dando como resultado del análisis 22 amenazas de tipo media y 10 de tipo baja (Ilustración 6-19) para realizar un análisis se creó la siguiente tabla resumen que permitirá analizar la cantidad de vulnerabilidades en dependencia de su criticidad (tabla 6-13).

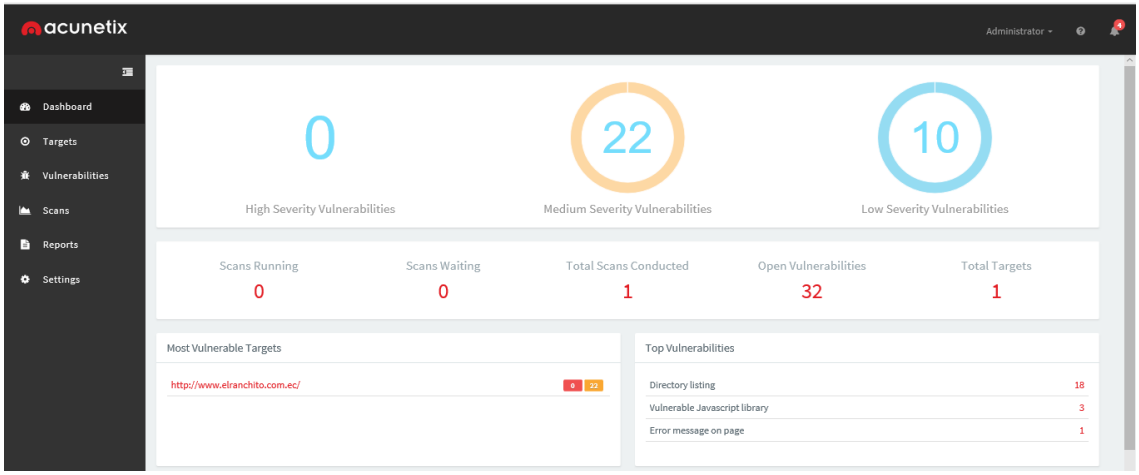


Ilustración 6-19: Escaneo Acunetix host

Elaborado por: Investigador

Host	High	Medium	Low
www.elranchito.com.ec/108.167.140.151	0	22	10
Total	**0**	**22**	**10**

Tabla 6-14: Escaneo Acunetix host

Elaborado por: Investigador

Vulnerabilidades de categoría media

El resultado del análisis obtenido por Acunetix para la página web de la institución arrojó 22 vulnerabilidades de categoría media; La mayoría tiene relación con la configuración del servidor web que permite mostrar los archivos contenidos en el directorio raíz.

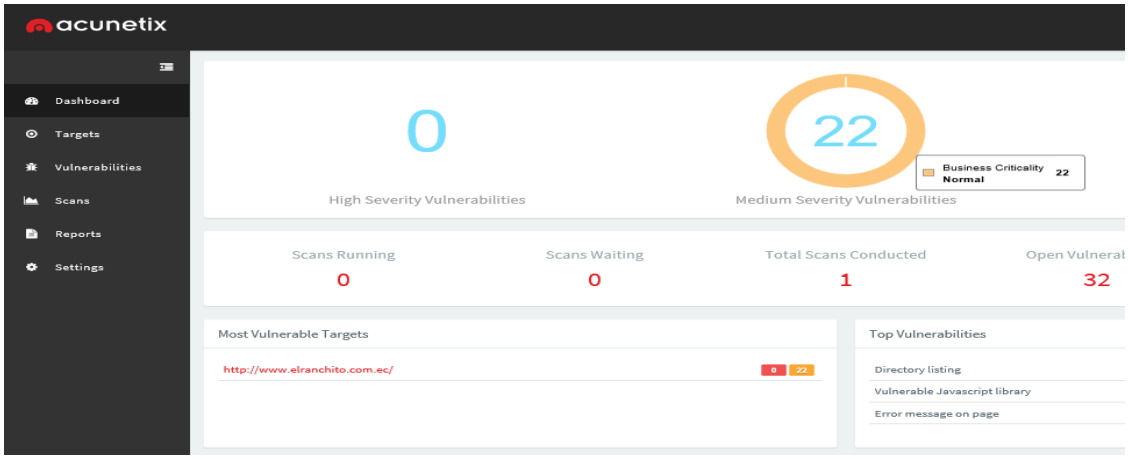


Ilustración 6-20: Vulnerabilidades medias Acunetix

Elaborado por: Investigador

Vulnerabilidades de categoría baja

El resultado de Acunetix arrojó 10 vulnerabilidades de criticidades medias; mismas que tienen relación con un posible archivo sensible el cual no está directamente vinculado desde el sitio web. Esta comprobación busca recursos sensibles comunes como archivos de contraseña, archivos de configuración, archivos de registro, archivos de inclusión, datos estadísticos, volcados de bases de datos.

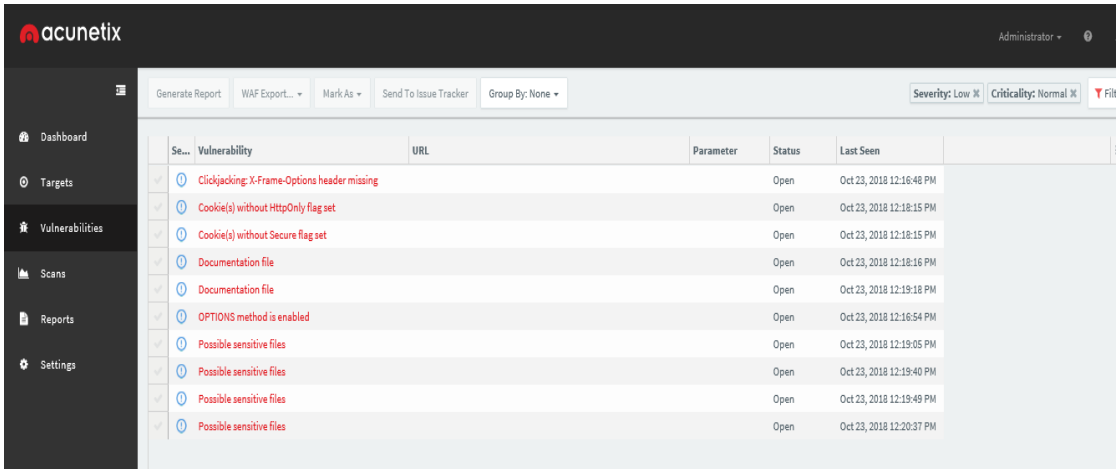


Ilustración 6-21: Vulnerabilidades bajas Acunetix

Elaborado por: Investigador

A través del análisis de vulnerabilidades realizado a la institución del caso de estudio se pudo evaluar el estado de seguridad de la información que mantiene la entidad;

evidenciando en gran medida vulnerabilidades de categoría baja, lo que permitió demostrar que los mecanismos de control implementados han brindado tratamiento a los riesgos de seguridad que sufría pasteurizadora el Ranchito, con esto ha logrado optimizar el uso de los recursos económicos y humanos con los que cuenta la organización. Se puede demostrar que las pequeñas empresas pueden optar por métodos como los mencionados en el desarrollo del presente trabajo, y enfocar en principio sus esfuerzos en la concienciación de los empleados y la limitación de privilegios, tanto a nivel de perfiles de usuarios como configuración de equipos, esto ayuda a tener un punto de inicio con un bajo costo de inversión y poder ir avanzando progresivamente con un ciclo de mejora continua, hacia inversiones futuras más sofisticadas, cuando el costo beneficio, sea en favor de las pequeñas empresas y se vaya generando una cultura de seguridad de la información, que permita visualizar los beneficios de ocuparse de este tema

6.6.7 Previsión de la Evaluación.

La implementación del modelo de gestión para la seguridad de la información propuesto está en concordancia con la experiencia obtenida por el autor ya que el análisis de vulnerabilidades ejecutado en la empresa del caso de estudio, cuya efectividad se evaluó a través de las encuestas aplicadas y los datos estadísticos obtenidos. Los resultados se expusieron en el capítulo 4.

Una vez aplicado el modelo propuesto se sugiere que se evalúe su usabilidad, fiabilidad y calidad de la información de identificación obtenida a través los mecanismos indicados en la Tabla 6-14 presentada a continuación.

Preguntas	**Explicación**
¿Qué evaluar?	La seguridad que poseen las PEQUEÑAS EMPRESAS al momento de resguardar sus activos de información frente a ataques informáticos.
¿Por qué evaluar?	Porque es necesario indagar si las PEQUEÑAS EMPRESAS están preparadas ante un eventual ataque.
¿Para qué evaluar?	Para Constatar si la propuesta es aplicable.

¿Indicadores?	Seguridad de la información, políticas, iso 27001.
¿Quién Evalúa?	El Coordinador de Sistemas.
¿Cuándo se Evalúa?	Luego de ser aplicada la propuesta.
¿Con que evaluar?	Cuestionario aplicado a los usuarios.
¿Fuentes de Información?	Usuarios del proceso de los sistemas de información análisis del estado actual de la información.

Tabla 6-15: Previsión de la Evaluación

Elaborado por: Investigador

7. Bibliografía

(s.f.).

Alejandro, G. T. (2017). *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACION DEL DISTRITO 18D01 DE EDUCACIÓN*. Obtenido de Universidad Técnica de Ambato.

Alvares, G. F. (2012). *Guía de Aplicación de la Norma UNE-ISO/IEC 27001*. España: AENOR. ASOCIACION ESPAÑOLA DE NORMALIZACION Y CERTIFICACION.

Areitio, J. (2008). *Seguridad de la Información, redes, informática y Sistemas de Información.* Madrid, ESPAÑA: Ediciones Praninfo S.A.

Bravo, D. (26 de julio de 2015). *El Comercio*. Obtenido de www.elcomercio.com: http://www.elcomercio.com/actualidad/ecuador-muestra-vulnerable-ciberataques.html

Capital. (04 de enero de 2015). *Capital Online*. Obtenido de http://www.capital.cl/negocios/2015/01/04/99010/aumento-de-ciberataques-se-instala-como-nueva-amenaza-en-economia-global/

Carranza, R. G. (2010). *Probabilidades y estadística.* Buenos aires: Cornell University.

Catalunya, U. P. (10 de 01 de 2015). *Sistemas de Información*. Obtenido de Facultat d'Informàtica de Barcelona: https://www.fib.upc.edu/es/estudios/grados/grado-en-ingenieria-informatica/plan-de-estudios/especialidades/sistemas-de-informacion

Chacón Mejía, P. E. (s.f.). Tesis de Pre grado. *Propuesta de un modelo de sistema de gestión de seguridad de la información para institutos superiores tecnológicos de educación aeronáutica.* Escuela Politecnica Nacional, Quito.

Chile, S. d.–G. (1 de Diciembre de 2016). *Sistema nacional de información de fiscalización ambiental*. Obtenido de http://snifa.sma.gob.cl/doc/SSI/ProcedimientosSeguridadInformacion.pdf

Clavijo, C. A. (2006). Políticas de Seguridad Informática. *Red de Revistas Científicas de América Latina y el Caribe, España y Portugal*, 92.

CodeJobs. (07 de 09 de 2012). *Seguridad Informática*. Obtenido de Qué es una vulnerabilidad, una amenaza y un riesgo: https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

Ecuadorencifras. (01 de 10 de 2018). *Instituto nacional de estadísticas y censos INEC Ecuador*. Obtenido de Instituto nacional de estadísticas y censos INEC Ecuador: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Economicas/DirectorioEmpresas/Directorio_Empresas_2017/Documentos_DIEE_2017/Documentos_DIEE_2017/Principales_Resultados_DIEE_2017.pdf

Excellence, I. (21 de 05 de 2015). *Sistema de Gestión de Seguridad de la Información*. Obtenido de Qué significa la Seguridad de la Información: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

F Laudon, J. L. (1996). *Sistemas de Información.* Mexico: Editorial Diana.

GALLEGO, M. L., & OSPINA, M. Á. (01 de 01 de 2010). *MODELOS DE GESTIÓN TECNOLÓGICA*. Obtenido de MODELOS DE GESTIÓN: https://es.slideshare.net/toretto333/modelos-de-gestin-tecnolgica

Gardey, J. P. (12 de 01 de 2016). *Tecnología de la Información*. Obtenido de Definición de: https://definicion.de/tecnologia-de-la-informacion/

Gestión, B. e. (06 de 04 de 2015). *Amenazas y vulnerabilidades*. Obtenido de Vulnerabilidades: http://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

ISO 27001. (10 de 01 de 2015). Obtenido de ISOTOOLS: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISO 27001:2005, I. (15 de Octubre de 2005). *Internacional standard ISO/IEC 27001:2005.* Obtenido de http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27001.pdf

ISO 27002:2005, I. (15 de Junio de 2005). *INTERNATIONAL STANDAR ISO 27002*. Obtenido de http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27002.pdf

ISO 27003, I. (1 de Febrero de 2010). *Internacional standard ISO/IEC 27003*. Obtenido de https://www.sis.se/api/document/preview/911960/

ISO 27004, I. (15 de Diciembre de 2009). *Internacional standard ISO/IEC 27004*. Obtenido de https://www.sis.se/api/document/preview/911894/

ISO 27005, I. (1 de Julio de 2018). *Internacional standard ISO/IEC 27005*. Obtenido de https://www.sis.se/api/document/preview/80005503/

ISO 27006, I. (1 de Octubre de 2015). *Internacional standard ISO/IEC 27006*. Obtenido de https://www.sis.se/api/document/preview/919537/

ISO 27011, I. (15 de Diciembre de 2008). *Internacional standard ISO/IEC 27011*. Obtenido de https://webstore.iec.ch/preview/info_isoiec27011%7Bed1.0%7Den.pdf

ISO 27032, I. (15 de Julio de 2012). *Internacional standard ISO/IEC 27032*. Obtenido de https://webstore.iec.ch/preview/info_isoiec27032%7Bed1.0%7Den.pdf

ISO 27034-1, I. (15 de 11 de 2011). *Internacional standard ISO/IEC 27034-1*. Obtenido de https://webstore.iec.ch/preview/info_isoiec27034-1%7Bed1.0%7Den.pdf

ISO 2731, I. (1 de Marzo de 2011). *Internacional standard ISO/IEC 27031*. Obtenido de https://webstore.iec.ch/preview/info_isoiec27031%7Bed1.0%7Den.pdf

ISO 2733-5, I. (1 de Agosto de 2013). *Internacional standard ISO/IEC 27033-5*. Obtenido de https://www.sis.se/api/document/preview/916418/

ISO 27799, I. (1 de Julio de 2016). *Internacional standard ISO/IEC 27799*. Obtenido de https://infostore.saiglobal.com/preview/iso/updates2016/wk29/iso_27799-2016_2.pdf?sku=1872172

López, P. A. (2008). *Seguridad Informática.* Editex.

Mantulak, M. J., Hernández Pérez, G., & Michalus, J. C. (1 de 12 de 2016). *SciELO Analytics*. Obtenido de SciELO Analytics: http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1668-87082016000200002

Márquez, B. A. (01 de 01 de 2009). *Un modelo conceptual para gestionar la tecnología en la organización*. Obtenido de A conceptual model to manage the technology in the organization: http://www.revistaespacios.com/a09v30n01/09300122.html

Media, E. (19 de 10 de 2017). *La MiPyME y su importancia en la economía Ecuatoriana*. Obtenido de Ekos Media: https://www.eltelegrafo.com.ec/noticias/economia/4/el-42-de-las-companias-registradas-en-el-pais-son-pymes

Políticas de Seguridad Informática. (06 de 05 de 2017). Obtenido de Tutorial de Seguridad Informática: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

Sánchez, L. F. (2009). Obtenido de https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

site, J. a. (01 de 12 de 2010). *Definicion de Porceso Tecnológico*. Obtenido de Procesos Tecnológicos: https://isme2210.wordpress.com/definicion-de-proceso-tecnologico/

Smith, J., & Galleguillos, H. (15 de Septiembre de 2011). *studylib*. Obtenido de https://studylib.es/doc/197029/pol%C3%ADtica-de-protecci%C3%B3n-contra-c%C3%B3digo-movil-y-malicioso

Tecno Secundaria. (08 de 09 de 2017). Obtenido de Recursos de Tecnología e Informática: http://www.tecnosecundaria.es/index.php/el-proceso-tecnologico/56-fases-del-proceso-tecnologico-metodo-de-proyectos

telégrafo, E. (28 de 09 de 2017). El 42% de las compañías registradas en el país son Pymes. *El 42% de las compañías registradas en el país son Pymes*, págs. https://www.eltelegrafo.com.ec/noticias/economia/4/el-42-de-las-companias-registradas-en-el-pais-son-pymes.

Vera, J. G., & Quintana, R. A. (2017). Análisis de la Productividad de la Industria Manufacturera del Ecuador. *Economics and Statistics*, 5.

Zapata, F. X. (24 de Noviembre de 2014). *Universidad Central del Ecuador*. Obtenido de http://www.dspace.uce.edu.ec/bitstream/25000/4244/1/T-UCE-0011-55.pdf

8. Anexos

Anexo 1: ENCUESTA N°1 DIRIGIDA, EXPERTOS EN SEGURIDAD DE LA INFORMACION.

Objetivo: Conocer los procesos actuales para identificar Vulnerabilidades de seguridad para una mejor identificación.

Instrucciones: Marque con una x la alternativa que considere adecuada

No.	PREGUNTAS	RESPUESTAS	
		SI	NO
1	Poseen requisitos de seguridad para conceder acceso a la información a personal ajeno a la institución?		
2	¿Mantienen inventario actualizado del hardware y software de la institución?		
3	¿Los derechos de acceso a la información son retirados después de la culminación del contrato con el empleado?		
4	El área de servidores estará protegido por controles apropiados de entrada para asegurar que sólo el personal autorizado se les permite el acceso?		
5	Disponen de políticas para asegurar el mantenimiento de hardware lo que permitirá mantener la disponibilidad e integridad continua de las TIC?		
6	¿Se realiza copia de seguridad de la información que genera la empresa?		
7	La información sensible que genera la organización se encuentra protegida contra pérdida, destrucción y falsificación?		

GRACIAS POR LA COLABORACIÓN!!!

Anexo 2: ENCUESTA N°2 DIRIGIDA EXPERTOS EN SEGURIDAD DE LA INFORMACION

Objetivo: Conocer los procesos actuales para identificar Vulnerabilidades de seguridad para una mejor identificación.

No.	PREGUNTAS	RESPUESTAS	
		SI	NO
1	El computador que utiliza tiene instalado antivirus y se encuentra actualizado?		
2	Ha firmado algún acuerdo de confidencialidad antes de ingresar a laborar en la institución?		
3	¿La información que usted maneja es respaldada periódicamente según sus necesidades?		
4	¿Ha recibido capacitación sobre temas de seguridad de la información?		

GRACIAS POR LA COLABORACIÓN!!!

Anexo 3: PLANTILLA DE CARTA DE COMPROMISO DE LA DIRECCIÓN

COMPROMISO DE LA DIRECCIÓN SGSI

La Gerencia General de Pequeñas empresas manifiesta a través de éste documento su compromiso con el SGSI, a través de las siguientes acciones:

- Tener disponibilidad de recurso humano para el proyecto, incluyendo un líder por parte de la organización, que tenga toma de decisión.
- Disponer de recursos necesarios para el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información, su mantenimiento y su mejora continua.
- Formulando la política del SGSI y promoviendo su cumplimiento al interior de la organización.
- Disposición para participar en cada una de las actividades del proyecto y aplicar las recomendaciones en beneficio del mismo.
- Velar por el cumplimiento de los objetivos y planes del SGSI.
- Promoviendo actividades de mejora continua y apoyando al Representante de Seguridad para liderar los procesos del SGSI.
- Velando por que se realicen las auditorías internas del SGSI.
- Decidiendo los criterios de aceptación de riesgos y los niveles aceptables de riesgos.
- Apoyando las capacitaciones que permitan que el personal este consiente de las actividades de seguridad de la información.

Se firma en Salcedo_____a los_____días, del mes de_____del año _____

_____

Nombre y Firma

Gerente General

Anexo 4: PLANTILLA DE REGISTROS

Los formatos de registros, deben llevar el encabezado y la codificación definida para ellos en el documento del procedimiento de control de documentos. A continuación muestran estructuras de los formatos, cuándo los formatos son diligenciados, estos se convierten en registros, que permiten evidenciar la ejecución y seguimiento de las actividades propuestas en el sistema de gestión.

FORMATO PARA REGISTRO DE BACKUPS

Fecha de Backup	Nombre del Archivo	Lugar de almacenamiento	Firma Responsable

FORMATO PARA REGISTRO DE BACKUPS

ITEM	DESCRIPCIÓN	OBSERVACIONES
NOMBRE EQUIPO		
SERIAL		
DIRECCIÓN IP		
FECHA COMPRA:		
FECHA INSTALACIÓN:		
USUARIO ADMINISTRADOR:		
CONTRASEÑA ADMINISTRADOR:		
AREA ASIGNADO		
SISTEMA OPERATIVO		
SW OFIMÁTICO		

RAM		
PROCESADOR		
MONITOR		
USUARIO AUTORIZADO		
PROGRAMAS INSTALADOS		
IMPRESORAS INSTALADAS		

FORMATO PARA CONTROL DISPOSITIVOS EXTERNOS

Fecha Uso	Origen – Propietario	Archivo usado	Responsable Uso

Anexo 5: PLANTILLA PARA PROCEDIMIENTO DE CONTROL DE DOCUMENTOS

LISTA DE DISTRIBUCIÓN			
Área	**Responsable**	**Firma**	**Fecha**

CONTROL DE CAMBIOS

Fecha revisión	**Versión del documento**	**Cambio**	**Por qué**

REVISÓ	**APROBÓ**

OBJETIVO

Controlar, aprobar, revisar, conservar y actualizar los documentos y registros (internos y externos) del Sistema de Gestión de Pequeñas empresas, para asegurar la eficacia de sus procesos.

RESPONSABLES

- Coordinador de sistemas.
- Coordinador de Seguridad Industrial.

CONTENIDO

Creación y modificación de documentos.

- Cuando se identifica la necesidad de elaborar o actualizar un documento dentro del Sistema de Gestión, se informa al jefe del proceso quien es el encargado de transmitir esta necesidad al responsable de seguridad del sistema de gestión.
- El responsable de seguridad analiza y evalúa con el jefe del proceso la justificación para la creación o modificación del documento y establece las bases y responsabilidades para la elaboración del mismo.
- Una vez elaborado según los requerimientos de este procedimiento (verificar que incluya encabezado, esquema general, etc.) el responsable le asigna el código correspondiente y diligencia las tablas de control de cambios (se registra las razones por las cuales se modifica el documento) y lista de distribución (personas a las cuales se entregara copia física del documento).
- El documento es revisado y aprobado mediante la firma del responsable de seguridad y la gerencia general en la primera página.
- El responsable de seguridad actualiza la lista maestra de documentos.
- Las copias de los documentos se entrega según la lista de distribución en documentos electrónicos para quienes tienen acceso a un computador y en documentos físicos para el resto del personal, en cuyo caso se hace firmar la lista de distribución por parte de quien recibe el documento.
- De todos los documentos se tiene una copia física original en oficina de sistemas (la cual tendrá las firmas de revisión, aprobación y recepción de

documentos) y una copia electrónica en el PC de sistemas, cada proceso tiene una carpeta en la cual tiene una copia actualizada de los documentos que le competen directamente y que son entregados por el responsable de seguridad.

- En la carpeta de red \\respaldosranchito\2018\sgcsistemas hay acceso a los documentos que cada proceso maneja y allí se encuentran en red los formatos, procedimientos, programas y registros que conforman el programa, cada semana se realiza la copia de la carpeta del Sistema de Gestión en el servidor de documentos que posee la institución como backup en caso de algún incidente.
- El responsable de seguridad es el encargado de identificar y desechar los documentos obsoletos inmediatamente se publique la nueva versión, exceptuando aquellos de manejo especial por exigencias legales.
- El jefe de cada proceso evalúa la necesidad de aplicar algún documento externo que tenga incidencia en la seguridad del sistema de gestión y lo notifica al responsable de seguridad para adquirirlo y registrarlo en el Listado Maestro de Documentos y Registros. Cada dueño de proceso es responsable de notificar la actualización de los documentos externos al responsable de seguridad.
- Los registros son controlados en el Listado Maestro de Documentos y Registros. En este formato se define el tipo de registro y lugar de almacenamiento. En la casilla de almacenamiento se hace un comentario que detalla el Acceso (abierto o restringido), Tiempo de Conservación y Disposición.

INSTRUCCIONES PARA ELABORACIÓN DE DOCUMENTOS

La base documental del Sistema de Gestión de Seguridad de la Información, está conformada por los siguientes niveles:

- **Políticas (PO)**: Son líneas generales de actuación de la organización, en una declaración que estará firmada por la dirección y que será de aplicación según el alcance definido del Sistema de Gestión.

- **Procedimientos (PR)**: Son documentos que definen y describen de forma detallada los procesos o actividades de la organización y aseguran el buen desarrollo y funcionamiento del Sistema de Gestión de Seguridad de la Información. Este documento contiene: encabezado, lista de distribución, control de cambios, firma de revisión y aprobación, objetivo, responsable, normas asociadas, contenido y documentos anexos.
- **Formatos (FR) y anexos (AX):** Son los documentos de soporte y ayuda a los procedimientos, los cuales son de libre configuración a excepción del encabezado.

  Permite generar una estructura que sirva para el ingreso de información que se considerará como registro.
- **Registros:** Son el resultado de diligenciar los formatos, con los que se demuestra el cumplimiento legal y las especificaciones del Sistema de Gestión, algunos podrían ser de una configuración específica según su origen o según la ley.
- **Documentos externos:** Existen documentos y registros de origen externo que son controlados pero mantienen su estructura documental original.

Codificación: se realiza de la siguiente manera:

- Primero se coloca el código del tipo de documento (PO, PR, FR, AX).
- Luego se escribe la sigla del proceso al que aplica: En este caso las iniciales identifican al proceso de la organización al que corresponde el documento, aquí se colocan los datos del.
    - RS: Responsable de Seguridad
    - DG: Directrices gerenciales
    - GA: Gestión administrativa
    - GF: Gestión Financiera
    - GA: Gestión Ambiental
    - GC: Gestión de Calidad
    - PR: Producción.
    - Finalmente se escribe un número consecutivo de tres cifras el

cual inicia en 001 para cada proceso.

Encabezado: se realiza según la siguiente plantilla:

<table>
<tr><td rowspan="3">LOGO DE LA EMPRESA</td><td rowspan="2">NOMBRE DEL PROCEDIMIENTO</td><td>Versión: 0</td></tr>
<tr><td>Fecha de entrada en vigencia: Octubre 08 de 2020</td></tr>
<tr><td>PR-RS-001
<<CODIFICACIÓN>></td><td>Página N de N</td></tr>
</table>

Anexo 6: PLAN DE CONTINGENCIA PARA PEQUEÑAS EMPRESAS. INTRODUCCIÓN

Todo Sistema de Redes de Computadoras (Computadores, periféricos y accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos. Estos problemas menores y mayores sirven para retroalimentar los procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable.

La coordinación de Sistemas de Pequeñas empresas tiene el propósito de proteger la información y así asegurar su procesamiento y desarrollo de funciones institucionales. En base a eso es importante contar con un plan de contingencia adecuado de forma que ayude a Pequeñas empresas a restablecer rápidamente los sistemas de información y capacidades para procesar la información, permitiendo así restablecer la marcha normal de la institución.

El coordinador de Sistemas está obligado a hacer de conocimiento y explicar con lenguaje comprensible a los líderes de los procesos, las posibles consecuencias que la inseguridad insuficiente o inexistente pueda acarrear; de esa manera proponer y poner a consideración las medidas de seguridad inmediatas y a mediano plazo, que han de tomarse para prevenir los desastres que pueda provocar el colapso de los sistemas.

Para realizar el Plan de contingencia informático en Pequeñas empresas se tiene en cuenta la información como uno de los activos más importantes de la Institución, además que la infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para el correcto funcionamiento de la institución. Este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así afrontar contingencias y desastres de diversos tipos.

Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con los sistemas de información (entrada de datos, generación de reportes, consultas, etc.). El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre.

Es necesario prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo mejor posible.

1. GENERALIDADES

1.1. Objetivos

1.1.1. Objetivo General

Formular un adecuado Plan de Contingencia, que permita la continuidad en los procedimientos informáticos de Pequeñas empresas, así como afrontar falla y eventos inesperados; con el propósito de asegurar y restaurar los equipos sistemas de información con las menores pérdidas posibles en forma rápida, eficiente y oportuna.

1.1.2. Objetivos Específicos

- Prevenir o minimizar la pérdida o la corrupción de archivos de datos críticos para la continuidad de las operaciones de Pequeñas empresas.
- Indicar los lineamientos para la recuperación de los servicios informáticos ante un desastre o falla.
- Prevenir o minimizar el daño permanente a los recursos informáticos.

1.2. Alcance

El Plan de Contingencias Informático está basado en la realidad que manifiesta Pequeñas empresas, y puede servir como punto de partida hacia la adecuación y establecimiento de políticas en los diferentes procesos.

2. Marco Conceptual

2.1. Definiciones:

AMENAZA: probabilidad de ocurrencia, durante un período específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo.

VULNERABILIDAD: La vulnerabilidad se refiere al grado de pérdidas relacionadas con un elemento en riesgo (o un conjunto de elementos en riesgo), que resulta como consecuencia de un fenómeno natural o artificial con una determinada magnitud.

ELEMENTOS EN RIESGO: Se refiere a la población, las construcciones, la infraestructura, las edificaciones de las actividades económicas y otros espacios donde éstas se desarrollan, los servicios públicos y el medio ambiente natural que son susceptibles de daños como consecuencia de la ocurrencia de un fenómeno natural o producido por falla humana.

RIESGO: Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.

CONTIGENCIA: Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una organización.

GRAVEDAD: Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación).

SEGURIDAD: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

DATOS: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

INCIDENTE: Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

ACTIVO: Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.

PLAN DE CONTIGENCIA: Es una estrategia que se compone de una serie de procedimientos que facilitan una solución alternativa que permite restituir rápidamente el funcionamiento de los servicios críticos de la Fundación ante la eventualidad que lo afecte de forma parcial o total.

3. Tiempo De Inactividad.

El término tiempo de inactividad es usado para definir cuando el sistema no está disponible (solo para servidores). Los casos inactividad pueden ser planeados o no planeados.

Los casos de tiempos de inactividad planeadas pueden ser por cambio del sistema, cambios de datos, reconfiguración del sistemas o reinicio de servicios.

Los casos de tiempos de inactividad no planeadas pueden ser provocados por fallas del sistema, daño en los servidores, fallas de la red de datos, fallas en el fluido eléctrico.

4. Determinación y detalle de las medidas preventivas

Recurso	**Problema relacionado (riesgo asumido)**	
	Posibilidad de ocurrencia del problema	**Periodo aceptable de inactividad**
Equipo de Escritorio	Media/Alta	4 horas

Sistema de información	Baja	2 horas
Servidores	Baja	2 horas
Impresoras	Media/Alta	4 horas
Telefonía IP	Baja	1 día

5. Análisis de la evaluación de riesgos y estrategias

5.1. Análisis de riesgos

OPERACIÓN	**CONTENIDO DE LA OPERACIÓN**	**PRIORIDAD DE LA OPERACIÓN**
Gestión Productiva	• Control de calidad • Control de la Producción • Seguridad Industrial	ALTA
Gestión Administrativa	• Contabilidad • Marketing • Atención al usuario. • Ventas • Cobros • Evaluación de Costos	MEDIA
Programas	• SAP B1 • Fenix Pro • Control de Pesas	MEDIA

Comunicaciones	• Telefonía IP • Internet	ALTA

5.2. Evaluación y calificación del impacto de los procesos críticos para la continuidad del servicio

RECURSOS	NIVEL DE IMPACTO
Servidores	3
Estaciones de trabajo	2
Sistema de Información	3
Página WEB	1
Teléfono IP	2
Internet	3
Fluido eléctrico	3
Impresoras	1
Red de datos	3

Nivel de Impacto: Alto = 3, Medio = 2, Bajo = 1

5.3. Factores de afectan la seguridad física y la infraestructura

Dentro de estos factores se encuentran los riesgos de origen natural como los desastres y los riesgos artificiales como los ataques terroristas. Ambos riesgos tienen su origen de causas externas Pequeñas empresas y su grado de previsión es muy mínimo. La probabilidad de origen natural es baja, mientras, que los riesgos artificiales son de probabilidad media.

De igual forma se encuentran las descargas o cortes eléctricos, los cuales pueden generar interrupción en las labores administrativas que pueden afectar las Ventas y atención al cliente.

Para la clasificación de los activos de la tecnología informática de la institución se han considerado tres criterios:

- **Grado de negatividad**: Un evento se define con grado de negatividad (Leve, moderado, grave y muy grave).
- **Frecuencia del evento:** Puede ser (Nunca, aleatorio, periódico o continuo).
- **Impacto:** El impacto de un evento puede ser (Leve, moderado, grave y muy grave).

Plan de contingencia: Son procedimientos que definen el cómo una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada. Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en:

- **Leves**: Fallos de energía de corta duración, defecto en disco duro, equivocaciones, daño de archivos, acceso no autorizado etc.
- **Severas**: Destrucción de equipos, incendios, inundaciones, robos, etc.

Riesgo: Es la vulnerabilidad de un activo o un bien, ante un posible o potencial perjuicio o daño. Existen distintos tipos de riesgos:

- **Riesgos Naturales**: Mal tiempo, terremoto, inundaciones, etc.
- **Riesgos tecnológicos**: Incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.
- **Riesgos sociales**: Actos terroristas, desordenes, etc.

Tipos de contingencias de acuerdo al grado de afectación:

- En los sistemas de Información.
- En el equipo computo en general (Procesadores, unidades de disco, impresoras)
- En comunicaciones (ruteadores, nodos, líneas telefónicas)

5.3.1. Posibles Fallas:

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.
- Imposibilidad de acceso a los recursos informáticos, sean estos por cambios voluntarios o involuntarios, tales como cambio de claves de acceso, eliminación de los archivos o proceso de información no deseado.
- Divulgación de información a instancias fuera de la institución fuera de la institución sea mediante robo o infidelidad del personal.

5.3.2. Fuentes de la falla:

- Acceso no autorizado.
- Ruptura de las claves de acceso a los sistemas computacionales.
- Desastres naturales (terremotos, inundaciones, falla en los equipos de soportes causados por el ambiente, la red de energía eléctrica o el mal acondicionamiento de los equipos.
- Fallas del personal clave (enfermedad, accidente, renuncias, abandono del puesto de trabajo.)
- Fallas de hardware (fallas en los servidores o falla en el cableado de red, Router, etc.)

5.3.3. Clases de riesgo

- Incendio
- Robo común de equipos y archivos
- Falla en los equipos
- Acción de virus informático
- Fenómenos naturales
- Accesos no autorizados
- Ausencia del personal de sistemas.

5.4. Factores asociados con la seguridad lógica

Estos riesgos están asociados con fallas en el funcionamiento de los equipos o de los programas de protección, cuyo deterioro o mal uso pueden generar:

- Daños en Discos duros, controladores de red, etc.
- Fallas en equipos de comunicaciones (switches, Routers)
- Daños graves en los archivos del sistema, por error de Hardware o Software
- Intrusión de virus u otros programas malintencionados que puedan dañar los archivos y los equipos computó.

5.5. Factores asociados con la seguridad técnica integral

Daños y/o deterioros por mal uso, falta de mantenimiento y/u culminación de vida util para, switch's, dispositivos, backup, Pc, impresoras.

5.6. Minimizar el Riesgo

Corresponde al plan de contingencia informático, el cual permite minimizar esta clase de riesgos con medidas preventivas y correctivas sobre cada uno.

5.6.1. Incendio o fuego

Grado de negatividad: Muy Severo

Frecuencia de evento: Aleatorio

Grado de impacto: Alto.

Situación Actual	Acción correctiva
El área donde están ubicados los servidores cuenta con un extintor cargado, ubicado muy cerca del Área. De igual forma todos los pisos de la institución cuenta con un extintor debidamente cargados.	No se cumple se recomienda ubicar extintores dentro del are de servidores.
Se ejecutó un programa de capacitación sobre temas de seguridad de la información, a todo el personal perteneciente al área administrativa.	Se cumple
	Realizar copia de seguridad diariamente al servidor de Backup y

No se realiza copias de seguridad periódicas de las BD de los sistemas de información al servidor de Backup.	además realizar Backup del servidor mensual, almacenándolo en donde lo dispongan (CD- ROM, disco duro, base de datos u otros medios de almacenamientos).

5.6.2. Robo común de equipos y archivos

Grado de negatividad: Grave

Frecuencia de evento: Aleatorio

Grado de impacto: Moderado

Situación Actual	Acción correctiva
Se toma registro de la hora de entrada y salida de las personas particulares que ingresan a la institución. En caso de que se presente un incidente, se revisaran las cámaras de seguridad.	Se cumple
Autorización escrita firmada por coordinador del área o el responsable para salidas de equipos de Pequeñas empresas.	NO se cumple es necesario la creación de formato.
Hurto o Robo	Solicitar los guardias de seguridad revise a la salida de la institución a los empleados que culminen sus labores.

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización de Área y el coordinador de Sistemas, esto demuestra que los equipos se encuentran protegidos por cada funcionario autorizado. Tampoco se han reportado casos donde haya habido hurtos de nuestro sistema computo en la fundación sin embargo se recomienda siempre estar alerta.

5.6.3. Falla en los equipos

Situación Actual	Acción correctiva
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Realizar mantenimiento preventivo de equipos por lo menos dos veces al año.
La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Contar con proveedores en caso de requerir remplazo de piezas y de ser posible contar con repuestos de quipos que están para dar de baja.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Colocar UPS a los equipos de Pequeñas empresas.

Analizando el riesgo de falla de los equipos, es recomendable realizar mantenimiento preventivo a los equipos computo e implementar UPS a los equipos para en caso de una falla de energía eléctrica los dispositivos se puedan apagar correctamente.

5.6.4. Acción de virus informático

Situación Actual	Acción correctiva
Se cuenta con un software antivirus para la entidad.	Se cumple, la institución cuenta con antivirus de licenciamiento (Nod 32) válido hasta diciembre del 2019.
Únicamente el área de sistemas es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad.	Se cumple

5.6.5. Terremotos

- **Daños Menores de las instalaciones (Sin Pérdida):** El siniestro puede afectar únicamente parte de la estructura de las instalaciones, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera de las instalaciones, el impacto sería menor, puesto que las actividades se interrumpirían por unas horas o hasta por un día completo como máximo.
- **Con Pérdida De Las Instalaciones:** La pérdida de las instalaciones afectaría gravemente a las operaciones de la institución y los datos pueden verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

5.6.6. Sabotaje

La protección contra el sabotaje requiere:

- Una selección rigurosa de los colaboradores.
- Buena administración de los recursos humanos.
- Buenos controles administrativos.
- Buena seguridad física en los ambientes donde están los principales componentes del equipo.

Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

El problema de la seguridad del computador debe ser tratado como un **problema importante** de dirección. Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Se menciona a continuación algunas medidas que se deben tener muy en cuenta para tratar de evitar las acciones hostiles:

- Ubicar los equipos en lugares más seguros en donde se prevea cualquier contingencia de este tipo.
- Mantener una lista de números telefónicos de las diferentes dependencias

policiales a mano y en lugares donde se pueda hacer un llamado de emergencia.

- Siempre habrá de tomarse en cuenta las Políticas de Seguridad en caso como terrorismo y sabotaje. Es importante la medida de ingreso de personas debidamente identificadas, marcación de zonas de acceso restringido, prevención para explosivo, etc.
- Mantener adecuados archivos de reserva (backup).
- Identificar y establecer operaciones críticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
- Montar procedimientos para remitir registro de almacenamiento de archivos y recuperarlos.
- Usar rastros de auditoría o registro cronológico (Logs) de transacción como medida de seguridad.

6. Plan de recuperación y respaldo de la información

6.1. Actividades previas al desastre

Se considera las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad. Se establece los procedimientos relativos a: Sistemas e Información, Equipos de Cómputo, Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

- **Sistemas de Información:** La Entidad cuenta con una relación de los Sistemas de Información de software de datos, para respaldarla con backup.
- **Equipos de Cómputo:** Se debe tener en cuenta el catastro de Hardware, impresoras, scanner, módems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).

Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia,

teniendo en cuenta la depreciación tecnológica.

- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación o buscar información importante.
- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la entidad.

6.1.1. SERVIDORES

Situación: Falla del servidor controlador de Pequeñas empresas Falla total o parcial del hardware o software del servidor

Contingencia:

Para restablecer los servicios de DHCP, PROXY, ACTIVE DIRECTORY, se deben seguir los siguientes pasos:

- Se desconecta totalmente de la red el servidor.
- Se restablecen las copias de configuración almacenadas en el servidor externo PARADOX.
- Se reinician los servicios Tiempo aproximado: 1 Hora.
- Recursos: Personal de la Coordinación de Sistemas

Situación: Falla del servidor de aplicaciones. Falla total o parcial del hardware o software del servidor

Contingencia:

Para restablecer los servicios de aplicaciones, se deben seguir los siguientes pasos:

- Se reinicia el servidor virtual de FENIX o SAP B1 según sea el caso.
- Se restaura la última copia realizada a la base de datos almacenada en el disco \\Servidor_archivos\administracion\sistemas\respaldosSAP o Resapaldos_FENIX(FECHA), también existe un consolidado mensual en el servidor de respaldos externo PARADOX.
- Se restaura la base de datos de fénix o Sap B1.

- En caso de FENIX Pro se debe realizar un UPDATE de la BD para que la información se indexe al último cambio.
- En caso de SAP B1 se debe reiniciar el servicio SQL server.
- Se reinician todos los PC que acceden al sistema integral de información o algún otro servicio alojado en este servidor

Tiempo aproximado: De 2 a 4 horas
Recursos: Personal de la Coordinación de Sistemas.

Si el plan de contingencia es ejecutado parcial o totalmente, es obligación del coordinador de sistemas, realizar un análisis de las causas que ocasionaron la falla, presentar el respectivo informe a la gerencia y caso de ser necesario se realizara un plan de mejora.

6.2. Falla en las comunicaciones (Teléfono, internet)

Ante una falla en las comunicaciones (telefonía fija e internet), se optará por la telefonía móvil, para lo cual se informará el número celular de emergencia a las entidades aseguradoras que con mayor frecuencia tenemos contacto, esta línea la tendría a cargo el recepcionista y los líderes de los procesos.

Para soportar una falla en las comunicaciones, la clínica realizara las siguientes actividades:

- Contar con un celular con minutos permanente en registro y control.
- Entrenar al recepcionista para que pueda brindar la información adecuada ante estos casos.

Anexo 7: MODELO DE CLÁUSULA DE CONFIDENCIALIDAD

Este modelo propuesto se presenta como una orientación que sirve de guía, que deberá ser adaptada en cada contrato con empleado o proveedor, incluso se recomienda su revisión por un abogado, antes de la firma del mismo.

CONTRATO DE CONFIDENCIALIDAD

El presente Acuerdo de Confidencialidad es un instrumento que lo suscriben el empleado/a (bajo cualquier modalidad de prestación de servicios), y tiene como fin afianzar el compromiso del empleado/a con la institución, respecto del uso de los recursos informáticos que la institución dispone y que entrega a cada uno de sus empleados/as, para el cumplimiento de sus funciones; en consecuencia, quienes forman parte de esta entidad, al suscribirlo aceptan las limitaciones y restricciones de acceso a la información y a la divulgación de la misma.

El acceso a la información que los empleados/as tienen para cumplir con las funciones a ellos encomendadas, es libre de acuerdo al nivel de competencia que desempeñen, por tanto, es preciso proteger la información constituida en patrimonio institucional. El uso indebido o ilegal de la información acarrearía consecuencias negativas en contra de los intereses institucionales y nacionales, por tanto, a partir de la firma de este acuerdo, el empleado/a que haga mal uso de la misma o de los medios que la contienen, se someterá a las sanciones que las disposiciones legales y reglamentarias establecen para el efecto.

COMPARECIENTES:

Comparecen a la celebración de este Acuerdo de Confidencialidad, el/la Señor/a

,

en su calidad de empleado/a, titular de la cédula de ciudadanía: ; y, la institución XXXXXXXXXXX, representada por XXXXXXXXXX en su calidad de gerente general, quienes libre y voluntariamente suscriben este acuerdo, conforme las siguientes disposiciones:

CLAUSULA PRIMERA.- La institución XXXXXXXXX posee una plataforma y sistemas informáticos debidamente registrados que conforman el patrimonio

tecnológico de la entidad, constituidos por la plataforma informática, red de comunicación, dispositivos informáticos
(hardware y software) y todos los demás recursos integrados con la tecnología de la información, que permiten el desarrollo diario de sus actividades, los cuales están a disposición limitada de todos los empleados/as, conforme sus funciones y las necesidades institucionales.

La institución XXXXXXXX, en el cumplimiento de su misión y de las disposiciones constitucionales y legales que regulan su actividad, crea información a través de sus diferentes procesos generadores de valor y habilitantes, información que es de su propiedad y, cada empleado/a acepta y reconoce tal calidad sin objeción alguna, por lo que, el acceso a ésta es limitado, y los empleado/a podrán acceder a la misma, conforme las necesidades de cada función y con las restricciones que al respecto señalan las normas legales.

Se considera información de propiedad de la institución y de prohibida publicación y/o divulgación, toda clase de documentos, archivos e información que se encuentren en soportes físicos o electrónicos, así como registros, diagramas, flujogramas, dibujos, fotografías, disposiciones internas, memorándums, programas para computadora desarrollados al interior de la entidad, creaciones en multimedia o equipos digitales, logotipos, ideas, proyectos y en general toda clase de datos que se generen en la entidad, como parte de sus labores.

Conforme lo expuesto, el/la empleado/a XXXXXXXXXXXXXXXXXX, reconoce y acepta que toda la información es de propiedad de la entidad, salvo aquella que por su naturaleza es pública y se encuentra a disposición de la sociedad por intermedio del portal institucional.

El empleado/a reconoce y acepta que todos los recursos informáticos que se encuentran definidos bajo el dominio “xxx.xx.xx” son de propiedad exclusiva de la institución XXXXXXXXX.

El empleado/a reconoce y acepta que el uso del correo electrónico de la institucional y el acceso al servicio de Internet a través de la red interna, constituyen una herramienta que la entidad otorga, a fin de que pueda realizar sus labores, por lo que, su uso a más de estar limitado al ejercicio de las funciones de cada empleado/a,

podrá ser restringido total o parcialmente, sin previo consentimiento del empleado/a.

De ser dispuesta la medida de restricción total o parcial para los servicios de correo electrónico o de internet o ambos a la vez, se comunicarán al empleado/a para que pueda adoptar medidas de comunicación diferentes, a fin de cumplir con sus funciones.

Por ser el acceso a correo externo ilimitado, toda clase de información, documentos, comunicación o mensaje de datos enviado por esta vía, deben de guardar cuidado con la imagen institucional, por lo que la empresa XXXXXXXXX adoptará las medidas necesarias para evitar daños en su imagen y fugas de información, sin que por ello se pueda alegar violación de privacidad.

El/la empleado/a acepta y reconoce que la información de la Institución XXXXXXXXX constituye un bien intangible invalorable, por lo que los riesgos por mal uso y/o divulgación indebida de la misma comportan que la entidad deba tomar medidas respecto de la integridad documental e informática.

El empleado/a se obliga a mantener y guardar confidencialidad y reserva respecto de la información relevante que le sea entregada para cumplir con sus labores, quedando prohibido divulgar por cualquier medio, distribuir, reproducir, traducir, utilizar, disponer, y/o publicar la información que le haya sido proporcionada, que haya obtenido o que llegue a conocer por cualquier canal de comunicación institucional.

En el soporte informático que la institución proporcione a cada empleado/a, siempre que así se requiera para cumplir con sus funciones, éste/a podrá almacenar y mantener información personal, si la información no causa problemas a los sistemas de la entidad y si no supera el tamaño de almacenamiento que impida el normal funcionamiento del equipo.

Cada empleado/a será responsable de la asignación, uso y cuidado de sus claves de acceso a los sistemas informáticos, las cuales son personales e Intransferibles, sin que se pueda alegar necesidades personales o institucionales, para divulgarlas por cualquier medio, permitiendo que otros usuarios/as accedan a los sistemas con claves ajenas.

El empleado/a que ingrese información a las herramientas tecnológicas y de información que la Institución XXXXXXXXX le ha proveído para el desempeño y desarrollo de su trabajo, deberá asumir la responsabilidad de los datos ingresados procurando que los mismos sean veraces, coherentes y oportunos.

CLÁUSULA SEGUNDA.- El empleado/a se compromete a utilizar tanto la información documental como digital y los recursos tecnológicos de la Institución XXXXXXXXX, con ética, reserva y profesionalismo conforme las normas y reglamentos vigentes.

La Institución XXXXXXXXX respetará las normas y procedimientos que garantizan la privacidad de los empleado/a, siempre que las mismas no alteren las medidas de seguridad institucional.

El empleado/a acepta que la Institución XXXXXXXXX puede ejercer control y seguimiento de la información institucional que estén bajo su custodia, así como de los recursos tecnológicos a él proporcionados, con la finalidad de garantizar el uso correcto de la información y los sistemas informáticos, cuando lo estime pertinente y sin necesidad de notificación previa.

CLÁUSULA TERCERA.- La Institución XXXXXXXXX, previa autorización judicial y con la Obligación de guardar en secreto la información para cuando sea necesario, podrá abrir, retener y examinar la correspondencia electrónica contenida en la cuenta individual de correo electrónico del usuario/a de la institución, así como la información electrónica que este contenida en los recursos tecnológicos asignados

CLÁUSULA CUARTA.- El empleado/a acepta y declara que se somete a las responsabilidades y sanciones que por omisión a este acuerdo le sean imputables, sin perjuicio de las responsabilidades civiles o penales a que hubiere lugar en virtud de la ley.

El presente Acuerdo de Confidencialidad de la Información, tendrá vigencia durante el tiempo que el/la empleado/a preste sus servicios a la Institución XXXXXXXXX; y, por ética profesional, posteriormente a su salida de la institución, sin perjuicio de que se vaya adoptando nuevas medidas de seguridad, las cuales serán parte de este acuerdo.

Para constancia, las partes lo suscriben por duplicado, aceptándolo en todas su partes. Lugar y fecha:

Firmas:

Anexo 8: ACTA DE DEVOLUCION DE ACTIVOS DE INFORMACION

YO, xxxxxxxxxxxxx con ci xxxxxxxxxx, por medio de la presente Acta vengo a hacer devolución de los siguientes activos de información, asignados a mi cargo para el desempeño de mis funciones:

A) Activos tales como teléfono fijo, teléfono móvil, CPU, Teclado, Mouse, Máquina fotográfica, muebles de oficina, etc.

N°	BIEN	MARCA	N° SERIE	PLACA INVENTARIO
1				
2				
3				
4				
5				

B) En cuanto a temas de seguridad de información, se entrega lo siguiente:

1.1.- Computador

1.2.- Notebook

1.3.- Sistemas Internos (detallar)

1.4.- Otros (detallar)

2) Carpetas y/o documentos con temas relacionados con:

Nombre / Firma Nombre / Firma

Anexo 9: MODELO INVENTARIO DE SOFTWARE Y APLICACIONES

N°	DEPENDENCIA / UBICACIÓN	DISPOSITIVO	MARCA Y MODELO	SERIE	CARACTERÍSTICAS	ESTADO	CUSTODIO	OBSERVACIONES

Anexo 10: MATRIZ SOLICITUD ACCESO A SISTEMAS INFORMÁTICOS.

CI	NOMBRE	CARGO	FECHA	RESPONSABLE	MODULO	OBSERVACIONES	FIRMA

Anexo 11: TABLA COPARATIVA DE HERRAMIENTAS DE CIFRADO.

La presente tabla comparativa sirve como guía para que la institución pueda elegir la mejor herramienta que se ajuste a sus necesidades, se ha elegido 5 herramientas open source que ayudan a realizar la gestión de encriptación en las pequeñas empresas.

Nombre	SO Soportados	Licencia	Tipo de encriptación
GnuPG	Linux, Mac, Windows	OpenPGP	Algoritmo de cifrado de 256 bits
AES Crypt	Linux, Mac, Windows	Software de código abierto totalmente gratuito	Algoritmo de cifrado de 256 bits
DiskCryptor	Windows	OpenPGP	Algoritmo AES-256 en modo LRW
EncFS	Linux	Licenciado bajo la GPL	Algoritmo de cifrado de 256 bits
Axcrypt	Windows	Gratis, versión premium tiene costo.	Seguridad de archivos con encriptación de 128 bits o 256 bits AES.

Anexo 12: LISTA DE VERIFICACIÓN DEL PROYECTO PARA IMPLEMENTACIÓN DE ISO 27001

Controles de seguridad de la información pequeñas empresas **CHECK LIST ISO 27001**				
ACTIVIDAD	**DOCUMENTADO**			
	COMPLETO	PARCIAL	NINGUNO	PORCENTRAJE
POLÍTICAS	19	0	0	100%
SEGURIDAD FISICA	6	0	0	32%
1. Uso adecuado de los activos	0	0	0	0%
2. Gestión de los recursos tecnológicos	0	0	0	0%
3. Control de acceso físico	0	0	0	0%
4. Protección y ubicación de los equipos	0	0	0	0%
5. Gestión de medios removibles	0	0	0	0%
6. Riesgos relacionados con terceros.	0	0	0	0%
SEGURIDAD LOGICA	7	0	0	36%
1. Control de acceso lógico	0	0	0	0%
2. Definición de roles de usuario	0	0	0	0%
3. Protección contra software malicioso	0	0	0	0%
4. Copias de respaldo	0	0	0	0%
5. Seguridad para el intercambio de información	0	0	0	0%
6. Gestión de contraseñas de usuario	0	0	0	0%
7. Escritorio y pantalla limpia	0	0	0	0%
SEGURIDAD LIGADA AL PERSONAL	3	0	0	16%
1. Acuerdos de confidencialidad	0	0	0	0%
2. Gestión del talento Humano	0	0	0	0%
3. Culminación o cambio de contrato laboral	0	0	0	0%
COMINICACION Y OPERACIONES	3	0	0	16%
1. Acceso a internet	0	0	0	0%
2. Correo electrónico	0	0	0	0%
3. Segregación de redes	0	0	0	0%

Anexo 13: MATRIZ RIESGOS Y OPORTUNIDADES

IDENTIFICACIÓN DE LOS RIESGOS		ANALISIS DE RIESGOS			EVALUACIÓN DEL RIESGO			CONTROLES EXISTENTES		REVISIÓN DE LA EFECTIVIDAD	
PROCEDIMIENTO	DESCRIPCIÓN DEL RIESGO	FUENTE DEL RIESGO	CAUSAS	CONSECUENCIAS	PROBABILIDAD	IMPACTO	INDICE DE RIESGO	MEDIDA DE CONTROL Y TEMPORALIDAD	EFECTIVIDAD DEL CONTROL	ACCIÓN DE MEJORA	RESPONSABLE DE IMPLEMENTAR