UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO/A EN SISTEMAS INFORMÁTICOS

TEMA: Propuesta de Sistema de Gestión de Seguridad de la Información para el centro de datos de la empresa Leterago del Ecuador S.A

AUTOR/ A: Alvaro Alejandro Vallejo Cáceres

TUTOR/ A: Ing. Tannia Cecilia Mayorga Jácome
Ing. Joe Luis Carrión Jumbo

QUITO- ECUADOR

AÑO: 2018

DECLARACIÓN DE AUTORÍA

El documento de tesis con título: “PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE DATOS DE LA EMPRESA LETERAGO DEL ECUADOR S.A”, ha sido desarrollado por el señor Álvaro Alejandro Vallejo Cáceres con C.C. No. 0604264192 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

_____

Álvaro Alejandro Vallejo Cáceres

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación **"PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE DATOS DE LA EMPRESA LETERAGO DEL ECUADOR S.A."**, presentado por Álvaro Alejandro Vallejo Cáceres, estudiante de la Carrera Ingeniería en Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D. M., 27 de junio del 2018

TUTOR	TUTOR
---	---
Ing. Joe Carrión Jumbo	Ing. Tannia Mayorga

AGRADECIMIENTO

Agradezco a mis Directores de Tesis Ing. Tannia Mayorga y al Ing. Joe Carrión por su apoyo, aporte con sus conocimientos y su valioso tiempo que fue dedicado en las reuniones para llevar a cabo la elaboración de esta tesis.

A la Ing. Tannia Mayorga y el Ing. Joe Carrión quien me encaminó durante la elaboración del Plan de Tesis.
A Ing. Víctor Tolcachier Gerente de tecnología informática de la empresa Leterago del Ecuador S.A quien autorizó el desarrollo de esta Tesis en la Organización con el objetivo de mejorar la seguridad informática del Centro de Datos de la empresa.

A Ing. Carlos Estévez y a la Ing. Tatiana Pozo miembros del departamento de tecnología informática de la empresa Leterago del Ecuador S.A por colaborar durante el proceso de investigación durante las entrevistas y reuniones.

Compañeros de trabajo de la empresa Leterago del Ecuador S.A por colaborar en forma voluntaria y eficaz para esta indagación que ayudará a que los usuarios tengan conocimientos acerca de la seguridad informática.

DEDICATORIA

Dedico este trabajo a Dios principalmente que ha sido mi fuente de fortaleza y por su incondicional amor hacia mí y por haberme bendecido en mi camino.

A mis padres Ivonne del Rocío Cáceres Noboa y Álvaro Javier Vallejo Rodríguez por su ejemplo de esfuerzo y lucha constante para lograr mis objetivos.

A mis hermanos Antonio Xavier Vallejo Cáceres y María Belén Vallejo Cáceres por su apoyo incondicional y por ser mi ejemplo a seguir que todo lo que uno desea se consigue con esfuerzo y perseverancia y aprendí de ellos una valiosa enseñanza: “en el camino al éxito va a estar lleno de obstáculos y fracasos pero al final valdrá la pena.”

TABLA DE CONTENIDOS

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN (ABSTRACT)

El mencionado proyecto se basa en la elaboración de una propuesta de un Sistema de Gestión de Seguridad de la información para el Centro de Datos de la empresa Leterago del Ecuador S.A, utilizando las Normas ISO 27001 e ISO 27005 que permitieron identificar los riesgos existentes en los activos de información y la forma de mitigarlos, controles que utilizan en la organización para evitar riesgos con esta información se logró realizar las políticas de seguridad de la información y la propuesta de SGSI que permitirá a la organización disminuir los riegos a un nivel aceptable por lo tanto poder proteger las actividades que son esenciales en el giro del negocio.

PALABRAS CLAVE

Seguridad, Información, Normas, Riesgos, Controles.

ABSTRACT

The aforementioned project is based on the elaboration of a proposal of an Information Security Management System for the Data Center of the company Leterago del Ecuador SA, using the ISO 27001 and ISO 27005 Standards that allowed to identify the existing risks in the information assets and the way to mitigate them, controls that are used in the organization to avoid risks with this information, it was possible to carry out the information security policies and the ISMS proposal that will allow the organization to reduce the risks to an acceptable level. so much to be able to protect the activities that are essential in the turn of the business.

KEY WORDS

Security, Information, Standards, Risks, Controls.

INTRODUCCIÓN

Antecedentes de la situación objeto de estudio

La seguridad informática en las organizaciones es un tema que requiere de especial atención por el avance tecnológico apresurado que en la actualidad se presenta, además de las constantes preocupaciones por reincidencias de fallas en los procesos, malos entendidos, conformismo de ciertos trabajadores en obtener un salario suficiente para pagar sus obligaciones, un desinterés por el futuro, crecimiento de la organización, y sí le añadimos la falta de control interno operativo de la organización, esto quiere decir entonces que existe una posibilidad de incidir en una pérdida financiera.

El control interno encuadra un propósito de la organización y el conjunto de medidas a ser adoptadas dentro de una organización para así poder tener a buen recaudo sus activos, cotejar la veracidad de su información financiera-administrativa, impulsar la efectividad en las operaciones, alentar la indicación de las políticas fomentando el cumplimiento de los objetivos planteados, ya que el control interno es un compromiso de todos los miembros de la organización.

La información del personal, los sistemas, entre otros elementos, como pieza medular en una organización, se puede alcanzar mediante medidas preventivas o correctivas, o mediante un plan de proyectos de prevención para la disminución de riesgos para lo cual es de vital importancia tener en cuenta las normas ISO 27001 e ISO 27005, que ayudarán en el presente proyecto.

Planteamiento del problema

Contextualización

Macro

"Según el Computer Security Institute (CSI) de San Francisco; Aproximadamente entre el 60 y el 80% de los incidentes de red son causados desde dentro de la misma.". Significa que por la cantidad de activos, su información, los servicios que ofrece es importante considerar la evaluación de riesgos a los que se expone la organización.

Meso

"En Estados Unidos según el Instituto Nacional de Estándares y Tecnología (NIST) se está aplicando una guía para la construcción de programas de seguridad de tecnologías de la información y soporte efectivos, con requerimientos especificados en la Administración de Seguridad de la Información Federal (FISMA)" su función principal es: "establecer de manera clara la diferencia entre los tres componentes principales de un programa para desarrollar la cultura en seguridad de la información: concientización, entrenamiento y educación" en las organizaciones que consideren: lineamientos, supervisión, evaluación, retroalimentación por parte del personal en el programa. (Villamizar, 2013). Esto significa que una organización que tiene varios usuarios, y una excelente infraestructura es fundamental dar a conocer la importancia que tiene la seguridad de la información para así evitar futuras pérdidas de información y además pérdidas económicas.

Micro

En Ecuador, según la revista Ekos (2013), menciona acerca de una "campaña de concienciación a cargo de la empresa Netlife, una empresa que brinda servicio de internet de alta velocidad en nuestro país junto con McAfee, designando embajadores por la seguridad informática dentro del personal comercial de Netlife, la tarea se centra en buscar métodos de concienciación para informar a la ciudadanía sobre los riesgos asociados a la falta de seguridad, bullying y las mejores formas de prevenir problemas de seguridad informática en su hogar y trabajo." (Ekos, 2013)

Según Deloitte en el Ecuador las organizaciones no realizan muchas campañas de seguridad informática, por lo que las empresas son más más vulnerables y son víctimas de los ciberataques provocando pérdidas finacieras.

En la figura 1.1 se muestra el Árbol del problema el cuál se ha elaborado en función a la carencia de medidas de seguridad en el centro de datos de la empresa Leterago del Ecuador S.A

Árbol de problemas

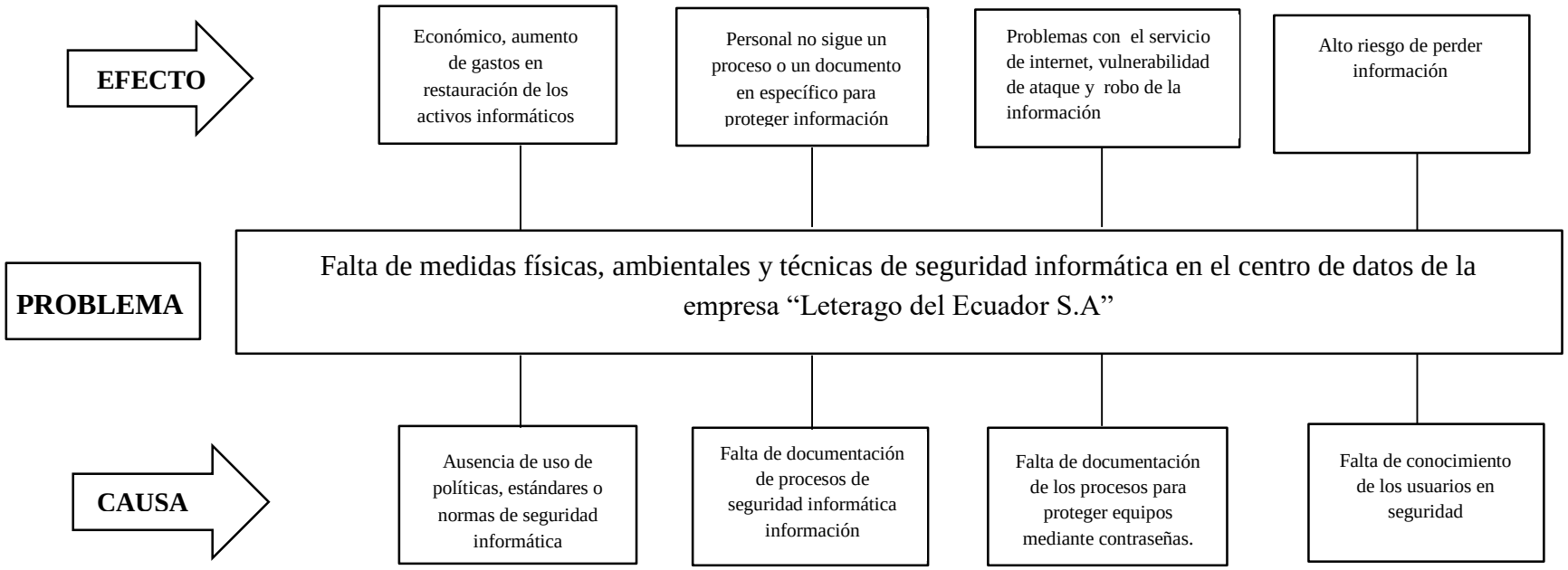


Figura. 1.1. Árbol del Problema
Fuente: Investigación propia

Formulación del problema

La seguridad informática en el manejo del centro de datos incide en el desarrollo de negocio de la empresa Leterago del Ecuador S.A.

Justificación

En el sector empresarial, específicamente en la capacitación del personal es necesario el uso del internet, correo electrónico interno, etc. La compañía se ve obligada a actualizar o modernizar su software para una mejor funcionalidad de los mismos. La instalación de los parches, para lo cual se necesita guiar y orientar a los usuarios en el aspecto de seguridad para evitar justamente la inseguridad de la información. Actualmente la seguridad informática en las organizaciones no es tomada con la seriedad que requiere, en muchos casos cuando el riesgo se materializa en esos instantes las organizaciones toman, sugieren o desarrollan medidas para poder contrarrestar.

En toda compañía deben existir reglas, normas y políticas que ayuden a los usuarios a evitar cometer errores de seguridad. Según Deloitte Latinoamérica en el año 2016 menciona: “es deseable que la inversión en ciber-riesgos y seguridad de la información no sea inferior al 3% del presupuesto de Tecnología Informática. En las industrias más maduras el porcentaje supera el 10%” (Deloitte, 2016). En la empresa Leterago del Ecuador S.A el jefe del departamento de infraestructura de tecnología informática en lo que le resta de tiempo lo dedica en revisar temas de seguridad informática ya que generalmente sus funciones son: realizar control, instalación, configuración y reparación de servidores, por este motivo dicha investigación será de utilidad para proponer el sistema de gestión de seguridad de la información para mejorar la seguridad informática de la compañía, colaborando de esta manera a jefaturas del área de Tecnología Informática como a los usuarios a mantener un ambiente tecnológico que brinde confianza a los usuarios.

En ocasiones los usuarios que usan el Internet y Correo Electrónico sin restricción alguna en las organizaciones se viene convirtiendo en un tema de importancia ya que en muchas ocasiones no tienen el suficiente conocimiento para saber en qué páginas puede navegar y cuáles no.

Al tener libre acceso, la curiosidad de los usuarios conlleva a ingresar a páginas web diferentes a las utilizadas en sus labores cotidianas causando falta de atención y concentración en sus labores.

La investigación se puede llevar a cabo ya que se cuenta con la aprobación de la gerencia de T.I de la empresa Leterago del Ecuador S.A

Objetivo General

- Realizar una propuesta de sistema de gestión de seguridad de la información para reducir el número de incidencias evitando pérdidas económicas en la empresa utilizando la Norma ISO 27001.

Objetivos Específicos

- Contextualizar los conceptos básicos de la seguridad de la información para la propuesta del Sistema de Gestión de Seguridad de la Información.
- Realizar un análisis de riesgos amenazas y vulnerabilidades para establecer la situación actual de la empresa Leterago del Ecuador S.A.
- Elaborar una propuesta que permita disminuir a un nivel aceptable los riesgos, amenazas y vulnerabilidades en que se encuentra el centro de datos.
- Crear la propuesta del sistema de gestión de seguridad de la información del centro de datos de la empresa Leterago del Ecuador S.A.

Alcance

El presente proyecto, permitirá la elaboración de una propuesta de un Sistema de Gestión de Seguridad de la Información para el Centro de Datos de la empresa Leterago del Ecuador S.A, basada en las normas ISO 27001 e ISO 27005 para los sistemas de información. Se analizará los riesgos que puedan existir en la organización, y se verificará la necesidad de que exista un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa Leterago del Ecuador S.A,

mediante un estudio que aborde la situación actual de la seguridad de la información de la compañía.

Se examinarán las demandas de seguridad de la información a través de las operaciones y transacciones realizadas para elaborar una propuesta de Sistema de Gestión de Seguridad de la Información para la compañía, evaluando que tan acertado sea el proyecto.

La propuesta de un Sistema de Gestión de Seguridad de la Información para la empresa Leterago del Ecuador S.A permitirá que los riesgos de seguridad de la información sean analizados, contrarrestados y sea factible minimizarlos por la organización de una manera que permita al personal de Tecnología Informática documentar, valorar los riegos de tal forma que cuando ocurra algún siniestro con la información se pueda actuar de manera rápida y eficaz.

Descripción de los capítulos

Capitulo I. Fundamentación Teórica, en este capítulo se describe los conceptos fundamentales acerca de las Normas ISO 27001 e ISO 27005 y la forma de elaborar un Sistema de Gestión de Seguridad de la Información tomando en cuenta los activos de información y sus características para poder apoyar a la continuidad de negocio, etc.

Capítulo II. Propuesta, en este capítulo se describe el modelo de propuesta a seguir en la organización Leterago del Ecuador S.A empezando por la descripción de la empresa, la ubicación geográfica, información del representante legal, la propuesta que se basa en el modelo de negocio que tiene la organización.

Capítulo III. Implementación, en este capítulo se describe la identificación de riesgos, los controles vigentes, normas para mitigar y minimizar los riesgos, políticas propuestas y la implementación de la propuesta.

1. CAPÍTULO I. FUNDAMENTACIÓN TEÓRICA

1.1 ISO 27001

"La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización." (Advisera, 2018). Pemite que las organizaciones se certifiquen mediante el uso y la aplicación de sus normas y que pueda garantizar su funcionamiento en base a las normas ISO 27001.

ISO 27001, es una federación mundial de organismos nacionales de normalización alrededor de 160 países, trabajan a nivel de Comités Técnicos, tienen al menos 19,000 estándares publicados desde 1947 (creación), 1951 (publicación). Trabaja en función a 8 principios de gestión: 1.Orientación al cliente, 2.Liderazgo, 3.Participación del personal, 4.Enfoque de procesos, 5.Enfoque de sistemas de gestión, 6.Mejora Continua, 7.Enfoque de mejora continua, 8.Relación mutuamente beneficiosa con el proveedor. Incremento de la demanda en las empresas por implementar sistema de gestión estándares (ISO 9001, ISO 27001, ISO 22301, ISO 20000 otras). Los estándares ISO son aplicables a cualquier tipo y tamaño de empresa. (Alvaro, 2018)

A continuación se detalla las normas ISO, sus estándares y la evolución que ha tenido al pasar de los años, como se ilustra en la Tabla 1.1:

Tabla. 1.1. Iso y sus estándares

NOMBRE DE LA NORMA	NÚMERO DE CERTIFICACIONES EN EL 2013	NÚMERO DE CERTIFICACIONES EN EL 2012	EVOLUCIÓN	EVOLUCIÓN EN %
ISO 9001	1 129 446	1 096 987	32 459	3%
ISO 14001	301 647	284 654	16 993	6%
ISO 50001	4 826	2 236	2 590	116%
ISO/IEC 27001	22 293	19 620	2 673	14%
ISO 22000	26 847	23 278	3 569	15%
ISO/TS/ 16949	53 723	50 071	3 652	7%
ISO 13485	25 666	22 317	3 349	15%
TOTAL	1 564 448	1 499 163	65 285	4%

Fuente: **(GlobalSTD, 2018)**

1.1.1. Función de la ISO 27001 en una organización

La parte principal en donde se centra dicha norma es la de proteger la confidencialidad, integridad y disponibilidad de la información en una organización. Esto se lo realiza investigando cuál o cuáles son los potenciales problemas que podrían afectar la seguridad de la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). (Advisera, 2018)

Activos de Información: Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección. En los activos se encuentran relacionados directa o indirectamente (SSI, 2015).

Como se muestra en la figura 1.2 los activos de información dependiendo de su configuración son vulnerables a los diferentes ataques o amenazas que a la vez causan un impacto importante a la organización y esto representa un riesgo para la continuidad del negocio.

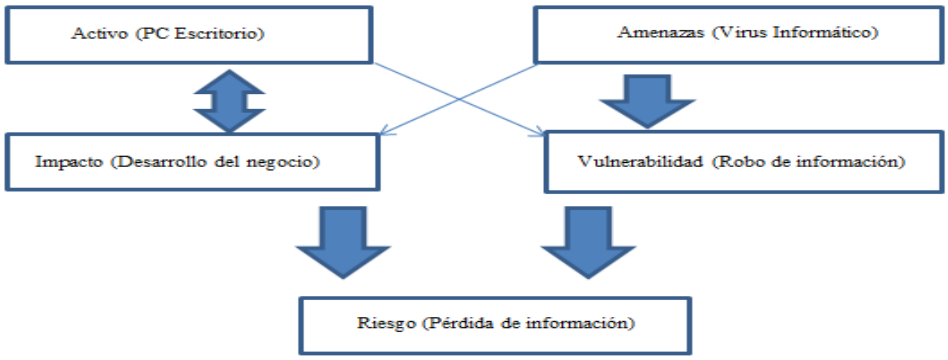


Figura. 1.2. Activos de información
Fuente: (SSI, 2015)

Básicamente, "la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información." (Advisera, 2018), como se puede observar en la figura 1.3:

Figura. 1.3. SGSI en una empresa
Fuente: (Advisera, 2018)

1.1.2. Gestión del riesgo

"El análisis de riesgos proporciona términos de activos, amenazas y salvaguardas, controla todas las actividades. La fase de tratamiento estructura las acciones a realizar en materia de seguridad para anular las amenazas detectadas por el análisis" (Amutio, 2013).

Se entiende como peligro o daño todo aquello que pueda afectar a su funcionamiento directo o a los resultados que se obtienen. (Calidad, 2017)

En la figura 1.4 según la norma ISO 31000, se ilustra cómo se determina un riesgo, a partir de la identificación del riesgo, el análisis y la evaluación del mismo para poder determinar si dicho riesgo requiere o no de atención, si el riesgo requiere atención hay que tratarlo de inmediato mediante la comunicación y consulta para poder minimizarlo de alguna manera y si no requiere de atención simplemente se realiza un seguimiento del riesgo y se realiza una revisión si es posible se realiza una bitácora del mismo.

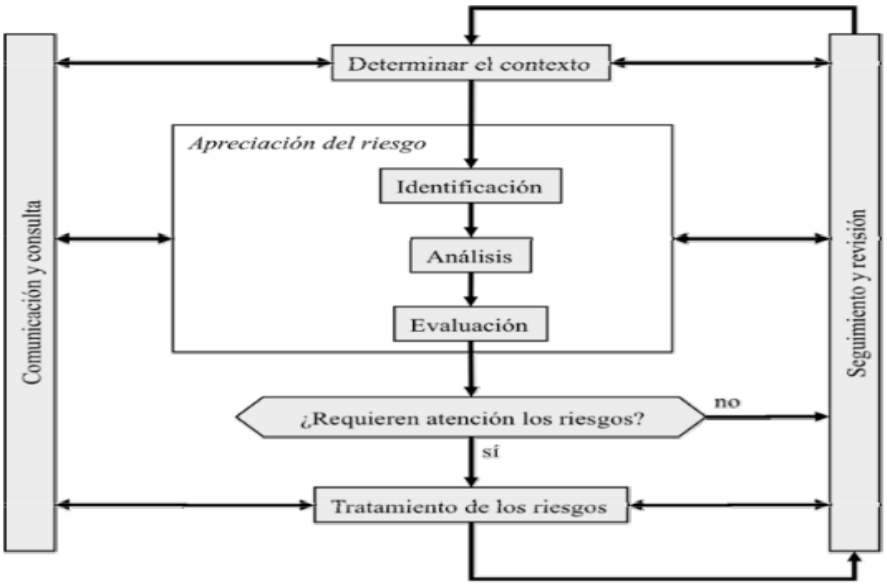


Figura. 1.4. Proceso de gestión de riesgos.
Fuente: (Colorado et al., 2015)

1.1.3. Seguridad de la información

La seguridad de la información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada. La seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Podemos entender como seguridad un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo.

1.1.4. Continuidad del negocio

"Es un conjunto de medidas que adopta una empresa para garantizar que su operación no se vea afectada, de una forma substancial, por eventos que están fuera de su control. Existe una amplia gama de dichos eventos llamados contingencias, desde una simple caída de sistema, hasta un incendio, una inundación o una pandemia." (Greenhouse, 2017).

La continuidad del negocio es importante en una organización para poder tener a salvo la infraestructura y los servicios que brinda a sus clientes internos y externos. También garantiza sus operaciones diarias a pesar de cualquier emergencia que pueda suscitar en un futuro, además para no perder credibilidad con los clientes.

1.1.5. Ciberseguridad

"Es un proceso que implica prevención, detección y reacción o respuesta, y que debe incluir un elemento de aprendizaje para la mejora continua del propio proceso." (Telefónica, 2016)

Tabla. 1.2. Etapas de la gestión de la ciberseguridad

ELEMENTOS	ACCIÓN			
	PREVENCIÓN	DETECCIÓN	RESPUESTAS	INTELIGENCIA
Control de accesos y gestión de identidades	X			
Prevención de fuga de datos	X			
Seguridad de red	X			
Gestión de vulnerabilidades	X	X		
Monitorización continua		X		
Sistemas de recuperación			X	
Contramedidas			X	
Compartición de datos				X
Datos Open Source				X

Fuente: (Telefónica, 2016)

1.1.6. Tecnología de la información

"Se consideran tecnologías de la información aquéllas cuyo propósito es el manejo y tratamiento de la información, entendida ésta como conjunto de datos, señales o conocimientos, registrados o transportados sobre soportes físicos de muy diversos tipos. Las tecnologías de la información abarcan técnicas, dispositivos y métodos que permiten obtener, transmitir, reproducir, transformar y combinar dichos datos, señales o conocimientos." (Valle, 1986)

Se expone en la tabla 1.3 la inversión de la empresa en recursos tecnológicos, recursos humanos, instalaciones, aquí se detallan los servicios principales que la empresa brinda a sus usuarios para el normal desenvolvimiento de sus actividades cotidianas y el personal de T.I responsable de cada uno de los servicios y soportes a cargo del departamento, además se detalla las instalaciones que tienen para mantener una infraestructura tecnológica de calidad en sus instalaciones.

Tabla. 1.3. Inversión de la organización en recursos tecnológicos

NOMBRE DEL RECURSO	CANTIDAD	PRECIO UNITARIO	TOTAL
Servidor Correo Electrónico	1	$ 35.000,00	$ 35.000,00
Central Telefónica	1	$ 15.000,00	$ 15.000
Servicio Video Conferencia	1	$ 2.000,00	$ 2.000
Aplicaciones Web	5	$ 20.000	$ 100.000,00
Redes Móviles	6	$ 500	$ 3.000
Equipos Móviles	18	$ 1.000	$ 18.000
Computadoras	100	$ 1.000	$ 100.000,00
Portables	65	$ 1.200	$ 78.000,00
Impresoras	53	$ 1.000	$ 53.000,00
Switch	15	$ 1.000	$ 15.000,00
Firewall	1	$ 5.000	$ 5.000,00
Windows Server 2017 (Datacenter)	1	$ 10.000	$ 10.000,00
Microsoft SQL Server 2012 Enterprise	1	$ 15.000	$ 15.000,00
Microsoft Windows 10 para PC	165	$ 200	$ 33.000,00
Gerente de T.I	1	$ 20.000	$ 20.000,00
Jefe Nacional de T.I	1	$ 3.500	$ 3.500,00
Jefe Regional de T.I	1	$ 1.900	$ 1.900,00
Jefe de Infraestructura de T.I	1	$ 1.600	$ 1.600
Especialista de Tecnología Informática	1	$ 1.100	$ 1.100
Jefe de Gestión de la Información	1	$ 1.400	$ 1.400
Analista de Gestión de la Información	2	$ 1.000	$ 2.000
Líder de proyectos de T.I	1	$ 1.200	$ 1.200
Asistentes de T.I	3	$ 1.000	$ 3.000
		TOTAL:	$ 517.700

Fuente: Investigación propia

1.2. ISO 27005

Es uno de los estándares internacionales que se ocupan de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001. Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización. No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria (Excellence, 2014)

1.3. Organigrama de la empresa

El organigrama de una organización me permite conocer el nivel jerárquico del personal que compone el área mediante una gráfica donde especifica el cargo que desempeña cada miembro del departamento.

El organigrama de una empresa consiste en la representación gráfica de la estructura de una empresa, esto no representa únicamente a los empleados y recursos humanos con los que cuenta la empresa, sino que también representa las estructuras departamentales, además es un buen esquema de las relaciones jerárquicas (GESTION.ORG, 2018).

En la figura 1.5 se expone el organigrama del departamento de Tecnología Informática de la empresa Leterago del Ecuador S.A:

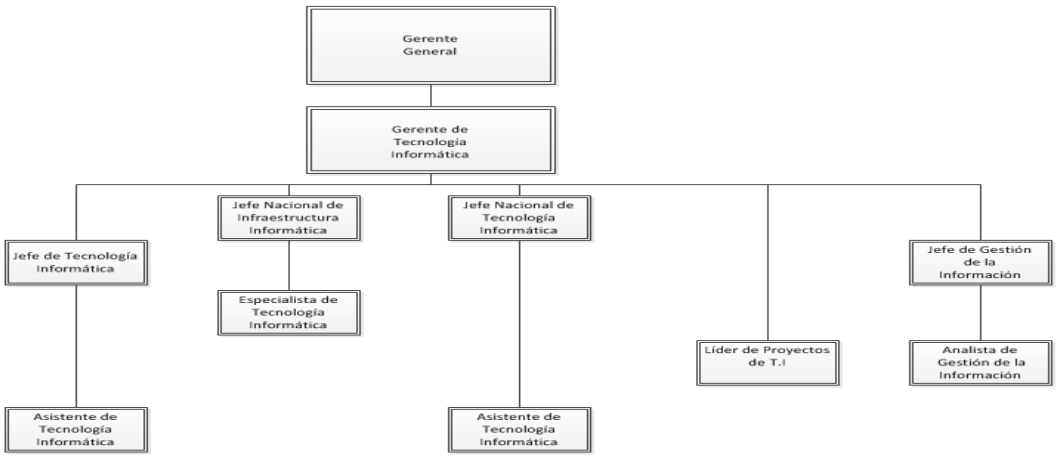


Figura. 1.5. Organigrama del departamento de T.I
Fuente: (LETERAGO, 2018)

Es necesario considerar otras definiciones importantes al momento de hablar de seguridad informática, las cuales se ilustran en la Tabla. 1.4:

1.3.1. Vocabulario propuesto

Tabla. 1.4. Vocabulario de términos

VOCABULARIO PROPUESTO POR EL AUTOR			
TÉRMINO	SIGNIFICADO	REFERENCIA	EJEMPLO
Activo	Son los recursos que pertenecen al propio sistema de información o que están relacionados con este.	(López, 2010)	Computador de escritorio
Amenaza	Es la posibilidad de ocurrencia de cualquier tipo de evento acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema.	(Fernández J., 2013)	Hurto de equipo
Análisis de Riesgo	Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.	(Fernández J., 2013)	Pérdida de información
Ataque	Son las consecuencias de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema, o dicho de otra manera, el daño causado. Los impactos pueden ser cuantitativos, si los perjuicios pueden cuantificarse económicamente, o cualitativos, si suponen daños no cuantificables, como los causados contra los derechos fundamentales de las personas.	(López, 2010)	Envío de virus vía correo electrónico
Desastre o Contingencia	Determinadas amenazas a cualquiera de los activos del sistema de información pueden poner en peligro la continuidad de un negocio. El plan de contingencias es un instrumento de gestión que contiene las medidas tecnológicas, humanas y de organización) que garanticen la continuidad de negocio protegiendo el sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto.	(López, 2010)	Realizar pruebas de funcionalidad con los backups de la organización
Impacto	Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad.	(Fernández J., 2013)	Impacto financiero, pérdidas económicas
Riesgo	Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad.	(López, 2010)	Robo de información
Vulnerabilidad	Es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas en la organización.	(Vieites, 2011)	Contraseñas débiles

Fuente: investigación propia

A continuación en la figura 1.6 se ilustra un claro ejemplo de la forma en que interviene todos los elementos antes mencionados y su repercusión a los activos de información.

Figura. 1.6. Proceso de evaluación y gestión de riesgos
Fuente: (Vieites, 2011)

1.4. Inventario de activos

Es la parte donde se reconocen los activos de la organización, el activo de mayor relevancia es la información que se almacena en los sistemas, es decir los datos, además de los datos se pueden identificar otros activos que también tienen como se muestra en la Tabla 1.5:

Tabla. 1.5. Inventario de activos

SERVICIOS	APLICACIONES INFORMÁTICAS	EQUIPOS INFORMÁTCOS	SOPORTES DE INFORMACIÓN	EQUIPAMIENTO AUXILIAR	REDES DE COMUNICACIÓN	INSTALACIONES	PERSONAL
Se prestan gracias a la existencia de los datos que luego se convierte en información ya que es el resultado de los servicios requeridos para tramitar dichos datos	Son las que autorizan procesar los datos	Son los que permiten acoger aplicaciones, datos y servicios	Son dispositivos donde se guarda la información	Perfecciona las herramientas informáticas	Autorizan el intercambio de datos	En donde se almacenan los equipos informáticos y de telecomunicaciones	Son los encargados de operar todos los elementos informáticos
Ejemplo: Reportes de SQL Server	Ejemplo: Sistema Administrativo Comercial (SAC)	Ejemplo: Servidores	Ejemplo: Cintas para backup	Ejemplo: Cable de red	Ejemplo: Red corporativa	Ejemplo: Centro de Datos	Ejemplo: Jefe de Infraestructura de T.I

Fuente: **Investigación propia**

En la tabla 1.6 se expone los activos primarios de la organización en la cual detallamos las actividades que realiza la empresa Leterago del Ecuador S.A como distribuidora farmacéutica y los activos de soporte que utiliza para llevar a cabo dichas actividades en la cual se detallan los equipos tecnológicos, software, redes,

comunicaciones, el personal responsable de llevar a cabo actividades de mantenimiento, soporte de dichos activos que utilizan los usuarios para poder realizar las operaciones que requiere una empresa de grandes magnitudes, adicional se detalla las ubicaciones del personal de tecnología informática y el organigrama del departamento donde se detalla la jerarquía del departamento de tecnología.

Tabla. 1.6. Inventario de activos por departamento

ACTIVOS PRIMARIOS	ACTIVOS DE SOPORTE					
ACTIVIDADES DEL NEGOCIO	HARDWARE	SOFTWARE	REDES	PERSONAL	UBICACIÓN	ORGANIZACIÓN
Ventas	Computadores de escritorio (8 PCS)	Microsoft Office 365 (8 licencias)	Access Point (1 equipo)	Asistente de ventas	Administración	Organigrama de la compañía
Distribución	Computadores de escritorio (3 PCS)	Microsoft Office 365 (3 licencias)	Access Point (1 equipo)	Operarios de Bodega	Bodega	
Importaciones	Computadores de escritorio (5 PCS)	Microsoft Office 365 (5 licencias)	Access Point (1 equipo)	Asistentes de importaciones	Administración	
Recepción de producto	PDA'S (8 equipos)	WMS / SCMI	Access Point (2 equipos)	Operarios de Bodega	Bodega	
Tecnología Informática	Computadores de escritorio (8 PCS)	Microsoft Office 365 (5 licencias)	Access Point (1 equipos)	Asistentes de T.I	Administración	
Facturación de producto	Computadores de escritorio (3 PCS)	Sistema Administrativo Comercial (SAC)	Access Point (1 equipos)	Operarios de Bodega	Bodega	

Fuente: **Investigación propia**

Se detalla en la Tabla 1.7 las definiciones de los principales recursos tecnológicos que se utilizan en la organización:

Tabla. 1.7. Recursos tecnológicos

No.	DESCRIPCIÓN	DEFINICIÓN	CANTIDAD
1	Access Point	Es un dispositivo que permite interconectar dispositivos de comunicación inalámbrica para formar una red inalámbrica	6
2	Central Telefónica	Es un contenedor utilizado por una empresa donde se alberga el equipo de conmutación para la operación de llamadas	1
3	Computador de escritorio	Es un tipo de computadora para ser utilizada en el escritorio de una oficina.	100
4	CD-ROM externo	Es un dispositivo externo generalmente se conecta mediante USB y sirve para leer la información almacenada en discos compactos y también para grabar en ellos.	4
5	Disco duro externo	Es un dispositivo de almacenamiento de rápido y fácil intercambio entre computadores, posee de conexión USB y sirve para respaldar información.	10
6	HUB	Es un dispositivo canalizador del cableado de una red para poder ampliarla.	4
7	Impresora	Es un equipo que sirve para imprimir información desde un computador, se puede configurar mediante cable USB o también se puede colocar en red.	53
8	Laptop	Es un equipo que posee una pantalla líquida, que se alimenta con una batería y corriente alterna y es liviana.	65
9	Nube de red	Ofrece servicios de cómputo a través de una red.	2
10	Pantalla de proyección	Superficie que sirve para poder proyectar ya sea presentaciones o proyectos.	3
11	PDA	Es un organizador personal su funcionamiento es prácticamente igual al de un computador.	8
12	Proyector	Equipo eléctrico que se utiliza para proyectar imágenes ópticas o diapositivas (presentaciones), videos,etc.	3
13	Router	Es un dispositivo que permite la interconexión de computadores en la red.	10
14	Servidor	Es un equipo físico que está integrado en una red informática en donde se configura un sistema operativo específico y sirve para poder instalar uno o varios software de uso corporativo.	20
15	Switch	Es un dispositivo que sirve para interconectar redes informáticas.	15
16	Tablet	Es un ordenador portátil caracterizada por tener una pantalla táctil.	35
17	Televisor	Aparato eléctrico que recibe y reproduce imágenes, videos y sonidos.	8
18	Tóner	Tinta en forma de polvo que se emplea para poder imprimir información sobre el papel.	30

Fuente: **Investigación propia**

En la figura 1.7 se detalla los activos, su valoración y sus vulnerabilidades a los riesgos, los requisitos mínimos para salvaguardarlos y protegerlos contra cualquier tipo de amenazas para evitar explotar una vulnerabilidad de los activos.

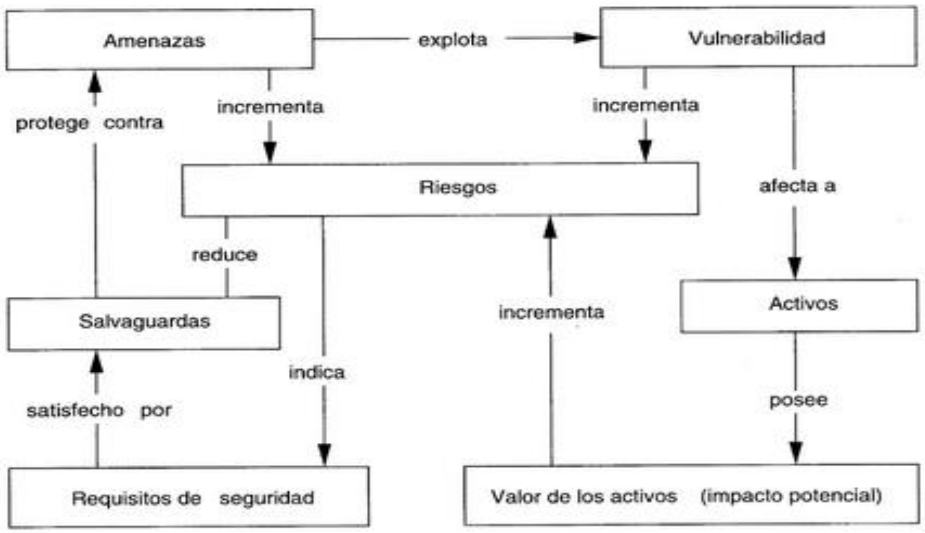


Figura. 1.7. Relación entre componentes de la gestión de la seguridad
Fuente: (AREITIO J, 2008)

A continuación vamos a conceptualizar lo que es la valoración de activos:

Según mi perspectiva la valoración de un activo es el recurso de hardware y software con los que cuenta una organización, es decir todo elemento que compone el proceso completo de comunicación.

1.4.1. Valoración Cuantitativa de Activos

Se trata de una valoración realizada a través de las características que tienen como base un escenario de amenaza sobre los activos, y generalmente está asociado a una calificación de los riesgos que utiliza como parámetros cualidades como alto, medio o bajo. Debido a que cada persona posee un concepto de lo que representa una característica "alta, media o baja" como una manera de clasificación, la evaluación cualitativa puede convertirse en un elemento subjetivo, por lo que en términos de seguridad de la información resulta básico definir criterios precisos de lo que cada categoría representa. Probablemente sea más sencillo identificar que un riesgo clasificado como "alto" deba tener mayor prioridad que uno etiquetado como "bajo". El desafío consiste en definir

claramente cuando se asigna una cualidad de este estilo a cada uno de los riesgos (Mendoza M. Á., 2015).

1.4.2 Probabilidad

Según mi perspectiva es cuando una amenaza intenta materializar una vulnerabilidad.

Se detalla en la Tabla 1.8 la definición de escalas de las probabilidades según Sosa:

Tabla. 1.8. Definición de probabilidad

No.	NIVEL DE PROBABILIDAD		DEFINICIÓN DE LA PROBABILIDAD	NIVEL DE OCURRENCIA
	CUALITATIVA	CUANTITATIVA		
1	**ALTA**	3	La fuente de amenaza es altamente motivada y suficientemente capaz. Los controles para prevenir que la vulnerabilidad suceda son ineficientes.	1-5 VECES AL MES
2	**MEDIA**	2	La fuente de amenaza es motivada y capaz. Los controles pueden impedir el éxito de que la vulnerabilidad suceda.	1-3 VECES AL MES
3	**BAJA**	1	La fuente de amenaza carece de motivación. Los controles están listos para prevenir o para impedir significativamente que la vulnerabilidad suceda.	1 VEZ AL MES

Fuente: (Sosa, 2012)

En la Tabla 1.9 muestra la valoración de probabilidad de los activos de la empresa de forma cualitativa.

Tabla. 1.9. Valoración de probabilidades

VALORACIÓN DE PROBABILIDADES		
No.	DESCRIPCIÓN	VALORACIÓN (CUALITATIVO)
1	Computadores de Escritorio	Bajo
2	Laptops	Bajo
3	Impresoras	Medio
4	PDA'S	Medio
5	Tabletas	Medio
6	Impresoras móviles	Medio
7	Proyectores	Bajo
8	Pantallas de proyección	Bajo
9	Televisores para proyección	Bajo
10	Servidores	Alto
11	Unidad externa de disco duro	Bajo
12	Unidad externa de CD-ROM	Bajo
13	Toners de respaldo para impresora	Bajo
14	Papel	Bajo
15	Documentación	Bajo
16	Microsoft office 2016	Bajo
17	Iso Manager	Bajo
18	SCMI	Alto
19	WMS	Alto
20	Adobe professional	Bajo
21	WIN-RAR	Bajo
22	Sistema Administrativo Comercial (SAC)	Alto
23	NetOrder	Alto
24	Microsoft office communicator	Bajo
25	Evolution	Alto
26	Windows 10	Bajo
27	Windows server 2016	Bajo
28	SQL Server 2012	Bajo
29	Switch	Bajo
30	Hub	Bajo
31	Router	Bajo
32	Nube de red	Bajo
33	Access point	Bajo
34	Central telefónica	Bajo

Fuente: Investigación propia

1.4.3 Valoración del impacto

El impacto se entiende que es una valoración o un análisis de los daños causados a la organización si un riesgo llegara a materializarse causando cuantiosas pérdidas materiales, económicas y de información.

"Impacto: es la medición y valoración del daño que podría producir a la organización un incidente de seguridad." (Vieites, 2011)

Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un valor relativo a cada sistema y la información sobre ella. Dentro de los valores para el sistema se pueden distinguir: confidencialidad de la información, la integridad (aplicaciones e información) y finalmente la disponibilidad del sistema información) y finalmente la disponibilidad del sistema. (Fernández J. , 2013)

Para valorar el impacto es necesario tener en cuenta tanto los daños tangibles como la estimación de los daños intangibles (incluída la información). En este sentido, podría resultar de gran ayuda la realización de entrevistas en pronfundidad con los responsables de cada departamento, función o proceso de negocio, tratando de determinar el impacto real de la revelación, alteración o pérdida de la información para la organización, y no sólo del elemento TIC que la soporta. (Vieites, 2011)

Se expone los siguientes criterios de la valoración de impacto de los activos.

Tabla. 1.10. Criterios de valoración del impacto

No.	TIPO DE IMPACTO	SIGNIFICADO	ESCALA
1	DIRECTO	Cuando se ve involucrado la reposición del activo	2
2	INDIRECTO	Cuando se ve involucrado la interrupción del servicio	1

Fuente: Investigación propia

Tabla. 1.11. Valoración del impacto de los activos

VALORACIÓN DE IMPACTO		
No.	DESCRIPCIÓN	VALORACIÓN (IMPACTO)
1	Computadores de Escritorio	Directo
2	Laptops	Directo
3	Impresoras	Directo
4	PDA'S	Directo
5	Tabletas	Directo
6	Impresoras móviles	Directo
7	Proyectores	Directo
8	Pantallas de proyección	Directo
9	Televisores para proyección	Directo
10	Servidores	Directo
11	Unidad externa de disco duro	Directo
12	Unidad externa de CD-ROM	Directo
13	Toners de respaldo para impresora	Indirecto
14	Papel	Indirecto
15	Documentación	Indirecto
16	Microsoft office 2016	Directo
17	Iso Manager	Indirecto
18	SCMI	Indirecto
19	WMS	Indirecto
20	Adobe professional	Directo
21	WIN-RAR	Directo
22	Sistema Administrativo Comercial (SAC)	Indirecto
23	NetOrder	Indirecto
24	Microsoft office communicator	Indirecto
25	Evolution	Indirecto
26	Windows 10	Directo
27	Windows server 2016	Directo
28	SQL Server 2012	Directo
29	Switch	Directo
30	Hub	Directo
31	Router	Directo
32	Nube de red	Directo
33	Access point	Indirecto
34	Central telefónica	Directo

Fuente: Investigación propia

1.5 Análisis de riesgos

En la figura 1.8 contempla las fases de la gestión del riesgo de cómo se identifica, estima y evalúa al riesgo y en caso de que amerite o no dar un tratamiento el riesgo o únicamente se lo puede documentar.

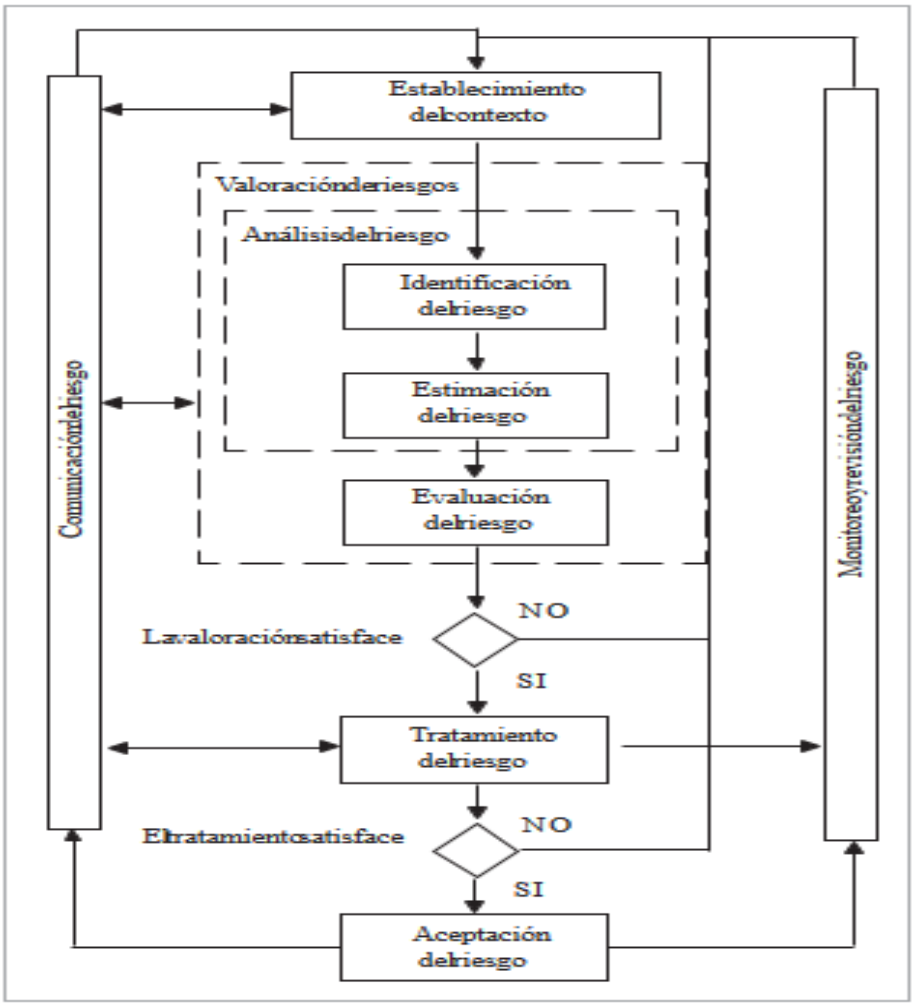


Figura. 1.8. Procesos para gestión de riesgos de acuerdo a ISO 27005
Fuente: (ISO27005, 2011)

Podemos ver un ejemplo de una matriz de riesgo en el Tabla 1.12 donde se ilustra la probabilidad de ocurrencia va de 0 – 4, donde la ocurrencia y el impacto se califica con la escala Baja (B), Media (M), Alta (A) y la valoración del riesgo va en una escala de 0 – 8.

Tabla. 1.12. Matriz de riesgo

	Probabilidad (Ocurrencia)	Baja			Media			Alta		
	Valor (Impacto)	B	M	A	B	M	A	B	M	A
Valor (Cumplimiento) Escala: (0-4)	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
Cumplimiento: Escala (0 = 0%), (1 = 25%), (2 = 50%), (3 = 75%), (4 =										
Ocurrencia: Escala Baja (B), Media (M), Alta (A)										
Impacto: Escala Baja (B), Media (M), Alta (A)										
Valoración Riesgo: Escala 0 - 8										
Criterios de Valoración del Riesgo: Valores mayores a 7 (7,8)										

Fuente: (ISO27005)

Adicionalmente se ilustra en el Tabla 1.13 el impacto que tiene en el negocio dependiendo del riesgo por el cual la organización este pasando con sus diferentes escalas de valoración e importancia que van desde el riesgo bajo al riesgo alto.

Tabla. 1.13. Matriz de impacto en el negocio

	Probabilidad del escenario de incidente	Muy baja (muy improbable)	Baja (Improbable)	Media (Posible)	Alta (Probables)	Muy Alta (Frecuente)
Impacto en el negocio	Muy baja	0	1	2	3	4
	Baja	1	2	3	4	5
	Media	2	3	4	5	6
	Alta	3	4	5	6	7
	Muy alta	4	5	6	7	8
	Riesgo bajo: 0 - 2					
	Riesgo medio: 3 - 5					
	Riesgo alto: 6 - 8					

Fuente: (ISO27005)

1.6. Identificación de vulnerabilidades

La ISO 27005 define a una vulnerabilidad como la debilidad del activo o activos de las compañías, las cuales podrían ser usadas por las amenazas para causar daño a los sistemas.

Enumeramos las vulnerabilidades más comunes que se presentan en una organización en la Tabla 1.14 según la norma ISO 27005:

Tabla. 1.14. Vulnerabilidades más comunes

TIPOS	DETALLE	VULNERABILIDADES	AMENAZAS
HARDWARE	CPU	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión
	CPU, Periféricos (scanner, impresora, etc)	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Impresoras	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Servidores	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
SOFTWARE	Sistema SAC	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Sistemas Empresariales	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Sistema de backups	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	NetOrder	Ausencia de documentación	Error en el uso
	Sistema SAC	Fechas incorrectas	Error en el uso
	Iso Manager	Gestión deficiente de las contraseñas	Falsificación de derechos
	Iso Manager	Gestión deficiente de las contraseñas	Falsificación de derechos
	Sistema de backups	Ausencia de copias de respaldo	Manipulación con software
RED	Outlook	Ausencia de pruebas de envío o recepción de mensajes	Negación de mensajes
	Central telefónica	Conexión deficiente de los cables	Falla del equipo de telecomunicaciones
	Central telefónica	Punto único de falla	Falla del equipo de telecomunicaciones
	Sistema SAC	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
PERSONAL	Personal de T.I	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Usuarios	Entrenamiento insuficiente en seguridad	Error en el uso
	Usuarios	Uso incorrecto de software y hardware	Error en el uso
	Usuarios	Falta de conciencia acerca de la seguridad	Error en el uso
LUGAR	Acceso a empresa	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y recintos	Destrucción de equipos o medios
	Empresa	Ubicación en un área susceptible de inundadión	Inundación
	Empresa	Red energética inestable	Pérdida del suministro de energía

Fuente: Investigación propia

En la Tabla 1.15 se ilustra la clasificación de las vulnerabilidades en una organización según la norma ISO 27005.

Tabla. 1.15. Ejemplos de vulnerabilidades

TIPOS	VULNERABILIDADES	AMENAZAS
ORGANIZACIÓN	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de registros en las bitácoras (logs) de administrador y operario	Error en el uso
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo

Fuente: **(ISO27005)**

1.7. Análisis de amenazas

1.7.1. Amenaza: "Una amenaza es un hecho que puede producir un daño." (Sosa, 2012), es decir que es un instrumento capaz de violentar la seguridad de la información y/o seguridad informática y este instrumento persistirá cuando se haga presente una vulnerabilidad.

1.7.2. Tipos de amenazas: A continuación enumeramos los tipos de amenazas que se encuentran descritas en la norma ISO 27005.

Se detalla el origen de las amenazas, su descripción y un ejemplo según lo establece la norma ISO 27005:

Tabla 1.16 Origen de las amenazas

ORIGEN AMENAZA	DESCRIPCIÓN	EJEMPLO
Natural	Son fenómenos naturales que afectan a los activos	Terremoto
Humano	Es un fenómeno causado por el ser humano	Consumir líquidos cerca de los equipos
Intencionado	Alteración de la información	Destrucción de la información
No Intencionado	Ponen en riesgo los activos informáticos inconscientemente	Divulgar contraseñas

Fuente: **Investigación propia**

Tabla. 1.17. Amenazas comunes

TIPO	AMENAZAS	ORIGEN		
		A	D	E
Daño Físico	Periféricos dañados por agua	X	X	X
	Accidente importante (cortocircuito)	X	X	X
	Equipos con polvo en su interior	X	X	X
Eventos Naturales	Inundación en oficinas			X
	Daño en televisores para proyección debido a la actividad sísmica en nuestro país			X
	Temperatura inestable en el cuarto de servidores			X
Pérdida de los servicios escenciales	Falla en el sistema de suministro de aire acondicionado en el cuarto de servidores	X	X	
	Pérdida de suministro de energía en el UPS	X	X	X
	Falla en el servicio de telecomunicaciones por parte del proveedor Level 3	X	X	
Perturbación debido a la radiación	Radiación electromagnética de equipos	X	X	X
	Impulsos electromagnéticos			X
Compromiso de la información	Escucha encubierta			X
	Datos provenientes de fuentes no confiables	X	X	
	Hurto de equipo			X
	Recuperación de medios reciclados o desechados			X
Fallas Técnicas	Falla de equipos de escritorio	X		
	Falla de laptops	X		
	Mal funcionamiento de computadores	X		
	Saturación del sistema de información (Sistema SAC)	X	X	
	Mal funcionamiento de software (ISO MANAGER)	X		
	Incumplimiento en el mantenimiento del sistema de información	X	X	
Acciones no autorizadas	Uso sin autorización de algún equipo informático		X	
	Uso de software falso o copiado		X	
	Copia fraudulenta del software		X	
Compromiso de las funciones	Incumplimiento en la disponibilidad del personal	X	X	X
	Negación de acciones	X	X	
	Abuso de derechos		X	

Fuente: (ISO27005, 2009)

2. CAPÍTULO II. PROPUESTA

2.1 Diagnóstico de la situación actual

El diagnóstico del Centro de Datos se detalla en la Tabla 2.1.

Tabla. 2.1 Diagnóstico del Centro de Datos

DIAGNÓSTICO DEL CENTRO DE DATOS							
DIMENSIÓN	TEMPERATURA Y HUMEDAD	SEGURIDAD FÍSICA Y CONTROL DE ACCESO	ACABADOS	GARANTÍA DE EQUIPOS	DETECCIÓN Y EXTINCIÓN DE INCENDIOS	SISTEMA DE ENERGÍA (UPS)	SISTEMA ELÉCTRICO
Dimensión física es de 6m - 9m de ancho y 2.10 m - 2.30 m de altura	Temperatura entre 18°-22° y una humedad de 55%, aire acondicionado independiente	Sistema de control de acceso, sitio libre de vibraciones mecánicas, rayos solares y goteras	Piso de vinil antiestático y muros con pintura vinílica	Garantía y soporte técnico del fabricante: CAREPACK	Tiene detectores de humo y extintores debidamente cargados	UPS modelo trifásico y salida monofásica	Sistema bifásico a 4 hilos

Fuente: Investigación propia

Cronograma de actividades

Se detalla en la Tabla 2.2 el cronograma de actividades para la elaboración de la propuesta del Sistema de Gestión de Seguridad de la Información.

Tabla. 2.2 Cronograma de actividades

No.	Actividades	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto
1	Elaboración del plan de tesis y aprobación									
2	Diagnóstico de la situación actual de la seguridad informática en la organización									
3	Estudio y elaboración del árbol de problemas									
4	Elaboración del marco teórico									
5	Análisis de amenazas									
6	Elaboración de la propuesta									
7	Análisis de los controles existentes									
8	Conclusiones y recomendaciones									

Fuente: Investigación propia

Situación de la Seguridad de la Información

Se analizó la situación actual de la seguridad de la información en la empresa Leterago del Ecuador S.A, se hallaron algunos aspectos importantes sobre la gestión de la seguridad de la información.

Tabla. 2.3. Situación de la seguridad de la información

FORTALEZAS	OPORTUNIDADES	DEBILIDADES	AMENAZAS
Apertura a nuevas sugerencias para la propuesta del Sistema de Gestión de Seguridad de la Información.	Aplicar estas sugerencias para la propuesta del Sistema de Gestión de Seguridad de la Información para el Centro de Datos de Leterago del Ecuador S.A.	Actualmente, la organización no cuenta con un departamento especializado a la gestión de la Seguridad de la información, por lo tanto el área de infraestructura tiene sus propios procedimientos para precautelar la seguridad de la información.	No se realiza auditorías de seguridad de la información con periodicidad.
Apertura a nuevas medidas para contrarestar el riesgo	Analizar las nuevas medidas para poder aplicarlas en la propuesta.	No posee un SGSI documentado, tampoco con políticas de seguridad definidas, ni divulgadas, cuentan con procedimientos pero no existe un debido cumplimiento al mismo.	No se realiza controles de seguridad de contraseñas.

Fuente: Investigación propia

Datos Informativos

La empresa Leterago del Ecuador S.A es una organización de carácter privado, que se dedica a la venta, distribución e importación de medicamentos, cuenta con 3 sucursales en Quito, Guayaquil y Cuenca.

Se encuentra ubicado en Cantón Quito, Parroquia Pomasqui, en la Av. Manuel Córdova Galarza km 7 1/2 vía a Pomasqui. Su representante legal en el país es el Sr. Daniel Leszcz Weinstock.

Sus valores corporativos son la innovación, creatividad, respeto, humildad, profesionalismo, orientación al cliente, trabajo en equipo y flexibilidad.

Antecedentes de la propuesta

Visión: Ser la empresa líder a nivel nacional en servicios de distribución y representación exclusiva de productos farmacéuticos y afines; distinguiéndonos por el

profesionalismo y calidad de nuestros servicios. lo que conlleva ir acorde a los avances tecnológicos ya que debido a la gran cantidad de usuarios, su infraestructura, su amplio espacio físico, dotar de capacitaciones a los usuarios sobre la responsabilidad y la seriedad que se debe tener con la seguridad de la información a través de charlas informativas, culturales y tecnológicas que crea los espacios de comunicación con la comunidad organizacional.

Misión: Somos una empresa dedicada a la comercialización y distribución de productos farmacéuticos y afines en todo el territorio nacional, por medio de un servicio a la vanguardia de las exigencias del mercado, que mantiene altos estándares de calidad, eficiencia y competitividad; generando valor para nuestros clientes, accionistas, colaboradores y proveedores."

Según Ponemon Institute, solo el 25 % de las empresas supervisa el acceso a los datos sensibles y su uso. (Informatica, 2018)

La revista Vistazo en el año 2017 realiza un ranking de las 500 mayores empresas en el Ecuador, colocando a la empresa Leterago del Ecuador S.A en el puesto número 30. (Vistazo, 2017: 140), con estos antecedentes se conoce que es una organización que ha ido creciendo de manera apresurada por lo tanto tiene que contar con normas y reglamentos que ayuden a la seguridad de la información.

En Ecuador en el año 2017 la empresa Deloitte presenta su primera edición de estudio de la seguridad de la información que fue realizada en más de 50 empresas nacionales y multinacionales de diversas industrias donde un 46% fue en empresas dedicadas a Servicios Financieros, 38% Bienes de Consumo, 10% Energía y Recursos Renovables, 4% Tecnología, Medios y Telecomunicaciones y 2% Ciencias de la Salud, en la cual el 32% de las empresas pertenecen a la Región Costa y el 68% de la Sierra y lo que mas se destaco de sus conclusiones fue de que casi el 50% de las empresas participantes sufrieron alguna brecha de seguridad en los últimos 12 meses, y de estos, el 20% no pudo determinar el impacto de dicha brecha ya que no cuentan con un proceso de gestión de incidentes. El componente humano continua siendo una pieza crítica en la gestión de seguridad de la información, lo cual es confirmado por casi el 50% de las organizaciones que indicaron que su principal iniciativa para el 2018 será la capacitación y sensibilización en seguridad de la información. La gran mayoría de iniciativas recae en el ámbito estratégico y táctico, acotaron también que la falta de suficiente presupuesto continua

estando entre las principales dificultades, lo cual es confirmado por más del 50% de las empresas participantes, seguido muy de cerca por aspectos como la falta de visibilidad e influencia y la falta de personal competente. Así mismo, casi el 75% de los participantes no mide el retorno de las inversiones en seguridad de información. (Deloitte, 2017)

Justificación

Esta propuesta se justifica porque cuenta con el respaldo de la Gerencia de Tecnología Informática adicionalmente la organización posee una gran infraestructura de la cual disponen dependiendo de las necesidades que se vayan presentando. Cada año cuenta con el presupuesto suficiente para poder implementar tecnología de punta en los proyectos.

Equidad Organizacional

La empresa Leterago del Ecuador S.A está debidamente organizada ya que se basa en la Ley de Compañías del Ecuador (LCE).

Equidad de Género

Esta propuesta está dirigida a hombres y mujeres de todas las áreas y cargos dentro de la organización que deseen impulsar la importancia que requiere en la actualidad la seguridad de la información.

Tabla. 2.4 Equidad de género

GÉNERO	CANTIDAD			
	Quito	Guayaquil	Cuenca	Total
Hombres	400	80	20	500
Mujeres	250	25	15	290
			Total general:	790

Fuente: Investigación propia

Ambiental

La organización se preocupa por preservar el medio ambiente utilizando hojas recicladas para las impresiones, evitan imprimir correos que no sean necesarios, en lugar

de imprimir documentación prefieren mandarlo en digital vía email. De tal manera que la empresa y sus usuarios puedan colaborar de alguna forma con el cuidado de la naturaleza.

Legal

La empresa Leterago del Ecuador S.A está legalmente constituida, por escritura pública que fue otorgada 15 de Mayo del año 2002, ante el Notario Décimo Cuarto del Cantón Quito, Doctor Alfonso Freire Zapata. Fue Aprobada por la Superintendencia de Compañías mediante Resolución No. 02-G-IJ-0004104 el 14 de Junio del 2002. Con el número del Registro Mercantil 13.420.

2.1.1 Recopilación de información

Se realizó una encuesta a la Especialista de Tecnología Informática, Jefe de Infraestructura y un Asistente de Tecnología Informática en diferentes aspectos de la seguridad informática tomando en consideración 7 de los 14 dominios descritos en la norma ISO 27001 que fueron apropiados para obtener información de primera mano, la misma obtuvo los siguientes resultados (**Ver anexo 1, Anexo 3**).

Instrumentos de medición

La encuesta consta de 34 preguntas realizadas a 3 representantes del área de Tecnología Informática en el período de junio a julio del 2018 (**Ver Anexo 6**), los resultados de la información tabulada están agrupados a cada una de las preguntas que han sido formuladas las cuales se detallan a continuación:

En relación al dominio A5-Política de Seguridad, descrito en la norma ISO 27001, se realizaron 6 preguntas detalladas en la tabla 2.1 orientadas a 3 representantes del área de Tecnología Informática. Se obtuvieron los siguientes resultados:

Pregunta1: Existe documentos de políticas de seguridad de la información en la empresa?

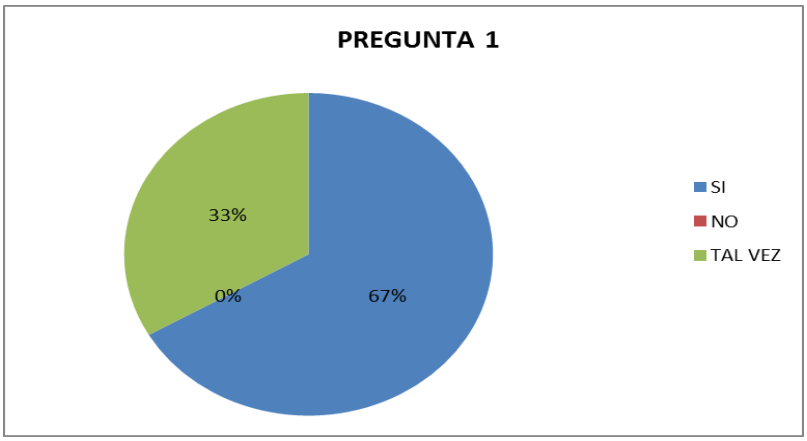


Figura. 2.1. Documentación de seguridad de la información
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.1 ilustra los resultados de la pregunta 1. Además se conoce que hay ciertos aspectos de la seguridad de la información que se encuentran documentados, se recalca que los encuestados nos aclararon que únicamente existen procedimientos que forman parte de la seguridad informática.

Pregunta 2: Existe alguna normativa relacionada a los sistemas de información?

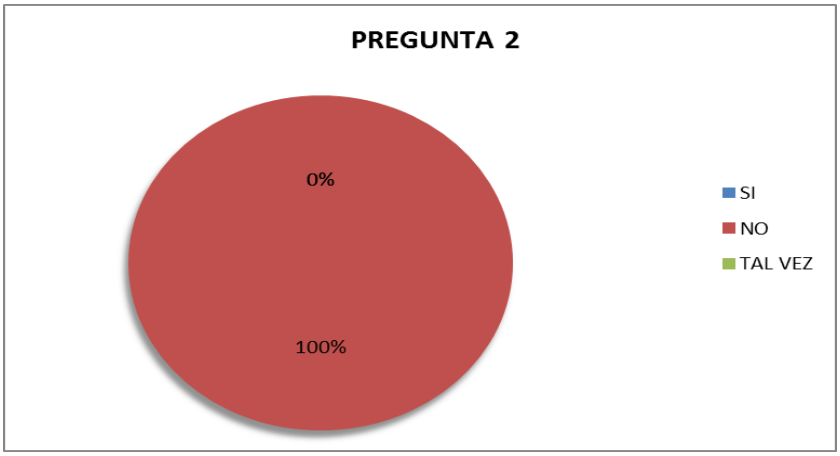


Figura. 2.2. Normativa de los sistemas de información
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.2 ilustra los resultados de la pregunta 2. Además se conoce que no existe una normativa de los sistemas de información lo cual es perjudicial para la

organización porque los usuarios no tienen conocimiento del manejo de ciertos aspectos de los sistemas informáticos.

Pregunta 3: Existe procedimientos relacionada a los sistemas de información?

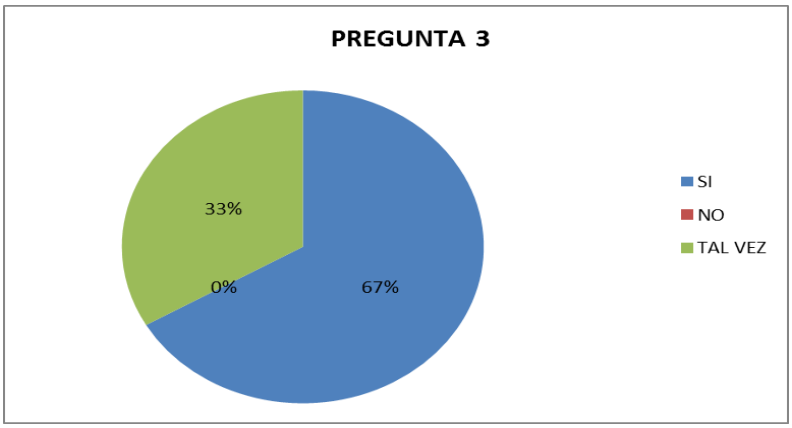


Figura. 2.3. Procedimientos de los sistemas de información
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.3 ilustra los resultados de la pregunta 3. Además se conoce que si existen procedimientos de los sistemas de información que se encuentran documentados para su correcto funcionamiento.

Pregunta 4: Existen responsables y/o controles para validar las políticas de seguridad?

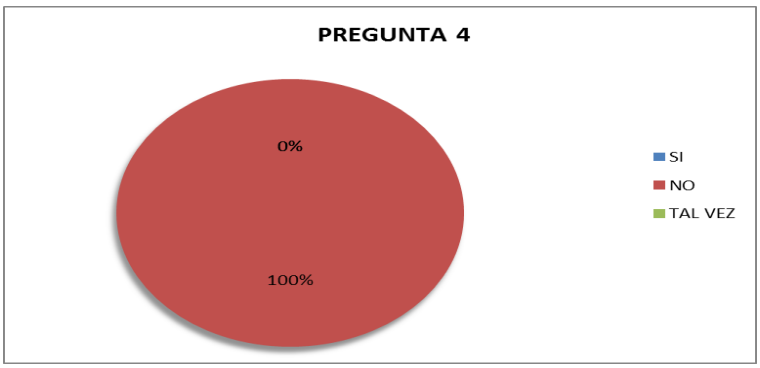


Figura. 2.4. Controles para validar política de seguridad
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.4 ilustra los resultados de la pregunta 4. Además se conoce que no hay controles para validar la política de seguridad, esto es una vulnerabilidad significativa para la organización.

Pregunta 5: Existen formas para dar a conocer a los usuarios de dichas normas?

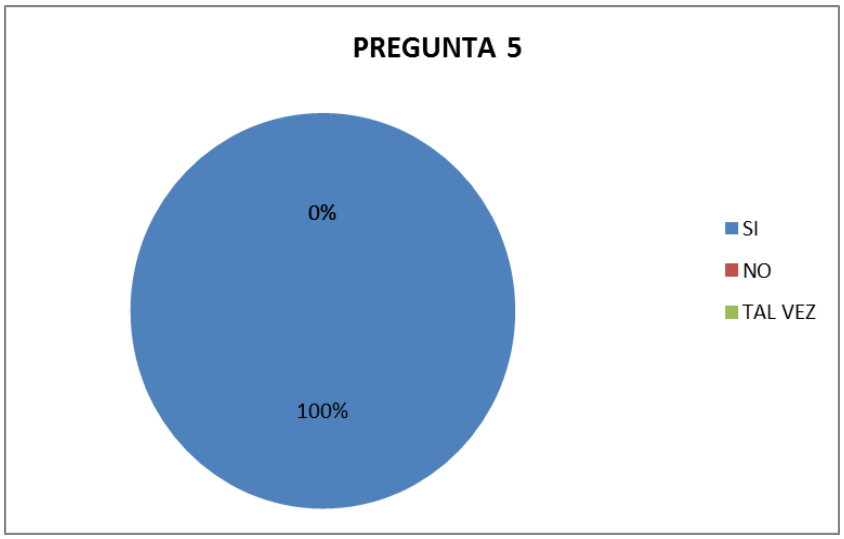


Figura. 2.5. Información de normas a los usuarios
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.5 ilustra los resultados de la pregunta 5. Además se conoce que existen formas de dar a conocer la información de las normas a los usuarios por los distintos medios de comunicación como son: comunicación interna (vía correo electrónico), carteleras informativas.

Pregunta 6: Existe algún tipo de control para verificar la validez de dichas políticas?

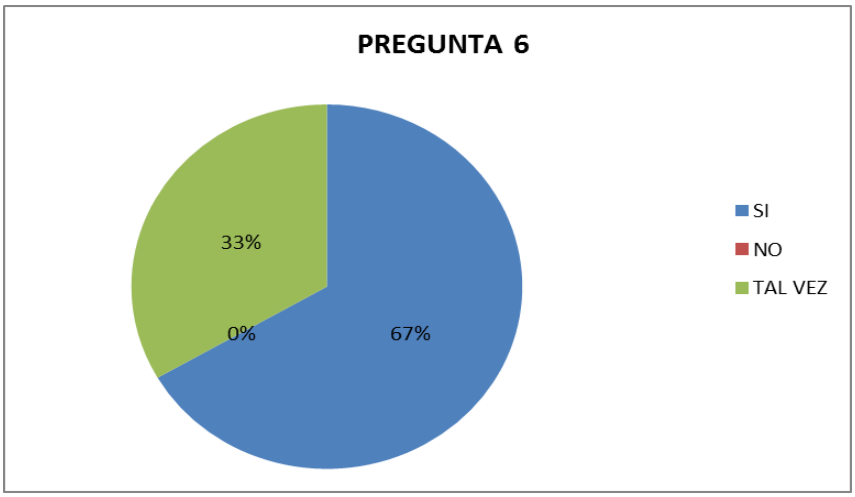


Figura. 2.6. Controles para validar políticas
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.6 ilustra los resultados de la pregunta 6. Además se conoce que no existen controles para validar las políticas, es decir la organización no tiene una persona especializada que pueda aprobar formalmente dichas políticas.

En relación al dominio A6-Organización de la SI, descrito en la norma ISO 27001, se realizaron 4 preguntas detalladas en la tabla N. 2.2 orientadas a 3 representantes del área de Tecnología Informática. Se obtuvieron los siguientes resultados:

Pregunta 7: Existen roles o responsabilidades definidas para el personal encargado de la seguridad de la información?

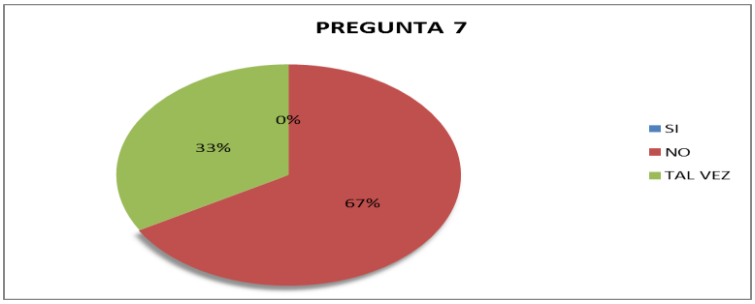


Figura. 2.7. Roles para la seguridad de la información
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.7 ilustra los resultados de la pregunta 7. Además se conoce que no existen roles o responsabilidades definidas para tratar a la seguridad de la información, causando una brecha de riesgos para la organización ya que no hay personal encargado de resolver problemas puntuales de la seguridad informática.

Pregunta 8: Existen condiciones contractuales de seguridad con terceras personas y outsourcing?

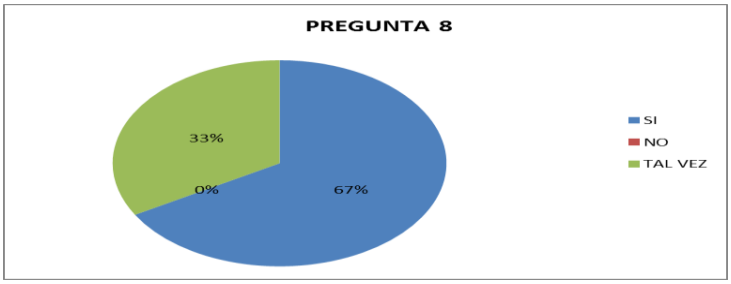


Figura. 2.8. Condiciones contractuales de seguridad con outsourcing
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.8 ilustra los resultados de la pregunta 8. Además se conoce que si existen condiciones contractuales de seguridad con terceras personas y outsourcing, en caso de que cualquier proveedor incumpla con la parte de seguridad informática estipulado en el contrato, se considerará como terminado.

Pregunta 9: Existen programas que ayuden a la formación en seguridad para los empleados?

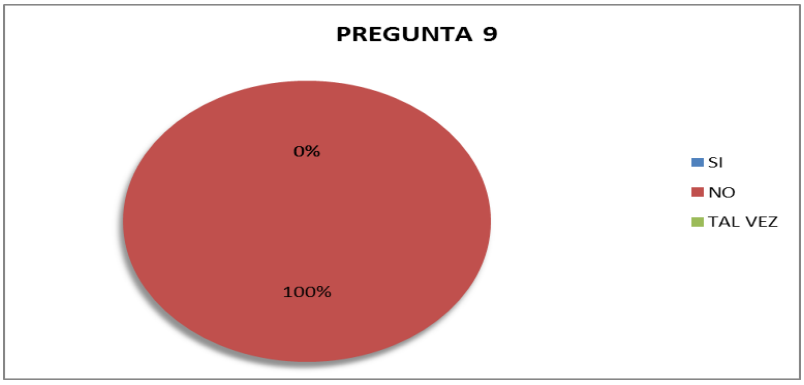


Figura. 2.9. Programas que ayuden a la formación en seguridad a empleados
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.9 ilustra los resultados de la pregunta 9. Además se conoce que no hay programas que ayuden a la formación en seguridad a empleados, la organización no ha realizado ninguna inversión todavía en el tema.

Pregunta 10: Se revisa el tema de la seguridad de la información de la organización con periodicidad por algún agente externo?

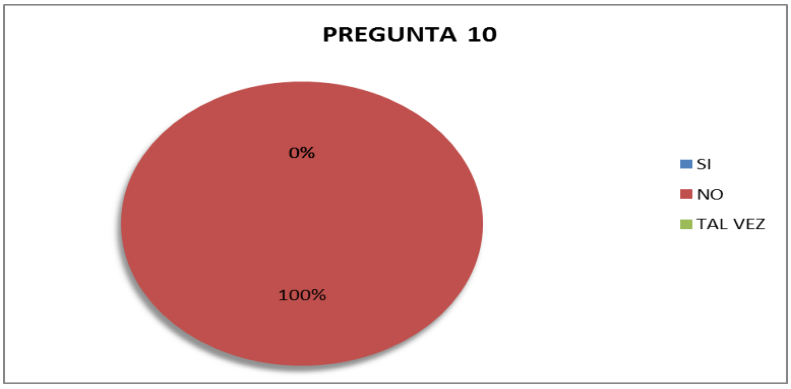


Figura. 2.10. Revisión de la seguridad de la información con algún agente externo
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.10 ilustra los resultados de la pregunta 10. Además se conoce que no hay revisión de la seguridad de la información con algún agente externo o auditorías de seguridad de la información realizado recientemente.

En relación al dominio A8-Gestión de Activos, descrito en la norma ISO 27001, se realizaron 5 preguntas detalladas en la tabla N. 2.3 orientadas a 3 representantes del área de Tecnología Informática. Se obtuvieron los siguientes resultados:

Pregunta 11: Existe un inventario de activos de T.I actualizado?

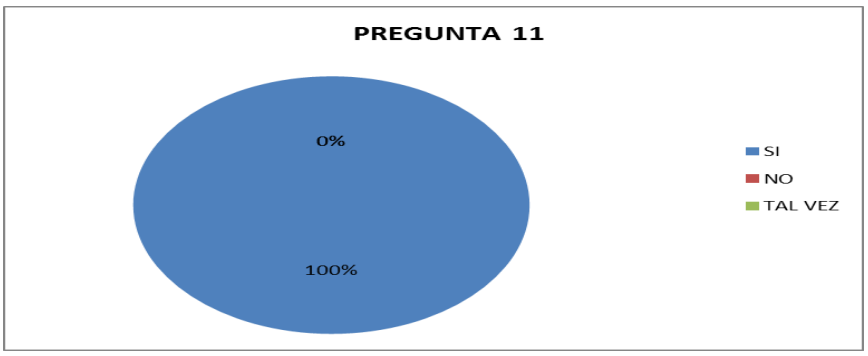


Figura. 2.11. Inventario de activos de tecnología informática actualizado
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.11 ilustra los resultados de la pregunta 11. Además se conoce existen inventarios de activos de tecnología informática actualizados ya que cada vez que se va a entregar un equipo al usuario se asigna en primera instancia en el sistema de activos.

Pregunta 12: En el inventario consta el software, equipos y activos de datos?

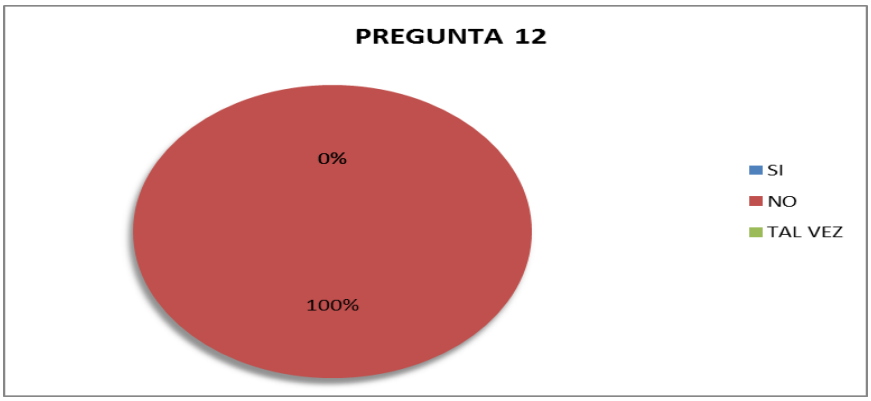


Figura. 2.12. Inventario de software, equipos y activos de datos
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.12 ilustra los resultados de la pregunta 12. Además se conoce que no existen inventarios de software, equipos y activos de datos, por lo cual no se puede llevar un control total de los activos informáticos.

Pregunta 13: Existe procedimientos relacionada a los sistemas de información?

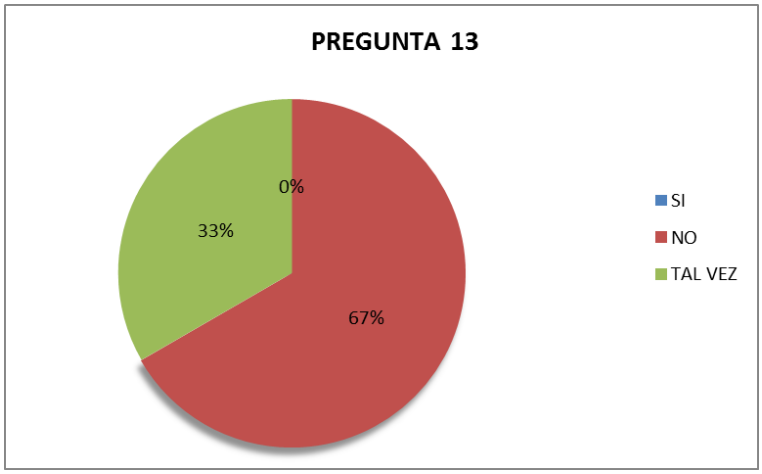


Figura. 2.13. Procedimientos para los sistemas de información
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.13 ilustra los resultados de la pregunta 13. Además se conoce que no existen procedimientos para los sistemas de información, por lo tanto no hay un control de la manera de tratar a los sistemas de información de la organización.

Pregunta 14: Existe un responsable a cargo de los activos?

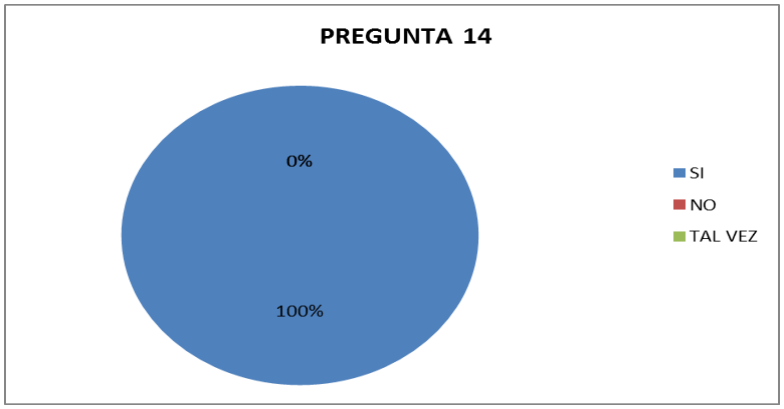


Figura. 2.14. Responsable a cargo de los activos
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.14 ilustra los resultados de la pregunta 14. Además se conoce que si existe un responsable a cargo de los activos, según los encuestados afirman que es el departamento contable que lleva control de los activos mediante etiquetas de activo fijo.

Pregunta 15: Existen normas y/o procedimientos para clasificar la información?

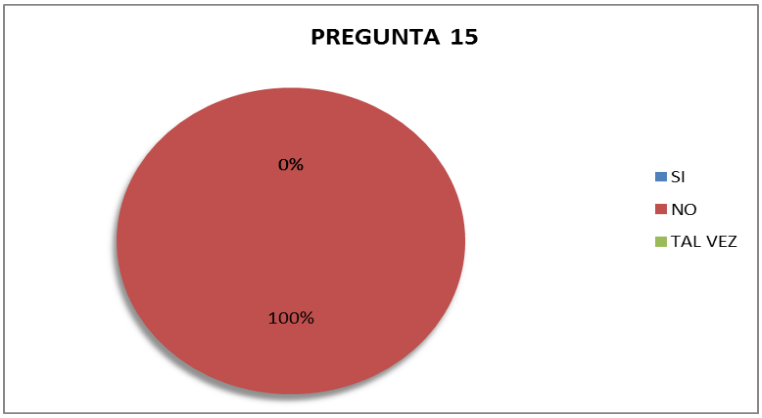


Figura. 2.15. Normas y procedimientos para clasificar la información
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.15 ilustra los resultados de la pregunta 15. Además se conoce que no existen normas y procedimientos para clasificar la información, por lo tanto no se conoce que tipo de información va a ser de dominio público en la organización y cual no.

En relación al dominio A7-Seguridad de los RRHH, descrito en la norma ISO 27001, se realizaron 5 preguntas detalladas en la tabla N. 2.4 orientadas a 3 representantes del área de Tecnología Informática. Se obtuvieron los siguientes resultados:

Pregunta 16: Se tiene definidas responsabilidades y/o roles de la seguridad informática?

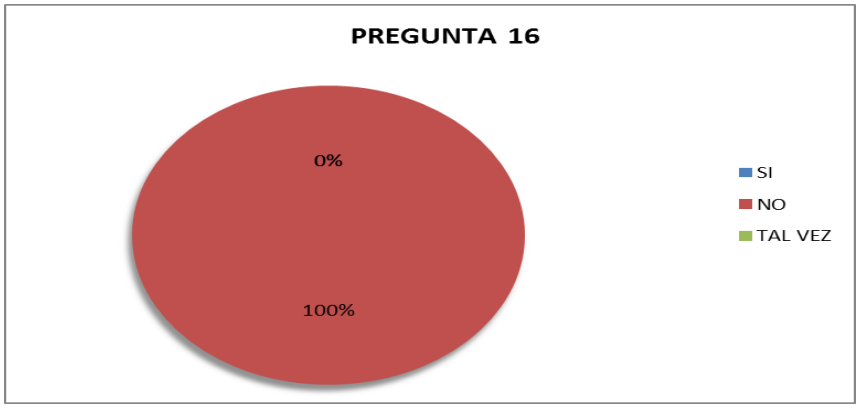


Figura. 2.16. Definición de responsabilidades y/o roles de la seguridad informática
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.16 ilustra los resultados de la pregunta 16. Además se conoce que no existen responsabilidades y/o roles de la seguridad informática, es decir que cuando se presente algún caso puntual de seguridad informática no va a haber personal especializado para resolver dicho problema.

Pregunta 17: Se tiene en consideración la seguridad de la información cuando se selecciona y se da de baja al personal?

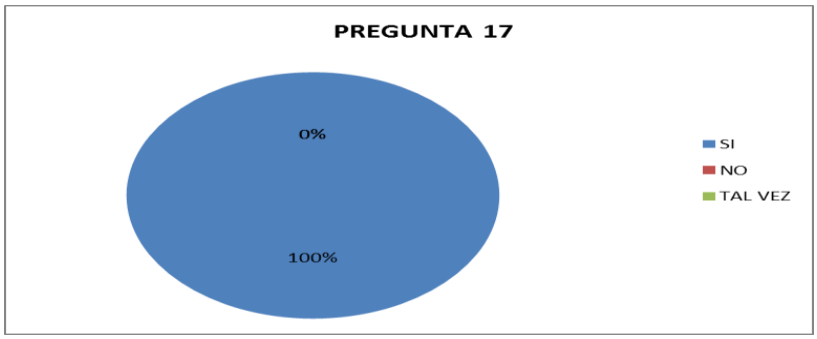


Figura. 2.17. Consideración de la seguridad de la información al dar de baja un usuario
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.17 ilustra los resultados de la pregunta 17. Además se conoce que si existen formas de precautelar la información cuando un empleado deja de trabajar en la organización, bloqueando de inmediato el usuario y los accesos a los sistemas de información.

Pregunta 18: En los contratos a los empleados se estipula las condiciones de confidencialidad de la información?

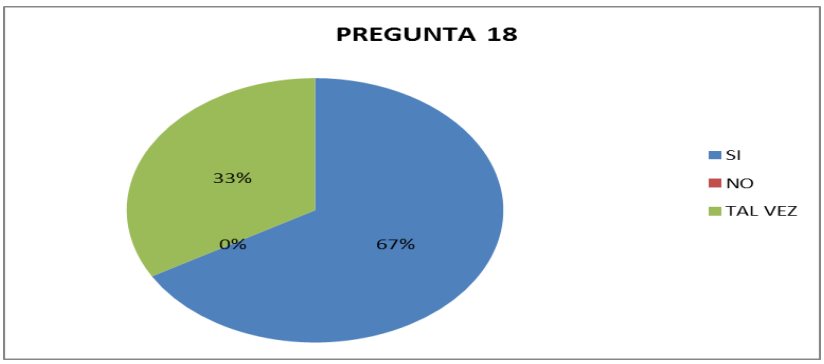


Figura. 2.18. Condiciones de confidencialidad de la información
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.18 ilustra los resultados de la pregunta 18. Además se conoce que existen condiciones de confidencialidad de la información, es decir que hay casos en que no permiten revisar información ya que es de uso de gerencias únicamente.

Pregunta 19: Se capacita a los empleados acerca del tratamiento de los activos?

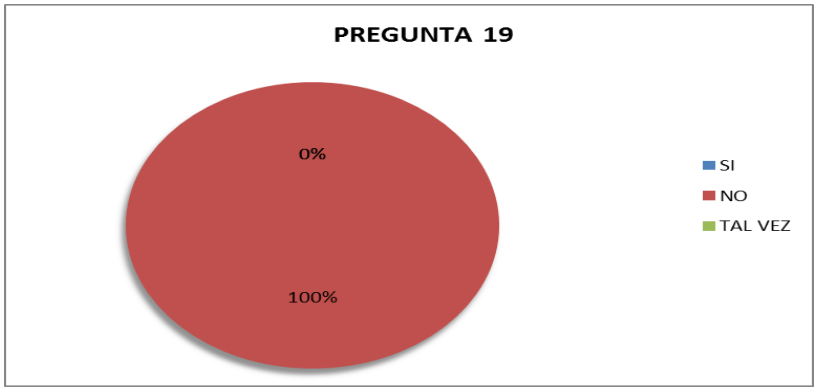


Figura. 2.19. Capacitación a los usuarios del tratamiento de activos
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.19 ilustra los resultados de la pregunta 19. Además se conoce que no existe en la organización capacitaciones a los usuarios del tratamiento de activos, en cierto caso habido problemas de funcionamiento de periféricos y de dispositivos por el desconocimiento de uso por parte de los usuarios.

Pregunta 20: Existe algún procedimiento aplicable en caso de un incidente de seguridad?

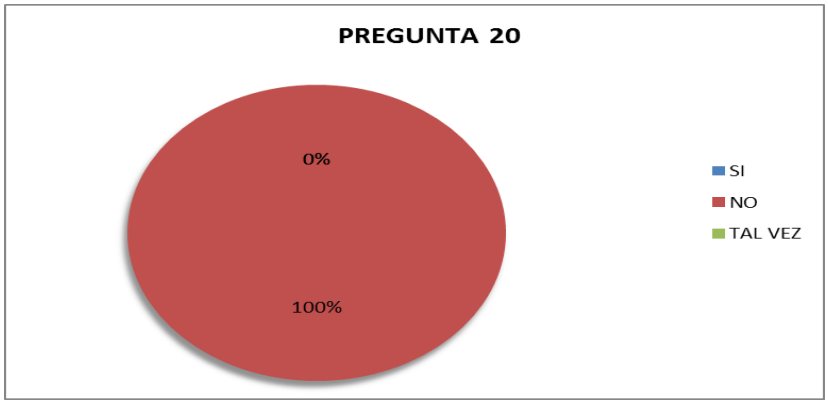


Figura. 2.20. Procedimientos aplicables ante un incidente de seguridad
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.20 ilustra los resultados de la pregunta 20. Además se conoce que no existen procedimientos aplicables ante un incidente de seguridad provocando riesgo de pérdida de información y financieras.

En relación al dominio A11-Seguridad Física y Ambiental, descrito en la norma ISO 27001, se realizaron 5 preguntas detalladas en la tabla N. 2.5 orientadas a 3 representantes del área de Tecnología Informática. Se obtuvieron los siguientes resultados:

Pregunta 21: Existen controles de acceso a las áreas restringidas para el personal no autorizado?

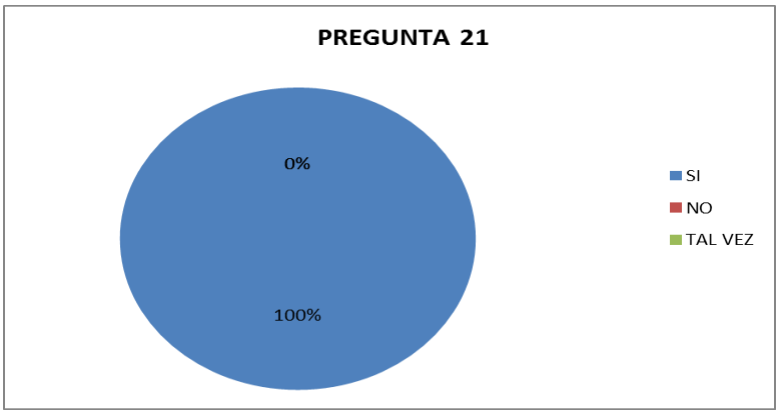


Figura. 2.21. Controles de acceso a las áreas restringidas
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.21 ilustra los resultados de la pregunta 21. Además se conoce que existen controles de acceso a las áreas restringidas, eso lo realizan mediante controles biométricos ya que para poder accesar a ciertas áreas únicamente puede hacer uso de su credencial.

Con estos antecedentes se expone en la Tabla 2.45 las 5 incidencias más importantes que se han presentado en los últimos meses en la empresa Leterago del Ecuador S.A, relacionados principalmente con correos maliciosos, cortocircuitos, errores de ingreso en el sistema SAC, etc. La empresa no cuenta con personal 24x7 y no posee herramientas para poder mitigar los riesgos de manera automática.

Tabla. 2.5 Registro de Incidentes en Leterago del Ecuador S.A

REGISTRO DE INCIDENTES EN LETERAGO DEL ECUADOR S.A									
No.	**DETALLE INCIDENTE**	**REGISTRO**		**SOLUCIÓN**		**TIEMPO**	**CRITICIDAD**	**TRATAMIENTO**	**ESTADO**
		FECHA	**HORA**	**FECHA**	**HORA**	**INCIDENTE**			
1	DoS	20-feb-18	10:55:00	20-feb-18	10:58:00	0:03:00	Alta	Bloqueo IP	Cerrado
2	Cortocircuito	11-abr-18	15:00:00	11-abr-18	15:15:00	0:15:00	Alta	Cambio de disco duro en PC	Cerrado
3	Correo electrónico malicioso	11-may-18	10:40:00	11-may-18	10:42:00	0:02:00	Alta	Comunicación interna de alerta	Cerrado
4	Correo electrónico malicioso	16-may-18	11:50:00	16-may-18	11:55:00	0:05:00	Alta	Comunicación interna de alerta	Cerrado
5	Error ingreso sistema SAC	27-jul-18	15:40:00	27-jul-18	15:45:00	0:05:00	Alta	Corrección del ingreso en el sistema	Cerrado

Fuente: **Investigación propia**

Pregunta 22: En áreas seguras existe algún control para el personal autorizado y ajeno?

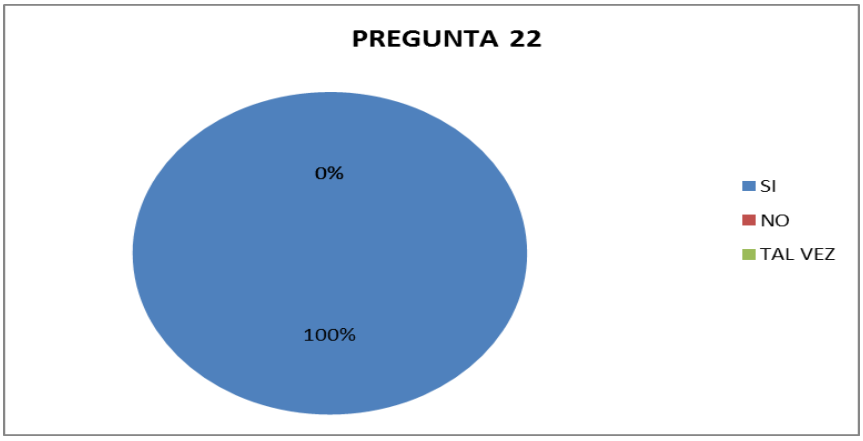


Figura. 2.22. Control de acceso a las áreas restringidas personal autorizado y ajeno
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.22 ilustra los resultados de la pregunta 22. Además se conoce que existe un control de acceso a las áreas restringidas a personal autorizado y ajeno, el departamento de Talento Humano se encarga de distribuir las credenciales al personal con los permisos necesarios para poder ingresar a áreas permitidas de la empresa.

Pregunta 23: Los equipos se encuentran en sitios seguros fuera de cualquier riesgo?

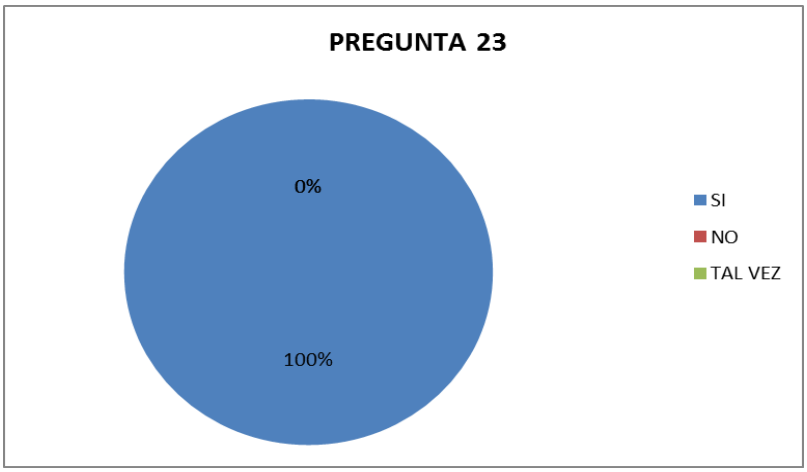


Figura. 2.23. Equipos ubicados fuera de cualquier riesgo
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.23 ilustra los resultados de la pregunta 23. Además se conoce que los equipos si se encuentran ubicados en lugares fuera de cualquier riesgo, goteras, humedad, calor, etc.

Pregunta 24: Existe seguridades frente a complicaciones con la alimentación eléctrica?

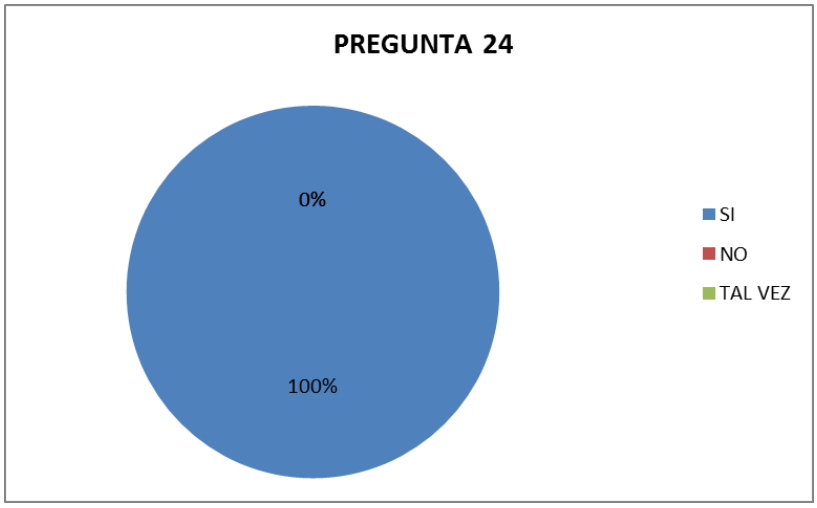


Figura. 2.24. Seguridades frente a complicaciones eléctricas
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.24 ilustra los resultados de la pregunta 24. Además se conoce que existen seguridades frente a complicaciones eléctricas, la compañía tiene el equipo UPS funcionando constantemente dotando de corriente continua a los equipos de cómputo.

Pregunta 25: Existe seguridad del cableado del Centro de Datos frente a posibles daños o intercepciones?

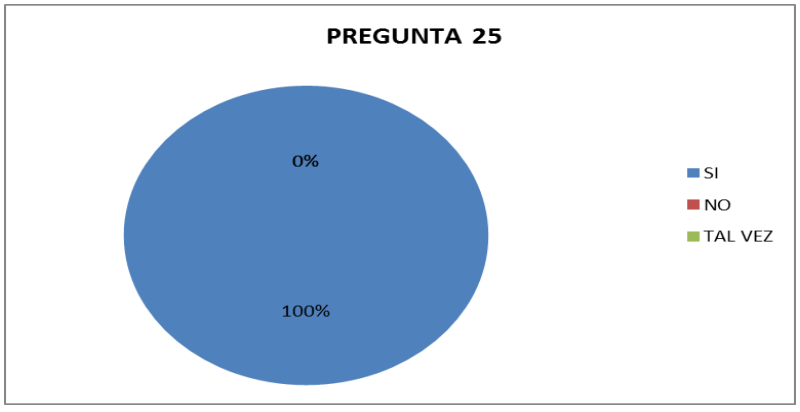


Figura. 2.25. Seguridades del cableado del centro de datos frente a posibles intercepciones
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.25 ilustra los resultados de la pregunta 25. Además se conoce que existen seguridades del cableado del centro de datos frente a posibles intercepciones ya que de no ser así se vería afectado los servicios de comunicación causando pérdidas de enlace a la organización.

En relación al dominio A13-Seguridad en las Comunicaciones, descrito en la norma ISO 27001, se realizaron 5 preguntas detalladas en la tabla N. 2.6 orientadas a 3 representantes del área de Tecnología Informática. Se obtuvieron los siguientes resultados:

Pregunta 26: Los procesos operativos se encuentran definidos en la documentación de la política de seguridad?

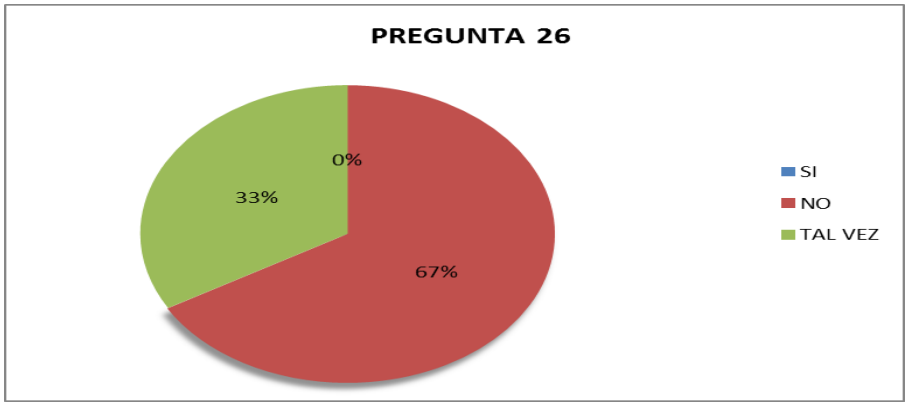


Figura. 2.26. Procesos operativos definidos en la política de seguridad
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.26 ilustra los resultados de la pregunta 26. Además se conoce que no están definidos en la política de seguridad los procesos operativos, causando de esta manera errores en el uso de los sistemas de información, en ingresos y egresos de productos.

Pregunta 27: Existe personal responsable de asegurar una reacción rápida y efectiva frente a un inconveniente de seguridad?

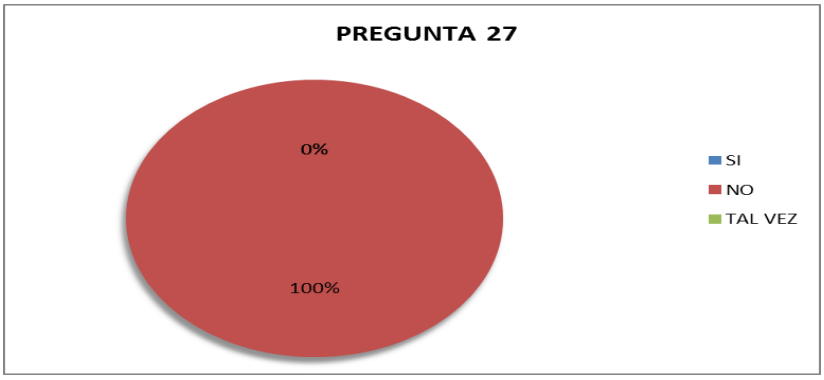


Figura. 2.27. Reacción efectiva del personal ante un incidente de seguridad
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.27 ilustra los resultados de la pregunta 27. Además se conoce que no existe una reacción efectiva del personal ante un incidente de seguridad por motivos de que no hay personal calificado para tal efecto.

Pregunta 28: Existe alguna forma para reducir el uso erróneo de los sistemas de información?

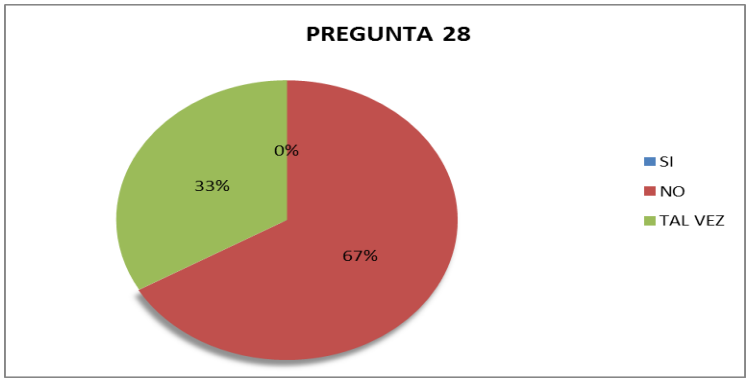


Figura. 2.28. Formas para reducir el uso erróneo de los sistemas de información
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.28 ilustra los resultados de la pregunta 28. Además se conoce no existen formas para reducir el uso erróneo de los sistemas de información, causando de esta manera retrasos en los despachos de productos.

Pregunta 29: Existe empresas externas encargadas de la gestión de los sistemas de información?

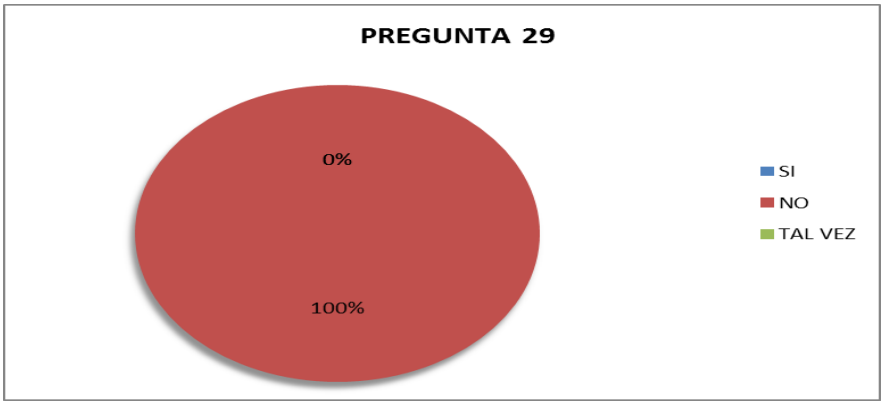


Figura. 2.29. Empresas externas encargadas de la gestión de los sistemas de información
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.29 ilustra los resultados de la pregunta 29. Además se conoce que no existen empresas externas encargadas de la gestión de los sistemas de información, la organización no ha realizado este tipo de inversiones hasta el momento.

Pregunta 30: Existe algún control para evitar el software malicioso?

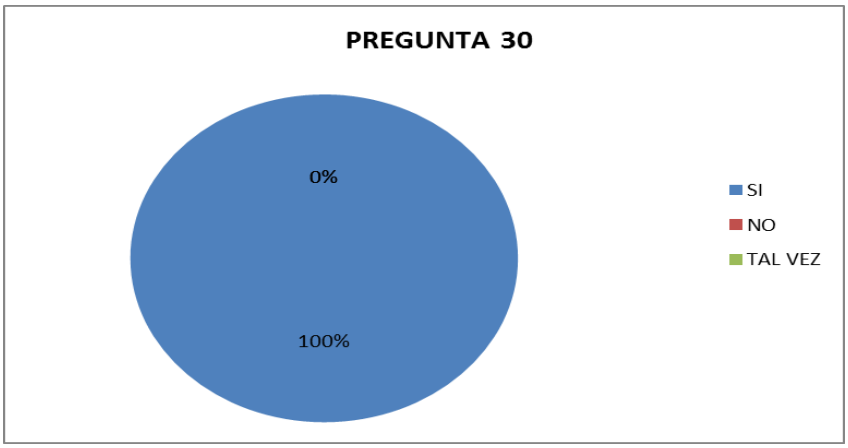


Figura. 2.30. Control para evitar software malicioso
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.30 ilustra los resultados de la pregunta 30. Además se conoce que si existe un control para evitar software malicioso, se lo realiza mediante la consola del antivirus corporativo McAfee.

En relación al dominio A9-Control de Accesos, descrito en la norma ISO 27001, se realizaron 4 preguntas detalladas en la tabla N. 2.7 orientadas a 3 representantes del área de Tecnología Informática. Se obtuvieron los siguientes resultados:

Pregunta 31: Existe alguna norma o política para el control de acceso?

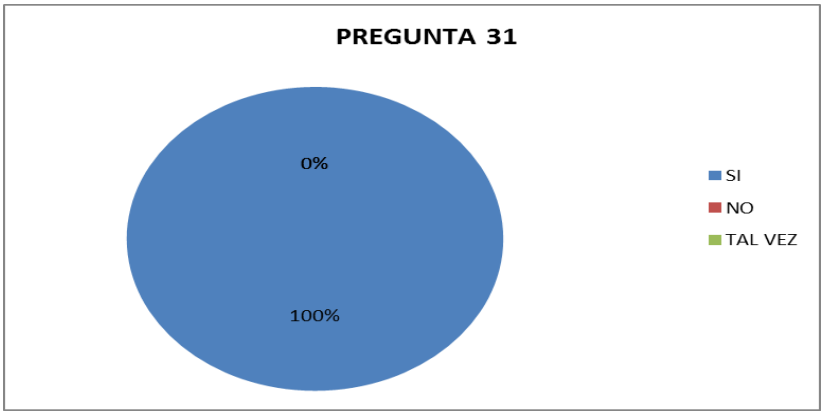


Figura. 2.31. Norma o política para control de acceso
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.31 ilustra los resultados de la pregunta 31. Además se conoce que si existe una norma o política para control de acceso, está aprobado y controlado por la gerencia de T.I.

Pregunta 32: Existe una norma o procedimiento de registro y quitar accesos?

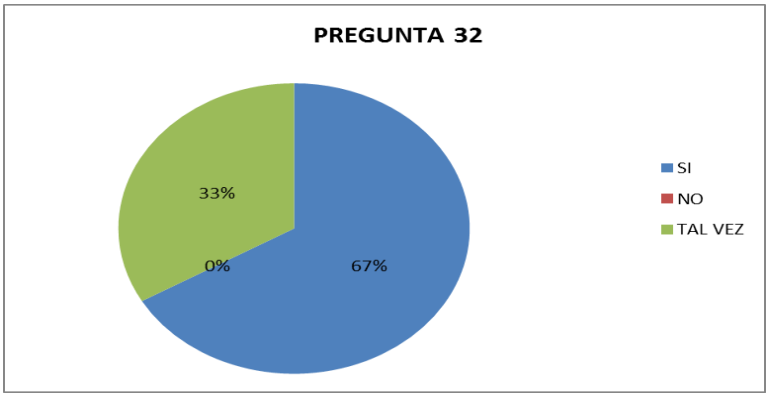


Figura. 2.32. Norma o procedimiento de registro y quitar accesos
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.32 ilustra los resultados de la pregunta 32. Además se conoce existe una norma o procedimiento de registro y quitar accesos, el mismo que lo realiza el departamento de servicios generales con el consentimiento de la gerencia de T.I.

Pregunta 33: Se controla el uso de privilegios a los usuarios?

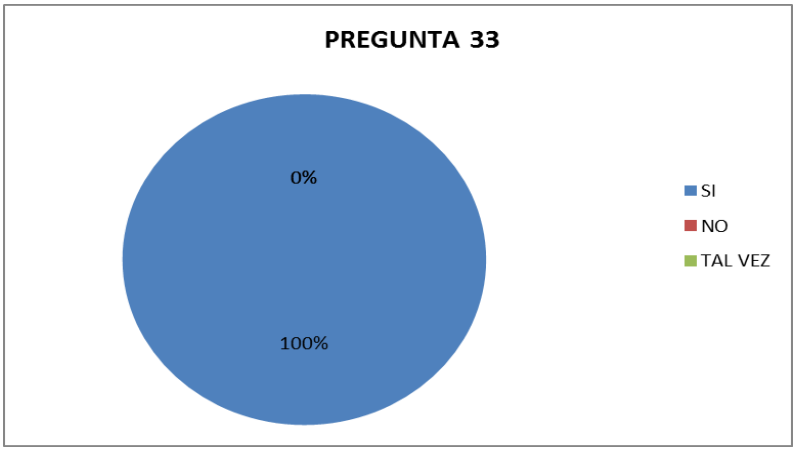


Figura. 2.33. Control de uso de privilegios a los usuarios
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.33 ilustra los resultados de la pregunta 33. Además se conoce que existen controles de uso de privilegios a los usuarios, eso se lo realiza al momento de crear

los perfiles de usuario y dependiendo las herramientas de software con las que vaya a trabajar el usuario.

Pregunta 34: Existe una política para el manejo de contraseñas a los usuarios?

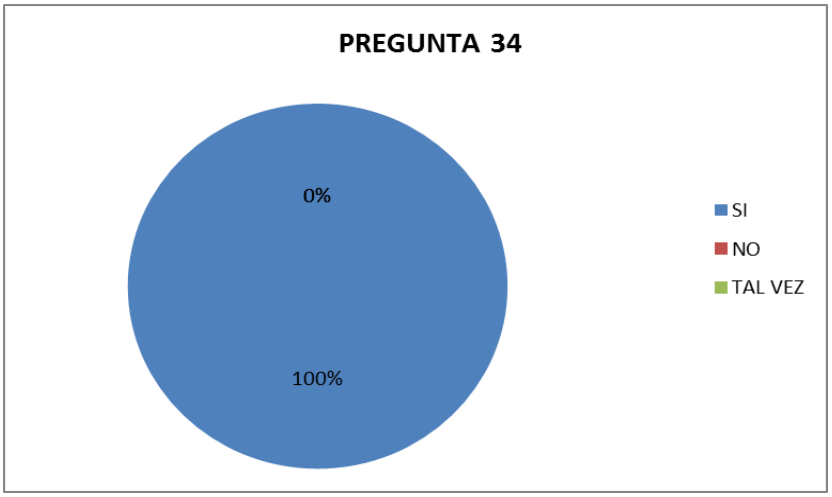


Figura. 2.34. Política para el manejo de contraseñas a los usuarios
Fuente: Investigación propia
Elaborado por: El autor

En la figura 2.34 ilustra los resultados de la pregunta 34. Además se conoce que existe una política para el manejo de contraseñas a los usuarios, permitiendo la creación de contraseñas fuertes y seguras.

Empleando las directrices detalladas en la Norma ISO 27005, una vez que el riesgo ha sido evaluado, hay que tomar medidas acerca de como va hacer tratado el riesgo, con lo cual nos vamos a apoyar con las siguientes opciones:

- Evitación del riesgo: Evitando defectos de los componentes.
- Comunicación del riesgo: Estableciendo ideas para tratar al riesgo y divulgarlas.
- Reducción del riesgo: Detectando de manera oportuna los factores internos y externos que afectan a la organización.
- Retención del riesgo: Creando ideas para solucionar las consecuencias de los riesgos.
- Transferencia del riesgo: Compartiendo parte del riesgo con terceros (proveedores) para que de soporte y solución al inconveniente.

Después de evaluar la forma de tratar al riesgo se propone realizar unas sugerencias a las políticas existentes, controles que sean necesarios para evitar que los riesgos se

materialicen, realizar un plan de comunicación interna mediante el correo electrónico de la compañía exponiendo pequeños tips informativos a los usuarios acerca de como evitar riesgos en la seguridad de la información para que las pongan en práctica.

Análisis de Factibilidad

La organización posee la suficiente infraestructura como para poder sugerir la opción de crear un departamento de seguridad de la información.

2.1.2. Factibilidad Técnica

El plan de seguridad informática es técnicamente factible ya que el personal se encuentra capacitado y experimentado en el tema, el jefe nacional de infraestructura tiene formación en seguridad informática ya que la organización le ha enviado a charlas y cursos dictados por profesionales, la especialista de tecnología informática ha realizado trabajos de seguridad y ha asistido a cursos obteniendo la certificación ISO 27001.

2.1.3. Factibilidad Operacional

La operatividad de la propuesta del Sistema de Gestión de Seguridad de la Información es factible ya que se cuenta con el apoyo y buena predisposición de la especialista de tecnología informática y el jefe nacional de infraestructura.

El aspecto operativo de los miembros del departamento de tecnología informática es óptimo ya que cuenta con un buen liderazgo por parte de la gerencia de T.I, facilitando incentivos a sus colaboradores tanto monetarios como a nivel profesional, promocionando a los miembros del equipo, asignando nuevas responsabilidades para poder canalizar las funciones de la mejor manera posible, de tal manera que se pueda llegar a los propósitos planteados por el departamento y la organización que permitan el incremento de la productividad debido al buen desempeño de los responsables a cargo de los proyectos tecnológicos.

2.1.4. Factibilidad Económica

A continuación se realiza un presupuesto de los recursos que se utilizarán en la propuesta del Sistema de Gestión de Seguridad de la Información, que se detalla en la Tablas 2.6 y 2.7:

Tabla N. 2.6 Flujo de Pago

FLUJO DE PAGO	
RECURSOS	**COSTOS**
RECURSOS HUMANOS	2.500
RECURSOS TECNOLÓGICOS	20.517
SOFTWARE	13.340,52
RECURSOS MATERIALES	334,50
IMPREVISTOS	120,00
TOTAL	36.812,02

Fuente: Investigación propia

Tabla N. 2.7 Presupuesto de Recursos

RECURSOS HUMANOS			
No.	**CARGO**	**COSTO INDIVIDUAL**	**COSTO TOTAL**
1	Ing. en Sistemas	$ 1.500	$1.500
1	Asistente de Sistemas	$1.000	$1.000
		TOTAL	$ 2.500
RECURSOS TECNOLÓGICOS			
CANTIDAD	**DESCRIPCIÓN**	**COSTO/HORA**	**TOTAL**
1	120 Horas Computadora	$ 0,95	$ 114,00
1	Impresora HP		$ 25,00
1	Equipamiento para sistemas de respaldo Data Center		$ 20.378,00
		TOTAL	$ 20.517

SOFTWARE			
CANTIDAD	**DESCRIPCIÓN**	**COSTO UNITARIO**	**COSTO TOTAL**
12	Licencia ARCSERVE UDP V6.5	$ 788,31	$ 9459,72
12	Licencia ARCSERVE UDP V6.5 MANTENIMIENTO	$ 323,4	$ 3880,8
		TOTAL	$ 13.340,52
RECURSOS MATERIALES			
CANTIDAD	**DESCRIPCIÓN**	**COSTO**	**TOTAL**
1	Resma de papel A4	$ 4,50	$ 4,50
4	Cartuchos para impresora a color	$ 45,00	$ 180,00
15	Viáticos	$ 10,00	$ 150,00
		TOTAL	$ 334,50

Fuente: Investigación propia

2.1.5 Modelo o estándar a aplicar

Fundamentación

Dicha propuesta se basa en los lineamientos establecidos en la norma ISO 27001, en el tema de determinar la propuesta de Sistema de Gestión de Seguridad de la Información, cuyo origen es el análisis de riesgo que se plantea en la ISO 27005.

La norma ISO 27001 “fue preparado por el Comité denominado: ISO/IEC JTC 1, y esta segunda edición (2013) anula y sustituye a la primera edición (2005) que ha sido revisada técnicamente.” (Activos Concursales S.L., 2016), en donde expone que requisitos se debe tener para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI).

Metodología

La metodología que se va a utilizar para elaborar la propuesta del Sistema de Gestión de Seguridad de la Información, se basa en los pasos expuestos en la norma ISO 27001:

Planificar

- Definir los objetivos.
- Valoración del riesgo.
- Tratamiento del riesgo.

Hacer

- Plan para tratar a los riesgos.

Verificar

- Registrar los niveles de cumplimiento.
- Procedimientos para la planificación de los procesos operativos.

Actuar

- Registro de resultados obtenidos de las acciones acogidas.
- Toma de acciones preventivas y correctivas.

Plan de la seguridad de la información

Ponemos en consideración un concepto acerca de lo que es y/o significa la seguridad de la información:

"La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización." (ISO27000, 2014)

Objetivos de la propuesta

- Disminuir el riesgo a un grado aceptable para reforzar la seguridad de toda la empresa Leterago del Ecuador S.A

- Involucrar a los empleados de la organización: usuarios (gerentes, jefes departamentales, asistentes) con el procedimiento de la seguridad de la información y sus controles.
- Mantener un estándar de calidad en la organización brindando confianza y seguridad al usuario con la información que se genera en el día a día.

Alcance y Límites

La presente propuesta compromete los siguientes aspectos:

- Software que maneja la organización.
- Hardware.
- Elementos que componen el Centro de Datos de la organización.
- Gerentes.
- Jefes departamentales.
- Asistentes.

Importancia

Es de vital importancia disponer de una propuesta del Sistema de Gestión de Seguridad de la Información ya que no sirve de nada tener una gran inversión en activos e infraestructura tales como: hardware, software, comunicaciones, redes, sistemas informáticos, bases de datos, etc. Si no existe el tratamiento adecuado y los riesgos que esto implica como es el Centro de Datos de Leterago del Ecuador S.A, donde se encuentra la pieza medular del negocio como son: los sistemas, servicios de comunicación, red, almacenamiento de información por recursos de red, servidores lo cual constituye una infrestructura de calidad para poder brindar a sus clientes internos y externos un servicio confiable y seguro.

Marco referencial

El marco referencial permite definir los objetivos de control, los controles a tener en cuenta ante el riesgo y además comprende la manera de evaluar y gestionar el riesgo.

3. CAPÍTULO III. IMPLEMENTACIÓN

Identificación del riesgo

Enumerar los riesgos de seguridad de la información para el control de los elementos más importantes del Centro de Datos de la empresa Leterago del Ecuador S.A.

Determinar una propuesta de seguridad de la información para el Centro de Datos de la empresa Leterago del Ecuador S.A.

Entre los elementos más importantes que componen el Centro de Datos de la organización se ilustra en la Tabla 2.8.

Tabla. 3.1. Elementos del Centro de Datos

TIPO	NOMBRE DEL ACTIVO
APLICACIONES INFORMÁTICAS	1. [SI_SAC] Sistema Administrativo Comercial 2. [SI_NETORDER] Sistema de Pedidos 3. [SI_EVOLUTION] Sistema de Talento Humano 4. [SO] Sistema Operativo 5. [HER_SW] Herramientas Software 6. [ANT_VIR] Anti-virus
SERVICIOS	7. [SV_DNS] Servidor DNS 8. [SV_DHCP] Servidor DHCP 9. [SV_BD] Servidor Bases de Datos 10. [SV_CAM] Servidor Cámaras IP 11. [SV_VoIP] Servidor Telefonía IP
REDES DE COMUNICACIONES	12. [RO_ISP] Router Proveedor de Servicios de internet 13. [RO_ISP] Router Cisco Meraki de control de navegación en internet
EQUIPAMIENTO INFORMÁTICO	14. [FW_UTM] Firewall / Equipo Unificado contra Amenazas 15. [PC] Equipos de cómputo 16. [LAPTOPS] Equipos portables 17. [SW_A] Switch Administrable
EQUIPAMIENTO AUXILIAR	18. [CAB_RED] Cableado de Red 19. [UPS] Sistema de Alimentación Ininterrumpida
INSTALACIONES	20. [GAB_INC] Gabinete de Incendios 21. [RACK_SV] Rack de Servidores
PERSONAL	22. [TEC_ADMIN] Técnico Administrativo 23. [TEC_ADMIN_EX] Técnico Administrativo Experto

Fuente: Investigación propia

3.1. Aplicación del modelo, estándar o metodología

Se detalla a continuación las matrices de impacto, probabilidad de ocurrencia y riesgo de los activos más importantes que componen el Centro de Datos de Leterago del Ecuador S.A, antes de empezar a definirlos es pertinente recordar las fórmula con la cual se esta elaborando la matriz de riesgo, la fórmula es la siguiente:

RIESGO = IMPACTO * PROBABILIDAD DE OCURRENCIA

En la Tabla 3.2 se ilustra las escalas para elaborar la matriz de impacto.

Tabla. 3.2. Escalas de la matriz de impacto

CLASIFICACIÓN DEL NIVEL	DESCRIPCIÓN	VALORES	VALOR MONETARIO
Alto	Grandes consecuencias económicas y financieras	9 - 10	$ 50.000
Significativo	Consecuencias Significativas	7 - 8	$ 25.000
Moderado	Consecuencias moderadas pero significativas	4 - 5 - 6	$ 10.000
Menor	Consecuencias minoritarias pero significativas	2 - 3	$ 5.000
Insignificante	Consecuencias insignificantes	1	$ 800

Fuente: (MAGERIT, 2013)

En la Tabla 3.3 se ilustra el cálculo de la probabilidad de ocurrencia.

Tabla. 3.3. Escalas de la matriz de ocurrencia

PROBABILIDAD	DESCRIPCIÓN	FRECUENCIA
Muy Probable (5)	Ocurre en la mayoría de las circunstancias	1
Probable (4)	Ocurre en la menoría de las circunstancias	0.75
Posible (3)	Podría ocurrir algunas veces	0.5
Incierto (2)	No es muy probable que ocurra	0.25
Improbable (1)	Ocurre en casos excepcionales	0.1

Fuente: (MAGERIT, 2013)

En la Tabla 3.4 se ilustra la matriz de impacto de las aplicaciones informáticas.

Tabla. 3.4. Matriz de impacto de las aplicaciones informáticas

MATRIZ DE IMPACTO						
ACTIVOS	IMPACTO EN RESULTADOS	IMPACTO EN CLIENTES	IMPACTO EN OPERACIONES	IMPACTO REGULATORIO	IMPACTO DE REPUTACIÓN	IMPACTO (IM)
Sistema SAC	10	10	10	4	10	44
Sistema NETORDER	9	9	9	2	9	38
Sistema EVOLUTION	9	8	8	2	9	36
Sistema Operativo	9	9	8	1	8	35
Herramienta de Software	9	9	8	1	6	33
Antivirus	9	8	8	1	9	35

Fuente: Investigación propia

En la Tabla 3.5 se ilustra la matriz de probabilidad de ocurrencia de las aplicaciones informáticas.

Tabla. 3.5. Matriz de probabilidad de ocurrencia de las aplicaciones informáticas

MATRIZ DE PROBABILIDAD DE OCURRENCIA				
ACTIVOS	NATURALES & AMBIENTALES	HUMANAS		PROBABILIDAD DE OCURRENCIA (PO)
		INTENCIONALES	DE INFRAESTRUCTURA	
Sistema SAC	0,25	0,5	0,5	0,063
Sistema NETORDER	0,25	0,5	0,5	0,063
Sistema EVOLUTION	0,25	0,5	0,5	0,063
Sistema Operativo	0,25	0,5	0,5	0,063
Herramienta de Software	0,25	0,5	0,5	0,063
Antivirus	0,25	0,5	0,5	0,063

Fuente: Investigación propia

En la Tabla 3.6 se ilustra la matriz de riesgo de ocurrencia de las aplicaciones informáticas.

Tabla. 3.6. Matriz de riesgo de las aplicaciones informáticas

MATRIZ DE RIESGO			
NOMBRE DEL RECURSO	IMPACTO (IM)	PROBABILIDAD DE OCURRENCIA (PO)	RIESGO (IM*PO)
Sistema SAC	44	0,063	2,75
Sistema NETORDER	38	0,063	2,38
Sistema EVOLUTION	36	0,063	2,25
Sistema Operativo	35	0,063	2,19
Herramienta de Software	33	0,063	2,06
Antivirus	35	0,063	2,19

Fuente: Investigación propia

En la Tabla 3.7 se ilustra la matriz de impacto de los servicios.

Tabla. 3.7. Matriz de impacto de los servicios

MATRIZ DE IMPACTO						
ACTIVOS	IMPACTO EN RESULTADOS	IMPACTO EN CLIENTES	IMPACTO EN OPERACIONES	IMPACTO REGULATORIO	IMPACTO DE REPUTACIÓN	IMPACTO (IM)
Servidor DNS	9	9	8	4	9	39
Servidor DHCP	9	9	8	4	9	39
Servidor Base de Datos	10	10	10	4	10	44
Servidor Cámaras IP	9	9	8	4	9	39
Servidor Telefonía IP	9	9	8	4	8	38

Fuente: Investigación propia

En la Tabla 3.8 se ilustra la matriz de probabilidad de ocurrencia de los servicios.

Tabla. 3.8. Matriz de probabilidad de ocurrencia de los servicios

MATRIZ DE PROBABILIDAD DE OCURRENCIA				
ACTIVOS	NATURALES & AMBIENTALES	HUMANAS		PROBABILIDAD DE OCURRENCIA (PO)
		INTENCIONALES	DE INFRAESTRUCTURA	
Servidor DNS	0,25	0,5	0,5	0,063
Servidor DHCP	0,25	0,5	0,5	0,063
Servidor Base de Datos	0,25	0,5	0,5	0,063
Servidor Cámaras IP	0,25	0,5	0,5	0,063
Servidor Telefonía IP	0,25	0,5	0,5	0,063

Fuente: Investigación propia

En la Tabla 3.9 se ilustra la matriz de riesgo de los servicios.

Tabla. 3.9. Matriz de riesgo de los servicios

MATRIZ DE RIESGO			
NOMBRE DEL RECURSO	IMPACTO (IM)	PROBABILIDAD DE OCURRENCIA (PO)	RIESGO (IM*PO)
Servidor DNS	39	0,063	2,44
Servidor DHCP	39	0,063	2,44
Servidor Base de Datos	44	0,063	2,75
Servidor Cámaras IP	39	0,063	2,44
Servidor Telefonía IP	38	0,063	2,38

Fuente: **Investigación propia**

En la Tabla 3.10 se ilustra la matriz de impacto de redes de comunicaciones.

Tabla. 3.10. Matriz de impacto de redes de comunicaciones

MATRIZ DE IMPACTO						
ACTIVOS	IMPACTO EN RESULTADOS	IMPACTO EN CLIENTES	IMPACTO EN OPERACIONES	IMPACTO REGULATORIO	IMPACTO DE REPUTACIÓN	IMPACTO (IM)
Router Central	10	10	7	4	9	40
Firewall 1	8	8	8	4	8	36
Switches de Core	10	10	9	4	9	42
Servidores de Aplicaciones	10	10	10	7	9	46

Fuente: Investigación propia

En la Tabla 3.11 se ilustra la matriz de probabilidad de redes de comunicaciones.

Tabla. 3.11. Matriz de probabilidad de ocurrencia de redes de comunicaciones

MATRIZ DE PROBABILIDAD DE OCURRENCIA				
ACTIVOS	NATURALES & AMBIENTALES	HUMANAS		PROBABILIDAD DE OCURRENCIA (PO)
		INTENCIONALES	DE INFRAESTRUCTURA	
Router Central	0,25	0,5	0,5	0,063
Firewall 1	0,25	0,5	0,5	0,063
Switches de Core	0,25	0,5	0,5	0,063
Servidores de Aplicaciones	0,25	0,75	0,75	0,141

Fuente: **Investigación propia**

En la tabla N.3.12 se ilustra la matriz de riesgo de redes de comunicaciones.

Tabla. 3.12. Matriz de riesgo de redes de comunicaciones

MATRIZ DE RIESGO			
NOMBRE DEL RECURSO	IMPACTO (IM)	PROBABILIDAD DE OCURRENCIA (PO)	RIESGO (IM*PO)
Router Central	40	0,063	2,50
Firewall 1	36	0,063	2,25
Switches de Core	42	0,063	2,63
Servidores de Aplicaciones	46	0,141	6,47

Fuente: Investigación propia

En la Tabla 3.13 se ilustra la matriz de impacto del equipamiento informático.

Tabla. 3.13. Matriz de impacto del equipamiento informático

MATRIZ DE IMPACTO						
ACTIVOS	IMPACTO EN RESULTADOS	IMPACTO EN CLIENTES	IMPACTO EN OPERACIONES	IMPACTO REGULATORIO	IMPACTO DE REPUTACIÓN	IMPACTO (IM)
Firewall	9	8	9	4	9	39
Equipos de escritorio	9	8	9	4	9	39
Equipos portables	9	8	9	4	9	39
Switch Administrable	9	9	9	4	10	41

Fuente: Investigación propia

En la Tabla 3.14 se ilustra la matriz de probabilidad de ocurrencia del equipamiento informático.

Tabla. 3.14. Matriz de probabilidad de ocurrencia del equipamiento informático

MATRIZ DE PROBABILIDAD DE OCURRENCIA				
ACTIVOS	NATURALES & AMBIENTALES	HUMANAS		PROBABILIDAD DE OCURRENCIA (PO)
		INTENCIONALES	DE INFRAESTRUCTURA	
Firewall	0,25	0,5	0,5	0,063
Equipos de escritorio	0,25	0,5	0,5	0,063
Equipos portables	0,25	0,5	0,5	0,063
Switch Administrable	0,25	0,5	0,5	0,063

Fuente: Investigación propia

En la Tabla 3.15 se ilustra la matriz de riesgo del equipamento informático.

Tabla. 3.15. Matriz de riesgo del equipamiento informático

MATRIZ DE RIESGO			
NOMBRE DEL RECURSO	IMPACTO (IM)	PROBABILIDAD DE OCURRENCIA (PO)	RIESGO (IM*PO)
Firewall	39	0,063	2,44
Equipos de escritorio	39	0,063	2,44
Equipos portables	39	0,063	2,44
Switch Administrable	41	0,063	2,56

Fuente: Investigación propia

En la tabla 3.16 se ilustra la matriz de impacto del equipamiento auxiliar.

Tabla. 3.16. Matriz de impacto del equipamiento auxiliar

MATRIZ DE IMPACTO						
ACTIVOS	IMPACTO EN RESULTADOS	IMPACTO EN CLIENTES	IMPACTO EN OPERACIONES	IMPACTO REGULATORIO	IMPACTO DE REPUTACIÓN	IMPACTO (IM)
Cableado de Red	9	9	9	4	9	40
Sistema de Alimentación Ininterrumpida	10	10	10	4	10	44

Fuente: **Investigación propia**

En la Tabla 3.17 se ilustra la matriz de probabilidad de ocurrencia del equipamiento auxiliar.

Tabla. 3.17. Matriz de probabilidad de ocurrencia del equipamiento auxiliar

MATRIZ DE PROBABILIDAD DE OCURRENCIA				
ACTIVOS	NATURALES & AMBIENTALES	HUMANAS		PROBABILIDAD DE OCURRENCIA (PO)
		INTENCIONALES	DE INFRAESTRUCTURA	
Cableado de Red	0,5	0,5	0,5	0,125
Sistema de Alimentación Ininterrumpida	0,5	0,5	0,5	0,125

Fuente: Investigación propia

En la Tabla 3.18 se ilustra la matriz de riesgo del equipamento auxiliar.

Tabla. 3.18. Matriz de riesgo del equipamiento auxiliar

MATRIZ DE RIESGO			
NOMBRE DEL RECURSO	IMPACTO (IM)	PROBABILIDAD DE OCURRENCIA (PO)	RIESGO (IM*PO)
Cableado de Red	40	0,125	5,00
Sistema de Alimentación Ininterrumpida	44	0,125	5,50

Fuente: Investigación propia

En la Tabla 3.19 se ilustra la matriz de impacto de las instalaciones.

Tabla. 3.19. Matriz de impacto de las instalaciones

MATRIZ DE IMPACTO						
ACTIVOS	IMPACTO EN RESULTADOS	IMPACTO EN CLIENTES	IMPACTO EN OPERACIONES	IMPACTO REGULATORIO	IMPACTO DE REPUTACIÓN	IMPACTO (IM)
Gabinete de incendios	9	9	9	4	9	40
Rack de servidores	9	8	9	4	8	38

Fuente: **Investigación propia**

En la Tabla 3.20 se ilustra la matriz de probabilidad de ocurrencia de las instalaciones.

Tabla. 3.20. Matriz de probabilidad de ocurrencia de las instalaciones

MATRIZ DE PROBABILIDAD DE OCURRENCIA				
ACTIVOS	NATURALES & AMBIENTALES	HUMANAS		PROBABILIDAD DE OCURRENCIA (PO)
		INTENCIONALES	DE INFRAESTRUCTURA	
Gabinete de incendios	0,25	0,5	0,5	0,063
Rack de servidores	0,25	0,5	0,5	0,063

Fuente: Investigación propia

En la Tabla 3.21 se ilustra la matriz de riesgo de las instalaciones.

Tabla. 3.21. Matriz de riesgo de las instalaciones

MATRIZ DE RIESGO			
NOMBRE DEL RECURSO	IMPACTO (IM)	PROBABILIDAD DE OCURRENCIA (PO)	RIESGO (IM*PO)
Gabinete de incendios	40	0,063	2,52
Rack de servidores	38	0,063	2,39

Fuente: Investigación propia

En la Tabla 3.22 se ilustra la matriz de impacto del personal.

Tabla. 3.22. Matriz de impacto del personal

MATRIZ DE IMPACTO						
ACTIVOS	IMPACTO EN RESULTADOS	IMPACTO EN CLIENTES	IMPACTO EN OPERACIONES	IMPACTO REGULATORIO	IMPACTO DE REPUTACIÓN	IMPACTO (IM)
Técnico administrativo	9	9	9	4	9	40
Técnico administrativo experto	10	10	10	6	9	45

Fuente: **Investigación propia**

En la tabla 3.23 se ilustra la matriz de probabilidad de ocurrencia del personal.

Tabla. 3.23. Matriz de probabilidad de ocurrencia del personal

MATRIZ DE PROBABILIDAD DE OCURRENCIA				
ACTIVOS	NATURALES & AMBIENTALES	HUMANAS		PROBABILIDAD DE OCURRENCIA (PO)
		INTENCIONALES	DE INFRAESTRUCTURA	
Técnico administrativo	0,25	0,5	0,5	0,063
Técnico administrativo experto	0,25	0,5	0,5	0,063

Fuente: Investigación propia

En la tabla 3.24 se ilustra la matriz de riesgo del personal.

Tabla. 3.24. Matriz de riesgo del personal

MATRIZ DE RIESGO			
NOMBRE DEL RECURSO	IMPACTO (IM)	PROBABILIDAD DE OCURRENCIA (PO)	RIESGO (IM*PO)
Técnico administrativo	40	0,063	2,52
Técnico administrativo experto	45	0,063	2,84

Fuente: Investigación propia

Manejo de los riesgos

Alcance y límites

- **Objetivo de la empresa Leterago del Ecuador S.A**

Contar con colaboradores competentes facilitando el mejoramiento de sus capacidades y habilidades requeridas.

- **Proceso de negocio**

El proceso de negocio del área farmacéutica se basa en los siguientes aspectos:

Las distribuidoras farmacéuticas son establecimientos farmacéuticos autorizados para realizar importación, exportación y venta al por mayor de medicamentos en general de uso humano, especialidades farmacéuticas, productos para la industria farmacéutica, auxiliares médicoquirúrgico, dispositivos médicos, insumos médicos, cosméticos y productos higiénicos. Deben cumplir con las buenas prácticas de almacenamiento y distribución determinadas por la autoridad sanitaria nacional. Funcionarán bajo la representación y responsabilidad técnica de un químico farmacéutico o bioquímico farmacéutico. (Articulo 45 De Las Distribuidoras Farmacéuticas, 2012)

- **Estructura**

En el siguiente organigrama se representa las gerencias que existen en la organización:

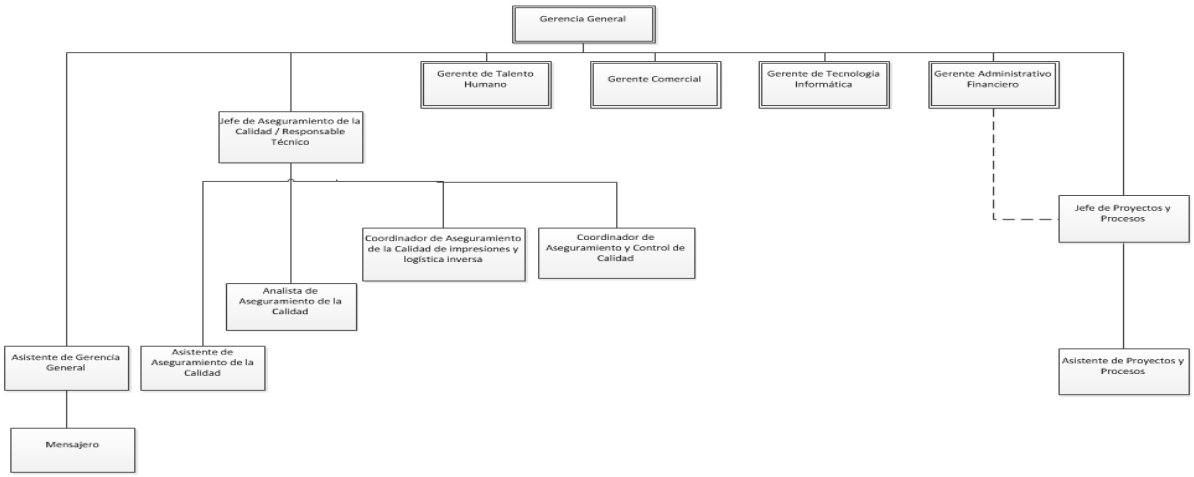


Figura. 2.35. Organigrama de las gerencias de Leterago del Ecuador
Fuente: Investigación propia
Elaborado por: El autor

- **Los requisitos legales**

Reglamento de Control y Funcionamiento de los Establecimientos Farmacéuticos (Acuerdo No. 0813)

- Tienen parcialmente definidas las políticas de seguridad de la información.
- La gestión de riesgo de la organización tiene como principal objetivo de implantar tácticas para evitar y confrontar posibles eventos adversos ya sean internos o externos (ambientales).
- El responsable de la información de los activos de la organización es el Ing. Cristian Mendia del departamento contable.

Controles

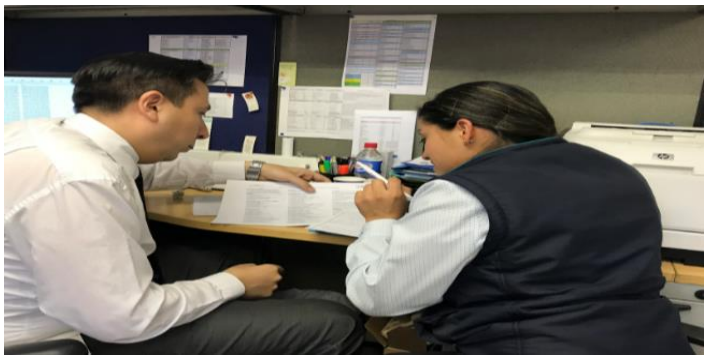


Figura. 2.36. Fotografía especialista de tecnología informática para toma de controles
Fuente: Investigación propia

Tabla 3.25. Controles existentes

No.	CONTROL	TABLA
1	Controles existentes de daños físicos	3.26
2	Controles existentes ante eventos naturales	3.27
3	Controles existentes ante la pérdida de servicios esenciales	3.28
4	Controles existentes ante fallas técnicas	3.29
5	Controles existentes ante acciones no autorizadas	3.30
6	Controles existentes ante funciones	3.31
7	Controles existentes de la gestión de activos	3.32

Fuente: Investigación propia

En la Tabla 3.26 se ilustra los controles existentes de daño físico en la organización.

Tabla. 3.26. Controles existentes de daños físicos

TIPO	AMENAZA	ORIGEN	SECCIÓN	CONTROL			
				TIPO		ESTADO DEL CONTROL	EVIDENCIA
				NO EXISTE	EXISTE	OBSERVACIONES	
DAÑO FÍSICO	Fuego	A, D, E	A.11.1.4		X	La organización cuenta con extinguidores de incendio en áreas estratégicas para cualquier emergencia	MAN.TI.001 Plan de contingencia de tecnología informática
	Accidentes graves	A, D, E	A.11.2.4		X	Existe un procedimiento cuando ocurre cualquier tipo de eventualidad con los equipos	INS.TI.001 Manejo de estaciones trabajo y equipos móviles
	Ubicación y protección de los equipos	A, D, E	A.11.2.1		X	Existe un instructivo para el manejo correcto de los equipos informáticos en el cual se detalla las politicas vigentes	INS.TI.001 Manejo de estaciones trabajo y equipos móviles
	Mantenimiento de equipos	A, D, E	A.11.2.4		X	Mantenimiento cuando se lo necesite pero no se lo hace con regularidad	INS.TI.001 Manejo de estaciones trabajo y equipos móviles

Fuente: Investigación propia

En la Tabla 3.27 se ilustra los controles existentes ante eventos naturales.

Tabla. 3.27. Controles existentes ante eventos naturales

TIPO	AMENAZA	ORIGEN	SECCIÓN	CONTROL			
				TIPO		ESTADO DEL CONTROL	EVIDENCIA
				NO EXISTE	EXISTE	OBSERVACIONES	
EVENTOS NATURALES	Fenómenos climáticos	E	A.11.1.4		X		MAN.TI.001 Plan de contingencia de tecnología informática
	Fenómenos sísmicos	E	A.11.1.4		X		MAN.TI.001 Plan de contingencia de tecnología informática
	Fenómenos volcánicos	E	A.11.1.4		X		MAN.TI.001 Plan de contingencia de tecnología informática
	Inundaciones	E	A.11.1.4		X		MAN.TI.001 Plan de contingencia de tecnología informática

Fuente: Investigación propia

En la Tabla 3.28 se ilustra los controles existentes ante la pérdida de servicios escenciales.

Tabla. 3.28. Controles existentes ante la pérdida de servicios esenciales

TIPO	AMENAZA	ORIGEN	SECCIÓN	CONTROL			
				TIPO		ESTADO DEL CONTROL	EVIDENCIA
				NO EXISTE	EXISTE	OBSERVACIONES	
PÉRDIDA DE SERVICIOS ESENCIALES	Seguridad de oficinas, recintos e instalaciones	A, D	A.11.1.3		X	La organización cuenta con el uso de toma corrientes UPS que permite que los equipos sigan encendidos	INS.TI.001 Manejo de estaciones trabajo y equipos móviles
	Falla en los equipos de telecomunicaciones	A, D	A.13.1.2		X	Se tiene un backup cuando existe caída de los enlaces, así como también se reporta al provedor dicho incidente para su respectiva solución	INS.TI.015 Adminstración de redes y comunicación de datos
	Manipulación del hardware	D	A.11.2.1		X	Existe una política donde hay una sanción al usuario por mala manipulación del hardware	INS.TI.001 Manejo de estaciones trabajo y equipos móviles
	Manipulación del software	D	A.12.6.2		X	Existe una política donde es obligatorio ingresar una clave de administrador para instalar las aplicaciones	INS.TI.001 Manejo de estaciones trabajo y equipos móviles
	Seguridad del cableado	A, D, E	A.11.2.3		X	Uso de tubos y canaletas para la protección del cableado	INS.TI.006 Condiciones generales y acondicionamiento físico y eléctrico del centro de datos de T.I
	Respaldo de la información	D	A.12.3.1		X	Se realiza respaldos de información regularmente y se lleva un control mediante una bitácora	INS.TI.003 RESTAURACIÓN Y RESPALDO DE LA INFORMACIÓN
	Protección de la información de registro	A, D	A.12.4.1		X	Las instalaciones son protegidas mediante un acceso biométrico y control de acceso a información mediante clave de administrador	INS.TI.003 Restauración y respaldo de la información

Fuente: Investigación propia

En la Tabla 3.29 se ilustra los controles existentes ante fallas técnicas.

Tabla. 3.29. Controles existentes ante fallas técnicas

TIPO	AMENAZA	ORIGEN	SECCIÓN	CONTROL			
				TIPO		ESTADO DEL CONTROL	EVIDENCIA
				NO EXISTE	EXISTE	OBSERVACIONES	
FALLAS TÉCNICAS	Daño en el equipo	A	A.11.2.1		X	Existe un instructivo sobre la administracion de garantias	INS.TI.014 Administración de garantías de equipos informáticos
	Malfuncionamiento del equipo	A	A.11.2.1		X	Existe un instructivo sobre la administracion de garantias	INS.TI.014 Administración de garantías de equipos informáticos
	Mal funcionamiento del software	A	A.12.5.1		X	Reinstalación del software	INS.TI.014 Administración de garantías de equipos informáticos

Fuente: Investigación propia

En la Tabla 3.30 se ilustra los controles existentes ante acciones no autorizadas.

Tabla. 3.30. Controles existentes ante acciones no autorizadas

TIPO	AMENAZA	ORIGEN	SECCIÓN	CONTROL			
				TIPO		ESTADO DEL CONTROL	EVIDENCIA
				NO EXISTE	EXISTE	OBSERVACIONES	
ACCIONES NO AUTORIZADAS	Uso de equipo sin autorización	D	A.12.4.2		X	Se cuenta con una norma que prohibe a los usuarios ingresar a equipos ajenos sin la debida autorización	INS.TI.001 Manejo de estaciones trabajo y equipos móviles
	Copia de software fraudulento	D	A.12.5.1		X	Se cuenta con una norma de licencimiento de software, donde se detalla las politicas que el usuario debe tomar en cuenta para el manejo del sofware	NOR.010 Licenciamiento de software
	Uso de software falsificado	D	A.12.5.1		X	Se cuenta con una norma de licencimiento de software, donde se detalla las politicas que el usuario debe tomar en cuenta para el manejo del sofware	NOR.010 Licenciamiento de software

Fuente: Investigación propia

En la Tabla 3.31 se ilustra los controles existentes ante acciones no autorizadas.

Tabla. 3.31. Controles existentes ante funciones comprometedoras

TIPO	AMENAZA	ORIGEN	SECCIÓN	CONTROL			
				TIPO		ESTADO DEL CONTROL	EVIDENCIA
				NO EXISTE	EXISTE	OBSERVACIONES	
FUNCIONES COMPROMETEDORAS	Error en el uso	A	A.8.1.3		X	Existen pistas de auditoria para ciertas transacciones en las cuales se puede dar seguimiento sobre algo inusual	MAN.TI.006 Manual del usuario del módulo de ventas del sistema SAC
	Abuso de derechos	A, D	A.9.4.1	X		Ausencia de proceso formal para la supervisión de los derechos de acceso	
	Incumplimiento de disponibilidad del personal	A, D, E	A.7.1.2		X	Si existe politica	FORM.MAN.TI.004.01 Responsabilidades de equipo de trabajo en proyectos de validación de sistemas

Fuente: **Investigación propia**

En la Tabla 3.32 se ilustra los controles existentes de la gestión de activos.

Tabla. 3.32. Controles existentes de la gestión de activos

TIPO	AMENAZA	ORIGEN	SECCIÓN	CONTROL			
				TIPO		ESTADO DEL CONTROL	EVIDENCIA
				NO EXISTE	EXISTE	OBSERVACIONES	
GESTIÓN DE ACTIVOS	Inventario de activos	D	A.8.1.1		X	Se tiene un control de inventario de los activos en el sistema de la empresa	INS.TI.001 Manejo de estaciones trabajo y equipos móviles
	Propiedad de los activos	D	A.8.1.2		X	Se elabora un acta de entrega recepción de los equipos a cada uno de los usuarios	INS.TI.001 Manejo de estaciones trabajo y equipos móviles
	Uso aceptable de los activos	D	A.8.1.3		X	Se cuenta con carpetas personales para cada usuario en las cuales deben almacenar la información relacionada al trabajo, la cual se indica a los usuarios cuando se les otorga un equipo de cómputo	INS.TI.001 Manejo de estaciones trabajo y equipos móviles
	Devolución de activos	D	A.8.1.4		X	Se recepta los equipos según acta una vez culmina el contrato la empresa con el usuario	INS.TI.001 Manejo de estaciones trabajo y equipos móviles
	Robo de equipos	D	A.8.2.3		X	Existe una politica cuando existe robo de portátiles, en la cual se detalla que dicho incidente se lo debe reportar al áerea de Talento Humano con su respectiva denuncia, en la cual al usuario le descuentan del 30% del valor del equipo	INS.TI.001 Manejo de estaciones trabajo y equipos móviles
	Retiro de activos	A, D	A.11.2.5		X	La organización cuenta con un sistema de inventario de activos de T.I actualizado	INS.TI.001 Manejo de estaciones trabajo y equipos móviles

Fuente: **Investigación propia**

Políticas

Responsables

- Gerencia de tecnología informática.
- Jefe de infraestructura.
- Jefe de tecnolgía informática.
- Especialista de tecnología informática.

En la figura 2.37 se ilustran los procesos con los que actualmente se rige la organización:

Código	Estado	Nombre
FORM.INS...	APROBADO	Inventario de Cuentas con Máximos Privilegios
FORM.MA...	APROBADO	RESPONSABILIDADES Y EQUIPO DE TRABAJO EN PROYECTOS DE VALIDACIÓN DE SISTEMAS
FORM.SOP...	REVISADO	Solicitud Creación y Modificación de Cuentas Usuario
FORM.SOP...	REVISADO	Solicitud de Creación y Modificación de cuentas de Usuario Sistema SAC
FORM.SOP...	APROBADO	Solicitud de Bloqueo de Usuario
INS.TI.001	APROBADO	Manejo de Estaciones de Trabajo y Equipos Móviles
INS.TI.002	APROBADO	Sistema de Tickets
INS.TI.003	APROBADO	Respaldo y Restauración de la Información
INS.TI.004	APROBADO	Administración de Antivirus
INS.TI.005	APROBADO	Manejo de Desechos Electrónicos
INS.TI.006	APROBADO	Condiciones Generales y Acondicionamiento Físico y Eléctrico del Centro de Datos de T.I.
INS.TI.007	APROBADO	Administración de Cuentas con Máximos Privilegios
INS.TI.008	APROBADO	Calificación del Diseño (DQ)
INS.TI.009	APROBADO	Calificación de la Instalación (IQ)
INS.TI.010	APROBADO	Calificación de la Operación (OQ)
INS.TI.011	APROBADO	Calificación del Desempeño (PQ)
INS.TI.012	REVISADO	Uso Adecuado del Correo Electrónico
INS.TI.013	APROBADO	DISTRIBUCIÓN DE ACTUALIZACIONES DE SOFTWARE
INS.TI.014	APROBADO	Administración de Garantías de Equipos Informáticos
INS.TI.015	APROBADO	Administración de Redes y Comunicación de Datos
INS.TI.016	APROBADO	Retiro de Sistemas Informáticos
MAN.TI.001	APROBADO	Plan de Contingencia de Tecnología Informática
MAN.TI.002	APROBADO	Plan Maestro de Validación de Sistemas Informáticos
MAN.TI.003	APROBADO	Manual de Usuario del Módulo de Stock del Sistema SAC
MAN.TI.004	APROBADO	Plan de Ejecución y Validación del sistema SAC
MAN.TI.005	APROBADO	Manual de Usuario del Módulo de Configuración del Sistema SAC
MAN.TI.006	APROBADO	Manual de Usuario del Módulo de Ventas del Sistema SAC
NOR.010	APROBADO	Uso de Licenciamiento de Software
NOR.011	APROBADO	Uso Correcto del Internet
SOP.TI.001	APROBADO	Administración y Gestión de Usuarios
SOP.TI.002	APROBADO	Control de Cambios de Sistemas Informáticos

Figura. 2.37. Procesos de seguridad de la información
Fuente: Investigación propia
Elaborado por: El autor

Políticas propuestas

Las políticas de seguridad de la información debe contemplar un conjunto de recomendaciones y normativas sobre como se deberán tratar los siguientes aspectos:

- **Recursos Humanos:** Medidas de seguridad de la información cuando los empleados ingresen y salgan de la organización.
- **Gestión de Operaciones y Comunicaciones:** Garantizar el manejo de los sistemas de una manera más rápida y eficaz en las operaciones de la empresa.
- **Abuso de derechos:** Garantizar el buen uso de los privilegios que cada usuario mantiene para el manejo de los sistemas de la empresa.
- **Políticas de seguridad informática:** Garantizar la seguridad de la informacion en la empresa por parte de los usuarios.
- **Políticas de uso aceptable de los activos informáticos:** Garantizar el buen uso de lo equipos de la organización por parte de los usuarios.
- **Política del buen manejo de contraseñas:** Garantizar la creación y el buen manejo de las claves por parte de los usuarios.
- **Reporte de las incidencias y soluciones de la seguridad informática:** Este reporte garantizará que se lleve un registro cuidadoso de cada incidencia que suceda con su respectiva solución la cual se va a documentar detalladamente en caso de que se vuelva a presentar para que el/la responsable pueda actuar de manera rápida y efectiva.

Se describen las abreviaturas con las cuales se van a trabajar en los presentes documentos, como se puede ilustrar en la Tabla 3.33:

Tabla. 3.33. Abreviaturas del tipo de documento

INICIAL	FUNCIÓN	DESCRIPCIÓN
D	Documento	Documento Compromiso
L	Política	Documento que sirve como un lineamiento que se debe cumplir en la empresa Leterago del Ecuador S.A
R	Registros	Documento que evidencian ciertas actividades que se demuestra que el plan de Seguridad Informática se cumple

Fuente: Investigación propia

A. Documento de seguridad cuando ingresa o se despide un empleado

Leterago Documento de Medidas de Seguridad de la Información cuando un empleado ingrese o sea despedido de la organización			
Fecha de emisión: 14/08/2018	**Fecha de modificación:** 14/08/2018	**Fecha de aprobación:** 14/08/2018	**Identificador D-GER-01**
Elaborado por: Alvaro Vallejo		**Revisado y aprobado por:** Víctor Tolcachier	

I. INTRODUCCIÓN

Este documento permite conocer qué medidas de seguridad informática se adoptará cuando un empleado de la empresa Leterago del Ecuador ingrese o sea despedido por cualquier circunstancia.

II. POLÍTICAS

Las políticas que se adoptan en la empresa Leterago del Ecuador S.A involucran a: gerencia de tecnología informática, jefe de tecnología informática, asistentes de tecnología informática, gerencia de talento humano, jefes departamentales.

Gerencia de tecnología informática – Jefe de tecnología informática debe:

1. Aprobar un documento donde conste las políticas o normas a seguir, el mismo
   que será publicado y divulgado a gerentes, jefes departamentales, asistentes, demás personal administrativo y entidades externas relevantes.
2. Establecer un documento con las políticas de las medidas de seguridad informática en caso de que algún empleado ingrese o sea despedido aplicables en la empresa Leterago del Ecuador S.A.
3. Apoyar de manera activa la seguridad informática dentro de la empresa Leterago del Ecuador S.A mediante un acuerdo, reconociendo las responsabilidades que conlleva la seguridad de la información.

Documento 1: Normas cuando ingresa o despide un empleado (Elaborado por: El Investigador)

A. Documento de seguridad cuando ingresa o se despide un empleado

Documento de Medidas de Seguridad de la Información cuando un empleado ingrese o sea despedido de la organización
4. Dar el seguimiento necesario a la presente política para hacer cumplir en todas las áreas de la empresa y no se pasen por alto los procedimientos a seguir. **Asistentes de tecnología informática debe:** 1. Realizar el respectivo backup de la información del perfil de usuario de los archivos más relevantes del computador que pueda comprometer la actividad del negocio. 2. Revisar que el computador quede en óptimas condiciones para el futuro usuario que vaya a ocupar dicho equipo. 3. Configurar el nuevo perfil del usuario que va a utilizar el equipo con todos los programas y dispositivos que va a utilizar para la elaboración de su trabajo diario. 4. Proporcionar al nuevo usuario las claves de acceso. 5. Brindar a los usuarios unas pequeñas recomendaciones acerca del cuidado con los equipos informáticos y su correcto uso. 6. Copiar la información del usuario anterior en el nuevo perfil de usuario con la información que vaya a ocupar el nuevo usuario con la debida autorización de su jefe directo. **Jefes departamentales debe:** 1. Comunicar con la debida anticipación del despido del empleado a la Gerencia de talento humano para las acciones correspondientes. 2. Comunicar al jefe de tecnología informática con la debida anticipación para que los asistentes de tecnología informática puedan respaldar la información más relevante que el empleado tenga en su computador antes de que sea borrada o alterada. 3. Informar al jefe de tecnología informática mediante la creación de un ticket el ingreso del nuevo empleado con sus nombres completos, servicios y programas que va a utilizar en la elaboración de sus tareas diarias y además autorizar que información necesita el usuario anterior para proceder a copiar en el nuevo perfil de usuario.

Documento 1: Normas cuando ingresa o despide un empleado (Elaborado por: El Investigador)

A. Documento de seguridad cuando ingresa o se despide un empleado

Medidas de Seguridad de la Información cuando un empleado ingrese o sea despedido de la organización
Gerencia de talento humano debe: 1. Notificar al jefe y gerente de tecnología informática anticipadamente mediante la elaboración de un correo electrónico de manera que quede documentado la salida del empleado para que el jefe de tecnología informática pueda dar de baja al usuario en el Active Directory. 2. Avisar mediante la elaboración de un correo electrónico a los asistentes de tecnología informática para que revisen todos los equipos y dispositivos que estuvieron a cargo del empleado para que procedan a revisar si no hay alguna anomalía o mal funcionamiento de dichos equipos para proceder al descuento respectivo en la liquidación del empleado. 3. Informar al jefe de tecnología informática mediante la elaboración de un correo electrónico el ingreso del nuevo empleado. 4. Elaborar un contrato laboral donde especifique el cuidado que debe tener el empleado con la seguridad de la información. 5. Establecer roles y responsabilidades a los empleados para llevar a cabo una buena gestión en la seguridad informática. Respetar las políticas de las medidas de seguridad de la información cuando un empleado ingrese o sea despedido de la organización.

Documento 1: Normas cuando ingresa o despide un empleado (Elaborado por: El Investigador)

B. Documento para el buen manejo de sistemas y operaciones en la empresa

Leterago Documento de Políticas para el buen manejo de los Sistemas y Operaciones de la empresa			
Fecha de emisión: 14/08/2018	**Fecha de modificación:** 14/08/2018	**Fecha de aprobación:** 14/08/2018	**Identificador** **D-GER-02**
Elaborado por: Alvaro Vallejo		**Revisado y aprobado por:** Víctor Tolcachier	

I. INTRODUCCIÓN

Este documento permite conocer las políticas que se adoptarán para el buen manejo de los sistemas y operaciones de la empresa Leterago del Ecuador S.A.

II. POLÍTICAS

Las políticas que se adoptan en la empresa Leterago del Ecuador S.A involucran a: Gerencia de tecnología informática, Jefe de tecnología informática, Jefe de operaciones, asistentes de operaciones.

Gerencia de tecnología informática – Jefe de tecnología informática debe:

1. Aprobar un documento donde conste las políticas o normas del buen manejo de los sistemas y operaciones de la empresa, el mismo que será publicado y divulgado a jefes departamentales y asistentes de operaciones.
2. Establecer un documento con las políticas o normas del buen manejo de los sistemas y operaciones de la empresa Leterago del Ecuador S.A.
3. Colaborar de manera activa a las capacitaciones que sean necesarias para apoyar tanto a jefes departamentales como a los asistentes de operaciones en el manejo y funcionamiento de los diferentes módulos del Sistema Administrativo Comercial (SAC) para el buen manejo y desempeño de las operaciones de la organización que garantice la integridad de la información.

Documento 2: Documento para el buen manejo de sistemas y operaciones (Elaborado por: El investigador)

B. Documento para el buen manejo de sistemas y operaciones en la empresa

Documento de Políticas para el buen manejo de los Sistemas y Operaciones de la empresa
4. Planificar las capacitaciones con la colaboración del departamento humano para que pueda organizar le fecha, la hora el lugar y los asistentes a dicha capacitación. 5. Realizar un seguimiento de la información ingresada al sistema y según sea el caso contactar al jefe de operaciones para indicar alguna inconsistencia en la información o la forma de ingresar la información al sistema que tienen los asistentes de operaciones. 6. Notificar al personal mediante un correo electrónico (comunicación interna) acerca de un mantenimiento o actualización que se vaya a realizar al sistema SAC para garantizar la mejora continua del negocio. 7. Tener aprobada una documentación formal acerca del manejo, funcionamiento de los diferentes módulos que componen el sistema SAC. 8. Tener un ambiente de pruebas donde se pueda probar las nuevas actualizaciones del sistema SAC antes de ponerla en producción. 9. Garantizar el buen funcionamiento del sistema SAC después de cada actualización. **Jefe de operaciones debe:** 1. Encargado de velar por el correcto uso e ingreso de información al sistema SAC por parte de los asistentes de operaciones. 2. Notificar al Gerente de tecnología informática cuando alguna función o actualización que se haya hecho al sistema SAC no haya quedado claro en cuanto a su funcionamiento, para organizar una capacitación para su mejor comprensión. 3. Notificar al Gerente de tecnología informática de manera formal cualquier inconsistencia en el funcionamiento del sistema SAC que este dificultando el ingreso o consulta de información a los asistentes de operaciones.

Documento 2: Documento para el buen manejo de sistemas y operaciones (Elaborado por: El Investigador)

B. Documento para el buen manejo de sistemas y operaciones en la empresa

Documento de Políticas para el buen manejo de los Sistemas y Operaciones de la empresa
4. Mantener reuniones frecuentes con los asistentes de operaciones para notificar cualquier cambio o modificación en los procesos de ingreso de información en el sistema SAC. 5. Asignar permisos y funciones sobre los módulos a acceder cada usuario del sistema SAC así como también dar de baja a los mismos cuando estos hayan sido despedidos o se hayan cambiado a otro departamento. 6. Precautelar el buen uso que le den al perfil de usuario creado en el sistema SAC para que el personal no vaya a cometer errores de ingreso o modificación de información sin notificación previa para que de esta manera se mantenga la integridad de la información. 7. Realizar un seguimiento de los ingresos que realizan los asistentes de operaciones en el sistema SAC. 8. Sancionar a los usuarios que presten sus claves a personal de un departamento ajeno al departamento de operaciones. **Asistentes de operaciones debe:** 1. Encargado de realizar ingresos al sistema SAC sobre nuevas condiciones comerciales de los laboratorios asignados a cada uno de ellos. 2. Garantizar de que la información ingresada al sistema SAC sea aprobada antes por los laboratorios y Jefe de operaciones. 3. Garantizar la minimización de los errores de digitación de la información que ingresan al sistema SAC antes de dar de alta verificar que toda la información este correctamente ingresada. 4. Notificar al Jefe de tecnología informática de cualquier error de ingreso en el sistema SAC mediante la creación de un ticket detallando de la mejor manera que campo quiere modificar con su respectiva justificación del caso.

Documento 2: Documento para el buen manejo de sistemas y operaciones (Elaborado por: El Investigador)

C. Documento de políticas de seguridad informática

<table>
<tr><th colspan="4">Leterago Documento de políticas de Seguridad Informática</th></tr>
<tr><td>Fecha de emisión:
14/08/2018</td><td>Fecha de modificación:
14/08/2018</td><td>Fecha de aprobación:
14/08/2018</td><td>Identificador
L-GER-01</td></tr>
<tr><td colspan="2">Elaborado por: Alvaro Vallejo</td><td colspan="2">Revisado y aprobado por: Víctor Tolcachier</td></tr>
<tr><td colspan="4">

I. INTRODUCCIÓN

Este documento permite conocer las políticas de seguridad informática que se adoptarán en la empresa Leterago del Ecuador S.A.

II. POLÍTICAS

Las políticas que se adoptan en la empresa Leterago del Ecuador S.A involucran a: gerencia de tecnología informática, jefe de infraestructura de tecnología informática, especialista de tecnología informática, jefe de servicios generales, asistente contable.

Gerencia de tecnología informática debe:

1. Aprobar un documento donde conste las políticas o normas a seguir, el mismo será publicado y divulgado a gerentes, jefes departamentales, asistentes, demás personal administrativo y entidades externas relevantes.
2. Establecer un documento con las políticas de la seguridad informática aplicables al Centro de Datos de la empresa Leterago del Ecuador S.A.
3. Apoyar de manera activa la seguridad informática dentro del Centro de Datos de la empresa Leterago del Ecuador S.A mediante un acuerdo, reconociendo las responsabilidades que conlleva la seguridad de la información.
4. Aprobar las actividades de mantenimiento de los equipos del Centro de Datos de la empresa Leterago del Ecuador S.A.

</td></tr>
</table>

Documento 3: Políticas de seguridad de la información (Elaborado por: El Investigador)

C. Documento de políticas de seguridad informática

Documento de políticas de Seguridad Informática
5. Revisar la ejecución de las actividades planificadas en el Centro de Datos de la empresa Leterago del Ecuador S.A. 6. Aprobar a los proveedores que serán los encargados de brindar los servicios de mantenimiento, enlace, comunicaciones, control de incendios al Centro de Datos de la empresa Leterago del Ecuador S.A. 7. Designar al personal que se hará cargo de mantener la seguridad informática dentro y fuera del Centro de Datos. 8. Definir con claridad las responsabilidades de la seguridad de la información. 9. Respetar y hacer respetar las presentes políticas de seguridad informática para el Centro de Datos. 10. Contratar a un agente externo para que realice una auditoría interna del grado de madurez en que se encuentra la seguridad informática del Centro de Datos debidamente documentada y registrada para futuras auditorías. 11. Definir todos los requerimientos necesarios para poder mantener un buen grado de seguridad informática en el Centro de Datos. 12. Mantener la confidencialidad necesaria de las claves de administrador con las cuales se administran los servidores. **Jefe de infraestructura de tecnología informática debe:** 1. Coordinar con los proveedores para los mantenimientos de los equipos ya sean servidores, UPS, extintores de incendio, aire acondicionado, equipos de comunicaciones, red además de actualizar el firmware en los equipos para mejorar la funcionalidad y seguridad de los mismos. 2. Proteger los equipos de condiciones ambientales adversas y del acceso no autorizado. 3. Llevar una bitácora de control de los proveedores que visitan el Centro de Datos para los mantenimientos planificados. 4. Mantener siempre la puerta cerrada y controlar el acceso de personal no autorizado.

Documento 3: Políticas de seguridad de la información (Elaborado por: El Investigador)

C. Documento de políticas de seguridad informática

Documento de políticas de Seguridad Informática
5. Mantener un control de los mantenimientos del UPS para así evitar futuros mal funcionamientos del mismo y de esta manera evitar fallas eléctricas que pueden afectar el funcionamiento de los equipos informáticos y pérdida de información. 6. Proteger el cableado de energía y telecomunicaciones de daños o intercepciones. 7. Mantener claves de acceso a servidores con la confidencialidad que esto requiere. 8. Encargado de montar servidores nuevos y desmontar servidores que van hacer dados de baja. 9. Realizar mantenimientos, arreglos, formateo de servidores según sea requerido y además verificar que el software instalado tenga licencia de uso y sea exclusivamente para realizar las labores diarias, actualizar los sistemas fuera de horarios de oficina y probar su funcionamiento. 10. Instalar los parches y el antivirus a los servidores antes de ingresarlos al dominio. 11. Contactarse con el proveedor de comunicaciones en caso de haber problemas que afecten los servicios de la compañía. 12. Actualizar los planos de red cada vez que exista un cambio que haya sido previamente autorizado por la Gerencia de tecnología informática. 13. Velar por el buen funcionamiento de servicios de telecomunicaciones, red, sistemas que maneja la organización, equipos de red y de ser el caso reemplazarlos en caso de que tenga algún daño y protegerlos con una configuración segura que evite le intrusión en los equipos. 14. Gestionar la garantía de los equipos informáticos con el proveedor en caso de algún desperfecto en el hardware. 15. Ingresar los activos que componen el Centro de Datos al sistema de inventarios de tecnología informática y llevar un control de los mismos. 16. Llevar un control mediante una bitácora del backup diario de la información de los servidores.

Documento 3: Políticas de seguridad de la información (Elaborado por: El Investigador)

C. Documento de políticas de seguridad informática

Documento de políticas de Seguridad Informática
Asistente Contable debe: 1. Llevar un control de inventario de los equipos del Centro de Datos con el respectivo valor del activo, características del activo, custodio, etc. 2. Identificar los activos del Centro de Datos con una etiqueta de activo fijo que identifique en el sistema contable las características del mismo. **Jefe de servicios generales debe:** 1. Planificar la limpieza del Centro de Datos con el jefe de infraestructura de tecnología informática con la debida anticipación para no interrumpir trabajos o mantenimientos que estén en proceso. 2. Verificar cada 15 días que el aire acondicionado del Centro de Datos esté funcionando correctamente. 3. Planificar un mantenimiento del aire acondicionado del Centro de Datos cada 6 meses y llevar un control de la temperatura en una bitácora. 4. Revisar que el área del Centro de Datos cumpla con los requerimientos exigidos por el jefe de infraestructura de tecnología informática. **Especialista de tecnología informática debe:** **1.** Brindar ayuda y soporte al jefe de infraestructura de tecnología informática cuando lo requiera. **2.** Documentar todas las políticas, procesos, procedimientos y manuales de uso de los sistemas y equipos que componen el Centro de Datos. **3.** Llenar la bitácora de los backups realizados diariamente y dar parte al jefe de infraestructura de tecnología informática de las novedades encontradas en el proceso.

Documento 3: Políticas de seguridad de la información (Elaborado por: El Investigador)

D. Documento para uso aceptable de los activos informáticos

<table>
<tr><th colspan="4">Leterago Documento para uso aceptable de los Activos Informáticos</th></tr>
<tr><td>Fecha de emisión:
14/08/2018</td><td>Fecha de modificación:
14/08/2018</td><td>Fecha de aprobación:
14/08/2018</td><td>Identificador
L-GER-02</td></tr>
<tr><td colspan="2">Elaborado por: Alvaro Vallejo</td><td colspan="2">Revisado y aprobado por: Víctor Tolcachier</td></tr>
<tr><td colspan="4">

I. INTRODUCCIÓN

Este documento permite conocer las responsabilidades que tendrán el personal administrativo, gerencia de tecnología informática, jefe de infraestructura de tecnología informática de la empresa Leterago del Ecuador S.A.

II. POLÍTICAS

Las responsabilidades quedan distribuidas de la siguiente forma:
La empresa Leterago del Ecuador S.A requiere que los activos informáticos sean empleados de una manera aceptable, acorde a las exigencias del negocio.

LINEAMIENTO PARA USO DEL CORREO ELECTRÓNICO

- La empresa Leterago del Ecuador S.A deberá proveer el servicio de correo electrónico a toda persona que lo requiera para realizar sus labores diarias, previa solicitud del jefe inmediato del empleado mediante la creación de un ticket.
- Es responsabilidad de cada uno de los usuarios hacer buen uso de las cuentas de correo electrónico de la organización.
- No enviar ni contestar cadenas de correo electrónico que no tengan nada que ver con sus labores diarias.
- El uso de la cuenta es únicamente con fines laborales.

</td></tr>
</table>

Documento 4: Políticas para uso aceptable de activos (Elaborado por: El Investigador)

Documento para uso aceptable de los activos informáticos

Documento para uso aceptable de los Activos Informáticos
• Deben usar un lenguaje apropiado para la elaboración de correos. • Cambiar la contraseña cada trimestre o cada vez que el sistema lo solicite. • El usuario será el directamente responsable del tipo de información que envía mediante su cuenta de correo electrónico por lo cual se tiene que percatar de no enviar SPAMS, ni información confidencial de la empresa a direcciones ajenas a la organización a menos que sea autorizada por el jefe inmediato o que sean proveedores de la organización. • El usuario es el responsable de respaldar sus archivos de correo. **LINEAMIENTO DEL USO DEL INTERNET** • El internet será autorizado únicamente para realizar las siguientes actividades: **Para el personal administrativo:** El jefe de infraestructura de tecnología informática concederá acceso a los usuarios para que puedan trabajar únicamente en páginas de proveedores de la organización, para realizar consultas de temas de trabajo o con fines laborales. • Los asistentes de tecnología informática serán encargados de asignar un equipo de cómputo al usuario quien se hará responsable durante el tiempo que permanezca bajo su custodio. • Los asistentes de tecnología informática harán firmar un acta de entrega recepción a los usuarios que se les asignen un equipo informático. • Cualquier mala manipulación que provoque efectos adversos a las operaciones de la empresa Leterago del Ecuador S.A o ponga en riesgo la red de la compañía será analizado y dependiendo la gravedad de la situación será sancionado por la Gerencia de tecnología informática y autoridades pertinentes.

Documento 4: Políticas para uso aceptable de activos (Elaborado por: El Investigador)

D. Documento para uso aceptable de los activos informáticos

Documento para uso aceptable de los Activos Informáticos

LINEAMIENTO PARA USO DE EQUIPOS

- Cuando el personal se vea en la necesidad de sacar los equipos fuera de las instalaciones de Leterago del Ecuador S.A tendrá que tener autorización de la Gerencia de tecnología informática y Jefatura de tecnología informática y firmar un acta de salida de equipos.
- Los usuarios no pueden utilizar los equipos para tareas o asuntos personales.
- Cuando los usuarios saquen los equipos fuera de las instalaciones deben transportarlos de una manera confiable, cómoda y segura para así garantizar la devolución en óptimas condiciones del equipo a la empresa.

LINEAMIENTO PARA USO DE DOCUMENTOS

- En la empresa Leterago del Ecuador S.A existe documentación de las Normas de Gestión de Información, la misma que es manejada por la Especialista de tecnología informática para poder ser utilizada dentro de la organización.
- En caso de ser necesario sacar la documentación de manuales de funcionamiento de los sistemas del departamento de tecnología informática de Leterago del Ecuador S.A se debe contar con la autorización de la Gerencia de tecnología informática mediante un correo electrónico.

LINEAMIENTO PARA USO DE LA RED INALÁMBRICA

- La empresa Leterago del Ecuador S.A dispone de varias redes inalámbricas para lo cual deben solicitar el acceso al Jefe de tecnología informática o al Jefe de infraestructura de tecnología informática.
- Cada una de las redes inalámbricas tienen su propósito de uso y deben ser usadas para la finalidad por la cual fueron creadas.

Documento 4: Políticas para uso aceptable de activos (Elaborado por: El Investigador)

D. Documento para uso aceptable de los activos informáticos

Documento para uso aceptable de los Activos Informáticos
• La clave de acceso a cada una de las redes inalámbricas deberá estar bajo custodia del Jefe de infraestructura de tecnología informática. **LINEAMIENTO PARA CONTROL DE ACCESO A REDES** La red de la empresa Leterago del Ecuador S.A deberá ser administrada por el Jefe de infraestructura de tecnología informática por lo cual deberá hacer las siguientes funciones: • Creación de perfiles de usuarios. • Asignar los permisos correspondientes a cada usuario dependiendo de las funciones a desempeñar en la organización. • Compartir recursos de red (impresoras, carpetas o archivos, CD-ROM). • Bloqueo y desbloqueo de usuarios según sea el caso. • Reseteo de contraseñas a los usuarios. • Realizar un backup de todos los servidores de aplicaciones. • Revisar que el antivirus se encuentre actualizado en los servidores y equipos de cómputo. • Revisar constantemente los logs de los servidores para detectar posibles anomalías en el funcionamiento de los servicios. • Revisar los procesos activos y analizar que no afecten al resto de procesos que estén trabajando. • Controlar el uso de recursos. • Revisar regularmente los parches que se van a instalar en el sistema operativo del servidor. • Tener servidores de respaldo como medida de contingencia. • Realizar pruebas con regularidad del funcionamiento de los backups realizados.

Documento 4: Políticas para uso aceptable de activos (Elaborado por: El Investigador)

D. Documento para uso aceptable de los activos informáticos

Documento para uso aceptable de los Activos informáticos

LINEAMIENTO PARA USO DEL SOFTWARE

- Se deberá utilizar el software suministrado por el departamento de tecnología informática que se especifica a continuación:
- Sistema Operativo: Windows 10.
- Antivirus: McAfee.
- Microsoft Office 2016.
- Descomprimidor de archivos WINRAR.
- Navegadores: Internet Explorer, Mozilla Firefox, Google Chrome y Edge.
- Abode Acrobat Reader.
- Adobe Flash Player.
- Java Virtual Machine.
- Iso Manager.
- Sistema Administrativo Comercial (SAC).
- Software DIMM (Departamento Contable).
- Visio (Departamento de Control de Calidad).
- Y demás software que se instala de acuerdo a los requerimientos de cada departamento con la previa autorización del jefe de área.

LINEAMIENTO PARA REALIZACIÓN DE BACKUPS

- Respaldar las bases de datos que se generan diariamente en los horarios establecidos por la Gerencia de tecnología informática.
- Respaldar la información de las bases de datos en una unidad de disco externo que está conectada en el servidor y en cintas de servidor.
- Etiquetar a las cintas de los backups de acuerdo al día de la semana y almacenarlas en un lugar seguro y confiable.

Documento 4: Políticas para uso aceptable de activos (Elaborado por: El Investigador)

E. Documento de Reporte y Solución de Incidencias de seguridad informática

Leterago Documento de Reporte y Solución de Incidencias de seguridad informática			
Fecha de emisión: 14/08/2018	**Fecha de modificación:** 14/08/2018	**Fecha de aprobación:** 14/08/2018	**Identificador** **R-JEF-01**
Elaborado por: Alvaro Vallejo		**Revisado y aprobado por:** Víctor Tolcachier	

I. INTRODUCCIÓN

Este documento permite reportar las incidencias a los Responsables de la Seguridad Informática y las posibles soluciones a la incidencia.

II. REGISTRO

Nombre de la persona que reporta: .....

Fecha: .....

Incidente: .....

.....

.....

.....

.....

Solución de la incidencia: …….

…….

…….

Firma	Firma
_____	_____
Persona que reporta	Responsable de la seguridad de la información
Documento de identidad	Documento de identidad

Documento 5: Reporte de incidencias y soluciones (Elaborado por: El Investigador)

Propuesta para mitigar los riesgos encontrados en la empresa Leterago del Ecuador S.A.

Aplicaciones informáticas

- **Sistema SAC**

Tener un backup diario de las bases de los módulos que componen el Sistema Administrativo Comercial (**Ver Anexo 4 y Anexo 5**).

Probar la funcionalidad de los backups de las bases cada 15 días en caso de que se necesite una restauración de la base.

Tener un ambiente de pruebas para probar las funcionalidades de las actualizaciones del sistema antes de ponerlas en producción.

Aplicar las actualizaciones al Sistema SAC fuera de las horas laborales.

Tener un servidor como backup en caso de existir algún daño en el hardware o en el software que pueda dificultar el normal funcionamiento del Sistema SAC.

Adquirir los nuevos servidores con garantía extendida en caso de algún daño en los equipos.

Mantener a los servidores en un ambiente adecuado para el efecto y con una temperatura entre los 18°C y 22°C.

Revisar la temperatura del Centro de Datos regularmente y de igual manera el sistema de aire acondicionado para que pueda cumplir de forma eficaz su trabajo.

Tener un control de las transacciones ingresadas al Sistema SAC para que no perjudique el aspecto financiero del negocio.

Capacitar al personal nuevo de manera que los errores en el uso del Sistema SAC se minimicen.

Llevar un control de los logs de los usuarios que utilizan el Sistema SAC para poder detectar alguna anomalía en su comportamiento.

Garantizar que tanto software como hardware sea el adecuado para el correcto funcionamiento del servicio del Sistema SAC a los usuarios.

En caso de una caída del enlace el Jefe de infraestructura de tecnología informática debe comunicarse de inmediato con el proveedor del servicio para que pueda reestablecer el servicio lo más pronto posible para evitar la pérdida de ventas.

Manejar un contrato con el proveedor del enlace que estipule en caso de existir algún problema grave como es la interrupción del servicio tenga un tiempo estipulado o tiempo límite para poder reestablecer el servicio caso contrario multarle al proveedor de la forma que la organización crea conveniente.

- **Sistema NETORDER**

Revisar y documentar las actualizaciones que se realice al Sistema NetOrder para poder brindar un mejor servicio de soporte a los usuarios.

Capacitar de manera oportuna de las actualizaciones en las funciones del sistema NetOrder a los usuarios para evitar el mal uso de la herramienta de pedidos.

Revisar con regularidad los logs del Sistema NetOrder para poder verificar que los paquetes de actualizaciones hayan sido enviados exitosamente a los usuarios.

Realizar pruebas de funcionamiento de las actualizaciones antes de ponerlas en producción.

Revisar que la información que se cargue en el sistema NetOrder sea la correcta y que cumpla las exigencias de los laboratorios.

Adquirir un servidor que cumpla las exigencias para que el servicio del Sistema NetOrder no se vea afectado ni interrumpido bajo ningún concepto.

- **Sistema EVOLUTION**

Actualizar el sistema EVOLUTION con el archivo que es enviado por el proveedor exclusivamente.

Aplicar la actualización en un horario que no afecte el trabajo del personal de talento humano.

Comunicar al personal vía correo electrónico de la actualización que se va a realizar.

Realizar las pruebas pertinentes una vez se haya aplicado la actualización.

- **Sistema Operativo**

Revisar de forma regular los parches que se van a instalar en equipo.

Actualizar los parches del sistema operativo cada vez que se lo solicite.

Reiniciar el equipo cada vez que se termine de descargar las actualizaciones.

Mandar un correo de notificación a los usuarios para que no apaguen los equipos para que las actualizaciones del sistema operativo sean distribuidas a todos los equipos de la organización.

- **Herramienta de software**

Revisar las actualizaciones del software instalado en el equipo de forma regular ya que estas actualizaciones sirven como escudo de los ciberataques.

Instalar el software estrictamente necesario para que el usuario pueda trabajar.

Prohibido instalar un software no permitido o que no tenga nada que ver con las labores diarias del usuario.

Instalar software con la debida licencia de uso para poder aprovechar las actualizaciones que brinda el proveedor.

- **Antivirus**

Instalar el antivirus a todos los equipos que estén unidos en el dominio de trabajo.

Revisar las actualizaciones regularmente del antivirus.

Llevar un control de los equipos que tienen el antivirus instalado.

Dar seguimiento a los equipos que por varias circunstancias no se puede instalar el antivirus y de ser el caso pedir soporte al corporativo para poder solventar el inconveniente.

Desinstalar el antivirus a los equipos que sean sacados del dominio.

Redes de comunicación

- **Router Central**

Actualizar el firmware del equipo para evitar posibles ataques.

Restringir el acceso remoto al equipo.

Configurar el router WLAN mediante cable.

Cambiar la contraseña de acceso a la configuración del equipo y personalizarla, es decir cambiar la clave que viene de fábrica y poner una más segura con al menos 20 dígitos que pueden ser números o letras.

Personalizar el nombre de la red.

Configurar el equipo en una web segura (https).

- **Firewall**

Brindar un mantenimiento adecuado al firewall.

Tener un firewall de backup en caso de alguna contingencia.

Revisar las políticas a implantar en el firewall para evitar posibles ataques.

Reforzar las políticas de seguridad en el firewall para evitar un ciberataque.

- **Switches de Core**

Reforzar las contraseñas de usuario de los switches.

Tratar de mantener una jerarquía de red adecuada.

Mantener instalada la última versión del sistema operativo del equipo.

Configurar de manera adecuada los niveles de privilegio de los equipos (0 - 15).

Desactivar los servicios de red que no sean necesarios.

Asignar una VLAN exclusivamente para administración.

- **Servidores de Aplicaciones**

Mantener actualizado los parches de los servidores.

Usar contraseñas fuertes para administrar los servidores.

Cambiar las contraseñas regularmente o establecer una política de cambio de contraseñas trimestralmente.

Eliminar usuarios y grupos que ya no se utilicen.

Implementar la separación de privilegios en el servidor cuando los proveedores tengan que ingresar al servidor para poder dar soporte de sus aplicaciones para que tengan un control limitado del hardware para que únicamente puedan tener control de reparar, instalar el software a su cargo y que no afecte el normal funcionamiento del equipo.

Establecer los permisos de lectura y escritura adecuados sobre las carpetas y archivos que utilizan los usuarios para sus labores diarias según sea el caso para evitar la alteración de la información almacenada en el servidor.

Realizar un análisis de virus en el servidor de manera regular, en especial los archivos que son almacenados por los usuarios en las unidades de red.

Evitar la instalación de software de fuentes que no son confiables.

Proteger el acceso al servidor mediante un firewall.

Asegurarse de la ejecución del firewall.

Usar un sistema de detección de intrusos.

Realizar auditorías regularmente de los servidores y controlar los accesos a los mismos.

Realizar un análisis de vulnerabilidades del servidor de manera regular.

Realizar backups diarios de la información almacenada en el servidor.

Servicios

- **Servidor DNS**

Establecer que hosts están autorizados para realizar consultas en dicho servidor.

Establecer que hosts están autorizados para receptar las transferencias de dicho servidor.

Establecer que hosts están autorizados para realizar consultas recursivas de dicho servidor.

Establecer una lista de hosts que no están autorizados para receptar consultas ni para resolver consultas de dicho servidor.

Configurar el servidor web para evitar que la memoria cache sea contagiada por virus provenientes de sitios maliciosos que puedan ser reenviados a varios usuarios.

Configurar la directiva del Firewall para controlar los accesos al servidor DNS.

Configurar el servidor de una manera adecuada para evitar ataques y mantenerlo siempre actualizado.

- **Servidor DHCP**

Controlar que el personal no autorizado tenga prohibido el acceso físico e inalámbrico a la red de la organización.

Realizar una auditoría de los servidores DHCP que se encuentren en la red de la organización y revisar regularmente los registros y analizar si el servidor recibe solicitudes de concesión extrañamente altas.

Tener un control de acceso al Centro de Datos, revisar regularmente los ingresos del personal y el motivo por el cual están ingresando.

Tener instalado un antivirus y mantenerlo actualizado.

Instalar regularmente los parches de software o cada vez que el sistema operativo lo solicite.

Instalar software licenciado que brinde actualizaciones de seguridad constantes.

- **Servidor Base de Datos**

Tener un control del personal que puede ingresar a las diferentes bases de datos y el motivo por el cual tienen acceso a dichas bases.

Realizar backups diarios de la información almacenada en el servidor de base de datos.

Tener documentado los privilegios de acceso de cada usuario del servidor de base de datos de la organización.

Realizar reportes de la información que se extrae de la base de datos con la debida autorización de la Gerencia de tecnología informática.

Configurar la directiva del Firewall para controlar los accesos al servidor de base de datos.

- **Servidor Cámaras IP**

Tener instalado un software licenciado y especialmente para tipo de cámaras IP.

Tener identificado el modelo, tipo de cámara y a qué área de la organización pertenece cada equipo.

Tener protegida cada cámara IP con una clave distinta para poder visualizar las imágenes.

Tener activado una opción de grabación automática para poder tener registrado cualquier tipo de eventualidad que se suscite en las instalaciones.

Tener documentado las claves, modelos, tipos de equipos y el área que corresponden cada cámara IP y la forma de instalación.

- **Servidor telefonía IP**

Limitar la duración de las llamadas tras un periodo razonable de tiempo y de esta manera se evita que llamadas fraudulentas se realicen sin límite alguno.

Realizar un límite de gasto mensual por usuario y si se sobrepasa del límite la llamada se corta de manera automática.

Controlar el número de llamadas simultáneas por usuario.

Controlar los permisos de llamadas salientes por extensión.

Configurar las llamadas internacionales mediante una contraseña.

Equipamiento informático

- **Firewall**

Tener el firewall en un sitio cómodo y seguro fuera de temperaturas altas, goteras.

Realizar un mantenimiento preventivo del firewall.

Permitir únicamente las comunicaciones autorizadas.

Revisar periódicamente la configuración y políticas del firewall.

- **Equipos de cómputo**

Tener en un sitio alejado de cualquier filtración, humedad, temperaturas altas.

Tener instalado un antivirus y actualizarlo periódicamente.

Instalar los parches de seguridad cada vez que lo solicite.

Instalar software con licencia para tener las ventajas de actualizaciones periódicas.

- **Equipos portables**

Protegerlo de ambientes inadecuados (exponer al sol).

Llevar el equipo portable en su respectivo maletín.

Cuando sea transportado ubicar en un sitio no visible para los delincuentes.

Conectarse a la red periódicamente para que el antivirus y parches de seguridad se actualicen.

- **Switch administrable**

Configurar los equipos según requerimientos de la organización.

Revisar la configuración realizada a los equipos.

Asignarle una contraseña fuerte para poder administrar el equipo.

Verificar los accesos que se asignan en los equipos periódicamente.

Equipamiento auxiliar

- **Cableado de red**

Revisar costos y asignación formal de los proveedores.

Tener documentado la diagramación de la red y aprobada por la Gerencia de tecnología informática.

Proteger al cableado de red mediante tubos o canaletas que eviten cualquier tipo de daño o contacto.

Tendido adecuado del cableado de red respetando las normas establecidas para tal efecto.

Instalar el cableado de red en lugares que no puedan dañarlo o deteriorarlo.

- **Sistema de alimentación ininterrumpida**

Realizar mantenimientos con regularidad al UPS.

Llevar una bitácora de la fecha y hora del mantenimiento realizado, observaciones y responsable del trabajo realizado.

Reemplazar las baterías del UPS cuando sea necesario.

Las baterías usadas llevarlas a una organización especializada de su tratamiento.

Dar a conocer a los usuarios que el uso de la energía ininterrumpida es única y exclusivamente para conectar el monitor y CPU.

Evitar conectar otro tipo de dispositivos en él toma del UPS ya que podría causar inconvenientes eléctricos.

Revisar que todos los equipos se encuentren conectados en él toma del UPS.

Revisar que las tomas del UPS estén correctamente instaladas y de esta manera evitar cortocircuitos en los equipos y por ende pérdida de información (**Ver Anexo 2**).

Instalaciones

- **Gabinete de incendios**

Revisar que el gabinete de incendios se encuentre en lugares estratégicos para poder actuar de forma oportuna ante un riesgo de incendio.

Revisar que los extintores se encuentren cargados y funcionando.

Realizar un mantenimiento preventivo con el personal calificado.

- **Rack de servidores**

Revisar que los racks se encuentren en buenas condiciones (libre de óxido).

Verificar que el rack sea específicamente para soportar el peso de los equipos.

Revisar que los racks se encuentren perfectamente armados y ajustados.

Revisar que los racks estén lejos de cualquier humedad, goteras, etc.

Personal

- **Técnico administrativo**

Contrata personal calificado para que se responsabilice del Centro de Datos.

Tener conocimientos de infraestructura y telecomunicaciones.

Contar con la experiencia para administrar el Centro de Datos.

Realizar informes y auditorías constantes de los servidores: fecha de compra, garantías, soporte técnico del proveedor, estado del servidor, años de servicio del equipo, mantenimiento preventivo.

Respetar los horarios de trabajo y cumplirlos.

- **Técnico administrativo experto**

Revisar que tenga experiencia y tenga certificaciones del manejo de riesgos en el Centro de Datos.

Verificar que domine el manejo, configuración y ensamblaje de los equipos.

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Se analizó a profundidad los conceptos básicos referentes a la seguridad de la información.
- Gracias a las Normas ISO 27001, ISO 27002, ISO 27005 facilitará realizar el análisis de riesgos, amenazas y vulnerabilidades de los activos de información del Centro de Datos de la empresa Leterago del Ecuador S.A.
- Mediante la elaboración de la propuesta la organización tendrá una herramienta para disminuir los riesgos encontrados en el Centro de Datos a un nivel aceptable.
- La propuesta del Sistema de Gestión de Seguridad de la Información permitirá a la organización tomar medidas acertadas para combatir los riesgos de seguridad en el Centro de Datos.

4.2 Recomendaciones

- Realizar un análisis de la terminología que ha servido de base para realizar la propuesta del SGSI.
- Se recomienda revisar periódicamente el estado de los riesgos, amenazas y vulnerabilidades que afectan al Centro de Datos para poder evitar futuras pérdidas de información.
- Analizar diferentes alternativas para poder disminuir los riesgos del Centro de Datos de una manera acertada.
- Revisar la propuesta del SGSI y si es factible proponer nuevas vías de solución a los riesgos que puedan ocurrir en el Centro de Datos.

Referencias bibliográficas

Activos Concursales S.L. (17 de 12 de 2016). *Activos Concursales V2*. Obtenido de Activos Concursales V2: http://www.activosconcursales.com/iso-27001-seguridad-informacion/ [Consulta: 11 de junio de 2018]

Advisera. (2018). *Advisera*. Obtenido de Advisera: https://advisera.com/27001academy/es/que-es-iso-27001/ [Consulta: 12 de junio de 2018]

Alvaro. (2018). *PRESENTACION MANUEL COLLAZOS 1*. Obtenido de PRESENTACION MANUEL COLLAZOS 1: https://www.academia.edu/35348100/PRESENTACION_MANUEL_COLLAZOS_1?auto=download [Consulta: 18 de junio de 2018]

Amutio, A. (2013). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wwj6k4oh3IU [Consulta: 20 de junio de 2018]

AREITIO J, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Paraninfo.

Articulo 45 De Las Distribuidoras Farmacéuticas. (2012). *REGLAMENTO DE CONTROL Y FUNCIONAMIENTO DE LOS ESTABLECIMIENTOS FARMACÉUTICOS.* Obtenido de REGLAMENTO DE CONTROL Y FUNCIONAMIENTO DE LOS ESTABLECIMIENTOS FARMACÉUTICOS: https://www.controlsanitario.gob.ec/wp-content/uploads/downloads/2014/04/ESTABLECIMIENTOS-FARMACEUTICOS.pdf [Consulta: 25 de junio de 2018]

Calidad, A. E. (2017). *AEC*. Obtenido de AEC: https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion [Consulta: 26 de junio de 2018]

Colorado et al. (12 de 2015). *Revista Ingeniería Biomédica*. Obtenido de Revista Ingeniería Biomédica: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-97622015000200014 [Consulta: 14 de agosto de 2018]

Deloitte. (julio de 2016). *Cyber Risk & Information Security Study – Latinoamérica.* Obtenido de Cyber Risk & Information Security Study – Latinoamérica: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte%202016%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Latinoam%C3%A9rica%20-%20Resultados%20Generales%20vf%20(Per%C3%BA).pdf [Consulta: 9 de julio de 2018]

Deloitte. (2017). Seguridad de la Información en Ecuador. *Estudio 2017 Deloitte Ecuador*, 1-5.

Ekos, R. (09 de 08 de 2013). *Ekos Negocios*. Obtenido de Ekos Negocios: http://www.ekosnegocios.com/negocios/verArticuloContenido.aspx?idArt=2326 [Consulta: 15 de julio de 2018]

Excellence, I. (31 de 01 de 2014). *PMG SSI - ISO 27001*. Obtenido de PMG SSI - ISO 27001: https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/ [Consulta: 27 de junio de 2018]

Fernández, J. (10 de 2013). *Aprocal*. Obtenido de Aprocal: http://www.aprocal.org.mx/files/2200/03SeguridadenInformaticaV1.0.pdf [Consulta: 27 de junio de 2018]

Fernández, P. (2016). *GESTION.ORG*. Obtenido de GESTION.ORG: http://www.gestion.org/recursos-humanos/5936/organigrama-de-una-empresa/ [Consulta: 14 de agosto de 2018]

Garrido, J. (03 de 03 de 2014). *Clavei | Expertos en Transformación Digital*. Obtenido de Clavei | Expertos en Transformación Digital: https://www.clavei.es/blog/la-seguridad-informatica-en-las-organizaciones/ [Consulta: 19 de junio de 2018]

GESTION.ORG. (2018). *GESTION.ORG*. Obtenido de GESTION.ORG: https://www.gestion.org/organigrama-de-una-empresa/ [Consulta: 25 de junio de 2018]

Gitman, L. (2012). *Principios de Administración Financiera Décimo Segunda Edición.* México: PEARSON EDUCACIÓN.

Greenhouse, S. (2017). *Software Greenhouse*. Obtenido de Software Greenhouse: https://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio [Consulta: 22 de julio de 2018]

Informatica. (2018). Obtenido de Informatica: https://www.informatica.com/ec/products/data-security.html [Consulta: 22 de julio de 2018]

ISACA. (2014). *La función de seguridad de la información.* Obtenido de La función de seguridad de la información.: https://www.isaca.org/Journal/archives/2014/Volume-6/Documents/The-Information-Security-Function_joa_Spa_1114.pdf [Consulta: 22 de julio de 2018]

ISO.ORG. (2011). *ISO - International Organization for Standardization*. Obtenido de ISO - International Organization for Standardization: https://www.iso.org [Consulta: 05 de junio de 2018]

ISO27000. (10 de 02 de 2014). *Sistema de Gestión de Seguridad de la Información (SGSI).* Obtenido de Sistema de Gestión de Seguridad de la Información (SGSI): http://www.iso27000.es/download/doc_sgsi_all.pdf [Consulta: 05 de junio de 2018]

ISO27005. (2009). Normas ISO 27005. Colombia.

Legislación para el cumplimiento del reglamento de seguridad y salud. (s.f.). Obtenido de Reglamento de Seguridad y Salud de los Trabajadores: http://www.higieneindustrialyambiente.com/reglamentos-seguridad-salud-planes-de-emergencia [Consulta: 03 de junio de 2018]

López, A. (2010). *Seguridad informática.* Editex.

MAGERIT. (09 de 06 de 2013). GESTIÓN DEL RIESGO. *CAPÍTULO III GESTIÓN DEL RIESGO*.

Mendoza, M. (29 de Septiembre de 2014). *Welivesecurity*. Obtenido de Welivesecurity: https://www.welivesecurity.com/la-es/2014/09/29/8-pasos-evaluacion-de-riesgos-1/ [Consulta: 25 de julio de 2018]

Mendoza, M. A. (29 de Septiembre de 2014). *Welivesecurity*. Obtenido de Welivesecurity: https://www.welivesecurity.com/la-es/2014/09/29/8-pasos-evaluacion-de-riesgos-1/ [Consulta: 25 de julio de 2018]

Mendoza, M. Á. (23 de 03 de 2015). *welivesecurity*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2015/03/23/evaluacion-de-riesgos-cualitativa-o-cuantitativa/ [Consulta: 25 de julio de 2018]

Meyer, I. C. (03 de 2014). *Normas seguridad 2014* . Obtenido de Normas seguridad 2014 : http://www.criptored.upm.es/descarga/normas_segu_info_marzo_2014.pdf [Consulta: 27 de julio de 2018]

Sosa, J. (27 de 01 de 2012). *Análisis de Riesgos* . Obtenido de Análisis de Riesgos : http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf [Consulta: 28 de julio de 2018]

SSI, P. (30 de 03 de 2015). *PMG SSI - ISO 27001*. Obtenido de PMG SSI - ISO 27001: https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/ [Consulta: 28 de julio de 2018]

Telefónica, F. (2016). *CIBERSEGURIDAD, LA PROTECCIÓN DE LA INFORMACIÓN EN UN MUNDO DIGITAL*. España: Ariel.

Valle, R. R. (1986). *Tecnologías de la información: electrónica, informática y telecomunicaciones.* Madrid: Fundamentos y función de la ingeniería.

Vieites, Á. G. (2011). *Enciclopedia de la Seguridad Informática. 2ª edición.* Grupo Editorial RA-MA.

Villamizar, C. (30 de 08 de 2013). *Magazcitum*. Obtenido de Magazcitum: http://www.magazcitum.com.mx/?p=2361#.Wu-8j38h3IU [Consulta: 02 de julio de 2018]

Vistazo. (2017). Revista Vistazo. *Vistazo*, pp 140.

Glosario de términos

Sistema SAC: Sistema Administrativo Comercial, consta de varios módulos con los cuales trabajan los usuarios de la empresa Leterago del Ecuador S.A.

Sistema NetOrder: Sistema de pedidos con los cuales se realiza la toma de pedidos a los clientes (Farmacias, Distribuidoras, Cadenas de Farmacias, etc.)

Sistema Evolution: Sistema dedicado para el manejo de nómina de la empresa Leterago del Ecuador S.A, donde se calcula sueldo, vacaciones, bonificaciones de ley.

Seguridad de la información: el concepto de seguridad de la información ha venido evolucionando con el tiempo. Así fue como la Seguridad de la Información fue pasando de lo técnico a la gestión y de aquí a la institucionalización bajo normas universales, para actualmente fortalecer la toma de conciencia que la seguridad es parte de los negocios, puesto que la información es un activo corporativo crítico para mantener sustentables las operaciones, entroncándose así en el paradigma del Corporate Governance. (Meyer, 2014)

ANEXOS

Anexo 1: Encuesta dirigida al Jefe de infraestructura de tecnología informática referente a la seguridad informática en la organización

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE INGENIERÍA EN SISTEMAS INFORMÁTICOS

ENCUESTA DIRIGIDA AL JEFE DE INFRAESTRUCTURA DE TECNOLOGÍA INFORMÁTICA DE LA EMPRESA LETERAGO DEL ECUADOR S.A

Objetivo: Conocer el estado de la seguridad de la informática en la empresa Leterago del Ecuador S.A.

Instructivo:

Puntos a tomar en cuenta.

*** Respuesta:** Describir brevemente la situación actual de la organización en relación al aspecto evaluado.

*** Responsable:** Nombre del responsable que ha realizado la evaluación.

*** Fecha:** Fecha en la que se realizó la evaluación.

SEGURIDAD DE LA INFORMACIÓN

1.- Actualmente la empresa cuenta con una valoración de sus activos informáticos?

Respuesta:

Responsable:

Fecha:

2.- La empresa ha tenido algún riesgo de robo de información que comprometa el negocio?

Respuesta:

Responsable:

Fecha:

3.- Se ha dado a conocer a los usuarios alguna política de seguridad de la información, incluyendo beneficios y riesgos que puede ocurrir?

Respuesta:

Responsable:

Fecha:

4.- Se monitorea periódicamente los procedimientos y operaciones de la empresa de forma tal que las políticas de seguridad de la empresa puedan actualizarse de forma oportuna?

Respuesta:

Responsable:

Fecha:

5.- La empresa cuenta con alguna política de seguridad de la información?

Respuesta:

Responsable:

Fecha:

6.- La alta gerencia está seguro que los usuarios comprenden los asuntos importantes de la seguridad de la información?

Respuesta:

Responsable:

Fecha:

7.- Las políticas de seguridad están sujetas a las estrategias del negocio?

Respuesta:

Responsable:

Fecha:

8.- ¿Se han implantado perímetros de seguridad (paredes, puestos de recepción, entradas controladas por tarjeta) para proteger las áreas de acceso restringido?

Respuesta:

Responsable:

Fecha:

9.- ¿Las copias se seguridad se realizan regularmente de acuerdo con la política de backup establecida?

Respuesta:

Responsable:

Fecha:

10.- ¿Se verifica regularmente la correcta realización de las copias se seguridad?

Respuesta:

Responsable:

Fecha:

11.- ¿Se registran las actividades de los administradores y operadores de sistema?

Respuesta:

Responsable:

Fecha:

12.- ¿Se ha definido una política de asignación de privacidad para la asignación y uso de privilegios en el sistema?

Respuesta:

Responsable:

Fecha:

13.- ¿Los usuarios se aseguran de proteger los equipos desatendidos? (Ej. bloqueando o cerrando la sesión?

Respuesta:

Responsable:

Fecha:

14.- ¿Se controla la instalación de software en sistemas en producción?

Respuesta:

Responsable:

Fecha:

15.- ¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?

Respuesta:

Responsable:

Fecha:

16.- ¿Se ha desarrollado un proceso de gestión para la continuidad del negocio?

Respuesta:

Responsable:

Fecha:

17.- ¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?

Respuesta:

Responsable:

Fecha:

18.- ¿Se han establecido e implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?

Respuesta:

Responsable:

Fecha:

Anexo 2: Fotografías de Amenazas

Susceptibilidad al polvo

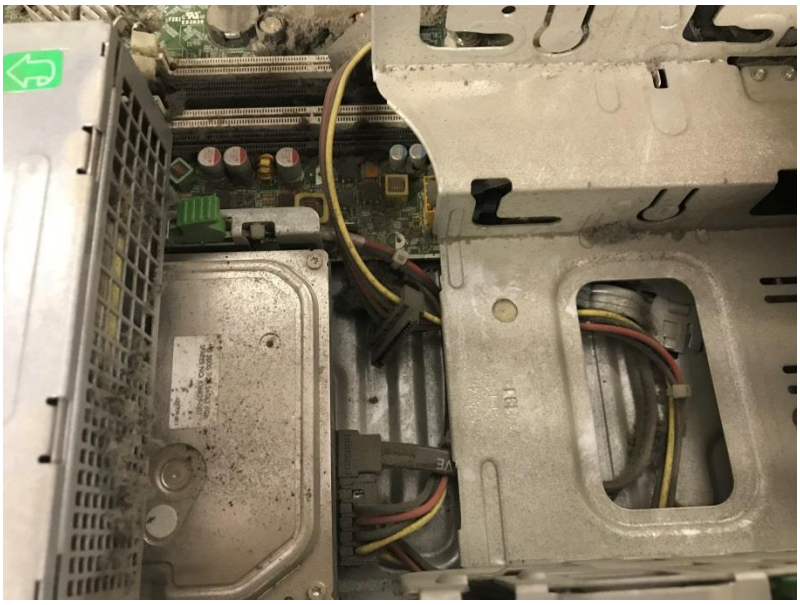


Figura. A.1. Fotografía de equipos sin protección para el polvo
Fuente: Investigación propia

Susceptibilidad a la suciedad

Figura. A.2. Fotografía donde se evidencia polvo y basura en los equipos
Fuente: Investigación propia

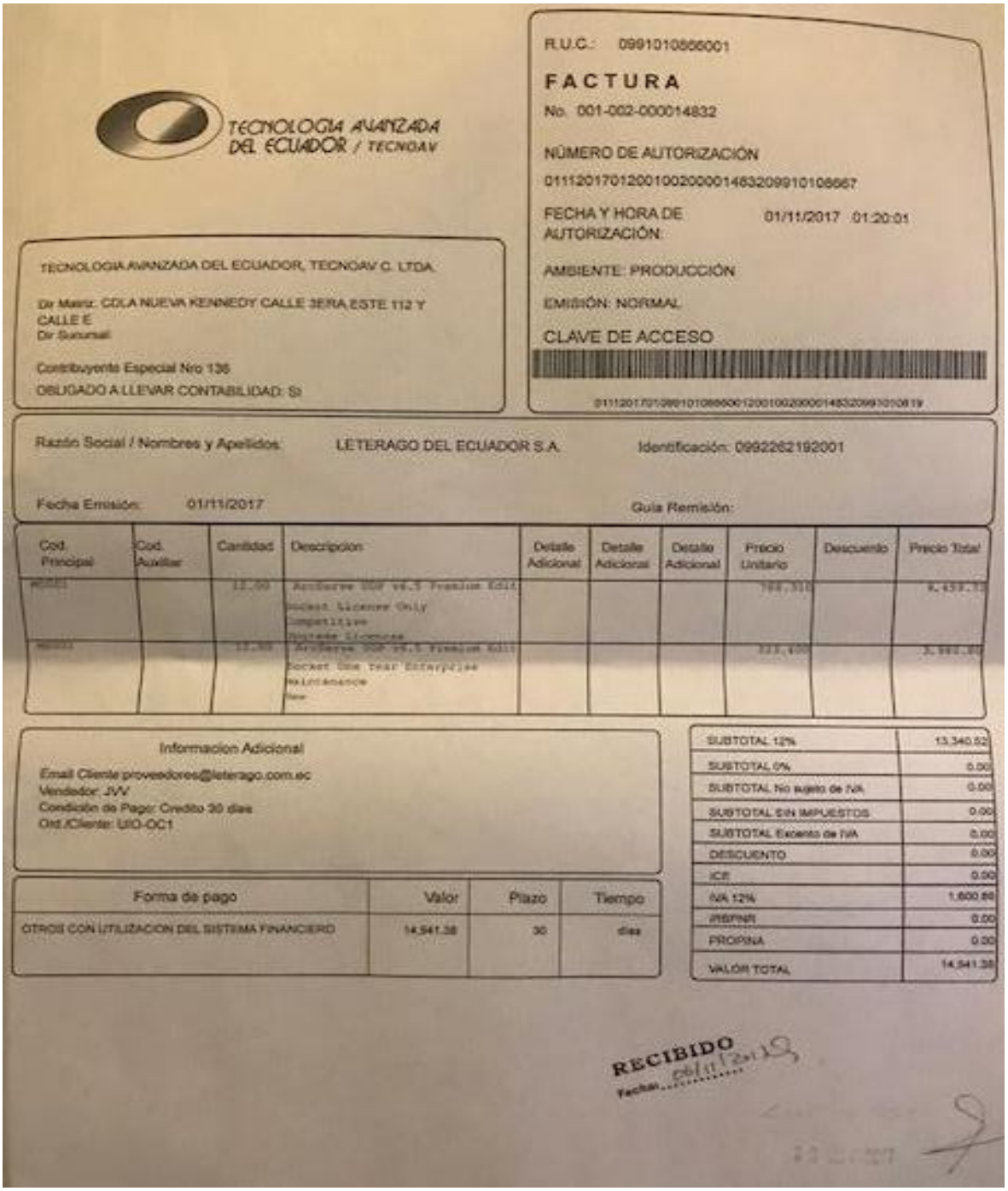
Instalaciones eléctricas

Figura. A.3. Fotografía donde se evidencia que los cables eléctricos están sin protección
Fuente: Investigación propia

Anexo 3: Fotografía de socialización con la Especialista de tecnología informática

Figura. A.4. Fotografía donde se evidencia el trabajo del SGSI
Fuente: Investigación propia

Anexo 4: Factura de adquisición de licencias de software para realizar backups de los servidores



TECNOLOGIA AVANZADA DEL ECUADOR / TECNOAV

R.U.C.: 0991010866001

FACTURA

No. 001-002-000014832

NÚMERO DE AUTORIZACIÓN

0111201701200100200000146320991010866 7

FECHA Y HORA DE AUTORIZACIÓN: 01/11/2017 01:20:01

AMBIENTE: PRODUCCIÓN

EMISIÓN: NORMAL

CLAVE DE ACCESO

TECNOLOGIA AVANZADA DEL ECUADOR, TECNOAV C. LTDA.

Dir Matriz: CDLA NUEVA KENNEDY CALLE 3ERA ESTE 112 Y CALLE E

Dir Sucursal:

Contribuyente Especial Nro 136

OBLIGADO A LLEVAR CONTABILIDAD: SI

Razón Social / Nombres y Apellidos: LETERAGO DEL ECUADOR S.A. Identificación: 0992262192001

Fecha Emisión: 01/11/2017 Guia Remisión:

Cod. Principal	Cod. Auxiliar	Cantidad	Descripcion	Detalle Adicional	Detalle Adicional	Detalle Adicional	Precio Unitario	Descuento	Precio Total
[illegible]		12.00	Acronis [illegible] Socket License Only Competitive Upgrade Licenses				[illegible]		[illegible]
[illegible]		12.00	Acronis [illegible] Socket One Year Enterprise Maintenance New				[illegible]		[illegible]

Informacion Adicional

Email Cliente proveedores@leterago.com.ec
Vendedor: JVV
Condición de Pago: Credito 30 dias
Ord./Cliente: UIO-OC1

Forma de pago	Valor	Plazo	Tiempo
OTROS CON UTILIZACION DEL SISTEMA FINANCIERO	14,541.38	30	dias

SUBTOTAL 12%	13,340.52
SUBTOTAL 0%	0.00
SUBTOTAL No sujeto de IVA	0.00
SUBTOTAL SIN IMPUESTOS	0.00
SUBTOTAL Exento de IVA	0.00
DESCUENTO	0.00
ICE	0.00
IVA 12%	1,600.86
IRBPNR	0.00
PROPINA	0.00
VALOR TOTAL	14,541.38

RECIBIDO

Fecha 06/11/2017

Anexo 5: Factura de adquisición de equipos para realizar backup de información del Centro de Datos

COMPSESA

COMPUTADORA SAN EDUARDO S.A

Dir Matriz	Cdla. Adace Primer Pasaje Mz 25 Solar 5 y Abel Romeo Castillo
Dir Sucursal	Eloy Alfaro 2013 y Suiza, Edificio Suiza Oficina B
Obligado a llevar Contabilidad	SI

R.U.C.: 0990347506001

FACTURA

No. 002-001-000021477

NUMERO DE AUTORIZACION:

1306201701200200100002147709903475064

FECHA Y HORA DE AUTORIZACION:	2017-06-13T10:40:40-05:00
AMBIENTE:	Producción
EMISION:	Normal

CLAVE DE ACCESO

1306201701099034750600120020010000214779999999911

Razón Social/Nombre Completo: LETERAGO DEL ECUADOR S.A.

Fecha Emisión: 13/06/2017 **R.U.C/C.I.:** 0992262192001 **Guía Remisión:**

Cod.Principal	Descripcion	Cant.	Precio Unitario	Descto	Precio Total
EQUIP-MIGRA	EQUIPAMIENTO PARA MIGRACION DE DOMINIO	1.00	8800.00	0.00	8800.00
EQUIP-RESP-DATA	EQUIPAMIENTO PARA SISTEMAS DE RESPALDO DATA CENTER	1.00	20378.00	0.00	20378.00
EQUIP-RESP-POMASQUI	EQUIPAMIENTO PARA SISTEMA DE RESPALDO POMASQUI	1.00	15845.00	0.00	15845.00
EQUIP-CLUST-VIRT-POMASQUI	EQUIPAMIENTO CLUSTER DE VIRTUALIZACION POMASQUI	1.00	22780.00	0.00	22780.00

INFORMACION ADICIONAL

formaPago	OTROS UTIL SISTEMA FINANCIERO (Valor 75939.36)
plazo	CREDITO 30 DIAS
Dir.Cliente	Av. Manuel Cordova Galarza Km 7 1/2frente al Colegio Frances - Quito
OrdenCompra	UIO-OC1 - 5.072/0

SUBTOTAL 12%	67803.00
SUBTOTAL 0%	0.00
SUBTOTAL No objeto de IVA	0.00
SUBTOTAL Exento de IVA	0.00
SUBTOTAL SIN IMPUESTOS	67803.00
TOTAL Descuento	0.00
IVA 12%	8136.36
VALOR TOTAL	75939.36

Anexo 6: Encuesta de la seguridad de la información

PREGUNTAS	RESPUESTAS (Si /No /Tal vez)		
	Especialista de Tecnología Informática	Jefe de Infraestructura	Asistente de Tecnología Informática
Estado de la seguridad de la información			
1.- Existe documentos de políticas de seguridad de la información en la	Si	Si	Tal vez
2.- Existe alguna normativa relacionada a los sistemas de información?	No	No	No
3.- Existe procedimientos relacionada a los sistemas de información?	Si	Si	Tal vez
4.- Existen responsables y/o controles para validar las políticas de seguridad?	No	No	No
5.- Existen formas para dar a conocer a los usuarios de dichas normas?	Si	Si	Si
6.- Existe algún tipo de control para verificar la validez de dichas políticas?	Si	Si	Tal vez
Organización de la información			
7.- Existen roles o responsabilidades definidas para el personal encargado de la seguridad de la información?	No	No	Tal vez
8.- Existen condiciones contractuales de seguridad con terceras personas y	Si	Si	Tal vez
9.- Existen programas que ayuden a la formación en seguridad para los empleados?	No	No	No
10.- Se revisa el tema de la seguridad de la información de la organización con	No	No	No
Control de activos			
11.- Existe un inventario de activos de T.I actualizado?	Si	Si	Si
12.- En el inventario consta el software, equipos y activos de datos?	No	No	No
13.- Existe procedimientos relacionada a los sistemas de información?	Si	Si	Tal vez
14.- Existe un responsable a cargo de los activos?	Si	Si	Si
15.- Existen normas y/o procedimientos para clasificar la información?	No	No	No
Recursos humanos			
16.- Se tiene definidas responsabilidades y/o roles de la seguridad informática?	No	No	No
17.- Se tiene en consideración la seguridad de la información cuando se selecciona y se da de baja al personal?	Si	Si	Si

Anexo 6: Encuesta de la seguridad de la información

PREGUNTAS	RESPUESTAS (Si /No /Tal vez)		
	Especialista de Tecnología Informática	Jefe de Infraestructura	Asistente de Tecnología Informática
18.- En los contratos a los empleados se estipula las condiciones de	Si	Si	Tal vez
19.- Se capacita a los empleados acerca del tratamiento de los activos?	No	No	No
20.- Existe algún procedimiento aplicable en caso de un incidente de seguridad?	No	No	No
Seguridad física y del ambiente			
21.- Existen controles de acceso a las áreas restringidas para el personal no autorizado?	Si	Si	Si
22.-En áreas seguras existe algún control para el personal autorizado y ajeno?	Si	Si	Si
23.-Los equipos se encuentran en sitios seguros fuera de cualquier riesgo?	Si	Si	Si
24.- Existe seguridades frente a complicaciones con la alimentación	Si	Si	Si
25.- Existe seguridad del cableado del Centro de Datos frente a posibles daños o	Si	Si	Si
Gestión de operaciones y comunicaciones			
26.- Los procesos operativos se encuentran definidos en la documentación	No	No	Tal vez
27.-Existe personal responsable de asegurar una reacción rápida y efectiva	No	No	No
28.-Existe alguna forma para reducir el uso erróneo de los sistemas de	No	No	Tal vez
29.- Existe empresas externas encargadas de la gestión de los sistemas de información?	No	No	No
30.- Existe algún control para evitar el software malicioso?	Si	Si	Si
Control de accesos			
31.- Existe alguna norma o política para el control de acceso?	Si	Si	Si
32.-Existe una norma o procedimiento de registro y quitar accesos?	Si	Si	Tal vez
33.-Se controla el uso de privilegios a los usuarios?	Si	Si	Si
34.- Existe una política para el manejo de contraseñas a los usuarios?	Si	Si	Si