UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

AUDITORÍA INFORMÁTICA APLICANDO LA NORMA ISO 27001 PARA OPTIMIZAR LA SEGURIDAD DE LA INFORMACIÓN EN EL DEPARTAMENTO DE TIC's DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO FAE.

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

ÁREA: Administrativas informáticas

LÍNEA DE INVESTIGACIÓN: Sistemas administradores de recursos

AUTOR: Remigio Leonel Chagmana Pomaquero

TUTOR: Ing. Franklin Oswaldo Mayorga Mayorga Mg.

Ambato - Ecuador

julio – 2022

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: AUDITORÍA INFORMÁTICA APLICANDO LA NORMA ISO 27001 PARA OPTIMIZAR LA SEGURIDAD DE LA INFORMACIÓN EN EL DEPARTAMENTO DE TIC's DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO FAE, desarrollado bajo la modalidad Proyecto de Investigación por el señor Remigio Leonel Chagmana Pomaquero, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, julio 2022.

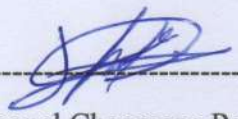
Firmado electrónicamente por:
FRANKLIN OSWALDO MAYORGA MAYORGA

Ing. Franklin Oswaldo Mayorga Mayorga, Mg.
TUTOR

AUTORÍA

El presente trabajo de investigación titulado AUDITORÍA INFORMÁTICA APLICANDO LA NORMA ISO 27001 PARA OPTIMIZAR LA SEGURIDAD DE LA INFORMACIÓN EN EL DEPARTAMENTO DE TIC's DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO FAE, es absolutamente original, autentico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor

Ambato, julio de 2022.



Remigio Leonel Chagmana Pomaquero

CC: 1803825056

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Remigio Leonel Chagmana Pomaquero, estudiante de la Carrera de ingeniería en Sistemas Computacionales e informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado AUDITORÍA INFORMÁTICA APLICANDO LA NORMA ISO 27001 PARA OPTIMIZAR LA SEGURIDAD DE LA INFORMACIÓN EN EL DEPARTAMENTO DE TIC's DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO FAE, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, julio 2022.

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Pilar Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
VICTOR HUGO GUACHIMBOSA VILLALBA

PhD. Víctor Guachimbosa
PROFESOR CALIFICADOR

Firmado electrónicamente por:
CARLOS ISRAEL NUNEZ MIRANDA

Ing. Carlos Nuñez, Mg
PROFESOR CALIFICADOR

DERECHOS DE AUTOR

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

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, julio 2022.

Remigio Leonel Chagmana Pomaquero

CC: 1803825056

AUTOR

DEDICATORIA

El presente trabajo lo dedico en primer lugar a Dios, quien me brindó sabiduría y tenacidad a lo largo de mi carrera universitaria.

En segundo lugar, a mi familia ya que con amor, paciencia y fortaleza guiaron cada momento de mi vida, siendo los pilares fundamentales en mi formación tanto personal como académica.

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, quien con su guía y bendición llena siempre mi vida.

A toda mi familia quien me ha apoyado incondicionalmente, pese a las adversidades e inconvenientes que se presentaron a lo largo del camino.

También quiero agradecer a mis docentes por compartir su conocimiento, sabiduría, apoyo y experiencias laborales para ser un mejor profesional en la vida diaria.

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

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

En la Actualidad la información es uno de los activos más importantes dentro de toda organización, su seguridad y administración requieren de un análisis exhaustivo para identificar cualquier riesgo al que se encuentra expuesto para que de esta manera se garantice la integridad, confidencialidad y disponibilidad de la información de forma óptima.

El proyecto de Investigación tiene como finalidad minimizar riesgos y brindar seguridad a la información que se maneja diariamente en el Departamento de TIC's del Centro de Investigación y Desarrollo FAE, a través de la aplicación de políticas de seguridad de la información que se basan en la norma ISO 27001.

Primeramente, se realizó un análisis del estado actual de seguridad en el Departamento de TIC's mediante la aplicación de entrevistas y encuestas, las cuales fueron aplicadas al Jefe y a los empleados del Departamento mencionado.

La metodología utilizada se basó en el ciclo de Deming que está constituida por 4 fases (Planear, Implementar, Verificar y Actuar), en la que cada fase constituye actividades que permiten planificar, determinar su alcance, realizar un inventario de los activos de información y la valoración de los activos con el objetivo de determinar y analizar los riesgos, amenazas y vulnerabilidades que intervienen en la gestión de la seguridad de la información.

Después, se procedió a la elaboración de un Plan de Seguridad de la Información en el cual se definirán el Alcance, Caracterización, Análisis de Riesgos y la Creación de nuevas Políticas de Seguridad de la Información para su aprobación y aplicación en el Departamento de TIC's en el Centro de Investigación y Desarrollo FAE, con ello se espera que el Jefe y los empleados del Departamento den cumplimiento a las políticas establecidas para garantizar un control adecuado en las áreas en donde existan falencias en cuanto a seguridad de la información se refiere, manteniendo seguimientos constantes en las áreas correspondientes.

Palabras Clave: Integridad, confidencialidad, disponibilidad, riesgos, ISO 27001

ABSTRACT

At present, information is one of the most important assets within any organization, its security and administration require a complete analysis to identify any risk to which it is exposed so that in this way the integrity, confidentiality and availability of the information is guaranteed. information optimally.

The purpose of the research project is to minimize risks and provide security to the information that is handled daily in the ICT Department of the FAE Research and Development Center, through the application of information security policies that are based on the standard ISO27001.

First, an analysis of the current state of security in the ICT Department was carried out through the application of interviews and surveys, which were applied to the Chief and the employees of the aforementioned Department.

The methodology used was based on the Deming cycle, which is made up of 4 phases (Plan, Implement, Verify and Act), in which each phase constitutes activities that allow planning, determining its scope, making an inventory of information assets and the valuation of assets with the aim of determining and analyzing the risks, threats and vulnerabilities that intervene in the management of information security.

Afterwards, an Information Security Plan was prepared in which the Scope, Characterization, Risk Analysis and the Creation of new Information Security Policies will be defined for approval and application in the ICT Department on FAE Research and Development Center, with this it is expected that the Head and employees of the Department comply with the policies established to guarantee adequate control in the areas where there are shortcomings in terms of information security, maintain constant monitoring in the corresponding areas.

Keywords: Integrity, confidentiality, availability, risks, ISO 27001

.

CAPÍTULO I.- MARCO TEÓRICO

1.1 Tema

AUDITORÍA INFORMÁTICA APLICANDO LA NORMA ISO 27001 PARA OPTIMIZAR LA SEGURIDAD DE LA INFORMACIÓN EN EL DEPARTAMENTO DE TIC's DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO FAE.

1.1.1 Planteamiento del Problema

Las organizaciones utilizan la tecnología como medio para procesar, almacenar y resguardar su información, aún más en tiempo de pandemia; la tecnología está jugando un rol fundamental dentro del funcionamiento de sus procesos, pero que, a la vez, estos están sometidos a un elevado número de riesgos y amenazas informáticas [1].

Toda organización está expuesta cada vez más a amenazas y es vulnerable a cualquier ataque informático; es decir, la variedad de amenazas en contra de sus activos puede causar la pérdida, manipulación o la no disponibilidad de la información. Paralelamente, pueden ocasionar cuantiosas pérdidas económicas, tal como dicen Wiley et al. (2020), el Foro Económico Mundial, en 2018, reportó que el 65 % de organizaciones australianas fueron víctimas de ataques, una de cada diez sufrió pérdidas superiores a $ 1 millón [1].

La mayoría de los robos o pérdidas de información en Latinoamérica recaen sobre el sector empresarial, pues Aguilar-Antonio (2019) explica que estos incidentes se deben a las insuficientes medidas de protección, lo que causa pérdidas de productividad, credibilidad, competitividad y perjuicios financieros que comprometen la continuidad de la organización. El uso de políticas basadas en la ISO 27001 mejoran la gestión de la seguridad de la información, pues como argumentan Angulo et al. (2018), ayudan a controlar los procesos de seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información.

Por ejemplo, tras el diseño e implantación de un modelo de políticas en las empresas proveedoras de internet en Ecuador se mostró mejoras significativas. Por esta razón, Cueva y Alvarado (2017) señalan que las organizaciones han adoptado nuevas formas de protección de sus activos de información [1].

En Ecuador en los últimos 5 años las Pymes han crecido significativamente en su cartera de inversión y producción generando más el empleo, pero en la parte de seguridad informática se están aislando del progreso y está obteniendo perdidas por los ataque dañinos causados por phishing o malware, no implementan métodos eficaz de detección temprana, no le dan importancia y porque creen que invertir en ciberseguridad es un gasto innecesarios, así mismo no invierten en capacitación de su personal, no adquieren paquetes de programa informático de protección [2].

Las TI y su seguridad dentro de las compañías si estas son fundamentales es decir el pilar del factor socioeconómico, a pesar que ciertos microempresarios lo ven como una causa amenazante por avance tecnológico otros creen que van a reemplazar la mano de obra existente reduciendo el componente productivo, lo menos optimistas ven que no podrán utilizar estas herramientas ya que los habitantes jóvenes han migrado a las grandes ciudades dejando estas Pymes (agrícolas) en total abandono y sería en vano automatizar su microempresa [2].

Las Cooperativas de Ahorro y Crédito, son instituciones de carácter financiero y sus servicios se enfocan básicamente en satisfacer las necesidades económicas a nivel empresarial o personal. Por lo que contar con un Balanced ScoreCard (Cuadro de Mando Integral) para la toma de decisiones en cuanto a Seguridad de información es muy importante, esto permitirá enfocar la inversión anual en los activos que muestren mayor riesgo y sean parte de los procesos más importantes [3].

Actualmente el Centro de Investigación y Desarrollo FAE no cuenta con ningún estándar implementado, únicamente toma ciertas medidas preventivas las cuales no garantizan la correcta gestión y seguridad de la información, por lo que personas o entidades mal

intencionadas podrían tener acceso a dicha información confidencial que se manejan internamente y hacer uso inadecuado de los mismos.

1.2 Antecedentes Investigativos

Según Oscar Gabriel Muñoz Pinto en el año 2017, en su trabajo titulado "Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001, en el Departamento de Tecnologías de la Información en la Cooperativa de Ahorro y Crédito indígena SAC", investigó los siguientes temas, y llegó a las siguientes conclusiones importantes: La Norma ISO/IEC 27001, lo que se busca es mejorar y/o garantizar dicha información, a través del Sistema de Gestión de la Seguridad de la Información (SGSI), aplicando cada una de las políticas de seguridad, como la gestión de activos, controles de acceso, seguridad física, etc. Dentro de cada uno de los dominios que la norma dicta, los cuales fueron analizados detalladamente [4].

Según Naranjo Camacho, Jefferson Mesías en el año 2019 en su trabajo titulado "Auditoría Informática dirigida al Centro de Cómputo de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil con base en las Normas ISO 27001 Y 27002" investigó los siguientes temas, y llego a las siguientes conclusiones importantes: La auditoría informática está basada en evaluaciones ISO 27001 e ISO 27002, las que van a permitir recomendar controles que reduzcan los riesgos que afecten a la seguridad de la información, lo principal para este propósito es la elaboración de políticas de seguridad para el centro de cómputo de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil.

Es necesario evaluar el estado de implementación de la norma ISO 27001 mediante los requerimientos obligatorios de la propia norma para la obtención de información sobre el nivel de implementación del sistema de gestión de seguridad de la información [5].

Según Diego A. Arcentales-Fernández, Xiomara Caycedo-Casas en el año 2017 en su trabajo titulado "Auditoría informática: un enfoque efectivo", investigó los siguientes temas, y llegó a las siguientes conclusiones importantes: Lo más importante que debe

considerar un auditor es conocer con propiedad, cual es la evidencia que debe recopilar; si no se prepara antes del proceso de auditoría, todo el proceso puede estar cuestionado por las partes involucradas. Un adecuado indicador de madurez en el desempeño puede utilizarse como referencia para la comparación y como una herramienta para comprender las mejores prácticas en gestión de auditorías informáticas. La Auditoría Informática permite a las organizaciones, alcanzar los estándares internacionales en el uso adecuado de las tecnologías de información, con miras a una certificación de calidad; así mismo, da cuenta del uso adecuado de los controles de riesgos de mayor impacto [6].

1.3 Fundamentación Teórica

Auditoria

La auditoría se origina como una necesidad social generada por el desarrollo económico, la complejidad industrial, que han producido empresas sobre dimensionadas en las que se separan los titulares del capital y los responsables de la gestión. Es toda la información que utiliza el auditor para llegar a la conclusión en que se basa su opinión [7].

Auditar implica someter a un proceso de revisión, por un experto profesional suficientemente cualificado, determinado procedimiento, actividad, informe, proceso, entre otros, con intención de obtener un alto grado de garantía de la correcta elaboración o desarrollo de los mismos [8].

En este sentido, se consideran principios de auditoría “las ideas fundamentales que rigen en el desarrollo de la práctica auditora”.

Las normas derivan de los principios generales y son reglas a las que deben ajustarse las conductas y las actividades.

De acuerdo con el concepto anterior, serán normas de auditoría las reglas que deben seguirse para el desarrollo de los principios de auditoría [9].

Auditoria Informática

Son una herramienta que ayuda a la organización a identificar posibles fallas del sistema, pero también oportunidades de mejora de los procesos internos, lo cual permite: Evaluar la eficacia de los controles internos. Contribuir al proceso de mejoría de los procesos y del Sistema en general. Comprobar y monitorear el cumplimiento de las normas y los procedimientos vigentes. Analizar la aparición de nuevos riesgos, permitiendo la implementación de procedimientos para minimizar o neutralizar su impacto [10].

La auditoría informática se presenta como la herramienta imprescindible para revisar y examinar de manera sistemática y analítica los sistemas de información, los procedimientos, actividades, programas u operaciones que realiza el sector público, lo que permite evaluar el cumplimiento de legalidad, la conformidad financiera, su eficacia, eficiencia y economía en la utilización de los recursos disponibles [11].

Al hablar de términos de seguridad informática se debe entender a las bases que conforman los cimientos de esta ciencia, para las partes más complejas de esta disciplina, una de estas bases es el concepto de seguridad, la cual consiste en un estado de bienestar, es la ausencia de riesgo por la confianza que existe en alguien o algo, si la seguridad se aborda desde el tema disciplinario el concepto se puede definir como una ciencia interdisciplinaria para evaluar y gestionar los riesgos a los que se encuentra una persona, un animal, el ambiente o un bien. Existen países en donde la seguridad es un tema nacional, aunque depende del tipo de seguridad, existen muchos tipos de ésta, por ejemplo, la seguridad ambiental, la seguridad económica, la seguridad sanitaria y en casi la mayoría de los países cuando se hace un análisis de la palabra seguridad, se hace referencia a la seguridad de las personas, por ejemplo, evitar el estado de riesgo de un robo, de un daño físico o de un bien material [12].

Auditoria Informática aplicando la norma ISO 27001

Es un examen que se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas del negocio. Se puede aplicar un SGSI de acuerdo con la ISO 27001 una norma internacional

que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

Estas auditorías están destinadas a mejorar el nivel de seguridad de la información, evitar diseños de seguridad de la información inadecuados y optimizar la eficiencia de las medidas de seguridad y los procesos de seguridad. El término "marco de seguridad" se ha utilizado de diversas maneras en la literatura de seguridad durante el años, pero en 2006 pasó a utilizarse como un término agregado para los diversos documentos, algunas piezas de software y la variedad de fuentes que brindan asesoramiento sobre temas relacionados con la seguridad de los sistemas de información, en particular, con respecto a la planificación, gestión o auditoría de las prácticas generales de seguridad de la información para una institución dada [13].

La Auditoría en informática se refiere a la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una entidad con el fin de emitir un informe o dictamen sobre la situación en que se desarrollan y se utilizan esos recursos [14].

Las auditorías internas deben poseer un alto entendimiento en la implementación del SGSI y la utilización de normas ISO/IEC 27001 en la organización, ya que este personal ejecutara el servicio de valorar y verificar controles complejos, desarrollando y utilizando metodologías de auditoría. Para ejecutar las auditorías internas se puede aplicar los siguientes métodos: revisión, estudio, entrevistas, documentación y procedimientos analíticos a los sistemas informáticos de la organización [15].

Es la revisión y evaluación de los controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para la adecuada toma de decisiones [16].

Al implementar una auditoria informática a través de una ISO 27001 la cual es una certificación internacional no solo provee lineamientos, sino beneficia en la reducción de los puntos de riesgos que serán mitigados por los valores añadidos de dicha certificación [17].

El auditor es la persona que comprueba que el SGSI de una organización se ha diseñado, implementado, verificado y mejorado conforme a lo detallado en la norma. En cuanto a la práctica de la auditoría, al auditor se le exige que se muestre ético, con mentalidad abierta, diplomático, observador, perceptivo, versátil, tenaz, decidido y seguro de sí mismo. Estas actitudes son las que deberían crear un clima de confianza y colaboración entre auditor y auditado. El auditado debe tomar el proceso de auditoría siempre desde un punto de vista constructivo y de mejora continua, y no de fiscalización de sus actividades. Para ello, el auditor debe fomentar en todo momento un ambiente de tranquilidad, colaboración, información y trabajo en equipo [18].

Control y Calidad de la Información

El Control de la Información es una evaluación de acciones, para detectar posibles riesgos o inconvenientes que serán corregidos mediante la utilización de un sistema de gestión informático. La Calidad de la Información significa poseer calidad, consistencia para que sea considerada como información [19].

Como control debemos entender aquellos procedimientos destinados a evaluar el rendimiento real, comparar ese rendimiento con los objetivos fijados, o corregir las diferencias entre los resultados y los objetivos. Esta etapa es esencial, ya que, de no existir, no podría conocerse si lo planificado, organizado y ejecutado se ha realizado correctamente, y por tanto ha funcionado bien [20].

Desde el inicio de operaciones de una empresa es necesario establecer un sistema de dirección y control simple pero eficaz. El control es el establecimiento de programas y sistemas que permiten medir resultados. En cambio, el objetivo del control es proporcionar apoyo técnico y administrativo para lograr la consecución de los objetivos señalados en los programas. Es conveniente establecer controles desde el inicio de operaciones para evitar que los empleados, posteriormente, se vuelvan reacios a utilizarlos e, inclusive, los puedan sabotear. Llevar controles debe formar parte del trabajo diario de todo el personal [21].

La calidad de la información (CI) se define como la medición de las salidas de datos de las TI en términos de ser exacta, oportuna, completa, confiable, relevante y precisa. Los

datos e información producidos por los SIC (Sistemas de Información y Comunicación) usados para planear, analizar, administrar, dirigir y controlar las operaciones del negocio se volvieron importantes desde hace mucho tiempo [22].

El estudio, basado en un análisis documental clásico, reflexiona sobre algunas directrices conceptuales-metodológicas relativas a la medición de la calidad de la información (CI) en el marco de la gestión de información (GI) en las organizaciones. Es descrito el proceso de GI y la importancia de la aplicación de principios de calidad en éste [23].

La Calidad de la información va de la mano en conformidad con los requerimientos. Los requerimientos tienen que estar claramente establecidos para que no haya malentendidos; las mediciones deben ser tomadas continuamente para determinar conformidad con esos requerimientos; la no conformidad detectada es una ausencia de calidad [24].

Seguridad de la Información

Permite preservar la confidencialidad, la integridad y la disponibilidad de la información; además, deben incluir otras propiedades, como la autenticidad, responsabilidad, la confiabilidad. Una de las normas de seguridad de la información es la norma ISO 27001 debido a que miden el riesgo y ayudan a mejorar la gestión de la seguridad de la información en una empresa, por tal motivo si una empresa no aplica normas de gestión de seguridad como la norma ISO 27001 está expuesta al riesgo de quedarse muy por detrás de sus competidores, dado que las normas ISO admiten una mejora notable para las empresas.

La seguridad de la información, para conseguir el objetivo se apoya a la seguridad informática, es decir, la seguridad de la información será la encargada de regular y establecer las pautas a seguir para la protección de la información [25].

En la actualidad, uno de los factores más importantes que se debe tener en cuenta en todo tipo de organizaciones es la seguridad de la información, ya que los incidentes relacionados con ésta comprometen los activos de las empresas y las ponen en riesgo, lo anterior genera la necesidad de implementar sistemas de seguridad a partir de un análisis de riesgos y minimizar así consecuencias no deseadas [26].

La seguridad de la información es fundamental para la supervivencia de las organizaciones en la era de la información. Varios problemas están involucrados, dado que la sociedad depende de la información almacenada en los sistemas informáticos para la toma de decisiones en las empresas, entidades del gobierno, entre otros contextos organizacionales. La información puede existir en varios formatos: impresa, almacenada electrónicamente, hablada, transmitida por correo convencional de voz o electrónico, etc. Cualquiera que sea el formato o medio de transmisión o almacenamiento, se recomienda proteger la información de manera adecuada. Por lo tanto, es responsabilidad de la seguridad de la información protegerla de los diversos tipos de amenazas para garantizar. La seguridad de la información incluye la protección de información, sistemas, recursos y demás activos contra desastres, errores (intencionales o no) y manipulación no autorizada, para reducir la probabilidad y el impacto de los incidentes de seguridad [27].

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. El concepto de seguridad de la información no debe ser confundido

con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos [28].

Tomando como base la seguridad de la información, en la actualidad la seguridad informática es un aspecto muy importante en las organizaciones, donde los protocolos, las tecnologías (hardware o software), los dispositivos, las herramientas y las técnicas que permiten proteger los datos son ahora esenciales para la disminución de las amenazas presentes, cuyo único objetivo es socavar la información con fines diferentes a los ya definidos para la organización [29].

Informática

Es una ciencia técnica que se centra en comprender los problemas y aplicar las tecnologías de información según sea necesario. Una de las ramas más importantes de la informática

es la Ingeniería en Sistemas que busca dar soluciones a diversos problemas informáticos, ya sea en el desarrollo del software e inclusive a la seguridad informática [30].

Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores. De una forma más sintetizada, podemos identificar la Informática con información automática [31].

La Informática es una disciplina emergente-integradora que surge producto de la aplicación-interacción sinérgica de varias ciencias, como la computación, la electrónica, la cibernética, las telecomunicaciones, la matemática, la lógica, la lingüística, la ingeniería, la inteligencia artificial, la robótica, la biología, la psicología, las ciencias de la información, cognitivas, organizacionales, entre otras, al estudio y desarrollo de los productos, servicios, sistemas e infraestructuras de la nueva sociedad de la información.[32]

Es el proceso que le permite a los seres humanos diseñar herramientas y máquinas para controlar su ambiente material y aumentar la comprensión de este. El termino proviene de dos palabras griegas: tecné, que significa "arte" u "oficio", y logos, que significa "conocimiento" o "tratado".

En conclusión, la tecnología es el conocimiento de los oficios. La información es todo lo que reduce incertidumbre entre varias alternativas posibles, son los datos que necesitamos conocer para tomar decisiones de manera más efectiva [33].

Informática es un concepto sinónimo de computación, y lo definiremos como conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. La informática combina los aspectos teóricos y prácticos de la ingeniería electrónica, teoría de la información, matemática, lógica y comportamiento humano. Los aspectos de la informática cubren desde la programación y la arquitectura informática hasta la inteligencia artificial y la robótica [34].

La informática surgió de la necesidad de transmitir y tratar información de manera automática. Su propósito inicial era ayudar al hombre en aquellos trabajos rutinarios y

repetitivos, generalmente de cálculo y de gestión, donde es frecuente la repetición de tareas [35].

Seguridad

Preservación de los bienes y servicios a través de normas de confianza para con el fin de evitar algún daño o riesgo [36].

La seguridad implica un conjunto amplio de asuntos que trascienden a la seguridad pública, y que deben atenderse a través de políticas públicas, que integren al gobierno y a sus diferentes órdenes de forma coordinada [37]**.**

Entienden la seguridad como medio y no como fin. Se presenta pues el término como un medio para la consolidación de la soberanía, y su ejercicio implica la eliminación de amenazas (tanto internas como externas) y el control sobre el territorio [38].

La seguridad siempre se refiere a una amenaza existencial a un objeto de referencia. El término seguridad se encuentra en diversos documentos de organismos internacionales como objetivo a lograr [39].

La seguridad es por tanto un estado de cosas o una situación en la que no es factible la concreción de amenazas que vayan en detrimento de determinados valores, sean estos materiales o inmateriales [40].

La capacidad de las personas, los Estados o las sociedades de librarse de las amenazas y de mantener su independencia en lo que se refiere a su identidad y a su integración funcional frente a fuerzas de cambio consideradas hostiles [41].

Gestión de Seguridad

Tiene como objetivo fundamental garantizar una adecuada implementación de los controles de seguridad a través de evaluaciones de las políticas de una organización. Además, su función es administrar y monitorear la integridad y privacidad de la información procesada por la infraestructura tecnológica institucional.

La gestión de la seguridad en el trabajo se está consolidando a nivel mundial, como un pilar necesario de toda empresa para mejorar las condiciones de sus trabajadores

alcanzando una mayor productividad y por consiguiente, mayor rentabilidad de su actividad laboral. Alrededor del mundo, este beneficio ha llevado que varias instituciones no gubernamentales y de instancia de derecho público, hayan desarrollado metodologías de aplicación para la gestión de la seguridad y salud ocupacional, con clara líneas en común [42].

Permite demostrar que la seguridad es una fuente de ventajas competitiva que puede hacer la diferencia entre permanecer o salir del mercado y que las pérdidas generadas por los accidentes, enfermedades ocupacionales, fatiga física o mental y por la insatisfacción laboral no permiten optimizar la productividad empresarial y que el trabajo que no genere satisfacción de sus y para sus actores no cumple su razón de ser [43].

El objetivo principal es solventar el cumplimiento y resolver las fallas importantes que se presenten en la compañía y propone ayudar a la organización a comprender y mejorar las actividades y resultados de la prevención de riesgos laborales [44].

Para la correcta gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metodológica, documentada y basada en unos objetivos claros de seguridad y una acertada evaluación de los riesgos a los que está sometida la información de la organización [45].

La Gestión de la Seguridad en el Trabajo busca con la intervención de varias disciplinas y con la participación activa de todos los niveles de la empresa, mejorar las condiciones de trabajo y salud de la población trabajadora, mediante acciones coordinadas de promoción de la salud y la prevención y control de los riesgos, de manera que faciliten el bienestar de la comunidad laboral y la productividad de la empresa [46].

1.4 Objetivos

1.4.1 Objetivo General

Implantar la norma de seguridad informática ISO 27001 para optimizar la seguridad de la información en el departamento TIC's del Centro de Investigación y Desarrollo FAE.

1.4.2 Objetivos Específicos

- Determinar los riesgos informáticos existentes en el departamento de TIC´s del Centro de Investigación y Desarrollo FAE.
- Analizar las buenas prácticas o controles establecidos en la norma ISO 27001 para la auditoria informática.
- Aplicar la norma de seguridad informática ISO 27001 para optimizar la seguridad, mantenimiento y el manejo del Sistema de Gestión de Seguridad de la información en el departamento de TIC's del Centro de Investigación y Desarrollo FAE.

CAPITULO II.- METODOLOGÍA

2.1 Materiales

Como materiales para la investigación científica para el presente proyecto, se utilizó una entrevista y la encuesta detallada a continuación

FORMULARIO DE LA ENTREVISTA

Encuestado Preguntas	Jefe de Mantenimiento de Informática	Conclusiones
1. ¿Cuál es el riesgo informático más común que se detecta con mayor frecuencia en la empresa?		
2. ¿Se realiza gestión de riesgos en cuanto a la seguridad de la información?		
3. ¿Los sistemas de informáticos han sido víctimas de robo de información?		
4. ¿Los Controles de seguridad que se emplean en la empresa son suficientes y adecuados para garantizar la seguridad de la información y en las aplicaciones informáticas?		
5. ¿Cuál es el proceso que se lleva a cabo para la gestión y administración de los		

activos informáticos en la empresa?		
6. En cuanto a la Seguridad Física ¿Cuál es el procedimiento del personal para el acceso a los servidores de base de datos en la empresa?		

Tabla 1: Formulario de la Entrevista

FORMULARIO DE LA ENCUESTA

1.- ¿Actualmente el departamento de TIC'S con que políticas de seguridad para la gestión de información dispone?

a) Control de acceso ( )
b) Seguridad de la información ( )
c) Seguridad física ( )
d) Seguridad ambiental ( )
e) Ninguna ( )

2.- ¿Se han presentado fallas en los equipos de cómputo en su empresa que conlleven a la pérdida de información?

a) Siempre ( )
b) Ocasionalmente ( )
c) Nunca ( )

3.- ¿Qué técnica de seguridad se aplica para el cuidado y uso de la información?

a) Control de usuario ( )
b) Firewall ( )

c) NAT ( )

d) Ninguno ( )

4.- ¿Cada que tiempo se realizan tareas de monitoreo a los sistemas de información en conjunto con los empleados?

a) Siempre ( )

b) Ocasionalmente ( )

c) Nunca ( )

5.- ¿Cada que tiempo periódicamente se realiza el mantenimiento preventivo y correctivo de los equipos informáticos en la empresa?

a) 1 vez al mes ( )

b) cada 2 meses ( )

b) cada 3 meses ( )

c) cada 6 meses ( )

d) cada año ( )

6.- ¿Con que frecuencia los sistemas informáticos presentan fallas?

a) Siempre ( )

b) Ocasionalmente ( )

c) Nunca ( )

7.- ¿Cuál es el nivel de conocimiento en seguridad de la información del personal en el Departamento de TIC's?

a) Alto ( )

b) Medio ( )

c) Bajo ( )

8.- ¿Con que frecuencia actualiza el Sistema Operativo y las aplicaciones?

a) Siempre ( )

b) Ocasionalmente ( )

c) Nunca ( )

9. ¿Cada que tiempo se realizan copias de seguridad de la información?

a) 1 vez al mes ( )

b) cada 2 meses ( )

b) cada 3 meses ( )

c) cada 6 meses ( )

d) cada año ( )

10.- ¿Se han presentado inconvenientes en las redes de internet durante la transmisión de los datos?

a) Siempre ( )

b) Ocasionalmente ( )

c) Nunca ( )

2.2 Métodos

La presente investigación utilizó los enfoques cuantitativo y cualitativo en razón de que se procedió a la recolección de los datos relacionados con la seguridad de la información mediante entrevista y encuesta, con la finalidad de tener un análisis completo de la actual situación del departamento de TIC's.

2.2.1 Modalidad de la Investigación

Investigación bibliografía documental

Porque se utilizará fuentes como libros, tesis, artículos científicos, para el desarrollo del marco teórico y el análisis de la aplicación de la norma ISO con documentación empresarial.

Investigación de Campo

Porque se buscará aplicar una auditoría informática de seguridad de la información en el departamento de TIC's y analizar cómo se realizan los distintos procesos mediante la aplicación de la norma ISO 27001.

2.2.2 Población y Muestra

La población a considerarse en el siguiente proyecto es:

Población	Número	Porcentaje
Jefe del CIDFAE	1	14%
Jefe de TIC's	1	14%
Desarrollador del Software	2	29%
Jefe de Mantenimiento de Informática	1	14%
Analista de Soporte Técnico	2	29%
Total	7	100%

Tabla 2: Población y Muestra

2.2.3 Recolección de Información

Para poder obtener un diagnóstico de los procesos informáticos que se manejan actualmente en el Departamento de TIC's de la Institución, se realizó una entrevista al Jefe del departamento y una encuesta a cada uno del personal dentro del departamento, para así poder evidenciar cómo se manejan los procesos y poder encontrar falencias de seguridad en el mismo. Con la finalidad de poder determinar si existían actualmente

políticas de seguridad, se mantuvo visitas al departamento, se hizo un levantamiento de información.

Para la realización de la entrevista se utilizaron cuestionarios de evaluación que fueron elaborados en base a los estándares de seguridad informática, dirigida al departamento de TIC´s con el fin de conocer las actividades que se realizan diariamente de manera que no se omita ningún aspecto de la relevante durante la investigación.

2.2.4 Procesamiento y Análisis de Datos

La información que se obtuvo fue revisada, organizada e interpretada, de tal manera que los resultados obtenidos fueron representados en forma de gráficos y porcentajes que fueron de ayuda para el desarrollo de la solución del problema planteado aplicando los siguientes procedimientos:

- Elaboración de instrumentos para entrevista y encuestas.
- Tabulación de la información obtenida
- Estudio estadístico de datos para presentación de resultados

CAPÍTULO III.- RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados

3.1.1 Determinación de los riesgos informáticos existentes en el departamento de TIC's del Centro de Investigación y Desarrollo FAE

3.1.1.1 Resultados de la Entrevista

Al aplicar la entrevista al Jefe de Mantenimiento de Informática se obtuvo los siguientes resultados.

Encuestado Preguntas	Jefe de Mantenimiento de Informática	Conclusiones
1. ¿Cuál es el riesgo informático más común que se detecta con mayor frecuencia en la empresa?	Problemas de Virus, Pishing y Fuga de Información	Se puede evidenciar que en el departamento existe un déficit de seguridad en cuanto malware se refiere, además existe problemas de Pishing y riesgo de pérdida de información.
2. ¿Se realiza gestión de riesgos en cuanto a la seguridad de la información?	Si, se dispone de planes de contingencia y recuperación de la información.	Se concluye que el personal está preparado ante catástrofes.
3. ¿Los sistemas de informáticos han sido víctimas de robo de información?	Por el momento no se ha suscitado caso de robo de información.	Se comprueba que el robo de información internamente es escaso.

Encuestado Preguntas	Jefe de Mantenimiento de Informática	Conclusiones
4. ¿Los Controles de seguridad que se emplean en la empresa son suficientes y adecuados para garantizar la seguridad de la información y en las aplicaciones informáticas?	Si, aquí disponemos de un equipo de Seguridad Perimetral	Se puede verificar que los controles de seguridad que posee la empresa son suficientes y son adecuados gracias a la Seguridad Perimetral que posee.
5. ¿Cuál es el proceso que se lleva a cabo para la gestión y administración de los activos informáticos en la empresa?	El Control de lado el parque informático de la Unidad se realiza el control y la administración con el Departamento de Activos Fijos	Se puede demostrar que no existe un proceso técnico para gestionar y administrar los activos informáticos en la empresa
6. En cuanto a la Seguridad Física ¿Cuál es el procedimiento del personal para el acceso a los servidores de base de datos en la empresa?	Solo pueden ingresar personal informático que trabajan desde la dirección vía remota	Se determina que existe Seguridad Física para que solo el personal informático pueda acceder a los servidores de base de datos.

Tabla 3: Resultado de la Entrevista

Fuente: Resultado de aplicación de la Entrevista

3.1.1.2 Resultados de la Encuesta

Al aplicar la encuesta a los 7 empleados del Departamento de TIC's, se obtuvieron las siguientes respuestas, a cada una de las preguntas realizadas en la misma.

Pregunta 1: ¿Actualmente el departamento de TIC'S con que políticas de seguridad para la gestión de información dispone?

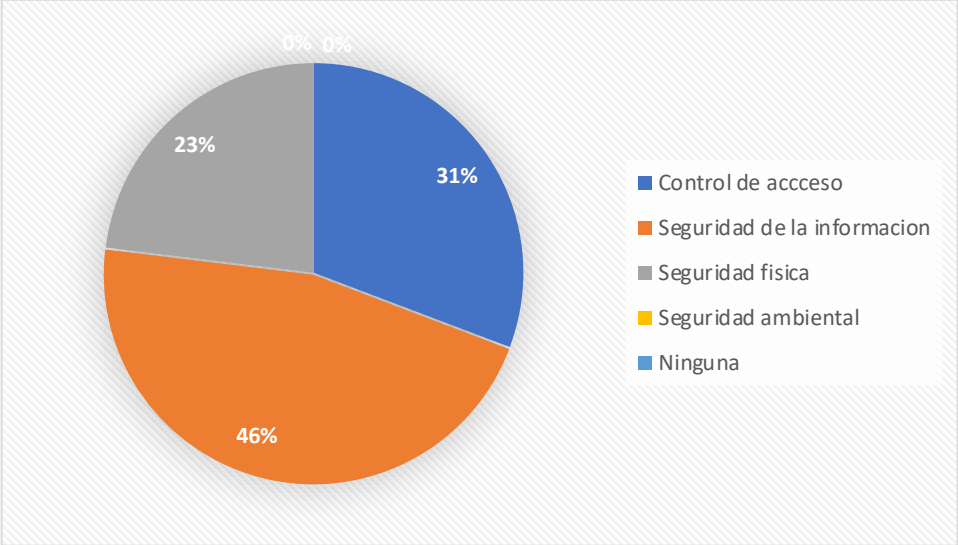


Figura 1: Políticas de Seguridad.

Fuente: Resultado de aplicación de la Encuesta

Análisis e interpretación de resultados:

De acuerdo con los resultados representados en la Figura 1, se puede determinar el 46% de los encuestados indican que existe Seguridad de la información, el 31% de las respuestas obtenidas indican que existe Control de acceso, el 23% indican tener Seguridad física, lo que se demuestra que en cuanto a la Seguridad ambiental no se registra ninguna política.

Pregunta 2: ¿Se han presentado fallas en los equipos de cómputo en su empresa que conlleven a la pérdida de información?

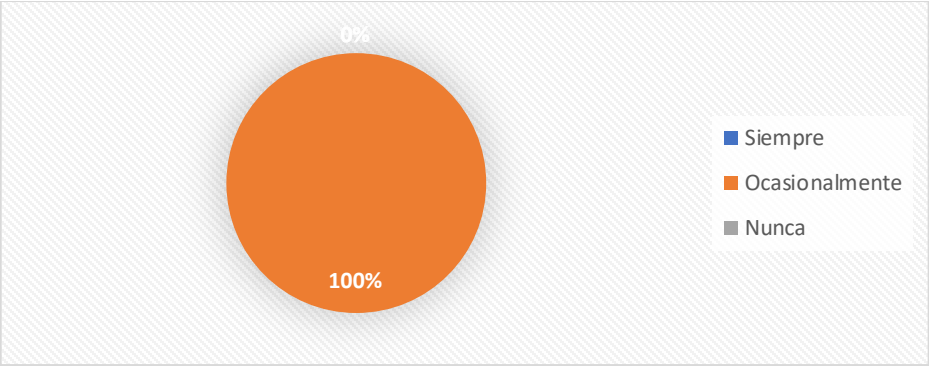


Figura 2: Fallas en los equipos de computo

Fuente: Resultado de aplicación de la Encuesta

Análisis e interpretación de resultados:

De acuerdo con los resultados representados en la Figura 2, se determina que el 100% de los encuestados indican que Ocasionalmente suelen tener fallas los equipos de cómputo, lo que se demuestra que los equipos de cómputo presentan fallas de hardware.

Pregunta 3: ¿Qué técnica de seguridad se aplica para el cuidado y uso de la información?

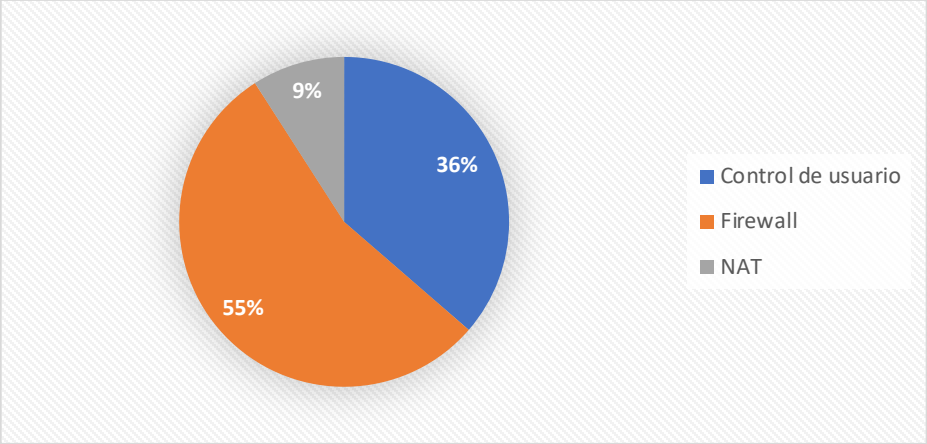


Figura 3: Técnica de seguridad y uso de información

Fuente: Resultado de aplicación de la Encuesta

Análisis e interpretación de resultados:

De acuerdo con los resultados representados en la Figura 3, se concluye que el 55% de los encuestados indican que se aplica Firewall, el 36% indican que se aplica el Control de usuario, mientras el 9% indican que se aplica NAT, lo que demuestra que la técnica de seguridad más utilizada es el Firewall.

Pregunta 4: ¿Cada que tiempo se realizan tareas de monitoreo a los sistemas de información en conjunto con los empleados?

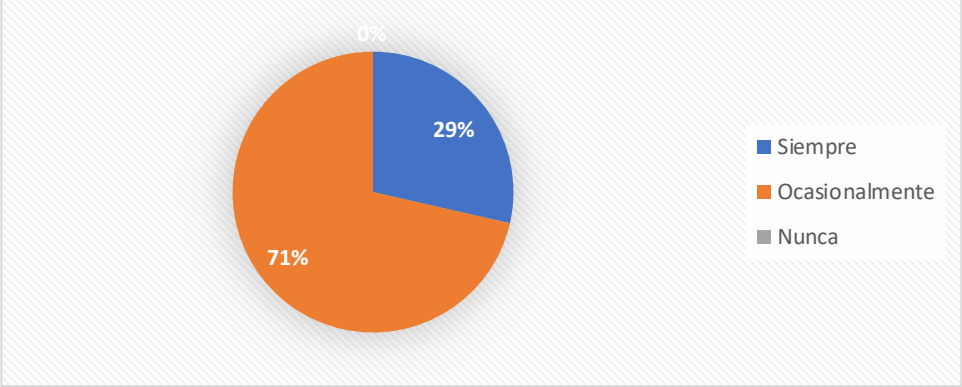


Figura 4: Tareas de monitoreo a los sistemas de información

Fuente: Resultado de aplicación de la Encuesta

Análisis e interpretación de resultados:

De acuerdo con los resultados representados en la Figura 4, se determina que 71% de los encuestados indican que Ocasionalmente se realizan tareas de monitoreo a los sistemas de información, el 29% de las respuestas obtenidas indican que Siempre se realizan tareas de monitoreo, lo que se requiere que los sistemas de información deben ser monitoreados en todo momento.

Pregunta 5: ¿Cada que tiempo periódicamente se realiza el mantenimiento preventivo y correctivo de los equipos informáticos en la empresa?

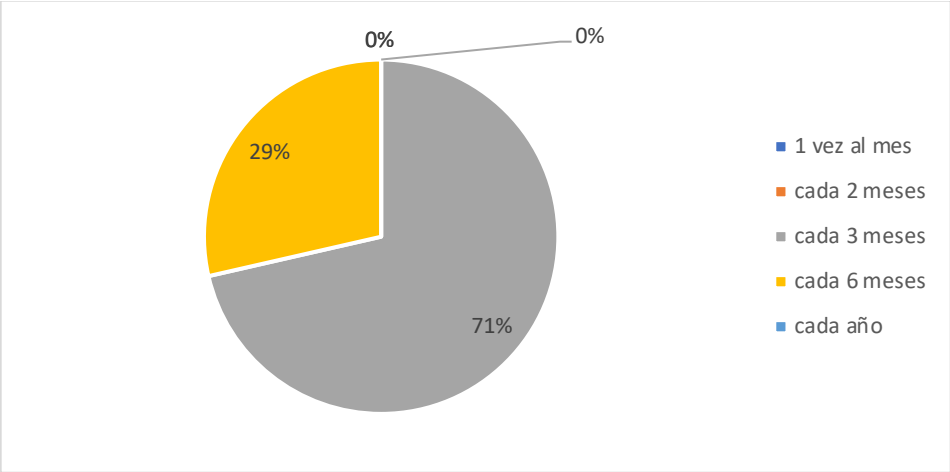


Figura 5: Tiempo en el que se realiza el mantenimiento preventivo y correctivo de los equipos

Fuente: Resultado de aplicación de la Encuesta

Análisis e interpretación de resultados:

De acuerdo con los resultados representados en la Figura 5, se puede determinar que el 71% de los encuestados indican que cada 3 meses se realiza el mantenimiento preventivo y correctivo a los equipos informáticos, el 29% de las indican que cada 6 meses se realiza dicho mantenimiento, lo que se concluye una cierta irregularidad en cuanto a la planificación del mantenimiento.

Pregunta 6: ¿Con que frecuencia los sistemas informáticos presentan fallas?

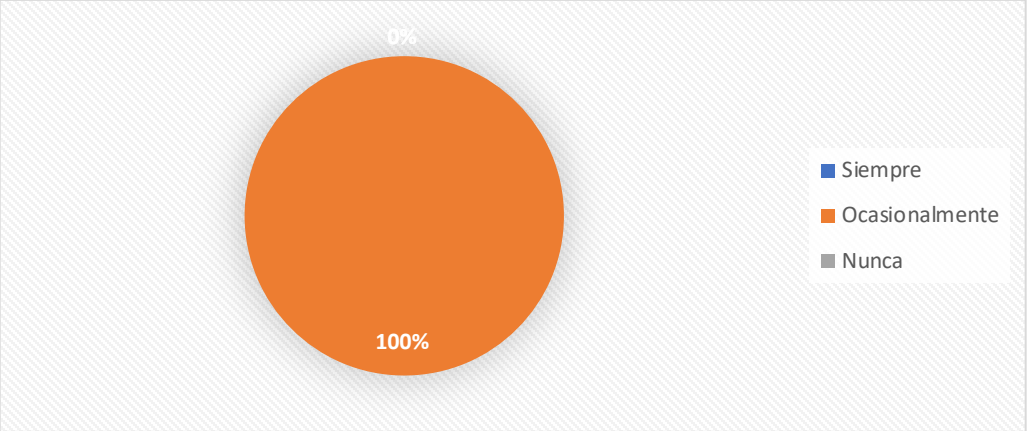


Figura 6: Frecuencia de los sistemas informáticos que presentan fallas

Fuente: Resultado de aplicación de la Encuesta

Análisis e interpretación de resultados:

De acuerdo con los resultados representados en la Figura 6, se concluye que el 100% de los encuestados indican que Ocasionalmente los sistemas informáticos presentan fallas, lo que se interpreta que los sistemas informáticos presentan fallas de software.

Pregunta 7: ¿Cuál es el nivel de conocimiento en seguridad de la información del personal en el Departamento de TIC's?

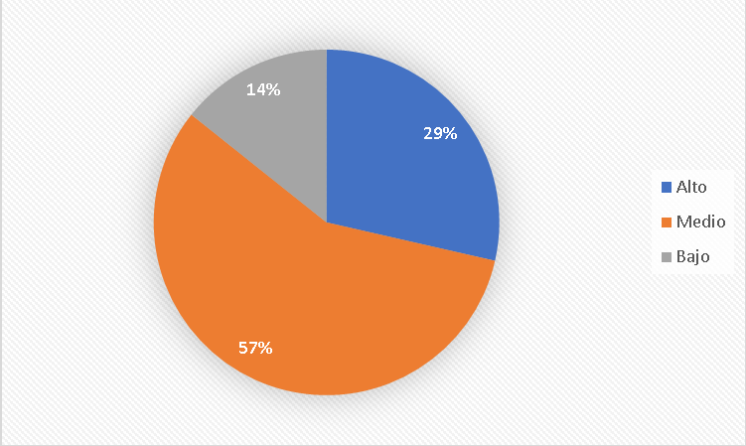


Figura 7: Nivel de conocimiento en seguridad de la información

Fuente: Resultado de aplicación de la Encuesta

Análisis e interpretación de resultados:

De acuerdo con los resultados representados en la Figura 7, se determina que el 57% de los encuestados indican que tienen un Medio nivel de conocimiento en seguridad de la información, el 29% indican que existe un Alto nivel de conocimiento, mientras que 14% indican que tienen un Bajo nivel de conocimiento, lo que se comprueba que existe un considerable porcentaje con conocimiento Medio y Bajo en el departamento de TIC's.

Pregunta 8: ¿Con que frecuencia actualiza el Sistema Operativo y las aplicaciones?

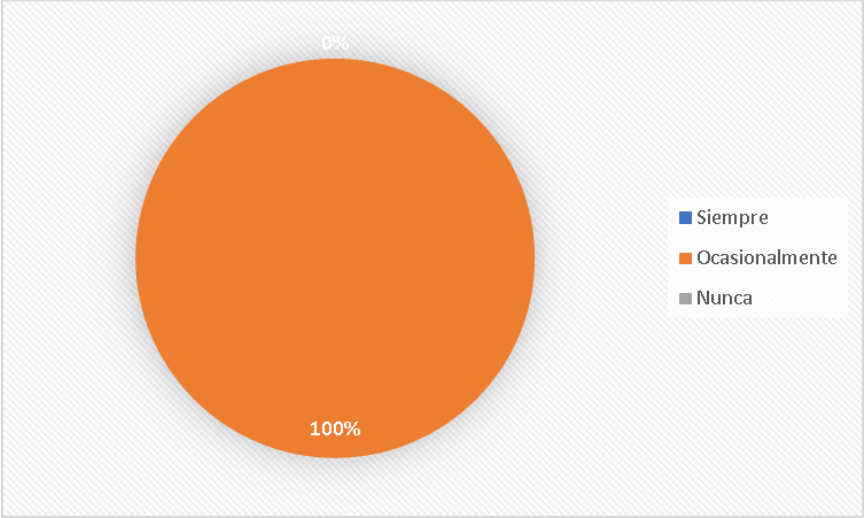


Figura 8: Actualización del Sistema Operativo y las aplicaciones

Fuente: Resultado de aplicación de la Encuesta

Análisis e interpretación de resultados:

De acuerdo con los resultados representados en la Figura 8, se concluye que el 100% de los encuetados indican que Ocasionalmente se actualiza el Sistema Operativo y las aplicaciones, lo que se manifiesta que los equipos pueden ser expuestos a fallas y vulnerabilidades de seguridad.

Pregunta 9: ¿Cada que tiempo se realizan copias de seguridad de la información?

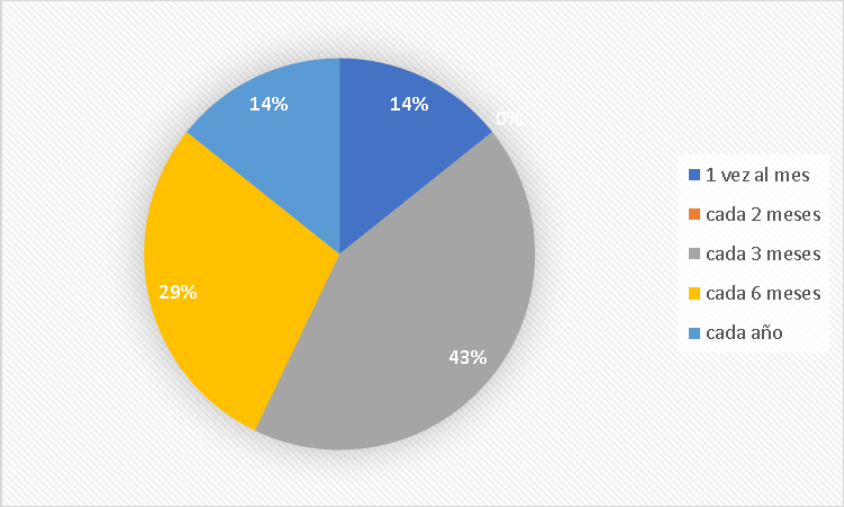


Figura 9: Copias de seguridad de la información

Fuente: Resultado de aplicación de la Encuesta

Análisis e interpretación de resultados:

De acuerdo con los resultados representados en la Figura 9, se puede determinar que el 43% de los encuestados indican que cada 3 meses se realizan copias de seguridad de la información, el 29% indican que cada 6 meses, el 14% indican que 1 vez al mes, el 14% indican que cada año se realizan dichas copias, lo que se manifiesta que se realiza las copias de seguridad cada 3 meses.

Pregunta 10: ¿Se han presentado inconvenientes en las redes de internet durante la transmisión de los datos?

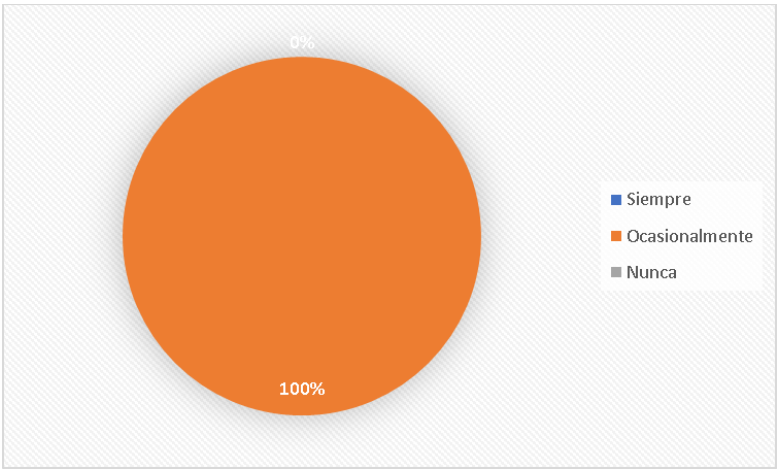


Figura 10: Inconvenientes en las redes de internet durante la transmisión de los datos

Fuente: Resultado de aplicación de la Encuesta

Análisis e interpretación de resultados:

De acuerdo con los resultados representados en la Figura 10, se determina que el 100% de los encuestados indican que Ocasionalmente se presenta inconvenientes en las redes de internet durante la transmisión de los datos, lo que se presenta que las redes en el departamento poseen ciertos inconvenientes al momento de la transmisión de datos.

3.1.1.3 Interpretación de Resultados de la Información Recopilada

- En base con los resultados obtenidos en la entrevista y en la encuesta se determinaron que el departamento de TIC's existen riesgos informáticos tales como la presencia de virus informáticos en los equipos, problemas de Pishing y perdida de información.

- Existe un plan de contingencia ante eventualidades, pero se pudo evidenciar falta de un proceso para gestionar y administrar los activos informáticos, lo cual es recomendable establecer dicho proceso.

- En cuanto a la seguridad física se determinó la existencia de un control de acceso al personal informático, así como de usuarios ajenos a la institución.

- No existe ninguna política de seguridad ambiental, lo que es necesario implementar un sistema de gestión ambiental para reducir impactos ambientales.

- Los equipos informáticos presentan fallas de hardware, lo que es necesario realizar una revisión periódica a cada equipo.

- En cuanto a las técnicas de seguridad de la información se puede concluir que NAT, no es una técnica muy utilizada en el departamento, es necesario utilizarla con mayor frecuencia para que los equipos conectados a la red no sean visibles desde el exterior.

- Las tareas de monitoreo a los sistemas de información se lo realizan por momentos, lo cual es necesario realizarlos siempre para identificar riesgos y amenazas.

- Algo que se pudo notar es la falta de capacitación al personal del Departamento de TIC's con respecto a Seguridad de la Información.

- No existe control y resguardo de toda la red interna y externa, lo que es muy necesario asegurar la red con herramientas de seguridad.

3.1.2 Buenas Prácticas establecidas por la Norma ISO 27001

Las buenas prácticas o controles de seguridad de la Norma ISO 27001 se aplica dentro del sistema de la seguridad de la información a todo tipo de empresas ya sea comerciales gubernamentales para afirmar el procedimiento del diseño en el manejo de la protección de activos dentro de una organización.

Las buenas Prácticas que establece la norma ISO 27001 son:

- A.5 Política de Seguridad
- A.6 Organización de la Seguridad de la Información
- A.7 Gestión de Activos
- A.8 Seguridad Ligada a los Recursos Humanos
- A.9 Seguridad Física y del Ambiente
- A.10 Gestión de Comunicaciones y Operaciones
- A.11 Control de Acceso
- A.12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- A.13 Gestión de Incidentes de Seguridad de la Información
- A.14 Gestión de la Continuidad del Negocio
- A.15 Cumplimiento

A.5 Política de Seguridad

La finalidad es establecer todo un conjunto de normas y controles necesarios que se van a aplicar en la organización para resguardar la seguridad de la información.

A.6 Organización de la Seguridad de la Información

Su finalidad es gestionar y controlar la seguridad de la información dentro de la organización, mediante la asignación de responsabilidades para garantizar el resguardo de la información.

A.7 Gestión de Activos

Se enfoca en aplicar y preservar la seguridad sobre los activos de información que posee una organización, el cual permitirá identificar, valorar, clasificar y tratar dichos activos.

A.8 Seguridad Ligada a los Recursos Humanos

Se define como medida para controlar el cumplimiento de las responsabilidades del personal con respecto a la seguridad de la información previo y durante el empleo.

A.9 Seguridad Física y del Ambiente

Evita accesos no autorizados para prevenir daños en la infraestructura de la organización, hurtos que comprometan la seguridad de los equipos informáticos y a los sistemas de información.

A.10 Gestión de Comunicaciones y Operaciones

Su finalidad es administrar y monitorear todas las actividades de comunicación y seguridad de la información dentro de la organización.

A.11 Control de Acceso

Establece el acceso solo al personal autorizado a los equipos informáticos, a los servicios de red y a los sistemas de información, para evitar el robo de información

A.12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Su finalidad es controlar la validación integral de la información en la adquisición y desarrollo de los sistemas de información, además define técnicas de seguridad y mantenimiento a dichos sistemas

A.13 Gestión de Incidentes de Seguridad de la Información

Establece que todos los eventos y debilidades de seguridad suscitados en los sistemas de información sean comunicados de forma inmediata, de tal manera que se puedan aplicar acciones correctivas correspondientes.

A.14 Gestión de la Continuidad del Negocio

Se finalidad es prevenir interrupciones en las actividades del negocio contra desastres de gran magnitud suscitados en los sistemas de información para garantizar la reanudación óptima y oportuna.

A.15 Cumplimiento

Está enfocado en cumplir con las políticas, normas y legislación referentes a la seguridad de la información

Para poner en ejecución estas buenas prácticas primero se va a realizar un análisis del estado actual de la seguridad informática en la empresa a través de la gestión de la seguridad de la información.

3.1.2.1 Gestión de la Seguridad

Para analizar y evaluar el estado actual de la seguridad de la información se utilizaron varias herramientas informáticas las cuales permitirán verificar vulnerabilidades en los puertos, en la infraestructura, y en los servicios dichas herramientas se detallan a continuación:

3.1.2.1.1. Herramientas para la ejecución del análisis de vulnerabilidades

Para el análisis de vulnerabilidades se realizó pruebas con varias herramientas que permitieron recopilar resultados específicos los mismos que serán analizados más adelante detalladamente, dentro de las herramientas que se escogieron tenemos las que se especifican a continuación:

A Herramienta de Monitoreo de puertos

Herramientas Características	Nmap	SuperScan4	NetScan6
Costo	Gratuita	Libre y Pagada	Libre y Pagada
Plataforma	Windows Mac Linux Unix	Windows	Windows
Soporte Direcciones	IPv4 / IPv6.	IPv4	IPv4 / IPv6.
Funciones	Escaneo de Servidores, Puertos abiertos, servicios, aplicaciones corriendo, versión del sistema operativo, DNS, resolución inversa IP, direcciones MAC	Escaneo de Puertos TCP, Pruebas de ping a direcciones IP, servicios, particulares en puertos específicos.	Escaneo de Puertos NetBIOS Direcciones IP, direcciones MAC, barrido de ping, sistemas operativos, acceso carpetas compartidas
Uso	Auditorias de seguridad en red, pruebas y recolección de información de futuros ataques.	Monitoreo y control de host y dominios, evaluación de la seguridad de la red de computadores.	Administración de la red, recopilación de información.
Actualizaciones Soporte	Si	Si	Si

Tabla 4: Herramienta de sondeo de puertos

Fuente: Elaboración Propia

De acuerdo al análisis de la Tabla 4. se seleccionó la herramienta Nmap con la que se realizó el análisis debido a que es la más utilizada en Auditorias de red, además la misma cuenta con la detección de Servidores, puertos abiertos, servicios, aplicaciones en ejecución, versión del sistema operativo, DNS, resolución inversa IP, direcciones MAC, de idéntica manera soporta direcciones IPv4 e IPv6.

B Herramientas de detección de vulnerabilidades

Herramientas Características	OpenVAS	Nessus	IBM Security QRadar
Costo	Libre	Libre y de paga	Paga
Plataforma	Windows Linux	Windows Mac Linux	Windows
Funciones	Escaneo concurrente de múltiples nodos. Escaneo concurrente de múltiples nodos. Escaneo automático temporizado. Servidor web integrado. Multiplataforma	Análisis en tiempo real de los Hosts Controles, configuración y permisos de acceso. Escaneo de redes Evaluación de riesgos. Rastreo de sitios web. Detección de recursos Seguridad en aplicaciones web	Análisis para detectar amenazas en la red y en equipos Analiza datos de registro de varios dispositivos Dispone de alerta de seguridad. Realiza un monitoreo y visibilidad sobre una amenaza potencial
Reportes	Formatos (XML, HTML, LaTeX, entre otros).	Formatos (PDF, CSV, XML, HTML),	
Actualización Soporte	Si	Si	Si

Tabla 5: Herramientas de detección de vulnerabilidades

Fuente: Elaboración Propia

De acuerdo al análisis de la Tabla 5 se seleccionó Nessus para la búsqueda de vulnerabilidades la cual permite escaneos detallados y se pueden analizar varios ordenadores, también cuentan con varias funciones como escaneo automáticos, avanzados y personalizados, análisis de vulnerabilidades, análisis web, escaneo de redes, Controles, configuración y permisos de acceso, Detección de recursos, evaluación de riesgos, además cuentan con reportes flexibles y fáciles de interpretar en diferentes formatos.

3.1.2.1.2 Identificación de vulnerabilidades y riesgos

A Monitoreo de Red

Para el análisis de la red se obtuvieron direcciones IP las mismas que fueron proporcionadas por el departamento de TIC's, las cuales van a ser auditadas, para lo cual se procederá a realizar una búsqueda avanzada en la red, es necesario mencionar que el auditor no puede obtener información confidencial de la CIDFAE.

B Listado de Servidores de la Institución

N°	Dirección IP	Nombre	Sistema Operativo
1	192.168.4.18	Servidor de Archivos	Windows Server 2012 R2
2	192.168.4.19	Servidor de Archivos	Windows Server 2016
3	192.168.4.20	Servidor de Base de Datos	Windows Server 2012 R2
4	192.168.4.21	Servidor de Base de Datos	Windows Server 2016

Tabla 6: Listado de Servidores a auditar

Fuente: Elaboración Propia

C Identificación de Servicios

Se realizó un sondeo en los puertos en cada servidor para poder identificar los servicios que se están ejecutando

Para el análisis y sondeo de puertos se utilizó la herramienta Nmap en el Sistema Operativo Kali Linux, la misma que fue elegida anteriormente. A continuación, nos indica los puertos y servicios de cada servidor.

Servidor 192.168.4.18

Puerto	Protocolo	Estado	Servicio	Detalle
21	tcp	Abierto	tcpwrapped	
22	tcp	Abierto	ssh	OpenSSH for_windows_8.6 (protocol 2.0)
23	tcp	Abierto	telnet	
25	tcp	Abierto	smtp	Microsoft ESMTP 8.5.9600.16384
80	tcp	Abierto	http	Microsoft IIS httpd 8.5
110	tcp	Abierto	pop3	
111	tcp	Abierto	rpcbind	2-4 (RPC #100000)
119	tcp	Abierto	nntp	
135	tcp	Abierto	msrpc	Microsoft Windows RPC
139	tcp	Abierto	netbios-ssn	Microsoft Windows netbios-ssn
443	tcp	Abierto	https	
445	tcp	Abierto	microsoft-ds	Microsoft Windows Server 2008 R2 – 2012 microsoft-ds
808	tcp	Abierto	ccproxy-http	
1080	tcp	Abierto	socks	
2049	tcp	Abierto	mountd	1-3 (RPC #00005)
2121	tcp	Abierto	ccproxy-ftp	
3260	tcp	Abierto	tcpwrapped	
8080	tcp	Abierto	http	Apache httpd 2.4.52 ((Win64) OpenSSL/1.1.1m PHP7.4.27)
49153	tcp	Abierto	msrpc	Microsoft Windows RPC
49154	tcp	Abierto	msrpc	Microsoft Windows RPC
49155	tcp	Abierto	msrpc	Microsoft Windows RPC
49156	tcp	Abierto	msrpc	Microsoft Windows RPC
49157	tcp	Abierto	msrpc	Microsoft Windows RPC

Tabla 7: Nmap a 192.168.4.18

Fuente: Resultado de aplicación de la Herramienta Nmap

Servidor 192.168.4.19

Puerto	Protocolo	Estado		Servicio	Detalle
21	tcp	Abierto		tcpwrapped	
22	tcp	Abierto		ssh	OpenSSH for_windows_8.6 (protocol 2.0)
25	tcp	Abierto		smtp	Microsoft ESMTP 10.0.14393.0
80	tcp	Abierto		http	Microsoft IIS httpd 10.0
111	tcp	Abierto		rpcbind	2-4 (RPC #00000)
135	tcp	Abierto		msrpc	Microsoft Windows RPC
139	tcp	Abierto		netbios-ssn	Microsoft Windows netbios-ssn
443	tcp	Abierto		ssl/http	Microsoft IIS httpd 10.0
445	tcp	Abierto		microsoft-ds	
2049	tcp	Abierto		mountd	1-3 (RPC #00005)
3260	tcp	Abierto		iscsi	

Tabla 8: Nmap a 192.168.4.19

Fuente: Resultado de aplicación de la Herramienta Nmap

Servidor 192.168.4.20

Puerto	Protocolo	Estado	Servicio	Detalle
22	tcp	Abierto	ssh	OpenSSH for_windows_8.6 (protocol 2.0)
80	tcp	Abierto	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135	tcp	Abierto	msrpc	Microsoft Windows RPC
139	tcp	Abierto	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	Abierto	microsoft-ds	Microsoft Windows Server 2008 R2 – 2012 microsoft-ds
1433	tcp	Abierto	ms-sql-s	Microsoft SQL Server 2012 11.00.2100; RTM
49152	tcp	Abierto	msrpc	Microsoft Windows RPC
49153	tcp	Abierto	msrpc	Microsoft Windows RPC
49154	tcp	Abierto	msrpc	Microsoft Windows RPC
49155	tcp	Abierto	msrpc	Microsoft Windows RPC
49156	tcp	Abierto	msrpc	Microsoft Windows RPC
49157	tcp	Abierto	msrpc	Microsoft Windows RPC
49158	tcp	Abierto	msrpc	Microsoft Windows RPC

Tabla 9: Nmap a 192.168.4.20

Fuente: Resultado de aplicación de la Herramienta Nmap

Servidor 192.168.4.21

Puerto	Protocolo	Estado	Servicio	Detalle
22	tcp	Abierto	ssh	OpenSSH for_windows_8.6 (protocol 2.0)
135	tcp	Abierto	msrpc	Microsoft Windows RPC
139	tcp	Abierto	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	Abierto	microsoft-ds	Microsoft Windows Server 2008 R2 – 2012 microsoft-ds
1521	tcp	Abierto	oracle-tns	Oracle TNS listener 11.2.0.1.0

Tabla 8: Nmap a 192.168.4.21

Fuente: Resultado de aplicación de la Herramienta Nmap

En los escaneos realizados de los servidores en la institución con la herramienta Nmap se pudo determinar lo siguiente:

- Se utiliza el protocolo FTP para subir páginas web.
- Se utiliza el protocolo SSH para acceder remotamente a un servidor
- Se utilizan los protocolos SMTP para el correo de salida e IMAP para el correo de entrada.
- Se utilizan como servicios de Base de Datos a SQL Server y Oracle
- Se utilizan NFS y SAMBA como servicios para compartir archivos y carpetas a través de la red.
- Como servicios web se utilizan Apache, IIS, httpd
- Se utiliza el servidor Proxy para restringir el contenido en la red

3.1.2.1.3. Búsqueda y verificación de vulnerabilidades

A continuación, a través de la herramienta Nessus se procedió al escaneo de vulnerabilidades de los sistemas operativos de cada servidor en el departamento de TIC's, dicha herramienta realiza un escaneo exhaustivo y posteriormente muestra el nivel de riesgo que tiene ante un posible ataque.

Nessus es una herramienta de seguridad para Sistemas Operativos Windows y Linux, se utiliza mediante un navegador web predeterminado.

Para realizar el escaneo se procedió a crear un nuevo escaneo en la página principal (New Scan), luego se eligió el tipo de escaneo en este caso se eligió el escaneo recomendado para el análisis que es el Avanzado (Advanced Scan), en el mismo se procederá a colocar un nombre del proceso, la descripción y la dirección IP del Host a analizar, y finalmente se guardó el escaneo, posteriormente se ejecutó el análisis de vulnerabilidades de cada Host.

Servidor de Archivos

Servicio	Vulnerabilidad	Riesgo	Observación
Apache httpd 2.4.12	Varias vulnerabilidades del servidor HTTPD	Alto	Este host ejecuta HTTP Apache y es propenso a múltiples vulnerabilidades.
NFS	El servidor NFS remoto exporta recursos compartidos legibles a nivel mundial.	Medio	El servidor NFS remoto está exportando uno o más recursos compartidos sin restringir el acceso (basado en el nombre de host, la IP, o rango de IP).
SSL Certificate Signed Using Weak Hashing Algorithm	Se ha firmado un certificado SSL en la cadena de certificados mediante un algoritmo hash débil.	Medio	El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un algoritmo de hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables

Servicio	Vulnerabilidad	Riesgo	Observación
			a los ataques de colisión. Un atacante puede aprovechar esta circunstancia para generar otro certificado con la misma firma digital, lo que le permitiría enmascarar la identidad de un atacante. firma digital, permitiendo a un atacante hacerse pasar por el servicio afectado
SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto admite el uso de cifrados SSL de potencia media	Medio	El host remoto soporta el uso de cifrados SSL que ofrecen una encriptación de fuerza media.
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	El servicio remoto soporta el uso del cifrado RC4.	Medio	El host remoto soporta el uso de RC4 en una o más suites de cifrado. El cifrado RC4 es defectuoso en su generación de un flujo pseudo-aleatorio de bytes de modo que una amplia variedad de de pequeños sesgos se introducen en el flujo, disminuyendo su aleatoriedad.

Servicio	Vulnerabilidad	Riesgo	Observación
			Si el texto plano se cifra repetidamente (por ejemplo, las cookies HTTP), y un atacante es capaz de obtener muchos (es decir, decenas de millones) de textos cifrados, el atacante puede ser capaz de obtener el texto plano.
SSL Self-Signed Certificate	La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido	Medio	La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque de tipo man-in-themiddle contra el host remoto.
SMB Signing not required	SMB Signing not required	Medio	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para llevar a cabo ataques man-in-the-middle contra el servidor SMB.

Servicio	Vulnerabilidad	Riesgo	Observación
Msrpc	Informes de enumeración de servicios DCE / RPC y MSRPC	Medio	El entorno de computación distribuida / llamadas a procedimientos remotos (DCE / RPC) o los servicios MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas
TLS Version 1.0 Protocol Detection	El servicio remoto encripta el tráfico utilizando una versión antigua de TLS.	Medio	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene una serie de defectos de diseño de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estos fallos y deberían utilizarse siempre que sea posible.

Tabla 10: Vulnerabilidades encontradas en 169.168.4.18

Fuente: Resultado de aplicación de la Herramienta Nessus

Servidor de Archivos

Servicio	Vulnerabilidad	Riesgo	Observación
SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto admite el uso de cifrados SSL de fuerza media.	Medio	El host remoto soporta el uso de cifrados SSL que ofrecen una encriptación de fuerza media. Nessus considera fuerza media como cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el conjunto de cifrado 3DES.
SMB Signing not required	La firma no es necesaria en el servidor SMB remoto.	Medio	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para llevar a cabo ataques man-in-the-middle contra el servidor SMB.
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	El servicio remoto soporta el uso del cifrado RC4.	Medio	El host remoto soporta el uso de RC4 en una o más suites de cifrado. El cifrado RC4 es defectuoso en su generación de un flujo pseudo-aleatorio de bytes de

			modo que una amplia variedad de de pequeños sesgos se introducen en el flujo, disminuyendo su aleatoriedad. Si el texto plano se cifra repetidamente (por ejemplo, las cookies HTTP), y un atacante es capaz de obtener muchos (es decir, decenas de millones) de textos cifrados, el atacante puede ser capaz de obtener el texto plano.
Msrpc	Informes de enumeración de servicios DCE / RPC y MSRPC	Medio	El entorno de computación distribuida / llamadas a procedimientos remotos (DCE / RPC) o los servicios MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas
TLS Version 1.0 Protocol Detection	El servicio remoto encripta el tráfico utilizando una versión antigua de TLS	Medio	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0

			tiene una serie de defectos de diseño de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estos defectos y deberían utilizarse siempre que sea posible.

Tabla 11: Vulnerabilidades encontradas en 169.168.4.19

Fuente: Resultado de aplicación de la Herramienta Nessus

Servidor de Base de Datos

Servicio	Vulnerabilidad	Riesgo	Observación
Microsoft SQL Server 2012	Detección de fin de vida de Microsoft SQL Server	Alto	La versión de Microsoft SQL Server en el host remoto ha llegado al final de su vida útil y ya no debe utilizarse.
Microsoft- ds	Microsoft Windows SMB Server Múltiple vulnerabilidades remotas	Alto	A este host le falta una actualización de seguridad crítica según Microsoft Bulletin MS17-010.
SSL Certificate Signed Using Weak Hashing Algorithm	Un certificado SSL en la cadena de certificados ha sido firmado utilizando un algoritmo hash débil.	Medio	El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada utilizando un algoritmo de hash

Servicio	Vulnerabilidad	Riesgo	Observación
			criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede aprovechar esta circunstancia para generar otro certificado con la misma firma digital, lo que le permitiría enmascarar la identidad de un atacante. mismo, lo que le permitiría hacerse pasar por el servicio afectado.
SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto admite el uso de cifrados SSL de fuerza media.	Medio	El host remoto soporta el uso de cifrados SSL que ofrecen una encriptación de fuerza media. Nessus considera fuerza media como cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el conjunto de cifrado 3DES.

Servicio	Vulnerabilidad	Riesgo	Observación
Msrpc	informes de enumeración de servicios DCE / RPC y MSRPC	Medio	El entorno de computación distribuida / llamadas a procedimientos remotos (DCE / RPC) o los servicios MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas.
Microsoft IIS httpd 6.0	Vulnerabilidad en la divulgación de información de carácter de tilde de Microsoft IIS	Medio	Este host ejecuta el servidor web Microsoft IIS y es propenso a la divulgación de información.
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	La cadena de certificados X.509 utilizada por este servicio contiene certificados con claves RSA inferiores a 2048 bits.	Bajo	Al menos uno de los certificados X. 509 enviados por el host remoto tienen una clave inferior a 2048 bits. De acuerdo con los estándares de la industria establecidos por el Foro de Autoridades de Certificación/Browser (CA/B), los certificados emitidos después del 1 de enero de 2014 deben tener al menos 2048 bits

Tabla 12: Vulnerabilidades encontradas en 169.168.4.20

Fuente: Resultado de aplicación de la Herramienta Nessus

Servidor de Base de Datos

Servicio	Vulnerabilidad	Riesgo	Observación
Oracle TNS Listener Remote Poisoning	Era posible registrarse con un oyente remoto de Oracle TNS	Alto	El listener remoto de Oracle TNS permite el registro de servicios desde un host remoto. Un atacante puede explotar este problema para desviar datos de un servidor de base de datos legítimo o de un cliente a un sistema especificado por el atacante.
SMB Signing not required	No se requiere la firma de SMB	Medio	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para llevar a cabo ataques man-in-the-middle contra el servidor SMB.

Tabla 13: Vulnerabilidades encontradas en 169.168.4.21

Fuente: Resultado de aplicación de Nessus

En el escaneo realizado con Nessus se encontró lo siguiente:

- Los servidores de archivos en el servidor NFS está exportando archivos sin restringir el acceso, esto provocaría otros usuarios no autorizados puedan visualizar la información

- En los servidores de archivos se encontraron vulnerabilidades de SSL en cuanto a la firma de certificaciones, lo que ocasionaría que un atacante pueda explotar dicho certificado para generar otro con la misma firma digital, posibilitnado que el atacante se haga pasar por el servicio afectado.

- Se determinó que no se aplica la firma en el servidor SMB, lo que ocasionaría que un atacante remoto no autenticado puede aprovechar esto para llevar a cabo ataques man-in-the-middle contra el servidor SMB

- Las versiones de Microsoft IIS, SMB, TLS se encuentran obsoletas, las cuales deben ser actualizadas, debido al fin de su vida útil o por incompatibilidad con el servidor.

- Se detectó que en uno de los servidores de base datos el fin de vida útil de SQL Server 2012.

- El servidor de Base datos con Oracle que el TNS Listener, permite registros de servicios desde un host remoto, lo que ocasionaría que un atacante puede explotar este problema para desviar datos de un servidor de base de datos legítimo.

3.1.2.1.3 Metodología para la gestión de la seguridad de la información

Se adoptará la metodología del ciclo Deming o también conocido como ciclo continuo (PDCA), tradicional en los sistemas de gestión de seguridad. Se selecciono dicha metodología porque garantiza la mejora continua de los procesos y servicios en una organización. Son actividades realizadas dentro de un sistema de información para resguardar la integridad y la veracidad de los datos en la entidad

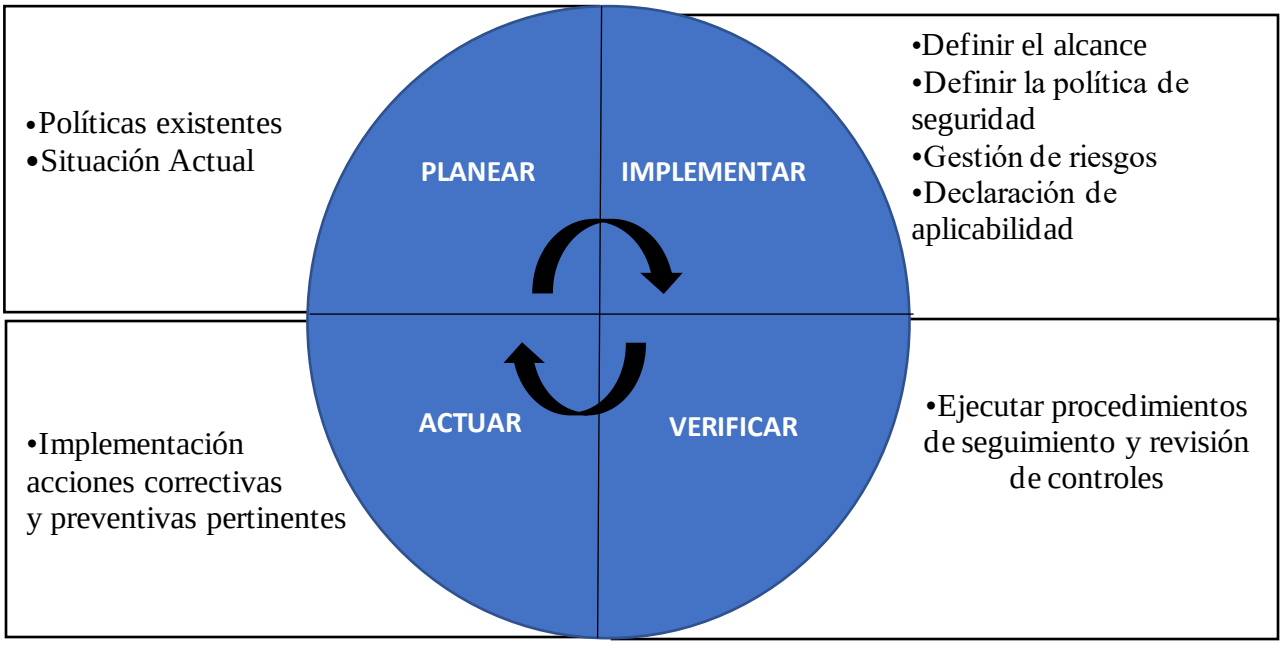


Figura 11: Metodología de aplicación -ciclo de Deming

Fuente: [47]

A Planear

A.1 Políticas existentes en el Departamento de Tecnologías de la Información

El Departamento de TIC's del Centro de Investigación y Desarrollo FAE, al momento no cuenta con políticas de seguridad para realizar los diferentes técnicas y procesos que garanticen la seguridad de la información dentro del departamento, existen varias pautas que se implementaron para cubrir los diferentes procesos los cuales deberían tener y contar con una política estructurada con las diferentes normas para la seguridad de la información.

Entre las normas que se encontraron en el departamento de TIC's, podemos detallar las siguientes:

- Mantenimiento de los equipos activos de las redes Lan.
- Instalación y reparación del cableado estructurado.

- Asignación de direcciones IP y acceso a las diferentes páginas web a los usuarios.
- Mantenimiento del parque informático.
- Rastreo y monitoreo de la Red Lan.
- Implementación de seguridades en los diferentes equipos informáticos.

A.2 Situación Actual de la empresa

Se realizó un análisis para evaluar el estado actual de la empresa y de los sistemas de información utilizados en el departamento de TIC's

A.2.1 Información de la Empresa

- Beneficiario

Centro de Investigación y Desarrollo FAE.

- Ubicación

Ecuador

Tungurahua / Ambato

Aeropuerto Chachoan, Sector De Izamba/Ambato

- Introducción a la Empresa

Es la encargada de proporcionar soluciones a los problemas técnico-operacionales de la flota de aviones militares, así como a los equipos y sistemas de la Institución, fortaleciendo al poder aeronáutico del Ecuador a través de la autosuficiencia tecnológica.

- Misión

Desarrollar investigación científica y tecnológica aeroespacial, para mejorar la capacidad operativa de la Fuerza Aérea y contribuir a la producción científica tecnológica y al desarrollo nacional.

A.2.2 Organigrama Estructural

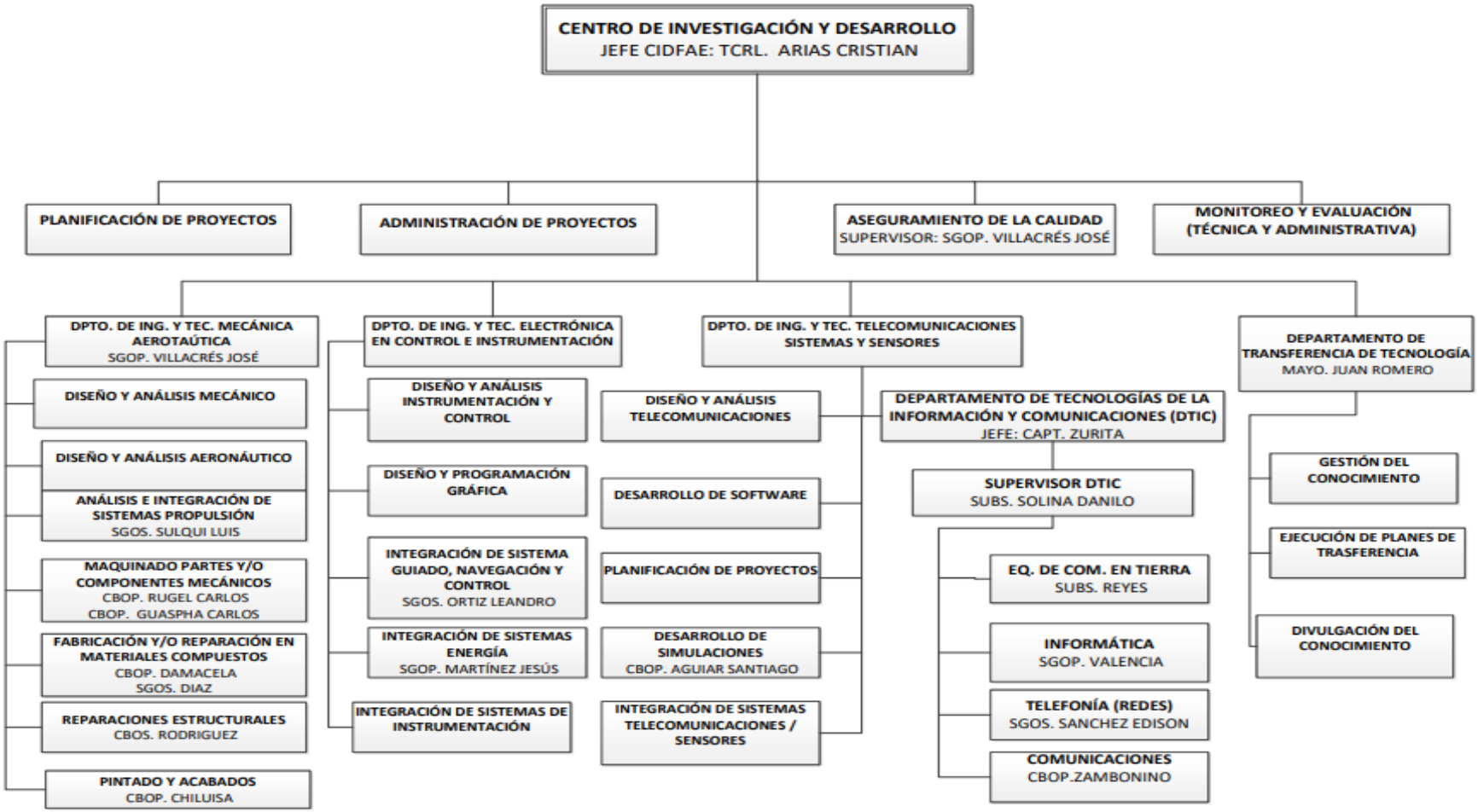


Figura 12: Organigrama Estructural CIDFAE

Fuente: [48]

A.2.3 Sistemas y aplicaciones existentes en la empresa

Sistema/Aplicación	Definición	Características
Squarenet	Es una herramienta que permite gestionar y administrar al personal de una manera más eficaz en una empresa, es el más utilizado en el trabajo diario gracias a su facilidad de uso y flexibilidad.	• Mayor flexibilidad, con la funcionalidad de programación • Permite la presentación a través de reportes con diferentes formatos a Excel, Word, HTML, • Soporte con bases de datos • Permite la replicación de datos.
SIFFAE	Es un sistema de información financiera de Fuerza Aérea Ecuatoriana que funciona como instrumento de control previo al gasto corriente	• Evaluación de gastos • Ejecución de presupuestos • Monitoreo de cuentas y actividades
AnyDesk	Es un software de escritorio remoto desarrollado Permite el acceso remoto bidireccional entre computadoras personales y está disponible para todas las plataformas.	• Acceso remoto bidireccional entre Windows, Linux, Mac. • Permite la transferencia de archivos • Interacción cliente a cliente • Facilidad de uso • Registro de sesiones de usuarios • Acceso para dispositivos móviles Android • Integra portapapeles.
CHASQUI	Es un sistema de gestión documental y de archivos de la FAE	• Administración eficiente de los archivos documentales. • Gestión de usuarios • Agrupación de todos los procesos

Sistema/Aplicación	Definición	Características
eSIGEF	Es una herramienta informática a través de la cual se facilita el desarrollo de los procesos de la gestión financiera pública del Presupuesto General del Estado, con el fin de obtener de manera ágil y oportuna la información r	• Registros contables • Monitoreo de la evaluación de presupuestos • Información contable automática • Estados financieros consolidados
esByE	Es un Sistema que tiene como objetivo principal garantizar la eficiencia y el control financiero y administrativo de los bienes y existencias, que son propiedad del Estado	• Administración de bienes del sector publico • Asignación y reasignación de bienes • Control de inventarios
Sistema Moving Map	Es un sistema multifunción de manejo de misiones para búsqueda, rescate, fuerzas de seguridad.	• Integración de una variedad de mapas ATC, de aeropuertos. • Monitoreo de búsquedas y rescates.
AGI & STK Training	Es un software para la creación de sistemas aeroespaciales y de defensa, permite realizar exploraciones automatizadas a través de modelos analíticos.	• Creación de modelos analíticos de sistemas aeroespaciales y de defensa • Análisis de simulaciones de misiones • Exploración de la API de STK para la integración y la automatización

Tabla 14: Sistemas y aplicaciones existentes en la empresa

Fuente: Elaboración Propia

B Implementar

B.1 Diseño del SGSI

Aplicando la metodología propuesta se procede a desarrollar el Modelo SGSI basado en la ISO 27001 con el cual se pretende garantizar que los riesgos de la seguridad de la información sean gestionados y sobre todo minimizados por el Centro de Investigación y Desarrollo CIDFAE.

El sistema de Gestión de Seguridad de la información propuesto tiene los siguientes aspectos:

- Definir el alcance
- Definir la política de seguridad
- Gestión de riesgos
- Declaración de aplicabilidad
- Implementación de procedimientos y controles

B.1.1 Alcance del SGSI

El alcance se definirá tomando en cuenta los aspectos más importantes de la empresa como activos, organización, recursos, etc.
El departamento de TIC's define el alcance del SGSI de acuerdo a los servicios y sistemas en los que esta involucrados los procesos que manejan la información en la empresa
El alcance del SGSI contemplará los siguientes procesos:

- Gestión de Activos: Es uno de los apartados más importantes del CIDFAE, aquí se definirán las responsabilidades del personal, las cuales serán asignadas después de un previo análisis y gestión de los mismos con respecto a riesgos y vulnerabilidades potenciales dentro de la empresa.
- Gestión de recursos humanos: El compromiso del personal para salvaguardar la información, además de una capacitación adecuada garantizará un mejor control de recursos e información durante el periodo laboral o transición del mismo.

- Control de acceso: La verificación de identidad de un empleado previo al ingreso es necesario para que tenga acceso a los recursos de la empresa, de esta manera se mantendrá la confidencialidad e integridad de la información.
- Gestión de Operaciones y comunicaciones: Con la finalidad de garantizar la disponibilidad de la información y la funcionalidad de los sistemas de información ante eventualidades que puedan suscitarse, se definirán procesos que permitan garantizar el adecuado funcionamiento.

B.1.2 Política de Seguridad

Para implantar la siguiente política de seguridad que cubra todas las necesidades relacionadas con la gestión de la seguridad de la información en la empresa, la misma que posteriormente ayudará a implementar el SGSI dentro del departamento de TIC's en el Centro de Investigación y Desarrollo FAE.

"Fomentar las buenas prácticas de seguridad de la información dentro de la empresa, las mismas que permitan asegurar la continuidad y el manejo adecuado de los procesos del departamento de TIC's a través de un Sistema de Gestión de Seguridad de la Información basado en un control preventivo y enfocado a mantener la integridad, confidencialidad y disponibilidad de la información".

Objetivos:

Se han definido los siguientes objetivos para asegurar el cumplimiento de la política de seguridad:

- Establecer controles para prevenir o mitigar riesgos relacionados a la seguridad de la información.
- Elaborar el plan de gestión de riesgos para el control de la información.
- Implementar el plan de gestión de seguridad de la información.
- Supervisar el plan de gestión de la seguridad de la información.

B.1.3 Gestión de Riesgos

Es de vital importancia analizar y evaluar el impacto que tienen los diferentes riesgos que pueden encontrarse tomando en cuenta las posibles consecuencias que afecten los procesos que se llevan a cabo en la empresa y más aún si en ellos se maneja información de suma importancia.

El objetivo principal de la evaluación es identificar si los riesgos suscitados en los activos de la empresa infringen las normas de seguridad de la información

Para la gestión se definió un método cualitativo donde se detallan todos los activos de la empresa, se identifican las amenazas relacionado con cado uno de ellos y la posibilidad de ocurrencia.

Esquema metodológico a utilizar:

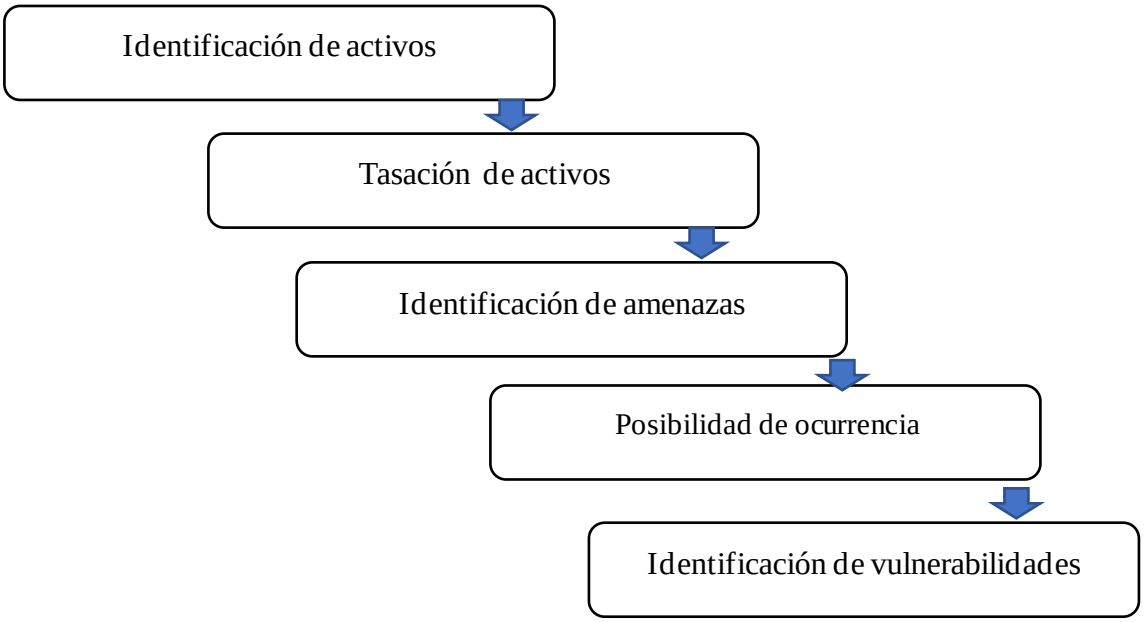


Figura 13: Metodología para la gestión de riesgos

Fuente: Elaboración Propia

B.1.3.1 Identificación y tasación de activos

Los activos son uno de los recursos más importantes dentro de la empresa debido a que mediante estos se manipula la información por tal motivo es de vital importancia brindarle una adecuada protección, una vez identificados los activos existentes se procede a tasarlos con la finalidad de establecer los de mayor importancia siempre basándose en los niveles de integridad, disponibilidad y confidencialidad de la información.

Posteriormente a la tasación de los activos se define la probabilidad de incidencia con respecto a las amenazas considerando el impacto en el caso de ocurrirse, lo que supone un riesgo a la confidencialidad disponibilidad e integridad de la información.

Por consiguiente, el valor del riesgo se consigue del valor total de la tasación del activo por el valor de la probabilidad de la amenaza

B.1.3.2 Inventarios de Activos Informáticos

Los activos informáticos forman un complemento de los procesos que se realizan en la empresa, los principales tipos de activos que existen son: sistemas de información, software y fisios.

Para el proceso de evaluación de los activos se estableció un rango entre 1 y 5, siendo los valores de 5 con mayor importancia y los de menos importancia con valores de 1.

Activos	Confidencialidad	Disponibilidad	Integridad	Total
Servidor de Archivos	3	4	4	4
Computadores de oficina y laptops	3	4	3	3
Switch	3	4	3	3
Central Telefónica IP	2	4	4	3
Router	3	4	3	3
Cuentas de usuario	3	3	3	3

Activos	Confidencialidad	Disponibilidad	Integridad	Total
Correo Institucional	4	4	4	4
CHASQUI documental de las fuerzas armadas y FAE (Sistema de Gestión Documental)	3	3	4	3
ESIGEF (Sistema Contable)	4	4	4	4
SIFFAE Y ESBYE (sistema de control de activos fijos y control administrativo-finanzas)	3	4	3	3
Impresora Multifunción	3	4	3	3
Sistema Moving Map	4	4	4	4
AGI & STK	4	4	4	4

Tabla 15: Identificación y Tasación de riesgos

Fuente: Elaboración Propia

Seguidamente se procede a determinar los activos cuyos valores son mayores o iguales a 3 para calcular la probabilidad del riesgo, en la Tabla 16 corresponde a los Activos de mayor importancia encontrados en el departamento de TIC's.

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
Servidor de Archivos	Alteración de información	Escasez de medidas de seguridad	4	3	12
	Robo de información	Falta de mantenimiento			
Computadoras de escritorio y laptops	Phishing	Escasez de herramientas de monitoreo de correo	3	4	12
	Virus	Falta de mantenimiento			
	Malware	Uso inapropiado de internet			
	Spyware	Falta de control de acceso			
Switch	Recalentamiento	Problemas en la alimentación eléctrica	3	3	9
	Daño o pérdida total				
	Bajo rendimiento	Falta de mantenimiento			

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
Central Telefonía IP	Perdida de la Conexión	Inadecuada configuración de la central telefónica	3	2	6
Router	Recalentamiento	Problemas en la alimentación eléctrica	3	3	9
	Bajo rendimiento	Falta de mantenimiento			
Cuentas de usuario	Alteración de cuentas	Inadecuado control de acceso	3	2	6
	Eliminación de cuentas				

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
CHASQUI documental de las fuerzas armadas y FAE(Sistema de Gestión Documental)	Robo de información	Falta de políticas de seguridad	3	3	9
	Fuga de Información	Falta de control de acceso			
ESIGEF(Sistema Contable)	Robo de información	Falta de políticas de seguridad	4	3	12
	Fuga de Información	Falta de control de acceso			

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
SIFFAE Y ESBYE (sistema de control de activos fijos y control administrativo-finanzas)	Robo de información	Falta de políticas de seguridad	3	3	9
	Fuga de Información	Falta de control de acceso			
Impresora Multifunción	Daño en los cartuchos	Falta de mantenimiento	3	4	12
	Cabezales dañados				
	Falta de tinta	Falta de control de recursos			
	Cartuchos incompatibles				
	Atasco de papel	Inadecuado formato de papel			

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total
Sistema Moving Map(sistema multifunción de manejo de misiones areas)	Robo de información	Falta de políticas de seguridad	4	2	8
	Fuga de Información	Falta de control de acceso			
AGI & STK Training (sistema de simulación de sistemas espaciales)	Robo de información	Falta de políticas de seguridad	4	2	8
	Fuga de Información	Falta de control de acceso			

Tabla 16: Activos de mayor importancia

Fuente: Elaboración Propia

Luego del análisis y evaluación de riesgos existentes en la empresa se pudo identificar de manera clara y precisa los activos con las tasas más altas de afectación dando origen a posibles ataques externos.

B.1.3.3 Selección de Objetivos de Control

A partir de las buenas prácticas establecidas por la Norma ISO 27001 se puede agregar una columna donde se muestre el "Objetivo de Control" en el cual se elegirá el dominio pertinente que cumpla con las condiciones de evaluación realizada en la tabla 11 con la finalidad de describir la amenaza de cada activo informático.

La selección adecuada de los objetivos de control permite asegurar que cada aspecto de los activos de información de la organización, que se valoraron con algún grado de riesgo, sea cubierto y auditable.

A continuación, se muestra la columna "Objetivo de control" la misma que contiene los dominios que corresponden con las amenazas detalladas en cada activo informático:

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total	Objetivos de control
Servidor de Archivos	Alteración de información	Escasez de medidas de seguridad	4	3	12	• A.11 Control de Acceso
	Robo de información	Falta de mantenimiento				
Computadoras de escritorio y laptops	Phishing	Escasez de herramientas de monitoreo de correo	3	4	12	• A.11 Control De Acceso • A.9 Seguridad Física Y Del Ambiente • A.10 Gestión De Comunicaciones Y Operaciones
	Virus	Falta de mantenimiento				
	Malware	Uso inapropiado de internet				
	Spyware	Falta de control de acceso				
Switch	Recalentamiento	Problemas en la alimentación eléctrica	3	3	9	• A.7 Gestión De Activos • A.9 Seguridad Física Y Del Ambiente • A.13 Gestión De Incidentes. Seguridad De La Información
	Daño o pérdida total					
	Bajo rendimiento	Falta de mantenimiento				

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total	Objetivos de Control
Central Telefonía IP	Perdida de la Conexión	Inadecuada configuración de la central telefónica	3	2	6	• A.10 Gestión de comunicaciones y operaciones.
Router	Recalentamiento	Problemas en la alimentación eléctrica	3	3	9	• A.7 Gestión de activos. • A.9 Seguridad Física y del Ambiente • A.13 Gestión de Incidentes de Seguridad de la Información
	Bajo rendimiento	Falta de mantenimiento				
Cuentas de usuario	Alteración de cuentas	Inadecuado control de acceso	3	2	6	• A.11 Control de acceso

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total	Objetivos de Control
CHASQUI documental de las fuerzas armadas y FAE(Sistema de Gestión Documental)	Robo de información	Falta de políticas de seguridad	3	3	9	• A.6 Organización de la Seguridad de la Información • A.11 Control de Acceso
	Fuga de Información	Falta de control de acceso				
ESIGEF(Sistema Contable)	Robo de información	Falta de políticas de seguridad	4	3	12	• A.6 Organización de la Seguridad de la Información • A.11 Control de Acceso

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total	Objetivos de Control
			3	3	9	

SIFFAE Y ESBYE (sistema de control de activos fijos y control administrativo-finanzas)	Robo de información	Falta de políticas de seguridad				• A.6 Organización de la Seguridad de la Información • A.11 Control de Acceso
	Fuga de Información	Falta de control de acceso				
Impresora Multifunción	Daño en los cartuchos	Falta de mantenimiento	3	4	12	• A.9 Seguridad Física y del Ambiente
	Cabezales dañados					
	Falta de tinta	Falta de control de recursos				
	Cartuchos incompatibles					
	Atasco de papel	Inadecuado formato de papel				

Activo	Amenazas	Vulnerabilidades	Valoración del activo	Probabilidad de amenaza	Riesgo Total	Objetivos de control
Sistema Moving Map(sistema multifunción de manejo de misiones áreas)	Robo de información	Falta de políticas de seguridad	4	2	8	A.6 Organización De La Seguridad de la Información A.11 Control De Acceso
	Fuga de Información	Falta de control de acceso				
AGI & STK Training (sistema de simulación de sistemas espaciales)	Robo de información	Falta de políticas de seguridad	4	2	8	A.6 Organización de la Seguridad de la Información A.11 Control De Acceso
	Fuga de Información	Falta de control de acceso				

Tabla 17: Selección de Controles

Fuente: Elaboración Propia

B.1.4 Declaración de Aplicabilidad

Se elaboró la Declaración de Aplicabilidad – SOA (Arquitectura Orientada a Servicios) el cual es un documento basado en los apartados de la norma ISO 27001, que es uno de los puntos de partida para la aplicación del SGSI en el departamento de TIC's del CIDFAE

La finalidad consiste en analizar e identificar cada uno de los controles aplicables que se implementaran en el departamento de TIC's para su debida utilización, así como la justificación de los controles que no son aplicables.

La presente Declaración de Aplicabilidad fue revisada y aprobada previamente por el Jefe del Departamento de TIC's.

La declaración de Aplicabilidad constituirá de:

- Apartados del control de la norma ISO 27001
- Los objetivos de control correspondientes a cada apartado.
- Los objetivos de control seleccionados con su debida justificación

La persona encargada de revisar y aprobar la Declaración de Aplicabilidad fue el Jefe del Departamento de TIC's, en este caso el Teniente Carlos Yagual Gutiérrez. Es importante recalcar que se ha empleado el formato de SOA de la misma norma ISO.

A.5 POLÍTICA DE SEGURIDAD					
A.5.1 Política de seguridad de la información					
SECCIÓN	CONTROLES ISO 27001	APLICABILIDAD		JUSTIFICACIÓN DE APLICABILIDAD	JUSTIFICACIÓN DE EXCLUSIÓN
		SI	NO		
A.5.1.1	Documento de política de seguridad de la información	x		Es de suma importancia diseñar un documento en donde se establezcan las políticas de seguridad, debido a que la información es uno de los activos más importantes, dicho documento debe ser aprobado, publicado y comunicado en el departamento de TIC’s.	
A.5.1.2	Revisión de la política de seguridad de la información	x		Es muy importante realizar revisiones periódicas de las políticas de seguridad de la información, para asegurar la conveniencia, suficiencia y eficacia de estas.	
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					
A.6.1 Organización interna					
A.6.1.1	Compromiso de la dirección con la seguridad de la información	x		Es necesario el apoyo activo en cuanto a la gestión de la seguridad de la información dentro de la empresa por parte de la alta dirección	
A.6.1.2	Coordinación de la seguridad de la información	x		Las actividades en cuanto a la seguridad de la información deben estar coordinadas por el personal del departamento de TIC's bajo la supervisión de la alta dirección	
A.6.1.3		x			

	Asignación de responsabilidades sobre seguridad de la información			Es imprescindible la establecer a través de un documento todas las responsabilidades de seguridad de la información	
A.6.1.4	Proceso de autorización para las instalaciones de procesamiento de información	x		Es importante implementar un procedimiento en el que se gestionen todas las autorizaciones para el procesamiento de información	
A.6.1.5	Acuerdos de confidencialidad	x		Es necesario definir acuerdos de confidencialidad en los contratos laborales, dichos acuerdos se establecerán sobre la no divulgación de información	
A.6.1.6	Contacto con autoridades	x		Se debe mantener un contacto con las autoridades de la dirección con el fin de monitorear todos los procesos que se realizan	
A.6.1.7	Contacto con grupos de interés especial		x		No es aplicable debido a que la empresa no tiene interés en establecer contacto con terceros ya que la información se maneja internamente con los responsables del departamento de TIC's del CIDFAE
A.6.1.8	Revisión independiente de la seguridad de la información	x		Es imprescindible realizar una revisión periódica de manera independiente de los objetivos de control, controles, políticas y procedimientos de la seguridad de la información.	

A.6.2 Partes externas					
A.6.2.1	Identificación de los riesgos relacionados con partes externas		x	Es importante establecer normas y controles relacionado al acceso de entidades externas que ofrecen sus productos o servicios, así como de otros usuarios que solicitan alguna información de la empresa	
A.6.2.1	Tener en cuenta la seguridad cuando se trata con clientes		x		
A.6.2.3	Tener en cuenta la seguridad en los acuerdos con terceras partes		x		

A.7 GESTIÓN DE ACTIVOS					
A.7.1 Responsabilidad sobre los activos					
SECCIÓN	CONTROLES ISO 27001	APLICABILIDAD		JUSTIFICACIÓN DE APLICABILIDAD	JUSTIFICACIÓN DE EXCLUSIÓN
		SI	NO		
A.7.1.1	Inventario de activos		x		Actualmente la empresa cuenta con este apartado
A.7.1.2	Propiedad de los activos		x		La empresa cuenta con el personal responsable que tiene a cargo todos los activos informáticos
A.7.1.3	Uso aceptable de los activos	x		Es indispensable implementar normas para el uso aceptable de los activos informáticos y de los activos asociados al procesamiento de la información	
A.7.2 Clasificación de la información					
A.7.2.1	Directrices de clasificación	x		Es importante que en el departamento de TIC's se disponga de un plan para la clasificación de la información de acuerdo a su valor, legalidad, y sensibilidad para la empresa	
A.7.2.2	Etiquetado y manejo de la información	x		Es indispensable establecer un proceso para el etiquetado de información de acuerdo con las directrices del plan de clasificación	

A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS					
A.8.1 Previo al empleo					
SECCIÓN	CONTROLES ISO 27001	APLICABILIDAD		JUSTIFICACIÓN DE APLICABILIDAD	JUSTIFICACIÓN DE EXCLUSIÓN
		SI	NO		
A.8.1.1	Roles y responsabilidades	x		Es necesario documentar los roles y responsabilidades de seguridad de los empleados, así como la información de los mismos	
A.8.1.2	Selección		x		No existe un proceso de selección interno para elegir candidatos se eligen de acuerdo a la especialidad los militares graduados de las escuelas de formación
A.8.1.3	Términos y condiciones de la relación laboral		x		
A.8.2 Durante el empleo					
A.8.2.1	Responsabilidades de la dirección	X		Es primordial realizar una capacitación al personal del departamento de TIC's de manera adecuada y periódica mientras labore en la empresa, para garantizar la seguridad de la información	

A.8.2.2	Concientización, educación y formación en seguridad de la información	x			
A.8.2.3	Proceso disciplinario	x			
A.8.3 Finalización o cambio de la relación laboral o empleo					
A.8.3.1	Responsabilidades en la desvinculación	x		Es necesario definir las responsabilidades correspondientes a la desvinculación laboral	
A.8.3.2	Devolución de activos	x		Los empleados que no tengan ninguna relación laboral con la empresa deben devolver todos los activos que están bajo su cargo	
A.8.3.2	Remoción de derechos de acceso	x		Los derechos de acceso de un empleado deben ser removidos como consecuencia de la desvinculación laboral	

A.9 SEGURIDAD FÍSICA Y DEL AMBIENTE					
A.9.1 Áreas seguras					
SECCIÓN	CONTROLES ISO 27001	APLICABILIDAD		JUSTIFICACIÓN DE APLICABILIDAD	JUSTIFICACIÓN DE EXCLUSIÓN
		SI	NO		
A.9.1.1	Perímetro de seguridad física		x		La empresa cuenta con barreras y paredes de protección, puertas de entrada controladas por guardias de seguridad
A.9.1.2	Controles de acceso físico		x		Se cuenta con controles de seguridad en la entrada que solo se permite el acceso al personal autorizado
A.9.1.3	Seguridad de oficinas, despachos e instalaciones	x		Es necesario aplicar un diseño de seguridad física a la oficina del departamento de TIC's	
A.9.1.4	Protección contra amenazas externas y del ambiente	x		Es de vital importancia disponer de un plan de protección física ante desastres naturales para evitar daños a los equipos informáticos	
A.9.1.5	El trabajo en las áreas seguras	x		Es necesario el diseño y aplicación de plan de protección física para laborar en áreas seguras	

A.9.1.6	Áreas de acceso público, de entrega y de carga		x		No es aplicable debido a que existe una sola entrada a la empresa la misma que sirve de acceso público como también para la entrega y carga
A.9.2 Seguridad del equipamiento					
A.9.2.1	Ubicación y protección del equipamiento	x		Es necesario la ubicación y protección del equipamiento informático, para evitar amenazas	
A.9.2.2	Elementos de soporte	x		Es necesario que la empresa requiera contratar un suministro de energía propio, en el departamento de TIC's, para que no se vea afectado la falta de energía eléctrica y así garantizar el normal funcionamiento de los servidores	
A.9.2.3	Seguridad en el cableado	x		Es indispensable proteger todo el cableado de energía eléctrica y de transmisión de datos ante posibles interferencias y otras interrupciones	
A.9.2.4	Mantenimiento del equipamiento	x		Es de vital importancia la elaboración y la aplicación de un plan de mantenimiento en tiempos periódicos para garantizar la disponibilidad e integridad de la información	
A.9.2.5	Seguridad del equipamiento fuera de las instalaciones de la organización		x		No es aplicable debido a que no se puede justificar la salida de los equipos fuera de la empresa

A.9.2.6	Seguridad en la reutilización o eliminación de equipos	x		Los equipamientos que tengan unidades de almacenamiento deben revisarse para aseverar que todos los datos se hayan removido en su totalidad o a su vez se haya sobrescrito con seguridad	
A.9.2.7	Retiro de bienes	x		Debe existir un control de autorización para el retiro del equipamiento, de la información o del software en utilización en el departamento de TIC's	

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES					
A.10.1 Procedimientos operacionales y responsabilidades					
SECCIÓN	CONTROLES ISO 27001	APLICABILIDAD		JUSTIFICACIÓN DE APLICABILIDAD	JUSTIFICACIÓN DE EXCLUSIÓN
		SI	NO		
A.10.1.1	Procedimientos documentados de operación	x		Es necesario que los procedimientos de operación este debidamente documentados para ponerlos a disposición de los demás	
A.10.1.2	Gestión de cambios	x		Se debe llevar un control de todos los cambios que se realicen en los sistemas de información.	
A.10.1.3	Segregación de tareas	x		Es necesario separar las tareas en conjunto con las áreas responsables para evitar modificaciones no autorizadas	
A.10.1.4	Separación de los recursos para desarrollo, prueba y producción	x		Se debe separar los recursos para desarrollo, prueba y producción para evitar el acceso no autorizado a las instalaciones de procesamiento de información	
A.10.2 Gestión de la entrega del servicio por terceras partes					
A.10.2.1	Entrega del servicio	x		Se debe revisar y asegurar que los controles de seguridad, y las normas de entrega del servicio son implementados y operados por terceras partes	
A.10.2.2		x			

	Supervisión y revisión de los servicios por terceras partes			Es Indispensable supervisar y revisar los servicios, sobre todo los informes proporcionados por terceras partes, esto debe realizarse periódicamente para posteriormente realizar auditorias	
A.10.2.3	Gestión de cambios en los servicios de terceras partes	x		Se debe gestionar todos los cambios en los servicios, incluyendo el mantenimiento y las políticas de seguridad de la información, así como los controles y procesos	
A.10.3 Planificación y aceptación del sistema					
A.10.3.1	Gestión de la capacidad	x		Para asegurar el desempeño y eficacia del sistema, se debe supervisar y adaptar la utilización de recursos.	
A.10.3.2	Aceptación del sistema	x		Es necesario definir criterios de aceptación para nuevos sistemas de información, mediante la realización de pruebas al sistema, en el momento de su desarrollo y antes de la aceptación del mismo	
A.10.4 Protección contra código malicioso y código móvil					
A.10.4.1	Controles contra código malicioso	x		Es de vital importancia implementar controles de detección de ataques a través de la utilización de herramientas informáticas para garantizar la protección contra códigos maliciosos	

A.10.4.2	Controles contra código móvil	x		Se debe garantizar la seguridad del código móvil autorizado, que opera bajo alguna política de seguridad, y se debe evitar la ejecución de código móvil no autorizado	
A.10.5 Respaldo					
A.10.5.1	Respaldo de la información	x		Es Indispensable la realización de las copias de seguridad para garantizar que la información esté disponible en todo momento en caso de ocurrir algún incidente.	
A.10.6 Gestión de la seguridad de red					
A.10.6.1	Controles de red	x		Es necesario el control y gestión de la red para garantizar la integridad y confidencialidad de la información	
A.10.6.2	Seguridad de los servicios de red	x		Se debe identificar los niveles del servicio, las características de seguridad y los requerimientos de gestión de todos los servicios de red.	
A.10.7 Manejo de los medios					
A.10.7.1	Gestión de los medios removibles	x		Debe implementarse procesos para gestionar los medios removibles	
A.10.7.2	Eliminación de los medios	x		Se debe utilizar procedimientos para eliminar los medios de forma segura cuando ya no se necesario utilizarlos	

A.10.7.3	Procedimientos para el manejo de la información	x		Es necesario definir procedimientos para utilizar y almacenar la información para evitar su uso indebido	
A.10.7.4	Seguridad de la documentación de sistemas	x		Se debe garantizar la protección de la documentación de sistemas para evitar el acceso no autorizado	
A.10.8 Intercambio de información					
A.10.8.1	Políticas y procedimientos para intercambio de información		x		No se aplica, la información que se maneja en el departamento de TIC's es ajena a terceras personas y se maneja internamente en la empresa
A.10.8.2	Acuerdos de intercambio		x		
A.10.8.3	Medios físicos en tránsito		x		
A.10.8.4	Mensajería electrónica.	x		Es indispensable garantizar la seguridad de toda la información involucrada en la mensajería electrónica	
A.10.8.5	Sistemas de información de negocio	x		Es necesario establecer políticas y procesos para garantizar que la información relacionada con la interconexión de los sistemas de información sea seguros.	

A.10.9 Servicios de comercio electrónico					
A.10.9.1	Comercio electrónico		x		No aplica debido a que la empresa no maneja sistemas de compra y venta en línea
A.10.9.2	Transacciones en línea		x		
A.10.9.3	Información accesible públicamente		x		
A.10.10 Seguimiento					
A.10.10.1	Registros de auditoría	x		Es necesario establecer registros de auditoria durante un periodo establecido para todas las actividades de los usuarios para garantizar el apoyo y supervisión de los controles de acceso	
A.10.10.2	Supervisión del uso de sistemas	x		Para mantener el uso eficaz de los sistemas de información se debe implementar procesos de monitoreo del uso de la infraestructura de procesamiento de información.	
A.10.10.3	Protección de la información de registros (logs)	x		Se debe garantizar la seguridad de la información de registros para evitar alteraciones y accesos no autorizados	
A.10.10.4	Registros del Administrador y el operador	x		Se deben registrar todas las actividades del administrador y operador del sistema	

A.10.10.5	Registro de fallas	x		Es necesario registrar y analizar todos los registros de fallas de los sistemas de información para posteriormente tomar las acciones correspondientes	
A.10.10.6	Sincronización de relojes	x		Se deben sincronizar los relojes de los sistemas de información con un horario planificado y confiable	

A.11 CONTROL DE ACCESO					
A.11.1 Requisitos de negocio para el control del acceso					
SECCIÓN	CONTROLES ISO 27001	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD**	**JUSTIFICACION DE EXCLUSIÓN**
		SI	**NO**		
A.11.1.1	Política de control de acceso	x		Es necesario la elaboración de un documento en el que se establezca la política de control de acceso a las instalaciones como a los recursos de la empresa para garantizar la integridad de la información.	
A.11.2 Gestión del acceso de usuarios					
A.11.2.1	Registro de usuarios	x		Se debe implementar un procedimiento de registro y cancelación para otorgar y revocar los accesos a todos los sistemas de información	
A.11.2.1	Gestión de privilegios	x		Es necesario gestionar los privilegios de los usuarios para controlar y restringir el acceso a los sistemas de información	
A.11.2.3	Gestión de contraseñas del usuario	x		Se debe llevar un control de todas las contraseñas asignadas a los usuarios.	
A.11.2.4	Revisión de los derechos de acceso de los usuarios	x		Es necesario establecer una revisión periódica de los derechos de acceso de los usuarios por parte de la dirección.	
A.11.3 Responsabilidades del usuario					
A.11.3.1	Uso de contraseñas	x		Los usuarios deben establecer contraseñas fuertes y seguras para evitar vulnerabilidad a los sistemas de información	

A.11.3.2	Equipo de usuario desatendido	x		Los equipos desatendidos se les deben dar la debida protección y cuidado	
A.11.3.3	Política de escritorio y pantalla limpios	x		Es necesario implementar una política de limpieza para el escritorio y para la pantalla	
A.11.4 Control de acceso a redes					
A.11.4.1	Políticas sobre el uso de servicios en red	x		Se debe tener un control sobre el acceso directo a los servicios en red para los usuarios autorizados	
A.11.4.2	Autenticación de usuarios para conexiones externas	x		Se debe controlar el acceso de usuarios remotos a través de procedimientos de autenticación	
A.11.4.3	Identificación de equipamiento en la red	x		Es necesario identificar el equipamiento para considerarla como un factor de autenticación a los equipos conectados a la red	
A.11.4.4	Protección de puertos de diagnóstico y configuración remotos	x		Es indispensable el diagnóstico y configuración de los puertos para controlar el acceso y flujo de la información	
A.11.4.5	Separación en redes	x		Los grupos de trabajo, los servicios, los usuarios y los sistemas de información deben separarse en redes.	
A.11.4.6	Control de conexión de red	x		Los usuarios conectados en la red deben estar restringidos en las redes compartidas especialmente de la red de la dirección	

A.11.4.7	Control de enrutamiento de red	x		Es necesario la elaboración e implementación de controles de enrutamiento para la red, para garantizar la seguridad de las conexiones entre computadores	
A.11.5 Control de acceso al sistema operativo					
A.11.5.1	Procedimientos de conexión (log-en) seguros	x		Es indispensable controlar el acceso a los sistemas operativos a través de un proceso de conexión seguro	
A.11.5.2	Identificación y autenticación de usuarios	x		Es vital elegir un método de autenticación para verificar la identidad de un usuario	
A.11.5.3	Sistema de gestión de contraseñas	x		Se debe utilizar los sistemas de gestión de contraseñas para garantizar la seguridad de las contraseñas, dichos sistemas deben ser interactivos y fáciles de utilizar	
A.11.5.4	Uso de utilitarios (utilities) del sistema	x		Se debe controlar y restringir el uso de utilitarios informáticos	
A.11.5.5	Desconexión automática de sesiones	x		Se debe programar el apagado del equipo cuando existan sesiones inactivas durante un periodo determinado	
A.11.5.6	Limitación del tiempo de conexión	x		Es necesario restringir los tiempos de conexión, para garantizar la seguridad en los sistemas de información	
A.11.6 Control de acceso a la información y a las aplicaciones					
A.11.6.1	Restricción de acceso a la información	x		Se debe restringir el acceso a la información a usuarios ajenos a los procesos.	

A.11.6.2	Aislamiento de sistemas sensibles	x		Los sistemas sensibles deben estar aislados a entornos dedicados para el procesamiento de la información.	
A.11.7 Informática móvil y trabajo remoto					
A.11.7.1	Informática y comunicaciones móviles	x		Es necesario establecer una política como medida de seguridad, y así evitar riesgos a causa del uso de recursos informáticos	
A.11.7.2	Trabajo remoto	x		Se debe adoptar una política para desarrollar procesos y planes operativos para actividades de teletrabajo	

A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN					
A.12.1 Requisitos de seguridad de los sistemas de información					
SECCIÓN	CONTROLES ISO 27001	APLICABILIDAD		JUSTIFICACIÓN DE APLICABILIDAD	JUSTIFICACION DE EXCLUSIÓN
		SI	NO		
A.12.1.1	Análisis y especificación de requisitos de seguridad	x		Se deben coordinar y especificar los requisitos con el jefe del departamento de TIC's	
A.12.2 Procesamiento correcto en las aplicaciones					
A.12.2.1	Validación de los datos de entrada	x		Es necesario validar los datos de entrada para evitar datos incorrectos e inapropiados.	
A.12.2.1	Control de procesamiento interno	x		Se deben establecer revisiones en la validación para facilitar la detección de datos corruptos.	
A.12.2.3	Integridad de los mensajes	x		Para garantizar la seguridad en la integridad de los mensajes se debe identificar los requisitos de autenticación.	
A.12.2.4	Validación de los datos de salida	x		Es necesario validar los datos de salida para evitar datos incorrectos en el almacenamiento de la información	
A.12.3 Controles criptográficos					
A.12.3.1	Política sobre el uso de controles criptográficos	x		Se debe establecer una política sobre la utilización de controles criptográficos para garantizar la seguridad de la información	
A.12.3.2	Gestión de llaves	x		Es necesario el apoyo sobre la utilización de métodos criptográficos a través de un sistema de gestión de llaves	

A.12.4 Seguridad de los archivos del sistema					
A.12.4.1	Control del software en producción	x		Para garantizar la instalación del software en los sistemas de producción se deben establecer procesos de control y seguridad	
A.12.4.2	Protección de los datos de prueba del sistema	x		Se debe proteger y controlar los datos de prueba del sistema.	
A.12.4.3	Control de acceso al código fuente de los programas	x		Es necesario establecer la restricción de acceso al código fuente de los programas	
A.12.5 Seguridad en los procesos de desarrollo y soporte					
A.12.5.1	Procedimientos de control de cambios	x		Es necesario documentar los cambios realizados de los procedimientos realizados para evitar fallas en el software y en los sistemas de información	
A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	x		Se deben revisar de manera técnica las aplicaciones del departamento de TIC'S, para garantizar que no exista consecuencias en los procesos operativos.	
A.12.5.3	Restricciones en los cambios a los paquetes de software	x		Se debe determinar un control estricto de todos los cambios, estableciendo que cambios deben realizarse y hasta qué punto son necesarios	

A.12.5.4	Fuga de información	x		Es indispensable controlar la seguridad en los procesos de los sistemas evitar la fuga de información, y así garantizar la confidencialidad de la información	
A.12.5.5	Desarrollo externo de software	x		Es necesario realizar un monitoreo y supervisión del desarrollo del software contratado externamente por la empresa	
A.12.6 Gestión de la vulnerabilidad técnica					
A.12.6.1	Control de vulnerabilidades técnicas	x		Se debe documentar la evaluación de vulnerabilidades encontradas en los sistemas de información que se utilizan en el departamento de TIC's, también se debe analizar el nivel de exposición de la empresa a la que está expuesto la empresa, finalmente se debe tomar las medidas correspondientes para afrontar el riesgo su citado	

A.13 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN					
A.13.1 Reporte de eventos y debilidades de seguridad de la información					
SECCIÓN	CONTROLES ISO 27001	APLICABILIDAD		JUSTIFICACIÓN DE APLICABILIDAD	JUSTIFICACION DE EXCLUSIÓN
		SI	NO		
A.13.1.1	Reporte de eventos de seguridad de la información	x		Los procedimientos de seguridad de la información se deben informar a la dirección principal	
A.13.1.2	Reporte de las debilidades de seguridad	x		Es indispensable analizar y reportar de forma inmediata cualquier vulnerabilidad en la seguridad de los sistemas de información.	
A.13.2 Gestión de incidentes y mejoras en la seguridad de la información					
A.13.2.1	Responsabilidades y procedimientos	x		Es necesario definir responsabilidades y procedimientos para garantizar una respuesta rápida, metódica y eficaz ante problemas de seguridad.	
A.13.2.2	Aprendiendo de los incidentes de seguridad de la información	x		Se debe optar procedimientos para garantizar que los costos de los incidentes de seguridad su citados sean medidos y monitoreados.	
A.13.2.2	Recolección de evidencia	x		Es indispensable recolectar la evidencia y presentarla de acuerdo con las reglas y normativas establecidas.	

A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO					
A.14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio					
SECCIÓN	CONTROLES ISO 27001	APLICABILIDAD		JUSTIFICACIÓN DE APLICABILIDAD	JUSTIFICACION DE EXCLUSIÓN
		SI	NO		
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	x		Es necesario desarrollar un proceso para la continuidad del negocio en el que se incluya los requerimientos de seguridad de la información.	
A.14.1.2	Continuidad del negocio y evaluación de riesgos	x		Es indispensable analizar e identificar los eventos que se puedan suscitar y que puedan surgir interrupciones y dificultades en los procesos de la continuidad del negocio.	
A.14.1.2	Desarrollo e implementación de planes de continuidad que incluyen seguridad de la información	x		Es de suma importancia documentar los procesos y controles respectivos para garantizar el resguardo y la continuidad del negocio que posteriormente permitirán solucionar inconvenientes en caso de suscitarlos.	
A.14.1.4	Estructura para la planificación de la continuidad del negocio	x			
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	x		Es necesario realizar una revisión periódica de los planes de continuidad del negocio, también es necesario mantenerlos actualizados con la finalidad de verificar su validez y eficacia.	

A.15 CUMPLIMIENTO					
A.15.1 Cumplimiento de los requisitos legales					
SECCIÓN	CONTROLES ISO 27001	APLICABILIDAD		JUSTIFICACIÓN DE APLICABILIDAD	JUSTIFICACION DE EXCLUSIÓN
		SI	NO		
A.15.1.1	Identificación de la legislación aplicable	x		Se debe establecer un documento en el que los reglamentos y estatutos se mantengan actualizados en cada sistema de información.	
A.15.1.2	Derechos de propiedad intelectual (DPI)	x		Es indispensable establecer procedimientos para garantizar el cumplimiento de los reglamentos sobre la utilización de recursos y de software patentado	
A.15.1.3	Protección de los registros de la organización	x		Es necesario promover buenas prácticas con respecto a la seguridad de los registros de acuerdo a los requisitos legales.	
A.15.1.4	Protección de los datos y privacidad de la información personal	x		Se debe garantizar la seguridad y privacidad de los datos como se exige en la legislación y reglamentación contractual.	
A.15.1.5	Prevención del uso inadecuado de las instalaciones de procesamiento de la información	x		Es necesario prevenir el uso inadecuado de las instalaciones de procesamiento de la información por parte de los usuarios	

A.15.1.6	Regulación de los controles criptográficos	x		Se debe implementar métodos de cifrado para garantizar la seguridad de la información de acuerdo a las leyes y regulaciones	
A.15.2 Cumplimiento de políticas y normas de seguridad y cumplimiento técnico					
A.15.2.1	Cumplimiento de las políticas y normas de seguridad	x		El jefe del departamento de TIC's debe revisar y controlar periódicamente el cumplimiento de las políticas y normas establecidas para garantizar la seguridad de la información	
A.15.2.2	Verificación del cumplimiento técnico	x		Se debe realizar un seguimiento periódico del cumplimiento técnico de las normas de implementación de la seguridad.	
A.15.3 Consideraciones de la auditoría de sistemas de información					
A.15.3.1	Controles de auditoría de sistemas de información	x		Se debe realizar una planificación para reducir riesgos e interrupciones en los sistemas de información de acuerdo a las actividades de auditoria	
A.15.3.2	Protección de las herramientas de auditoría de sistemas de información	x		Es indispensable preservar el acceso seguro a las herramientas de auditoria para prevenir peligros y amenazas a los sistemas de información	

Tabla 18: Declaración de Aplicabilidad

Fuente: Elaboración Propia

C Verificar

C.1 Ejecutar procedimientos de seguimiento y revisión de controles.

A continuación, se presenta los formatos elaborados con la finalidad de cumplir con las buenas prácticas de acuerdo con la norma ISO 27001 y garantizar la seguridad en los sistemas de información

REGISTRO DE USO DEL CIFRADO Versión: Fecha: Código:					
N°	Unidades de Almacenamiento/Archivo/Carpeta/Mensajes	Necesita Cifrado		Tipo de Cifrado utilizado	Herramienta Utilizada
		SI	NO		

Firma Responsable

Formato 1: Registro De Uso Del Cifrado
Fuente: Elaboración Propia

PROCESO PARA REALIZAR EL RESPALDO DE INFORMACIÓN	
Versión: Fecha: Código:	
RESPONSABLE	
Nombres y Apellidos	
Cargo	
Correo	
TIPO DE INFORMACIÓN A RESPALDAR	
Fuente de datos: (Carpetas, documentos Word, Excel, Base de datos SQL, Logs, Archivos del sistema, etc.)	
Respaldo alojado en unidades compartidas: (Especificar la ruta Ejemplo: C:\Program Files (x86)\Documento.doc)	
Indicar los archivos a los cuales se les realizará el respaldo: (Listar todos los archivos a respaldar)	
INFORMACIÓN DEL SERVIDOR A RESPALDAR	
Nombre del Servidor	
IP del Servidor	
Sistema Operativo	
Tipo de Respaldo	
Tamaño Información a respaldar MB, GB, TB	
DETALLE DEL RESPALDO	
Tipo de Respaldo: (Completa, Diferencial, Incremental)	
Frecuencia de Respaldo: (Diario, Semanal, Mensual, Anual)	
Horario	

Firma Responsable

Formato 2: Proceso Para Realizar El Proceso De Backup
Fuente: Elaboración Propia

PLAN DE MANTENIMIENTO DE EQUIPOS INFORMÁTICOS

Versión:
Fecha:
Código:

	RESPONSABLE:				PRIMER SEMESTRE						SEGUNDO SEMESTRE					
N°	EQUPO	ACTIVIDAD	FRECUENCIA	SEMANA INICIO	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE

Firma Responsable

Formato 3: Plan de Mantenimiento de Equipos Informáticos
Fuente: Elaboración Propia

CLASIFICACION DE LA INFORMACIÓN Versión: Fecha: Código:										
	Registro Información del Activo				Criticidad					
Nombre del Activo	Descripción Activo	Sistema Involucrado	Nivel de Confidencialidad (Información pública Reservada, Información pública Clasificada, Información pública, No clasificada)	Propietario del Activo	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor**	**Nivel de Tasación**	Fecha de Inventario

Firma Responsable

Formato 4: Clasificación de la información
Fuente: Elaboración Propia

CONTROL DE ACCESO A LOS SERVIDORES DE ARCHIVOS YBASE DE DATOS

Versión:
Fecha:
Código:

N°	Usuario	Correo Usuario	Cargo Usuario	IP Usuario	IP Servidor	Fecha Inicio	Fecha Finalización	Servicio	Estado (Vigente/Cerrado)

Firma Responsable

Formato 5: Control Acceso a los servidores y base de datos
Fuente: Elaboración Propia

ACCESO A LOS RECURSOS COMPARTIDOS EN RED		
Versión: Fecha: Código:		
DATOS DEL RESPONSABLE:		
Departamento		
Nombre y Apellido:		
Teléfono y extensión		
Correo:		
DATOS DEL SOLICITANTE:		
Departamento		
Nombre y Apellido		
Teléfono y extensión		
Correo		
DATOS DEL RECURSO		
Nombre del servidor		
Nombre del recurso		
Ruta a la cual se solicita acceder:		
DATOS DE LOS USUARIOS		
N°	Nombres y Apellidos	Permisos Asignados
		☐Lectura ☐Escritura ☐Denegar
		☐Lectura ☐Escritura ☐Denegar
		☐Lectura ☐Escritura ☐Denegar
		☐Lectura ☐Escritura ☐Denegar

Firma Responsable Firma Solicitante

Formato 6: Acceso A Los Recursos Compartidos En Red
Fuente: Elaboración Propia

ASIGNACION DE ROLES Y RESPONSABILIDADES DEL PERSONAL DEL CIDFAE EN EL DEPARTAMENTO DE TIC's Versión: Fecha: Código:			
Nombre	Rol	Responsabilidad	Actividad

Firma Responsable

Formato 7: Asignación de roles y responsabilidades del personal del CIDFAE en el departamento de TIC's

Fuente: Elaboración Propia

INFORME DE INSTALACION DEL SOFTWARE	
Versión: Fecha: Código:	
RESPONSABLE DEL EQUIPO	
Nombre y Apellido	
Cargo	
Correo	
Departamento	
RESPONSABLE DE LA INSTALACION	
Nombre y Apellido	
Cargo	
Correo	
DATOS DEL EQUIPO INFORMÁTICO	
Nombre del Equipo	
Marca del Equipo	
Modelo del Equipo	
Nro de serie del computador	
Código de Inventario del computador	
DETALLES DEL SOFTWARE	
CARACTERISTICAS	DESCRIPCION
Nombre	
Versión	
Fabricante	
N° de serie	
Fecha de instalación	
Código de licencia	
Tipo	
Plataforma	
Lenguaje de programación	
Base de datos	
Manual de Usuario	

Firma Responsable

Formato 8: Informe de Instalación de Software
Fuente: Elaboración Propia

INFORME DE DAÑOS EN LOS EQUIPOS DE CÓMPUTO		
Versión	Fecha	Código
Usuario del Equipo		
Departamento		
DETALLE		
Hardware		
Descripción Del Daño		
Como Se Identifico El Daño		
Consecuencias Del Daño		
Acciones A Realizar		

Firma Usuario

Formato 9: Informe de Daños en los equipos de Computo
Fuente: Elaboración Propia

PLAN DE PRUEBAS DEL SISTEMA DE INFORMACIÓN		
Nombre de la Prueba	Versión:	
	Fecha:	Código:
Descripción:		
Prerrequisitos		
Procedimiento a seguir:		
Resultado esperado:		
Resultado obtenido:		

Firma Responsable

Formato 10: Plan de Pruebas del Sistema de Información
Fuente: Elaboración Propia

DIRECTORIO DE SISTEMAS DE INFORMACIÓN Versión: Fecha: Código:	
ATRIBUTO	DETALLE
Nombre del sistema	
Nombre del servicio	
Categoría (administrativo, estratégico)	
Tipo	
Proveedor	
Estado (desarrollo, prueba, producción)	
Tipo de licencia	
Fecha de expiración de la licencia	
Plataforma	
Ubicación del servidor de archivos	
Gestor de base de datos	
Responsable de la base de datos	

Firma Responsable
Formato 11: Directorio de Sistemas de Información
Fuente: Elaboración Propia

INFORME DE UTILIZACIÓN DE ANTIVIRUS EN LOS EQUIPOS Versión: Fecha: Código:	
Nombre del Equipo	
Dirección IP	
Sistema Operativo	
Usuario del equipo	
Departamento	
Tipo de Antivirus Adquirido	
Tipo de Licenciamiento	
¿Protección en Tiempo real?	
¿Actualización Automática?	
OBSERVACIONES	

Firma Responsable

Formato 12: Informe de Utilización de Antivirus en los Equipos
Fuente: Elaboración Propia

INFORME DE ANALISIS DE LAS UNIDADES DE ALMACENAMIENTO Versión: Fecha: Código:	
Datos Generales	
Departamento	
Datos del Equipo	
Nombre del Equipo	
Dirección IP	
Sistema Operativo	
Datos del Usuario	
Nombre y Apellido del Usuario	
Cargo	
Correo	
Celular	
Análisis	
Tipo de Unidad de Almacenamiento	
Tipo de Antivirus con el cual se realizó el análisis	
Tiempo de Inicio	
Tiempo de Finalización	
¿Se encontró algún tipo de virus? Procedimiento que se realizó	
OBSERVACIONES	

Firma Responsable

Formato 13: Informe de Análisis de la Unidades de Almacenamiento
Fuente: Elaboración Propia

INFORME DEL USO DE CORREO ELECTRÓNICO Versión: Fecha: Código:	
Datos Generales	
Departamento	
Datos de Usuario	
Nombre y Apellido del Usuario	
Cargo	
Correo	
Celular	
Datos del Equipo	
Nombre del Equipo	
Dirección IP	
Sistema Operativo	
Nombre y Apellido del Usuario	
¿Eliminación de mensajes spam del buzón del correo electrónico?	
¿Integración con el Antivirus?	
Medio de respaldo del correo electrónico	
OBSERVACIONES	

Firma Responsable

Formato 14: Informe del uso del correo electrónico
Fuente: Elaboración Propia

INFORME DE GESTIÓN DE LA SEGURIDAD DE LAS REDES Y DE LOS SERVIDORES Versión: Fecha: Código:	
Gestión de la Seguridad de las redes	
Topología de la Red	
Estado del funcionamiento de la seguridad NAT	
Herramienta utilizada en el monitoreo de la red	
¿Monitoreo del Uso de Antivirus?	
¿Uso de Firewall en los equipos?	
Normas establecidas en el Firewall	
¿Monitoreo de la Red LAN?	
¿Uso de un servidor Proxy?	
Gestión de la Seguridad de los Servidores	
Dirección IP	
Sistema Operativo	
¿Monitoreo de puertos en los servidores?	
Herramienta utilizada en el monitoreo de puertos	
Resultados del monitoreo de puertos	
Acciones a realizar con los resultados	
Monitoreo de los servidores	
Herramienta utilizada en el monitoreo de servidores	
Resultados del monitoreo de los servidores	
Acciones a realizar con los resultados	
OBSERVACIONES	

Firma Responsable

Formato 14: Informe de Gestión de la seguridad de las redes y de los servidores
Fuente: Elaboración Propia

FORMULARIO PARA LA CREACIÓN DE USUARIOS Y CONTRASEÑAS SOLITUD DE ACCESO A LOS EQUIPOS, A LOS CORREOS Y A LOS SISTEMAS DE INFORMACIÓN Versión: Fecha: Código:	
Datos Generales	
Departamento	
Datos del Usuario	
Nombre y Apellido del Usuario	
Cargo	
Correo	
Celular	
Perfil del usuario a crear para los Equipos informáticos	
Dirección IP	
Sistema Operativo	
Usuario	
Contraseña	
Perfil del usuario a crear para los correos institucionales	
Usuario	
Contraseña	
Perfil del usuario a crear para los Sistemas de Información	
Sistema de Información	
Usuario	
Contraseña	
¿Doble Factor de Autenticación?	
Factor de Contraseña	
Código de Seguridad a través de un teléfono móvil o correo electrónico	
OBSERVACIONES	

Firma Responsable Autoriza Firma Solicitante

Formato 15: Formulario para la Creación de Usuarios y Contraseñas
Fuente: Elaboración Propia

3.3 Desarrollo de la Propuesta

D Actuar

D.1 Plan de la Seguridad de la Información

Se elaboró el plan de seguridad informática de acuerdo a las buenas prácticas establecidas por la ISO 27001. Dicho plan de seguridad se elaboró con la finalidad de gestionar toda la seguridad y protección de la información, el cual está constituido de los siguientes puntos:

- Alcance
- Caracterización
- Análisis de riesgos
- Políticas de seguridad

D.1.1 Alcance del Plan de Seguridad Informática

A continuación, se presenta el plan de seguridad de la información el cual es aplicable en el Departamento de TIC's del Centro de Investigación y desarrollo FAE que ese encuentra ubicado en la parroquia Izamba del cantón Ambato.

Las políticas presentadas en este plan son de carácter obligatorio para todo el personal del departamento en cuestión.

D.1.2 Caracterización del Sistema Informático

El Sistema informático del CIDFAE está incluido en los medios informáticos, los cuales están constituidos por servidores, computadoras de escritorio, laptops conectadas a la red.

En el departamento de TIC's existe una red LAN, la cual abarca todas dependencias situadas en la empresa.

En cuanto a la obtención y distribución de información está disponible 4 servidores que utilizan el Sistema Operativo Windows Server 2012 R2, 2016 respectivamente, en los puestos de trabajo utilizan Windows 10.

Las principales funciones de estos servidores son: el almacenamiento de archivos, y distribución de la información a diferentes secciones. Existen 2 servidores de archivos, y 2 servidores de base de datos, los cuales están constituidos de servicios como el de correo electrónico y de proxy.

Los servicios que están en funcionamiento en la red son: la navegación web, email, recursos compartidos en red, transmisión de archivos.

Entre los sistemas y bases de datos disponibles están:

- CHASQUI documental de las fuerzas armadas y FAE(Sistema de Gestión Documental)
- ESIGEF(Sistema Contable)
- SIFFAE (sistema de control de activos fijos y control administrativo-finanzas)
- ESBYE (sistema de control de activos fijos y control administrativo-finanzas)
- Sistema Moving Map(sistema multifunción de manejo de misiones áreas)
- AGI & STK Training (sistema de simulación de sistemas espaciales)

Además, se utiliza el paquete de Office 365 para la elaboración de documentos e informes en los equipos dispuestos para el trabajo interno.

El cableado de la red está estructurado por cable UTP categoría 6, con una velocidad de transmisión de 100Mbps, con topología estrella. Las estaciones de trabajo en la empresa están agrupadas por áreas por medio de swichts.

La conexión con el exterior se la realiza desde la red principal de la FAE la cual proporciona los demás servicios de internet.

El intercambio de información a nivel interno y externo se realiza a través del servicio SMB, y a través del correo electrónico

La información ordinaria del departamento de TIC's se procesa en las mimas estaciones de trabajo y la información clasificada se encuentra en los servidores principales de la alta dirección de la FAE en la Ciudad de Quito. La información que se transmite en la red es de carácter privado.

El edificio del CIDFAE se encuentra en el cantón Ambato Tungurahua, tiene una buena infraestructura para la protección y seguridad de los equipos de cómputo.

El personal que maneja los equipos posee los conocimientos y preparación necesaria para su uso, en la mayoría de los casos poseen conocimientos medios.

D.1.3 Resultados del análisis de Riesgos

Una vez determinado el PSI, y realizado una descripción detallada del sistema informático:

Los activos informáticos más importantes a proteger son:

- La red de trabajo
- El servidor de archivos
- El servidor de base de datos
- El servicio de correo electrónico
- Las bases de datos del sistema CHASQUI
- El sistema contable y de control de activos fijos SIFFAE
- Las bases de datos del sistema Moving Map
- Las bases de datos del sistema del sistema AGI & STK Training

Las amenazas que se identificaron y que son importantes a tomar en cuenta de acuerdo al impacto en la empresa:

- Presencia de virus informáticos en los equipos
- Problemas de Pishing.
- Fuga de información
- Los equipos informáticos presentan fallas de hardware
- Falta de monitoreo en la red
- Falta de monitoreo a los sistemas de información

E Políticas de seguridad de acuerdo a las buenas prácticas establecidas por la norma ISO 27001

E.1 Área de Operaciones

Responsable: Analista de soporte técnico / Desarrollador de Software

E.1.1 Política de Contraseñas

- El personal del departamento de TIC´s requiere de un nombre de usuario y una contraseña para utilizar los sistemas de información en los equipos asignados.
- Las contraseñas no deben de ser predecibles y además son personales, dicha contraseña debe ser fuerte y debe contener caracteres, especiales, numéricos.
- Las contraseñas de los sistemas de información se cambiarán al menos 30 días.
- Si el usuario detecto que su contraseña ha sido comprometida deberá notificarla de inmediato a la persona a cargo de las cuentas de usuario.
- Las contraseñas para los equipos deben ser diferentes a las que utilicen en los sistemas de información
- Las contraseñas de correo electrónico, de red, servidores de archivos, servidores de base de datos, deben estar alineados a los requerimientos de utilización definidas.
- Los usuarios no deberán utilizar la opción de recordar las contraseñas por los navegadores web.
- Los usuarios que manejen los sistemas de información en lo posible deberán manejar gestores de contraseñas de acuerdo a su facilidad de uso.
- Si un usuario se desvincula de la empresa o caso contrario se le asigna un rol diferente, se deberá notificar al jefe del departamento de TIC's, para la suspensión o cambio mismo.
- Para sistemas críticos se deberá emplear un sistema de doble autenticación.
- El empleado debe cerrar su sesión de usuario cuando no esté en uso.

Nota: Aplicar Formato 15

E.1.2 Política del uso de correo electrónico

- Las cuentas de correo electrónico asignados al personal del área deberán ser utilizadas con fines laborales relacionados con los propósitos institucionales.
- Los usuarios son los responsables de las actividades que realizan desde sus cuentas de correo.
- La información que se transmite por correo electrónico es personal y confidencial de cada usuario.
- Revisar periódicamente el buzón de correo.
- Se debe eliminar mensajes de correo que no se estén utilizando.
- Respaldar la información contenida en el correo, se lo podrá realizar solicitando soporte.
- Si el usuario identifica un correo desconocido del remitente, deberá evitar recepción del mismo, podría contener algún archivo malicioso.
- Los buzones de correo electrónico creados para los empleados del CIDFAE, y toda la información son propiedad de la empresa.
- Se deberá borrar el correo spam, y cualquier otro correo relacionado con estas características.

Nota: Aplicar Formato 14

E.1.3 Política de la información clasificada

- Se deberá clasificar correctamente la información que se maneja, para garantizar la seguridad al acceso de la misma por parte del personal.
- Se empleará un etiquetado de acuerdo a los procedimientos requeridos para la manipulación de la información.
- Se elaborará un documento en el que se registre la información de los activos y posteriormente clasificarlos de acuerdo a la confidencialidad, integridad y disponibilidad de la información con una criticidad del 1 al 3 (1 Bajo, 2 Medio, 3 Alto), luego se realizará el promedio de los valores y se establecerá el nivel de tasación.

- Se deberá realizar una clasificación de la documentación en la cual incluirá: informes, memorándums, oficios, mensajes militares dentro del departamento de TIC's.
- Se deberá realizar una calificación de la documentación, en el cual se establecerá: reservado, confidencial, secreto, secretísimo.
- Además, se incluirá en la Calificación de la documentación la Prioridad de los documentos en la cual comprenderá: normal, ordinario, urgente, y urgentísimo.

E.1.3.1 Clasificación de acuerdo a la confidencialidad

- Información pública Reservada: Disponible solo para un proceso de la entidad, en caso de ser conocida por terceras partes sin ninguna autorización, puede surgir un impacto negativo en el ámbito legal, operativo, económico.
- Información pública Clasificada: Disponible para todos los procesos de la empresa, esta información es propia de la empresa y puede ser utilizada por todo el personal de la entidad para realizar las labores diarias, pero no puede ser conocida sin autorización a terceros.
- Información pública: Puede ser entregada sin ninguna restricción a cualquier persona dentro y fuera de la entidad.
- No clasificada: Activos que deben ser incluidos en el inventario y que posteriormente no han sido clasificados.

E.1.3.2 Clasificación de acuerdo a la Integridad

- Alta (3): Información que de ser perdida puede surgir un impacto negativo alto.
- Medio (2) Información que de ser perdida puede surgir un impacto negativo medio
- Bajo (1): Información que de ser perdida puede surgir un impacto no negativo
- No clasificada: Activos que deben ser incluidos en el inventario y que posteriormente no han sido clasificados.

E.1.3.3 Clasificación de acuerdo a Disponibilidad

- Alta (3): Si la información no está disponible puede surgir un impacto negativo alto.

- Medio (2): Si la información no está disponible puede surgir un impacto negativo medio.
- Bajo (1): Si la información no está disponible puede surgir un impacto no negativo.
- No clasificada: Activos que deben ser incluidos en el inventario y que posteriormente no han sido clasificados.

Nota: Aplicar Formato 4

E.1.4 Política de Gestión de los sistemas de Información

- Se debe realizar un monitoreo de los sistemas de información en prueba.
- Se debe elaborar un directorio de Gestión de los sistemas de Información para identificar a cada uno de los sistemas desarrollados con sus especificaciones
- El encargado de elaborar el diccionario estará a cargo del Desarrollador y su equipo de trabajo.

Nota: Aplicar Formatos 10 y 11

E.1.5 Política de Seguridad contra el software malicioso

- Se deberá utilizar el antivirus adquirido y licenciado por el CIDFAE.
- El antivirus adquirido debe ser instalado y debe mantenerse actualizado tanto en los servidores como en los equipos de los usuarios.
- Se debe habilitar el tráfico de red solo para los servicios que se requieran.
- El antivirus debe tener la capacidad de gestionar los servicios.
- Los usuarios no deberán abrir archivos de correos electrónicos de dudosa procedencia.
- Siempre se deberá revisar con el antivirus a las unidades de almacenamiento interno y a las unidades de almacenamiento extraíble como pendrives.
- Si el equipo fuese infectado con algún virus, se deberá desconectarlo de la red y se procederá a su limpieza respectiva por parte del personal encargado.
- Se debe evitar compartir directamente archivos desde discos y carpetas compartidas del equipo con permisos de lectura /escritura.

Nota: Aplicar Formato 12 y 13

E.1.6 Política del uso del software

- Mantener seguridad en las licencias tanto del Sistema Operativo como de las aplicaciones instaladas en el equipo.
- Mantener actualizados todas aplicaciones instaladas en el equipo.
- Se debe desinstalar las aplicaciones que no posean licencias.
- Las aplicaciones deberán estar aprobadas por el jefe del departamento de TIC's.
- Se debe revisar periódicamente la vigencia de la licencia adquiridas.
- El software utilizado debe ajustarse a las especificaciones técnicas del equipo.
- Se debe autorizar la instalación de cualquier software en el equipo.
- Se debe elaborar un informe de las instalaciones de los softwares aprobados para ser utilizados en los equipos.

Nota: Aplicar Formato 8

E.2 Área de Acceso

Responsable: Jefe de Mantenimiento de Informática

E.2.1 Política de recursos compartidos

- Se debe establecer el tipo de acceso que sean necesarios para acceder a la carpeta compartida ya sea de lectura, escritura.
- Se establecerá el tiempo definido durante el cual estará disponible la información en red.
- Para la información clasificada, deben establecerse carpetas designadas en el servidor de archivos y de base de datos
- Se debe restringir el acceso a las carpetas compartidas a los usuarios no autorizados.
- El acceso a las carpetas compartidas debe estar protegidas con contraseñas.
- Se debe elaborar un registro de los usuarios solicitantes del recurso compartido en red.

Nota: Aplicar Formato 6

E.2.2 Política de acceso al código fuente del sistema.

- Se debe restringir el acceso al código fuente del sistema a los usuarios no autorizados, para evitar algún robo o modificación del código.
- Si el desarrollador del sistema termina la relación laboral con la empresa deberá dejar toda la información del sistema.
- El sistema desarrollado debe pasar por una de prueba, para determinar si existen fallos.
- Se debe elaborar un plan para realizar pruebas a los sistemas de información.

E.3 Área de Navegación

Responsable: Jefe de Mantenimiento de Informática

E.3.1 Política del uso del internet

- El acceso a los servicios de internet estará sujeto a las políticas presentes.
- El acceso a los servicios de internet debe ser solicitado al departamento de TIC's con autorización de la gerencia.
- El usuario no deberá tener acceso a redes sociales, dicho control se deberá controlar con la implementación de un proxy.
- Se debe monitorear el uso del internet.

E.4 Área de Redes

Responsable: Jefe de Mantenimiento de Informática

E.4.1 Política de control de acceso a la red y a los servidores

- El encargado del departamento de TIC's otorgara el acceso a los servidores y a la red.

- Para la obtención del acceso se deberá realizar por medio de una solicitud del departamento de TIC's con los datos del empleado encargado, este deberá ser aprobado por el jefe del departamento.
- Se debe monitorear los accesos de los usuarios a los servidores y a los sistemas de información, verificando que sean los autorizados por el personal encargado.
- Se debe elaborar procedimientos de revocación de privilegios.
- Se debe elaborar un control de registro del acceso a los servidores de archivos y base de datos.

Nota: Aplicar Formato 5

E.4.2 Política de Gestión de la seguridad de las redes y de los servidores

- Monitoreo de las redes LAN dentro y fuera del departamento de TIC's.
- Verificar el uso de la seguridad y funcionamiento NAT del direccionamiento IP.
- Se debe controlar el uso adecuado de Antivirus y Firewall en los equipos.
- En cuanto a la utilización del Firewall se deberán establecer normas de tipo restrictivas, la misma que deniegue el tráfico a través de la red y se habilitará el tráfico exclusivamente para los servicios que la necesiten
- Se debe realizar un monitoreo de los puertos que se encuentren abiertos en los servidores para encontrar amenazas, y de existir amenazas que afecten la seguridad de la información se deberá corregirlos inmediatamente por el personal del departamento de TIC's.
- Se deberá realizar un seguimiento constante de los puertos abiertos para determinar la actividad de los servicios en escucha del puerto, para evitar accesos no autorizados al servidor.
- Se deberán cerrar puertos innecesarios que no se estén utilizando para evitar intrusiones al servidor.
- Se deberá realizar un análisis de vulnerabilidades a todos los servidores y equipo de la estación de trabajo para detectar posibles amenazas a la seguridad de la información.

- Si se ha encontrado vulnerabilidades en el servidor se deberán corregirlos por el responsable encargado del departamento de TIC's.
- Se deberá realizar un seguimiento constante a los servidores para determinar la actividad de los servicios, para evitar accesos no autorizados al servidor.
- Para el análisis de vulnerabilidades a los servidores y equipos se deberá emplear las herramientas tecnológicas aprobadas por el jefe del departamento de TIC's.

Nota: Aplicar Formato 14

E.5 Área de respaldo de Información

Responsable: Analista de soporte técnico

E.5.1 Política de copias de Seguridad

- El jefe del departamento de TIC's determinará los componentes más eficientes para almacenar los respaldos de la información.
- Se deberá determinar la ubicación para guardar las copias de seguridad.
- Se debe elaborar procesos de copias y procesos de comprobación para la restauración de la información.
- Se deberá cifrar la información confidencial, de esta manera se evitará el robo de información y de accesos no autorizados.
- Se debe elaborar un documento en el que se establezca como será el proceso de copias de seguridad con los datos del solicitante, de responsable y las especificaciones del servidor a respaldar.

Nota: Aplicar Formato 2

E.6 Área de Personal

Responsable: Jefe del CIDFAE

E.6.1 Política de Asignación de roles y responsabilidades

- Se deberá elaborar un documento en el que se establezcan los roles y responsabilidades de acuerdo al rol o cargo asignado mediante una lista de actividades.
- Los roles y responsabilidades de la seguridad de la información deben ser definidos clara y posteriormente comunicados al jefe del departamento de TIC’s y la dirección principal.
- Verificar que se asigne al empleado la responsabilidad asignada.
- Informar sucesos de seguridad o riesgos que podrían afectar la seguridad de la información.

Nota: Aplicar Formato 7

E.6.1.1 Rol: Jefe del CIDFAE

Responsabilidades

- Garantizar de personal competente para liderar y controlar el desarrollo de la seguridad en el departamento de TIC's.
- Supervisión de las actividades que llevan a cabo en el departamento de TIC's
- Asignar responsabilidades a los empleados de acuerdo a sus funciones.
- Implementar programas de capacitación al personal de acuerdo al trabajo en equipo, ética, y cumplimiento de valores.
- Tomar medidas de sanción en caso de incumplimiento de las normas.
- Proporcionar los recursos informáticos para el adecuado funcionamiento del departamento.
- Avalar políticas de seguridad informática de acuerdo a sus objetivos establecidos
- Velar por la seguridad del personal laboral.

E.6.1.3 Rol: Jefe TIC's

Responsabilidades

- Asignar responsabilidades a los empleados de acuerdo a sus funciones.
- Supervisión de las actividades que llevan a cabo en el departamento.
- Evaluar el estado de los activos informáticos.
- Implementar programas de capacitación al personal, en cuanto a seguridad de la información.
- Comunicación de responsabilidades con el Jefe principal.
- Gestión y organización del desarrollo de sistemas informáticos.
- Gestionar procesos de investigación.
- Elaborar un plan de trabajo del área de desarrollo de software.

E.6.1.5 Rol: Jefe de Mantenimiento de Informática

Responsabilidades

- Seguimiento diario del estado de la red.
- Control de la instalación y configuración de la red.
- Administración de la seguridad de la red.
- Detección y corrección de fallas en la red.
- Mantenimiento de la red.
- Instalación de los sistemas en red.
- Ampliación de la red.
- Diagnosticar y solucionar problemas en los dispositivos de redes como: switches y routers.
- Planifica políticas de mantenimientos de acuerdo al modelo preventivo y correctivo
- Garantizar el correcto funcionamiento de los equipos en las estaciones de trabajo
- Crear manuales de mantenimiento
- Coordina procesos con el jefe del departamento de TIC's y con el jefe principal.

E.6.1.7 Rol: Desarrollador del Software

Responsabilidades

- Analizar los requerimientos del software para la implantación requerida.
- Investigar el ciclo de vida del software a desarrollar.
- Investigar nuevas tecnologías.
- Mantenimiento de las aplicaciones, con correcciones y actualizaciones del código
- Optimizar el rendimiento de todas las aplicaciones.
- Trabajar en conjunto con los gerentes para construir y realizar una comprobación del software desarrollado.
- Documentar las aplicaciones de acuerdo a los estándares establecidos como documentos de funcionalidad, arquitectura.

E.6.1.9 Rol: Analista de soporte técnico

Responsabilidades

- Examinar el estado de los equipos y de los sistemas de información.
- Instalar los nuevos sistemas en los equipos.
- Sustitución de los equipos dañados.
- Detección de fallas en el software.
- Brindar asistencia a los demás empleados de los distintos departamentos.
- Elaborar informes del estado de los equipos y de los sistemas de información.
- Pruebas de seguridad eléctrica en los dispositivos y sistemas.
- Revisiones de seguridad en los sistemas.

E.7 Área de Seguridad Física

Responsable: Jefe TIC's

E.7.1 Política de seguridad física y ambiental

- Se debe aplicar protección física para evitar daños por incendio, inundación, terremoto u otras formas de desastres naturales.
- Se debe verificar la señalización en los distintos puntos del área de trabajo
- Se debe constatar la presencia de equipos contra incendios, ubicados en lugares estratégicos.
- Se debe implementar la instalación de equipos de seguridad y sistemas de detección de intrusos según los estándares nacionales aprobados.
- Supervisar las actividades de limpieza en el área de procesamiento de información, bajo la capacitación de limpieza del personal del TIC's.
- Al personal de servicio se le debe otorgar un acceso restringido al área de procesamiento de información
- Se debe mantener organizado e identificado todo cableado de red y de las instalaciones eléctricas.
- Verificar que no se tomen fotografías o grabaciones de video en las áreas de procesamiento de información.
- Implementar sistemas de control ambiental de temperatura y humedad, los cuales deben monitorearse de forma permanente.
- Asegurar que los dispositivos informáticos cuenten con las medidas de seguridad física y eléctrica con la finalidad de evitar daños, robo de información, o accesos no autorizados.

Nota: Aplicar Formato 7

E.8 Área de Gestión de Activos

Responsable: Jefe de Mantenimiento de Informática

E.8.1 Política del uso aceptable de los activos de información

- Los activos de información se deben ser utilizados para actividades única y exclusivamente laboral con el fin de cumplir con las actividades de la empresa.
- El personal encargado debe brindar la confidencialidad, integridad y disponibilidad de la información.
- Los activos del departamento de TIC's solo podrán ser retirados de su lugar siempre y cuando se lo autorice con una solicitud al jefe del departamento.
- Se debe elaborar un registro para gestionar todos los activos de información de acuerdo a su integridad, disponibilidad, correspondiente.

E.8.2 Política de seguridad de la eliminación o re-huso de los equipos

- Si un equipo informático ha cumplido con su vida útil, el departamento de TIC's, elaborará un informe a la dirección principal para continuar con el proceso de eliminación.
- Una vez aprobado el informe se procederá a dar de baja al equipo, trasladándolo a las bodegas de la empresa y posteriormente se realizará un respaldo de la información de las unidades de almacenamiento contenida en ese equipo, finalmente a la eliminación del activo informático.

E.9 Área de Mantenimiento y Soporte Técnico

Responsable: Analista de soporte técnico

E.9.1 Política del uso de controles de Mantenimiento de los equipos

- Se debe implementar un plan de mantenimiento preventivo de los equipos, para para garantizar el uso y vida útil de los mismos y prevenir amenazas y futuros riesgos.

- Si se presenta fallos en los equipos, se deberá realizar un mantenimiento correctivo en el menor tiempo posible para asegurar la continuidad de los procesos.
- El usuario deberá notificar cualquier problema suscitado en el equipo.
- Se realizará un proceso de mantenimiento periódico a los equipos.
- Se definirá un proceso de mantenimiento semestral distribuidas en 2 periodos, para garantizar la seguridad de la información.
- La manipulación física de los equipos estará a cargo del personal del departamento de TIC's, está prohibido la manipulación de los usuarios sin ninguna autorización.
- Se debe elaborar un informe de todos los daños en los dispositivos de cómputo.

Nota: Aplicar Formatos 3 y 9

E.9.2 Política del uso de Criptografía

- Comprobar que los sistemas de información que necesiten realizar transmisión de información cuenten con mecanismos de cifrado de datos.
- Emplear controles criptográficos para la trasmisión de datos dentro y fuera del departamento.
- Garantizar que los sistemas de información tengan establecidos controles criptográficos.
- Disponer de herramientas tecnológicas que permitan el cifrado de la información en los medios de almacenamiento.
- Las llaves de cifrado deben estar disponibles en cualquier tiempo.
- Se debe llevar un control de cifrado de las unidades de almacenamiento y de los sistemas de información.

Nota: Aplicar Formato 1

3.3.1 Aplicación de la norma de Seguridad informática ISO 27001 para optimizar la seguridad, mantenimiento y el manejo del Sistema de Gestión de Seguridad de la Información en el departamento de TIC's del Centro de Investigación y Desarrollo FAE

Una vez elaboradas las Políticas de Seguridad de la Información, se procede a realizar su aplicación actual en la institución y se determina su porcentaje de cumplimiento de las Políticas más importantes con la finalidad de optimizar la seguridad de la información.

La valoración porcentual del cumplimiento de las políticas se realizó conjuntamente con el Teniente Carlos Yagual Gutiérrez Jefe del Departamento do TIC's del Centro de Investigación y Desarrollo FAE.

3.3.1.1 Política de Seguridad contra el software malicioso

El Departamento de TIC's, aseguró de manera eficiente el tratamiento de los recursos informáticos contra el software malicioso en los sistemas operativos de los equipos informáticos, implementando controles de detección, prevención, recuperación, y el uso de antivirus con licenciamiento actualizados hasta el momento que sirven como protección contra el código malicioso, además de capacitación a los usuarios.

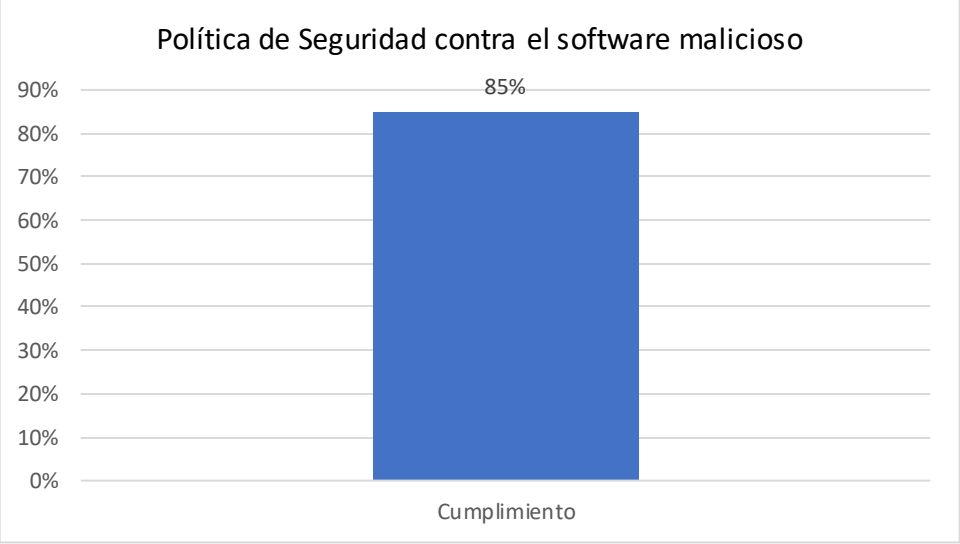


Figura 14. Política de Seguridad contra el software malicioso

Fuente: Resultado de la aplicación del Formato de Seguridad

Como se puede observar en la Figura 14. posee un nivel aceptable del 85% en cuanto al cumplimiento de la Política de Seguridad.

3.3.1.2 Política del uso de correo electrónico

El Centro de Investigación y Desarrollo FAE cuenta con el servicio de correo electrónico propio y está cumpliendo con la política de seguridad para el mismo, los cuales ha permitido el Control de mensajería anti spam, la prohibición de envío o recepción de archivos ejecutables, el Aseguramiento de direccionamiento y transporte de los mensajes y la Autorización para uso de otro tipo de mensajería instantánea o redes sociales.

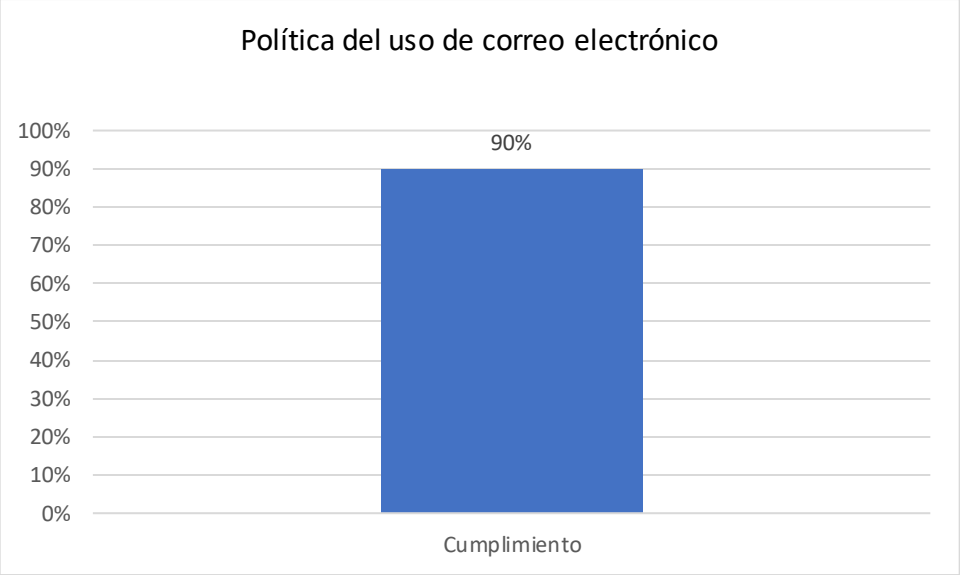


Figura 15. Política del uso de correo electrónico

Fuente: Resultado de la aplicación del Formato de Seguridad de la Información

Lo mencionado anteriormente se muestra en la Figura 15. que posee un nivel aceptable del 90% en cuanto al cumplimiento de la Política de Seguridad.

3.3.1.3 Política de Gestión de la seguridad de las redes y de los servidores

El Departamento de TIC's realiza un monitoreo constante de todas las redes en los diferentes puntos de la institución con lo cual se ha determinado hasta el momento conexiones seguras a oficinas o ubicaciones remotas, también el acceso remoto seguro a recursos compartidos en red, monitoreo de los servicios de cada uno de los servidores.

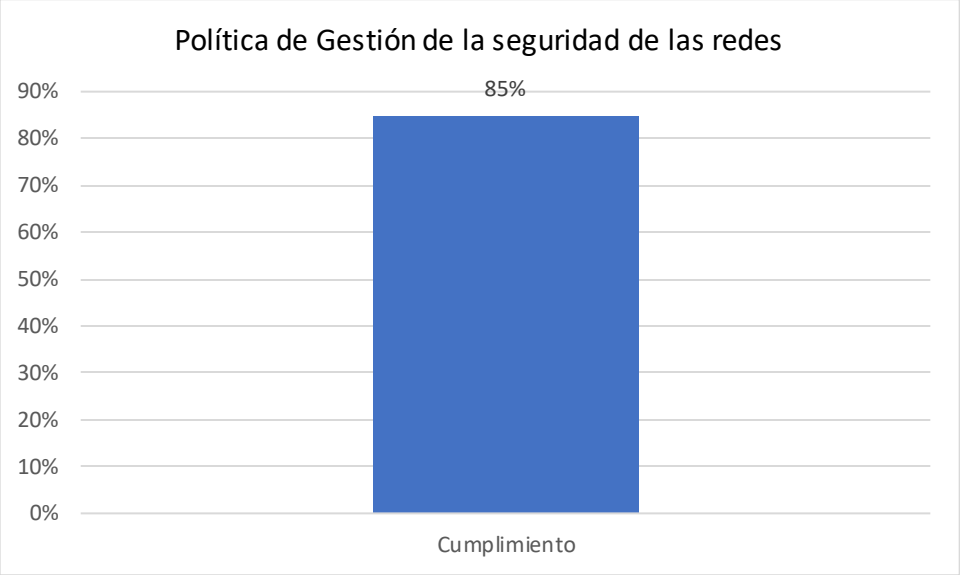


Figura 16. Política de Gestión de la seguridad de las redes

Fuente: Resultado de la aplicación del Formato de Seguridad de la Información

En la Figura 16. se puede observar que posee un nivel aceptable del 85% en cuanto al cumplimiento de la política de seguridad.

3.3.1.4 Política de Contraseñas

El departamento de TIC's realiza la gestión de las contraseñas de los usuarios para acceder a los equipos que pertenece a la institución, además de los correos institucionales y de las cuentas para acceder a los sistemas de información.

.

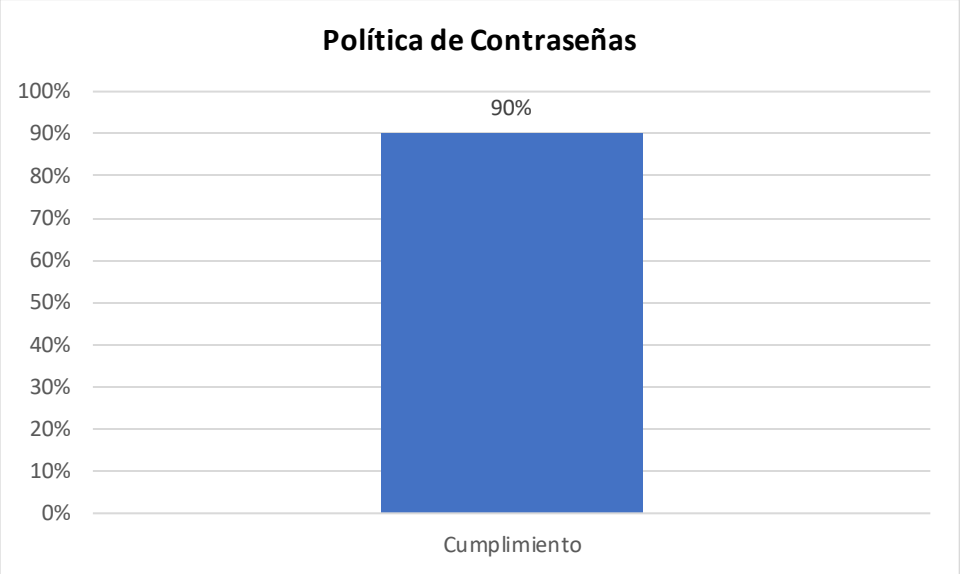


Figura 17. Política de Contraseñas

Fuente: Resultado de la aplicación del Formato de Seguridad de la Información

Como se puede observar en la Figura 17. posee un nivel aceptable del 90% en cuanto al cumplimiento de la Política de Seguridad.

CAPÍTULO IV.- CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Se evidenció que existen riesgos informáticos muy comunes tales como virus, malware, phishing y además se encontraron vulnerabilidades en los servidores los cuales ponen en riesgo la seguridad de la información, lo que no garantiza la confidencialidad, integridad y disponibilidad de la información en el Departamento de TIC's del Centro de Investigación y Desarrollo FAE.

- Se examinaron cada una de las buenas prácticas establecidos en la norma ISO 27001 para identificar y gestionar las vulnerabilidades existentes en el departamento de TIC's, de esta manera se podrá establecer políticas de seguridad que permitirán salvaguardar los activos informáticos y de información.

- Se aplicó las políticas de seguridad más importantes de acuerdo a la norma ISO 27001 las cuales tienen un porcentaje de satisfacción óptimo de cumplimiento, a través del establecimiento de políticas de seguridad permitirá optimizar la seguridad, mantenimiento y el manejo del SGSI.

- Se elaboró el plan de Seguridad de la información de acuerdo a las buenas prácticas establecidas por la norma ISO 27001 y a las necesidades de la institución, el cual ayudará a optimizar el manejo de la seguridad de la información y de los activos informáticos, lo que conllevará a mejorar la seguridad en cuanto a la confidencialidad, integridad y disponibilidad de la información en la institución.

4.2 Recomendaciones

- Es indispensable continuar con la aplicación de las políticas establecidas en el presente proyecto de investigación para garantizar la seguridad de la información.

- Es necesario brindar capacitaciones constantemente al personal del departamento de TIC's sobre el uso y el manejo de la seguridad de la información para garantizar la seguridad de la misma.

- Es fundamental salvaguardar la información en los servidores del departamento de TIC's con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información en la institución.

- La dirección principal deberá trabajar en conjunto con el departamento de TIC's en temas con respecto a la seguridad de la información para garantizar la confidencialidad, integridad y disponibilidad de la información.

- Se deberá asignar responsables para el control de cada una de las tareas de seguridad de la información que deben realizarse con la finalidad de que el encargado lleve un control de todas las actividades que se evaluarán a través de las políticas aplicadas por la institución.

MATERIALES DE REFERENCIA

Referencias Bibliográficas

[1] S. Bustamante García, M. Á. Valles Coral, I. E. Cuellar Rodríguez, and D. Lévano Rodríguez, "Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú," *Enfoque UTE*, vol. 12, no. 2, pp. 69–79, 2021, doi: 10.29019/enfoqueute.743.

[2] F. Armijos, A. Bermúdez, and N. Mora, "Cita sugerida (APA, sexta edición)," *Univ. y Soc.*, vol. 9, no. 2, pp. 313–318, 2019, [Online]. Available: http://scielo.sld.cu/pdf/rus/v11n1/2218-3620-rus-11-01-265.pdf

[3] L. R. Morales Alomoto, "Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito," 2019, [Online]. Available: http://repositorio.uta.edu.ec/handle/123456789/29216

[4] B. En, L. A. S. Normas, I. S. O. Iec, and E. N. E. L. D. De, "FACULTAD DE INGENIERÍA EN SISTEMAS , ELECTRÓNICA E INDUSTRIAL INFORMÁTICOS Tema : SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN TECNOLOGÍAS DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO INDIGENA SAC . Trabajo de Titulación Modalidad : Proyec," 2020.

[5] Y. Iso *et al.*, "Universidad De Guayaquil a En Universidad De Guayaquil Con Base En Las Normas Tutor," p. 308, 2019.

[6] D. Arcentales Fernández and X. Caycedo Casas, "Auditoría informática: un enfoque efectivo," *Dominio las Ciencias*, vol. 3, no. 3, pp. 157–173, 2017, doi: 10.23857/dom.cien.pocaip.2017.3.mono1.ago.157-173.

[7] M. Espino, *Fundamentos de auditoría*. 2014.

[8] S. Biler, "Auditoria. Elementos esenciales Audit. Essential elements Auditoria. elementos essenciais," *Dominio las Ciencias*, vol. 3, pp. 138–151, 2017, [Online]. Available: file:///C:/Users/María de los Ángeles/Downloads/379-1265-1-PB.pdf

[9] Sindicom, "Obtenido de Principios y normas de auditoría del sector público," *Com. Coord. los órganos públicos Control externo del Estado Español*, p. 33, 2002, [Online]. Available: http://www.sindicom.gva.es/web/wdweb.nsf/documento/normasauditoria/$file/PNASP.pdf

[10] W. A. Bailon Lourido, "Auditoria informática al control y mantenimiento de una infraestructura tecnológica," *Cienciamatria*, vol. 5, no. 1, pp. 73–87, 2019, doi: 10.35381/cm.v5i1.248.

[11] M. A. Abellan and G. Pardo Beneyto, "Los sistemas de información y la auditoría informática aplicados a una institución fiscalizadora subestatal: la Sindicatura de Comptes de la Comunidad Valenciana (España)," *Rev. Gestão e Secr.*, vol. 11, no. 2, pp. 120–138, 2020, doi: 10.7769/gesec.v11i2.1060.

[12] M. I. Romero *et al.*, *Mecanismo Correctivos en seguridad informática*. 2018.

[13] R. M. Slade, «"Security frameworks,",» Inf. Secur. Manag. Handbook, 2008.

[14] UNAM, "Auditoría en informática. La auditoría como actividad profesional," pp. 1–67, [Online]. Available: http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf

[15] W. Cuenca, *Gestión de la seguridad de la información basado en la Norma ISO 27001 y su incidencia en las Instituciones de educación superior de la ciudad de Machala*. 2019. [Online]. Available: http://repositorio.uta.edu.ec/bitstream/123456789/29844/1/Tesis_t1585msi.PDF

[16] T. V. Guachi Aucapiña, "Norma de Seguridad Informática ISO 27001 para mejorar la confiencialidad, integridad y disponibilidad de los sistemas de informacion y comunicación en el departamento de sistemas de la cooperativa de ahoroo y credito San Francisco LTDA"," *Repos. Univ. Técnica Ambato*, p. 162, 2012, [Online]. Available: http://repositorio.uta.edu.ec/bitstream/123456789/2361/1/Tesis_t715si.pdf

[17] E. De Contabilidad, Y. Auditoría, D. D. " Norte, O. Alejandro, and M. Cisneros, *Universidad Politécnica Salesiana Sede Quito "Efectos De La Implementación De Una Auditoría Informática a Las Empresas De Seguros a Través De La Iso 27001 :2013 Ubicadas En El Autor*. 2021.

[18] C. Lluch, "Guía de iniciación a actividad profesional; implantación de SGSI según la norma ISO 27001," *Coit*, p. 46, 2012, [Online]. Available: https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf

[19] M. J. Espona, "Calidad de Información: una nueva herramienta para la investigación," pp. 1–16, 2014, [Online]. Available: http://sedici.unlp.edu.ar/bitstream/handle/10915/44856/Documento_completo.pdf?sequence=1

[20] A. Mu *et al.*, "Sistemas de información en las empresas Sumario," no. 1970, pp. 1–34, 2007.

[21] J. Fleitman, "Negocios exitosos : cómo empezar, administrar y operar eficientemente un negocio," *La importancia los Sist. Inf. y Control en la Empres.*, 2000.

[22] J. M. Medina-Quintero and P. E. Aguilar-Gámez, "Management and information quality of SME's accounting information systems," *Cuad. Adm. (Universidad del Valle)*, vol. 29, no. 49, pp. 8–16, 2013, [Online]. Available: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-46452013000100002&lng=en&nrm=iso&tlng=es

[23] C. L. González-Valiente, "Measuring the quality of information managed: Some conceptual and methodological reflexions," *Biblios*, no. 54, pp. 42–50, 2014, doi: 10.5195/biblios.2014.149.

[24] M. J. Arévalo Haro, J. N. Cambal Condo, and V. E. Araque Cachiguango, "Gestión de la calidad en empresas de servicios: Evaluación de la empresa inmobiliaria crea en la provincia de pastaza," *Investig. Operacional*, vol. 41, no. 3, pp. 425–431, 2020.

[25] J. A. Figueroa-Suárez, R. F. Rodríguez-Andrade, C. C. Bone-Obando, and J. A. Saltos-Gómez, "La seguridad informática y la seguridad de la información," *Polo del Conoc.*, vol. 2, no. 12, p. 145, 2018, doi: 10.23857/pc.v2i12.420.

[26] M. A. Tejena-Macías, "Análisis de riesgos en seguridad de la información," *Polo del Conoc.*, vol. 3, no. 4, p. 230, 2018, doi: 10.23857/pc.v3i4.809.

[27] L. Johanna Cárdenas Solano, L. Eduardo Becerra Ardila, and H. Ernesto Martinez Ardila, "Gestión De La Seguridad De La Información," *Red Nac. Investig. y Educ. del Ecuador REDCEDIA*, pp. 1–21, 2013, [Online]. Available: http://congreso.investiga.fca.unam.mx/docs/xviii/docs/2.04.pdf

[28] S. Cohorte and S. Estrat, *INERMIú*. 2014.

[29] G. Vianey and R. Gutiérrez, "Capítulo X," no. July 2018, 2020.

[30] M. Fandos, "Formación basada en las Tecnologías de la Información y Comunicación: Análisis didáctico del proceso de enseñanza-aprendizaje," *Univ. Rovira I Virgili*, p. 341, 2003, [Online]. Available: http://www.tesisenred.net/bitstream/handle/10803/8909/Etesis_1.pdf?sequence=5

[31] E. Alcalde, "Informática Básica," 2005.

[32] R. Cañedo, R. Ramos, and J. Guerrero, "La Informática, la Computación y la Ciencia de la Información," *Acimed*, vol. 13, no. 5, pp. 1–15, 2007, [Online]. Available: http://scielo.sld.cu/pdf/aci/v15n3/aci07307.pdf

[33] R. Enap, "Informática," *Rev. do Serviço Público*, vol. 105, no. 2, pp. 315–320, 2017, doi: 10.21874/rsp.v0i2.2591.

[34] C. De Hardware, S. Operativos, B. De Datos, and I. O. General, "Conceptos Básicos".

[35] L. E. S. D. Socials, A. I. Entorn, H. Del, S. D. E. La, and P. Social, “Tema 1 . Introducció a La,” pp. 1–26, 2017.

[36] Ministerio de seguridad, “Ecuador : hacia una seguridad con enfoque integral de buen vivir Seguridad,” *Minist. Coord. Segur. Interna y Externa*, p. 8, 2015, [Online]. Available: https://repositorio.uasb.edu.ec/bitstream/10644/4125/1/Ministerio Coordinador Seguridad-Ecuador.pdf

[37] J. C. Montero Bagatella, “El concepto de seguridad en el nuevo paradigma de la normatividad mexicana,” *Región Y Soc.*, vol. 25, no. 58, 2015, doi: 10.22198/rys.2013.58.a128.

[38] L. F. Dávila L., “Conceptos y enfoques de seguridad,” *Pensam. Penal*, pp. 1–22, 2015, [Online]. Available: http://www.pensamientopenal.com.ar/system/files/2015/01/doctrina40562.pdf

[39] A. Fink, “Acerca del concepto de seguridad,” *Inst. Relac. Int.*, p. 19, 2010, [Online]. Available: https://www.iri.edu.ar/publicaciones_iri/IRI COMPLETO - Publicaciones-V05/Publicaciones/cd V congreso/ponencias/0 Fink_Acerca del concepto de seguridad.pdf

[40] J. P. Mesa Mejía, “El concepto de seguridad. Un análisis a partir de los enfoques de la seguridad pública, la seguridad ciudadana y la seguridad humana,” *Segur. y convivencia en Medellín. Aproximaciones empíricas a sus desafíos y atributos*, no. January 2015, pp. 99–127, 2015.

[41] W. E. B. R. Bolet and N. El, “Opinión,” pp. 1–23, 2017.

[42] M. C. Arias, “Implantación de un sistema de gestión de seguridad y Salud en el trabajo basado en el modelo Ecuador,” *Dominio las Ciencias*, vol. 3, no. 4, pp. 264–283, 2017, [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=6174484

[43] L. Vásquez, “Gestión integral e integrada de seguridad y salud: Modelo Ecuador ll,” *Salud Labor. concéptos y técnicas para la prevención riesgos laborales*, pp. 207–220, 2007.

[44] A. Villalba, “Título : Diseño de un Sistema de Gestión de Seguridad y Salud Ocupacional para una Empresa Química de la Ciudad de Guayaquil Title : Design of a management system occupational safety and health for a chemical company in the city of Guayaquil Autor : Álvar,” 2016.

[45] V. M. Orrego, “La gestión en la seguridad de la información según Cobit, Itil e Iso 27000,” *Rev. Pensam. Am.*, vol. 4, no. 6, pp. 21–23, 2013, [Online]. Available: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/view/57

[46] C. Ojeda, “Instituto Nacional De Formación Técnica Profesional,” *Infotep-Cienega*, pp. 10–45, 2017, [Online]. Available: http://www.infotephvg.edu.co/cienaga/hermesoft/portalIG/home_1/recursos/julio_2017/05072017/manual-sst.pdf

[47] M. González, V. C. De León, M. Espinoza, and G. Gracida, “Mejora Continua en una empresa en México: estudio desde el ciclo Deming,” *Rev. Venez. Gerenc.*, vol. 25, pp. 1863–1883, 2020, doi: 10.37960/rvg.v25i92.34301.

[48] C. Lascano Martínez, “Gestión de calidad para los procesos operativos en el área de ensamblaje del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana (CIDFAE) Ambato,” vol. 3, no. 2, pp. 124–133, 2015.