UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE INGENIERÍA DE SISTEMAS

PROPUESTA DE DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LAS ÁREAS DE EDUCACIÓN Y PROTECCIÓN SOCIAL DE LA FUNDACIÓN TIERRA NUEVA CON BASE EN LA NORMA INTERNACIONAL ISO/IEC 27001:2013

Trabajo de titulación previo a la obtención del

Título de Ingeniera de Sistemas

AUTORA: MISCHEL ESTEFANIA ESPINOZA RENGIFO

TUTOR: FRANKLIN EDMUNDO HURTADO LARREA

Quito - Ecuador

2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo Mischel Estefanía Espinoza Rengifo, con documento de identificación N° 1724186356 manifiesto que: Soy la autora y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 07 de marzo del 2022

Atentamente

Mischel Estefanía Espinoza Rengifo

1724186356

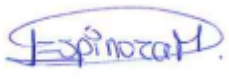
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITECNICA SALESIANA

Yo, Mischel Estefanía Espinoza Rengifo con documento de identidad N° 1724186356, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud que soy la autora del Proyecto Técnico: "Propuesta de Diseño de un Sistema de Gestión de Seguridad de la Información para las Áreas de Educación y Protección Social de la Fundación Tierra Nueva con base en la Norma ISO/IEC 27001:2013", el cual ha sido desarrollado para optar por el título de Ingeniera de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 07 de marzo del 2022

Atentamente,



Mischel Estefanía Espinoza Rengifo

1724186356

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Franklin Edmundo Hurtado Larrea, con documento de identificación N° 1713382016, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: PROPUESTA DE DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LAS ÁREAS DE EDUCACIÓN Y PROTECCIÓN SOCIAL DE LA FUNDACIÓN TIERRA NUEVA CON BASE EN LA NORMA ISO/IEC 27001:2013., realizado por Mischel Estefanía Espinoza Rengifo con documento de identificación N° 1724186356, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 07 de marzo del 2022

Atentamente,

Ing. Franklin Edmundo Hurtado Larrea, Mgtr

1713382016

DEDICATORIA

Quiero dedicar esta tesis en primer lugar a Dios por haberme permitido llegar hasta aquí hoy, por darme fuerza y salud para llevar a cabo mis metas y objetivos. Quiero dedicarles a mis padres Martha Rengifo y Jorge Espinoza, a mi hermana Katherine Espinoza, por su amor infinito, paciencia y apoyo. Siempre van a ser mi orgullo, y estaré para ustedes toda la vida.

También dedico mi tesis a toda mi familia de parte de madre y padre, en especial a Josefina Cajas, Aníbal Rengifo y Andrés Sambache, los extrañare toda una vida, ahora son unos angelitos en el cielo que nos cuidan a cada uno de la familia, sean muy felices en el cielo y compartan conmigo esta felicidad que siento al culminar mi carrera.

Finalmente, yo Mischel Espinoza me dedico esta tesis, porque fueron largos años de esfuerzo, dedicación y trabajo para llegar a este punto de mi vida, a esta felicidad que tengo, ahora vienen más metas por cumplir, más responsabilidades y es hermoso lo que a cada ser humano la vida nos tiene preparada.

AGRADECIMIENTO

Quiero expresar un sincero agradecimiento, a mis padres por su apoyo incondicional, en todo el proceso de mi carrera universitaria y que ahora está finalizando con mucho éxito. Así como también agradezco a la Universidad Politécnica Salesiana por permitirme ser parte de esta prestigiosa institución, a cada uno de los docentes que me brindaron toda su experiencia, en cada una de las materias recibidas y en especial a mi tutor el Ingeniero Franklin Hurtado, por haber aceptado ser mi guía en todo el proceso de desarrollo de este Proyecto Técnico. Agradezco también al Ingeniero Hugo Reinoso director del Área de Sistemas, a la Doctora Elena León directora del Área de Protección Social, y finalmente a la Doctora Elizabeth Pinos directora del Área de Educación de la Fundación Tierra Nueva, quienes me brindaron información referente a cada una de sus áreas y poder así cumplir con el desarrollo de mi proyecto de técnico.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En la actualidad, el mundo de la tecnología e información implica muchos retos a las empresas ante las amenazas y riesgos que infringen la integridad, disponibilidad y confidencialidad de la información, ya que, pueden afectar gravemente a las operaciones normales de las organizaciones.

Es por lo que en este proyecto de titulación se plantea la propuesta de diseño de un Sistema de Gestión de Seguridad de la Información para las áreas de Educación y Protección Social de la FTN, cuyo enfoque principal es proteger los activos de información de la FTN, en lo que respecta a las áreas citadas y con base en el estándar internacional de la ISO/IEC 27001:2013.

La norma ISO/IEC 27001:2013 sirvió como guía para este proyecto ya que permitió realizar su desarrollo acorde a los lineamientos establecidos en los controles del Anexo A, es decir se realizó un diagnóstico para comprender el estado actual en el que se encontraba la FTN, utilizando instrumentos como cuestionarios, entrevistas, lo cual permitió identificar que dominios cumplen y no cumplen y a raíz de ellos se procedió con el análisis de riesgos de la seguridad de la información y la propuesta de diseño de un SGSI.

Con la realización de este proyecto de titulación, se logró realizar una propuesta de SGSI para las áreas de Educación y Protección Social de la FTN que contiene políticas por cada dominio y controles que se deben implementar para proteger tanto sus activos de información como sus activos informáticos.

ABSTRACT

Nowadays, the world of technology and information involves many challenges to companies in the face of threats and risks that infringe the integrity, availability and confidentiality of information, since they can seriously affect the normal operations of organizations.

That is why this degree project proposes the design of an Information Security Management System for the areas of Education and Social Protection of the FTN, whose main focus is to protect the information assets of the FTN, with regard to the aforementioned areas and based on the international standard of ISO/IEC 27001:2013.

The ISO/IEC 27001:2013 standard served as a guide for this project since it allowed its development according to the guidelines established in the controls of Annex A, i.e. a diagnosis was made to understand the current state in which the FTN was, using instruments such as questionnaires, interviews, which allowed to identify which domains comply and do not comply and as a result of them we proceeded with the risk analysis of information security and the proposal for the design of an ISMS.

With the completion of this degree project, an ISMS proposal was made for the Education and Social Protection areas of the FTN, which contains policies for each domain and controls that must be implemented to protect both its information assets and its IT assets.

INTRODUCCIÓN

ANTECEDENTES

En la actualidad el manejo seguro de la información en todas las empresas ya sean públicas, privadas, con fines de lucro o sin fines de lucro es de vital importancia, debido a que hoy en día estamos expuestos a ciberataques, amenazas, vulnerabilidades, etc. que pueden llegar afectar el desempeño de las mismas, es por ello que contar con un Sistema de Gestión de Seguridad de la Información ayuda a estar preparados, ante diferentes escenarios que se puedan suscitar con relación al tipo de información que maneja cada organización, obteniendo así una correcta confidencialidad, integridad y disponibilidad de la misma que llevará a empresas a un correcto desempeño.

La Fundación Tierra Nueva fue creada por el Padre José Carollo en el año 1992, su labor inicia en los años 80 en el sur de Quito. Cuenta con tres áreas: Salud, Protección Social y Educación. Las áreas de Educación y Protección Social manejan información delicada ya que realizan proyectos de bien común para la FTN, por ende, tener es un manejo inadecuado de la información puede ocasionar efectos negativos que afectarían al funcionamiento de la FTN.

PROBLEMA

La Fundación Tierra Nueva cuenta con las áreas de Sistemas, Educación y Protección Social, al realizar un acercamiento inicial con el director del área de Sistemas, se identificó que dichas áreas manejan información crítica, poseen políticas mínimas referente a la seguridad de la información, un mínimo de controles integrados que pueden llegar a ser vulnerados.

Se pudo evidenciar también que en el año 2017 en el mes agosto se realizó una auditoría producto de la cual se obtuvieron varias conclusiones de las cuales, para fines de este proyecto de titulación, se considera relevantes las siguientes: “concluimos que la situación actual del Departamento de Sistemas presenta graves deficiencias, las cuales deberían ser rápidamente regularizadas ya que la situación actual no garantiza la integridad de las operaciones que se procesan, por lo tanto, tiene una calificación de DEFICIENTE” y “Es práctica habitual realizar cambios directamente en la base de datos, sin embargo, el parámetro de AUDIT TRAIL=NONE en la base de datos no se encuentra encendido, lo que implica la imposibilidad de rastrear e identificar posibles cambios no autorizados en temas de seguridad, la infraestructura adquirida para fortalecer la seguridad de la red ha sido vulnerada por eliminación de políticas que restringen el tráfico dentro del Firewall Fortinet, se desconoce si hubo fuga de información.” y es aquí cuando se hace evidente la vulnerabilidad en el manejo de la información que puede afectar a toda la Fundación y por consiguiente afectaría a las áreas de Educación y Protección Social que son objeto de estudio en el presente proyecto de titulación.

JUSTIFICACIÓN

La creación de un Sistema de Gestión de Seguridad de la Información para las áreas de Educación y Protección Social de la FTN con base en la norma ISO/IEC 27001, es de suma importancia debido a que permite la identificación de riesgos para gestionar controles pertinentes que ayudan a mantener la información segura.

Toda organización en la actualidad trabaja con información crítica y confidencial basada en políticas, priorización de activos de información y controles, es por ello que la elaboración del presente proyecto técnico busca solucionar la pérdida de información que existe dentro de las áreas ya mencionadas, así como también mitigar las vulnerabilidades encontradas tanto en la auditoría realizada, como en la falta de un correcto manejo de información.

El grupo que se beneficiará, son todos los colaboradores que pertenecen a la FTN, pues saben que en la actualidad las empresas u organizaciones que no posee un SGSI, tarde o temprano serán afectadas, la seguridad no es un trabajo de un solo grupo de personas, sino de toda la organización, obteniendo así una estructura de seguridad de la información correcta.

OBJETIVOS

General

Diseñar un Sistema de Gestión de Seguridad de la Información para las Áreas de Educación y Protección Social de la Fundación Tierra Nueva con base en la norma internacional ISO/IEC 27001:2013

Específicos

Analizar el contexto de la organización para el establecimiento del alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

Identificar los activos de información que tienen las áreas de Educación y Protección Social de la Fundación Tierra Nueva, además de los riesgos asociados a estos activos.

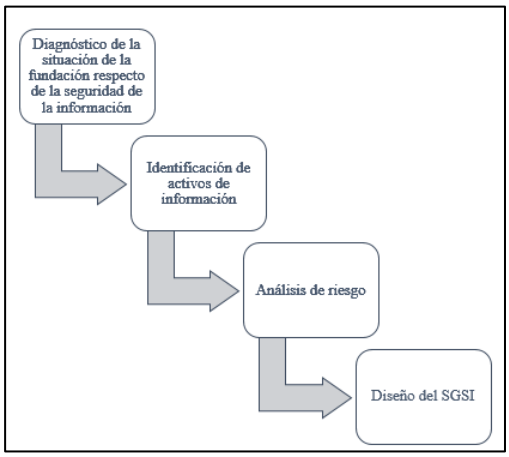
Construir la propuesta de Sistema de Gestión de Seguridad de la Información (SGSI).

METODOLOGÍA

Para la ejecución del presente proyecto de titulación se utilizó el modelo lineal secuencial o llamado modelo cascada donde se detectó la importancia de seguir una secuencia de etapas y como resultado se obtuvo un producto entregable, tal como se observa en la figura 1.

Figura 1

Modelo lineal secuencial del proyecto de titulación



Nota. Modelo lineal secuencial que describe las etapas del proyecto. Elaborado por: La autora.

Etapa1: Diagnóstico de la situación de la Fundación respecto de la seguridad de la información. Donde se utilizó como técnica la entrevista a los directores de las áreas de Educación, Protección Social y Sistemas para entender la situación inicial de cada área y como instrumento un cuestionario, el cual consta de treinta preguntas relacionadas a los catorce dominios que propone la norma ISO/IEC 27001, donde como resultado se obtuvo una matriz de cumplimiento y no cumplimiento de dominios. Todo este desarrollo fue en base a sustentos bibliográficos.

Etapa 2: Identificación de los activos de información. Donde se utilizó como técnica la entrevista para dialogar con cada una de las directoras de las áreas sobre que activos de

información, hardware, software o recursos humanos tenían y como instrumento una lista de verificación de activos, donde como resultado se obtuvo un inventario separado por activos tangibles, intangibles y recursos humanos de las áreas de Educación y Protección Social.

Etapa 3: Análisis de riesgo. Donde se utilizó como técnica la entrevista a cada una de las áreas con énfasis en el área de Sistemas, debido a que el director de la misma esta día a día con los activos que las áreas de Educación y Protección Social cuentan, y como instrumento la matriz de probabilidad e impacto donde como resultado se determinó cuáles son los riesgos más probables, cuales generan más impacto a cada uno de los activos encontrados en la etapa 2.

Etapa 4: Diseño del SGSI. Se realizó una estructura basada en investigación bibliográfica, es decir la utilización de tesis, artículos y el trabajo colaborativo con el director del área de sistemas de la FTN, debido a que se propuso como primer punto el resumen del diagnóstico realizado en el capítulo 2, la creación de política por dominio, la creación de procedimientos asociados a las políticas, la creación de instrumentos para la utilización de dominios que indica la norma ISO/IEC 27001, dominios en los que las áreas de Educación y Protección Social se encontraban en un estado de cumplimiento y no cumplimiento, se estableció una prioridad y responsables para la ejecución de la política propuesta.

Una vez que se ha tenido claridad de cuál es el contexto de las áreas de Educación y Protección Social de la FTN, además se han identificado y priorizado los activos de información y los riesgos asociados, se procede a la propuesta de diseño de un SGSI, tomando en cuenta cada una de las etapas mencionadas anteriormente.

CAPÍTULO I

1.1 MARCO TEÓRICO

1.1.1 Antecedentes investigativos

En los años 80’s cuando oficialmente se marca como el nacimiento de la red Arpa Internet y que con el paso de los años se quedaría solo con el nombre de Internet, es en donde empiezan a surgir protocolos para la transferencia de datos y a lo largo de este tiempo se han ido construyendo varios estándares para una mejora continua en los sistemas informáticos (Bahillo, 2021).

En la actualidad no se ha podido catalogar un sistema informático como un sistema perfecto esto debido a que siempre existirán brechas o vulnerabilidades en las mismas, las cuales se pueden manejar a través de la ejecución de controles para mejorar la integridad, confidencialidad y disponibilidad de la información de una organización (SGSI, 2018).

Los sistemas de información hoy en día son la adaptación tecnológica necesaria en los negocios para poder situarse y ponerse en contexto con el mundo actual, pero de la misma manera se debe tomar en cuenta varios aspectos importantes y uno de ellos es la seguridad sobre los activos de información de la empresa, por consiguiente el gerente debe ser consciente en la ejecución de un SGSI que permita llevar un continuo control sobre los activos de la organización y poder salvaguardarlos (SGSI, 2018).

1.1.2 Seguridad de la información

Considerada como la agrupación de normas y métodos que se deben usar para llevar un correcto control que permiten resguardar toda la información que tiene la empresa, evitando pérdidas significativas para las organizaciones, ya que la información son el core para las entidades es decir su actividad principal y es la que permite ejecutar sus operaciones o actividades diarias (SGSI, 2021).

La seguridad para la información es cambiante de acuerdo con el tipo de función que ejerce cada organización tales como actividades económicas, educativas, salud entre otras, pero todas comparten un objetivo en común que es la seguridad sobre su información y salvaguardar sus datos (SGSI, 2021).

1.1.2.1 ¿Qué es una falla de seguridad de la información? Hay variedades de fallas en la seguridad de la información que se presentan constantemente, pero las principales son las fallas en la seguridad de información a causa de los fraudes, luego están las fallas que pueden presentar los sistemas y finalmente las fallas generadas por los empleados.

Las fallas por fraudes generalmente son planificadas con la finalidad de perjudicar a la organización, también son mejor conocidos como ciber ataques a la seguridad de la información (Cárdenas-Solano, 2016).

Los fallos en los sistemas son errores técnicos que suceden de forma inesperada, estos problemas por lo general se resuelven de manera rápida y oportuna, la manera de evitar que se repita estos fallos es indagar cual fue la causa para así poder anticipadamente dar solución (Cárdenas-Solano, 2016).

Otra de las fallas generales se debe a erros cometidos por el personal que labora en la entidad, también suele presentarse de forma inesperada y son complicados de controlar como por ejemplo la pérdida de un documento o archivo o el registro incorrecto de información dentro de los activos de la empresa, por consiguiente, se puede minimizar este tipo de errores con políticas y normas que regulen estas fallas en la seguridad de la información (Cárdenas-Solano, 2016).

1.1.2.2 Importancia de la seguridad de la información en las organizaciones. En la actualidad para garantizar la seguridad de la información en las organizaciones es importante fortalecer tres puntos básicos que son la triada cid sobre los activos de

información ya que los riesgos y amenazas van a estar presentes todo el tiempo y es necesario tener medidas implementadas para poder evadir o minimizar el impacto de riesgo o amenaza *(HACKNOID, 2020)*.

1.1.3 Seguridad informática.

También conocida como ciberseguridad, su objetivo principal es mantener la disponibilidad, integridad y confidencialidad de la información manejada a través de las computadoras permitiendo prevenir y detectar intrusos en el uso de los recursos informáticos de la organización que tengan malas intenciones o fines lucrativos. Por consiguiente, la seguridad informática posee varias medidas de seguridad como son los programas de software de antivirus y firewalls (Muñoz, 2020).

1.1.4 Diferencia entre seguridad de la información y seguridad informática

La seguridad de la información son las técnicas, procesos que previenen y actúan sobre la protección de la información a la hora de almacenar los datos de una organización y la seguridad informática se encarga de la integridad y privacidad de la información guardada en un sistema informático, es decir la ciberseguridad abarcar no solo la protección del software sino también del hardware y la red que los comunica (LISA Institute, 2021).

1.1.5 Seguridad de los sistemas informáticos

La seguridad de los sistemas informáticos es la disciplina encargada de mantener la integridad y privacidad de los activos de información que posee una organización a través de políticas las cuales deben ser conocidas por todos los integrantes de la empresa. Además, se obtienen beneficios los cuales se centran en administrar la seguridad de los sistemas informáticos con el fin de proteger toda su estructura de ciberataques, es decir, proporcionando privacidad, protección, integridad, prevención, autenticación, productividad, control y accesibilidad (Movistar, 2015).

1.1.6 Sistema de gestión de seguridad de la información

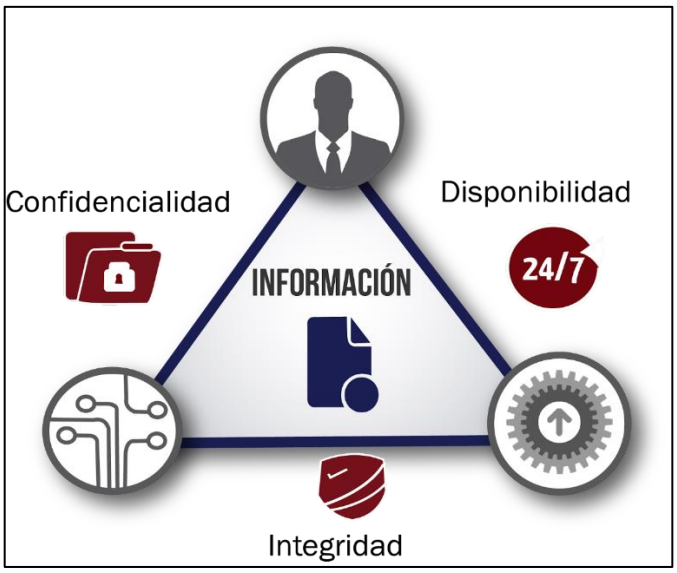
Los SGSI permiten evaluar el estado actual de una organización y diagnosticar los riesgos existentes para de esta manera poder implementar controles necesarios que minimicen los efectos negativos. Básicamente un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, métricas, procesos, herramientas e instrumentos que permiten tratar la información de la organización para reducir el riesgo y mejorar continuamente sus controles (Alvarado, 2021).

1.1.6.1 Triada CID. En el ámbito de seguridad de la información es conocida la palabra triada CID o también es conocida como la triada de la información que por sus siglas significa confidencialidad, integridad y disponibilidad, este modelo se diseñó para guiar las políticas de seguridad de la información dentro de una determinada empresa tal como lo muestra la norma ISO 27001.

Es decir que la información de cualquier empresa siempre debe velar por la confidencialidad, integridad y disponibilidad ya que es considerada un activo de suma importancias en el ámbito de la aplicación de un SGSI. A continuación, se muestra en la figura 2 la estructura de la triada CID, la cual se enfoca en que la información debe está disponible siempre 24 horas de los 7 días de la semana, así como también debe llevar un flujo apropiado es decir integra y lo más importante segura, sabiendo que persona puede tener acceso a la información que es considerada confidencial. (Alvarado, 2021).

Figura 2

Sistema de Gestión de Seguridad de la Información



Nota. Representación de la seguridad de los sistemas informáticos. Fuente: (Claudia Victoria Alvarado, 2021).

1.1.6.1.1 Confidencialidad. Son las medidas implementadas para asegurar la privacidad de los activos de información de una organización y están trazadas para reducir el riesgo de que acceda personas no autorizadas a la información confidencial y garantizando el acceso oportuno a las personas que si posean permisos *(Alvarado, 2021)*.

1.1.6.1.2 Integridad. Es la implicación de conservar la estabilidad, precisión y confiabilidad de los activos de información de la organización, mismos activos que no ser adulterados en un proceso de tránsito y que de la misma manera personas no autorizadas puedan adulterar la información *(Alvarado, 2021)*.

1.1.6.1.3 Disponibilidad. Ésta se garantiza llevando un control continuo sobre el mantenimiento de la infraestructura como por ejemplo ante la necesidad de la reparación

de un componente de hardware, sea de manera inmediata para así poder tener el entorno operativo y funcionando correctamente *(Alvarado, 2021)*.

1.1.6.2 Ciclo Deming. Es un enfoque para la gestión de calidad que permite crear, realizar, conservar y optimizar de forma continua un SGSI de una organización, facilitando la resolución de problemas de manera ordenada y sistematizada tal como se indica en la figura 4 *(Alvarado, 2021)*.

1.1.6.2.1 Plan (Planificar). En esta etapa su objetivo es definir el procedimiento que se va a mejorar y para ello se debe definir los métodos y herramientas necesarias para llevar a cabo esta fase que es la más influyente *(Alvarado, 2021)*.

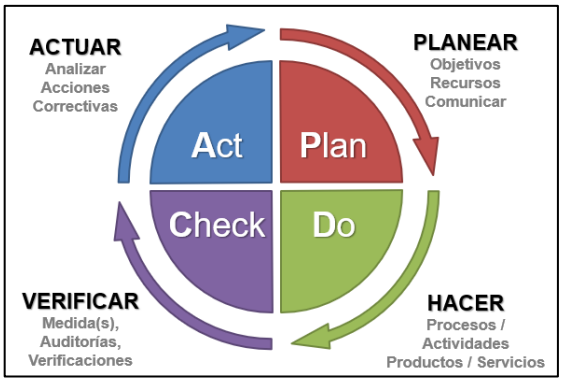
1.1.6.2.2 Do (Hacer). Esta etapa también es conocida como testeo, ya que consiste en ejecutar la acción elegida y eliminar las causas del problema *(Alvarado, 2021)*.

1.1.6.2.3 Check (Controlar). En esta fase el objetivo es inspeccionar y evaluar su desempeño o resultados *(Alvarado, 2021)*.

1.1.6.2.4 Act (Actuar). Esta es la última etapa y en esta fase se debe ajustar el plan de mejora para mantener el SGSI al máximo rendimiento *(Alvarado, 2021)*.

Figura 3

Ciclo Deming



Nota. Representación del enfoque para la gestión de calidad. Fuente: (Alvarado, 2021).

1.1.7 Etapas de un sistema de gestión de seguridad de la información

Un SGSI abarca varias etapas que direccionan a las organizaciones a cumplir con el desarrollo de tener un correcto proceso y estructura del mismo. A continuación, se detalla cada uno de los requisitos que debe cumplir la organización para asegurar la información (Alvarado, 2021).

1.1.7.1 Apoyo de la alta dirección. La alta dirección debe estar comprometida con la implementación de herramientas para integrar, comunicar y administrar la calidad y mejora del SGSI *(Alvarado, 2021)*.

1.1.7.2 Alcance del SGSI. Sirve para determinar e identificar los límites en función del entorno de trabajo de la organización que permitirá preservar la información requerida, es decir, que sin importar en donde se encuentre almacenada la información de la empresa, ya sea de forma local o en la nube es información sensible de la entidad lo cual debe estar dentro del alcance del SGSI *(Alvarado, 2021)*.

1.1.7.3 Inventario de activos de información. Esta etapa es importante ya que permite identificar todos los activos de la organización y clasificar de acuerdo con su grado de importancia entre estos activos están los datos digitales, activos tangibles, activos intangibles, tales como software, hardware y activos humanos *(Alvarado, 2021)***.**

1.1.7.4 Análisis y evaluación de riesgos. Una vez que se ha identificado todos los activos de la empresa se hace un análisis en el cual se hace la diferenciación de los activos considerados importantes y que están dentro del alcance del SGSI, posteriormente se realiza la evaluación de estos, en donde se identifica cuáles son sus

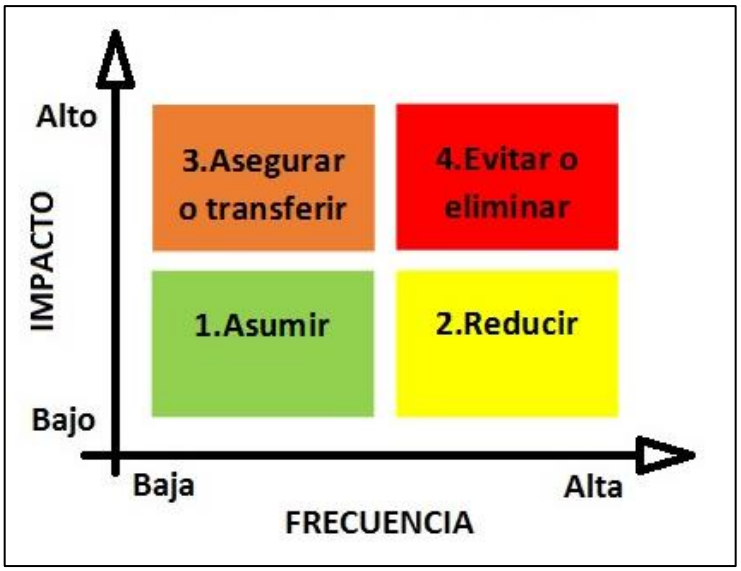
vulnerabilidades, amenazas y riesgos, por consiguiente, en el análisis y evaluación se consideran los activos tales como hardware, software y personal *(Alvarado, 2021)*.

1.1.7.5 Declaración de aplicabilidad. En esta etapa se elabora un documento el cual es muy importante en la auditoría ya que este establece el perfil de seguridad dentro de la empresa y el registro de los controles implementados para la prevención de riesgos *(Alvarado, 2021)*.

1.1.7.6 Tratamiento de riesgos. En esta fase, se realiza la selección de los controles adecuados para cada riesgo, los cuales están orientados a asumir el riesgo, reducir el riesgo, eliminar el riesgo y transferir el riesgo *(Alvarado, 2021)*.

Figura 4

Tratamiento de riesgos



Nota. Gráfico de tratamiento de riesgos. Fuente: (Claudia Victoria Alvarado, 2021).

1.1.7.6.1 Asumir el riesgo. Normalmente la organización no toma medidas de protección respecto a ese riesgo puesto que la probabilidad de que ocurra es muy baja (Alvarado, 2021).

1.1.7.6.2 Reducir el riesgo. La organización tiene que implementar varias medias que actúen para salvaguardar los activos, además toda acción debe ser documentada y administrada por la empresa *(Alvarado, 2021)*.

1.1.7.6.3 Eliminar el riesgo. Suele ser costoso para la empresa debido a que se deben eliminar los activos a los que el riesgo este asociado, esto con la finalidad de desaparecer el riesgo, solamente se aplica en los casos de que la probabilidad de ocurrencia sea muy alta *(Alvarado, 2021)*.

1.1.7.6.4 Transferir el riesgo. Esto significa que se migra el problema a alguien más como por ejemplo la contratación de una póliza de seguros que pueda indemnizar a la organización en caso de presentarse un problema, cabe recalcar que esto solo es factible si el valor del activo es superior al del propio seguro *(Alvarado, 2021)*.

1.1.7.7 Definición del diseño del SGSI. En esta etapa para la definición del diseño del SGSI se debe basar en la definición de políticas las cuales van a determinar cómo se lo va a realizar y con qué recursos. También se delega un responsable al momento de su implementación y evaluación de resultados para una posterior mejora del sistema *(Alvarado, 2021)*.

1.1.8 Norma de gestión de la seguridad de la información

Creada para brindar orientación, estructura, y sobre todo seguridad a organizaciones para el cumplimiento de objetivos es decir reducir costos y ser más efectivos (Intedya, 2015).

1.1.8.1 ISO 27000. Contiene las bases y estructura de las normas que tratan políticas que debe tener la información de organizaciones. *(Intedya, 2015)*.

1.1.8.2 ISO 27001. Esta norma presenta los requerimientos necesarios para crear y gestionar un SGSI (Intedya, 2015).

1.1.8.3 ISO 27002. Esta norma trata sobre buenas prácticas para la creación de un SGSI, a través de la utilización de dominios y controles (Intedya, 2015).

1.1.8.4 ISO 27003. Presenta una guía estructurada para la creación de un SGSI. (Intedya, 2015)**.**1.1.8.5 ISO 27004. ***Este estándar proporciona pauta orientadas a la correcta definición y establecimiento de métricas que permitan evaluar de forma correcta el rendimiento del SGSI*** **(Intedya, 2015).**

1.1.8.6 ISO 27005. Esta norma define como se debe realizar la gestión de riesgos vinculados a los sistemas de gestión de la información orientado en cómo establecer la metodología a emplear *(Intedya, 2015)*.

1.1.8.7 ISO 27006. Este estándar establece los requisitos que deben cumplir aquellas organizaciones que quieran ser acreditadas para certificar a otras en el cumplimiento de la ISO/IEC-27001 *(Intedya, 2015)*.

1.1.8.8 ISO 27007. Esta norma es una guía que establece los procedimientos para realizar auditorías internas o externas con el objetivo de verificar y certificar implementaciones de la ISO/IEC-27001 *(Intedya, 2015)*.

1.1.8.9 ISO 27008. Es un estándar define como se deben evaluar los controles del SGSI con el fin de revisar la adecuación técnica de los mismos, de forma que sean eficaces para la mitigación de riesgos *(SGSI, 2014)*

1.1.8.10 ISO 27009. Esta norma complementa la norma 27001 para incluir requisitos y nuevos controles añadidos que se aplican en sectores específicos, con el objetivo de hacer más eficaz su implantación *(Grupo ACMS, 2020)*.

1.1.9 ISO 27001

1.1.9.1 Descripción. Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la

información en una empresa. El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. También basada en temas relacionados con la gestión, investigación, y el tratamiento de riesgos.

El enfoque sistemático tiene como fin implementar un SGSI. No solo ofrece un balance apropiado entre tecnologías de información y los procesos de negocio, también requiere del involucramiento de los niveles directivos y ejecutivos de la organización, para asegurar que la implementación no solo tiene los recursos necesarios, sino que también respalda los objetivos estratégicos de la empresa.

1.1.9.2 ¿Cómo se organiza? Introducción: El propósito de esta norma es entregar los requisitos que se deben cumplir para tener un correcto sistema de gestión de seguridad de la información que cumpla con el establecimiento, implementación, mantenimiento y mejora continua *(ISO/IEC27001, 2013)*

- Alcance: Esta parte de la organización de la norma indica que entrega los requisitos para la evaluación y tratamiento de los riesgos que puede tener la información de una organización (ISO/IEC27001, 2013)
- Referencias Normativas: para la realización de un SGSI, se debe utilizar la norma ISO/IEC 27000 ya que es considerada una referencia obligatoria debido a que poseen términos y definiciones que ayudan a la ejecución de la misma (ISO/IEC27001, 2013)
- Términos y definiciones: Se encuentran en la norma ISO/IEC 27000 en la sección tres su principal objetivo es tener identificado toda la terminología y definiciones en una sola guía (ISO/IEC27001, 2013)
- Contexto de la Organización: En esta parte de la norma se identifica dos etapas, la primera es conocer cuál es el estado en el que se encuentra una organización evaluada

sus procesos internos y externos; y una segunda etapa es el conocimiento de expectativas de partes interesadas (ISO/IEC27001, 2013)

- Liderazgo: se refiere que para la correcta elaboración de un SGSI se debe contar con la responsabilidad de la alta dirección de organizaciones, ya que se debe cumplir con el establecimiento de políticas y objetivos, la comunicación de la misma a roles que se relacionas con la seguridad de la información (ISO/IEC27001, 2013)
- Planificación: enfocada en determinar riesgos y oportunidades que existen al realizar un SGSI (ISO/IEC27001, 2013)
- Soporte: Toda organización debe analizar y entregar recursos para el establecimiento, implementación, mantenimiento y mejora continua (ISO/IEC27001, 2013)
- Operación: establece requisitos para la medición del funcionamiento de un SGSI, es decir a las vulnerabilidades que pueden presentar los activos de información (ISO/IEC27001, 2013)
- Evaluación del desempeño: Toda organización debe determinar que métodos de monitoreo implementar para medir el desempeño de un SGSI (ISO/IEC27001, 2013)
- Mejora: relacionado con las no conformidades y acciones correctivas a tomar para un correcto desempeño de in SGSI (ISO/IEC27001, 2013)

1.1.9.3 ¿Cómo se gestiona? Los controles, lineamientos de seguridad que se implementan se presentan en forma de políticas, procedimientos e implementación técnica. Por ello la norma ISO 27001 detalla todos estos elementos que se debe cumplir dentro de un SGSI.

La gestión de la seguridad de la información no es solo seguridad de TI, sino también la gestión de procesos, de los recursos humanos, temas jurídicos, etc.

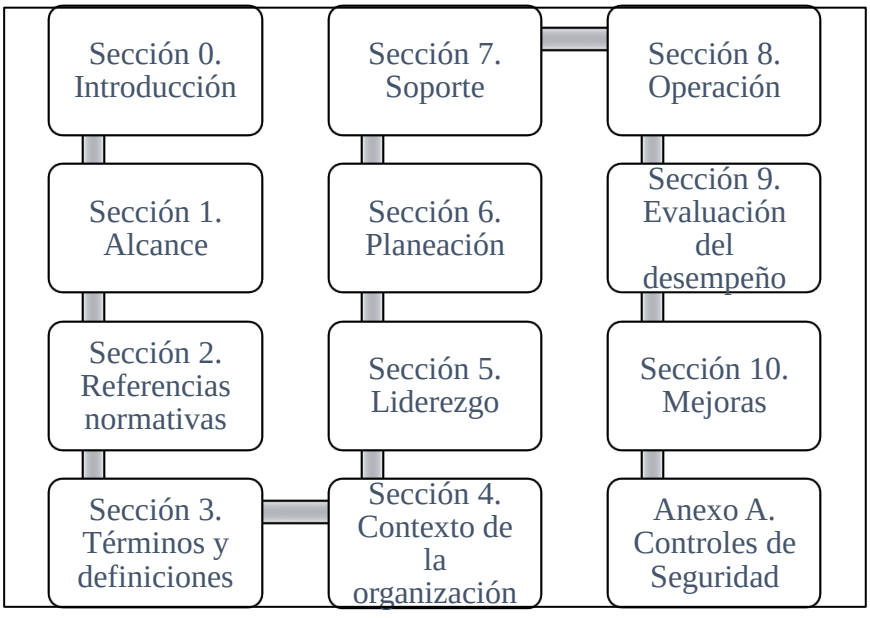
1.1.9.4 Importancia de la Norma ISO 27001. Utilizar la norma ISO/IEC 27001 en empresas u organizaciones demuestra que cuentan con un nivel de madurez alto y que la empresa ha puesto en marcha procesos de seguridad de información adecuados, es decir la aplicación de un SGSI, quiere decir que buscan que la empresa cuente con un conjunto de políticas, procedimientos, procesos y sistemas para evitar vulnerabilidades en la información.

1.1.9.5 Estructura de la Documentación

La norma ISO/IEC 27001 dentro de su anexo A se clasifica en secciones desde la cero a la tres ya que tienen que ver con la introducción y su cumplimiento no es obligatorio, las secciones 4 a 10 son obligatorias, es decir que todas las organizaciones deben ejecutarla para contar con un correcto SGSI.

Figura 5

Estructura de la documentación



Nota. Modelo estructural de la documentación del proyecto. Elaborado por: La autora, a través de (ISO/IEC27001, 2013)

1.9.1.6 Controles de seguridad. A continuación, se muestran los controles de seguridad que propone la norma ISO 27001, los cuales se tratan dentro del anexo A distribuido en catorce secciones de seguridad:

Tabla 1

Controles de Seguridad de la norma ISO/IEC 2001

N°	Control de Seguridad
A 5	Políticas de seguridad de la información
A 6	Organización de la seguridad de la información
A 7	Seguridad de los recursos humanos
A 8	Gestión de activos
A 9	Controles de acceso
A 10	Criptografía – cifrado y gestión de claves
A 11	Seguridad física y ambiental
A 12	Seguridad operacional
A 13	Seguridad de las comunicaciones
A14	Adquisición, desarrollo y mantenimiento del sistema
A 15	Relación con proveedores
A 16	Gestión de incidentes de seguridad de la información
A 17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio
A 18	Cumplimiento de los requisitos legales y contractuales

Nota. Controles de Seguridad de la norma ISO/IEC 2001. Elaborado por: La autora, a través de (INGERTEC, 2021)

1.1.10 Herramientas para la evaluación de riesgos.

Una vez que se han identificado todos los activos de la organización, existen varias herramientas que aportan en la administración de riesgos tales como: (Calle, 2020).

1.1.10.1 Lista de Verificación. Las listas de chequeo están hechas para llevar un control sobre actividades cotidianas permitiendo verificar su cumplimiento de forma ordenada y sistemática *(Opirani, 2014)*.

1.1.10.2 Cuestionario. Es una herramienta útil para la recolección de información en una organización y que a través de ésta se puede evaluar el estado actual en el que se encuentra la empresa *(QuestionPro, 2021)*.

1.1.10.3 Entrevista. Es una técnica usada para la recopilación de información que se la hace directamente el auditor al entrevistado permitiendo así obtener la información que se requiera *(Navarro, 2010)*.

1.1.10.4 Matriz de riesgo. Mediante la metodología magerit es fácil analizar y administrar los peligros de los sistemas de información mediante una tabla en donde se establece la probabilidad versus el impacto para así poder conocer el nivel de riesgo *(Opirani, 2014)*.

1.1.11 Métodos para la Evaluación de Riesgos.

Para realizar una calificación y evaluación de riesgos existen dos tipos de métodos que son el cualitativo y cuantitativo (Opirani, 2014).

1.1.11.1 Método cualitativo. Es una metodología de investigación la cual se basa en la calidad o la opinión de las personas, es decir, es convencional y este tipo de investigación no es cuantificable (Opirani, 2014).

1.1.11.2 Método cuantitativo. Es una metodología de investigación que, a través de cuestionarios, permite recoger datos cuantificables para de esta manera poder crear un análisis estadístico y convertirla en información de interés (Opirani, 2014).

1.1.12 Indicadores

Son una característica medible y específica, enfocada en mostrar progresos y cambios que tienen las organizaciones. A demás los indicadores pueden estar orientados a factores de medición como eficiencia, eficacia y efectividad, utilizados para la toma de decisiones y el acierto en mediciones repetitivas (Opirani, 2014).

1.1.12.1 Tipos de indicadores.

1.1.12.1.1 Indicador de cumplimiento. Conocidos también como indicadores de desarrollo son un conjunto de mediciones enfocados en monitorear el cumplimiento de objetivos o lineamientos de proyectos definidos en medianos y largo plazo *(Gomez, 2010)*

1.1.12.1.2 Indicador de gestión. Son valores medibles que se basan en el comportamiento y desempeño de organizaciones ayudan a la toma de decisiones a lo largo del tiempo *(Gomez, 2010)*

1.1.13 Valoración de prioridad

Establece un orden jerárquico de ejecución de lineamientos o proyectos que son manejados por organizaciones para un correcto desempeño de los mismos, de acuerdo a la matriz planteada por Eisenhower, la cual establece prioridades en función de cuatro cuadrantes, clasificando la ejecución de las tareas como importantes y urgentes.

Donde urgente es considerada aquella actividad cuyo tiempo límite está cerca a terminar e importante es considerada aquella actividad que dirige a un objetivo.

Tabla 2

Valoración de prioridad

	Urgente	No Urgente
Importante	**Cuadrante I** • Crisis • Presiones • Proyectos con fecha de vencimiento	**Cuadrante II** • Relaciones personales • Nuevas oportunidades • Planificación futuro • Actividades preventivas • Crecimiento Persona • Ocio, diversión
No Importante	**Cuadrante III** • Interrupciones • Email, reuniones, llamadas • Actividades populares • Presiones familiares	**Cuadrante IV** • Detalles • Ladrones de tiempo • Algunos mails y llamadas • Actividades placenteras

Nota. Gráfico de valoración de prioridad. Fuente: (Vispo, 2018)

CAPÍTULO II

2.1 DIAGNÓSTICO

Para iniciar con el diagnóstico o llamado también estado actual de las áreas de Educación y Protección Social es importante conocer cómo se encuentra estructurada la FTN. Por esa razón se muestra en la figura 6 su estructura.

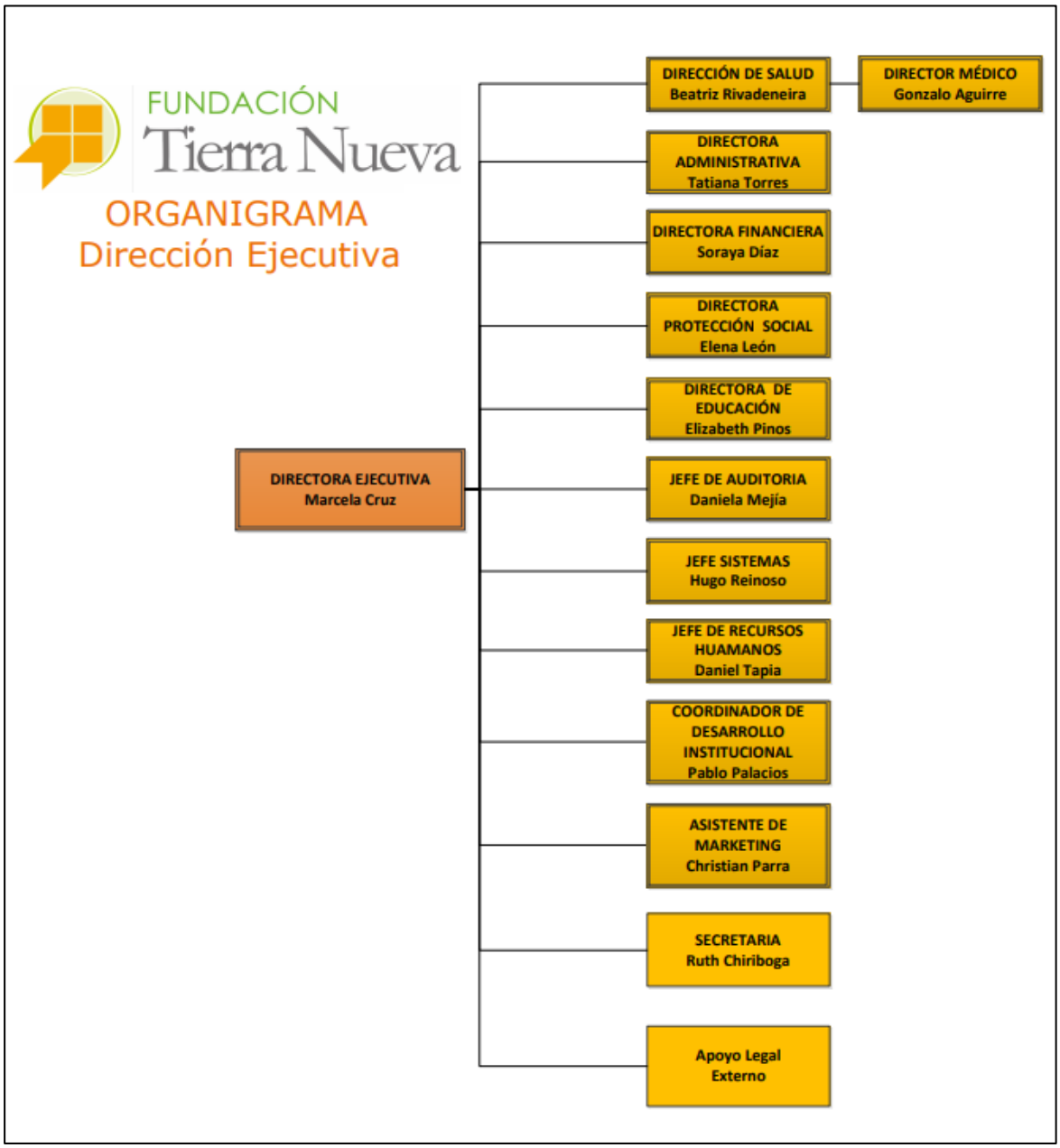
La FTN, creada por el padre José Carollo en el año 1992, enfocada en la línea humanista con opción preferencial a personas vulnerables, cuenta con tres áreas Salud, Educación y Protección Social.

La Fundación tiene como misión gestionar servicios de alta calidad humana y técnica en Protección Social, Salud y Educación, en donde como prioridad tienen a personas en situaciones de vulnerabilidad.

En cuanto a su estructura, la FTN, está conformada por dirección ejecutiva encargada de velar por el correcto funcionamiento de la misma, y bajo su cargo tiene la responsabilidad de verificar el trabajo de cada una de las áreas estas son, dirección de salud, administrativa, financiera, protección social, educación, auditoría, sistemas, recursos humanos, marketing, secretaria y apoyo legal.

Figura 6

Organigrama de la FTN



Nota. Gráfico del organigrama de la FTN. Fuente: Fundación Tierra Nueva (FTN).

2.1.1 Comité técnico

Una vez entendiendo como se encuentra organizada la FTN, es importante conocer que además cuentan con un comité técnico que se presenta a través la figura 7, conformado por directores de área, coordinadores de centros y asistentes quienes realizan reuniones con el objetivo de toma de decisiones para el mejoramiento de la FTN.

Figura 7

Estructura del comité técnico de la FTN

Nota. Gráfico de la estructura del comité técnico de la FTN. Fuente: (FTN, 2018).

2.1.2 Área de Educación

Encargada de desarrollar procesos educativos inclusivos, es decir que permitan integrarse al entorno familiar, escolar y a la comunidad en general. El área cuenta con tres centros de educación estos son: (DTICS Fundación Tierra Nueva , 2022)

- Centro de discapacidad para niños (CDI)
- Centro de jóvenes con discapacidad intelectual.
- Atención a familias con discapacidad.

Cada uno enfocado en derechos y responsabilidad, para ayudar a sectores vulnerables para fortalecer capacidades educativas y sociales.

2.1.3 Área de Protección Social

Encargada de brindar servicios de prevención, atención integral a jóvenes, familias y grupos vulnerables. Esta área cuenta con cuatro centros de protección social estos son: (DTICS Fundación Tierra Nueva , 2022)

- Centro de desarrollo infantil
- Centro de apoyo psicosocial Ubuntu
- Centro de atención para adultos mayores
- Centro de mediación

Cada centro enfocado en abordar problemáticas afectivas, cognitivas, psicoeducativas, desde terapia, familiar, individual o de pareja.

2.1.4 Técnicas e instrumentos para el levantamiento de la información

Para la realización del diagnóstico, se alinearon 30 preguntas en base a los dominios de la norma ISO/IEC 27001, como resultado se obtuvo información esencial que permitió determinar de manera global la situación actual de las áreas de Educación y Protección Social de la FTN.

En resumen, los elementos fundamentales que estuvieron presentes para el desarrollo del diagnóstico fueron:

- El establecimiento de directrices de gestión de la seguridad de la información.
- El establecimiento de un comité con roles y responsabilidades.
- Que la alta dirección apoye a la iniciativa y sea sensible al igual que toda la organización de la importancia de la gestión adecuada de la información.
- La clasificación de la información en pública, privada.
- El uso adecuado de tecnologías de información.

- La gestión en el cumplimiento, mantenimiento y revisión.

2.1.4.1. Matriz informativa de controles y dominios ISO 27001. Dado que la ISO 27001 es la norma que se enfoca en la gestión de la seguridad de la información es importante conocer la referencia de los controles de seguridad bajo el estándar de la ISO 27001 y cómo están vinculados con sus dominios, por consiguiente, en la tabla 3, se presenta una descripción más detallada de cada uno de ellos, en donde se hace énfasis la parte de objetivos que tiene cada dominio e identificados o clasificados de acuerdo al tipo de indicador ya sea de cumplimiento o de gestión.

Esta matriz se utilizó como punto de partida para la creación de SGSI para las áreas de Educación y Protección Social de la FTN debido a que se señala dos tipos de indicadores, cumplimiento y de gestión, el indicador de cumplimiento es cualitativo que afirma que todas las operaciones ya sean administrativas, económicas o de otra índole de la organización cumplan con las normas reglamentarias, así como también apoyan a la alta dirección en la toma de decisiones que serán oportunas para el desarrollo de la misma y el indicador de gestión es cuantitativo es decir consiste en una evaluación aplicada a la organización con el propósito de medir el nivel de eficiencia y eficacia para la planificación, control y usos de los recursos.

Tabla 3

Matriz de controles y dominios

MATRIZ DE CONTROLES Y DOMINIOS				
NOMBRE	**INDICADOR**	**DOMINIO**	**OBJETIVO**	**TIPO DE INDICADOR**

Control A-5	1	Política de seguridad	Propone orientación y soporte, por parte de la alta gerencia para la seguridad de la información de acuerdo con los requisitos del negocio	Cumplimiento
Control A-6	2	Organización de la información	Establece un marco de referencia de gestión y controla la implementación y operación de la seguridad de la información de la organización	Gestión
Control A-7	3	Seguridad en recursos humanos	Asegura que los empleados comprendan sus responsabilidades	Cumplimiento
Control A-8	4	Gestión de activos	Identifica y define los activos organizacionales y responsabilidades de protección	Cumplimiento
Control A-9	5	Control de accesos	Limita el acceso a información y a instalaciones de procesamiento de información.	Gestión
Control A-10	6	Criptografía	Asegura el uso apropiado y eficaz de la criptografía	Gestión
Control A-11	7	Seguridad física y ambiental	Evita el daño, robo o compromiso hacia la información y a las instalaciones de procesamiento de información de la organización	Cumplimiento
Control A-12	8	Seguridad en las operaciones	Asegura y protege las operaciones correctas de las instalaciones de procesamiento de la información y códigos maliciosos que puedan causar perdida de datos	Cumplimiento

Control A-13	9	Transferencia de información	Asegura la protección de la información en las redes, instalaciones y transferencia de información dentro de la organización y externamente	Gestión
Control A-14	10	Adquisición de sistemas, desarrollo y mantenimiento	Asegura que la información sea una parte integral de los sistemas de información durante todo el ciclo de vida	Cumplimiento
Control A-15	11	Relación con proveedores	Fija la protección de los activos de la organización que sean accesibles a los proveedores	Gestión
Control A-16	12	Gestión de los incidentes de seguridad	Asegura un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información.	Gestión
Control A-17	13	Continuidad de negocio	Mantiene la continuidad de la seguridad de la información	Gestión
Control A-18	14	Cumplimiento con requerimientos legales y contractuales	Evita el incumplimiento de las obligaciones legales o contractuales relacionadas con seguridad de la información	Cumplimiento

Nota. En la matriz se describe cada objetivo de los dominios que son aplicados al proyecto.

Elaborado por: La autora, a través de (ISO/IEC27001, 2013)

2.1.4.2 Cuestionario. Las preguntas de este cuestionario fueron creadas utilizando el Anexo A planteado por la norma ISO/IEC 27001 ver tabla 4, documento cuyo enfoque son los objetivos de control y controles de referencia detallados en la cláusula del 5 al 18, ya que son controles específicamente relacionados con la seguridad de la

información. es decir, este proceso fue aplicado a las áreas de Educación y Protección Social de la FTN.

Al momento de efectuar las ponderaciones para cada pregunta concerniente a los controles, se tuvo presente la importancia de los dominios de la norma ISO 27001, evitando escenarios del tipo “calificación alta o considerado como muy importante” y exigiendo así al evaluador a realizar una valoración que discierna entre lo que es realmente importante y lo que no es tan importante.

Tabla 4

Cuestionario

Control	**Dominio**	**Preguntas**
A.5	Políticas de Seguridad	¿La FTN tiene un sistema de gestión de seguridad de la información (SGSI)?
A.5		¿Dentro de la FTN usted tiene conocimientos sobre si existe algún comité interno que administre las políticas de seguridad de la información de la organización?
A.5		¿De existir este comité en la organización, usted tiene conocimientos sobre dichas políticas de seguridad de la información?
A.5		¿En caso de que la FTN no posea un SGSI, estaría de acuerdo con el involucramiento en la iniciativa de un SGSI?
A.6	Organización de la Información	¿El departamento posee mecanismos que le permitan tener la información organizada?

A6		¿El departamento cuenta con una correcta gestión de dispositivos informáticos para las Tics?
A7	Seguridad en Recursos Humanos	¿Existen procesos basados en la seguridad de la información durante la selección de funcionarios y colaboradores?
A7		¿En el departamento están identificadas las responsabilidades de cada actividad que deben tener los trabajadores en relación con la seguridad de la información?
A.8	Gestión de Activos	¿Existe la participación de terceros para el manejo de la información dentro del departamento?
A.8		¿Existe en el departamento un inventario de los activos de información?
A8		¿Si posee un inventario de los activos de información en el departamento, existe la asignación de un responsable en la clasificación de la información?
A.9	Control de Accesos	¿El departamento posee algún software para la gestión de los activos?
A.9		¿Existe tecnologías como el directorio activo, virtualización, dominio de servicios que estén implementadas dentro del departamento?

A.10	Criptografía	¿En el departamento para el control de accesos existen procesos definidos que permitan al usuario ejecutar acciones o acceder a recursos?
A11	Seguridad Física y Ambiental	¿El departamento cuenta con tecnología de cifrado o criptografía como principal base para la seguridad de datos?
A.12	Seguridad de las Operaciones	¿Tiene conocimiento si la fundación cuenta con pólizas de seguros que le permita salvaguardar sus activos tangibles e intangibles?
A.12		¿Tiene conocimientos si dentro del departamento existe tecnologías que permitan llevar a cabo una administración centralizada proactiva sobre las Tics?
A.12		¿El departamento cuenta con tecnología para evitar y responder amenazas cibernéticas?
A.13	Transferencia de Información	¿El departamento cuenta con tecnología para el respaldo y recuperación de la información?
A.14	Adquisición de Sistemas Desarrollo y Mantenimiento	¿El departamento posee seguridad para la tecnología de las comunicaciones e información tales como firewalls o seguridad perimetral?
A15	Relación con Proveedores	¿El departamento cuenta con seguridad en la implementación de los procesos de adquisición, desarrollo o mantenimiento de aplicaciones?

A.16	Gestión de Incidentes de Seguridad	¿Existe dentro del departamento procesos para una adecuada gestión de relaciones con proveedores que permitan una buena coordinación y cooperación?
A.17	Continuidad del Negocio	¿El departamento cuenta con algún sistema para la gestión de incidentes de seguridad de información, tales como, servicio de escritorio o mesa de ayuda
A18	Cumplimiento con Requisitos Legales y Contractuales	¿Existe tecnología dentro del departamento que permita gestionar la continuidad y mejoramiento del negocio?
A18		¿En el departamento están identificados los requisitos legales?
A18		¿El departamento toma todas las medidas necesarias que garanticen el cumplimiento de la leyes y regulaciones?
A18		¿Se dispone dentro del departamento políticas de uso legal de productos de software?
A18		¿El personal del departamento tiene conocimiento de las políticas de uso legal de software que clarifiquen que cosas están permitidas y cuáles no?
A18		¿Existen procesos que definan un buen manejo de contratos para asegurar la confidencialidad, integridad y disponibilidad de los activos?
A18		¿Existe documentación que justifique y valide la propiedad de las licencias del software?

Nota. El cuestionario es la base para obtener una evaluación general del estado de la FTN.

Elaborado por: La autora.

La escala utilizada en la ponderación para el cuestionario fue realizada con la finalidad de obtener un conocimiento de lo que cumple y no cumplen las áreas de Educación y Protección Social. La tabla 4 explica los niveles de la ponderación es decir cuando una pregunta es señalada como cumple la escala de respuesta asigna un valor de 10, que significa un cumplimiento del dominio, cuando una pregunta es señalada como no cumple la escala de respuestas asigna un valor de 0 que significa el incumplimiento total del dominio y finalmente cuando una pregunta es señalada como desconoce la escala de respuestas asigna un valor de 5 que significa que existe un nivel de cumplimiento intermedio.

Tabla 5

Explicación de ponderación cuestionario

Escala de Respuestas	Explicación
0	No cumple con el dominio
5	Presenta un nivel intermedio de cumplimiento
10	Cumple completamente con el dominio

Nota. La explicación de la ponderación del cuestionario es importante para el resultado del diagnóstico. Elaborado por: La autora.

2.1.4.3 Estado de las áreas de Educación y Protección Social de la FTN. Para la identificación del estado actual de las áreas de Educación y Protección Social se procedió con la realización de la tabla 6 la cual fue creada en base al artículo académico realizado por la autora Pérez la cual realiza un análisis para aplicar en pequeñas y medianas empresas, además se realizó en base al juicio de expertos sobre seguridad de la información obteniendo como resultado los siguientes campos: Valoración: el total

que se evidencia en el campo valoración se obtiene del total de la ponderación obtenida del cuestionario realizado a las áreas de Educación y Protección Social.

Resultado: En base a la valoración obtenida cada una de las áreas se las clasifica como organización madura, si tiene un rango de 80 a 100 es decir que cumple la norma y es aspirante a una certificación, se considera organización evolutiva, si tiene un rango de 51 a 70 es decir que está en el camino correcto con mucho trabajo por realizar y se considera una organización inicial, si tiene un rango de 0 a 50 es decir que la organización se ha percatado de la importancia de la norma y está comprometida a caminar en el rumbo de la obtención de un SGSI.

Tabla 6

Estado de áreas

Valoración	Resultado	Descripción
[80 -100]	Organización Madura	Está cercana al cumplimiento de la Norma y aspirante a la certificación.
[51 - 79]	Organización Evolutiva	Está en el camino correcto, con mucho trabajo por realizar.
[0 - 50]	Organización Inicial	Se ha percatado de la importancia de la Norma y está comprometida a caminar en el rumbo.

Nota. Ésta tabla permite señalar con indicadores el estado actual de las áreas de Educación y Protección Social de la FTN. Elaborado por: La autora.

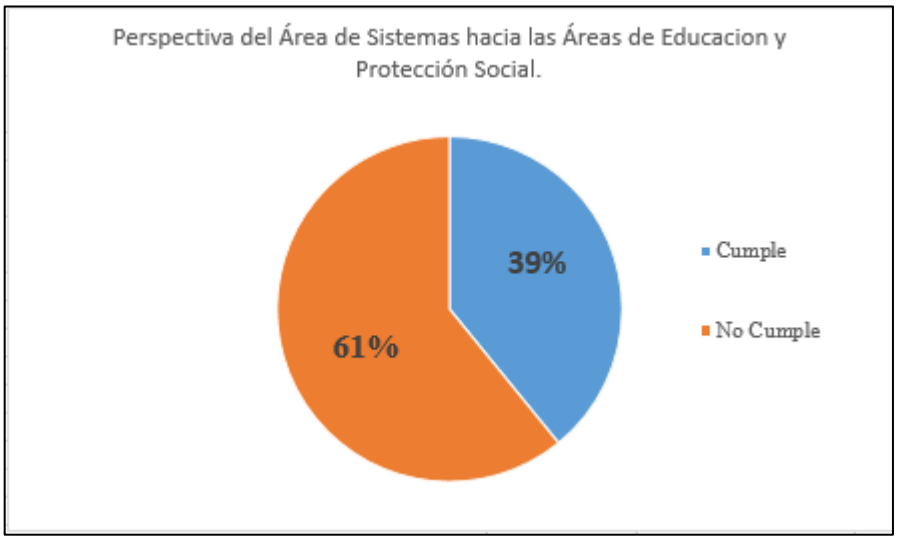
2.1.4.4 Entrevista. Al tener ya establecido el cuestionario, se utilizó la técnica denominada entrevista para establecer un mejor diálogo con las personas encargadas de las áreas de Educación, Protección Social y Sistemas.

2.1.4.4.1 Área de Sistemas. Se procedió con la entrevista que se puede observar en la tabla 3 al director del área de Sistemas, para identificar su perspectiva de las áreas de Educación y Protección Social evaluadas en relación a la seguridad de la información. Todo esto debido a que esta área tiene un rol importante en la gestión de la información ya que está dedicada a proveer tecnología tales como software y hardware, así como también encargada de proporcionar las herramientas e instrumentos adecuados para la manipulación información a las áreas de Educación y Protección Social.

2.1.4.4.2 Resultado. El resultado de aplicar el cuestionario al área de Sistemas fue obtener un 39% de cumplimiento y un 61% de no cumplimiento de aplicación de dominios de acuerdo con la perspectiva del director del área de Sistemas, explicado en tabla 2 hacia las áreas de Educación y Protección Social. Es decir que dichas áreas tratan en medida de lo posible asegurar la información que manejan en el día a día, es por ello que se evidencia la necesidad de un SGSI para llevar un correcto control y evitar vulnerabilidades dentro del área**.**

Figura 8

Perspectiva del Área de Sistemas hacia las Áreas de Educación y Protección Social



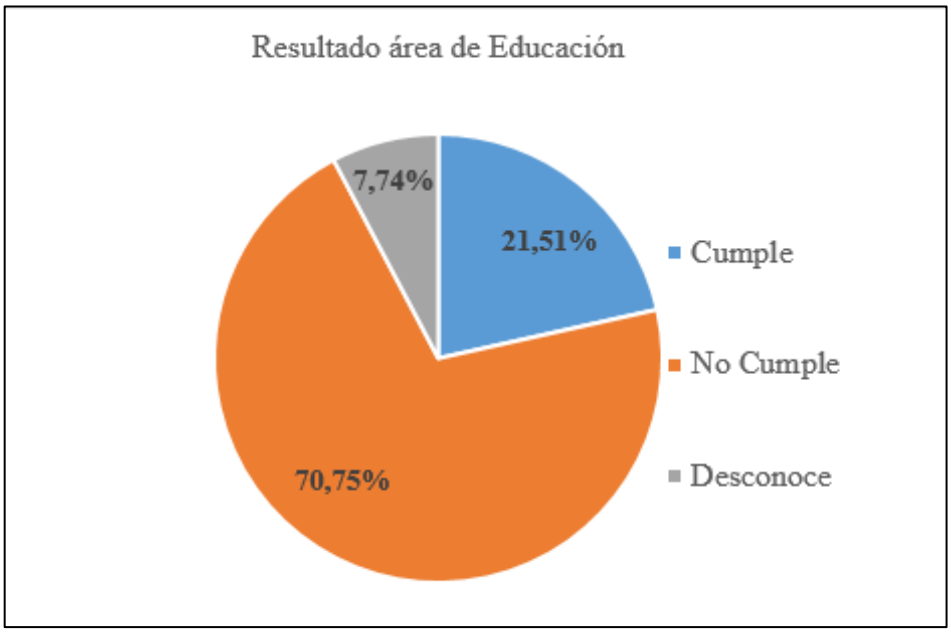
Resultado de la entrevista al área de Sistemas. Elaborado por: La autora.

2.1.4.4.3 Área de Educación. Se procedió con la entrevista que se puede observar en la tabla 4 a la directora del área de Educación, para identificar su perspectiva del área en concordancia a la seguridad de la información.

2.1.4.4.4 Resultado. El resultado de aplicar el cuestionario al área de Educación fue obtener un 21.51% de cumplimiento, un 70.75% de no cumplimiento y un 7.74% de desconocimiento de aplicación de dominios explicado en tabla 3. Es decir que dicha área trata en medida de lo posible asegurar la información que manejan en el día a día, es por ello que se evidencia la necesidad de un SGSI para llevar un correcto control y evitar vulnerabilidades dentro del área.

Figura 9

Resultado área de Educación



Resultado de la entrevista al área de Educación. Elaborado por: La autora.

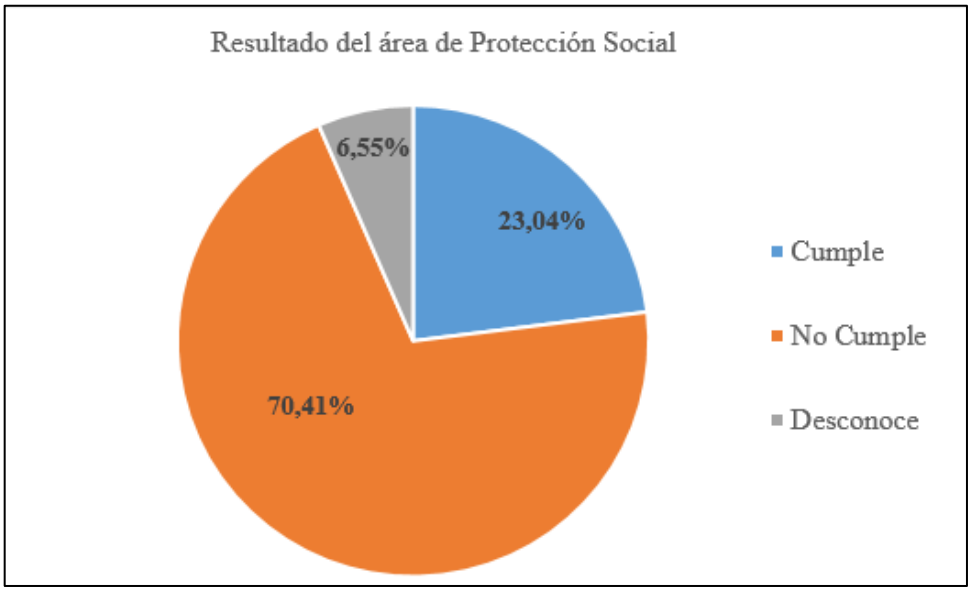
2.1.4.4.5 Área de Protección Social. Se procedió con la entrevista que se puede observar en la tabla 4 a la directora del área de Protección Social, para identificar su perspectiva del área en concordancia a la seguridad de la información**.**

2.1.4.4.6 Resultado. El resultado de aplicar el cuestionario al área de Protección Social fue obtener un 23.04% de cumplimiento, un 70,41% de no cumplimiento y un 6.55% de desconocimiento de aplicación de dominios explicado en tabla 3. Es decir que dicha área trata en medida de lo posible asegurar la información que manejan en el día a día,

es por ello que se evidencia la necesidad de un SGSI para llevar un correcto control y evitar vulnerabilidades dentro del área.

Figura 10

Resultado de Protección Social



Resultado de la entrevista al área de protección social. Elaborado por: La autora

2.1.4.5 Análisis de datos obtenidos. En este apartado, se realizó una diferenciación de resultados clasificándola como perspectiva técnica (área de Sistemas) y perspectiva funcional (áreas de Educación y Protección Social), debido a una divergencia relacionada con la percepción de cada área, por esa razón, se detalla en la tabla 7, tabla

8 y tabla 9 el estado actual del cumplimiento del estándar de la norma ISO 27001 de acuerdo con sus dominios.

Tabla 7

Perspectiva del área de Sistemas sobre el cumplimiento de dominios de las áreas de Educación y Protección Social

Dominios	Cumple	No Cumple
Políticas de seguridad	25%	75%
Organización de la información	100%	0%
Seguridad en recursos humanos	75%	25%
Gestión de activos	50%	50%
Control de accesos	50%	50%
Criptografía	50%	50%
Seguridad física y ambiental	0%	100%
Seguridad en las operaciones	33%	67%
Transferencia de información	0%	100%
Adquisición de sistemas, desarrollo y mantenimiento	0%	100%
Relación con proveedores	0%	100%
Gestión de los incidentes de seguridad	100%	0%
Continuidad de negocio	0%	100%
Cumplimiento con requerimientos legales y contractuales	64%	36%
Total	**39%**	**61%**

Cumplimiento y no cumplimiento de dominios del área de Sistemas y Educación Social Elaborado por: La autora a través de la norma (ISO/IEC27001, 2013)

Tabla 8

Perspectiva del área de Educación sobre el cumplimiento de dominios

Educación			
Dominios	**Cumple**	**No Cumple**	**Desconoce**
Políticas de seguridad	25,00%	50,00%	25,00%
Organización de la información	50,00%	50,00%	0%
Seguridad en recursos humanos	50,00%	0,00%	50%
Gestión de activos	33,33%	66,67%	0%
Control de accesos	0,00%	100,00%	0%
Criptografía	0,00%	100,00%	0%
Seguridad física y ambiental	0,00%	100,00%	0%
Seguridad en las operaciones	0,00%	66,67%	33%
Transferencia de información	0,00%	100,00%	0%
Adquisición de sistemas, desarrollo y mantenimiento	0,00%	100,00%	0%
Relación con proveedores	0,00%	100,00%	0%
Gestión de los incidentes de seguridad	100,00%	0,00%	0%
Continuidad de negocio	0,00%	100,00%	0%
Cumplimiento con requerimientos legales y contractuales	42,85%	57,14%	0%
Total	**21,51%**	**70,75%**	**7,74%**

Cumplimiento y no cumplimiento de dominios del área de Educación. Elaborado por: La autora a través de la norma (ISO/IEC27001, 2013)

Tabla 9

Perspectiva del área de protección social sobre el cumplimiento de dominios

Protección Social			
Dominios	**Cumple**	**No Cumple**	**Desconoce**
Políticas de seguridad	25,00%	50,00%	25,00%
Organización de la información	50,00%	50,00%	0%
Seguridad en recursos humanos	100,00%	0,00%	0%
Gestión de activos	0,00%	100,00%	0%
Control de accesos	0,00%	100,00%	0%
Criptografía	100,00%	0,00%	0%
Seguridad física y ambiental	0,00%	100,00%	0%
Seguridad en las operaciones	33,33%	0,00%	67%
Transferencia de información	0,00%	100,00%	0%
Adquisición de sistemas, desarrollo y mantenimiento	0,00%	100,00%	0%
Relación con proveedores	0,00%	100,00%	0%
Gestión de los incidentes de seguridad	0,00%	100,00%	0%
Continuidad de negocio	0,00%	100,00%	0%

Cumplimiento con requerimientos legales y contractuales	14,25%	85,71%	0%
TOTAL	**23,04%**	**70,41%**	**6,55%**

Cumplimiento y no cumplimiento de dominios del área de Educación. Elaborado por: La autora. A través de la norma (ISO/IEC27001, 2013)

2.1.4.6 Resultado general de las áreas de Educación y Protección Social. Después de haber realizado evaluaciones específicas al área de Sistemas, Educación y Protección social de la FTN, se da paso a la creación de una matriz cualitativa para constatar el cumplimiento de los controles de acuerdo con la ISO 27001, tal como se muestra en la tabla 10.

Tabla 10

Matriz cualitativa de cumplimientos de controles de acuerdo a la ISO/IEC 27001

Cumplimiento de Controles de la ISO 27001					
Pregunta	**Dominio**	**Preguntas**	**Resultado de Educación**	**Resultado Protección Social**	**Resultado Sistemas**
A.5	Políticas de Seguridad	¿La FTN tiene un sistema de gestión de seguridad de la información (SGSI)?	NO CUMPLE	NO CUMPLE	NO CUMPLE
A.5		¿Dentro de la FTN usted tiene conocimientos sobre si existe algún comité interno que administre las políticas de seguridad de la información de la organización?	INCOMPLETO	INCOMPLETO	NO CUMPLE
A.5		¿De existir este comité en la organización, usted tiene conocimientos sobre dichas políticas de seguridad de la información?	NO CUMPLE	NO CUMPLE	NO CUMPLE
A.5		¿En caso de que la FTN no posea un SGSI, estaría de acuerdo con el involucramiento en la iniciativa de un SGSI?	CUMPLE	CUMPLE	INCOMPLETO
A.6	Organización de la Información	¿El departamento posee mecanismos que le permitan tener la información organizada?	NO CUMPLE	NO CUMPLE	CUMPLE
A6		¿El departamento cuenta con una correcta gestión de dispositivos informáticos para las TIC's?	CUMPLE	CUMPLE	CUMPLE
A7	Seguridad en Recursos Humanos	¿Existen procesos basados en la seguridad de la información durante la selección de funcionarios y colaboradores?	INCOMPLETO	CUMPLE	INCOMPLETO
A7		¿En el departamento están identificadas las responsabilidades de cada actividad que deben tener los trabajadores en relación con la seguridad de la información?	CUMPLE	CUMPLE	CUMPLE
A.8	Gestión de Activos	¿Existe la participación de terceros para el manejo de la información dentro del departamento?	NO CUMPLE	NO CUMPLE	INCOMPLETO
A.8		¿Existe en el departamento un inventario de los activos de información?	CUMPLE	NO CUMPLE	INCOMPLETO
A8		¿Si posee un inventario de los activos de información en el departamento, existe la asignación de un responsable en la clasificación de la información?	NO CUMPLE	NO CUMPLE	INCOMPLETO
A.9	Control de Accesos	¿El departamento posee algún software para la gestión de los activos?	NO CUMPLE	NO CUMPLE	INCOMPLETO
A.9		¿Existe tecnologías como el directorio activo, virtualización, dominio de servicios que estén implementadas dentro del departamento?	NO CUMPLE	NO CUMPLE	INCOMPLETO
A.10	Criptografía	¿En el departamento para el control de accesos existen procesos definidos que permitan al usuario ejecutar acciones o acceder a recursos?	NO CUMPLE	CUMPLE	INCOMPLETO
A11	Seguridad Física y Ambiental	¿El departamento cuenta con tecnología de cifrado o criptografía como principal base para la seguridad de datos?	NO CUMPLE	NO CUMPLE	NO CUMPLE
A.12	Seguridad en las Operaciones	¿Tiene conocimiento si la fundación cuenta con pólizas de seguros que le permita salvaguardar sus activos tangibles e intangibles?	INCOMPLETO	INCOMPLETO	INCOMPLETO
A.12		¿Tiene conocimientos si dentro del departamento existe tecnologías que permitan llevar a cabo una administración centralizada proactiva sobre las TIC's?	NO CUMPLE	CUMPLE	INCOMPLETO
A.12		¿El departamento cuenta con tecnología para evitar y responder amenazas cibernéticas?	NO CUMPLE	INCOMPLETO	NO CUMPLE
A.13	Transferencia de Información	¿El departamento cuenta con tecnología para el respaldo y recuperación de la información?	NO CUMPLE	NO CUMPLE	NO CUMPLE
A.14	Adquisición de Sistemas, Desarrollo y Mantenimiento	¿El departamento posee seguridad para la tecnología de las comunicaciones e información tales como firewalls o seguridad perimetral?	NO CUMPLE	NO CUMPLE	NO CUMPLE
A15	Relación con Proveedores	¿El departamento cuenta con seguridad en la implementación de los procesos de adquisición, desarrollo o mantenimiento de aplicaciones?	NO CUMPLE	NO CUMPLE	NO CUMPLE
A.16	Gestión de los Incidentes de Seguridad	¿Existe dentro del departamento procesos para una adecuada gestión de relaciones con proveedores que permitan una buena coordinación y cooperación?	CUMPLE	NO CUMPLE	CUMPLE
A.17	Continuidad de Negocio	¿El departamento cuenta con algún sistema para la gestión de incidentes de seguridad de información, tales como, servicio de escritorio o mesa de ayuda	NO CUMPLE	NO CUMPLE	NO CUMPLE
A18	Cumplimiento con Requerimientos Legales y Contractuales	¿Existe tecnología dentro del departamento que permita gestionar la continuidad y mejoramiento del negocio?	NO CUMPLE	NO CUMPLE	NO CUMPLE
A18		¿En el departamento están identificados los requisitos legales?	CUMPLE	NO CUMPLE	INCOMPLETO
A18		¿El departamento toma todas las medidas necesarias que garanticen el cumplimiento de la leyes y regulaciones?	CUMPLE	NO CUMPLE	CUMPLE
A18		¿Se dispone dentro del departamento políticas de uso legal de productos de software?	NO CUMPLE	NO CUMPLE	NO CUMPLE
A18		¿El personal del departamento tiene conocimiento de las políticas de uso legal de software que clarifiquen que cosas están permitidas y cuáles no?	NO CUMPLE	NO CUMPLE	CUMPLE
A18		¿Existen procesos que definan un buen manejo de contratos para asegurar la confidencialidad, integridad y disponibilidad de los activos?	CUMPLE	CUMPLE	CUMPLE
A18		¿Existe documentación que justifique y valide la propiedad de las licencias del software?	NO CUMPLE	NO CUMPLE	CUMPLE

Nota. Ésta tabla permite visualizar de forma general el cumplimiento de los dominios de las áreas de Educación, Protección Social y perspectiva del área Sistemas.

Elaborado por: La autora.

2.1.4.7 Conclusión ejecutiva. En líneas generales una vez finalizadas las entrevistas a las áreas de Sistemas, Educación y Protección Social de la FTN, se determinó que es una organización que tiene un cumplimiento del 28% y un 72% de incumplimiento de los dominios. Con estos resultados se concluye que las áreas de Educación y Protección Social se percataron de la importancia de la norma y que están comprometidas a caminar al rumbo de la obtención de un SGSI, ya que con la documentación que cuentan actualmente de alguna manera se encuentran protegidas.

2.1.5 Identificación de activos de información

Esta sección fue realizada para cumplir con el segundo objetivo planteado en el presente proyecto de titulación es decir identificar los activos de información que tienen las áreas de Educación y Protección Social de la FTN, además de los riesgos asociados a estos activos.

Por esa razón se clasificaron los activos de información como tangibles, intangibles y recursos humanos.

2.1.5.1 Activos intangibles de las áreas de Educación y Protección Social. A continuación, se presenta todos los activos de información, es decir, software,

aplicaciones e información que poseen las áreas de Educación y Protección Social de la FTN.

2.1.5.1.1 Área de Educación. Para esta área se realizó la distribución de los activos de información tal como se muestra en la tabla 11.

Tabla 11

Activos de información del área de Educación

Nombre del Activo	Cantidad	Descripción
Adendum de contratos de trabajo	1	Documentos que garantizan las funcionalidades, remuneración de cada trabajador
Check List de documentos habilitantes para aprobaciones de proyectos	1	Documento que cuenta con pasos a seguir para que cada proyecto pueda ser aprobado
Cartas informativas sobre pago de personal	1	Documento informativo sobre situación de pagos a empleados
Descriptivos de cargo	4	Descriptivos de cargos de cada personal del área
Certificados	3	Formatos para solicitar información
Imagen institucional	1	La imagen es utilizada en la fundación tanto en documentos institucionales, como logotipos web y de rotulación
Lineamientos de apadrinamiento	1	Documento utilizado para identificar que lineamientos se debe cumplir para aprobar sistema de apadrinamientos a niños
Manual de convivencia sana	2	Documento que sirve de guía para identificar como llevar una convivencia sana con el personal
Matriz de responsabilidades de cargos	1	Documento que indica las responsabilidades de trabajo que debe tener cada persona
Nombramiento registro de directiva fundación	1	Documento que indica a las áreas de la fundación las personas que se encuentran en la directiva general

Reglamentos CAAP 2020	1	Documento que contiene políticas que debe cumplir cada proyecto de la fundación
Permisos de funcionamiento	1	Formatos para solicitar información

Nota. En la tabla se detalla todos los activos de información del área de Educación.

Elaborado por: La autora.

2.1.5.1.2 Área de protección social. Para esta área se realizó la distribución de la información tal como se observa en la tabla 10 para la documentación y para el software tal como se indica en la tabla 12.

Tabla 12

Activos de información del área de Protección Social

Nombre de Activo	Cantidad	Descripción
Planificación de proyecto	1	Documento informativo de todo lo que se realiza en el proyecto
Protocolo de atención integral de proyectos	1	Pasos a seguir en la atención de proyectos
Protocolo de ingreso y admisión de personas	1	Formato utilizado para el ingreso de personal que estarán asignados a diferentes proyectos
Protocolo de cuidado integral	1	Formato utilizado para el cuidado integral de usuarios
Afiches de donaciones	2	Formato donde se registran donaciones recibidas para el proyecto
Descriptivos de cargos	2	Descriptivos de cargos de cada personal del área
Imagen institucional	1	La imagen es utilizada en la fundación tanto en documentos institucionales, como logotipos web y de rotulación

Bitácora abordaje	1	Formato donde se lleva seguimiento de cada persona que ingresa al proyecto
Matriz de apoyo de organizaciones	1	Documento informativo de organizaciones que apoyan al proyecto, en cuestiones legales.

Nota. En la tabla se detalla los activos de información del área de Protección Social.

Elaborado por: La autora.

Tabla 13

Activos intangibles del área de Protección Social

Nombre de activo	Cantidad	Descripción
Medysis	1	Sistema Hospitalario, donde se registra pacientes que pertenecen al área de protección social

Nota. En la tabla se detalla el software del área de protección social. Elaborado por: La autora.

2.1.5.2 Activos tangibles de las áreas de Educación y Protección Social. En este apartado, se describe todos los activos correspondientes al hardware que posee las áreas de Educación y Protección Social de la FTN.

2.1.5.2.1 Área de educación. Para esta área se hizo la distribución del hardware tal como se presenta en la tabla 14.

Tabla 14

Activos tangibles del área de Educación

Nombre de activo	Cantidad	Descripción
Computadoras de escritorio-HP	2	Computadoras de escritorio utilizada por funcionarios del área de educación

Computadoras de escritorio-CLON	3	Computadoras de escritorio utilizada por funcionarios del área de educación
Computadoras de escritorio-DELL	7	Computadoras de escritorio utilizada por funcionarios del área de educación
Impresoras- EPSON	2	Impresoras utilizadas por personal del área de educación
Impresora-SHARP	1	Impresoras utilizadas por personal del área de educación

Nota. En la tabla se detalla el hardware del área de Educación. Elaborado por: La autora.

2.1.5.2.2 Área de protección social. Esta área presenta la siguiente distribución tal como se muestra en la tabla 15.

Tabla 15

Activos tangibles del área de Protección Social

Nombre del Activo	Cantidad	Descripción
Computadoras de escritorio ACER	5	Computadoras de escritorio utilizada por funcionarios del área de protección social
Computadoras de escritorio DELL	1	Computadoras de escritorio utilizada por funcionarios del área de protección social
Laptop- DELL	3	Laptop utilizada por funcionarios del área de protección social

Nota. En la tabla se detalla el hardware del área de Protección Social. Elaborado por: La autora.

2.1.5.3 Recursos humanos de las áreas de educación y protección social. En esta sección, se verificó la distribución del personal por cada área.

2.1.5.3.1 Área de educación. Para esta área se constató la distribución del personal tal como se presenta en la tabla 16.

Tabla 16

Recursos humanos del área de Educación.

Nombre del Activo	Cantidad	Descripción
Auxiliar de aula	3	Cantidad de funcionarios que pertenecen al área de educación con el cargo de auxiliar de aula
Auxiliar de servicios generales	2	Cantidad de funcionarios que pertenecen al área de educación con el cargo de auxiliar de servicios generales
Auxiliar de facilitación	1	Cantidad de funcionarios que pertenecen al área de educación con el cargo de auxiliar de facilitación
Chofer	2	Cantidad de funcionarios que pertenecen al área de educación con el cargo de chofer
Coordinadora administrativa centros infantiles	2	Cantidad de funcionarios que pertenecen al área de educación con el cargo de coordinadora administrativa
Directora del sistema de educación	1	Cantidad de funcionarios que pertenecen al área de educación con el cargo de directora del sistema de educación
Educadora	25	Cantidad de funcionarios que pertenecen al área de educación con el cargo de educadora
Facilitadora	2	Cantidad de funcionarios que pertenecen al área de educación con el cargo de facilitadora
Secretaria	3	Cantidad de funcionarios que pertenecen al área de educación con el cargo de secretaria
Técnico en discapacidades	8	Cantidad de funcionarios que pertenecen al área de educación con el cargo de técnico en discapacidades
Técnica de proyectos	3	Cantidad de funcionarios que pertenecen al área de educación con el cargo de técnica de proyectos
Trabajadora social	1	Cantidad de funcionarios que pertenecen al área de educación con el cargo de trabajadora social

Terapista físico/Técnico en discapacidades	1	Cantidad de funcionarios que pertenecen al área de educación con el cargo de terapista físico
Terapeuta ocupacional	1	Cantidad de funcionarios que pertenecen al área de educación con el cargo de terapeuta ocupacional

Nota. En la tabla se detalla el personal que hay en el área de Educación. Elaborado por: La autora.

2.1.5.3.2 Área de protección social. Para esta área se constató la distribución del personal tal como se presenta en la tabla 17.

Tabla 17

Recursos humanos del área de protección social

Nombre del activo	Cantidad	Descripción
Auxiliar de enfermería	3	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de auxiliar enfermería
Abogada	1	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de abogada
Auxiliar de taller	1	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de auxiliar de taller
Profesor en ciencia de la educación	1	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de ciencias de la educación
Carpintero	1	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de carpintero
Doctora en leyes	1	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de doctora en leyes

Fisioterapeuta	1	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de f}fisioterapeuta
Licenciada	1	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de licenciada
Médico general	1	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de médico general
Odontólogo	2	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de odontología
Psicoterapeuta	1	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de psicoterapeuta
Psicóloga clínica	5	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de psicóloga clínica
Paramédico	1	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de paramédico
Psicorrehabiltador	1	Cantidad de funcionarios que pertenecen al área de protección social con el cargo de Psicorrehabiltador

Nota. En la tabla se detalla el personal que hay en el área de protección social. Elaborado por: La autora.

2.1.6 Criterios de valoración de activos de las áreas de Educación y Protección Social de la FTN

En esta fase la valoración de los activos se los determina de acuerdo con los criterios en función de la triada cid tal como se muestra en la tabla 18.

2.1.6.1 Confidencialidad. Esta propiedad se encarga que la información solo esté disponible a personas o entidades autorizadas.

2.1.6.2 Integridad. Esta propiedad se encarga de mantener de manera correcta y exacta la información de la organización.

2.1.6.3 Disponibilidad. Esta propiedad permite la accesibilidad y usabilidad de la información bajo la demanda de una persona o entidad autorizada.

Tabla 18

Criterio de valoración de activos

CRITERIOS DE VALORACIÓN DE ACTIVOS		
Confidencialidad	Reservada	Se refiere a la disponibilidad de la información en un determinado proceso y en caso de ser vulnerada impacto negativo.
	Clasificada	La información puede estar categorizada como privada o pública tanto para personal de la organización como para externos.
	Pública	Todo personal interno o externo de las organizaciones pueden acceder libremente a la información.
Integridad	Alta	Indica que la información es exacta y clara para una buena ejecución de controles dentro de las organizaciones.
	Media	Se basa en que si la información deja de ser exacta puede generar un impacto negativo para los procesos de las organizaciones.
	Baja	Si la información no es exacta genera conflictos tanto internos como externos en las organizaciones.
Disponibilidad	Alta	La información que no esté disponible puede retrasar a las organizaciones en sus funciones y llegar a perder la reputación de las mismas.
	Media	La información que no esté disponible conlleva un impacto negativo de índole legal o económica
	Baja	La información considerada baja puede afectar la operación normal de las organizaciones, generando pérdidas económicas

Nota. En la tabla se detalla los criterios en función de la triada CID. Elaborado por: La autora a través de (Seguridad y Privacidad de la Información, 2016)

2.1.7 Matriz de evaluación de riesgos

En esta fase se seleccionó el método de evaluación con estimación cualitativa, esta técnica permitió tasar los riesgos utilizando los criterios numéricos tanto para la probabilidad como para la severidad tal como se muestra en la tabla 19, y para un mejor entendimiento se realizó una descripción cualitativa para cada valoración tal como se muestra en la tabla 18, permitiendo tener un mejor uso sobre la matriz de evaluación de riesgos.

Tabla 19

Matriz de valoración de riesgo

Matriz de Evaluación de Riesgos		**Probabilidad**		
		Baja	**Media**	**Alta**
Impacto	**Bajo**	1	2	3
	Medio	2	4	6
	Alto	3	6	9

Nota. En la tabla se define el riesgo de acuerdo con el impacto por la probabilidad. Elaborado por: La autora a través de (INGERTEC, 2021)

Tabla 20

Indicador del nivel de riesgo

Nivel de Riesgo	**Descripción**
Bajo [1-4]	Se refiere a las acciones que pueden tener riesgo mínimo y que no ocurren.
Medio [5-7]	Contienen un nivel de riesgo medio es decir que no ocurra
Alto [8-9]	Abarca riesgos potenciales que si pueden ocurrir.

Nota. En la tabla se transfiere el valor del nivel de riesgo de cuantitativo a cualitativo. Elaborado por: La autora a través de (Alemán Novoa, 2015).

2.1.8 Riesgos asociados a los activos de información

Una vez ya establecidos todos los criterios para la evaluación de riesgos sobre los activos de información, se procedió a evaluar los riesgos de los activos de información en función de los criterios de la metodología magerit, es decir permitió clasificar la información de las áreas como hardware, software, personal, además se valoró el nivel, grado y gravedad de estos a partir de criterios o valores definidos para la probabilidad o frecuencia de ocurrencia y como para la severidad, impacto o gravedad de las consecuencias.

2.1.8.1 Área de Educación. A continuación, se presenta de forma detallada el nombre del activo y su riesgo asociado, también se constató su consecuencia y la medición de su impacto de forma cualitativa, por consiguiente, se estableció un control para cada activo de la organización separado por tipo.

2.1.8.1.1 Activos de tipo información. En la tabla 21, se presenta todos los activos filtrados por tipo información del área de Educación.

Tabla 21

Riesgos de los activos de información del área de Educación

NOMBRE DEL ACTIVO	RIESGO	CONSECUENCIA	C	I	D	T	IMPACTO	CONTROL
Adendum de Contratos de Trabajo	Uso indebido de información por parte de personal encargado	Afectación al cumplimiento del contrato	3	3	3	9	Alto	Se deberá designar un encargado que llevara el manejo de documentación

	dentro del área							de contratos y Adendum
Check List de documentos habilitantes para aprobaciones de proyectos	No cumplimiento de documentación requerida para aprobación de proyectos	Perdida de Proyecto	3	3	3	9	Alto	Se deberá utilizar aplicaciones especializadas en el tema de cronogramas y recordatorios para no pasar por alto alguna documentación importante para la aceptación del proyectos
Cartas informativas sobre pago de personal	Alteración en el formato de elaboración de cartas	Perdida de Información	2	2	2	6	Medio	Designar un dueño del proceso de actualización de formatos de cartas.
Descriptivos de Cargo	Realización de actividades diferentes a los establecido en el descriptivo de cargo	Funciones mal desempeñadas	2	2	2	6	Medio	Creación de carpeta digital de cada personal y cargo asignado
Certificados	Divulgación de información	Perdida de Información	3	3	3	9	Alto	Se deberá designar un encargado que llevara el manejo de certificados dentro del área
Imagen Institucional	Mal uso de imagen institucional	Multas considerables a la fundación	3	3	3	9	Alto	Participación en capacitaciones para identificar como utilizar la imagen de la Fundación

Lineamientos de Apadrinamiento	Perdida de datos por mal uso de usuarios	Perdida de Información	1	2	2	5	Medio	Establecer metodologías de apoyo al documento de lineamientos que debe cumplir una persona o empresa para el tema de apadrinamiento
Manual de Convivencia Sana	Mal manejo de manual	Información Alterada	2	3	3	8	Alto	Capacitación sobre buena convivencia por parte de la fundación a personal de educación
Matriz de Responsabilidades de Cargos	Manejo inadecuado de información	Perdida de la Información	3	3	3	9	Alto	La documentación deberá ser archivada de manera física y digital, para evitar pérdidas de información
Nombramiento Registro de Directiva Fundación	Mal uso de información referente al nombramiento	Reprocesos en aceptación de proyectos de educación	2	3	3	8	Alto	La documentación deberá ser archivada en una carpeta compartida con el personal designado para la utilización del mismo en temas de proyectos
Reglamentos CAAP 2020	Uso inadecuado, o alteraciones a la información	Afecta a los acuerdos establecidos en el área	1	2	2	5	Medio	La documentación deberá ser archivada en una carpeta compartida con el personal designado para la utilización del mismo en temas de proyectos

Permisos de Funcionamiento	Uso inadecuado de información por parte de personal encargado dentro del área	Perdida de Información	3	3	3	9	Alto	La documentación deberá ser clasificada por tipo de documentación que será utilizada para la aceptación de proyectos.

Nota. En la tabla se identifica el riesgo que tienen los activos de información y cuáles son los controles que ayudaran a la mitigación del mismo. Elaborado por: La autora.

2.1.8.1.2 Activos de tipo hardware. En la tabla 22, se presenta todos los activos filtrados por tipo hardware del área de Educación.

Tabla 22

Riesgos de los activos tangibles del área de Educación

Activo	Riesgo	Consecuencia	C	I	D	T	Valor	Control
Computadoras de escritorio-HP	Daños físicos	Desastres naturales, apagones o interrupciones en la energía eléctrica y robo	3	3	3	9	Alto	Poseer un inventario de los bienes tangibles de la organización
Computadoras de escritorio-CLON	Daños físicos	Desastres naturales, apagones o interrupciones en la energía eléctrica y robo	3	3	3	9	Alto	Poseer un inventario de los bienes tangibles de la organización
Computadoras de escritorio-DELL	Daños físicos	Desastres naturales, apagones o interrupciones en la energía	3	3	3	9	Alto	Poseer un inventario de los bienes tangibles de la organización

		eléctrica y robo						
Impresoras-EPSON	Daños físicos	Desastres naturales, apagones o interrupciones en la energía eléctrica y robo	3	1	1	5	Medio	Poseer un inventario de los bienes tangibles de la organización
Impresora-SHARP	Daños físicos	Desastres naturales, apagones o interrupciones en la energía eléctrica y robo	3	1	1	5	Medio	Poseer un inventario de los bienes tangibles de la organización

Nota. En la tabla se identifica el riesgo con su consecuencia para cada activo y se establece un control. Elaborado por: La autora.

2.1.8.1.3 Activos de tipo empleado. En la tabla 23, se presenta todos los activos filtrados por tipo empleado del área de Educación.

Tabla 23

Riesgos de los recursos humanos del área de Educación

Activo	Riesgo	Consecuencia	C	I	D	T	Valor	Control
Auxiliar de Aula	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Auxiliar de servicios generales	Ausencia del personal por calamidad doméstica,	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición

	despido o renuncia							un alternante de requerirlo
Auxiliar de Facilitación	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Chofer	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Coordinadora Administrativa centros infantiles	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Directora del Sistema de Educación	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Educadora	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo

Facilitadora	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Secretaria	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Técnico en discapacidades	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Técnica de Proyectos	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Trabajadora Social	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Terapista Físico/Técnico en Discapacidades	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo

Terapeuta Ocupacional	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo

Nota. En la tabla se identifica el riesgo con su consecuencia para cada activo y se establece un control. Elaborado por: La autora.

2.1.8.2 Área de Protección Social. A continuación, se presenta de forma detallada el nombre del activo y su riesgo asociado, también se constató su consecuencia y la medición de su impacto de forma cualitativa, por consiguiente, se estableció un control para cada activo de la organización separado por tipo.

2.1.8.2.1 Activos de tipo información. En la tabla 24, se presenta todos los activos filtrados por tipo información del área de protección social.

Tabla 24

Riesgos de los activos de información del área de Protección Social

Activo	Riesgo	Consecuencia	C	I	D	T	Impacto	Control
Planificación de Proyecto	Enviar información a personal no identificado	vulneración de la confidencialidad de la información	2	2	2	6	Medio	Realizar un listado de personal que puede tener acceso a dicha información.
Protocolo de Atención Integral de Proyectos	No cumplir con la información que contiene el protocolo	Desorganización en la información del proyecto	2	3	3	8	Alto	Capacitar a personal que debe ejecutar el protocolo para evitar reprocesos

Protocolo de Ingreso y Admisión de personas	Perdida de datos por mal uso de información por parte del personal encargado	vulneración de la disponibilidad de la información	2	3	3	8	Alto	Definir perfiles y roles de personas que tienen acceso a la información
Protocolo de Cuidado Integral	No cumplir con la información que contiene el protocolo	Mal uso de la Información	2	3	3	8	Alto	Capacitar a personal que debe ejecutar el protocolo para evitar reprocesos
Afiches de Donaciones	No realizar la información	vulneración de disponibilidad de la información	1	1	1	3	Bajo	Definir perfiles y roles de personas que tienen acceso a la información
Descriptivos de Cargos	Realización de actividades diferentes a los establecido en el descriptivo de cargo	Funciones mal desempeñadas	2	3	3	8	Alto	Creación de carpeta digital de cada personal y cargo asignado
Imagen Institucional	Mal uso de imagen institucional	Multas considerables a la fundación	3	3	3	9	Alto	Participación en capacitaciones para identificar como utilizar la imagen de la Fundación
Bitácora Abordaje	No realizar la información	vulneración de disponibilidad de la información	1	1	1	3	Bajo	Definir perfiles y roles de personas que tienen acceso a la información
Matriz de apoyo de organizaciones	Manejo inadecuado de información	Perdida de la Información	2	2		4	Medio	La documentación deberá ser archivada de manera física y digital, para evitar pérdidas de información

Nota. En la tabla se identifica el riesgo con su consecuencia para cada activo y se establece un control. Elaborado por: La autora.

2.1.8.2.2 Activos de tipo hardware. En la tabla 25, se presenta todos los activos filtrados por tipo hardware del área de Protección Social.

Tabla 25

Riesgos de los activos tangibles del área de Protección Social

Activo	Riesgo	Consecuencia	C	I	D	T	Impacto	Control
Computadoras de escritorio-ACER	Daño físico	Desastres naturales, apagones o interrupciones en la energía eléctrica y robo	3	3	3	9	Alto	Poseer un inventario de los bienes tangibles de la organización
Computadoras de escritorio-DELL	Daño físico	Desastres naturales, apagones o interrupciones en la energía eléctrica y robo	3	2	3	8	Alto	Poseer un inventario de los bienes tangibles de la organización
Laptop-DELL	Daño físico	Desastres naturales, apagones o interrupciones en la energía eléctrica y robo	3	2	2	7	Medio	Poseer un inventario de los bienes tangibles de la organización

Nota. En la tabla se identifica el riesgo con su consecuencia para cada activo y se establece un control. Elaborado por: La autora.

2.1.8.2.3 Activos de tipo software. En la tabla 26, se presenta todos los activos filtrados por tipo software del área de Protección Social.

Tabla 26

Riesgos de los activos intangibles del área de Protección Social

Activo	Riesgo	Consecuencia	C	I	D	T	Impacto	Control
Medysis	Riesgo de presupuesto	Inhabilitación del software	3	3	3	9	Alto	El área de sistemas debe contar con matrices, recordatorios de pagos mensuales relacionados con software para evitar suspensiones

Nota. En la tabla se identifica el riesgo con su consecuencia para cada activo y se establece un control. Elaborado por: La autora.

2.1.8.2.4 Activos de tipo empleado. En la tabla 27, se presenta todos los activos filtrados por tipo empleado del área de Protección Social.

Tabla 27

Riesgos de los recursos humanos del área de Protección Social

Activo	Riesgo	Consecuencia	C	I	D	T	Impacto	Control
Auxiliar de Enfermería	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo

Abogada	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Auxiliar de taller	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Ciencia de la Educación	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Carpintero	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	1	2	2	5	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Doctora en Leyes	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Fisioterapeuta	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Licenciada	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un

								alternante de requerirlo
Médico General	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Odontólogo	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Psicoterapeuta	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Psicóloga Clínica	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Paramédico	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo
Psicorrehabiltador	Ausencia del personal por calamidad doméstica, despido o renuncia	Inactividad del área que ejerce el personal	3	3	3	9	Alto	Verificar su importancia en el cargo y de ser el caso tener a su disposición un alternante de requerirlo

Nota. En la tabla se identifica el riesgo con su consecuencia para cada activo y se establece un control. Elaborado por: La autora.

2.1.9 Análisis de riesgo de las áreas de Educación y Protección Social de la FTN

Al concluir la sección anterior se procede en este apartado con el análisis de riesgo, es decir valorizando los activos de las áreas de Educación y Protección Social de manera cuantitativa cabe mencionar que este análisis es uno de los puntos importante en los que hay que enfocarse al momento de elaborar la propuesta del SGSI.

2.1.9.1 Área de Educación. A continuación, se presenta de forma detallada el nombre del activo, grupo al que pertenece, cantidad, valor que se midió de manera cuantitativa y la criticidad en donde se midió de forma cualitativa.

2.1.9.1.1 Activos de tipo hardware. En la tabla 28, se presenta todos los activos filtrados por tipo hardware del área de Educación.

Tabla 28

Valorización de activos de hardware del área de Educación

Descripción	Cantidad	Valor	Criticidad
Computadoras de escritorio HP	1	1.699	Alto
Computadoras de escritorio CLON	1	1.250	Alto
Computadoras de escritorio DELL	1	1.271	Alto
Impresoras EPSON	1	500	Medio
Impresora SHARP	1	500	Medio

Nota. En la tabla se valoriza los activos de hardware. Elaborado por: La autora.

2.1.9.1.2 Activos de tipo empleado. En la tabla 29, se presenta todos los activos filtrados por tipo empleado del área de Educación.

Tabla 29

Valorización de activos de recursos humanos del Área de Educación

Descripción	Cantidad	Valor	Criticidad
Auxiliares	3	488	Alto
Chofer	1	360	Alto
Coordinadora	2	1.634	Alto
Directora	1	2.000	Alto
Educadora	1	778	Alto
Secretaria	1	585	Alto
Técnicas	2	1.466	Alto
Terapeutas	2	1.250	Alto
Trabajadora Social	1	986	Alto

Nota. En la tabla se valoriza los activos de RRHH. Elaborado por: La autora.

2.1.9.2 Área de Protección Social. A continuación, se presenta de forma detallada el nombre del activo, grupo al que pertenece, cantidad, valor que se midió de manera cuantitativa y la criticidad en donde se medió de forma cualitativa.

2.1.9.2.1 Activos de tipo software. En la tabla 30, se presenta todos los activos filtrados por tipo software del área de Protección Social.

Tabla 30

Valorización de activos de software del área de Protección Social

Grupo	Descripción	Cantidad	Valor	Criticidad
Desarrollo	Aplicativo	1	1.500	Alto

Nota. En la tabla se valoriza los activos de software. Elaborado por: La autora.

2.1.9.2.2 Activos de tipo hardware. En la tabla 31, se presenta los activos tipo hardware que tiene el área de Protección Social.

Tabla 31

Valorización de activos de hardware del área de Protección Social

Descripción	Cantidad	Valor	Criticidad
Computadoras de escritorio- ACER	1	750	**Alto**
Computadoras de escritorio- DELL	1	1.271	**Alto**
Laptop- DELL	1	1.772	**Alto**

Nota. En la tabla se valoriza los activos de hardware. Elaborado por: La autora.

2.1.9.2.3 Activos de tipo empleado. En la tabla 32, se presenta todos los activos filtrados por tipo empleado del área de Protección Social.

Tabla 32

Valorización de activos de recursos humanos del área de Protección Social

Descripción	Cantidad	Valor	Criticidad
Auxiliar de Enfermería	2	488	Alto
Abogada	2	986	Alto
Ciencia de la Educación	1	585	Alto
Carpintero	1	400	Alto
Fisioterapeuta	1	800	Alto
Licenciada	1	880	Alto
Médico General	1	1.212	Alto
Odontólogo	1	810	Alto
Psicoterapeuta	1	850	Alto
Psicóloga Clínica	1	1.086	Alto
Paramédico	1	950	Alto
Psicorrehabiltador	1	1.000	Alto

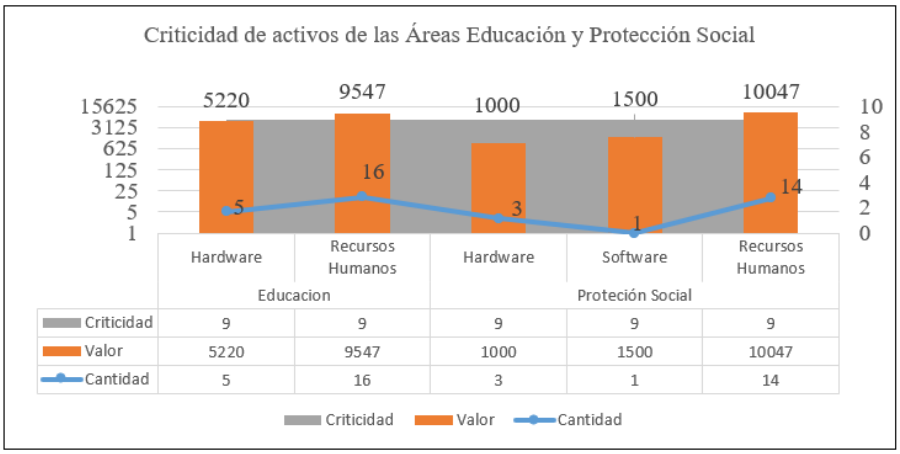
Nota. En la tabla se valoriza los activos de RRHH. Elaborado por: La autora.

2.1.9.3 Resultado del análisis de riesgo de las áreas de Educación y Protección Social

En la figura 8 se presenta el resultado de realizar el análisis a las áreas de Educación y Protección Social, demostrando que tanto los activos de información como recursos humanos son los más afectados, ya sea en temas de desastres naturales, despidos de personal, por ello tal como se muestra en la tabla 24, se propone un control para proteger a dichos activos.

Figura 11

Criticidad de activos de las Áreas Educación y Protección Social



Criticidad de activos de las Áreas Educación y Protección Social

La realización de diferenciación de activos, el análisis de riesgos, y el diagnostico tienen relación ya que se logró identificar que dominios de la norma ISO/IEC 27001 cumplen y no cumplen, se analizó con qué tipos de activos cuentan las áreas de Educación y Protección Social de la FTN, que nivel de impacto generan y a partir de ello se propuso un control que ayuda en gran parte a la prevención del riesgo.

CAPÍTULO III

3.1 PROPUESTA

3.1.1 Alcance del diseño del SGSI

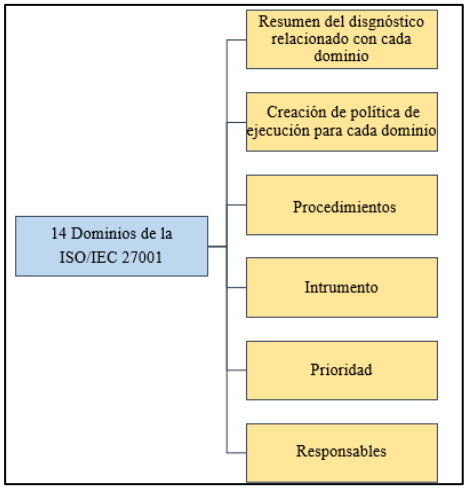
La propuesta de un SGSI para las áreas de Educación y Protección Social de FTN plantea la creación de políticas, controles, procedimientos apropiados para minimizar riesgos que puede tener la información con base al diagnóstico realizado y presentado en el capítulo anterior, garantizando así la triada cid de la misma, basado en la norma internacional ISO/IEC 27001.

3.1.2 Propuesta del sistema de gestión de seguridad de la información para las áreas de educación y protección social de la FTN

En el presente capítulo se presenta la propuesta de implementación de SGSI para las áreas de Educación y Protección Social de la FTN con la siguiente estructura por cada uno de los dominios:

Figura 12

Estructura de SGSI para las áreas de Educación y Protección Social



Nota: Es la estructura con la que se describe cada uno de los dominios para la propuesta del SGSI. Elaborado por: La autora.

A continuación, se explica cada uno de los elementos de la estructura, presentados en la Figura9.

3.1.2.1 Resumen del diagnóstico relacionado con cada dominio. En base al diagnóstico realizado en el capítulo 2, se realiza un resumen analizando si las áreas de Educación y Protección Social realizan el cumplimiento de dominios establecidos en la norma ISO/IEC 27001.

3.1.2.2 Creación de política de ejecución para cada dominio. Se crea la propuesta de política para cada dominio que deberá ser ejecutada por las áreas de Educación y Protección Social.

3.1.2.3 Procedimientos. Se propone la creación de procedimientos, es decir grupo de pasos que se deben cumplir para que la ejecución de la política sea correcta y poder así cumplir con el objetivo de cada dominio**.**

3.1.2.4 Instrumentos. Se propone la creación de instrumentos que se asocian a los procedimientos y a su vez se relacionan con el diagnóstico realizado en el capítulo 2, debido a que es ahí donde se visualizan las principales falencias y necesidades de las áreas de Educación y Protección Social**.**

3.1.2.4 Prioridad. El establecimiento de prioridad se realizó con la colaboración del director del área de Sistemas y mediante la utilización de la tabla 33 la cual presenta cuatro tipos de prioridad estos son inmediato, obligatorio, permanente y periódico. Estos tipos de prioridad se determinaron tomando en cuenta lo establecido en la norma ISO/IEC 27001 y en la perspectiva del director del área de Sistemas debido a que es la autoridad que se encuentra día a día en el manejo de tecnología de la Fundación Tierra Nueva y en base al diagnóstico realizado donde se evidencio la no existencia de un SGSI

lo cual puede traer riesgos hacia la información y convertirse en una vulnerabilidad que afectaría al desarrollo de la misma.

Tabla 33

Prioridad de ejecución

Tipo	Prioridad	Descripción
Urgente	Inmediato	Se considera aquella actividad cuyo tiempo límite está cerca a terminar
	Obligatorio	
Importante	Permanente	Se considera aquella actividad cuyo tiempo límite es variable, es decir puede ser ejecutado en un periodo establecido
	Periódico	

Nota: Prioridad de ejecución. Elaborado por La autora.

3.1.2.5 Responsables. Par el manejo de responsables se maneja por áreas y Comité Interno de Seguridad de la Información, identificando si son encargados de la ejecución o el seguimiento de la propuesta.

3.1.3 Descripción de la propuesta del SGSI por cada dominio de la norma ISO/IEC 27001

3.1.3.1 Dominio de política para la seguridad de la información. A continuación, se presenta la política general que debe ser tomada en cuenta para toda la Fundación, debido a que a partir de ella se puede continuar con el desarrollo de cada dominio específicamente para las áreas de Educación y Protección Social.

Resumen de diagnóstico:

En el diagnóstico realizado al dominio de políticas de seguridad ver tabla 10 se evidenció la inexistencia de un SGSI en la FTN por lo tanto es de vital importancia la

implementación de la política y para ello se determinó el alcance del SGSI de acuerdo con los términos de la organización.

Creación de política de seguridad de la información:

La Fundación Tierra Nueva, enfocada en brindar servicios de Salud, Educación y Protección Social con calidad y calidez en el cumplimiento de su misión, visión y valores para satisfacer las necesidades de usuarios, colaboradores, se compromete en la ejecución de un SGSI de la siguiente manera:

- La seguridad de la información debe estar liderada por la alta gerencia, quien desempeña un papel fundamental para la adopción de los lineamientos a nivel de toda la fundación, deberá definir la estructura, los roles y responsabilidades con respecto a la seguridad de la información.
- Se debe conformar un comité de seguridad de la información que estará conformado por los funcionarios de la FTN, los cuales aprobaran la implementación de las políticas y controles necesarios para preservar la seguridad de la información de la Fundación.
- Cumplir con los requerimientos legales y reglamentarios aplicables a la Fundación y al SGSI.
- Entregar resultados, con sentido de pertenencia, actitud proactiva y comunicación continua y propia.
- Deben existir requisitos obligatorios de capacitaciones en temas técnicos de su rol, de procesos de calidad, de capacitación y concienciación en temas relacionados con la seguridad de la información.
- Deberán implementarse controles de personal para asegurar que los individuos a los que se les concede el acceso a los activos son adecuadamente seleccionados,

evaluados y capacitados, teniendo en cuenta los principios de segregación de funciones sean utilizados en la asignación de funciones críticas.

- Los activos informáticos deberán tener apropiados controles físicos y lógicos para protegerlos contra accesos no autorizados. Para lograr esto de forma periódica se deberá realizar una evaluación de riesgos de los activos de información para establecer los adecuados requisitos de protección.

Procedimientos

Para la creación de procedimientos, se tomará en cuenta los dos primeros objetivos, que se consideran críticos debido a que tal como lo indica la Norma ISO/IEC 27001 la alta gerencia y la creación de comité interno de seguridad son la base fundamental para que el SGSI se desarrolle correctamente.

Procedimiento para la seguridad de la información liderada por la alta gerencia

Para cumplir con el objetivo, se debe ejecutar el siguiente procedimiento:

1. Identificar los miembros que pertenecen a la alta gerencia
2. Definir los roles que tendrá cada miembro con respecto a la seguridad de la información.
3. Planificar reuniones cada seis meses para comprobar el desempeño de roles de cada miembro de la alta gerencia.
4. Receptar y aprobar políticas de seguridad de la información

Procedimiento para la creación de comité de seguridad de la información

Para cumplir con el objetivo, se debe ejecutar el siguiente procedimiento:

1. Deberá ser conformado de forma paritaria es decir por representantes de cada una de las áreas que se manejan en la fundación, por un especialista en seguridad de la información.
2. Cada miembro se comprometerá a tener un suplente elegido de igual manera mencionado en el punto 1.
3. Analizar y proponer políticas y controles referentes a la seguridad de la información que ayudarán a mantener un control en cada una de las áreas de la fundación.
4. Realizar reuniones cada tres meses con la alta gerencia para mostrar las políticas y controles desarrollados y obtener su aprobación para poder ejecutarlas.
5. Ejecutar las políticas y controles
6. Difundir cada aprobación de política y control a todo el personal de la fundación para tener un mejor conocimiento de lo que se está realizando para mejorar de la misma.

Instrumentos:

- Documentación física y digital de la política de seguridad de la FTN.

Prioridad:

- Su ejecución es inmediata, tal como se justifica en la sección 3.2.1

Responsable:

- Alta gerencia y el Comité Interno de Seguridad de la Información, encargado de la ejecución.

Nota: El dominio de políticas de seguridad de la información es el único que tiene alcance para toda la organización, a partir del segundo dominio son de alcance del área de Educación y Protección Social.

3.1.3.2 Dominio de organización de la información. A partir de este dominio se realiza la propuesta de seguridad de la información para las áreas de Educación y Protección Social**.**

Resumen de diagnóstico:

En las preguntas aplicadas al dominio de organización de la información ver tabla 10 se pudo verificar que existe un cumplimiento parcial del dominio, que necesita ser reforzado ya que como lo indica la norma ISO/IEC 27001, el enfoque del dominio es tener claras las actividades de gestión de riesgo hacia la información por lo que es necesario mantener la gestión e ir realizando mejoras continuas para fortalecer el cumplimiento de este dominio.

Establecimiento de la organización de la información:

Para llevar una correcta administración de la información en las áreas de Educación y Protección Social de la FTN se debe contar con lineamientos tanto para la parte interna como externa de la misma para ello se propone lo siguiente:

Área de Educación y Protección Social

- Identificar y definir los activos y procesos de seguridad de la información
- Instruir a cada responsable designado en temas de seguridad de la información para que cumplan con responsabilidad su rol.

- Asignar y documentar los responsables que se encargaran de cada proceso de seguridad de la información
- Mantener un apropiado contacto con las autoridades
- Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
- Deberán existir políticas, normas y procedimientos para los proveedores que son consideradas partes externas a la fundación con el fin de proteger el nivel apropiado de seguridad de la información y cumplimiento de servicios, en base a una administración de entrega, monitoreo, revisión de auditoría de sus servicios.
- La administración de respaldos, que establezcan las reglas para mantener la integridad y disponibilidad de procesamiento de información y servicios de comunicación.
- La manipulación de medios, que indiquen las reglas para proteger documentos, medios de almacenamiento (cintas, discos, y otros medios) y documentación de sistema contra los daños, acceso no autorizado, y para prevenir interrupciones de las actividades de la fundación.

Procedimientos

Para la creación de procedimientos, se tomará en cuenta los dos primeros objetivos, que se consideran críticos esto debido a como lo indica la norma ISO/IEC 27001 la identificación, definición y capacitación de los activos de seguridad de la información es fundamental en cada organización.

Procedimiento para identificar y definir los activos y procesos de seguridad de la información.

1. Analizar cada uno de los activos que tienen las áreas de Educación y Protección Social.
2. Identificar responsabilidades que tienen cada una de las áreas con cada activo asignado.
3. Realizar un inventario de activos que tiene cada área referente a la información para llevar un control de los mismos.

Capacitar a cada responsable designado en temas de seguridad de la información para que cumplan con responsabilidad su rol.

1. Identificar que cada activo cuente con responsables de cada una de las áreas mencionadas.
2. Evaluar el nivel de conocimiento de cada responsable de los activos de la información.
3. Solicitar autorización de alta gerencia para la capacitación de responsables de activos de información.
4. Capacitar a los responsables de cada activo de información.

Instrumento.

- Acuerdo de confidencialidad para terceros
- Formulario para la gestión de accesos para terceros

Prioridad.

- Su ejecución debe ser de forma permanente.

Responsable.

- Comité interno de seguridad encargado de la ejecución.
- Alta gerencia, encargado del seguimiento.

3.1.3.3 Dominio de seguridad en recursos humanos.

Resumen de diagnóstico:

En las preguntas aplicadas al dominio de seguridad de recursos humanos ver tabla 10 se pudo verificar su cumplimento y dos procesos incompletos para mejorar los mismos, tal como lo indica la norma ISO/IEC 27001, es importante identificar en qué estado se encuentra el recurso humano, antes, durante o después de asumir el empleo.

Establecimiento de la seguridad de recursos humanos:

Para llevar un correcto cumplimiento del dominio en las áreas de Educación y Protección social de la FTN, para ello se propone lo siguiente:

Área de Educación

- Implementación de acuerdos de confidencialidad que contemple reglamentos y acuerdos de leyes según lo establecido en el código de trabajo y que deberán ser proporcionales a los requisitos de la fundación.
- Verificar los antecedentes penales de los candidatos que aplican a un empleo.
- Confirmación de calificaciones académicas y profesionales

Área de Protección Social

- Mantener actualizado cada fin de mes los roles que cada empleado del área realiza
- Los empleados de la fundación deben hacer conciencia en temas de seguridad de la información.
- Los empleados deberán estar en constantes capacitaciones referente a sus roles dentro del área.

Procedimientos:

Para la creación de procedimientos se tomará en cuenta para el área de Educación la implementación de un acuerdo de confidencial, y para el área de Protección Social la actualización de roles de los empleados, todo esto basado en la norma ISO/IEC 27001.

Área de Educación:

Implementación de acuerdos de confidencialidad que contemple reglamentos y acuerdos de leyes según lo establecido en el código de trabajo y que deberán ser proporcionales a los requisitos de la fundación.

1. Definir responsable del área encargado de la realización del acuerdo
2. Identificar que numerales del código de trabajo tiene relación con los requisitos de la Fundación
3. Solicitar revisión y autorización a la directora del área
4. Entregar el acuerdo al recurso humano que se encuentra por ingresar a la Fundación para su aceptación

<u>Área de Protección Social:</u>

Mantener actualizado cada fin de mes los roles que cada empleado del área debe realizar.

1. Definir responsable de realizar dicha actualización.
2. Identificar si los roles que cada empleado realiza han aumentado o disminuido
3. Solicitar revisión y autorización a la directora del área
4. Divulgar información de roles a cada empleado del área para mantener un orden y seguridad con la información que cada uno utiliza para realizar sus roles dentro de la fundación.

Instrumentos:

- Acuerdos de confidencialidad
- Registro de verificación de antecedentes para el ingreso de personal
- Descripciones de roles de cada empleado
- Evaluaciones de aptitudes

Prioridad:

- Obligatorio al contratar personal para la empresa.

Responsable.

- Comité interno de Seguridad de la Información, encargado del seguimiento.
- Área de Recursos Humanos, encargado de la ejecución.

3.1.3.4 Dominio de Gestión de activos.

Resumen de diagnóstico:

En las preguntas aplicadas al dominio de gestión de activos ver tabla 10 se pudo verificar el no cumplimiento del mismo para llevar un correcto cumplimiento del dominio se aplica lo indicado en la norma ISO/IEC 27001, es decir que se debe llevar un inventario exacto, actualizado, consistente y alineado. A su vez alineado con la gestión de riesgos

Por esa razón en el Capítulo II se elaboró el primer paso para llevar un correcto control de activos, es decir la diferenciación de activos el cual primero identifica el activo para de esta manera ver los riesgos a los cuales se encuentran asociados y qué consecuencias pueden tener estos activos de acuerdo con el nivel de impacto que generaría en las áreas de Educación y Protección social, una vez realizada esa evaluación se planteó un control para cada riesgo de los activos permitiendo llevar un mejor manejo de los mismos.

Establecimiento de la gestión de activos:

Para llevar una correcta gestión de activos tangibles e intangibles dentro de las áreas de Educación y Protección Social de la FTN, para ello se propone lo siguiente:

Área de Educación y Protección Social

- Implementación de inventarios correctamente categorizados y protegidos
- Se deberá considerar como activo crítico, todo aquel que cuyo análisis de impacto en la confidencialidad, integridad y disponibilidad, sea clasificado como medio o alto.

- Todo activo de información deberá tener asignado un propietario o responsable de cada activo de información que le asigne un grado de criticidad de acuerdo a su sensibilidad e importancia para el negocio y que garantice la protección efectiva de dicho activo.
- Se debe identificar y documentar reglas para el uso aceptable de información que usan activos de la Fundación o cuentan con accesos a ellos.
- Todos los empleados, usuarios externos deberán presentar los activos de información que se encuentran a su cargo, a la culminación de contrato.

Procedimientos:

Para la creación de procedimientos se tomará en cuenta para el área de Educación y Protección Social la implementación de inventarios de activos de información correctamente clasificados y protegidos todo esto basado en la norma ISO/IEC 27001.

1. Identificar todos los activos de información que poseen las áreas mencionadas.
2. Clasificar al activo por tipo es decir si es un activo tangible, intangible o un recurso humano.
3. Establecer responsables para cada activo de información
4. Inspeccionar habitualmente las restricciones y clasificaciones de acceso a los activos considerados importantes.
5. Solicitar revisión y autorización a las directoras de cada área

Instrumentos.

- Matriz de inventario de activos,

- Matriz de evaluación de riesgo y control de activos.

Prioridad.

- Obligatorio.

Responsable.

- Directoras de las áreas Educación y Protección Social, encargadas de la ejecución.
- Comité interno de seguridad de la información, encargado del seguimiento.

3.1.3.5 Dominio de control de accesos

Resumen de diagnóstico:

En las preguntas aplicadas al dominio de control de accesos, ver tabla 10, se pudo verificar el no cumplimiento del dominio para llevar un correcto cumplimiento del mismo se aplica lo indicado en la norma ISO/IEC 27001, es decir que se debe restringir el acceso a la información y a la infraestructura donde se procese información.

Establecimiento del control de accesos

Para llevar un correcto cumplimiento del dominio en las áreas de Educación y Protección Social de la FTN, para ello se propone lo siguiente:

<u>Área de Educación y Protección Social</u>

- Se deberá informar a los beneficiarios y empresas de servicios de las obligaciones que deben cumplir en temas de controles de acceso.
- Se prohíbe el acceso a oficinas sin la debida autorización de las directoras de las áreas
- Se deberá contar con una persona encargada de autorizar el acceso a documentación física que reposa en archivadores dentro de cada área de la FTN.
- Se deberá contar con un documento que contenga los perfiles de usuarios existentes, los cargos y la opción a la que tiene acceso.
- Para colaboradores de las áreas de Educación y Protección Social de la FTN que requieran acceso remoto a los servicios de la misma, se deberá solicitar al director del área de Sistemas la creación de VPN, es decir red privada virtual de esta manera se controla la integridad, confidencialidad y disponibilidad de la información.
- Es responsabilidad de cada colaborador el cumplimiento de las medidas de seguridad.

Procedimientos:

Para la creación de procedimientos se tomará en cuenta para el área de Educación y Protección Social, el informar a los beneficiarios y empresas de servicios las obligaciones que deben cumplir en temas de controles de acceso, todo esto basado en la norma ISO/IEC 27001.

<u>Área de Educación y Protección Social</u>

Informar a los beneficiarios empresas de servicios los requisitos que deben cumplir en temas de controles de acceso

1. Las directoras de las áreas deben identificar que personas pueden tener acceso a la información física y digital que se manejan dentro de las mismas
2. Crear identificaciones únicas para cada empleado o proveedor externo que les permita estar vinculados a la información de cada una de las áreas.
3. Eliminar o deshabilitar las identificaciones a empleados o proveedores externos que terminaron su periodo de acceso a la información.
4. Establecer reglamentos y lineamientos de bloqueo cuando los empleados de las áreas se encuentran en vacaciones para evitar pérdidas de usuario y contraseñas

Instrumentos.

- Ficha de documentación de control de acceso a la información

Prioridad.

- Su ejecución es de carácter inmediato

Responsables.

- Comité Interno de Seguridad de la Información y área de Sistemas, encargados de la ejecución y seguimiento

3.1.3.6 Dominio de criptografía.

Resumen de* diagnóstico*:

En las preguntas aplicadas al dominio de criptografía ver tabla 10, se logró verificar el no cumplimiento del dominio para llevar un correcto cumplimiento del mismo se aplica lo indicado en la norma ISO/IEC 27001, es decir proteger la triada CID de la información.

Establecimiento de criptografía:

Para llevar un correcto cumplimiento del dominio en las áreas de Educación y Protección Social de la FTN, para ello se propone lo siguiente:

Área de Educación y Protección Social

- Analizar y definir los métodos criptográficos de cada una de las áreas y la recuperación de la mismas.
- Identificar los responsables de claves y roles dentro de cada área referente al manejo de la información.
- Definir fechas de activación y desactivación de claves, previniendo así el uso inapropiado

Procedimientos:

Para la creación de procedimientos se tomará en cuenta tanto para el área de Educación y Protección Social, el analizar y definir los métodos criptográficos para cada una de las áreas y la recuperación de la misma, todo esto basado en la norma ISO/IEC 27001.

Área de Educación y Protección Social

Analizar y definir los métodos criptográficos para el resguardo de información de cada una de las áreas y la recuperación de la misma.

1. Para poder implementar un método criptográfico, se deberá considerar las restricciones que existen en temas de exportación o importación de hardware y software.
2. Establecer responsables para la ejecución del método criptográfico seleccionado para las áreas de Educación y Protección social.
3. Definir y revisar periódicamente la ejecución del método criptográfico seleccionado relacionado con la confidencialidad, integridad y disponibilidad de la información.

Instrumentos:

- Documentación física y digital de la política de criptografía.
- Solicitud de creación, cambio o eliminación de claves.

Prioridad.

- Su ejecución es de carácter inmediato y obligatorio.

Responsables.

- área de Sistemas y Comité Interno de Seguridad de la Información, encargados de la ejecución y seguimiento.

3.1.3.7 Dominio de seguridad física y ambiental.

Resumen de diagnóstico:

En las preguntas aplicadas al dominio de seguridad física y ambiental ver tabla 10 se logró verificar el no cumplimiento del dominio para llevar un correcto cumplimiento del mismo se aplica lo indicado en la norma ISO/IEC 27001, es decir prohibir el acceso físico no autorizado, el deterioro de las instalaciones donde se trata información y la seguridad ambiental hace referencia a la protección de amenazas que se puede enfrentar al medio ambiente de las áreas de Educación y Protección Social.

Establecimiento de la seguridad física y ambiental:

Área de Educación y Protección Social

El objetivo de esta política es evitar el daño e interferencias tanto del software como del hardware que maneja la fundación protegiéndola de agentes como personal no autorizado, agua, fuego, temperatura, fallos en el suministro eléctrico para ello se propone lo siguiente:

- Se debe considerar que las instalaciones de las áreas mencionadas deben ser físicamente sólidas.
- Se debe contar con sistemas inteligentes como lector de tarjetas que permiten el acceso a personal autorizado.
- Se debe crear un documento donde se llevaría un control de registro de fecha y hora de entrada y salida de personal.

- Para la parte de seguridad de hardware, se toma como ejemplo servidores donde se deberá considerar que debe estar inaccesible para personal no autorizado, además debe soportar cualquier tipo de catástrofe natural.
- Se debe proteger toda clase de equipos para evitar daño, perdidas, o robo por ello todo equipo debe contar con seguro y además se debe crear un documento de acta de entrega, donde se le informa al colaborador de la responsabilidad que tiene con los equipos.

Procedimientos:

Para la creación de procedimientos se tomará en cuenta tanto para el área de Educación y Protección Social, considerar que las instalaciones de las áreas mencionadas deben ser físicamente sólidas, seguridad tecnológica todo esto basado en la norma ISO/IEC 27001.

Área de Educación y Protección Social

Considerar que las instalaciones de las áreas mencionadas deben ser físicamente sólidas.

1. Analizar e identificar el estado que se encuentran las instalaciones con la ayuda de proveedores expertos en el tema.
2. Establecer responsables que interactúen con proveedores para realizar el mantenimiento de las instalaciones de cada área.
3. Solicitar presupuesto para realizar mantenimientos a las instalaciones de cada área.
4. Establecer protocolos de seguridad para el personal que permanece a diario en las instalaciones de cada una de las áreas
5. Solicitar revisión y aprobación de cambios de las instalaciones.

Seguridad tecnológica.

1. Identificar los riesgos a los que se presenta el hardware utilizado en las áreas mencionadas.
2. Establecer responsables que interactúen con proveedores para realizar el mantenimiento de las instalaciones de cada área.
3. Solicitar revisión y aprobación de cambios de las instalaciones.

Instrumento:

- Sistema de video vigilancia en las áreas mencionadas.
- Control de accesos, es decir: tarjetas magnéticas o huellas dactilares
- Registro de accesos para empleados o visitantes

Prioridad:

- Su ejecución es de carácter inmediato y obligatorio.

Responsable:

- Comité Interno de Seguridad de la Información, encargado de la ejecución.

3.1.3.8 Dominio de seguridad en las operaciones.

Resumen de diagnóstico:

En las preguntas aplicadas al dominio de seguridad en las operaciones ver tabla 10 se logró verificar el no cumplimiento del dominio para llevar un correcto cumplimiento del mismo, se aplica lo indicado en la norma ISO/IEC 27001.

Establecimiento de la seguridad en las operaciones.

Área de Educación y Protección Social

Para llevar un correcto cumplimiento del dominio en las áreas de Educación y Protección Social de la FTN, para ello se propone lo siguiente:

- Se deberá realizar instrucciones para el manejo de errores que podrían surgir durante la ejecución del trabajo dentro de las áreas mencionadas
- Se deberá valorar los impactos potenciales que generan cambios que afectan la seguridad de la información.
- Realizar procesos de validación de instalación, configuración y administración de sistemas y aplicaciones.
- Se deberá incluir un manejo de errores y condiciones exponenciales que pueden definirse como incidentes de seguridad.
- Se debe proteger las operaciones sobre software malicioso, utilizando técnicas como doble factor de autenticación, la implementación de la herramienta antígeno, la cual examina si el correo electrónico es considerado virus, si lo es no permite el ingreso del mismo al sistema, genera una alerta para que el área de Sistemas este vigilante diariamente y sobre todo que se asegure la información.

Procedimientos:

Para la creación de procedimientos se tomará en cuenta tanto para el área de Educación y Protección Sociall, considerar la realización de instrucciones para el manejo de errores que podrían surgir durante la ejecución del trabajo dentro de las áreas mencionadas todo esto basado en la norma ISO/IEC 27001.

Área de Educación y Protección Social

Realizar instrucciones para el manejo de errores que podrían surgir durante la ejecución del trabajo.

1. Identificar el responsable que realizará las instrucciones dentro de las áreas mencionadas.
2. Verificar lo sucedido con el manejo de errores y generar reporte explicando lo sucedido.
3. Ejecutar un plan de control de cambios para mejor el proceso de manejo de errores.
4. Solicitar revisión y aprobación

Instrumento.

- Lista para la verificación de la implementación de firewalls en los sistemas de comunicación de las áreas de Educación y Protección Social.
- Solicitudes de Cambio

Prioridad.

- Su ejecución es periódica.

Responsable.

- Área de Sistemas, encargada de la ejecución.

3.1.3.9Dominio de transferencia de información.

Resumen de diagnóstico:

En la pregunta aplicada sobre el dominio de transferencia de información ver tabla 7 se logró verificar el no cumplimiento del dominio para llevar un correcto cumplimiento del mismo se aplica lo indicado en la norma ISO/IEC 27001, es decir asegurar el intercambio de información de forma adecuada y bajo la protección necesaria.

Establecimiento de transferencia de la información:

Para llevar un correcto cumplimiento del dominio en las áreas de Educación y Protección Social de la FTN, para ello se propone lo siguiente:

Área de Educación y Protección Social

- El intercambio de información reservada, pública o sensible deberán ser llevados por medio de acuerdos, controles o protocolos indicando en ellos como será tratada la información.
- Debe existir un responsable, encargado de guiar el traspaso de información.
- Para el traslado de la información se deben mitigar los riesgos.

Procedimientos:

Para la creación de procedimientos se tomará en cuenta tanto para el área de Educación y Protección Social, considerar la política de debe existir un responsable, encargado de guiar la transferencia de información, todo esto basado en la norma ISO/IEC 27001.

Área de Educación y Protección Social

Debe existir un responsable, encargado de guiar la transferencia de información.

1. Definir el rol que va a realizar el miembro dentro de las áreas mencionadas.
2. Capacitar al miembro de las áreas que realizara la transferencia de información.
3. Verificar el trabajo realizado por el miembro de las áreas cada tres meses.

Instrumento:

- Acta de trasferencia de información.

Prioridad.

- Su ejecución es de carácter inmediato y obligatorio.

Responsable.

- Comité interno de seguridad, encargado de la ejecución.

3.1.3.10 Dominio de adquisición de sistemas, desarrollo y mantenimiento.

Resumen de diagnóstico:

En las preguntas aplicadas al presente ver tabla 10 se logró verificar el no cumplimiento del dominio para llevar un correcto cumplimiento del mismo se aplica lo indicado en la norma ISO/IEC 27001, es decir cerciorar que la seguridad de la información sea parte integral de los sistemas de información.

Establecimiento de adquisición de sistemas, desarrollo y mantenimiento:

Para llevar un correcto cumplimiento del dominio en las áreas de Educación y Protección Social de la FTN, para ello se propone lo siguiente:

Área de Educación y Protección Social

- Llevar un registro de controles de cada aplicación implementada para asegurar el correcto procesamiento de información dentro de cada una de las áreas mencionadas.
- Identificar el uso y ubicación de los aplicativos, además de controlar, verificar y revisar continuamente los registros y controles de integridad de la información.
- Se deberá realizar un proceso formal de adquisición y pruebas, cuando un producto se adquiere por primera vez.
- Se deberá contar con normas de programación, versionamiento y documentación para los sistemas a realizarse.
- Se deberá incluir pruebas funcionales y no funcionales a la información
- Se deberá considerar los procedimientos necesarios en la etapa de diseño, para realizar revisiones periódicas de contenidos de campos, registros o archivos considerados sensibles y con procesos de limpieza de datos y otros procesos relacionados con optimización y rendimiento.
- Se debe tener dos o más responsables que están a cargo en el proceso de adquisición, desarrollo y mantenimiento de sistemas.
- Se deberá realizar capacitaciones a los colaboradores de las áreas para tener un conocimiento sobre el tiempo en el que se debe realizar mantenimiento tanto a sistemas como al equipo físico.

Procedimientos:

Para la creación de procedimientos se tomará en cuenta tanto para el área de Educación y Protección Social, considerar la política de llevar un registro de controles de cada

aplicación implementada para asegurar el correcto procesamiento de información dentro de cada una de las áreas mencionadas, todo esto basado en la norma ISO/IEC 27001.

Área de Educación y Protección Social

Llevar un registro de controles de cada aplicación implementada para asegurar el correcto procesamiento de información.

1. Identificar el personal responsable de la realización de registro de controles en cada una de las áreas mencionadas.
2. Verificar el cumplimiento y la correcta ejecución del aplicativo que ayudará al desarrollo de las áreas mencionadas anteriormente

Instrumento:

- Verificación de cláusulas de control de mantenimiento en contratos.
- Formato de solicitud de cambios-desarrollo
- Acuerdos de desarrollo-pruebas e implementación de sistemas.

Prioridad:

- Su ejecución es inmediato y obligatoria.

Responsable.

- Área de Sistemas, encargado de la ejecución
- Comité de Seguridad de la Información, encargado del seguimiento.

3.1.3.11 Dominio de relación con proveedores.

Resumen de diagnóstico:

En la pregunta aplicada al dominio de relación con proveedores ver tabla 7 se logró verificar el no cumplimiento del dominio para llevar un correcto cumplimiento del mismo se aplica lo indicado en la norma ISO/IEC 27001, es decir asegurar la información de las áreas de Educación y Protección Social que sea accesibles a los proveedores

Establecimiento de la relación con proveedores:

Para llevar un correcto cumplimiento del dominio en las áreas de Educación y Protección Social de la FTN, para ello se propone lo siguiente:

Área de Educación y Protección Social

- Identificar y documentar tipos de proveedores.
- Se deberá documentar y establecer acuerdos de privacidad entre las áreas mencionadas anteriormente y los proveedores para el aseguramiento de lo solicitado y evitando así malentendidos.
- Crear un proceso para la gestión de relaciones con proveedores.
- Exigir controles de seguridad de la información
- Se implantarán mecanismos necesarios para que las decisiones de contratación con proveedores se tomen en beneficio de la fundación.
- Se deberá realizar documentación que valide el cumplimiento de acuerdo de nivel de servicio que el proveedor ofrece al realizar su trabajo.

Procedimientos:

Para la creación de procedimientos se tomará en cuenta tanto para el área de Educación y Protección Social, considerar las dos primeras políticas ya que es de suma importancia identificar y documentar tipos de proveedores y establecer acuerdos de privacidad entre las áreas mencionadas anteriormente y los proveedores, todo esto basado en la norma ISO/IEC 27001.

Área de Educación y Protección Social

Identificar y documentar tipos de proveedores.

1. Identificar que se necesita obtener de los proveedores
2. Identificar el personal responsable de mantener acercamiento con proveedores externos.
3. Definir controles a aplicar con proveedor externos.
4. Solicitar revisión y aprobación a directora del área.

Establecer acuerdos de privacidad entre las áreas mencionadas anteriormente y los proveedores.

1. Identificar el personal responsable de mantener acercamiento con proveedores externos.
2. Realizar una descripción de la información que el proveedor obtendrá acceso.
3. Identificar los requisitos legales referente a los datos, derechos de propiedad intelectual y derechos de autor.

Instrumento.

- Documentación física y digital de las políticas para la relación con proveedores.
- Acuerdo de confidencialidad
- Lista de control de personal de proveedor autorizado a tener acceso a la información

Prioridad.

- Su ejecución es inmediato y obligatorio.

Responsable.

- Comité Interno de Seguridad de la Información, encargado de la ejecución y seguimiento.

3.1.3.12 Dominio de gestión de los incidentes de seguridad.

Resumen de diagnóstico:

En la pregunta aplicada al dominio de relación con proveedores, ver tabla 10, se logró verificar el cumplimiento parcial del dominio para llevar un correcto cumplimiento del mismo se aplica lo indicado en la norma ISO/IEC 27001, es decir que, para la gestión de incidentes de las áreas de Educación y Protección Social, debe existir un objetivo claro y eficaz.

asegurar un enfoque claro y eficaz para la gestión de incidentes de seguridad de la información de las áreas de Educación y Protección Social.

Establecimiento de la gestión de incidentes de seguridad:

Para llevar un correcto cumplimiento del dominio en las áreas de Educación y Protección Social de la FTN, para ello se propone lo siguiente:

Área de Educación y Protección Social

- Para la evaluación de riesgos se deben definir roles y responsabilidades dentro de las áreas mencionadas anteriormente.
- Debe existir un responsable de seguridad de la información para tratar incidentes que podría afectar a las operaciones de las áreas.
- Todo incidente de seguridad que sea reportado debe ser registrado y elaborado creando un documento que contemple, nombre del reporte, asignación, tratamiento, respuesta y cierre.
- Se propone una clasificación de alta, medio, baja al incidente para poder gestionarlo en tiempos que se acorde con comité de seguridad de la información.

Procedimientos:

Para la creación de procedimientos se tomará en cuenta tanto para el área de Educación y Protección Social, considerar las dos primeras políticas que son definir roles y responsabilidades e informar de manera inmediata al responsable de Seguridad de la Información, la existencia de incidentes que podría afectar a las operaciones de las áreas, todo esto basado en la norma ISO/IEC 27001.

Área de Educación y Protección Social

Definir roles y responsabilidades.

1. Identificar el personal responsable de realizar planificación y preparación de respuestas a incidentes.
2. Identificar brechas en las responsabilidades asignadas al personal.
3. Realizar una matriz para definir los roles que cada personal asignado al tema de incidentes debe realizar.

Informar de manera inmediata al responsable de seguridad de la información, la presencia de incidentes que podría afectar a las operaciones de las áreas.

1. Identificar la causa del incidente
2. Preparar reporte del incidente
3. Solicitar revisión y aprobación del director de cada una de las áreas.

Instrumento.

- Formulario de aviso de incidente dentro de la FTN.

Prioridad.

- Su ejecución es inmediato y obligatorio.

Responsable.

- Comité Interno de Seguridad de la Información y el área de Sistemas, encargados de la ejecución y seguimiento

3.1.3.13 Dominio de continuidad del negocio.

Resumen de diagnóstico:

En la pregunta aplicada al dominio de continuidad del negocio ver tabla 10 se logró verificar el no cumplimiento del dominio. Para llevar un correcto cumplimiento del mismo se aplica lo indicado en la norma ISO/IEC 27001, es decir especificar los requisitos para una correcta planificación, implementación y mantenimiento continuo de la gestión de continuidad de negocio permitiendo proteger y responder a incidentes.

Establecimiento de la continuidad del negocio:

Para llevar un correcto cumplimiento del dominio en las áreas de Educación y Protección Social de la FTN, para ello se propone lo siguiente:

Área de Educación y Protección Social

- Establecer los requerimientos para llevar una correcta continuidad del negocio.
- Realizar un análisis de impacto en la seguridad de la información.
- Asignar responsables para activar el plan de continuidad en situaciones consideradas emergencia.
- Los procesos críticos deben ser recuperados en tiempo estipulado en el plan de continuidad de negocio.
- La continuidad del negocio deberá cuidar por la seguridad que aplica al personal de las áreas mencionadas.

Procedimientos:

Para la creación de procedimientos se tomará en cuenta tanto para el área de Educación y Protección Social, las dos primeras políticas que son establecer los requerimientos

para llevar una correcta continuidad del negocio y realizar un análisis de impacto en la seguridad de la información todo esto establecido en la norma ISO/IEC 27001.

Área de Educación y Protección Social

Establecer los requerimientos para llevar una correcta continuidad del negocio

1. Mantener reuniones con directores de las áreas mencionadas para identificar los requisitos a implementar para tener una correcta continuidad del negocio.
2. Asignar responsables que se encarguen de la verificación y estimación de la continuidad de la seguridad de la información.

Asignar responsables para activar el plan de continuidad en situaciones consideradas emergencia.

1 Identificar el personal encargado de realizar las funciones de activación de plan de contingencia.
2 Comprobar el estado físico de los componentes de hardware y software
3 Crear un protocolo de recuperación de los mismos.
4 Solicitar revisión y aprobación.

Instrumento.

- Documentación física y digital del plan de continuidad del negocio.

Prioridad.

- Su ejecución es inmediata y obligatoria.

Responsable.

- Comité interno de seguridad, encargado de la ejecución y seguimiento.

3.1.3.14 Dominio de cumplimiento con requerimientos legales y contractuales.

Resumen de diagnóstico:

En las preguntas aplicadas al presente dominio ver tabla 10 se logró verificar el cumplimiento parcial del mismo. Para llevar un correcto cumplimiento del mismo se aplica lo indicado en la norma ISO/IEC 27001, es decir controlar y garantizar el cumplimento de las políticas, normas y legislación enfocándose a la seguridad de la información.

Establecimiento de cumplimientos legales y contractuales:

Para llevar un correcto cumplimiento del dominio en las áreas de Educación y Protección Social de la FTN, para ello se propone lo siguiente:

Área de Educación y Protección Social

Cumplir con las leyes, los reglamentos y obligaciones contractuales requeridas para la seguridad de la información, entre los procedimientos aplicarse para este dominio están los siguientes:

- Identificar la documentación de proveedores.
- Definir tipos de acceso a la información.

- Realizar un seguimiento a proveedores sobre el cumplimiento en el aseguramiento de la información.
- Revisión independiente de la seguridad de la información.
- Cumplimiento de la política y las normas de seguridad.

Procedimientos:

Para la creación de procedimientos se tomará en cuenta tanto para el área de Educación y Protección Social, las dos primeras políticas que son la identificación de la documentación de proveedores y definir tipos de acceso a la información, todo esto basado en la norma ISO/IEC 27001.

Área de Educación y Protección Social

Identificar la documentación de proveedores.

1. Identificar y documentar requisitos legales que deben tener las áreas mencionadas.
2. Identificar el personal encargado en recolectar temas legales de las áreas mencionadas.
3. Solicitar revisión y aprobación.

Definir tipos de acceso a la información

1 Realizar lineamientos que definan el uso legal del software, como por ejemplo temas de licenciamiento.

2 Realizar pruebas de capacidad de licenciamiento para evitar redundancia de usuarios.

Prioridad.

- Su ejecución es inmediato y obligatorio.

Responsable.

- Comité Interno de Seguridad de la Información, encargado de la ejecución y seguimiento.

CONCLUSIONES

- Con la ejecución del diagnóstico realizado a las áreas de Educación y Protección Social de la Fundación Tierra Nueva, se determinó la no existencia de un Sistema de Gestión de Seguridad de la Información, lo cual permitió el planteamiento de la propuesta del mismo para que las áreas mencionadas empiecen a manejar su información de manera segura y con base en la norma ISO/IEC 27001 para lograr si lo desean una certificación a futuro.
- Con la identificación de los activos de las áreas de Educación y Protección Social se logra tener una visión clara de lo que cada área tiene internamente, es decir activos de información tal como acuerdo de confidencialidad, hardware, software y recursos humanos, permitiendo asegurar la calidad y credibilidad de los mismos.
- El análisis de riesgos realizado a cada uno de los activos de las áreas de Educación y Protección Social, permite establecer controles que ayuda a evitar vulnerabilidades dentro de la Fundación.
- La utilización de la norma ISO 27001 en el proyecto de titulación fue fundamental, ya que, es la fuente de lineamientos en cada uno de sus dominios que aportan para el desarrollo de un Sistema de Gestión de Seguridad de la Información.
- La implementación de un Sistema de Gestión de Seguridad de la Información es la base primordial en organizaciones con cierto nivel de madurez, debido a que se protege a su activo más importante que es la información y sus tres principios que son la confidencialidad, integridad y disponibilidad.
- Con la elaboración de la propuesta de Sistema de Gestión de Seguridad de la Información, se tienen políticas e instrumentos que serán evaluados por el Comité de

Seguridad de la Información y la Alta Gerencia para la toma de decisiones llevando a un manejo correcto de información dentro de la Fundación Tierra Nueva.

RECOMENDACIONES

- Es sumamente importante que la alta gerencia y el Comité de Seguridad de la Información se comprometan a revisar, cumplir y poner en marcha cada uno de los puntos tratados en esta propuesta para obtener un correcto aseguramiento de la información, con el objetivo de reducir el nivel de riesgo tanto de los activos de información como los activos informáticos, que cumplen un papel importante en todo este proceso.
- Se recomienda realizar inventarios de activos tangibles e intangibles anuales con la finalidad de que cada área de la fundación sepa en qué estado se encuentran cada uno de ellos y poder tomar iniciativas en conjunto con el comité de Seguridad de la Información para la implementación de nuevos controles y así evitar pérdidas o daños que pueden generar ruido en el desarrollo de las actividades de la Fundación.
- Se recomienda la creación de una política continua de capacitación hacia el personal de las áreas de Educación y Protección Social con respecto de la Seguridad de la Información y sobre el Sistema de Gestión de Seguridad de la Información para mantener una cultura y compromiso frente a la confidencialidad, integridad y disponibilidad de la información.
- Se recomienda llevar un correcto manejo de control de accesos, utilizando lo establecido en la propuesta, identificando así que colaborares o personas externas a la fundación pueden tener acceso a la información, evitando así vulnerabilidades de la misma.
- Se recomienda que toda creación de políticas, controles, lineamientos realizada por el Comité de Seguridad de la Información y aprobada por la alta gerencia sea publicada a todo el personal de la Fundación y con ello evitar un desconocimiento de todos los cambios que la Fundación tome para su crecimiento y fortalecimiento en la seguridad.

GLOSARIO

FTN: Fundación Tierra Nueva.

SGSI: Sistema de Gestión de la Seguridad de la Información.

ISO: International Organization for Standardization.

IEC: Comisión Electrotécnica Internacional.

CID: Confidencialidad, Integridad, Disponibilidad.

PDCA: Plan, Do, Check, Act.

TI: Tecnologías de la Información

LISTA DE REFERENCIAS

Articulo Académico:

Leidy-Johanna Cárdenas-Solano, H. M.-A.-E.-A. (2016). GESTION DE SEGURIDAD DE LA INFORMACION: REVISION BIBLIOGRAFICA. *Gale Power*, 18. doi:http://bibliotecas.ups.edu.ec:2099/10.3145/epi.2016.nov.10

Libro:

Cardel, A. (2017). Nueve pasos para el exito- Una visión de conjunto para la aplicación de la ISO 27001:2013. Reino Unido: IT Governance Ltd- ISBN: 9781849290. Obtenido de https://bibliotecas.ups.edu.ec:2708/lib/upsal/detail.action?docID=5255165

Páginas Web:

Alvarado, C. V. (2021). *PENSEMOS* . Obtenido de https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

Bahillo, L. (2021). *Marketing4ecommerce*. Obtenido de https://marketing4ecommerce.net/historia-de-internet/

Calle, J. P. (2020). *Opirani*. Obtenido de https://www.piranirisk.com/es/blog/5-m%C3%A9todos-de-an%C3%A1lisis-de-riesgos

Cardel, A. (2017). *Nueve pasos para el exito- Una visión de conjunto para la aplicación de la ISO 27001:2013.* Reino Unido: IT Governance Ltd- ISBN: 9781849290. Obtenido de https://bibliotecas.ups.edu.ec:2708/lib/upsal/detail.action?docID=5255165

Copyright. (2015). Obtenido de https://destinonegocio.com/co/gestion-co/recursos-materiales-co-co/sistemas-de-seguridad/#:~:text=En%20este%20sentido%2C%20los%20sistemas,almacenada%20en%20sus%20sistemas%20inform%C3%A1ticos.

DTICS Fundación Tierra Nueva . (2022). *Fundación Tierra Nueva*. Obtenido de https://www.fundaciontierranueva.org.ec/

Gomez, M. M. (2010). Método de análisis por indicadores para evaluar la gestión del conocimiento en empresas manufactureras.

Grupo ACMS. (2020). *Grupo ACMS CONSULTORES*. Obtenido de https://www.grupoacms.com/noticias/iso-27009-seguridad-en-la-informacion-actualizada

HACKNOID. (2020). *HACKNOID*. Obtenido de https://www.hacknoid.com/hacknoid/importancia-de-la-seguridad-informatica-de-las-empresas/

INGERTEC. (2021). *Fase 4- Planificación del SGSI*. Obtenido de https://normaiso27001.es/fase-4-planificacion-del-sgsi/

INGERTEC. (2021). *ISO 27001*. Obtenido de https://normaiso27001.es/fase-5-documentacion-del-sgsi/

Intedya. (2015). *Intedya International Dynamic Advisors*. Obtenido de https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjunto-de-estandares-de-seguridad-de-la-informacion.html

ISO/IEC27001. (10 de 01 de 2013). Tecnología de la información, técnicas de seguriddad sistemas de gestión de la seguridad de la información, requisitos.

ISO27000.ES. (2005). *ISO27000*. Obtenido de SGSI-Información fundamental sobre el significado y sentido de implantación y mantenimento de los Sistemas de Gestión de la Seguridad de la Información: https://www.iso27000.es/iso27000.html

ISOTools. (2016). *ISOTools*. Obtenido de https://www.isotools.cl/principales-causas-los-fallos-la-seguridad-la-informacion/

Leidy-Johanna Cárdenas-Solano, H. M.-A.-E.-A. (2016). GESTION DE SEGURIDAD DE LA INFORMACION: REVISION BIBLIOGRAFICA. *Gale Power*, 18. doi:http://bibliotecas.ups.edu.ec:2099/10.3145/epi.2016.nov.10

LISA Institute. (2021). *LISA Institute*. Obtenido de https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion

Movistar. (2015). Obtenido de https://destinonegocio.com/co/gestion-co/recursos-materiales-co-co/sistemas-de-seguridad/#:~:text=En%20este%20sentido%2C%20los%20sistemas,almacenada%20en%20sus%20sistemas%20inform%C3%A1ticos.

Muñoz, I. (2020). *IBERO*. Obtenido de https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

Navarro, J. (2010). *Curso de Auditoría en Informática*. Obtenido de https://sites.google.com/site/avauditoriaeninformatica/home/modulo-3-tecnicas-y-herramientas-de-la-auditoria-de-sistemas/entrevistas-cuestionarios-y-encuestas-para-la-auditoria-de-sistemas#:~:text=La%20entrevista%20como%20la%20principal,los%20aspectos%20q

Opirani. (2014). *Opirani*. Obtenido de https://www.piranirisk.com/es/academia/especiales/14-metodos-y-herramientas-para-gestionar-el-riesgo

QuestionPro. (2021). *QuestionPro*. Obtenido de https://www.questionpro.com/blog/es/cuestionario-de-control-interno/

Seguridad y Privacidad de la Información. (15 de 03 de 2016). *Guía para la Gestión y Clasificación de Activos de Información*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

SGSI. (2014). *Sistema de Gestión de Seguridad de la Información*. Obtenido de https://www.pmg-ssi.com/2014/02/isoiec-27008-controles-de-seguridad-de-informacion/

SGSI. (2018). *Sistemas de Gestión*. Obtenido de https://www.pmg-ssi.com/2018/04/verificaciones-seguridad-segun-iso-27001/

SGSI. (2021). *Sistema de Gestión de Seguridad de la Información*. Obtenido de https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Vispo, Y. (9 de julio de 2018). *RumboEficiente*. Obtenido de https://www.rumboeficiente.com/estrategias-establecer-prioridades/