Política de Seguridad de la Información basada en la Norma ISO/IEC 27001 para la Secretaria de Educación del Chocó

Jahaira Ceballos Córdoba

Asesor

Cesar Villamizar

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTIC

Maestría en Gestión de Tecnologías de la Información

2025

Resumen

Este proyecto desarrolla una Política de Seguridad de la Información basada en la Norma ISO/IEC 27001 para la Secretaría de Educación del Chocó (SEDCHOCÓ), con el propósito de fortalecer la protección y gestión de la información dentro de la entidad, garantizando confidencialidad, integridad y disponibilidad de los activos. A través de un diagnóstico detallado, se identificaron riesgos y vulnerabilidades, permitiendo estructurar una política de control en áreas clave como acceso a la información, uso de activos, respaldo de datos y gestión de incidentes. La propuesta también contempla la capacitación del personal, monitoreo continuo y evaluación de la seguridad, asegurando el cumplimiento de estándares internacionales y normativas colombianas para mejorar la gestión de TI en la institución.

Palabras clave: Política de Seguridad de la Información, Norma ISO/IEC 27001, Secretaría de Educación del Chocó.

Abstract

This project develops an Information Security Policy based on the ISO/IEC 27001 Standard for the Ministry of Education of Chocó (SEDCHOCÓ), with the purpose of strengthening the protection and management of information within the entity, guaranteeing confidentiality, integrity and availability of assets. Through a detailed diagnosis, risks and vulnerabilities were identified, allowing a control policy to be structured in key areas such as access to information, use of assets, data backup and incident management. The proposal also contemplates staff training, continuous monitoring and security evaluation, ensuring compliance with international standards and Colombian regulations to improve IT management in the institution.

Keywrds: Information Security Policy, ISO/IEC 27001 Standard, Chocó Ministry of Education.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Introducción

Cuando hablamos de información nos vemos obligados a enfocarnos en que está cada vez es más vulnerable en las entidades públicas, razón por la cual, los riesgos que corre el manejo de la información se convierten en un tema de gran relevancia. Esta investigación se enfocará en una problemática que aborda la gobernación del Chocó, a través de la Secretaria de Educación, con respecto a la información que circula en los equipos del ente gubernamental y la información que subyace en los equipos de los empleados y/o contratistas, debido a que la información de suma importancia para el desarrollo de las actividades de manera eficaz y eficiente, reposa en los computadores personales de los funcionarios y/o contratistas, siendo esto un motivo para que la información confidencial de la empresa este guardada en espacios que inadecuados, convirtiéndola en vulnerable, principalmente, porque no se garantiza la confiabilidad de los procesos que se adelantan en las diferentes dependencias de esta secretaría, debido a la libertad frente del manejo de la información y los archivos importantes que reposan en sus computadores personales, que además, una vez dejan de ser funcionarios de la entidad, aumenta el riesgo de que dicha información pueda ser utilizada para fines desconocidos, es por eso que se percibe la necesidad de una investigación de base que permita dar solución a este proceso, mediante el estudio detallado del manejo de la información y los equipos por lo que rota la información, haciendo cumplir los protocolos de manejo de información en la SEDCHOCÓ, visualizando la implementación de protocolos que sirvan para control dicha problemática.

Planteamiento del Problema

El planteamiento del problema, se enmarca en que, tal y como lo plantea Yaima (2022) en la investigación titulada "requerimientos para un sistema de gestión de documento electrónico de archivo en entidades privadas del sector real en Bogotá", en la actualidad la transformación del sistema documental al electrónico con capacidad de almacenamiento y seguridad idónea para la gestión documental, es una de las mayores preocupaciones que enfrentan las entidades públicas.

En igual sentido, Corrales (2020) ha afirmado que, teniendo en cuenta que el proceso de gestión documental es transversal a toda organización, ello implica que cuando se requiera diseñar un proyecto de transformación digital para el proceso de gestión documental, se verifique que haya una alineación con la plataforma estratégica de la entidad, es decir, con los objetivos estratégicos de la entidad, a fin de poder trabajar de forma articulada con la entidad y lograr el éxito del proyecto, facilitando con ello que la entidad mejore su modo de operación para la prestación de servicios públicos, siendo más eficiente y efectiva, ofreciendo a su vez mayor transparencia, operatividad y satisfacción a la ciudadanía.

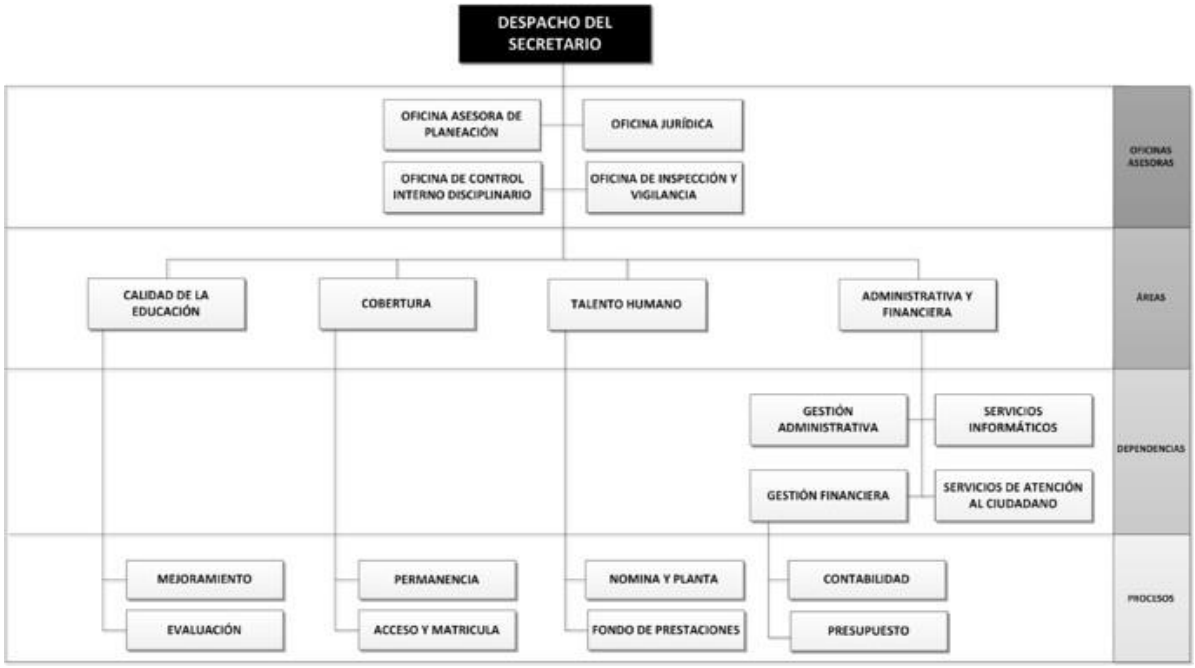
De igual manera, debe resaltarse que, el Estado colombiano, ha impartido una serie de instrucciones y orientaciones, a través de diferentes normas, ello con el fin de avanzar en la implementación de estrategias de transformación digital enfocadas al proceso de gestión documental, las cuales se han puesto a disposición de la administración pública y el sector empresarial en general, herramientas fundamentales para integrar los procesos de transformación digital y gestión documental, y ello obedece a que, la gestión de documentos está ligada a la

actividad administrativa del Estado, al cumplimiento de las funciones y al desarrollo de los procesos y procedimientos de todas las entidades.

En concordancia con lo anterior, y a fin de adentrarnos al tema objeto que nos ocupa, en la figura 1 se presenta la estructura organización de la SEDCHOCÓ, a saber:

Figura 1

Estructura Organizacional de la SEDCHOCÓ



Nota. Cruz Mosquera, Secretaría de Educación Departamental del Chocó (2024)

Tal y como se evidencia en la figura 1, la SEDCHOCÓ se encuentra distribuida por oficinas: 4 oficinas asesoras, 4 oficinas de áreas, 4 dependencias y 8 procesos, en las cuales se ha hecho evidentes las falencias relacionadas principalmente por temas como, los procesos mal estructurados, debido al mal manejo de la información incluyendo los medios por los que esta circula, así como también, por el control de protocolos implementados en entidades para manejo de información confidencial; bajo este contexto, y teniendo en cuenta que, es mucha la

información que circula en dicha secretaria, ya que en ella reposa información de todo el departamento del Chocó, el desarrollo de esta investigación se convierte en gran alivio para la entidad, por un lado porque le permitirá evidenciar ante los entes de control disciplinarios que hace uso adecuado de los protocolos a la hora de manejar la información.

Al respecto, Amaya (2022), afirmó que:

(…) el mal uso de las herramientas tecnológicas, el mal manejo de la información y la falta de cultura en las organizaciones sobre el uso de las Tecnologías de la información, pueden convertirse en riesgos que afectan el cumplimiento de los objetivos institucionales, hasta la integridad de los funcionarios que componen dichas instituciones educativas (p. 11).

Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información: consiste en desarrollar procesos y procedimientos que hagan uso de las tecnologías de la información, a través de la incorporación de esquemas de manejo seguro de la información (MIN TIC, 2020).

los sistemas tecnológicos en tanto que allí logra realizarse una clasificación de la información recibida, posibilitando el hecho de que exista mayor eficacia a la hora de su recolección y almacenamiento, y reforzando a su vez un sistema de datos seguro y optimo, por medio del cual actualmente no sólo se da dicha recolección, sino que también se da una automatización frente al procedimiento.(Ariza, Ayala y González, 2020)

Por lo anterior se plantea como pregunta de investigación la siguiente: ¿Bajo qué método sistemático de seguridad de la información se puede lograr mitigar la problemática que hoy subyace en la secretaria de educación del chocó con los empleados de contratación a término fijo en lapsus de tiempo de 1 un año?

Justificación

Desde el punto de vista de la justificación, se resalta que, los ataques cibernéticos en la actualidad cada vez son más frecuentes, no obstante, en la investigación realizada por Ramírez y Montoya (2022) la cual consistió en realizar hasta la fase de planeación un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013, los autores afirman que, es posible que las distintas organizaciones afectadas por ciber ataques no lo reporten, ello con la finalidad de no dañar su imagen institucional.

En igual sentido, Poma (2022) manifestó que, aunque el uso de la tecnología puede ser tanto positivo como negativo, también es cierto que este e es esencial para la funcionalidad de una entidad dado que, siempre generan información de diferente índole la cual suelen almacenar en dispositivos electrónicos.

Bajo ese contexto y teniendo en cuenta el objeto de esta investigación, es importante resaltar que, dentro de las instalaciones de la secretaria de SEDCHOCÓ, se presenta una situación particular que quizás suceda en otras entidades públicas, lo cual ya se ha convertido a parte de una molestia una forma de atrasar los procesos que se encuentran en curso, convirtiéndose además, en una pérdida de tiempo e inversión en lo relacionado con el manejo de la información confidencial, puesto que los funcionarios y/o contratistas consideran que en un menor tiempo lo hacen desde computadores personales, siendo así esta una forma de sujetar los puestos que desempeñan obligando a la entidad seguir utilizando sus servicios o en su efecto la entidad deberá iniciar de cero.

De igual manera, en la actualidad, la habitual forma de trabajo empleada por los contratistas directos con esta entidad pública, genera una situación de desagrado ya que al llegar

el nuevo mandato se ve obligado a buscar las personas que siempre han manejado la información contractual hasta lograr que estos organicen la trazabilidad de la información de la manera correcta como se ha venido procesando, generando en si un retroceso en los planes de contratación del nuevo equipo de trabajo con el cual el mandatario electo desea laborar por la razón que tenga. De esta manera se puede percibir la relevancia adoptada por los funcionarios, sin mirar las consecuencias a las que someten el manejo de la información, y los procesos que sufren un trauma debido a las razones antes mencionadas. Por ello, tal y como lo ha expresado, Poma (2020) es necesario que, las entidades integren el sistema de gestión de seguridad a sus procesos y estructura de gestión, y que consideren como importante la seguridad de la información sea tenida en cuenta en la elaboración del diseño de procesos y sistemas de información (Poma, 2020)

Además, la política de seguridad en gestión de la información en una entidad pública determina un margen de calidad y excelencia en los procesos que llevan a cabo denotando transparencia ante los entes de control, lo cual en palabras de Ramírez y Rincón (2022, p.88) garantiza también que se logre "generar credibilidad entre la comunidad". Del mismo modo podemos asegurar que a través de esta política se está promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de seguridad digital. Con relación a los requisitos que establece la norma NTC ISO/IEC 27001, Benavides y Blandón (2018), afirmaron que son una "base para garantizar la disponibilidad, integridad y confidencialidad de la información" (párr. 4).

En consecuencia, con esta problemática se derivan innumerables subproblemas que afectan la confiabilidad de la información, iniciando con la procedencia de la información ya que

las direcciones IP, de las cuales se envía cierta información no corresponden a las adoptadas por la entidad, como también se desconoce el firewall en dichas computadoras.

Objetivos

Objetivo General

Elaborar una política de seguridad para el modelo en gestión de TI, apoyado en la implementación de la norma ISO/IEC 27001, para la definición de los medios de transmisión de la información en la secretaria de educación del departamento del Chocó.

Objetivos Específicos

Realizar un análisis diagnóstico de los procesos y procedimientos que se ejecutan en la entidad, para el mejoramiento y optimización de la información por medio de encuestas a los empleados de la SEDCHOCÓ.

Elaborar los elementos del modelo de gestión TI, basado en la norma ISO/IEC 27001.

Crear una política de seguridad de la información para mejorar el proceso de transmisión de la información.

Evaluar el impacto de la aplicación de la política de seguridad para modelo de gestión TI, a partir de la aplicación de cuestionarios.

Marco de Referencias

Marco Teórico

Seguridad de la Información

La Seguridad de la Información según (Carvajal, Cardona, y Valencia, 2019) es un principio transversal en la protección de los derechos de los ciudadanos, la integridad del estado y la industria, es por ello que el estado colombiano desarrollo la estrategia gobierno en línea (GE) que tiene como objetivo tener un estado más eficiente, transparente y participativo, reglamentado de forma unificada a través del decreto 1078 de 2015 (p. 69).

De acuerdo con (Lerma Vinlasaca y Donoso Gallo, 2018) la seguridad de la información es la protección de la información contra amenazas presentes en el entorno a fin de minimizar los posibles daños causados sobre los activos, por lo que es necesario la implementación de un estándar que regule la gestión de la seguridad de la información para minimizar daños, ampliar las oportunidades del negocio, maximizar el retorno de las inversiones y asegurar la continuidad del negocio".

Por su parte, *ISOTools Excellence* (2017), citado por (Figueroa-Suárez, Rodríguez-Andrade, Bone-Obando, y Saltos-Gómez, 2017) expresan que la seguridad informática "protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contienen", y en ese orden de ideas, la definen como la implementación de medidas técnicas con las cuales se logra preservar la infraestructura de la comunicación encargada de soportar la operación de una empresa, esto es, el hardware y el software. (p. 147)

Sistema de Gestión de Seguridad de la Información (SGSI)

En palabras de (Vegas Varona, 2019) Sistema de Gestión de Seguridad de la Información (SGSI), según la NTP ISO/IEC 27001, surge para mitigar las distintas modalidades de ataques, casos de fuga de información, modificación indebida de datos, accesos indebidos a los sistemas informáticos entre otros, ajustándose a la normativa a la cual está sujeta la institución para cubrir las necesidades de seguridad que actualmente carece dicha casa de estudios y que en un futuro pueda servir como referencia a otras universidades y estamentos públicos y privados (p. 3)

De acuerdo con (Lerma Vinlasaca y Donoso Gallo, 2018) un Sistema de Gestión de Seguridad de la Información (SGSI), permite la empresa conozca cuales son los riesgos a los que están expuestos los activos de información y permite realizar su tratamiento mediante instructivos bien definidos, documentados, disponibles, conocidos por todos y que constantemente deben ser expuestos a mejoras continuas (p. 2).

Riesgo

En palabras de (Rodríguez Díaz y Ruíz Rojas, 2021), el riesgo representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos.

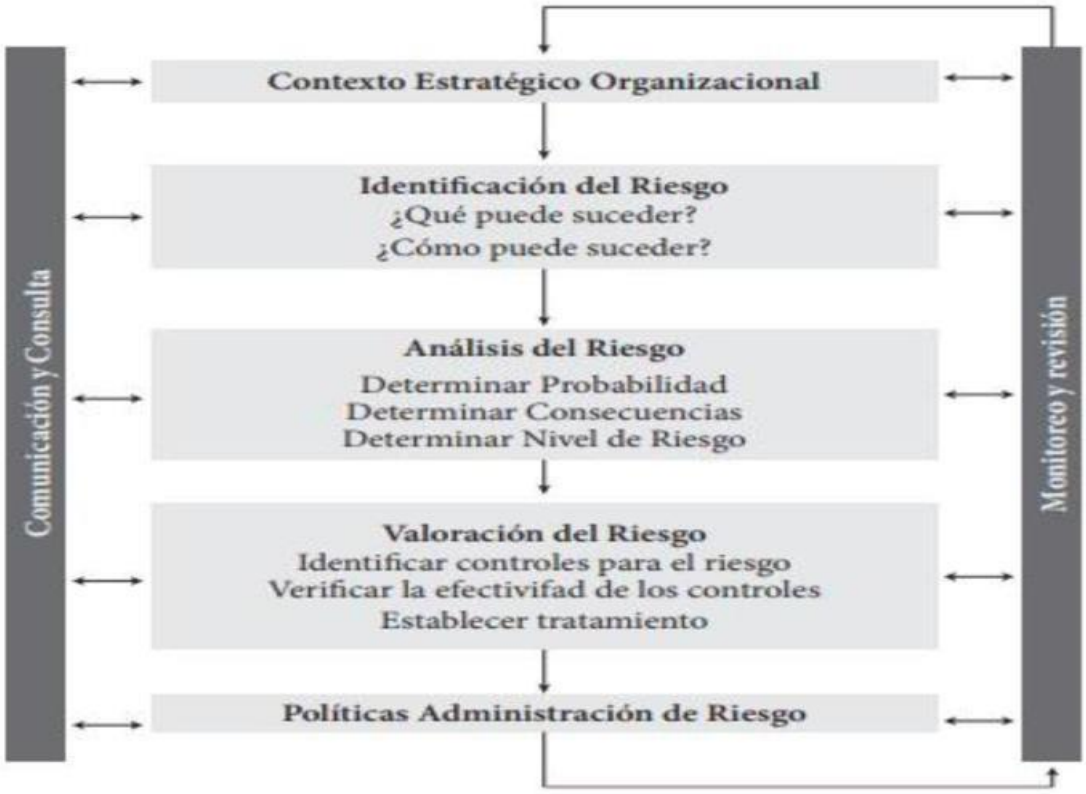
Aseguran los autores que, algunas entidades durante el proceso de identificación del riesgo pueden hacer una clasificación de este, con el fin de establecer con mayor facilidad el análisis del impacto, considerado en el siguiente paso del proceso de análisis del riesgo (p. 22).

En ese sentido, consideran que el manejo adecuado favorece al desarrollo y crecimiento de la entidad y expresan que, para asegurar dicho manejo, es importante se establezca el entorno y ambiente organizacional de la entidad, la identificación, análisis,

valoración y definición de las alternativas de acciones de mitigación de los riesgos, en desarrollo de los elementos que se observan en la Figura 4:

Figura 2

Proceso para la Administración del Riesgo



Nota. Rodríguez Díaz y Ruíz Rojas (2021

Rodríguez Díaz y Ruíz Rojas (2021) afirmaron que, el adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad. Con el fin de asegurar dicho manejo es importante que se establezca el entorno y ambiente organizacional de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos, esto en desarrollo de los siguientes elementos: contexto estratégico, identificación de riesgos, análisis de riesgos, valoración de riesgos y políticas de administración de riesgos (p. 19).

De igual manera, en un SGSI, resulta necesario establecer una metodología con la cual se pueda conocer las debilidades y fortalezas con que cuenta la organización, en otras palabras, contar con una metodología de análisis de riesgo efectiva para la seguridad de la información.

Al respecto, la adopción de la metodología Magerit, permite que se puedan identificar de forma oportuna y probable, el impacto de los riesgos, a fin de que se puedan establecer controles para prevenirlos, teniendo en cuenta que no todas las amenazas afectan a todos los activos o que, en su efecto, no todos los activos son afectados por la amenaza. En ese sentido, la degradación, esto es, el daño causado al valor activo, es importante que sea valorado. Por lo cual, con la metodología Magerit, se puede medir la escala por degradación, tal y como se presenta en la siguiente tabla:

Tabla 1

Medición por Degradación

MA	100%	Muy alta	Daño muy grave
A	75%	Alta	Daño grave
M	50%	Media	Daño importante
B	25%	Baja	Daño menor
MB	1%	Muy baja	Daño despreciable

Nota. Medición por Degradación según la metodología de Magerit versión 3

Norma NTC-IEC ISO 27001

De acuerdo con Vegas Varona (2019), esta norma cubre todo tipo de organizaciones y, además, específica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema documentado de Gestión de Seguridad de

Información en el contexto de los riesgos de negocio que presenta la organización. Indica los requisitos para la aplicación de controles de seguridad según las necesidades de la organización (p. 15).

De igual manera, Calder y Walkins (2010), citados por Vegas Varona (2019) manifestaron que la ISO 27001 no se encarga de definir lo que es riesgo u otros aspectos relacionados, sino definir las actividades que guardan relación con el riesgo y mostrar como alinearlas políticas de gestión de seguridad de información con el contexto de gestión estratégica de riesgos (p. 15).

Por otra parte, (Moreno Novoa, 2021) consideró que, el estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos (p. 13).

Lineamiento Modelo de Seguridad de la Información MINTIC

De acuerdo con (Rodríguez Díaz y Ruíz Rojas, 2021) quien manifestó que, el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: "TIC para servicios, TIC para gobierno abierto y TIC para gestión.

Razón por la cual, aseguraron que, el Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad deber ser actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de

Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información. (p. 24).

Marco Normativo

A continuación, se relacionan algunas de las leyes y normatividad que sustenta el marco legal en Colombia:

Decreto 1008 de 2018

Mediante este decreto se define la política de Gobierno Digital, por el cual se establecen los lineamientos generales de la política de Gobierno Digital, la cual tiene por objeto promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital (Decreto 1008, 2018).

Decreto 415 de 2016

Por el cual adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015. Estableció los lineamientos para la implementación de la figura de Director de Tecnologías y Sistemas de Información, quien será pieza clave en la construcción de un Estado más eficiente y transparente gracias a la gestión estratégica de las Tecnologías de la Información y las Comunicaciones (TIC). Y en su Artículo 2.2.35.3. Objetivos del fortalecimiento institucional. Para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones las entidades y organismos a que se refiere el presente decreto, deberán: Liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo

integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado (Decreto 415, 2016).

Decreto 1078 de 2015

Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Y especialmente en sus artículos a partir del 2.2.9.1.1.1. título 9. Define los lineamientos, instrumentos y plazos de la estrategia de gobierno en línea para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones (Decreto 1078, 2015).

Ley 1753 de 2015

Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país" en el artículo 45 establece:" Estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano (Ley 1753, 2015).

Ley 1712 del 2014

Por medio de la cual se crea la ley de Transparencia y del Derecho de Acceso a la información pública nacional y se dictan otras Disposiciones (Ley 1714, 2014).

Decreto 2573 de 2014

El marco de cumplimiento normativo que está sujeto el desarrollo del proyecto es el decreto 2573 de 2014 y el 1078 de 2015, teniendo encuentra todas sus disposiciones legales en la contratación pública y privada según ley 80 (Decreto 2573, 2014).

Decreto 333 de 2014

Define el régimen de acreditación de las entidades de certificación, aplicable a personas jurídicas, públicas y privadas (Decreto 333, 2014).

Norma ISO/IEC 27001:2013

Estándar internacional que se aplica para la gestión de la seguridad de la información. Al manejar el Sistema de Gestión de Seguridad de la Información SGSI, se busca minimizar los riesgos, para esto se deben establecer procesos y procedimientos que ayuden a la organización a llegar a la excelencia (Norma ISO 27001, 2013).

Ley 1581 del 2012

Por la cual se dictan disposiciones generales para la protección de datos personales (Ley 1581, 2012).

Decreto 2578 de 2012

Por el cual se reglamenta el Sistema Nacional de Archivos, se establece la Red Nacional de Archivos, se deroga el Decreto 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los Archivos del Estado (Decreto 2578, 2012).

Decreto 2609 de 2012

Por la cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado (Decreto 2609, 2012).

Decreto 2482 de 2012

Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión (Decreto 2482, 2012).

CONPES 3670 de 2010

Sobre los lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones (Compes 3670, 2010).

Ley 1273 de 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Ley 1273, 2009).

Ley 1341 de 2009

Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones (Ley 1341, 2009).

Ley 1266 de 2008

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones (Ley 1266, 2008).

Ley 962 de 2005

Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o presten servicios públicos (Ley 962, 2005).

Ley 603 de 2000

Esta ley se refiere a la protección de los derechos de autor en Colombia. En ella se establece que, el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales (Ley 603, 2000).

Ley 599 del 2000

Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático (Ley 599, 2000).

Metodología

Para el diseño de la política de seguridad en gestión de la información en la SEDCHOCÓ, inicialmente se hizo una revisión metodológica desde un enfoque cualitativo, con la finalidad de obtener el mayor número de datos e información necesaria, desarrollar el tema objeto de estudio, por lo cual, fue necesario acudir a fuentes secundarias, entre ellas, artículos de revistas, libros, etc., los cuales fueron recolectados a través de bases de datos académicas y en algunos casos de las páginas web de entidades públicas, entre ellas, la página web de la SEDCHOCÓ.

Además, se utilizó la metodología Magerit, ya que esta permite que se puedan clasificar los activos de una organización en diferentes grupos, los cuales permitan identificar de forma detallada los riesgos que presenta cada uno a fin de tomar los controles necesarios, ya que esta metodología ofrece un método sistemático que permite analizar los riesgos, planificar las medidas optimas y necesarias para que los riesgos estén bajo control, siguiendo los siguientes pasos: identificación de activos, activos esenciales, arquitectura del sistema, datos/ información, software/aplicaciones informáticas, equipamiento informático (hardware), redes de comunicaciones, instalaciones y personal (Restrepo, 2017).

De igual manera, para lograr identificar el macroproceso y el manejo actual que se da a la información en dicha entidad, fue necesario utilizar fuentes primarias, para ello se aplicaron encuestas a los empleados y al personal del área TIC de la entidad, lo cual permitió identificar el porcentaje de cumplimiento de la norma técnica colombiana ISO/IEC 27001:2013, y a su vez, las necesidades y acciones que se deben desarrollar a fin de lograr la implementación y mejoras de la seguridad de la información en la entidad.

Tipo de Investigación

La investigación fue de tipo aplicado, ya que lo que se pretendió fue diseñar una política de seguridad de la información en la Secretaria de Educación del Chocó, teniendo como referencia las necesidades que enfrenta la entidad, aportando una solución innovadora.

Diseño de la Investigación

El diseño de este estudio es cuasi experimental, debido a lo que se busca con esta investigación es diseñar una política de seguridad con la que se pueda proteger la información en la Secretaria de Educación del Chocó.

Población y Muestra

La población del presente estudio investigativo lo constituirá 35 trabajadores de la Secretaria de Educación del Departamento del Chocó, compuesto de la siguiente manera:

Funcionarios Administrativos:	30
Funcionarios de la oficina TI:	5
Total:	**35**

Para esta investigación, la muestra será el total de la población.

Técnicas e Instrumento de Recolección de Datos

Para la recolección de los datos que permitirán el desarrollo de la información, se utilizará la técnica de la encuesta, y como instrumento, se elegirá el cuestionario, en el cual se incluirán ocho (8) preguntas con las cuales se obtendrá y procesará la información del tema objeto de estudio.

Procedimiento para el Análisis de los Datos Obtenidos

La información que se obtenga a través de la aplicación de la encuesta se estudiará, clasificará y ordenará, utilizando el programa de análisis estadísticos Microsoft Excel.

Además, teniendo en cuenta los objetivos planteados, únicamente se extraerá la información relevante para lograr desarrollar y ejecutar la investigación, de tal forma que, el presente estudio pueda utilizarse como referente o guía en investigaciones futuras con las que se pretenda implementar o diseñar políticas de seguridad de la información en entidades públicas.

Desarrollo del Proyecto

Contexto de la Secretaria de Educación del Chocó

Misión: gerenciar los procesos educativos en concordancia con los principios y fines establecidos en la Constitución Nacional y las competencias asignadas a los Departamentos, garantizando la cobertura y equidad de la educación, y facilitando los medios a las instituciones educativas, para la prestación de un servicio educativo con calidad y eficiencia, acorde con las necesidades y potenciales de las diferentes comunidades que lo conforman, apuntando hacia una participación democrática, autonomía escolar y formación ciudadana (Secretaría de Educación Departamento del Chocó, 2024).

Visión: en el 2020 seremos una entidad reconocida por garantizar educación con calidad, inclusión, acceso y permanencia de los niños, niñas, adolescentes y jóvenes del Departamento del Chocó; regida por altos estándares en la gestión de sus procesos misionales y de apoyo, con un sistema de gestión de Establecimientos Educativos en los municipios no certificados del Departamento del Chocó que contribuya a la formación de ciudadanos participativos, innovadores y con conciencia social y cultural que aporten al desarrollo de sus comunidades (Secretaría de Educación Departamento del Chocó, 2024).

Política de Calidad: administrar la prestación del servicio educativo, brindando respuesta oportuna a las necesidades y requerimientos de la ciudadanía, a través de un equipo de trabajo orientado al servicio, con sentido de pertenencia y comprometidos con el mejoramiento continuo de nuestros procesos (Secretaría de Educación Departamento del Chocó, 2024).

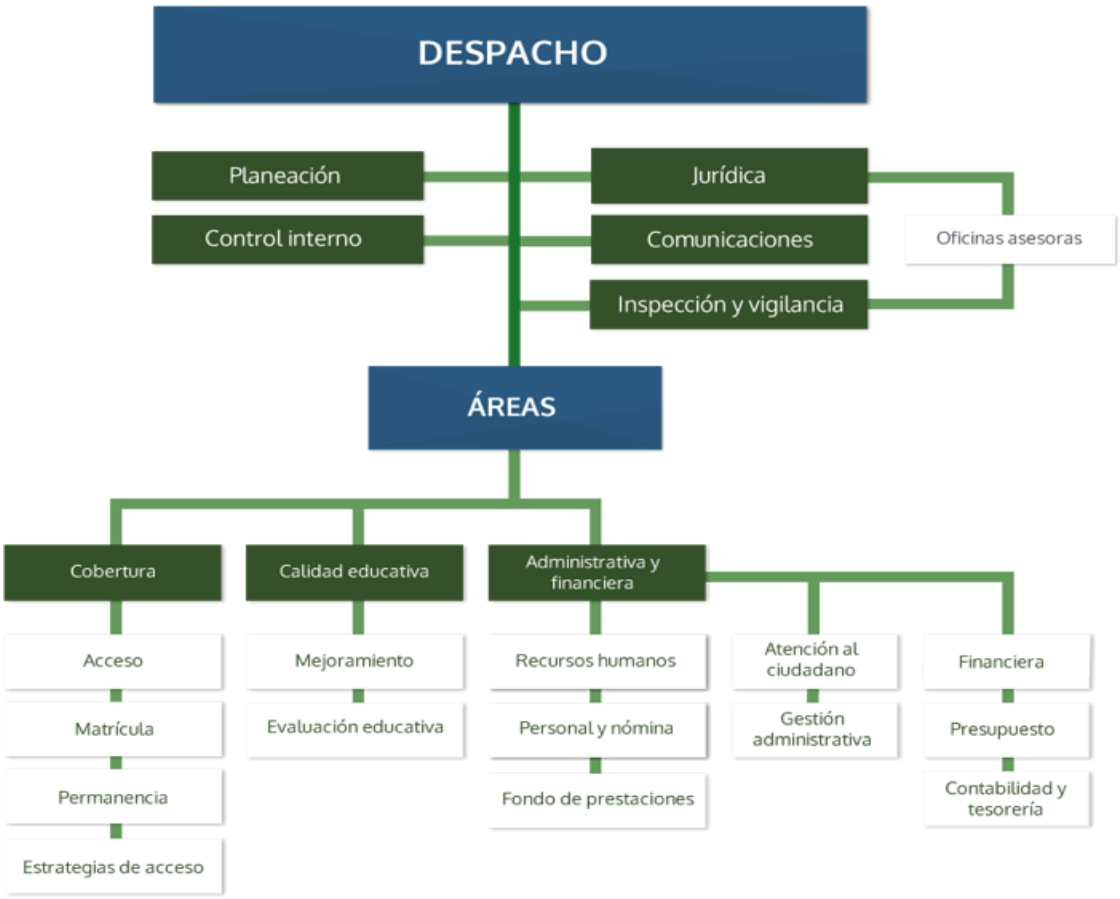
Objetivos de Calidad:

- Aumentar el nivel de confiabilidad y el grado de satisfacción de la atención y servicios prestados.
- Fortalecer la prestación de los servicios incrementando la eficiencia, eficacia y efectividad de los procesos.
- Garantizar la disponibilidad, el uso eficiente de los recursos financieros y la disponibilidad y competencia del recurso humano.
- Implementar y mantener un sistema de gestión de la calidad conforme con las reglamentaciones que le apliquen.
- Fortalecer el desempeño de los macroprocesos establecidos en el ministerio de educación nacional.
- Aplicación de mecanismos de autocontrol y de evaluación para garantizar la mejora continua (Secretaría de Educación Departamento del Chocó, 2024).

Organigrama de la Entidad : en la figura 2, se describe el organigrama de la SEDCHOCÓ:

Figura 3

Organigrama de la SEDCHOCÓ 2O24



Nota. Secretaría de Educación Departamental del Chocó (2024)

Dependencias: administrativa: la política de eficiencia está orientada a afianzar el proceso de descentralización, con fundamento en la modernización de la administración y la gestión del sector educativo para posibilitar el logro de las metas que se han planteado en términos de cobertura, calidad y pertinencia. De igual forma, se trabaja en la modernización de la gestión de las Instituciones y Centros Educativos.

Financiera: Garantizar la eficiente utilización de los recursos para una vigencia fiscal, de acuerdo con la normatividad vigente y el desarrollo del sector educativo, logrando el pago de los compromisos de manera transparente y oportuna.

Planeación: apoya y coordina la gestión de la Secretaría de Educación en su componente estratégico, planes y programas, para asegurar el cumplimiento de parámetros técnicos, legales y sectoriales.

Control Interno Disciplinario: la oficina de Control Interno disciplinario la cual está facultada a través de la ley 734 de 2002 para liderar los asuntos disciplinarios que se adelanten en la Secretaría de Educación Departamental del Chocó.

La oficina disciplinaria le corresponde iniciar, investigar y fallar en primera instancia las quejas que le sean interpuestas exclusivamente en contra de los servidores adscritos a esta entidad.

Calidad Educativa: esta área busca garantizar una educación de calidad, para todos los estudiantes, entendida ésta como aquella que permite que todos los alumnos alcancen niveles satisfactorios de competencias para desarrollar sus potencialidades, participar en la sociedad en igualdad de condiciones y desempeñarse satisfactoriamente en el ámbito productivo, independientemente de sus condiciones o del lugar donde viven. Se trata de un principio básico de equidad y justicia social.

Talento Humano: Le corresponde definir, modificar y legalizar la planta de personal directiva, docente y administrativa, además de la administración de novedades, selección, ingreso, ascensos, formación, capacitación, bienestar y desarrollo del personal, manejo del fondo prestacional, administración de la nómina y las hojas de vida, Gestión de los Establecimientos Educativos.

Cobertura: Garantiza el acceso y la permanencia de los niños, niñas y jóvenes en edad escolar al sistema educativo, logrando una educación para todas las edades, para quienes cuentan y no con recursos y para aquellos que están cerca o lejos de los establecimientos educativos; lidera el proceso a través de la estrategia "Todos cuentan para garantizar el acceso y la permanencia educativa en el Departamento del Chocó", centrando sus prioridades en la población vulnerable, primera infancia, los niños y jóvenes afectados por la violencia, los adultos iletrados, los grupos étnicos y la población rural dispersa y convocando a aliados para la optimización del servicio educativo.

Inspección y Vigilancia: Autorizan, verifican, hacen seguimiento y evalúan los procesos y actividades de quienes prestan el servicio público de educación con el fin de que se cumplan las disposiciones constitucionales, legales y reglamentarias.

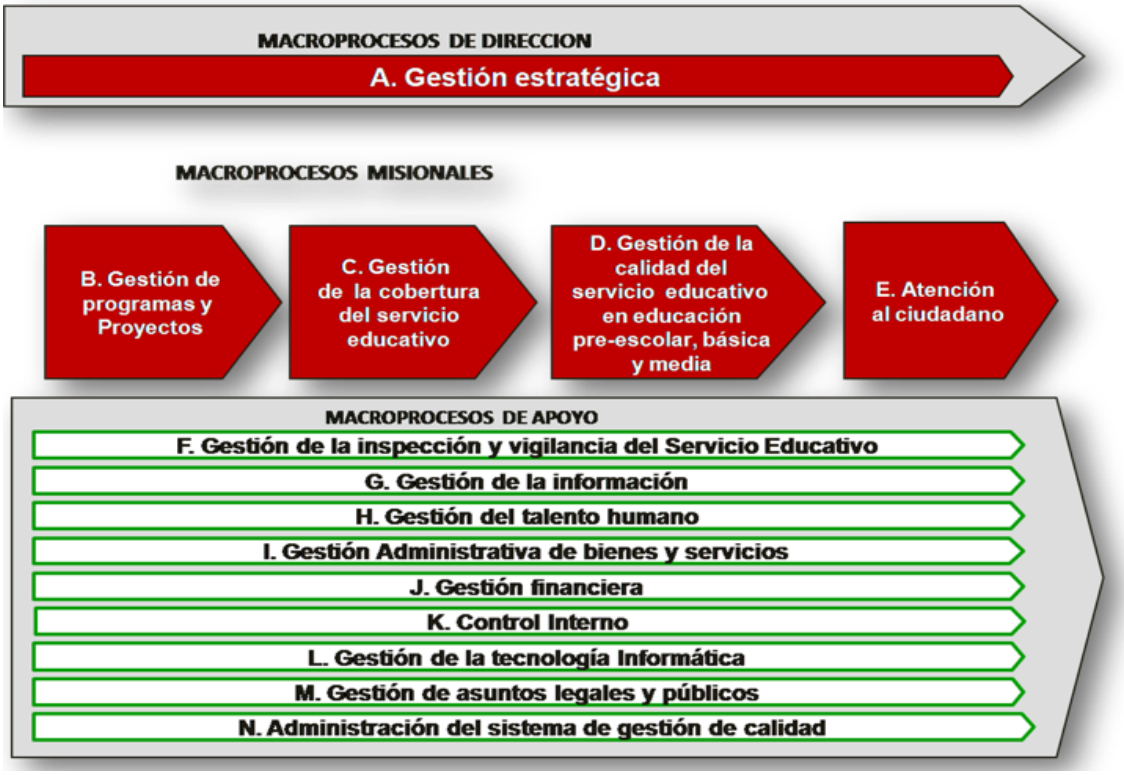
Jurídica: Lidera los procesos judiciales, extrajudiciales y prejudiciales, coordinando la labor de los profesionales del derecho de la Secretaría de Educación y ofreciendo asesoría jurídica dentro de los términos y el marco legal vigente (Chocó, 2024).

Mapa de procesos

En la figura 3, se describe el mapa de procesos de la SEDCHOCÓ:

Figura 4

Mapa de Procesos SEDCHOCÓ



Nota. Cruz Mosquera, Secretaría de Educación Departamental del Chocó (2024)

Modelo Operativo

El modelo operativo con que cuenta la Secretaria de Educación del Chocó, para su gestión y articulación, es el Plan de Desarrollo 2020-2023 "Generando Confianza**",** en este plan de desarrollo, la línea estrategia 3, respecto al tema de las TIC, el cual se denomina "Un Chocó productivo y competitivo para generar confianza", plantea diversas oportunidades y programas entre ellas, el aprovechamiento de las políticas y programas definidos en la normatividad interna sobre el desarrollo de la CT+I y garantizar que los establecimientos educativos del departamento, incluidos los no certificados, pueda contar

con el servicio de conectividad y con herramientas tecnológicas para fortalecer la calidad educativa.

Procesos y Sistemas de Información en la SEDCHOCÓ

En la Secretaria de Educación del Departamento del Chocó, los procesos de la entidad se desarrollan, con base en el uso de las TIC, como se relaciona en la siguiente tabla:

Tabla 2

Procesos y Sistemas de Información

Macroproceso	Proceso	Sistema de información
Dirección	Gestión estratégica	N/A
Misionales	Gestión de programas y proyectos	N/A
	Gestión de la cobertura del servicio educativo	Sistema Integrado de Matrícula - SIMAT
	Gestión de la calidad del servicio educativo en educación preescolar, básica y media	Sistema de Gestión de la Calidad Educativa - SIGSE
	Atención al ciudadano	Sistema de Atención al Ciudadano - SAC
	Gestión de la inspección y vigilancia del servicio educativo	N/A
Apoyo	Gestión de la información	N/A
	Gestión del talento humano	Sistema humano
	Gestión administrativa de bienes y servicios	Sistema PCTG
	Gestión financiera	Sistema PCTG

Macroproceso	Proceso	Sistema de información
	Control interno	N/A
	Gestión de TI	N/A
	Gestión de asuntos legales y públicos	N/A
	Administración del sistema de gestión de calidad	N/A

Nota. Procesos y sistemas de información en la SEDCHOCÓ. Elaboración propia

Servicios tecnológicos de la SEDCHOCÓ

Tabla 3

Servicios Tecnológicos de la SEDCHOCÓ

Servicio	Descripción	Funcionamiento
Portal WEB	Permiten visualizar la información institucional de la SEDCHOCÓ.	A través de la página web: www.sedchoco.gov.co, la SEDCHOCÓ publica información institucional, noticias y trámites relacionados con la entidad.

Servicio	Descripción	Funcionamiento
Infraestructura centro	Mantiene disponible y operativa los elementos que componen el centro de datos.	La SEDCHOCÓ, cuenta con 1 *rack* de 127 puntos de datos y 42 de voz; 4 *switch* de 24 puertos cada uno; 1 *router;* 8 *Access point;* 1 *microtick;* 5 *pitch panel, 1* planta telefónica, 1 UPS de 30 KVA.
Administraciones de bases de datos	Aquí se ejecutan los procesos operativos y administrativos, para la correcta operación de los servicios de bases de datos de la SEDCHOCÓ.	La SEDCHOCÓ, dispone de 4 sistemas de información, a saber: SAC, SIMAT, PCTG Y HUMANO
Correo electrónico	Es un canal de comunicación que permite el intercambio de mensajes de datos a nivel interno y externo.	La SEDCHOCÓ cuenta con 100 cuentas de correo electrónico en office 365 con el dominio: sedchoco.gov.co

Servicio	Descripción	Funcionamiento
Redes y seguridad	Es el conjunto de elementos que permite la conexión de todos los equipos de la SEDCHOCÓ con os servicios de internet, esto con la finalidad de brindar protección a la información que se transfiere por los diferentes canales de comunicación al interior de la entidad.	Conformada por: 1 *rack,* 4 switch, 1 *router*, 1 *mikrotik,* 8 *patch panel*, 8 *acces point.*
Almacenamiento y respaldo de la información	Se realizan copias de seguridad o *backup,* de la información almacenada en la infraestructura tocológica y los servicios prestados por la SEDCHOCÓ.	Se realizan 2 copias de seguridad por cada equipo anualmente, ya que no se cuenta con servicios ni espacios en la nube. Las copias de seguridad que se hacen de los sistemas de información, se hacen diariamente. En caso de que un equipo presente fallas, se le da de baja.

Servicio	Descripción	Funcionamiento
Sistemas de información	Ofrece soporte y acceso a los aplicativos y modificaciones funcionales, según las necesidades de cada área en la SEDCHOCÓ.	Las bases de datos que se manejan en la SEDCHOCÓ, están en cada sistema de información que se utiliza para la automatización de los procesos: - SAC (sistema de atención al ciudadano, - HUMANO(sistema de recursos humanos), - SIMAT (sistema de matrícula) y, - PCTG (sistema financiero).
Seguridad de la información	Administra y brinda seguridad de la información para los servicios TI, según las necesidades plasmadas en la Política de Seguridad de la Información con que cuenta la SEDCHOCÓ.	Según las políticas de seguridad de la información, en la SEDCHOCÓ se realizan 4 copias de seguridad.

Servicio	Descripción	Funcionamiento
Impresiones	Para el soporte y operación del servicio de digitalización, fax e impresiones.	La SEDCHOCÓ, cuenta con 17 impresoras al servicio de los funcionarios y contratistas de la entidad.
Servicios bases	Para el mantenimiento, la revisión y configuración de la infraestructura v=base de la SEDCHOCÓ.	La SEDCHOCÓ, cuenta con un Mikrotik el cual realiza el DHCP, el DNS es asignado por la empresa prestadora del servicio de internet a la entidad, se realizan 2 mantenimientos por cada equipo cada año y cuando alguno presenta fallas técnicas, se realiza asistencia técnica respondiendo a las peticiones de los usuarios.
Lugares de trabajo	Brinda soporte técnico adecuado en para los empleados de planta y a los colaboradores, incluidos los contratistas de la SEDCHOCÓ.	Son 78 equipos de cómputos ubicadas en cada dependencia de la entidad. El soporte técnico se brinda según las peticiones que se reciben en la oficina TI. Cada año la oficina TI de la SEDCHOCÓ, realiza el diagnóstico de la infraestructura tecnológica que se utiliza en la entidad.

Servicio	Descripción	Funcionamiento
Conceptos técnicos	Gestiona la adquisición de tecnologías (hardware, software y sistemas de información) para las dependencias de la SEDCHOCÓ.	Para la compra de equipos y sistemas tecnológicos que se requieran en la SEDCHOCÓ.

Nota. Servicios Tecnológicos de la SEDCHOCÓ. Elaboración propia

Resultados

Después de realizar la toma de datos, la característica de la población de estudio evidenció que la oficina de TI de la Secretaría de Educación del Chocó cuenta con cinco (5) empleados, 3 nombrados y 2 contratados, los 30 restantes, son empleados administrativos.

La estructuración de la encuesta se elaboró buscando que esta fuese compatible con los indicadores que se buscaban evaluar en esta investigación, y que sirvieran como insumos en la realización del análisis diagnóstico de los procesos y procedimientos que se ejecutan en la SEDCHOCÓ para el mejoramiento y optimización de la información.

Razón por la cual, se elaboró matriz, que evidencian la relación de las preguntas diseñadas en la encuesta con los correspondientes indicadores que permiten medir cada una de las respectivas variables, a saber:

Tabla 4

Matriz de Diseño de la Encuesta

Variable	Dimensiones	Indicadores	Preguntas	Opciones de respuestas
Seguridad de información bajo la norma ISO/IEC27001	Cumplimiento de los procesos de seguridad de la información	Grado de seguridad de la información	1. ¿La SEDCHOCÓ, tiene definida la Política de Seguridad de la Información basada en la Norma ISO/IEC 27001?	Si / No
			2. ¿La SEDCHOCÓ, revisa de manera periódica la Política de Seguridad de la Información que tiene?	Si / No
			3. ¿En la SEDCHOCÓ, se han definido las responsabilidades en materia de Seguridad de la Información?	Si / No
			4. ¿En la SEDCHOCÓ, existe un comité encargado de la gestión en los temas de Seguridad de la Información?	Si / No

Variable	Dimensiones	Indicadores	Preguntas	Opciones de respuestas
			5. ¿Los contratos y convenios que se firman con terceros, tienen clausulas sobre los requisitos de seguridad de la información de la entidad, tales como confidencialidad?	Si / No
			6. ¿La SEDCHOCÓ cuenta con un inventario de activos de información?	Si / No
			7. ¿La SEDCHOCÓ, verifica los sistemas de forma regular, para determinar si están adecuados a los estándares de seguridad implementados?	Si / No
			8. ¿Consideras que es posible que ocurra un riesgo en los activos de información dentro de la SEDCHOCÓ?	Si / No

Variable	Dimensiones	Indicadores	Preguntas	Opciones de respuestas
Implementación de la Norma ISO/IEC 27001	Planificación	Comprender las necesidades y expectativas	9. ¿La SEDCHOCÓ cuenta con horarios establecidos para acceder a la información?	Si / No
			10. ¿Existen tipos de acceso para usuarios?	Si / No
			11. ¿Los usuarios cuentan con los mismos tipos de acceso para acceder a la información?	Si / No
			12. ¿En la SEDCHOCÓ, existen unidades de almacenamiento de respaldo?	Si / No
			13. Existen controles de acceso para ingresar al computador de los usuarios?	Si / No
			14. ¿Cualquier usuario puede acceder a toda la información de la SEDCHOCÓ?	Si / No

Variable	Dimensiones	Indicadores	Preguntas	Opciones de respuestas
			15. ¿Considera que es importante que la SEDCHOCÓ realice copias de resguardo de forma periódica?	Si / No
			16. ¿La SEDCHOCÓ cuenta con horarios establecidos para acceder a la información?	Si / No
Uso TIC en procesos y procedimientos de la	Cumplimiento de los procesos de seguridad	Grado de uso de herramientas TIC en el desarrollo de las funciones en la SEDCHOCÓ	17. ¿Existen tipos de acceso para usuarios?	Si / No
			18. ¿Los usuarios cuentan con los mismos tipos de acceso para acceder a la información?	Si / No
			19. ¿En la SEDCHOCÓ, existen unidades de almacenamiento de respaldo?	Si / No

Variable	Dimensiones	Indicadores	Preguntas	Opciones de respuestas
			20. ¿Existen controles de acceso para ingresar al computador de los usuarios?	Si / No
			21. ¿Cualquier usuario puede acceder a toda la información de la SEDCHOCÓ?	Si / No
			22. ¿La SEDCHOCÓ cuenta con horarios establecidos para acceder a la información?	Si / No

Nota. Matriz de Diseño de la Encuesta. Elaboración propia

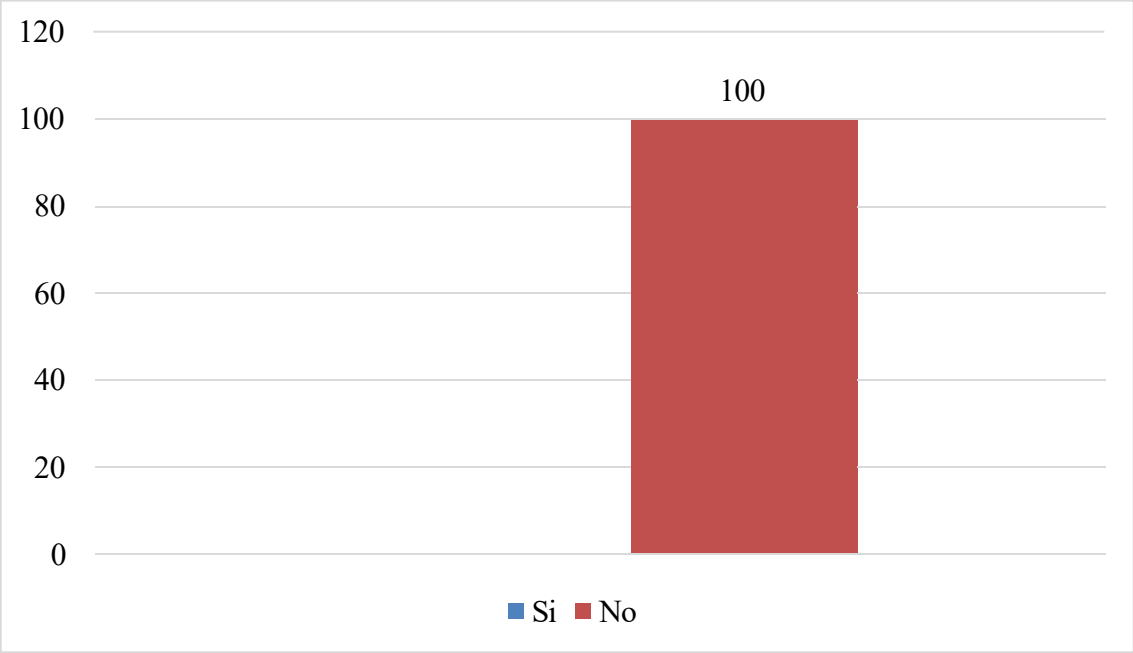
Resultados de la encuesta

A continuación, se relacionan los resultados de las encuestas aplicadas a los funcionarios y contratistas de la Secretaria de Educación del Chocó:

Pregunta 1:

Figura 5

¿La SEDCHOCÓ, tiene Definida la Política de Seguridad de la Información basada en la Norma ISO/IEC 27001?



Nota. Resultados de la pregunta 1. Elaboración propia

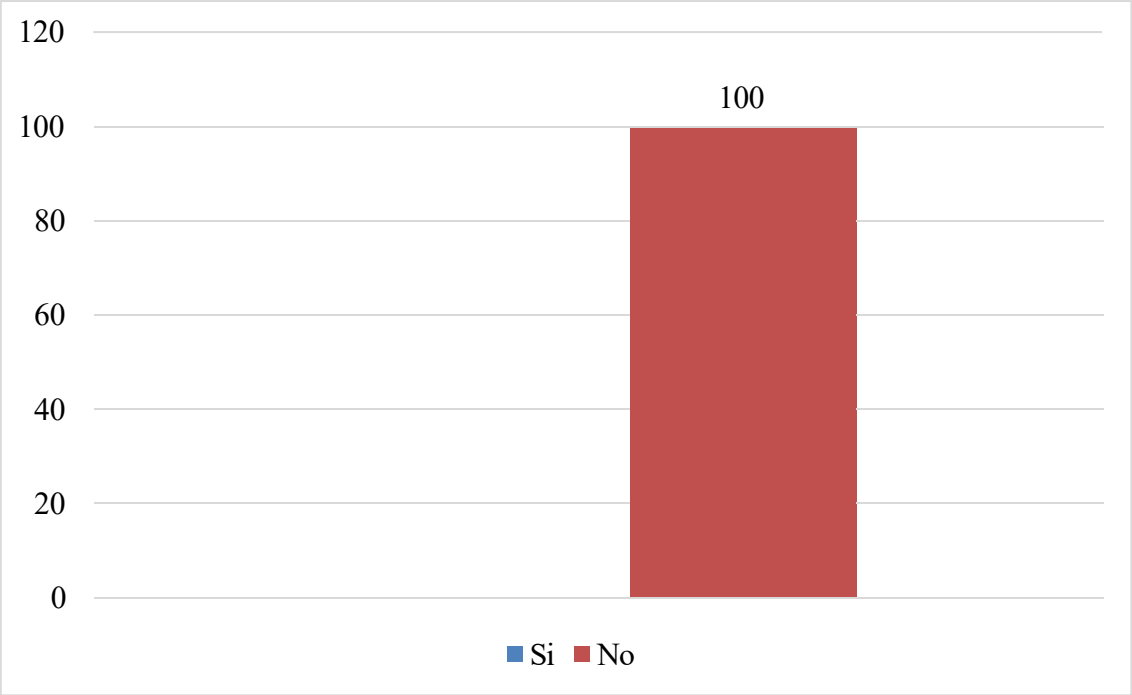
Como se observa en la figura 5, los 35 participantes opinaron que la SEDCHOCÓ, no tiene definida la Política de Seguridad de la Información bajo la Norma ISO/IEC 27001. En consecuencia, la seguridad de la información en la SEDCHOCÓ, se encuentra en riesgo, ya que no se está garantizando la seguridad de la información, haciéndola vulnerable a que

en algún momento no deseado pueda ocurrir un daño en los equipos y materiales de la entidad.

Pregunta 2:

Figura 6

¿La SEDCHOCÓ, Revisa de Manera Periódica la Política de Seguridad de la Información que Tiene?



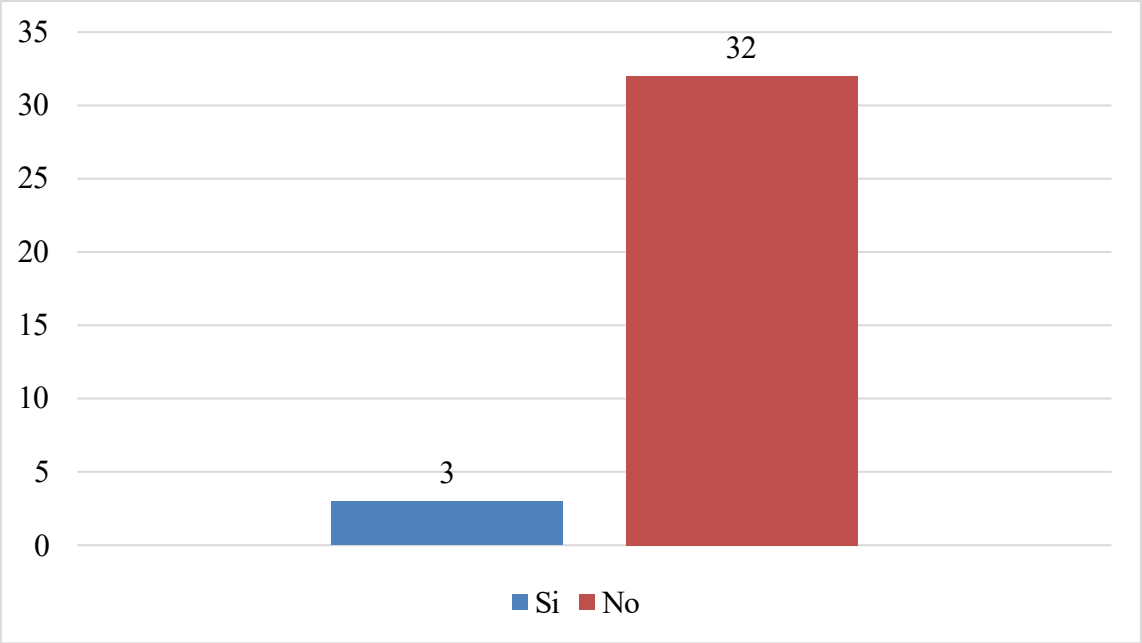
Nota. Resultados de la pregunta 2. Elaboración propia

Según se observa en la figura 6, los 35 participantes respondieron que la SEDCHOCÓ, no revisa de manera periódica la Política de Seguridad de la Información que tiene. En efecto esta información evidencio que el nivel de seguridad de la información en la entidad es deficiente.

Pregunta 3:

Figura 7

¿En la SEDCHOCÓ, se han Definido las Responsabilidades en Materia de Seguridad de la Información?



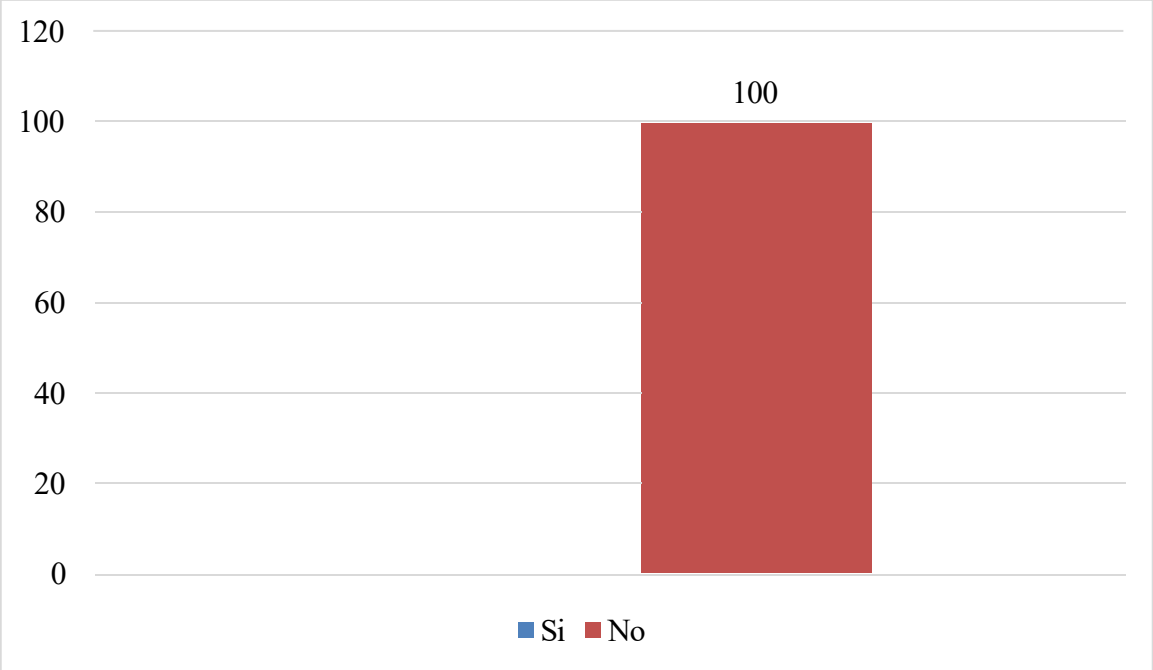
Nota. Resultados de la pregunta 3. Elaboración propia

Como se observó en la figura 7, la mayoría de los participantes, esto es 32 personas, manifestaron que, en la SEDCHOCÓ, no se han definido las responsabilidades en materia de Seguridad de la Información, mientras que 3 participantes opinaron que sí. En efecto, según este interrogante, en términos generales, la SEDCHOCÓ, no tiene definidas las responsabilidades en materia de Seguridad de la Información.

Pregunta 4:

Figura 8

¿En la SEDCHOCÓ, Existe un Comité Encargado de la Gestión en los Temas de Seguridad de la Información?



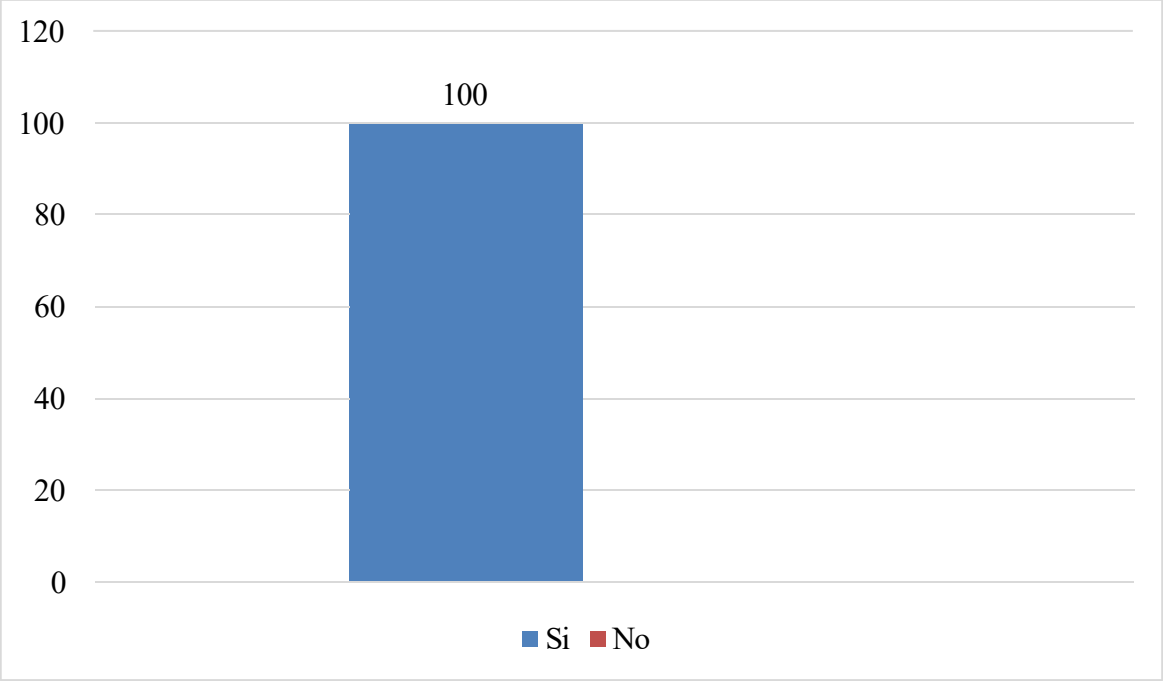
Nota. Resultados de la pregunta 4. Elaboración propia

Según la figura 8, todos los participantes opinaron que, en la SEDCHOCÓ, no existe un comité encargado de la gestión en los temas de Seguridad de la Información. En consecuencia, esta información evidencia que la identificación de riesgo en la SEDCHOCÓ no se está realizando ni cumpliendo con la Norma ISO/IEC 27001, dado que la entidad no la ha implementado.

Pregunta 5:

Figura 9

¿Los Contratos y Convenios que se Firman con Terceros, tienen Clausulas sobre los Requisitos de Seguridad de la Información de la Entidad, tales como Confidencialidad?



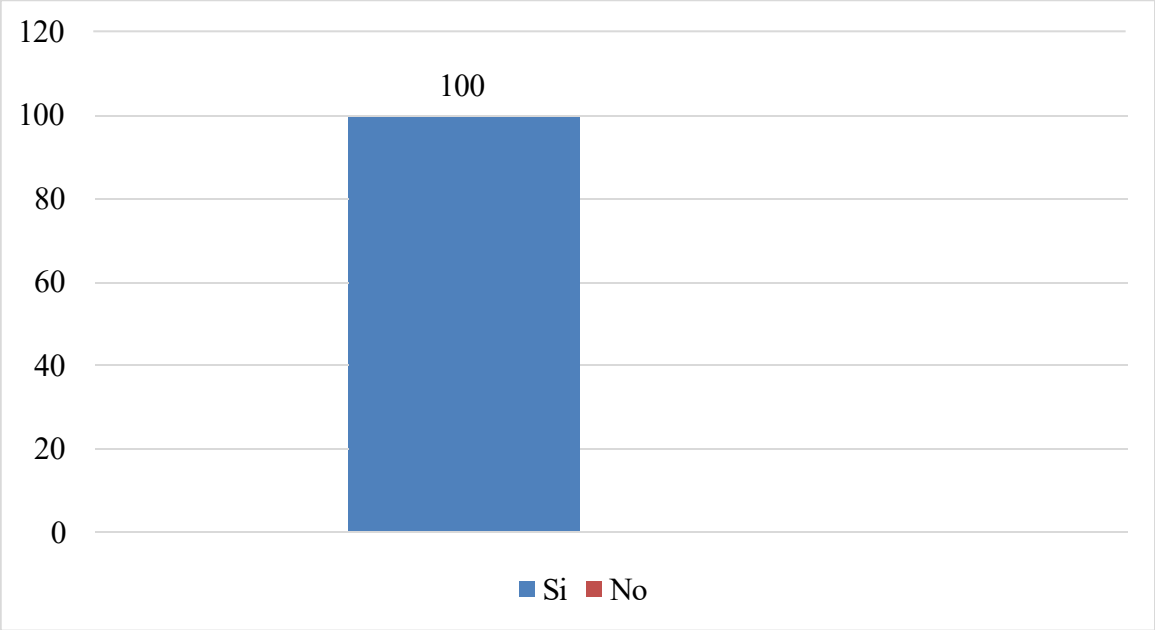
Nota. Resultados de la pregunta 5. Elaboración propia

Según la figura 9, se observó que todos los participantes que respondieron, manifestaron que la SEDCHOCÓ si incluyen en los contratos y convenios que suscribe con terceros, los requisitos de seguridad de la entidad. Lo anterior, evidencia que la SEDCHOCÓ, a la hora de celebrar contratos o convenios, tiene en consideración los requisitos de seguridad.

Pregunta 6:

Figura 10

¿La SEDCHOCÓ Cuenta con un Inventario de Activos de Información?



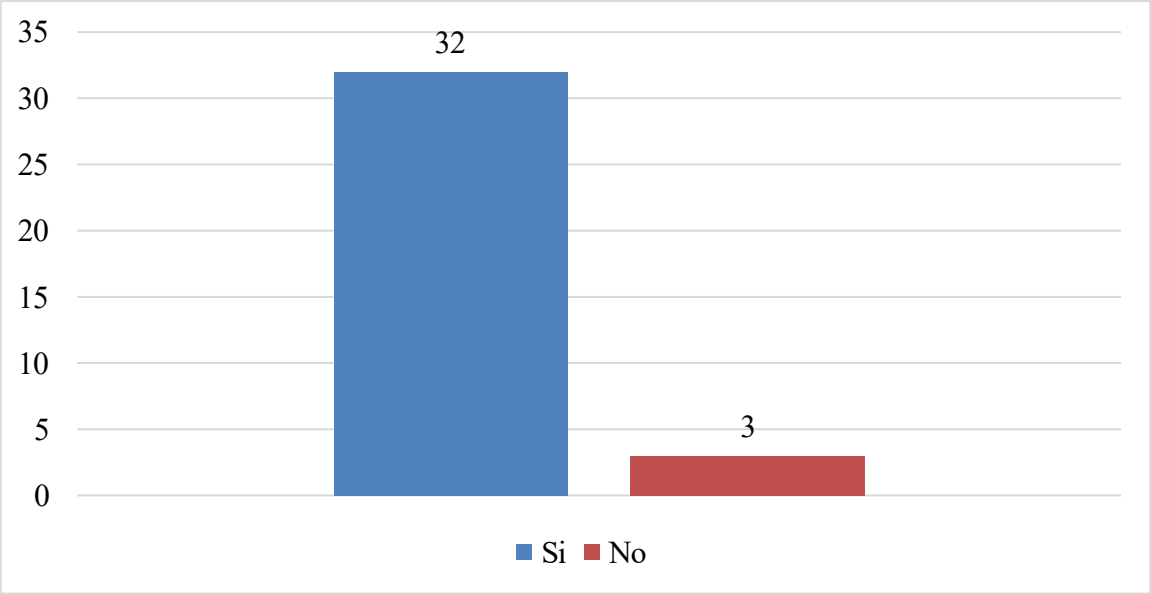
Nota. Resultados de la pregunta 6. Elaboración propia

Como se observó en la figura 10, todos los participantes opinaron que la SEDCHOCÓ cuenta con un inventario de activos de información. Esta información demostró que se puede identificar riesgos en los activos de la información de manera oportuna.

Pregunta 7:

Figura 11

¿La SEDCHOCÓ, Verifica los Sistemas de Forma Regular, para Determinar si están Adecuados a los Estándares de Seguridad Implementados?



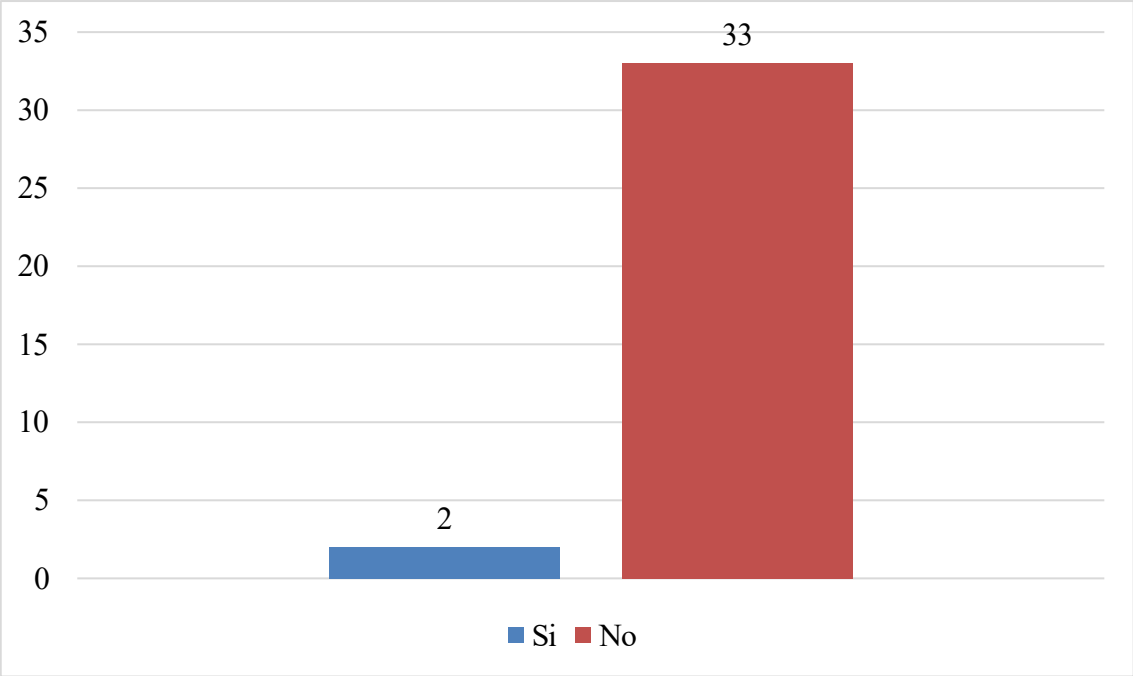
Nota. Resultados de la pregunta 7. Elaboración propia

Como se observó en la figura 11, la mayoría de los participantes, esto es, 32 personas opinaron que, en la SEDCHOCÓ, se verifican los sistemas de forma regular, a fin de determinar si están adecuados a los estándares de seguridad implementados, mientras que 3 participantes, respondieron que no. En consecuencia, con esta información se evidencia que la identificación de riesgos en la SEDCHOCÓ no se realiza e estricto cumplimiento de las normas.

Pregunta 8:

Figura 12

¿Consideras que es Posible que Ocurra un Riesgo en los Activos de Información Dentro de la SEDCHOCÓ?



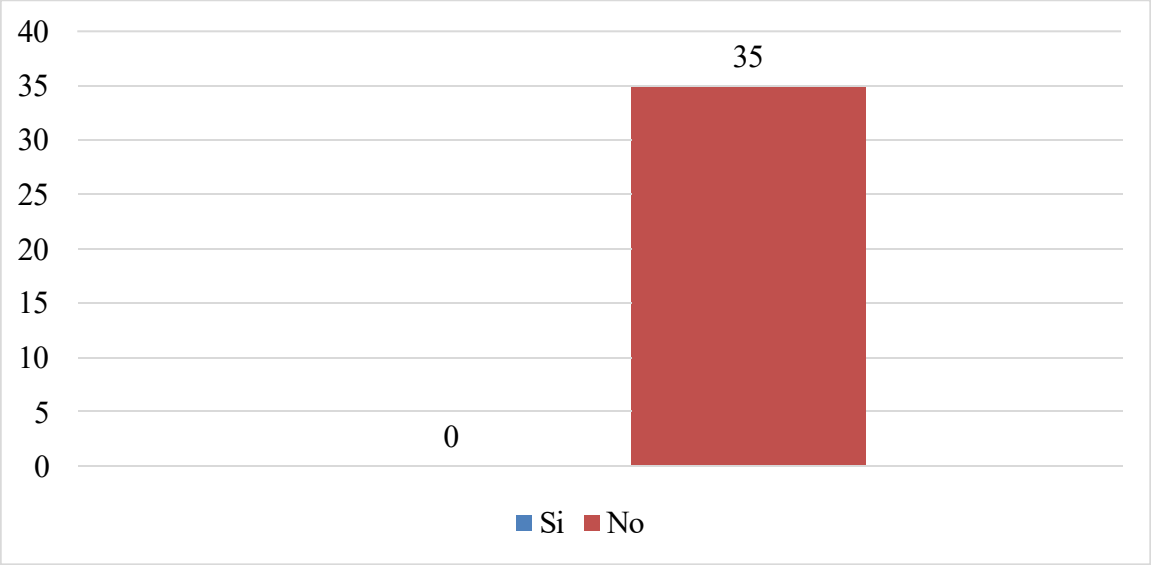
Nota. Resultados de la pregunta 8. Elaboración propia

Según la figura 12, se observó que 33 de los participantes expresaron sobre la estimación de riesgo no es posible que ocurra un riesgo frente a los activos de información dentro de la SEDCHOCÓ, mientras de 2 participantes, afirmaron que sí. En efecto, se evidencia que es posible que ocurra un riesgo en los activos de información de la SEDCHOCÓ.

Pregunta 9:

Figura 13

¿La SEDCHOCÓ Cuenta con Horarios Establecidos para Acceder a la Información?



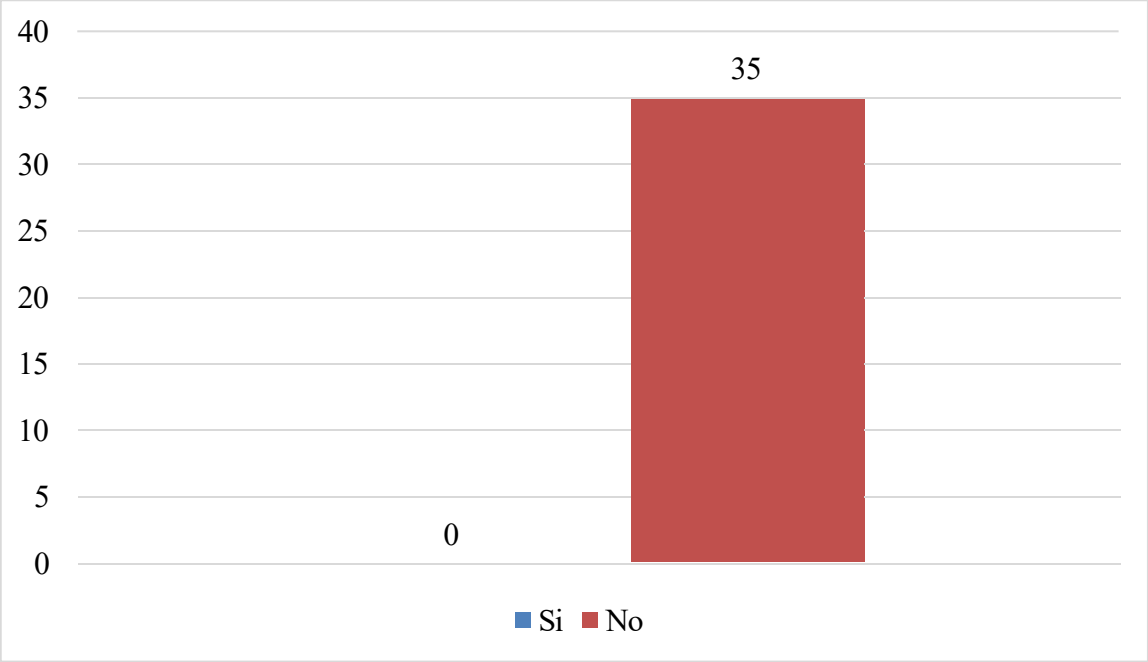
Nota. Resultados de la pregunta 9. Elaboración propia

Tal y como lo muestra la figura 13, todos los participantes respondieron que, la SEDCHOCÓ, no cuenta con horarios establecidos para acceder a la información. En consecuencia, esta información evidencia riesgo en la SEDCHOCÓ, dado que no se está realizando, ni cumpliendo con la Norma ISO/IEC 27001.

Pregunta 10:

Figura 14

¿Existen Tipos de Acceso para Usuarios?



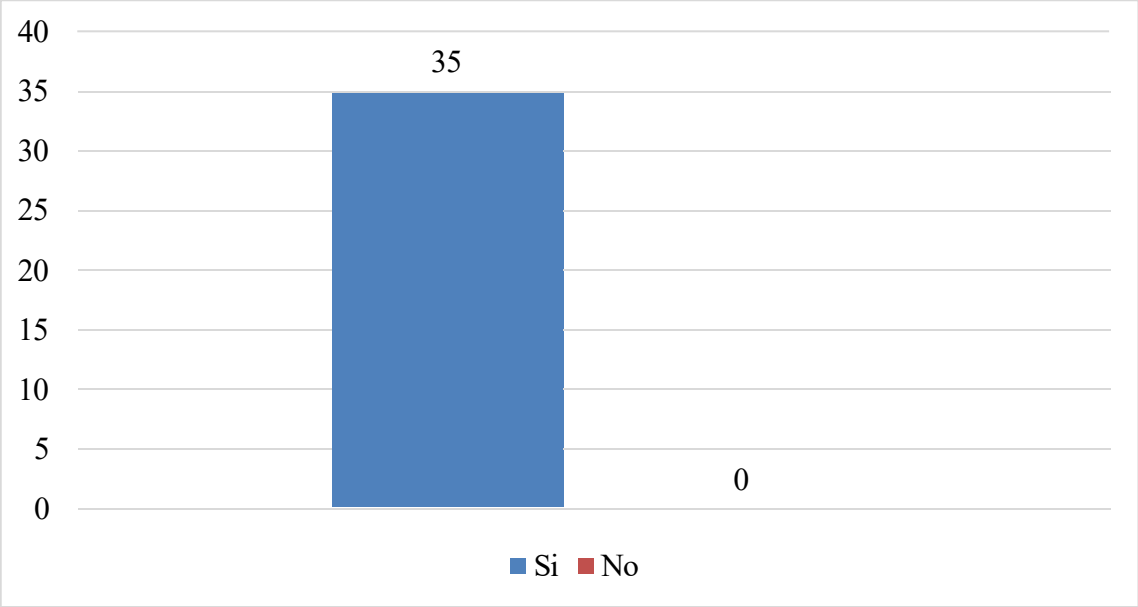
Nota. Resultados de la pregunta 10. Elaboración propia

La figura 14, muestra que todos los participantes manifestaron que en la SEDCHOCÓ, no existen tipos de acceso para los usuarios; evidenciando así que es posible que ocurra un riesgo ya que la SEDCHOCÓ, no se está cumpliendo con la Norma ISO/IEC 27001.

Pregunta 11:

Figura 15

¿Los Usuarios Cuentan con los Mismos Tipos de Acceso para Acceder a la Información?



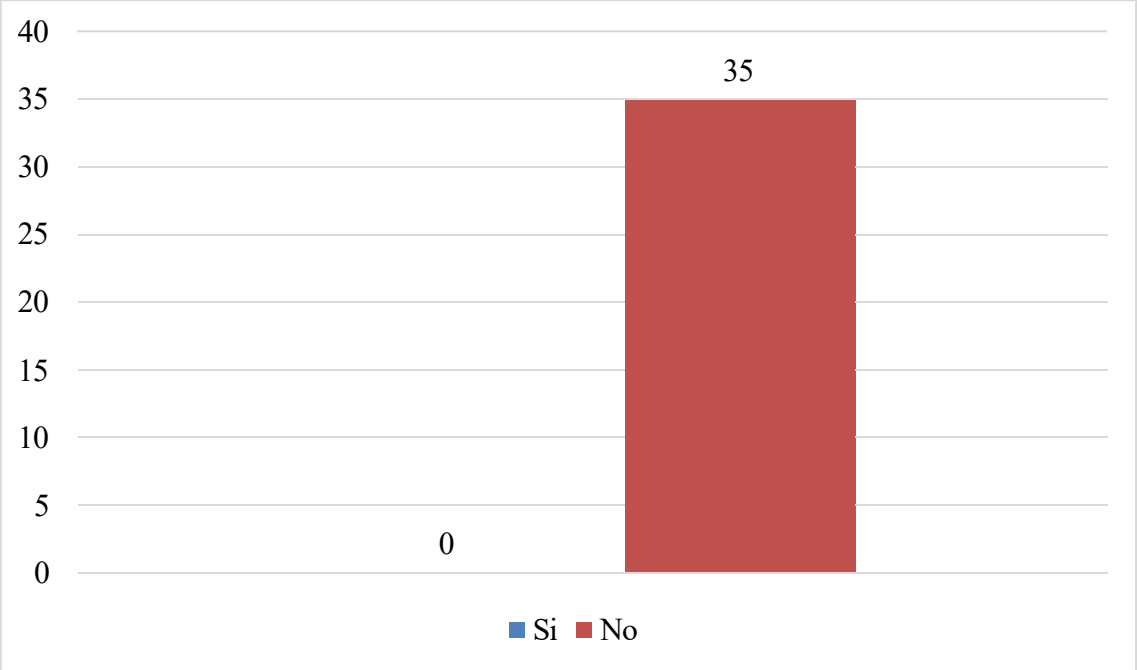
Nota. Resultados de la pregunta 11. Elaboración propia

Tal y como se evidencia en la figura 15, todo participantes respondieron que la SEDCHOCÓ, cuentan con los mismos tipos de acceso para acceder a la información, lo cual evidencia que existe riesgo en la SEDCHOCÓ, de que cualquier persona pueda acceder a la información y bases de datos de la entidad tal y como lo establece la Norma ISO/IEC 27001.

Pregunta 12:

Figura 16

¿En la SEDCHOCÓ, Existen Unidades de Almacenamiento de Respaldo?



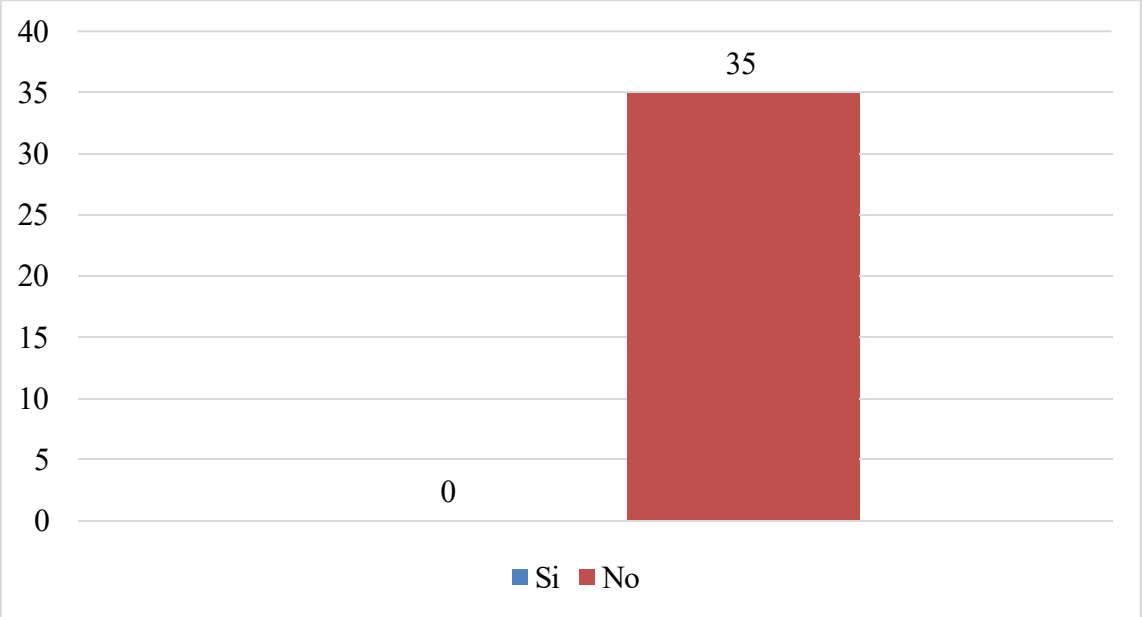
Nota. Resultados de la pregunta 12. Elaboración propia

De acuerdo con la figura 16, todos los participantes respondieron que, en la SEDCHOCÓ, no existen unidades de almacenamiento de respaldo, dejando así en evidencia el alto riesgo que existe para la SEDCHOCÓ, al no implementar, ni cumplir con la norma ISO/IEC 27001.

Pregunta 13:

Figura 17

¿Existen Controles de Acceso para Ingresar al Computador de los Usuarios?



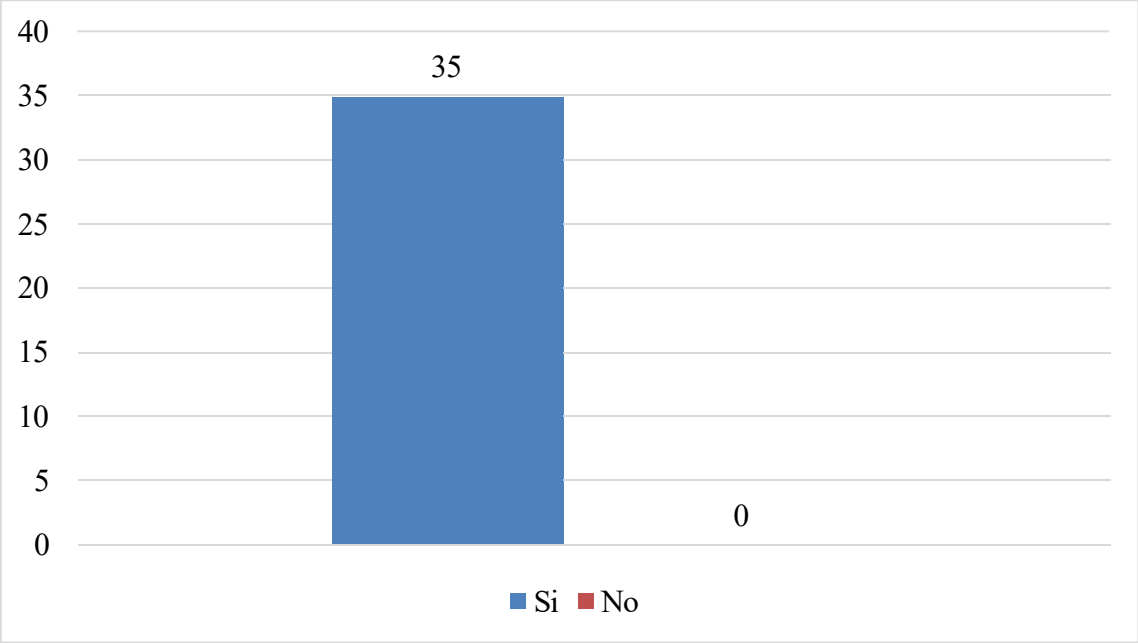
Nota. Resultados de la pregunta 13. Elaboración propia

Como se observó en la figura 17, todos los participantes opinaron que en la SEDCHOCÓ no existen controles de acceso para ingresar al computador de los usuarios. Lo cual demuestra que existen riesgos en los controles de acceso a la información de la entidad.

Pregunta 14:

Figura 18

¿Cualquier Usuario Puede Acceder a toda la Información de la SEDCHOCÓ?



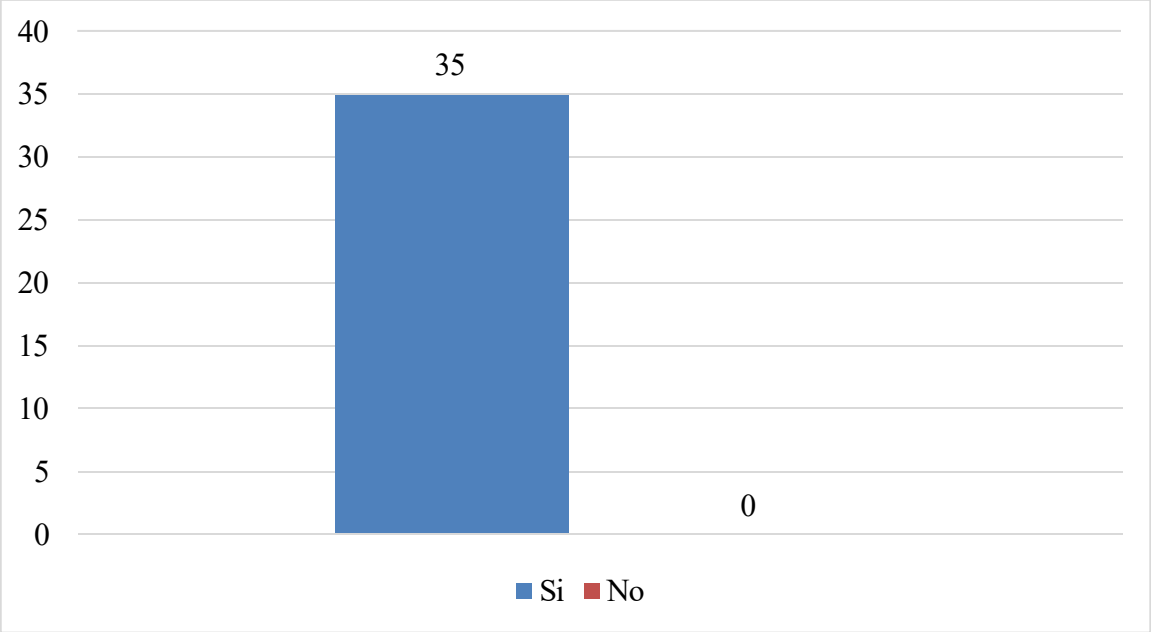
Nota. Resultados de la pregunta 14. Elaboración propia

Como se observó en la figura 14, todos los participantes, esto es 35 personas, manifestaron que, en la SEDCHOCÓ, cualquier usuario puede acceder a toda la información de la entidad. En efecto, según este interrogante, en términos generales, en la SEDCHOCÓ, se identifican riesgos con relación a acceso a la información de la entidad, cualquier persona ajena a la entidad puede acceder a la información, siempre y cuando tenga acceso al computador de un funcionario de la entidad.

Pregunta 15:

Figura 19

¿Considera que es Importante que la SEDCHOCÓ Realice Copias de Resguardo de Forma Periódica?



Nota. Resultados de la pregunta 15. Elaboración propia

De acuerdo con la figura 19, todos los participantes respondieron que, es importante que la SEDCHOCÓ se realice copias de resguardo de forma periódica. En consecuencia, con esta información se evidencia en la entidad no se está resguardando la información tal y como lo exige la norma ISO/IEC 27001.

Análisis Diagnóstico de los Procesos y Procedimientos que se Ejecutan en la SEDCHOCÓ para el Mejoramiento y Optimización de la Información

Para la realización del diagnóstico de los procesos y procedimientos que se ejecutan en la SEDCHOCÓ enfocado en el mejoramiento y optimización de la información se aplicó la técnica de la encuesta dirigida a los funcionarios administrativos y contratistas de la Oficina TI de la entidad que tienen algún tipo de responsabilidad sobre la información que se utiliza para el desarrollo de cada uno de los procesos efectuados en la SEDCHOCÓ.

De acuerdo con el análisis de la encuesta aplicada a funcionarios y contratistas que tienen un rol administrador en los diferentes sistemas de información o aplicativos de la entidad, tal y como se evidenció en las figuras 5 y siguientes, las situaciones que ameritan la toma de medidas para el mejoramiento y optimización de la información en la SEDCHOCÓ, son la definición y seguimiento de la Política de Seguridad de la Información bajo la Norma ISO/IEC 27001, así como también, la creación de un comité que se encargue de la revisión periódica y de la gestión en los temas de Seguridad de la Información.

De lo anterior, se puede afirmar entonces que, la propuesta de diseño de la política de seguridad de la información basada en la Norma ISO/IEC 27001 para la Servicios tecnológicos para la SEDCHOCÓ, se evitará que la información que reposa en la entidad, ya sea que contenga datos de esta o de terceros, caiga en manos de personas inescrupulosas que incluso puedan llegar a hacer uso de dicha información para fines delictivos, por ejemplo, suplantación de identidad, o extorsión.

Elementos del Modelo de Gestión TI, Basado en la Norma ISO/IEC 27001 para la Elaboración de la Propuesta de Diseño de la Política de Seguridad de la Información de la SEDCHOCÓ

Teniendo en cuenta los lineamientos que se deben tener en cuenta en el diseño de las políticas en las Tecnologías de la Información, propuestos en la Norma Técnica NTC-ISO-IEC 27001 del 2013, así como también, los lineamientos establecidos por el MINTIC, por ello, con la finalidad de asegurar la información de la SEDCHOCÓ y la implementación del Sistema de Gestión de Seguridad de la Información SGSI, el diseño de la política de seguridad debe tener en cuenta, inicialmente, la identificación de la misión, las necesidades y las prioridades que tenga la entidad respecto al entrenamiento y sensibilización del personal, además de los siguientes elementos: a) el diseño de la política, a fin de que se ejecute un plan de capacitación y sensibilización el cual incluya como tema principal la política de seguridad de la información; b) el alcance de la política; c) roles y responsabilidades de quienes desarrollaran, implementaran y mejoran continuamente la política; d) metas para cumplir con la política desarrollada; e) capacitaciones y talleres obligatorias para todo el personal; f) los temas a ser tocados en cada taller o capacitación; g) frecuencia de las capacitaciones o talleres y las situaciones en las que será necesaria una capacitación (reinducciones o capacitaciones para personal nuevo, etc.). h). documentación y evidencia de cada aspecto de la política (incluyendo evaluaciones). (MINTIC,2016, p. 17).

Con base en lo expuesto, a continuación, se presenta la propuesta de diseño de la política de seguridad de la información para la SEDCHOCÓ.

Propuesta de Diseño de la Política de Seguridad para Mejorar el Proceso de Transmisión de la Información Basada en la Norma ISO/IEC 27001 para la SEDCHOCÓ

Teniendo en cuenta que los resultados de las encuestas aplicadas en la SEDCHOCÓ, evidenciaron riesgos en la seguridad de la información, a continuación, se presenta una serie de políticas alineadas a la Guía número 2 del Modelo de Seguridad y privacidad de la Información para las Entidades del Estado del Ministerio de Tecnologías de la Información.

Para la SEDCHOCÓ, es importante contar con una política de seguridad, puesto es esta que guía el comportamiento del personal y profesional de los funcionarios, contratistas y terceros, frente a la información que se obtiene, genera y procesa por la entidad, además, la política le permite a la entidad, trabajar bajo las mejores prácticas de seguridad, así como también cumplir con los requisitos legales, los cuales está obligada a cumplir.

Razón por la cual, el Secretario de Educación Departamental, tendrá el deber de designar a un funcionario de la Oficina de las Tecnologías de la información, para que esta sea la persona encargada de asumir el compromiso de brindar el apoyo en las actividades de sensibilización a funcionarios y contratistas que hagan parte del proceso, para que cumplan las políticas relacionadas con la seguridad información de la entidad.

A continuación, se presenta la propuesta de diseño de la Política de Seguridad de la Información, bajo la Norma ISO/IEC 27001:2013 para la SEDCHOCÓ.

Objeto y campo de aplicación: la Política de Seguridad de la Información establece las directrices y normatividad nacional que se aplicará en la entidad, aplica a funcionarios y terceras partes autorizadas, incluidos los contratistas que forman parte de la SEDCHOCÓ.

Desarrollo de la Política de Seguridad

Objetivo: esta política busca establecer las directrices y normatividad con las que se pueda garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la SEDCHOCÓ, mediante la adecuada orientación y soporte para los procesos de gestión de la seguridad de la información en la entidad.

A continuación, se establecen tres (30 políticas de seguridad que soportan el SGSI para la SEDCHOCÓ:

Política de control de acceso

Tabla 5

Política de Control de Acceso

Entidad:	Secretaría de Educación del Departamento del Chocó – SEDCHOCÓ
Objetivo de la política:	Proveer las directrices para que únicamente los funcionarios y terceras partes autorizadas, incluidos los contratistas, puedan acceder a la información.
Gestión de acceso a usuarios:	● El funcionario encargado del proceso, será el responsable de la verificación, definición y autorización, previo al análisis de las funciones que desempeñará el usuario y los privilegios necesarios para la gestión de cuentas en lo relacionado con los sistemas de información, aplicativos, plataformas y correos institucionales. ● Semestralmente, se revisarán las competencias de los usuarios asignados con los perfiles, para que se ajusten a la política de control de acceso. ● La Oficina de Talento Humano, deberá notificar a la Oficina de la TI, la terminación de contratos o cambio de funciones de los funcionarios de la entidad.

Entidad:	Secretaría de Educación del Departamento del Chocó – SEDCHOCÓ
Responsabilidad del usuario:	● De igual manera, será necesario validar en la infraestructura tecnológica de la SEDCHOCÓ los accesos a servicios *tp, http, https, dns, icmp* y los que se encuentren disponibles en la red de datos de la SEDCHOCÓ. ● Los funcionarios y terceros autorizados, son los responsables de mantener la confidencialidad de sus contraseñas de forma personal e intransferible. ● Las contraseñas de acceso a cualquier servicio o plataforma de la entidad, no debe ser almacenada en hojas ni en ficheros o archivos de software que no tengan características de repositorios seguros de contraseñas, ni tampoco, deberán ser asociadas a las contraseñas de tipo personal de los usuarios.
Control de acceso a sistemas y aplicaciones:	● La Oficina Administrativa, debe verificar los mecanismos mediante los cuales hará efectiva la implementación de la política de trabajo en áreas seguras y lo referente a la seguridad física de los equipos y demás infraestructura tecnológica de la SEDCHOCÓ para controlar su acceso de personal no autorizado, por ello, será fundamental, asignar cuantas a las dependencias, las cuales

Entidad:	Secretaría de Educación del Departamento del Chocó – SEDCHOCÓ
	deberán mantener un identificador ID de usuarios y contraseña individual, la cual deberá ser cambiada periódicamente cada 6 meses. ● Los archivos que contengan las contraseñas de las cuentas de usuario, deben estar cifrados y protegidos.

Nota. Política de Control de Acceso. Elaboración propia

Política de uso aceptable de los activos

Tabla 6

Política de Uso Aceptable de los Activos

Entidad:	Secretaría de Educación del Departamento del Chocó - SEDCHOCÓ
Objetivo de la política:	Informar a los funcionarios y terceras partes autorizadas, incluidos los contratistas, sobre el tratamiento que debe tener para cada activo asociado a la información que tengan a su cargo en lo referente a la seguridad de la información.
Gestión de acceso a usuarios:	● El inventario de activos, se actualizará como documento de referencia permanente. Esta función, estará a cargo del líder del proceso, quien será el encargado de cumplir con la responsabilidad y gestión de los activos de información. ● En el inventario se hará referencia al tipo de activo, los cuales se agruparán por elementos, por lo cual será necesario referenciar cada activo, por ejemplo, la SEDCHOCÓ tiene 78 equipos de cómputo de usuario final, referenciándolo como “computador de funcionario”. ● Cada área u oficina de la entidad, será responsable del inventario de los activos.

Entidad:	Secretaría de Educación del Departamento del Chocó - SEDCHOCÓ

- El uso aceptable d ellos activos es responsabilidad del líder del proceso, el cual tendrá el deber de determinar los lineamientos que deban seguir todos los funcionarios y terceros autorizados, así como los usuarios en general, cuando tengan acceso a la información de la SEDCHOCÓ, conforme a los lineamientos legales y normativos.
- El uso aceptable de los activos, podrá tomarse con decisiones descritas a continuación:

Tipos de información:

Tipo de activo	Decisión
Información digital:	● Almacenarse en forma cifrada. ● Que sea transmitida en forma cifrada. ● Que sea transmitida con el uso de firma digital. ● Almacenarla con el uso de firma digital. ● Que sea imposible imprimirla. ● Realizar una búsqueda automática con DLP para detectar si se encuentra almacenado en forma no autorizada en algún equipo.

Entidad:	Secretaría de Educación del Departamento del Chocó - SEDCHOCÓ
Información física:	● Monitoreo de todo lo que se haga con el activo. ● Realizar búsqueda automática con DLP, a fin de determinar si se encuentra almacenado en forma no autorizada en algún equipo de la entidad. ● Monitorear todo lo que se haga con el activo de información ● Que únicamente se pueda almacenar bajo llave. ● Que no sea reciclable. ● Las cuales puedan destruirse una vez sean utilizadas. ● Que no se puede almacenarse en un escritorio. ● Puede ocurrir que activos de información que en la actualidad se manejan en forma física, sean vulnerables, por lo que, en el plan de tratamiento se restringirá su uso.
Hardware:	● Equipos portátiles solo pueden salir de las oficinas de la SEDCHOCÓ si cuentan con el cifrado de Disco.

Entidad:	Secretaría de Educación del Departamento del Chocó - SEDCHOCÓ
	● El suministro eléctrico solo debe hacerse desde fuentes reguladas y con monitoreo de la oficina TI. ● Cambios en el hardware solo pueden ser realizados por personal autorizado por la Oficina de TI de la entidad.

Nota. Política de Uso Aceptable de los Activos. Elaboración propia

Política de generación y restauración de copias de respaldo

Tabla 7

Política de Generación y Restauración de Copias de Respaldo

Entidad	Secretaría de Educación del Departamento del Chocó - SEDCHOCÓ
Objetivo de la política	Proveer las directrices para que el proceso de generación y restauración de copias de respaldo se realice con aplicación de los requerimientos de seguridad para los activos de información.
Responsabilidad de los usuarios:	● Los funcionarios y terceras partes autorizadas, incluidos los contratistas, deben suscribir actas de confidencialidad en las que se les informa respecto a la responsabilidad penal, respecto a las contraseñas que le sean asignadas, para acceder a los diferentes sistemas de información de la entidad. ● Dentro de sus responsabilidades, también estará el control *antimalware* que provee la SEDCHOCÓ de manera gratuita y/o licenciada, para la utilización de los equipos de cómputo. ● Ante incidentes relacionados con *malware,* el responsable será el propietario del equipo desde el cual se generó.

	● El jefe de la oficina TI, podrá desconectar el equipo de la red por el tiempo que considere necesario, a fin de tratar el *malware,* y evitar su propagación. ● Desde la vinculación en la entidad del funcionario y terceras partes autorizadas, incluidos los contratistas de la oficina de Talento Humano de la SEDCHOCÓ, será el responsable de mantener las copias de seguridad de la información de la entidad. ● Cada propietario de información será responsable de realizar de forma continua las copias de seguridad, ya que, ante una falla, la responsabilidad recaerá en él, y no en el jefe de la oficina.
Obligatoriedad del respaldo:	● Los jefes de procesos, deben garantizar la ejecución y custodia de las copias de seguridad, y velar por la propiedad intelectual de la información de la entidad. Por lo cual, deben verificar que los funcionarios y contratistas entreguen los respaldos de la información, o que, en su efecto, no la oculten o guarden para ellos. ● Los funcionario y terceras partes autorizadas, incluidos los contratistas, deben aplicar la disponibilidad, confidencialidad y custodia de la información clasificada en el inventario de

	activos, al igual que brindar, a la ciudadanía la información que requiera con base en la ley de transparencia ya acceso a la información pública.

Nota. Política de Generación y Restauración de Copias de Respaldo. Elaboración propia

Evaluación del Impacto de la Aplicación de la Política de Seguridad de la Información Basada en la Norma ISO/IEC 27001 para la Secretaria de Educación del Chocó, a partir de la Aplicación de Cuestionarios

Con base en los resultados de la aplicación del cuestionario, se puede afirmar que, el enfoque de la evaluación debe orientarse principalmente a identificar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información; donde el nivel de riesgo aceptable se define en función de la probabilidad de ocurrencia del riesgo y las consecuencias generadas en caso de que este llegara a materializarse (impacto).

Por ello, las evaluaciones de riesgos periódicas, a través de las cuales se puedan establecer mecanismos para planear y controlar las operaciones y requerimientos de seguridad, serán el enforque central para la gestión del sistema.

Otro aspecto importante a evaluar, es la efectividad y desempeño del sistema de gestión, a través de las auditorías internas, ya que estas permiten que se pueda hacer una evaluación detallada del sistema de información de la SEDCHOCÓ, para de detectar de forma eficaz, errores, amenazas, vulnerabilidades y riesgos a los que está expuesta, con la finalidad entre otras cosas de proteger los activos, minimizar los riegos y posibles fraudes, optimizar la calidad y seguridad de la información e incrementar la eficacia operativa, posibilitando además, el análisis de evaluaciones y medidas sobre las operaciones analizadas de la entidad.

Conclusiones

Después de desarrollar el diseño de la Política de Seguridad de la Información basada en la Norma ISO/IEC 27001 para la Secretaria de Educación del Chocó, se plantean como conclusiones las siguientes:

La seguridad de la información en la Secretaria de Educación del Chocó, se puede garantizar mediante la implementación del estándar para la gestión del sistema de seguridad de la información en cumplimiento de la Norma colombiana ISO/IEC 27001:2013, para los procesos de manejos de los servicios de la plataforma y entornos digitales de la entidad.

En la Secretaria de Educación del Chocó, existen vulnerabilidades en los activos de la información, por ello, la valoración del riesgo de manera oportuna, evitara que la amenaza logre impactar los activos de la información de gran importancia para la entidad, por ende, la implementación de actualización del análisis de riesgo de manera constante, ayudara a mitigar la probabilidad de amenaza en los activos de la entidad.

La Política de Seguridad de la información que se propone, incluye los aspectos, características, los modelos de seguridad y privacidad de la información y buenas prácticas recomendadas por la gestión de la seguridad son base en la Norma ISO/IEC 27001:2013, esto con el fin de que se pueda aplicar en la Secretaria de Educación del Chocó para así, gestionar de manera efectiva, los riesgos que afectan el cumplimento de los objetivos de la SEDCHOCÓ.

Recomendaciones

Con base en la experiencia adquirida con el desarrollo de esta investigación, se recomienda la aplicación de la metodología Magerit para la elaboración de proyectos, planes y procesos en los que se requieran estructurar de forma sistemática y organizada la gestión de riesgos, en razón a que esta metodología, en este estudio proporcionó la guía adecuada para abordar el análisis de la gestión de riesgo en la entidad objeto de estudio.

Con el objetivo de garantizar el cumplimento de la Política de Seguridad de la información en la SEDCHOCÓ, resulta necesario que se realice una evaluación de forma periódica, la cual permita verificar si los funcionarios y contratistas de la entidad, cumplen con las normas definidas, así como también, poder determinar si los controles aplicados satisfacen o no las necesidades de seguridad.

La Oficina TI de la SEDCHOCÓ, debe liderar y promover capacitaciones sobre la importancia de la seguridad de la información en la entidad, así como también desarrollar planes y políticas de seguridad de la información, especialmente, porque esta es una entidad pública y el manejo de la información debe ser estrictamente confidencial.

Referencias

Amaya Díaz, H. F. (2022). *Diseño de un SGSI basado en la ISO/IEC 27001 para el liceo Moderno José Celestino Mutis de San Sebastián de Mariquita*. Tesis de Maestría, Universidad Nacional Abierta y a Distancia – UNAD.

Ayala, J., Ariza, J. y González, L. (2020). La protección de datos en la era digital Colombia - España. *Revista Politécnico Grancolombiano*. Bogotá, Colombia. https://alejandria.poligran.edu.co/bitstream/handle/10823/2142/Articulo%20Proteccion%20de%20datos%20%20en%20la%20era%20digita%20Colombia-Espa%C3%B1a%20Nov.%2029..pdf?sequence=1yisAllowed=y

Benavides Sepúlveda, A. y Blandón Jaramillo, C. (2018). Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. *Sciencia et Technica, 23*(1), 85-92. https://www.redalyc.org/journal/849/84956661012/html/

Carvajal, D. L., Cardona, A., y Valencia, F. J. (2019). Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana1. *Entre Ciencia e Ingeniería, 13*(25), 68-76.

Corrales Rubiano, M. F. (2020). Factores de éxito en la implementación de proyectos de transformación digital, una mirada desde el proceso de gestión documental en entidades públicas colombianas. Universidad EAN, Facultad de Ingeniería, Bogotá D.C.

Cruz Mosquera, C. Y. (2022). *Secretaría de Educación Departamental del Chocó*. Recuperado el mayo de 2022, de Sedchoco: https://sites.google.com/site/sedsgc2014/estructura/estructura-organizacional

Chocó, S. D. (2024). Recuperado el mayo de 2024, de Sedchoco: http://www.sedchoco.gov.co/dependencias/

Compes 3670, 2. (28 de junio de 2010). *Mintic.* Recuperado el mayo de 2022, de https://www.mintic.gov.co/arquitecturati/630/articles-9029_documento.pdf

Cruz Mosquera, C. Y. (2022). *Secretaría de Educación Departamental del Chocó*. Recuperado el mayo de 2022, de Sedchoco: https://sites.google.com/site/sedsgc2014/estructura/mapa-de-procesos-sedchoco

Decreto 1008, 2. (2018). *Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la In.* Congreso de la República de Colombia. Diario Oficial No. 50624.

Decreto 415, 2. (2016). *Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información.* Congreso de la República de Colombia. Diario Oficial No. 49808.

Decreto 1078, 2. (2015). *Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.* Congreso de la República de Colombia. diario Oficial No. 49523.

Decreto 2573, 2. (2014). *Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.* Congreso de la República de Colombia. Diario Oficial No. 49363.

Decreto 333, 2. (2014). *Por el cual se reglamenta el artículo 160 del Decreto-ley 19 de 2012.* Congreso de la República de Colombia. Diario Oficial No. 49049.

Decreto 2578, 2. (2012). *Por el cual se reglamenta el Sistema Nacional de Archivos, se establece la Red Nacional de Archivos, se deroga el Decreto número 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los archivos del Estado.* Congreso de la República de Colombia. Diario Oficial No. 48643.

Decreto 2609, 2. (2012). *Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.* Congreso de la República de Colombia. Diario Oficial No. 48647.

Decreto 2482, 2. (2012). *Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión.* Congreso de la República de Colombia. Diario Oficial No. 48634.

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., y Saltos-Gómez, J. A. (2017). La seguridad informática y la seguridad de la información. *Polo del Conocimiento, 2*(12), 145-155.

Lerma Vinlasaca, R. C., y Donoso Gallo, D. F. (2018). *Implementación de un sistema de gestión de seguridad de información basado en la Norma ISO 27001:2013 para el control físico y digital de documentos aplicado a la empresa LOCKERS S.A.* Universidad de las Fuerzas Armadas ESPE, Maestría en Gerencia de Sistemas., Sangolqui.

Ley 1753, 2. (2015). *Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país".* Congreso de la República de Colombia. Diario Oficial No. 49538.

Ley 1714, 2. (2014). *Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.* Congreso de la República de Colombia. Diario Oficial No. 49084.

Ley 1581, 2. (2012). *Por la cual se dictan disposiciones generales para la protección de datos personales.* Congreso de la República de Colombia. Diario Oficial No. 48587.

Ley 1273, 2. (2009). *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.* Congreso de la República de Colombia. Diario Oficial No. 47223.

Ley 1341, 2. (2009). *Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.* Congreso de la República de Colombia. Diario Oficial No. 47426.

Ley 1266, 2. (2008). *Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dicta.* Congreso de la República de Colombia. Diario Oficial No. 47219.

Ley 962, 2. (2005). *Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.* Congreso de la República. Diario Oficial No. 46023.

Ley 603, 2. (2000). *Por la cual se modifica el artículo 47 de la Ley 222 de 1995.* Congreso de la República de Colombia. Diario Oficial No. 44108.

Ley 599, 2. (2000). *Por la cual se expide el Código Penal.* Congreso de la República de Colombia. Diario Oficial No. 44097.

Moreno Novoa, M. L. (2021). *Aplicación móvil para entrenamiento, seguimiento y evaluación en medidas de seguridad de la información basada en la norma NTC - ISO/IEC 27001.* Universidad Antonio Nariño, Facultad de Ingeniería de Sistemas y Computación, Bogotá D. C.

MINTIC. Ministerio de Tecnologías de la Información y las Comunicaciones. Marco de la transformación digital para el Estado colombiano. junio 2020 [en línea]. [citado 05, mayo, 2024]. Disponible en Internet: https://gobiernodigital.mintic.gov.co/692/articles-179145_Marco_Transformacion_Digital.pdf

MINTIC. Ministerio de Tecnologías de la Información y las Comunicaciones. Elaboración de la política general de seguridad y privacidad de la información. Guía No. 2 – Seguridad y Privacidad en la información [en línea]. Bogotá: El sitio [citado 28, junio, 2020]. Disponible en Internet: < URL: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>

Norma ISO 27001. (2013). *Norma ISO27001*. Recuperado el mayo de 2022, de https://normaiso27001.es/

Poma Moya, C. C. (2020). *Desarrollo de un modelo de sistema de gestión de seguridad de la información basado en la norma NB/ISO/IEC 27001 aplicado al área de TI en empresas corredoras de seguros y reaseguros*. Universidad Mayor de San Andrés, Facultad de Ingeniería, Bolivia.

Ramírez Camargo, E. A. y Rinconc Pinzón, M. A. (2022). La importancia de la seguridad de la información en el sector público en Colombia. *Revista Ibérica de Sistemas y Tecnologías de Información,* (46), 87-99. https://scielo.pt/pdf/rist/n46/1646-9895-rist-46-97.pdf

Ramírez Támara, G. D. (2022). *Diseño de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013 para la corporación Universitaria Antonio José de Sucre*. Universidad Nacional Abierta y A Distancia – UNAD, Escuela de Ciencias Básicas, Tecnologías e Ingeniería – ECBTI, Sucre.

Restrepo Santacruz, J. F. (2017). *Diagnóstico del estado actual de la seguridad de la información basado en la norma ISO 27001:2013, de la institución educativa técnico industrial sede Mercedes Pardo de Simmonds de la ciudad de Popayán*. Universidad Abierta y A Distancia (UNAD), Escuela de Cencías Básicas, Tecnología e Ingeniería, Popayán.

Rodríguez Díaz, J. A., y Ruíz Rojas, Y. A. (2021). *Diseño de un sistema de gestión de seguridad de la información para el área de talento humano de la secretaría de educación de Fusagasugá basado en la norma NTC-IEC ISO 27001:2013.* Universidad Piloto de Colombia, Facultad de Posgrados, Bogotá D. C.

Secretaría de Educación Departamento del Chocó. (2024). Recuperado el mayo de 2024, de Sedchoco: http://www.sedchoco.gov.co/horizonte-institucional/

Secretaría de Educación Departamental del Chocó. (2024). Recuperado el mayo de 2024, de Sedchoco: http://www.sedchoco.gov.co/organigrama/

Vegas Varona, I. A. (2019). *Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura*

según la NTP ISO/IEC 27001. Trabajo de grado de pregrado, Universidad Nacional de Piura, Ingeniería Industrial, Piura.

Watkins, S. (2013). An Introduction to Information Security and ISO27001:2013: A Pocket Guide: Vol. 2nd ed. ITGP. http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=trueydb=nl ebkyAN=838719ylang=esysite=eds-liveyscope=site

Yaima Vargas, J. S. (2022). *Requerimientos para un sistema de gestión de documento electrónico de archivo en entidades privadas del sector real en Bogotá*. Trabajo de grado, Universidad de La Salle, Departamento de Estudios de Información, Bogotá D. C.