METODOLOGÍA PARA LA ADAPTACIÓN DE LAS ACTUALES POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LAS CUATRO DIVISIONES DE LA UNIDAD DE TRANSFORACIÓN DIGITAL E INFORMÁTICA (UTDI) DE LA DIRECCIÓN EJECUTIVA DE ADMINISTRACION JUDICIAL AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI).

Autores:
CARLOS ALBERTO MENDEZ LOPEZ
FRANCISCO JAVIER GARCIA REYES

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERIA
MAESTRÍA EN SEGURIDAD DIGITAL
BOGOTÁ, D.C.
2025

METODOLOGÍA PARA LA ADAPTACIÓN DE LAS ACTUALES POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LAS CUATRO DIVISIONES DE LA UNIDAD DE TRANSFORACIÓN DIGITAL E INFORMÁTICA (UTDI) DE LA DIRECCIÓN EJECUTIVA DE ADMINISTRACION JUDICIAL AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI).

Autores:

CARLOS ALBERTO MENDEZ LOPEZ
FRANCISCO JAVIER GARCIA REYES

MEMORIA DEL TRABAJO DE GRADO REALIZADO PARA CUMPLIR UNO DE LOS REQUISITOS PARA OPTAR AL TITULO DE

MAGÍSTER EN SEGURIDAD DIGITAL

Director

GUSTAVO ERNESTO CUBIDES ROBAYO
Comité de Evaluación del Trabajo de Grado

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERIA
MAESTRÍA EN SEGURIDAD DIGITAL
BOGOTÁ, D.C.
2025

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERIA
MAESTRÍA EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

Rector Magnífico

Luis Fernando Múnera Congote, S.J.

Decano Facultad de Ingeniería

Ing. Diego Alejandro Patiño Guevara, Ph.D.

Director Maestría en Seguridad Digital

Ing. Rafael Vicente Páez Mendez, Ph.D.

Director Departamento de Ingeniería de Sistemas

Ing. César Julio Bustacara Medina, Ph.D.

Artículo 23 de la Resolución No. 1 de junio de 1946

"La Universidad no se hace responsable de los conceptos emitidos por sus alumnos en sus proyectos de grado. Sólo velará porque no se publique nada contrario al dogma y la moral católica y porque no contengan ataques o polémicas puramente personales. Antes bien, que se vean en ellos el anhelo de buscar la verdad y la Justicia"

AGRADECIMIENTOS

El presente trabajo de investigación está dedicado con profundo agradecimiento a nuestras familias, cuyo respaldo incondicional, comprensión y paciencia han sido fundamentales a lo largo de este proceso académico lo que siempre nos mantuvo motivados para seguir adelante, incluso en los momentos de mayores retos, y ha sido lo más importante para alcanzar este logro.

Extendemos un agradecimiento muy especial a nuestro tutor por su guía, dedicación y generosidad al compartir sus conocimientos, su acompañamiento permanente y su disposición para orientarnos fueron necesarios para cumplir con los objetivos propuestos al igual que su compromiso con nuestra formación académica ha dejado una huella significativa en nuestro crecimiento profesional y personal.

Contenido

Índice de Figuras

Índice de tablas

RESUMEN

La seguridad de la información es base para las instituciones públicas y privadas en Colombia cuya gestión enfrenta retos relacionados con la madurez digital, la implementación de políticas claras y la capacidad de respuesta ante incidentes, es por ello que la Constitución Política, a través del artículo 15 garantiza el derecho a la privacidad lo que obliga al Estado a adoptar metodologías y estándares adecuados y el Ministerio TIC promueve el Modelo de Seguridad y Privacidad de la Información (MSPI), basado en la norma ISO/IEC 27001 y requiere alinearse con las directrices gubernamentales actuales.

ABSTRACT

Information security is essential for both public and private institutions in Colombia; however, its management faces challenges related to digital maturity, policy implementation, and incident response. Article 15 of the Colombian Constitution guarantees the right to privacy, which requires the government to implement methodologies and standards such as the Information Security and Privacy Model (MSPI) developed by MINTIC, in alignment with national regulations. The Digital Transformation and IT Unit (UTDI) has an Information Security Management System (ISMS) based on ISO/IEC 27001, but it must be adapted to the MSPI to comply with current governmental guidelines.

INTRODUCCIÓN

El incremento de los ataques informáticos en todos los sectores digitalizados, junto con su creciente efectividad impulsada por el desarrollo y la evolución tecnológica, representa un reto para la gestión y control de la seguridad de la información, este panorama obliga a empresas e instituciones a adoptar métodos y herramientas cada vez más avanzadas considerando que la transformación tecnológica ha fortalecido la capacidad de los ataques, comprometiendo la protección de los datos; por todo lo anterior, es imperativo que las entidades públicas quienes se encargan de custodiar información crítica y sensible de los ciudadanos, modernicen sus prácticas de seguridad adoptando como mínimo los estándares básicos de protección para enfrentar nuevas amenazas y preservar los principios fundamentales de confidencialidad, integridad y disponibilidad.

Para hacer frente a esta situación que es visible a nivel mundial, se han desarrollado políticas, normas y estándares orientados a garantizar la protección de la seguridad de la información. En Colombia se han implementado normativas y modelos de cumplimiento, entre los que se destaca el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual está basado tanto en la normativa ISO27001 como el estándar de la NIST. Esta normativa está desarrollada sobre tres módulos y abarca un total de 181 controles distribuidos en cada uno:

1. Administrativo: 39
2. Técnico: 72
3. NIST: 70

Esta normativa está promovida por el Ministerio de Tecnologías de la Información y las Comunicaciones, este modelo establece lineamientos que fortalecen los sistemas de gestión de seguridad en las entidades públicas, tomando como referencia estándares

internacionales (ISO27001 y estándar NIST), además, su implementación está respaldada por normas nacionales como la Directiva Presidencial 03 y la Resolución 00500 del 10 de marzo de 2021, que exigen su aplicación en el sector público.

En este contexto, la presente propuesta de trabajo de grado tiene como objetivo alinear la política de seguridad vigente en las cuatro divisiones de la Unidad de Transformación Digital e Informática (UTDI): División de Servicios Tecnológicos, División de Seguridad y Protección de Datos, División de Infraestructura de Hardware, Comunicaciones y Centros de Datos, y División de Infraestructura de Software; actualmente, la UTDI opera bajo un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001, a pesar de esto, es necesario que este sistema se ajuste e integre con el MSPI, garantizando así el cumplimiento de legal aplicable a las entidades del sector público colombiano.

1. DESCRIPCIÓN GENERAL

Oportunidad y problemática

La gestión de la seguridad de la información en el sector público Colombiano enfrenta desafíos considerables que comprometen su eficacia frente a los crecientes retos de la era digital, en particular las cuatro divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial, las cuales operan bajo un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001, dicho sistema no se encuentra alineado con lo establecido por el Estado colombiano para las entidades públicas territoriales en el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

La integración estratégica de la normativa ISO 27001:2022 con el Modelo de Seguridad y Privacidad de la Información (MSPI) representa un beneficio sustancial para la Rama Judicial. Esta sinergia no solo optimiza la protección de datos sensibles, sino que también fortalece la confianza en el sistema judicial y salvaguarda los derechos fundamentales de los ciudadanos. La adopción de estos estándares es un paso crucial hacia una mayor madurez digital y una ciberseguridad robusta, elementos esenciales para garantizar la continuidad y la fiabilidad de los servicios judiciales en la era digital.

La adopción del MSPI es una oportunidad para fortalecer la seguridad de la información en la UTDI, este modelo alineado con directrices nacionales como la Directiva 03 de 2021 de la Presidencia de la República y la Resolución 00500 del 10 de marzo de 2021 proporcionando el marco integral que combina estándares internacionales con requisitos específicos del contexto colombiano.

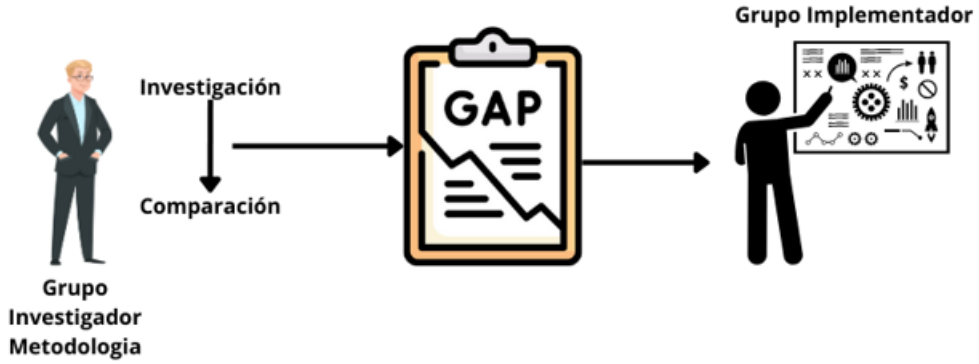
Implementar una metodología de adaptación al MSPI permitirá a la UTDI cumplir con la normatividad nacional aplicable, mejorar la protección de datos judiciales y optimizar la respuesta ante incidentes de ciberseguridad fomentando la madurez digital de la institución promoviendo capacitaciones, metodologías y estándares que no solo permitan el cumplimiento de requisitos legales, sino que también refuercen la confianza de los ciudadanos en la gestión de la información por parte del sector público; la transición hacia el MSPI representa una oportunidad para consolidar a la UTDI como referente en la protección de datos dentro del sector judicial Colombiano.

Para el flujo de trabajo, la metodología se basó en la investigación, comparación y adaptación del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC) con el Sistema de Gestión de Seguridad de la Información (SGSI) establecido en las cuatro divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial y el cual está basado en la norma ISO/IEC 27001.

Mediante el desarrollo de una herramienta de identificación de GAPS o no cumplimiento de controles de la MSPI se identificará el estado actual de la identidad y se procederá con la propuesta del objetivo de control que se adoptará para el cumplimiento de la norma MSPI.

Al final del ejercicio se deberán identificar los GAPS, los cuales el equipo implementador determinara su aplicación de acuerdo el requerimiento de esfuerzo y proceso de implementación

Figura 1 Proceso de implementación Metodología MSPI



Nota: Figura relacionada a los procesos realizados por parte del grupo investigador del proyecto para la implementación de adaptación de la MSPI. Fuente: Propia

2. DESCRIPCIÓN DEL PROYECTO

2.1. Objetivo general

Diseñar una metodología para la adaptación y cumplimiento del Modelo de Seguridad y Privacidad de la Información – MSPI desarrollado por el Ministerio de Tecnologías de la información y las Comunicaciones – MINTIC dentro de las cuatro divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial y quienes cuentan con un SGSI según la norma ISO/IEC 27001.

2.2 Objetivos específicos

1. Investigar y evaluar el estado actual de la implementación de la política de seguridad del Sistema actual de la Gestión de Seguridad de la Información (SGSI) bajo la norma ISO/IEC 27001:2022 en las cuatro divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial

2. Investigar y evaluar mediante un diagnóstico, los posibles cumplimientos del Modelo de Seguridad y Privacidad de la Información – MSPI por parte de las cuatro divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial y basados en su modelo actual.

3. Identificar las diferencias o gaps entre las normas ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información – MSPI vigentes por parte del gobierno nacional y los cuales están establecidos en la guía desarrollada por el MINTIC.

4. Diseñar la metodología de acuerdo con la investigación de las prioridades dentro de las cuatro divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial que permitan una adaptación eficiente hacia el cumplimiento del Modelo de Seguridad y Privacidad de la Información – MSPI del gobierno nacional por parte del grupo implementador.

5. Desarrollar una herramienta tipo plantilla que registre los gaps, la metodología a desarrollar y los planes de acción dentro del proceso de adaptación y cumplimiento del Modelo de Seguridad y Privacidad de la Información – MSPI.

2.3 Metodología y Fases de desarrollo

La metodología se desarrolló en cinco fases: Investigación, diagnóstico, identificación, diseño y desarrollo.

Tabla 1 Fases Actividades y sus resultados

Análisis	**Resultado**
Fase 1. Investigación	
A1. Comparativo ISO27001:2013	Investigación y comparación entre las versiones de las normas ISO/IEC 27001:2013 y la

vs ISO27001:2022	ISO/IEC 27001:2022.
A2. Investigación de los controles de la normativa MSPI (administrativo, técnico y NIST).	Investigación, identificación y entendimiento de los diferentes controles distribuidos en los módulos del MSPI.
A3. Consolidación de Información	Se investiga el sistema de Gestión de Seguridad implementado en la UTDI para iniciar las actividades que lleven al cumplimiento de la norma MSPI.
Fase 2. Diseño de la metodología	
B1. Comparación de controles ISO/IEC 27001:2022 vs MSPI.	Identificación y diferencias de los controles entre la norma MSPI (administrativo, técnico y NIST) con la norma ISO/IEC 27001:2022.
B2. Investigación de objetivos de control	Investigación y asignación de objetivos de control para cada control distribuido en los módulos del MSPI.
Fase 3. Identificación de GAPs	
C1. Asignación de criterios	Asignación de criterios para cada control (ID, control, descripción y criticidad).
C2. Asignación de objetivos de control	Asignación de objetivos de control a control de la norma MSPI en sus diferentes módulos (administrativo, técnico y NIST).

C3. Implementación de la herramienta	Implementación y desarrollo de la herramienta de acuerdo con la investigación ejecutada y el levantamiento de información realizada.
Fase 4. Implementación de la metodología	
D1. Identificación de brechas de seguridad	Identificación de GAPs y/o brechas de seguridad de la UTDI por medio de la funcionalidad de la herramienta
Fase 5. Resultados	
E1. Herramienta Final de Seguimiento	Visualización del reporte generado por la herramienta con el análisis de los GAPs identificados para UTDI

Nota: Tabla donde se relacionan las actividades a ejecutar dentro de la metodología de implementación propuesta.

3. MARCO TEÓRICO Y TRABAJOS RELACIONADOS

En la actualidad las instituciones del sector público están optando por digitalizar su información y de esta forma ser más eficientes en su funcionamiento. El gobierno nacional colombiano a través de su Decreto 620 de 2020 enmarca la Política de Gobierno Digital sobre entidades que ejerzan funciones públicas administrativas y de esta manera establecer lineamientos sobre uso y operación de los servicios ciudadanos digitales.

La rama judicial con la finalidad de modernizar y mejorar los procesos judiciales mediante proyectos tecnológicos y el marco estratégico en el "Plan Estratégico de Transformación Digital 2021 – 2025" PETD, su principal función es facilitar la Transformación Digital de la Rama Judicial, con el fin de mejorar la eficiencia, la transparencia y la calidad del servicio ofrecido y dirigido a los colombianos.

Con el "Plan Estratégico de Transformación Digital", la Rama Judicial a través de la Unidad de Transformación Digital e Informática, busca impulsar el uso de la tecnología por medio de la integración de herramientas tecnológicas las cuales permitan la digitalización de procesos, como por ejemplo el "expediente electrónico", el desarrollo de plataformas digitales encaminadas al acceso de los ciudadanos y la mejora en la gestión de los trámites judiciales, enfocándose principalmente en áreas claves como en la innovación tecnológica, la seguridad de la información y la protección de datos.

De igual manera bajo el acuerdo PCSJA23-12130 del 29 de diciembre de 2023 en su artículo 4 del presente acuerdo "Modificación de la denominación de la Unidad de Informática. A partir del 2 de enero de 2024, la Unidad de Informática de la Dirección Ejecutiva de Administración Judicial, se denominará Unidad de Transformación Digital e Informática." [5] y el artículo 5 "Creación de divisiones en la Unidad de Transformación Digital e Informática: Crear, con carácter permanente, a partir del 2 de

enero de 2024, en la Unidad de Transformación Digital e Informática las siguientes divisiones:

- División de Servicios Tecnológicos.
- División de Desarrollo de Productos Digitales
- División de Estrategia y Arquitectura Digital.
- División de Proyectos de Gestión Judicial.
- División de Gestión de Datos.
- División de Seguridad y Protección de Datos,

Queda estructurado y establecido de manera permanente la creación de la "Unidad de Transformación Digital e Informática" y sus respectivas Divisiones de la UDTI, las cuales llevaran a cabo los proyectos encaminados a la Transformación Digital de la Rama Judicial.

Dentro de la UDTI se estableció como Sistema actual de la Gestión de Seguridad de la Información (SGSI) bajo la norma ISO/IEC 27001:2022 en las cuatro divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial,

La norma ISO/IEC 27001 Es una norma internacional desarrollada por ISO (organización internacional de normalización) con el propósito de ayudar a gestionar la seguridad de la información de una empresa. Establece requisitos para implementar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), ayudando a las organizaciones a gestionar la seguridad de todos sus activos habilitando la confidencialidad, la integridad y la disponibilidad de sus datos.

Sin embargo; el gobierno colombiano a través de su Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), a través del Modelo de Seguridad y Privacidad de la Información (MSPI), entregan directrices puntuales para que las entidades públicas alineen sus políticas de seguridad con estándares nacionales e internacionales.

Según el artículo "La importancia de la seguridad de la información en el sector público en Colombia", la estrategia de gobierno en línea emitido por el Ministerio de tecnología y la información, (... estableció los criterios generales para la ejecución del MSPI (Modelo de Seguridad y Privacidad de la Información), la guía metodológica de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de incidentes de seguridad lógica ...) [10].

La política de gobierno digital establecida por el Min TIC tiene como objetivo promover lineamientos, planes, programas y proyectos de las TIC en el uso del entorno digital, definiendo de manera detallada la implementación de controles de seguridad físicos y lógicos con la finalidad de asegurar los tramites, servicios, sistemas de la información, plataformas tecnológicas e infraestructura física y gestionando de manera eficaz y eficiente los activos de información, infraestructura crítica, los riesgos e incidentes de seguridad y privacidad de la información.

Dicho lo anterior, el Min TIC desarrolló el Modelo de Seguridad y Privacidad de la Información (MSPI), esta normativa está desarrollada sobre tres módulos y abarca un total de 181 controles distribuidos en cada uno:

1. Administrativo: 39 controles
2. Técnico: 72 controles
3. NIST: 70 controles

esto con el objetivo de guiar al sector público, en la implementación de la estrategia de seguridad digital. Este modelo busca formalizar un Sistema de Gestión de Seguridad

de la Información (SGSI) basado en el ciclo PHVA (Planear, Hacer, Verificar y Actuar) el cual incluye requisitos legales, técnicos y normativos. Consta de cinco fases que permiten a las entidades gestionar y proteger sus activos de información de manera adecuada:

Figura 2 Fases para implementar MSPI basado en el ciclo PHVA

Nota: Descripción de las fases para la implementación de MSPI. Fuente: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles162621_Modelo_de_Seguridad_y_Privacidad__MSPI.pdf

4 – DESARROLLO DEL PROYECTO

4.1. Generalidades

La seguridad de la información se ha convertido en el pilar principal y fundamental para el correcto funcionamiento de las instituciones tanto públicas como privadas. En Colombia, la gestión de la seguridad en el sector público presenta brechas significativas como lo es la madurez digital, las políticas implementadas de seguridad de la información y la capacidad de respuesta ante incidentes de seguridad de la información y ciberseguridad. De acuerdo al artículo 15 de la constitución política de Colombia que denota que "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar…" [1], se vuelve indispensable implementar metodologías, capacitaciones, marcos, programas normativos y estándares nacionales e internacionales vigentes, como lo es el Modelo de Seguridad y Privacidad de la Información – MSPI desarrollado por el Ministerio de Tecnologías de la información y las Comunicaciones – MINTIC y el cual esta alineado con directrices Colombianas como la Directiva 03 de 2021 Presidencia de la Republica y la Resolución Numero 00500 de Marzo 10 de 2021.

En el marco del fortalecimiento de la seguridad de la información en las entidades del sector público en Colombia, cuatro divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial se han propuesto adaptar su Sistema de Gestión de Seguridad de la Información (SGSI), el cual se encuentra basado en la norma ISO/IEC 27001:2022, hacia el Modelo de Seguridad y Privacidad de la Información (MSPI). Este mismo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

El Modelo de Seguridad y Privacidad de la Información (MSPI) es un marco normativo el cual busca unificar y estandarizar la gestión de la seguridad de la información en las entidades públicas, esto con la finalidad de garantizar un enfoque integral

que logre incluir aspectos administrativos, técnicos y operativos. Sin embargo, la ISO/IEC 27001:2022 presenta algunas diferencias estructurales con el MSPI, lo cual genera la necesidad de implementar una metodología de adaptación que permita la convergencia de ambos modelos sin comprometer la efectividad del SGSI actual.

4.2 Objetivo

El objetivo principal del proyecto es diseñar una metodología para la adaptación y cumplimiento del Modelo de Seguridad y Privacidad de la Información – (MSPI), desarrollado por el Ministerio de Tecnologías de la información y las Comunicaciones – (MINTIC), dentro de las cuatro divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial. Dicha metodología tiene como finalidad facilitar la adopción de la norma MSPI desde la política existente actualmente y que está basada en la norma ISO/IEC 27001:2022, permitiendo la alineación con las normativas colombianas.

Con la implementación de este proyecto se busca conocer los cambios y actualizaciones de las versiones de la norma ISO/IEC 27001 de la versión 2013 a la versión más reciente 2022. Evaluar el estado actual de las cuatro divisiones de la UTDI frente a los controles de la norma ISO/IEC 27001:2022 e identificar las brechas entre la norma ISO/IEC 27001:2022 y el MSPI contemplando sus diferentes módulos: administrativo, técnico y NIST. Posteriormente diseñar una estrategia de adaptación que permita cumplir con los principios enunciados en el MSPI sin afectar la operatividad del SGSI y finalmente implementar herramientas de seguimiento para medir la efectividad del proceso de adaptación.

4.3 Alcance

Actualmente las cuatro Divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial cuenta con un

SGSI según la norma ISO/IEC 27001, la cual, no se encuentra completamente alineada con las leyes establecidas por el gobierno colombiano para las entidades públicas territoriales. Por lo anterior el proyecto abarca la evaluación, diseño e implementación de una metodología para la adaptación de la norma de la ISO/IEC 27001:2022 a la norma del Modelo de Seguridad y Privacidad de la Información – (MSPI), esto enfocado en:

1. Análisis comparativo entre las versiones de las normas ISO/IEC 27001:2013 y la ISO/IEC 27001:2022
2. Evaluación de los módulos del MSPI: administrativo, técnico y NIST
3. Comparación de controles entre la norma ISO/IEC 27001:2022 y los módulos de la norma MSPI
4. Propuesta de un plan de acción para la implementación de controles adicionales requeridos por el MSPI
5. Desarrollo de una herramienta de seguimiento para monitorear el cumplimiento de los controles de seguridad en la UTDI

4.4 Ámbito de aplicación

Esta metodología de adaptación va enfocada al cumplimiento de la norma MPSI del Ministerio de Tecnologías de la información y las Comunicaciones – MINTIC por parte de las cuatro Divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial. Sin embargo, la herramienta desarrollada como fase final de este proyecto, puede ser aplicada a cualquier organización estatal para su evaluación y cumplimiento del MSPI.

4.5 Variables críticas para obtener un resultado

1. Tener el entendimiento de los controles aplicados dentro de la organización y de esta manera establecer cuáles son los GAPs frente a la MSPI.
2. Establecer los objetivos de control adecuados para la implementación de la MSPI y teniendo en cuenta el alcance y necesidades de la UTDI.

3. Tiempo y recursos necesarios por parte de la organización para la adopción y aplicación de controles con criticidad alta.

4.6 Criterios de desarrollo de la metodología de Adaptación

Este proyecto tiene como objetivo diseñar una metodología para lograr la adaptación y el cumplimiento del Modelo de Seguridad y Privacidad de la Información – (MSPI), el cual es desarrollado por el Ministerio de Tecnologías de la información y las Comunicaciones – (MINTIC), dentro de las cuatro divisiones de la Unidad de Transformación Digital e Informática (UTDI) de la Dirección Ejecutiva de Administración Judicial. Esta metodología mencionada tiene como finalidad efectuar la migración de la norma ISO/IEC 27001:2022 hacia el cumplimiento de la normativa del MSPI, garantizando la alineación con las normativas nacionales colombianas.

La norma ISO/IEC 27001 es una norma desarrollada por la Organización Internacional de Normalización (ISO) con el propósito de ayudar a gestionar la seguridad de la información de una empresa. Establece requisitos para implementar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), ayudando a las organizaciones a gestionar la seguridad de todos sus activos asegurando la confidencialidad, la integridad y la disponibilidad de sus datos.

5- ETAPAS

Este capítulo presenta un análisis comparativo entre la norma ISO/IEC 27001 en sus versiones 2013 y 2022, y los controles establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC. Se identifican las diferencias clave entre ambas normativas, evaluando la cobertura y equivalencias entre los módulos administrativos, técnicos y de ciberseguridad del MSPI frente a los 93 controles actualizados de la ISO/IEC 27001:2022. Asimismo, se realiza un análisis de brechas (gaps) en la implementación actual del SGSI de la UTDI y se establece una priorización para la adaptación y cumplimiento de los controles del MSPI.

5.1. Comparación de la versión de la norma ISO/IEC 27001 de 2013 a 2022

La norma ISO/IEC 27001 versión 2013 contaba anteriormente con 114 controles de seguridad de la información. La norma ISO/IEC 27001 versión 2022 presentó una actualización de 93 controles de seguridad de la información.

En esta última versión de la ISO 27001:2022 varios controles de la antigua versión 2013 se unieron, dejando como resultado un solo control en la version 2022.

Posteriormente los 93 controles de la versión 2013 están distribuidos en 4 categorías:

1. A.5 Controles organizativos (37 controles)
2. A.6 Controles de personas (8 controles)
3. A.7 Controles físicos (14 controles)
4. A.8 Controles tecnológicos (34 controles)

Adicionalmente se agregaron 11 controles nuevos:

1. A.5.7 Inteligencia de Amenazas
2. A.5.23 Seguridad de la Información para el Uso de Servicios en la Nube

3. A.5.30 Preparación para las TIC para la Continuidad de los Negocios
4. A.7.4 Monitoreo de Seguridad Física
5. A.8.9 Gestión de configuración
6. A.8.10 Eliminación de Información
7. A.8.11 Enmascaramiento de Datos
8. A.8.12 Prevención de Fugas de Datos
9. A.8.16 Actividades de seguimiento
10. A.8.23 Filtrado Web
11. A.8.28 Codificación Segura

Figura 3 Comparación número de controles versión 2013 y versión 2022

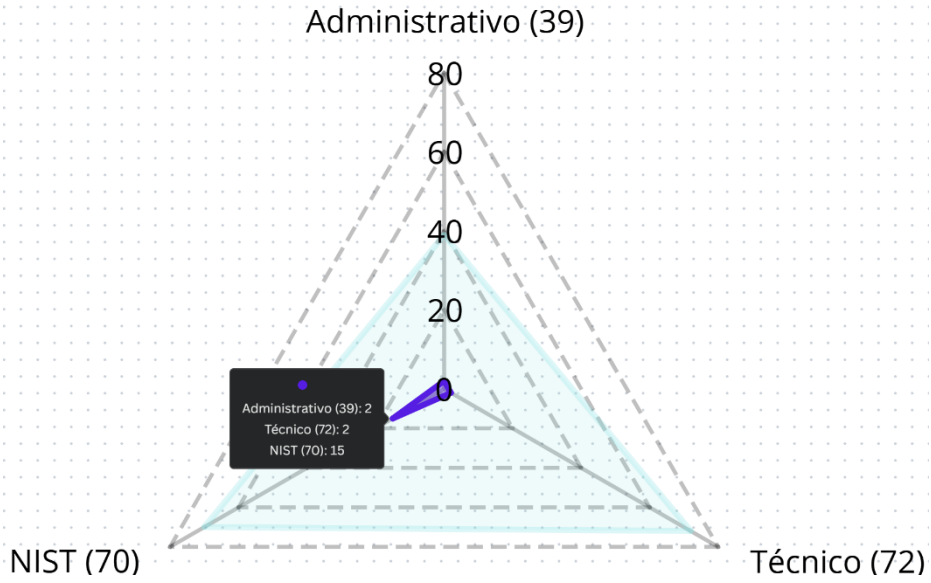
Nota: Comparación de versión de la ISO 27001:2013 y ISO 27001:2022 Fuente: https://sprinto.com/blog/iso-27001-2022/

Figura 4 Distribución de los 93 controles de la versión 2022

Nota: En la figura se define los 93 controles que se establecen en la ISO 27001:2022 Fuente: https://globaltrustassociation.org/es/sabes-cuales-son-las-mejoras-de-la-nueva-iso-270022022/

En la siguiente imagen se muestran únicamente los resultados finales de la UTDI después del assessment realizado, el cual por medio de un gráfico radial se evidencia el resultado de la comparación de los controles implementados y el estado actual en la UTDI Vs. los controles del MSPI. En este sentido se evidencian 19 controles que actualmente no están implementados en la UTDI, de los cuales hay 15 controles que corresponden al mapeo con la NIST y 4 controles que corresponden a la normativa ISO27001:2022, que de acuerdo con la certificación emitida por la UTDI delimitaron que los controles no aplicaban. Sin embargo, la UTDI no puede realizar excepciones a la norma, por tal motivo deben ser aplicados en su totalidad.

Figura 5 Imagen generada por canva



Nota: En la figura generada se plasman los 181 controles del MSPI y se observan los 19 controles que no tienen implementados la UTDI. Fuente: Propia

Los 19 controles están mapeados a la NIST como se observan en las siguientes tablas:

Tabla 2 Controles administrativos

Administrativo			
ID	Control	ID	NIST
AD.2.1.2	Separación de deberes / tareas	PR.AC-4	Se gestionan permisos y autorizaciones de acceso, incorporando los principios de menor privilegio y separación de deberes.
AD.4.3.3	Transferencia de medios físicos	PR.DS-3 PR.PT-2	Los activos se administran formalmente durante la eliminación, las transferencias y la disposición. Los medios extraíbles están protegidos y su uso restringido de acuerdo con la política

Nota: La tabla muestra el módulo administrativo con los 2 controles los cuales no tienen implementados la UTDI.

Tabla 3 Controles técnicos

Técnico			
ID	Control	ID	NIST
T.1.4.2	Procedimiento de ingreso seguro	PR.AC-1	Las identidades y credenciales se emiten, administran, verifican, revocan y auditan para dispositivos, usuarios y procesos autorizados.
T.5.2.3	Mensajería electrónica	PR.DS-2 PR.DS-5	Los datos en tránsito están protegidos. Se implementan protecciones contra fugas de datos

Nota: La tabla muestra el módulo técnico con los 2 controles los cuales no tienen implementados la UTDI.

Tabla 4 Módulo NIST

NIST	
ID	Control
DE.CM-5	Detección de código móvil no autorizado
ID.BE-4	Se establecen dependencias y funciones críticas para la prestación de servicios críticos.
PR.AT-2	Los usuarios privilegiados comprenden sus roles y responsabilidades.

PR.AT-3	Las partes interesadas externas (proveedores, clientes, socios) comprenden sus roles y responsabilidades.
PR.AT-4	Los ejecutivos senior comprenden sus roles y responsabilidades.
PR.AT-5	El personal de seguridad física y de la información comprende sus roles y responsabilidades.
PR.DS-1	Se protege la información en reposo.
PR.DS-5	Se implementan protecciones contra fugas de datos
PR.DS-6	Se utilizan mecanismos de verificación de integridad para verificar la integridad del software, el firmware y la información.
PR.IP-1	Se crea y mantiene una configuración base de sistemas de tecnología de la información/control industrial incorporando principios de seguridad (por ejemplo, el concepto de mínima funcionalidad)
PR.IP-11	La ciberseguridad se incluye en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección de personal)

PR.IP-2	Se implementa un Ciclo de Vida de Desarrollo de Sistemas para gestionar sistemas
PR.MA-1	El mantenimiento y reparación de los activos de la organización se realizan y registran, con herramientas aprobadas y controladas
PR.MA-2	El mantenimiento remoto de los activos de la organización se aprueba, registra y realiza de manera que se evite el acceso no autorizado.
PR.PT-3	El principio de menor funcionalidad se incorpora mediante la configuración de sistemas para proporcionar solo capacidades esenciales

Nota: La tabla muestra el módulo NIST con los 15 controles los cuales no tienen implementados la UTDI.

5.2. Identificación los diferentes controles del MSPI

Sobre la norma del Modelo de Seguridad y Privacidad de la Información – (MSPI) se realizó una identificación detallada de los controles definidos en el documento del MinTIC llamado: Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información.

En este instructivo se encuentra la herramienta: articles-482_Instrumento_Evaluacion_MSPI. Sobre este instructivo se analizaron los controles que se encuentran asignados a los módulos del MSPI:

1. Módulo de pruebas Administrativas (39 controles): Políticas, roles y cumplimiento normativo.
2. Módulo de ciberseguridad NIST (70 controles): Cifrado, seguridad en redes y protección contra malware.
3. Módulo de pruebas Técnicas (72 controles): Gestión de riesgos, control de accesos y monitoreo de eventos de seguridad)

Cada módulo tiene un grupo de controles asignados lo cuales conforman la totalidad de 181 controles del Modelo de Seguridad y Privacidad de la Información (MSPI).

5.3. Comparar el módulo de pruebas administrativas del MSPI con ISO/IEC 27001:2022

Los controles asignados al módulo de pruebas administrativas están orientados a los temas de seguridad de la información que no son directamente relacionados con las áreas tecnológicas de la organización. Este módulo cuenta con 39 controles distribuidos en temas de políticas de seguridad, recursos humanos, gestión de activos, continuidad del negocio, entre otros.

Cada uno de estos controles administrativos fueron analizados y comparados uno por uno contra los 93 controles de la norma ISO/IEC 27001 versión 2022, obteniendo como resultado 2 controles que sí se encuentran en la norma ISO/IEC 27001:2022:

Tabla 5 Gaps identificados en la comparación módulo de pruebas administrativas del MSPI con ISO/IEC 27001:2022.

ID MSPI	DESCRIPCION	ISO27001: 2022	CONTROL
AD.2.1.2	Separación de deberes / tareas	Si	5.3 – Segregación de deberes
AD.4.3.3	Transferencia de medios físicos	Si	7.10 – Almacenamiento de medios 7.11 – Seguridad del cableado 8.10 – Eliminación de información 8.11 – Enmascaramiento de datos

Nota: La tabla muestra los dos controles del MSPI que sí se encuentran en la norma ISO27001:2022.

5.4. Comparar el módulo de ciberseguridad NIST del MSPI con los controles de ISO/IEC 27001:2022

Los controles asignados al módulo de ciberseguridad NIST pretenden determinar cómo se encuentra la organización frente a las mejores prácticas del NIST basadas en ciberseguridad, esto con la finalidad de realizar un diagnóstico frente a los lineamientos de la política de ciberseguridad y ciberdefensa definidos en el documento Conpes 3701 y el Conpes 3854 y posteriormente mejorar la seguridad de la infraestructura crítica de la organización frente a los ciberataques.

El módulo cuenta con 70 controles distribuidos en temas de cifrado, seguridad en redes y protección contra malware. Cada uno de estos controles de la NIST fueron

analizados y comparados contra los 93 controles de la norma ISO/IEC 27001 versión 2022, en donde se encontraron 13 controles de la NIST que sí tienen equivalencia con los controles de la norma ISO/IEC 27001 versión 2022:

Tabla 6 Tabla comparativa módulo de ciberseguridad NIST del MSPI con los controles de ISO/IEC 27001:2022.

ID MSPI	DESCRIPCION	ISO27001: 2022	CONTROL
PR.AT-2	Los usuarios privilegiados comprenden sus roles y responsabilidades.	Si	6.3 Conciencia y formación 5.4 Responsabilidades de la dirección
PR.AT-3	Las partes interesadas externas (proveedores, clientes, socios) comprenden sus roles y responsabilidades.	Si	5.22 Gestión de servicios de proveedores 5.20 Contratos
PR.AT-4	Los ejecutivos senior comprenden sus roles y responsabilidades.	Si	5.4 Responsabilidades de la dirección
PR.AT-5	El personal de seguridad física y de la información comprende sus roles y responsabilidades.	Si	6.3 Conciencia y formación 7.1–7.4 Seguridad física

PR.DS-1	Se protege la información en reposo.	Si	8.24 Criptografía 8.6 Capacidad 8.10 Eliminación de información
PR.DS-5	Se implementan protecciones contra fugas de datos	Si	8.11 Prevención de fugas de datos
PR.DS-6	Verificación de integridad de software, firmware e información	Si	8.8 Gestión de vulnerabilidades 8.15 Registros, 8.6 Capacidad
PR.IP-1	Configuración base segura y mínima funcionalidad	Si	8.9 Gestión de configuración 8.6 Capacidad 8.32 Cambio
PR.IP-11	Seguridad en procesos de RR.HH. (selección, retiro)	Si	6.1–6.5 Gestión de recursos humanos 5.30 Continuidad TIC
PR.IP-2	Ciclo de vida seguro para sistemas	Si	8.25 Ciclo de vida de desarrollo seguro 8.27 Arquitectura segura

			8.32 Gestión de cambios
PR.MA-1	Mantenimiento controlado de activos con herramientas seguras	Si	7.13 Mantenimiento de equipos 7.9 Activos fuera de instalaciones
PR.MA-2	Mantenimiento remoto autorizado y registrado	Si	7.13 Mantenimiento 8.3 Restricción de acceso 8.5 Autenticación segura
PR.PT-3	Principio de mínima funcionalidad aplicado en sistemas	Si	8.9 Configuración 8.6 Capacidad 8.32 Gestión del cambio

Nota: La tabla muestra los 13 controles del MSPI que sí se encuentran en la norma ISO27001:2022.

5.5. Comparar el módulo de pruebas técnicas del MSPI con los controles de ISO/IEC 27001:2022

Los controles asignados al módulo de pruebas técnicas están orientados a los temas de gestión de riesgos, control de accesos y monitoreo de eventos de seguridad. Este módulo cuenta con 72 controles distribuidos en temas relaciones con el control de acceso, criptografía, seguridad física y del entorno, seguridad de las operaciones y entre otros.

Cada uno de estos controles de pruebas técnicas fueron analizados y comparados contra los 93 controles de la norma ISO/IEC 27001 versión 2022, en donde se encontraron 2 controles de las pruebas técnicas que sí tienen equivalencia con los controles de la norma ISO/IEC 27001 versión 2022:

Tabla 7 Tabla comparativa módulo de pruebas técnicas del MSPI con los controles de ISO/IEC 27001:2022

ID MSPI	DESCRIPCION	ISO27001: 2022	CONTROL
T.1.4.2	Procedimiento de ingreso seguro	Si	5.17 – Información de autenticación 5.16 – Gestión de identidades 5.18 – Derechos de acceso 8.5 – Autenticación segura
T.5.2.3	Mensajería electrónica	Si	8.11 – Prevención de fuga de datos 8.20 – Seguridad en redes 8.21 – Seguridad de los servicios de red 5.14 – Transferencia de información

Nota: La tabla muestra los 2 controles del MSPI que sí se encuentran en la norma ISO27001:2022.

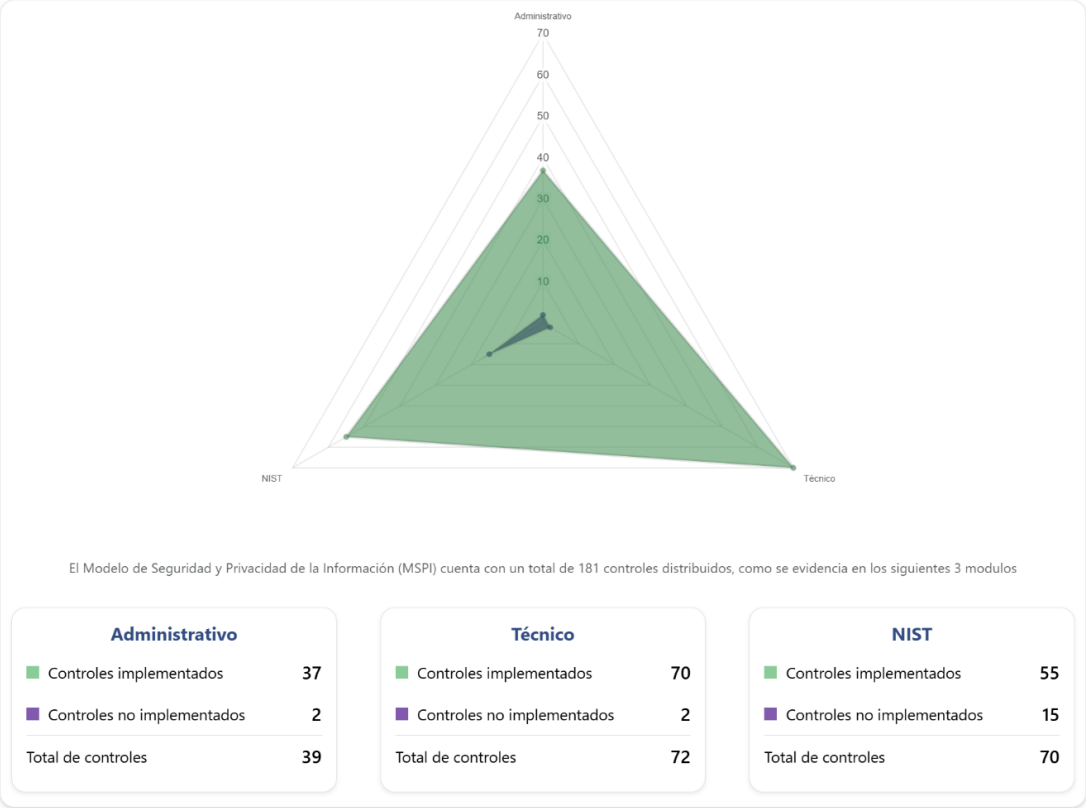
5.6. Análisis de Gaps Identificados entre el modelo actual implementado (ISO 27001 versión 2022) y el Modelo MSPI.

Durante el desarrollo de esta etapa de análisis de gaps/brechas entre ambas normativas y sus respectivos requerimientos, enfocado en las 4 divisiones de las cuatro

Divisiones de la Unidad de Transformación Digital e Informática (UTDI), se realizó un mapeo de controles donde se compararon los controles de seguridad de la norma ISO 27001 versión 2022 con los controles de los 3 módulos del MSPI (técnico, administrativo y NIST).

Utilizando nuestra herramienta diseñada para obtener resultados y facilitar la migración y/o adaptación al MSPI, se obtienen los siguientes resultados:

Figura 6 Figura con Gaps identificados con herramienta desarrollada



Nota: En la imagen se identifica un resumen grafico del complimiento de los controles. Fuente propia.

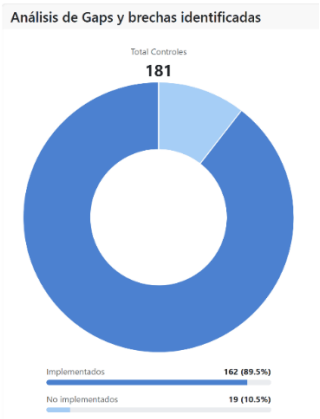
La imagen anterior muestra la herramienta que permite visualizar un resumen grafico por módulo en donde se identifica:

1. Controles implementados
2. Controles no implementados
3. Total, de controles

Figura 7 Porcentaje de cumplimiento de los controles establecidos por la MSPI

Nota: Imagen referente a porcentajes de cumplimiento de la MSPI entregado por la herramienta desarrollada. Fuente: propia

Figura 8 Análisis controles Implementados en la herramienta desarrollada



Nota: Figura que representa estadísticamente los controles implementados vs No implementados. Fuente: propia

La imagen anterior muestra gráficamente 181 controles los cuales son la totalidad de controles que contiene la normativa del MSPI en sus 3 módulos (técnico, administrativo y NIST), y muestra la totalidad de 19 controles no implementados, controles que están dentro del listado de la normativa del MSPI pero que no se encuentran enlistados en la normativa de la ISO 27001 versión 2022.

En resumen, para las 4 divisiones de la UTDI se evidencia un cumplimiento del 89.5 %, frente a un no cumplimiento del 10.5 %.

5.7. Priorización de Implementación de Gaps

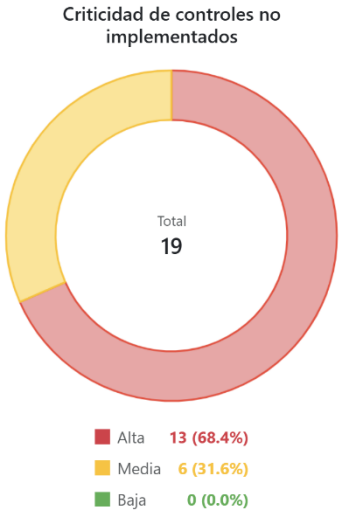
Durante la fase de categorización de la criticidad de los 181 controles de la normativa MSPI, se procedió a realizar sesiones de trabajo y socialización en conjunto con el área encargada de seguridad de la información.

Durante estas sesiones de trabajo se analizaron en detalle los 181 controles y dependiendo de la necesidad e impacto que tienen estos mismos en la entidad, se les asignó el nivel de criticidad correspondiente (alto, medio y bajo).

La priorización implementada fue realizada sobre la herramienta diseñada, en donde a cada control de los 181 controles de la normativa del MSPI, se le agregó por criterio el respectivo nivel de criticidad:

1. Alto
2. Medio
3. Bajo

Figura 9 Análisis de criticidad de controles implementados en la herramienta desarrollada



Nota: La figura muestra el porcentaje de controles no implementados por criticidad (alta, media, baja). Fuente: Propia.

La imagen anterior muestra la criticidad de los controles no implementados, en este caso 19 controles los cuales están categorizados de la siguiente manera:

1. Alta: 13 controles categorizados con criticidad alta, los cuales representan el 68,4% del total de controles no implementados
2. Media: 6 controles categorizados con criticidad media, los cuales representan el 31,6 % del total de controles no implementados
3. Baja: en este caso no se cuentan con controles categorizados con criticidad baja.

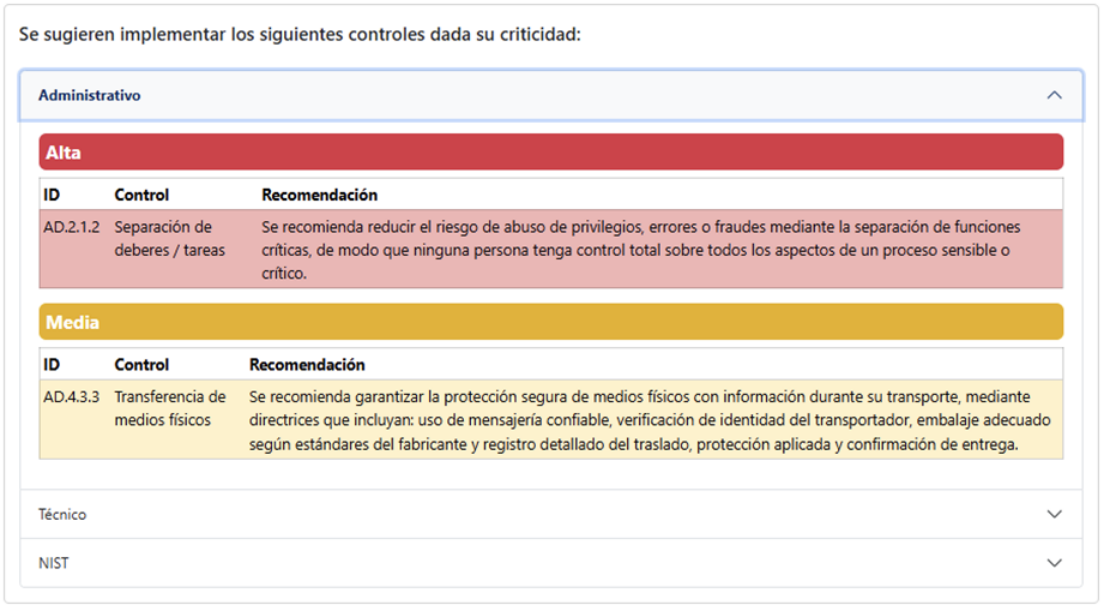
Posteriormente la herramienta fue diseñada para sugerir los objetivos de control y/o recomendaciones con base a cada control el cual no está implementado, por módulo.

6- OBJETIVOS DE CONTROL POR MODULO

Este capítulo presenta los objetivos de control sugeridos para la implementación de los controles del Modelo de Seguridad y Privacidad de la Información (MSPI), agrupados en los módulos Administrativo, Técnico y NIST, con base en las brechas identificadas previamente. A través de una herramienta desarrollada, se priorizó la implementación de estos controles según su nivel de criticidad, considerando factores como tiempo, costo y capacidades del equipo. Las brechas de alta criticidad requieren una atención inmediata, mientras que las de impacto medio o bajo se programan en plazos más amplios, siguiendo un cronograma estratégico de implementación.

6.1. Modulo Administrativo

Tabla 8 Objetivos de control sugeridos para implementación de controles administrativos en la herramienta desarrollada.



Se sugieren implementar los siguientes controles dada su criticidad:

Administrativo

Alta

ID	Control	Recomendación
AD.2.1.2	Separación de deberes / tareas	Se recomienda reducir el riesgo de abuso de privilegios, errores o fraudes mediante la separación de funciones críticas, de modo que ninguna persona tenga control total sobre todos los aspectos de un proceso sensible o crítico.

Media

ID	Control	Recomendación
AD.4.3.3	Transferencia de medios físicos	Se recomienda garantizar la protección segura de medios físicos con información durante su transporte, mediante directrices que incluyan: uso de mensajería confiable, verificación de identidad del transportador, embalaje adecuado según estándares del fabricante y registro detallado del traslado, protección aplicada y confirmación de entrega.

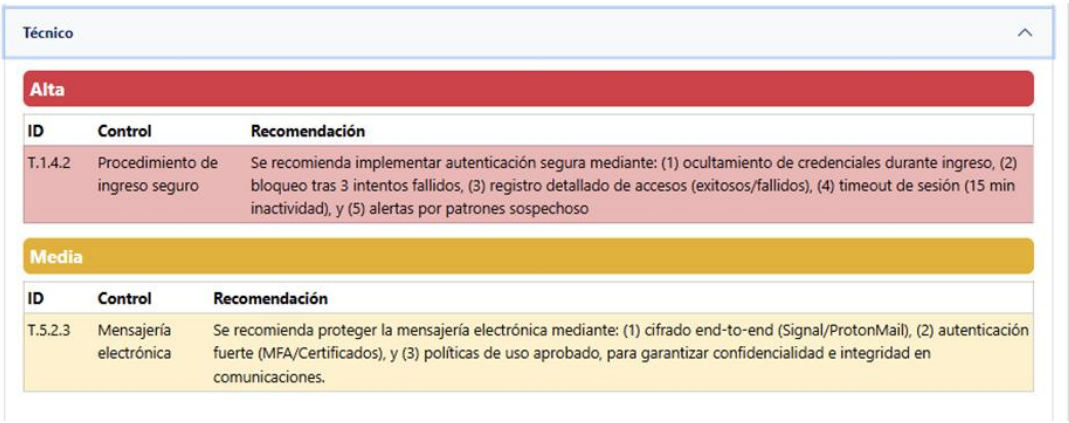
Técnico

NIST

Nota: La tabla muestra los objetivos de control sugeridos para el cumplimiento de los controles administrativos de la MSPI. Fuente: Propia

6.2. Modulo técnico

Tabla 9 Objetivos de control sugeridos para implementación de controles técnicos en la herramienta desarrollada



Técnico

Alta

ID	Control	Recomendación
T.1.4.2	Procedimiento de ingreso seguro	Se recomienda implementar autenticación segura mediante: (1) ocultamiento de credenciales durante ingreso, (2) bloqueo tras 3 intentos fallidos, (3) registro detallado de accesos (exitosos/fallidos), (4) timeout de sesión (15 min inactividad), y (5) alertas por patrones sospechoso

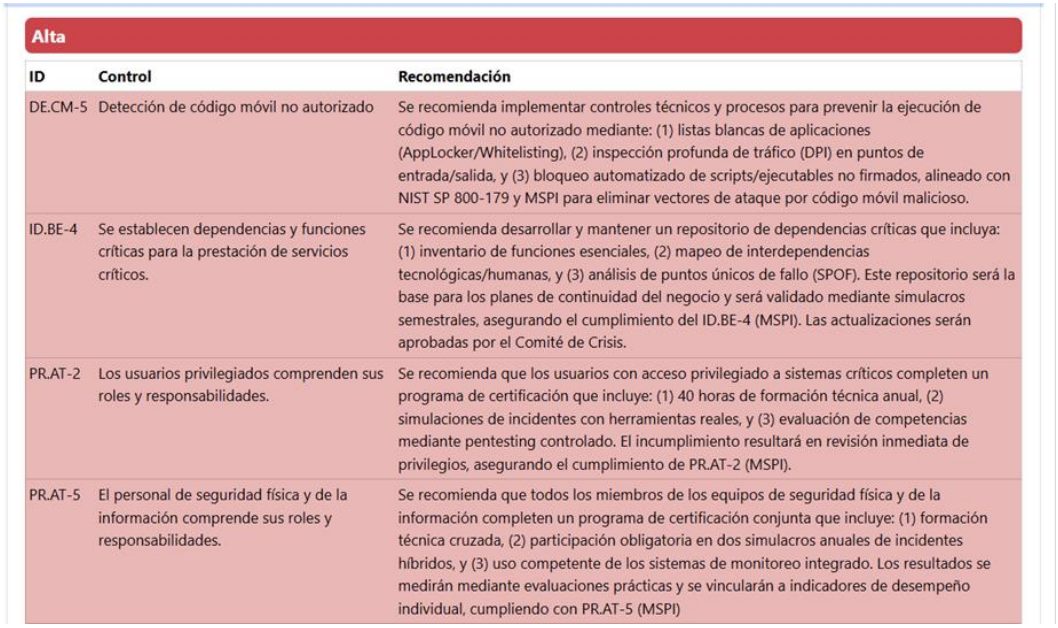
Media

ID	Control	Recomendación
T.5.2.3	Mensajería electrónica	Se recomienda proteger la mensajería electrónica mediante: (1) cifrado end-to-end (Signal/ProtonMail), (2) autenticación fuerte (MFA/Certificados), y (3) políticas de uso aprobado, para garantizar confidencialidad e integridad en comunicaciones.

Nota: El cuadro da una muestra los objetivos de control sugeridos para el cumplimiento de los controles técnicos de la MSPI. Fuente: Propia.

6.3. Módulo NIST

Tabla 10 Objetivos de control sugeridos para implementación de controles NIST en la herramienta desarrollada



Alta

ID	Control	Recomendación
DE.CM-5	Detección de código móvil no autorizado	Se recomienda implementar controles técnicos y procesos para prevenir la ejecución de código móvil no autorizado mediante: (1) listas blancas de aplicaciones (AppLocker/Whitelisting), (2) inspección profunda de tráfico (DPI) en puntos de entrada/salida, y (3) bloqueo automatizado de scripts/ejecutables no firmados, alineado con NIST SP 800-179 y MSPI para eliminar vectores de ataque por código móvil malicioso.
ID.BE-4	Se establecen dependencias y funciones críticas para la prestación de servicios críticos.	Se recomienda desarrollar y mantener un repositorio de dependencias críticas que incluya: (1) inventario de funciones esenciales, (2) mapeo de interdependencias tecnológicas/humanas, y (3) análisis de puntos únicos de fallo (SPOF). Este repositorio será la base para los planes de continuidad del negocio y será validado mediante simulacros semestrales, asegurando el cumplimiento del ID.BE-4 (MSPI). Las actualizaciones serán aprobadas por el Comité de Crisis.
PR.AT-2	Los usuarios privilegiados comprenden sus roles y responsabilidades.	Se recomienda que los usuarios con acceso privilegiado a sistemas críticos completen un programa de certificación que incluye: (1) 40 horas de formación técnica anual, (2) simulaciones de incidentes con herramientas reales, y (3) evaluación de competencias mediante pentesting controlado. El incumplimiento resultará en revisión inmediata de privilegios, asegurando el cumplimiento de PR.AT-2 (MSPI).
PR.AT-5	El personal de seguridad física y de la información comprende sus roles y responsabilidades.	Se recomienda que todos los miembros de los equipos de seguridad física y de la información completen un programa de certificación conjunta que incluye: (1) formación técnica cruzada, (2) participación obligatoria en dos simulacros anuales de incidentes híbridos, y (3) uso competente de los sistemas de monitoreo integrado. Los resultados se medirán mediante evaluaciones prácticas y se vincularán a indicadores de desempeño individual, cumpliendo con PR.AT-5 (MSPI)

PR.DS-1	Se protege la información en reposo.	Se recomienda implementar y mantener medidas técnicas y administrativas que garanticen la protección de la información en reposo, asegurando su confidencialidad, integridad y disponibilidad, mediante el uso de cifrado robusto, controles de acceso adecuados y políticas de clasificación de datos. Componentes claves: (1) Cifrado de Datos en Reposo, (2) Controles de Acceso Basados en Roles (RBAC), (3) Clasificación y Etiquetado de Información, (4) Monitoreo y Auditoría y (5) Políticas y Procedimientos Documentados
PR.DS-5	Se implementan protecciones contra fugas de datos	Se recomienda que la organización implemente controles DLP que incluyen: (1) monitoreo continuo de canales de transferencia, (2) enmascaramiento obligatorio de datos sensibles en entornos no productivos, y (3) aprobación explícita mediante flujos de trabajo documentados para cualquier excepción. Estos controles serán validados mediante auditorías trimestrales que verifiquen el cumplimiento de PR.DS-5 (MSPI), con reportes directos al comité de riesgos.
PR.DS-6	Se utilizan mecanismos de verificación de integridad para verificar la integridad del software, el firmware y la información.	Se recomienda que todos los activos digitales críticos sean protegidos mediante: (1) generación de hashes SHA-384 durante su estado conocido como bueno, (2) verificación automática antes de ejecución/uso, y (3) registro inmutable de resultados. Cualquier alteración no autorizada activará protocolos de contención inmediata, cumpliendo con PR.DS-6 (MSPI). Los reportes de integridad se generarán mensualmente para el comité de seguridad.
PR.IP-1	Se crea y mantiene una configuración base de sistemas de tecnología de la información/control industrial incorporando principios de seguridad (por ejemplo, el concepto de mínima funcionalidad)	Se recomienda que todos los sistemas operativos y dispositivos de red implementen configuraciones base alineadas con la compañía, incluyendo: (1) eliminación de cuentas/default passwords, (2) desactivación de servicios no esenciales, y (3) parámetros de hardening comprobados. Estas configuraciones serán validadas mediante scans automatizados semanales y auditorías manuales trimestrales, cumpliendo con PR.IP-1 (MSPI). Las excepciones requerirán justificación técnica y aprobación del CISO.
PR.IP-2	Se implementa un Ciclo de Vida de Desarrollo de Sistemas para gestionar sistemas	Se recomienda que todos los desarrollos de software sigan un SDLC seguro que requiere: (1) modelado de amenazas para proyectos nuevos, (2) revisiones de código automatizadas en cada commit, y (3) pruebas de penetración antes del despliegue en producción. Los equipos deberán remediar todas las vulnerabilidades de alta/crítica antes del despliegue, cumpliendo con PR.IP-2 (MSPI). Excepciones requerirán aprobación por el Comité de Seguridad con compensación de controles.

PR.MA-2	El mantenimiento remoto de los activos de la organización se aprueba, registra y realiza de manera que se evite el acceso no autorizado.	Se recomienda que todo mantenimiento remoto requiera: (1) solicitud electrónica aprobada por el dueño del activo, (2) autenticación multifactorial con certificado digital, y (3) grabación íntegra de sesiones almacenada por 90 días. Las conexiones se establecerán exclusivamente a través de servidores bastión con cifrado AES-256, cumpliendo con PR.MA-2 (MSPI). Accesos no autorizados activarán respuestas automáticas de bloqueo.
PR.PT-3	El principio de menor funcionalidad se incorpora mediante la configuración de sistemas para proporcionar solo capacidades esenciales.	Se recomienda que todos los sistemas en producción implementen configuraciones que: (1) eliminen servicios/protocolos innecesarios, (2) restrinjan privilegios al mínimo operativo, y (3) apliquen benchmarks CIS/NIST. Estas configuraciones serán validadas mediante scans automatizados semanales y auditorías manuales trimestrales, cumpliendo con PR.PT-3 (MSPI). Excepciones requerirán aprobación técnica documentada.

Media

ID	Control	Recomendación
PR.AT-3	Las partes interesadas externas (proveedores, clientes, socios) comprenden sus roles y responsabilidades.	Se recomienda que todo tercero con acceso a sistemas o datos deberá: (1) completar el programa de capacitación en seguridad antes del inicio operativo, (2) aceptar cláusulas de confidencialidad mediante firma digital, y (3) someterse a evaluaciones trimestrales de cumplimiento. El incumplimiento dará lugar a la terminación inmediata del contrato, conforme a PR.AT-3 (MSPI). Los acuerdos incluirán derecho a auditorías sorpresa.
PR.AT-4	Los ejecutivos senior comprenden sus roles y responsabilidades.	Se recomienda a la alta dirección participar en un programa de gobierno que incluya: (1) sesiones trimestrales con el CISO para revisar exposiciones clave, (2) ejercicios prácticos de toma de decisiones bajo crisis, y (3) firma electrónica de compromisos anuales de seguridad. Los resultados se reflejarán en el plan estratégico corporativo, cumpliendo con PR.AT-4 (MSPI). El CEO certificará anualmente el cumplimiento ante el consejo directivo.
PR.IP-11	La ciberseguridad se incluye en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección de personal)	Se recomienda que el departamento de RH coordine con el área de Seguridad de la Información: (1) incluir evaluaciones técnicas en procesos de selección para roles críticos, (2) garantizar la capacitación obligatoria en seguridad antes de otorgar accesos, y (3) automatizar la revocación de credenciales al terminar la relación laboral. Estos procesos serán auditados trimestralmente mediante muestreos aleatorios y cumpliendo con PR.IP-11 (MSPI). Las no conformidades generarán planes de acción con plazos máximos de 72 horas.
PR.MA-1	El mantenimiento y reparación de los activos de la organización se realizan y registran, con herramientas aprobadas y controladas	Se recomienda que todas las actividades de mantenimiento sobre activos tecnológicos requieran: (1) solicitud autorizada mediante flujo de trabajo electrónico, (2) uso exclusivo de herramientas del inventario controlado, y (3) registro inmutable de acciones realizadas. Los técnicos externos deberán firmar acuerdos de confidencialidad y ser supervisados por personal interno, cumpliendo con PR.MA-1 (MSPI). Las desviaciones generarán investigaciones disciplinarias.

Nota: El cuadro da una muestra los objetivos de control sugeridos para el cumplimiento de los controles NIST de la MSPI. Fuente: Propia.

Las imágenes anteriores muestran las recomendaciones (objetivos de control) por cada módulo y control que no está implementado y con su respectiva criticidad.

La priorización de implementación de las brechas identificadas y analizadas mediante la presente metodología busca optimizar el cumplimiento del modelo de Seguridad y Privacidad de la información (MSPI) pero para ello se basa en criterios de esfuerzo como lo son el tiempo, costo y la capacidad que debe tener los equipos involucrados en su implementación. También se debe tener en cuenta los objetivos planteados por la Unidad de Transformación Digital (UTDI) y de esta manera determinar su desarrollo.

Las brechas identificadas como sensibles o de criticidad alta- critica son de implementación inmediata, las de impacto medio-bajo su se programan para ser implementadas en tiempos más amplios. Para su ejecución se da un cronograma de apoyo para que sea base de una ejecución efectiva y generada por la presente metodología.

7- APLICACIÓN Y PRUEBAS

El presente proyecto queda bajo potestad de las cuatro Divisiones de la Unidad de Transformación Digital e Informática (UTDI) para dar cumplimiento a lo establecido en la MSPI.

La aplicación de la herramienta desarrollada se implementó para el presente proyecto de grado y el cual dio las respectivas pruebas e implementación de funcionamiento.

La herramienta cuenta con un acceso público a través del sitio WEB *https://metodo-tau.vercel.app/* donde se puede realizar la respectiva interacción para identificación de GAPs y su respectiva reportería de estadísticas para análisis.

8- RECOMENDACIONES PARA FUTURAS INVESTIGACIONES

El desarrollo del presente proyecto de implementación del modelo MSPI se dio para llevar a cabo un estado de cumplimiento de las cuatro Divisiones de la Unidad de Transformación Digital e Informática (UTDI); sin embargo, se establece que esta metodología y la herramienta desarrollada puede ser utilizada por otros estamentos del estado que requieran el cumplimiento del modelo MSPI.

Esta metodología puede ser tomada para futuras investigaciones e integraciones que lleven la línea de implementación de normas.

Para futuras investigaciones la herramienta desarrollada puede ser personalizada por medio de parametrizaciones que le permita adaptarse a cualquier institución del sector público para la medición y priorización del cumplimiento de la MSPI.

9- CONCLUSIONES Y TRABAJO FUTURO

Este proyecto logró diseñar una metodología para adaptar el sistema de gestión de seguridad de la información de la UTDI, basado en ISO/IEC 27001:2022, al Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC. El análisis comparativo reveló que, aunque el 78.6% de los controles ya cumplían con ambos estándares, existía un 21.4% de brechas críticas que requerían atención inmediata, particularmente en gestión de incidentes, controles NIST y aspectos administrativos. Estos hallazgos resaltan la importancia de armonizar los marcos internacionales con las regulaciones locales para fortalecer la ciberseguridad en el sector público.

La implementación de la metodología propuesta, estructurada en cinco fases claras, demostró ser práctica y escalable. La herramienta de seguimiento desarrollada permitió priorizar las brechas según su criticidad y facilitó la transición hacia el cumplimiento del MSPI. Este proceso no solo garantiza el ajuste a normativas como la Directiva 03 de 2021 y la Resolución 00500 de 2021, sino que también mejora la protección de datos sensibles y optimiza la respuesta ante incidentes de seguridad, posicionando a la UTDI como referente en ciberseguridad.

Finalmente, este proyecto evidenció que la gestión del cambio y la capacitación continua son elementos clave para mantener la efectividad del SGSI adaptado. La adopción del MSPI representa un avance significativo en la transformación digital segura de la Rama Judicial, ofreciendo un modelo replicable para otras entidades públicas. Este esfuerzo no solo cumple con requisitos normativos, sino que también contribuye a construir un ecosistema más resiliente frente a las crecientes amenazas cibernéticas en Colombia.

10- ANEXOS

Anexo 1. Definiciones

- **Asobancaria:** Es una entidad gremial sin ánimo de lucro que representa al sector financiero de Colombia.
- **Ataque:** Cualquier tipo de actividad maliciosa que intente obtener acceso no autorizado a los servicios, recursos o información del sistema; comprometer la seguridad de la información o interrumpir, denegar o degradar los recursos del sistema de información.
- **Ciberespacio**: Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.
- **Riesgo Cibernético**: Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.
- **Ciberseguridad**: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.
- **COBIT:** Es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT abarcando los controles específicos de tecnología.
- **CSIRT (Computer Security Incident Response Team):** Equipo responsable del desarrollo de medidas preventivas y de respuesta ante incidentes informáticos.
- **Evento De Seguridad**: Ocurrencia de una situación que tiene posibles implicaciones de seguridad potenciales para el sistema, la información o su entorno y que puede requerir una acción adicional (monitorear, investigar o reaccionar).

- **Modelo de Seguridad y Privacidad de la Información MSPI:** Modelo generado por el MinTic (Ministerio de telecomunicaciones e información) que imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad.
- **Incibe:** Es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza

  digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.
- **Incidente De Seguridad**: Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.
- **Información En Reposo**: Datos guardados en dispositivos de almacenamiento persistente (por ejemplo, cintas, copias de seguridad externas, dispositivos móviles, discos duros, entre otros).
- **Información En Tránsito**: Información que fluye a través de la red pública, como Internet, y los datos que viajan en una red privada, como una red de área local (LAN) corporativa o empresarial.
- **Información En Uso**: Hace referencia a datos activos que se almacenan en un estado digital no persistente, típicamente en la memoria de acceso aleatorio (RAM), las memorias caché de la CPU o los registros de la CPU.
- **Infraestructura Tecnológica**: Es el conjunto de hardware y software sobre

el que se basan los diferentes servicios que la entidad necesita tener en funcionamiento para poder llevar a cabo toda su actividad en función de los objetivos del negocio.

- **ISO 27035:** Norma internacional que proporciona las mejores prácticas y directrices para llevar a cabo un plan de gestión de incidentes estratégico y prepararse para una respuesta a incidentes.
- **National Institute of Standards and Technology (NIST):** es un laboratorio de estándares de medición, una agencia no regulada que trabaja bajo el Departamento de Comercio de los Estados Unidos. La agencia tiene como objetivo mejorar la innovación y la competitividad a través del avance de la tecnología, los estándares y la ciencia de la medición, así como mejorar la calidad de vida y mejorar la seguridad financiera.
- **OEA**: Organización de Estados Americanos.
- **Resiliencia**: Es la capacidad de un mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que pudo estar sometido.
- **SANS:** Instituto que se dedica a brindar y validar habilidades prácticas en ciberseguridad.
- **Seguridad De La Información**: Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preserva

  la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad.
- **SIEM (Security Information and Event Management):** Sistema de información que proporciona análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones, dispositivos de seguridad y los elementos de red. Suelen ser sistemas de centralización de logs.
- **Sistema De Información:** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados para cubrir una

necesidad u objetivo.

- **SOC (Security Operation Center):** Unidad encargada de monitorear, evaluar y defender los sistemas de información empresarial (sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, escritorios y otros dispositivos).
- **Terceros Críticos**: Terceros con quien se vincula la entidad y que, de acuerdo con los parámetros establecidos por la propia entidad, pueden tener incidencia directa en la seguridad de su información.
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio.

REFERENCIAS

1] *Constitución Política de Colombia [C.P.] art. 15. Actualizada con los actos legislativos a 2015 - Edición especial para la Corte Constitucional. Pag.15* https://www.corteconstitucional.gov.co/inicio/constitucion%20politica%20de%20colombia%20-%202015.pdf

2] *La historia de la Rama Judicial en Colombia (2012) - Pag .25 -* https://www.asojudiciales.org/wp-content/uploads/2016/11/Historia-de-la-Rama-Judicial.pdf

3] *Rama judicial - Manual del Estado - Función pública. (s. f.).* https://www.funcionpublica.gov.co/eva/gestornormativo/manual-estado/rama-judicial.php

4] *Plan Sectorial de Desarrollo Rama Judicial 2023 – 2024 (2022) - Pag.6, Pag.7 -* https://colaboracion.dnp.gov.co/CDT/portalDNP/PND-2023/05022023_Plan-Sectorial-Rama-Judicial-2023-2026.pdf

5] *ACUERDO PCSJA23-12130 29 de diciembre de 2023 (2023) - Pag.1, Pag.8 -* https://actosadministrativos.ramajudicial.gov.co/GetFile.ashx?url=%7e%2fApp_Data%2fUpload%2fPCSJA23-12130.pdf

6] *NORMA ISO 27001 -* https://www.normaiso27001.es/

7] *¿Qué es el MSPI? - https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/#:~:text=El%20Modelo%20de%20Seguridad%20y,de%20vida%20de%20la%20seguridad*

8] *Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones - https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888*

9] *RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 2021 - https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf - Pag.1*

10] *Camargo, E. A. R., & Pinzón, M. A. R. (2022). (Pág. 91,94). La importancia de la seguridad de la información en el sector público en Colombia. RISTI - Revista Ibérica de Sistemas E Tecnologias de Informação, 46, 87–99.* https://doi.org/10.17013/risti.46.87-99

11] *Henao Pereira, J. P. (2023). Pág. 11. Diseño del Sistema de Gestión de Seguridad de la Información, basado en el - MSPI -, Dirección Territorial de Salud de Caldas (Universidad de Manizales & Facultad de Ciencias e Ingeniería).* https://ridum.umanizales.edu.co/bitstream/handle/20.500.12746/6983/Henao_Pereira_Juan_Pablo_2023.pdf?sequence=1&isAllowed=y

12] *Agencia Presidencial de Cooperación Internacional de Colombia. (2020). Decreto 620 del 2 de mayo de 2020. https://www.apccolombia.gov.co/normativa/decreto-620-del-2-de-mayo-de-2020*