Propuesta de un Modelo de Gestión de Seguridad y Privacidad de la Información para la Gobernación del Huila

Brayan Alexander Beleño García

Universidad EAN

Facultad de Ingeniería

Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Neiva, Colombia

2022

Propuesta de un Modelo de Gestión de Seguridad y Privacidad de la Información para la Gobernación del Huila

Brayan Alexander Beleño García

Trabajo de grado presentado como requisito para optar al título de:
Magister en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Director (a):
CARMEN ELIZABETH CHAPARRO MALAVER

Modalidad:
Trabajo Dirigido

Universidad EAN
Facultad de Ingeniería
Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos
Neiva, Colombia
2022

Nota de aceptación

_____

_____

_____

_____

_____

_____

Firma del jurado

_____

Firma del jurado

_____

Firma del director del trabajo de grado

Bogotá D.C. 22- 11 – 2022

Dedicado a mi papá Orlando, quien, con su ejemplo, sacrificio,
y nobleza, me enseñó como ser una gran persona,
un excelente profesional, y, sobre todo, un gran padre para mis hijas.
A mi mamá María del Carmen, quien, con su amor, entrega,
y atención, me ha apoyado en todas mis metas.
A mi esposa Carolina, por su paciencia, apoyo, y confianza
en mí, para lograr éste y otros objetivos personales.
A mis hijas, Sara Lucía y María Juliana, por dar color,
amor y alegría, en los momentos más difíciles de mi vida.

Brayan Alexander Beleño García

Agradecimientos

Gracias a Dios por la vida, la salud y la familia. Por los momentos de felicidad y alegría a lo largo de esta experiencia, que me han permitido aprender y crecer, a pesar de los obstáculos y las dificultades.

Gracias a mis padres, Orlando Beleño Pava, en la eternidad, y María del Carmen García Urango, quienes, con su amor, ejemplo, y apoyo incondicional, siempre han estado ahí cuando más los he necesitado, y sé que siempre lo estarán.

Gracias mi esposa Carolina Alarcón Jiménez y a mis hijas Sara Lucía y María Juliana, por su apoyo y comprensión, a pesar de los momentos de ausencia y desconexión familiar que se presentaron, en el camino a este objetivo.

Gracias a la profesora Dra. Carmen Elizabeth Chaparro Malaver, en su calidad de directora de proyecto, por su acompañamiento, conocimientos, experiencia, motivación, apoyo y atención, y sobre todo, porque además estuvo presente y atenta para guiar el desarrollo final de este proyecto, ante las dificultades que a nivel personal presenté en este último tiempo.

Gracias al profesor Dr. Edicson Jair Gil Acosta, quien, con su orientación, conocimientos y pedagogía, acompañó en primera instancia el desarrollo de este proyecto, encaminando la obtención de este importante logro.

Gracias a la Universidad EAN por abrirme las puertas en este proceso de aprendizaje y crecimiento, y cada uno de los docentes que, con su tutoría, experiencia, apoyo, e instrucción, aportaron para este objetivo profesional y, sobre todo personal.

Resumen

La adopción y mantenimiento de la gestión de seguridad de la información genera retos importantes para las organizaciones en la actualidad, puesto que requieren inversiones para garantizar la continuidad del negocio y la obtención de las metas y objetivos estratégicos, alineando políticas requeridas en materia de seguridad y privacidad de la información, que cumplan con los diferentes planes de tipo operativo, táctico y estratégico, y que, a partir del establecimiento, medición y seguimiento de indicadores de gestión, soporten la toma de decisiones de manera transversal en la organización.

Con base en lo anterior, el presente documento tiene como fin elaborar una propuesta de modelo de gestión de seguridad de la información para la Gobernación del Huila, bajo los lineamientos de la Estrategia de Gobierno Digital del Ministerio TIC, que permita disminuir amenazas y vulnerabilidades sobre los activos de TI de la entidad, teniendo en cuenta el bajo nivel de gestión de la seguridad de la información existente.

El proyecto a desarrollar será de tipo no experimental y aplicada, con enfoque cuantitativo, recopilando y analizando información a través de diferentes técnicas, lo que permitirá establecer el modelo acorde a las necesidades. Así mismo, la aplicación del modelo propuesto requiere la revisión de un marco teórico, que permita la identificación de posibles modelos de gestión de seguridad a adoptar, conocer el estado actual de la entidad desde el marco institucional, determinando un marco metodológico que después permita diagnosticar los activos de TI, sus vulnerabilidades, amenazas, posibles riesgos, y controles existentes, e identificarlos a partir de un censo aplicado a la población objetivo del presente proyecto de investigación.

Posteriormente, plantea el modelo de gestión de seguridad y privacidad de la información, ajustada al contexto, normatividad, legislación y necesidades organizacionales, y los diferentes planes de acción que se derivan de este modelo, estableciendo recursos, tiempos, roles, responsabilidades, e indicadores, que faciliten su inclusión en la cultura organizacional de la Gobernación del Huila.

Palabras clave: Activo, Control, Información, Modelo, Privacidad, Riesgo, Seguridad.

Abstract

Adoption and maintaining information security management generates significant challenges for organizations today, since they require investments to ensure business continuity and obtain the strategic goals and objectives, aligning policies required in terms of security and information privacy, which comply with the different operational, tactical, and strategic plans, and which, based on the establishment, measurement and monitoring of management indicators, support decision-making across the organization.

Based on the above, this document aims to develop a proposal for an information security management model for the Government of Huila, under the guidelines of the *Gobierno Digital* strategy of the ICT Ministry, which allows to reduce threats and vulnerabilities on the IT assets, taking into account the low level of information security management in the organization.

The project to be developed will be of a non-experimental and applied type, with a quantitative approach, collecting and analyzing information through different techniques, which will allow establishing the model according to the needs. Likewise, the application of the proposed model requires the review of a theoretical framework, which allows the identification of possible security management models to be adopted, knowing the current state of the entity from the institutional framework, determining a methodological framework that later allows diagnosing IT assets, their vulnerabilities, threats, possible risks, and existing controls, and identify them from a census applied to the target population of this research project.

Subsequently, the information security and privacy management model is proposed, adjusted to the context, regulations, legislation and organizational needs, and the different action plans that are derived from this model, establishing resources, times, roles, responsibilities, and indicators that facilitate their inclusion in the organizational culture of the Government of Huila.

Keywords: Asset, Control, Information, Model, Privacy, Risks, Security.

Tabla de contenido

Lista de figuras

Pág.

Lista de tablas

Pág.

Introducción

La información es el activo más importante de cualquier organización, ya que es la materia prima para proveer servicios y/o productos, y cumplir con las exigencias y expectativas de los clientes. Con los avances tecnológicos que se desarrollan a diario, las personas tienen diversas herramientas y dispositivos a su disposición, como celulares, portátiles, dispositivos inteligentes, entre otros, y requieren mayor velocidad y acceso a cualquier tipo de información, con el fin de aplicarlas y aprovecharlas en los diferentes aspectos de su diario vivir.

El inconveniente surge cuando con estos avances, también se desarrollan esfuerzos para conocer sus debilidades y las de las herramientas desarrolladas, y posteriormente acceder a la información de una persona u organización, con el objetivo de usarla de forma e intenciones diferentes a las inicialmente planteadas.

Para evitar al mínimo que se presenten estas situaciones, el concepto de seguridad se convierte en una herramienta que las personas, instituciones académicas, empresas, compañías, corporaciones, o cualquier tipo de organización, utilizan para adoptar y/o desarrollar lineamientos que propicien el uso responsable de la información y de las herramientas que disponen para acceder a ella, y evitar que sea usada para las situaciones antes descritas, logrando que la información que poseen o que les ha sido suministrada y confiada, sea destinada para los fines descritos y empleada de forma responsable. De esta forma, garantizan a sus clientes la calidad tanto de sus procesos, como de los productos y/o servicios que se ofrecen.

A nivel nacional, el Ministerio TIC ha establecido lineamientos para el establecimiento de planes y políticas relacionadas con seguridad de la información, a través de la Política de Gobierno Digital, la cual tiene como objetivo el uso y aprovechamiento de las tecnologías de la información y las comunicaciones por parte de entidades del orden público y privado, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital, y a través de su habilitador Seguridad y Privacidad de la Información, soporta el desarrollo de las líneas de acción de dicha Política, para cumplir con los

propósitos establecidos, garantizando el buen uso de los activos de información y la privacidad de los datos de las entidades estatales (Ministerio TIC, 2019, pág. 24).

Sin embargo, el nivel de respuesta de los entes territoriales ante la materialización de una amenaza que genere graves consecuencias a la operación, servicios y actividades estratégicas y misionales, es una incógnita por resolver, y según estadísticas mostradas por el Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional, se reportaron 19.298 eventos cibernéticos durante el año 2019, aumentando un 54% con respecto a 2018, y con el escenario generado a raíz de la pandemia ocasionada por el COVID-19, este número llegó hasta los 35.184, correspondientes a un incremento del 82% con relación al año 2019 (Centro Cibernético Policial, 2020).

Para el caso de la Gobernación del Huila, la dependencia de servicios tecnológicos sumada a la falta de modernización en TI, y de directrices relacionadas en la entidad, constituyen factores clave para la identificación de serios riesgos en materia de seguridad de la información de la entidad, que pueden afectar la prestación de sus servicios y ejecución de actividades de administración de los asuntos seccionales y la planificación y promoción del desarrollo económico y social de su territorio, y a partir de lo anterior es necesario determinar ¿cómo reducir amenazas y vulnerabilidades sobre los activos de TI que soportan los servicios tecnológicos de la Gobernación del Huila?.

De esta forma, el presente proyecto tiene como fin elaborar una propuesta de modelo de gestión de seguridad de la información para la Gobernación del Huila, que permita disminuir amenazas y vulnerabilidades sobre los activos de TI de la entidad, teniendo como justificación la necesidad de impulsar y fortalecer la gestión de seguridad y privacidad de la información de manera estratégica en la Administración Departamental, estableciendo lineamientos, políticas y directrices que apoyen y faciliten el desarrollo del gobierno corporativo, preserven la confidencialidad, la integridad y la disponibilidad de los activos y la información, y generen confianza, mejorando y optimizando la prestación de los servicios de la entidad a las partes interesadas en el Departamento del Huila.

Así mismo, el presente documento se encuentra estructurado en siete (7) grandes ítems, siendo el primero -*Referentes*- en el que se aborda la información previa al desarrollo del proyecto: antecedentes e identificación del problema en la entidad a intervenir, pregunta de investigación, justificación del desarrollo del proyecto y los objetivos

establecidos. En el segundo ítem -*Marco teórico*- se realiza la revisión y análisis de conceptos, investigaciones, normatividad y antecedentes en general, válidos para contextualizar la investigación.

El tercer ítem -*Marco Institucional*- permite identificar la entidad a intervenir, a partir de información general y estratégica actual, como la reseña histórica, misión, visión, facultades, estructura organizacional, mapa de procesos, sector al que pertenece, portafolio de servicios, categorización del departamento, y servicios tecnológicos. El cuarto ítem -*Diseño Metodológico*- abarca la definición de los diferentes aspectos de la metodología a aplicar para el análisis y resolución del problema de investigación, de acuerdo con el alcance planteado. Estos aspectos son: el tipo de investigación, técnicas de recolección de información, enfoque y diseño de la investigación, población y muestra.

El quinto ítem -*Diagnóstico Organizacional*- presenta el análisis y los resultados del diagnóstico de activos de seguridad de la información, hallazgos respecto a la evaluación de la norma ISO/IEC 27001: 2013, amenazas y vulnerabilidades de los activos identificados, así como la identificación, valoración y tratamiento de riesgos de seguridad de la información. El sexto ítem -*Modelo de Gestión de Seguridad y Privacidad de la Información*- presenta el diseño del modelo de gestión de seguridad y privacidad de la Información para la Gobernación del Huila, detallando sus características, estructura, procesos, actores, herramientas tecnológicas, planes de acción, e indicadores de gestión planteados.

Posteriormente, el último ítem -*Recomendaciones y Conclusiones*- presenta las recomendaciones sugeridas y conclusiones del proyecto, incluyendo beneficios y ventajas en su implementación, así como acciones de mejora a partir de los resultados de diagnósticos y hallazgos identificados.

1. Referentes

En este punto, se desarrollan las actividades previas al desarrollo del proyecto, identificando los objetivos y las situaciones que justifican la necesidad de proponer un modelo de gestión de seguridad y privacidad de la información para la Gobernación del Huila.

1.1. Identificación del problema

Los niveles mínimos de gestión de seguridad y privacidad de la información, en la Gobernación del Huila, para mantener las propiedades de seguridad de sus activos de TI, soportar sus servicios y procesos de TI, y apoyar las áreas y procesos que requieren de éstos, han incrementado la probabilidad y el impacto de riesgos de seguridad de la información, así como también la identificación de amenazas y vulnerabilidades asociados, que facilitan su materialización, y afectación en la disponibilidad y confiabilidad de los servicios y procesos dirigidos a los usuarios de la entidad.

1.2. Pregunta de investigación

De esta forma, se establece el siguiente interrogante para el desarrollo del proyecto: ¿Cómo es posible, a través del diseño de un modelo de gestión de seguridad y privacidad de la información, disminuir las amenazas y vulnerabilidades sobre los activos de TI de la Gobernación del Huila, y garantizar su confidencialidad, integridad y disponibilidad?

1.3. Objetivos

1.3.1. Objetivo general

Elaborar una propuesta de modelo de gestión de seguridad de la información para la Gobernación del Huila, bajo los lineamientos de la Estrategia de Gobierno Digital del Ministerio TIC, que permita disminuir amenazas y vulnerabilidades sobre los activos de TI de la entidad.

1.3.2. Objetivos específicos

- Realizar el diagnóstico de los activos de TI de la Gobernación del Huila, para determinar los dominios que serán evaluados de acuerdo con los lineamientos del Ministerio TIC y de la Norma ISO 27001.
- Realizar la valoración de riesgos de seguridad de la información en la Gobernación del Huila, que incluya el análisis de causas, probabilidad de ocurrencia, y el nivel de impacto.
- Diseñar el plan de tratamiento de riesgos de seguridad y privacidad de la información de la Gobernación del Huila.
- Diseñar el plan de seguridad y privacidad de la información de la Gobernación del Huila, que incluya la definición de las políticas y procedimientos de seguridad de la información a establecer en la entidad.
- Diseñar el plan de sensibilización de seguridad y privacidad de la Información de la Gobernación del Huila, que abarque la promoción de la cultura de seguridad entre los funcionarios, y los indicadores de cumplimiento que correspondan.

1.4. Justificación

El establecer un modelo de gestión de seguridad y privacidad de la información para la Gobernación del Huila, a través de procedimientos específicos que brinden seguridad a los activos de TI, permitirá mejorar el bajo nivel de madurez de gestión de seguridad y privacidad existente (26/100 puntos, según Instrumento de Evaluación del MinTIC), a través del establecimiento de controles y acciones que conllevan a la disminución de amenazas y vulnerabilidades de los activos de TI, y que a su vez, disminuyan las probabilidades e impactos por la materialización de posibles riesgos asociados. De esta forma, se obtendrán beneficios para el correcto funcionamiento de la entidad, como (Ministerio TIC, 2016, pág. 18):

- Conocer a fondo las vulnerabilidades, amenazas y riesgos existentes, a fin de mitigarlos eficientemente, permitiendo que los activos de TI de la entidad sean utilizados de manera segura, confiable, duradera y con menos fallas.
- Proteger la información y los sistemas de la entidad, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Promover la cultura de seguridad y privacidad de la información en cada uno de los funcionarios de la Gobernación del Huila.
- Hacer uso eficiente y seguro de los activos de TI, para garantizar la continuidad de la prestación de los servicios, con el fin de cumplir los planes, políticas y objetivos estratégicos de la entidad.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones – TIC.

Otras contribuciones esperadas del presente proyecto son las siguientes:

Mejoras en la calidad y eficiencia de servicios, y en la imagen institucional: este proyecto permitirá el diseño de lineamientos para la gestión de la seguridad y privacidad de la información y activos de TI de la Gobernación del Huila, que a causa de vulnerabilidades y amenazas existentes, corren riesgo de ataques y afectaciones, beneficiando así tanto a usuarios y clientes internos -en el desarrollo de actividades de tipo

estratégico, misional y de apoyo- como a usuarios y clientes externos de servicios de la entidad, ya que contarán con mayor confiabilidad y tiempo de disponibilidad, con menos interrupciones, mejorando la imagen corporativa de la Gobernación.

Consolidación de cultura organizacional orientada hacia la seguridad y privacidad de la información: el desarrollo de una cultura preventiva en materia de seguridad y privacidad de la información, que mantenga la confidencialidad, integridad, y disponibilidad de los activos de TI de la Gobernación del Huila, se favorecerá con este proyecto, con el fin de evitar la materialización de riesgos con impactos económicos en la organización, y disminuir la probabilidad de ocurrencia e impacto de eventos que afecten dichos activos. En caso de que ocurran, los lineamientos de seguridad establecidos serán la principal contribución de este proyecto, manteniendo las funcionalidades en la entidad, minimizando impactos y afectaciones en los activos y servicios de las áreas que dependen de TIC. Igualmente, estos lineamientos se organizarán en planes, para que usuarios y clientes prueben y gestionen su cumplimiento, y midan el nivel de avance según el cronograma de implementación que se establezca.

Cumplimiento de estándares nacionales e internacionales: El proyecto planteado contribuirá a establecer un sistema de gestión de seguridad y privacidad de la información, consolidando definiciones, normatividad, estándares e información relevante para el diseño de una propuesta adaptada a la Gobernación del Huila, y dando herramientas para el establecimiento nuevos modelos y sistemas de gestión de TI en la entidad.

Modelo regional en materia de seguridad y privacidad: Este diseño permitirá generar políticas, procedimientos y estrategias de seguridad y privacidad de la información replicables en entidades descentralizadas departamentales, y otras entidades territoriales y públicas como alcaldías municipales y entes de control. Así mismo, facilitará la identificación de elementos y aspectos comunes para su integración a otros sistemas de gestión institucional de la entidad.

2. Marco teórico

En este marco teórico, se revisan conceptos, estándares, marcos de referencia, lineamientos, y metodologías, relacionadas con la presente propuesta de anteproyecto. Inicialmente se aborda la seguridad y privacidad de la información, desde algunos de los diferentes estándares, lineamientos y marcos de referencia, tanto a nivel nacional, como a nivel internacional, y desde diferentes puntos de vista.

2.1. Seguridad de la Información

Técnicamente, la seguridad de la información indica la capacidad de una organización de asegurar que la información y sus activos tecnológicos se utilicen de acuerdo a lo establecido, controlando el acceso y modificaciones solo por parte de las personas autorizadas, y para los fines autorizados (SGSI, 2015).

Para ello, la seguridad de la información busca preservar y asegurar el cumplimiento de las características de la información (Universidad Distrital Francisco José de Caldas, s.f.), como sigue:

- *Confidencialidad*: acceso y custodia de la información y activos de información solo para el personal debidamente autorizado.
- *Integridad*: garantía de inalterabilidad y fidelidad de la información, registrando sus cambios y modificaciones
- *Disponibilidad*: disposición de información y activos de información cuando sea requerida y para fines específicos.

La Metodología de Gestión de Riesgos –MAGERIT- tiene en cuenta, para la valoración de los activos, dos características o dimensiones adicionales (PAE - Portal de Administración Electrónica, 2012):

- *Autenticidad*: garantía de identidad de una entidad y/o fuente de procedencia de información.

- *Trazabilidad:* seguimiento y atribución de acciones sobre información o activos de información a una persona.

2.2. Privacidad de la Información

La privacidad de la información, o protección de datos**,** indica la capacidad de determinar los datos disponibles en un sistema de información que pueden ser utilizados y compartidos con terceros (Rouse, 2014). Esta protección contribuye a preservar la intimidad de las personas que, a través de interacciones en internet, comparten información sobre sus actividades, gustos, preferencias, etc., y que organizaciones o servicios en internet pueden usar hasta para obtener lucro (Mendoza, 2017). El Ministerio de TIC define la privacidad de la información como el establecimiento de acciones o medidas requeridas para garantizar la protección de la información y los derechos a la intimidad y el buen nombre de las personas, así como también salvaguardar secretos profesionales, industriales, o información privilegiada de particulares en poder de entidades de orden público (Ministerio TIC, 2016, pág. 15).

2.3. Legislación en Seguridad y Privacidad de la Información

En nuestro país, se cuenta con diversas legislaciones en materia de seguridad y privacidad de la información, que sirven de referencias normativas para desarrollar estudios relacionados (ADALID, 2018), siendo los más destacados los siguientes:

- *Ley 1273 de 2009*: Ley de Delitos informáticos y la protección de la información y de los datos: En esta ley (Superintendencia de Industria y Comercio, 2009), “Por medio del 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”, se definen los delitos, penas y multas a imponer, sobre quienes atenten contra sistemas de información de una organización, entre los que se encuentran:

- *Atentados en contra de los atributos de la información*: Acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, siendo agravados si son relacionados con sistemas financieros, estatales, o fines terroristas.
- *Atentados informáticos*: Hurto por medios informáticos y semejantes, transferencia no consentida de archivos.

- *Ley 1712 de 2014*: Ley de Transparencia y del Derecho de Acceso a la Información Pública: Ley que permite establecer lineamientos de regulación para el acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, teniendo como principio el derecho de todo ciudadano al acceso a la información pública, que se encuentra bajo control de las entidades públicas, organismos de control, personas naturales o jurídicas que presten servicios y funciones públicas, partidos o movimientos políticos y grupos significativos de ciudadanos, entidades administradoras de fondos parafiscales, entre otras (Procuraduría General, 2014).

- *CONPES 3854 de 2016*: Política Nacional de Seguridad Digital: Es una actualización de las políticas de seguridad digital nacional, que incluyen la gestión de riesgos para abordar la seguridad digital, bajo cuatro principios fundamentales: *Salvaguardar los derechos humanos y los valores fundamentales, Adoptar un enfoque incluyente y colaborativo, Asegurar una responsabilidad compartida, y Adoptar un enfoque basado en la gestión de riesgos*; y cinco dimensiones estratégicas: *Gobernanza de la seguridad digital, Marco legal y regulatorio de la seguridad digital, Gestión sistemática y cíclica del riesgo de seguridad digital, Cultura ciudadana para la seguridad digital, Capacidades para la gestión del riesgo de seguridad digital*; dimensiones que determinan las estrategias para fortalecer las capacidades de las múltiples partes interesadas, identificando, gestionando, tratando y mitigando los riesgos de seguridad digital en sus actividades socioeconómicas (Departamento Nacional de Planeación, 2016).

2.4. Modelos de Gestión de Seguridad de la Información

La Gestión de Seguridad de la Información se enfoca en mantener los atributos de la información (confidencialidad, integridad, y disponibilidad) mediante la aplicación de un proceso de gestión del riesgo, que permita generar confianza entre los grupos de interés de una organización, sobre la gestión efectiva de los riesgos (ICONTEC, 2012). Además, permite a las organizaciones mantener el impacto y la probabilidad ocurrencia de incidentes de seguridad de la información dentro de niveles de riesgo aceptables, abordando de manera efectiva los requisitos establecidos por la empresa, e implementando soluciones permanentemente (ISACA, 2013), de manera documentada, sistemática, estructurada, repetible, eficiente y adaptada a las variaciones que se presenten en los riesgos, el entorno y las tecnologías (Mantilla Guerra, 2018), permitiendo a las organizaciones ciertos beneficios y ventajas como lo son:

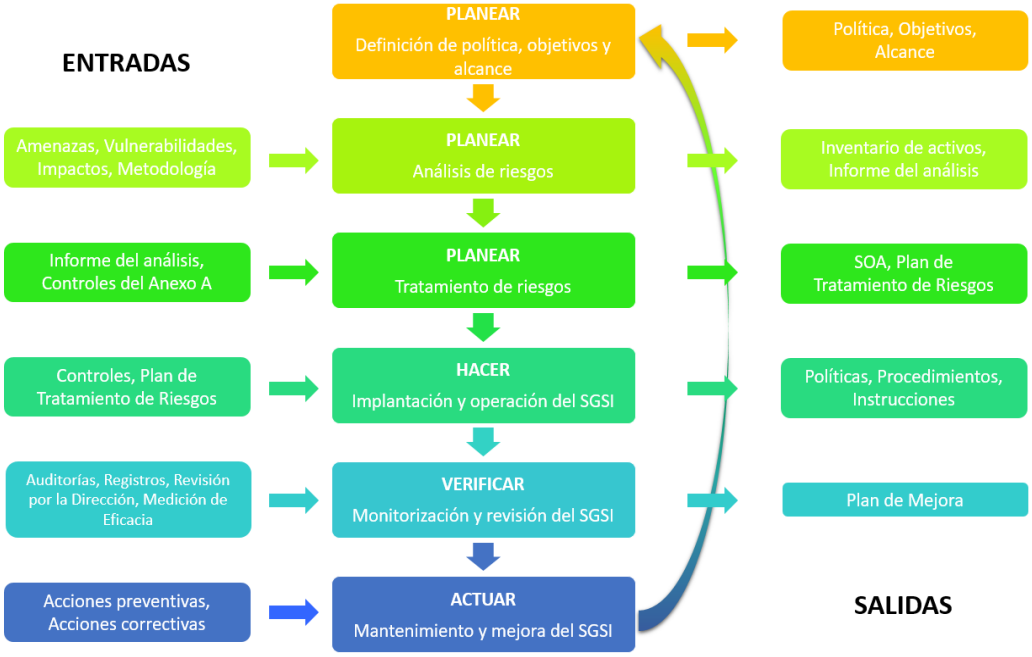
- Reducción de riesgos de seguridad de la información, y a su vez la probabilidad de ocurrencia y el impacto de incidentes de seguridad.
- Reduce las pérdidas para las organizaciones, permitiendo focalizar el gasto donde se produzcan mayores ventajas competitivas frente a la competencia.
- Incremento de la confianza y la credibilidad de la organización, por la garantía de calidad y confidencialidad comercial.

Por lo general, los sistemas de gestión de seguridad de la información, siguiendo el modelo del ciclo PHVA (Mantilla Guerra, 2018) como se muestra en la Figura 1, están compuestos por los siguientes pasos:

- *Planificar el SGSI,* analizando la situación de la empresa en materia de seguridad, estableciendo compromisos con la alta dirección para iniciar su ejecución, examinando información y sistemas estratégicos, y evaluando y tratando riesgos.
- *Implementar el SGSI,* mediante controles elegidos en la etapa de planeación. Se formula e implementa un plan de tratamiento de riesgos según vulnerabilidades y amenazas identificadas, y a posibles impactos de éstos.
- *Verificar el SGSI,* revisando procedimientos implementados, a través de exámenes periódicos para asegurar la eficacia de éste, la inspección de los niveles de riesgos aceptables y residuales, y las auditorías internas periódicas.

- *Mantener el SGSI,* desarrollando mejoras, acciones correctivas y preventivas, a partir de hallazgos identificados, y manteniendo comunicación con el personal de la empresa relevante para la gestión de la seguridad de la información.

Figura 1. Sistema de Gestión de Seguridad de la Información enmarcado en ciclo PHVA



Fuente: Norma ISO 27001:2013, Revista Espacios, (2018).
https://www.revistaespacios.com/a18v39n18/18391805.html#iden2

A continuación, se presentan algunos modelos de gestión de seguridad y privacidad de la información, con su descripción y sus características principales:

2.4.1. COBIT 5 – Proceso de Gestión APO13

El Marco COBIT propone el proceso "*APO13 - Gestionar la Seguridad*", mediante el cual propone una serie de buenas prácticas y actividades para definir, operar y supervisar un sistema para la gestión de la seguridad de la información en una organización, teniendo en cuenta el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de riesgo aceptados. Para esto se establecen las siguientes buenas prácticas (ISACA, 2013): Establecer y mantener un SGSI; Definir y gestionar plan de tratamiento de riesgos de seguridad de la información; y Supervisar y revisar el SGSI.

2.4.2. Modelo de Arquitectura de Seguridad de la Información - Jeimy Cano

El modelo propuesto por el profesor Jeimy Cano (Calvo Sánchez & Parada Serrano, 2010) establece tres elementos para la administración y gobierno de la seguridad de la información en las organizaciones: **estructuras, procesos y acuerdos**. La **estructura** está compuesta por la *información*, como activo del negocio a asegurar; las *estrategias* de negocio, base para alineación estratégica; los *fundamentos de seguridad informática*, para garantizar los requerimientos de seguridad de la información; y la *administración de riesgos*, implementando metodologías de análisis de riesgos para identificar vulnerabilidades de los sistemas de información (Ver Figura 2).

Como **procesos**, se incorpora la norma ISO27002 en los procesos de la organización, asimilando las directrices que allí se establecen, favoreciendo el uso adecuado de la información a nivel estratégico, táctico y operacional. En materia de **acuerdos**, se integra la seguridad de la información como proceso con las expectativas del negocio y de la alta dirección, alineándolos estratégicamente según las prioridades del negocio, competencias necesarias en seguridad de la información, compromiso de la alta dirección, inversión necesaria, roles y responsabilidades, entre otros aspectos.

Figura 2. Estructura de Modelo de Arquitectura de Seguridad de la Información propuesto por Jeimy Cano

Fuente: Calvo Sánchez & Parada Serrano: Metodología para la Implementación del Modelo de Arquitectura de Seguridad de la Información (MASI), (2010). https://repository.upb.edu.co/bitstream/handle/20.500.11912/1007/digital_19847.pdf?sequence=1

2.4.3. Modelo de Arquitectura de Seguridad de la Información – Jan Killmeyer

Este modelo propone cinco elementos: **organización de seguridad e infraestructura**, incorporando la seguridad de la información como apoyo y facilitador de las metas organizacionales; **políticas, estándares y procedimientos**, definiendo objetivos de seguridad de la información, directrices y procedimientos a nivel interno; **línea base de seguridad y valoración de riesgo**, verificando brechas sobre la infraestructura de TI existente para gestionar sus riesgos y establecer controles para su mitigación; **capacitación y entrenamiento de usuarios**, apoyando su entendimiento de la seguridad de la información para proteger la información e identificar posibles amenazas; y el **cumplimiento**, en el que se mide la eficacia de los objetivos de seguridad propuestos (Ver Figura 3).

Figura 3. Estructura de Modelo de Arquitectura de Seguridad de la Información propuesto por Jan Killmeyer

Fuente: Calvo Sánchez & Parada Serrano: Metodología para la Implementación del Modelo de Arquitectura de Seguridad de la Información (MASI), (2010). https://repository.upb.edu.co/bitstream/handle/20.500.11912/1007/digital_19847.pdf?sequence=1

2.4.4. Modelo de Seguridad y Privacidad de la Información - MinTIC

El Ministerio TIC, a través de su Modelo de Seguridad y Privacidad de la Información (2016, pág. 20), plantea el ciclo de operación para la gestión de la seguridad y privacidad de la información, en cinco fases que permiten la sostenibilidad del modelo dentro de las entidades, enfocándose en preservar la confidencialidad, integridad, y disponibilidad de sus activos de información, gestionando así la seguridad y privacidad de la información en la entidad (Ver Figura 4).

Cabe añadir que este modelo incluye dentro de su ciclo de operación, la gestión de la privacidad de la información, añadiendo a sus herramientas de diagnóstico, aspectos relacionados con la información y garantizando el cumplimiento de los lineamientos establecidos en la Ley de Transparencia (Ministerio TIC, 2016, pág. 21).

Figura 4. Ciclo de operación Modelo de Seguridad y Privacidad de la Información

Fuente: Modelo de Seguridad y Privacidad de la Información del Ministerio TIC, (2016, pág. 21). https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

- *Fase 1 - Diagnóstico*: Identificación del estado actual y el nivel de madurez, según requerimientos y necesidades de seguridad y privacidad de la información. Se evalúa el nivel de cumplimiento de la legislación y buenas prácticas asociadas, a través de revisión de documentación y controles existentes, reuniones con líderes y dueños de procesos, e identificación de amenazas y vulnerabilidades.

- *Fase 2 - Planificación*: Elaboración del plan de seguridad y privacidad de la información de la entidad, alineado con objetivos y metas estratégicas, y definiendo acciones para gestionar los riesgos asociados por cada proceso.
- *Fase 3 - Implementación*: Implementación de la fase de planificación del modelo de seguridad y privacidad de la información en la entidad, generando informes de ejecución del plan de tratamiento de riesgos de seguridad y privacidad de la información, y estableciendo indicadores de gestión relacionados:
- *Fase 4 - Evaluación de Desempeño*: Seguimiento y monitoreo del modelo de seguridad y privacidad de la información, con base en los resultados de los indicadores propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones establecidas e implementadas.
- *Fase 5 - Mejora Continua*: Consolidación de resultados obtenidos en la fase anterior, para diseñar el plan de mejoramiento de seguridad y privacidad de la información, que permita identificar y mitigar debilidades oportunamente, ajustando controles del modelo de seguridad, y la comunicación a grupos de interés, de resultados que incluya las actividades que fueron reformadas,

Debido a que, en su calidad de entidad pública, la Gobernación del Huila se encuentra obligada a implementar planes de seguridad y privacidad de la información, correspondiendo a uno de los tres habilitadores transversales que soportan el desarrollo de la Política de Gobierno Digital, y del Modelo Integral de Planeación y Gestión Institucional, se opta por utilizar el Modelo de Seguridad y Privacidad de la Información del Ministerio TIC, a fin de garantizar alineación y cumplimiento con lineamientos y legislación nacionales antes mencionados. Así mismo, la gestión de seguridad de la información planteada en este modelo, tiene como ventaja la fácil integración con los modelos de gestión de riesgos planteados para las entidades públicas en Colombia, al utilizar criterios similares para valorar la probabilidad, el impacto, y las consecuencias de los riesgos que se identifiquen.

Adicional a esto, es necesario revisar metodologías existentes para el diagnóstico y la gestión de activos de TI en las organizaciones, de modo que se escoja la opción que más se acople al Modelo de Seguridad y Privacidad de la Información del MinTIC, seleccionado para la gestión de seguridad y privacidad de la información en la Gobernación del Huila.

2.5. Metodologias de Gestión de Activos de TI

El análisis y valoración de activos de TI constituye un concepto clave para el desarrollo del diagnóstico de la organización, que para este caso es la Gobernación del Huila, a fin de determinar la criticidad y el valor de cada uno de los activos de la organización, asegurando que estén debidamente protegidos, y debidamente clasificados con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. Esta clasificación de activos de la entidad se basa en las características particulares de cada uno, y busca dar cumplimiento a los requerimientos estipulados en el ítem relacionado con la Gestión de Activos de los estándares 27001:2013, ISO 27002, e ISO 27005 (Ministerio TIC, 2016, pág. 16).

A continuación, se presentan algunos modelos de gestión de seguridad y privacidad de la información, con su descripción y sus características principales:

2.5.1. COBIT 5 – Proceso de Gestión BAI09

El Marco COBIT propone el proceso "*BAI09 - Gestionar los Activos*" (ISACA, 2013), para gestionar y asegurar el aporte de valor a la organización mediante el uso de los activos de TI, a un coste óptimo, manteniéndolos operativos y protegidos físicamente, para soportar los servicios. Como practicas base se incluyen: Identificar y registrar los activos vigentes, Gestionar los activos críticos, Gestionar el ciclo de vida de los activos, Optimizar el coste de los activos, y Gestionar licencias.

2.5.2. ITIL 4

El marco de trabajo ITIL versión 4 propone la "*Gestión de activos de TI*" como práctica de planificación y gestión del ciclo de vida de los activos de TI utilizados por las organizaciones para prestar servicios de TI internos y externos, analizando sus costos, riesgos, y soporte para la toma de decisiones (Freshservice Inc., s.f.). Como buenas prácticas incluye: Definir y mantener registro de activos de TI; Controlar el ciclo de vida de los activos de TI de manera conjunta con otras prácticas; Proporcionar datos, informes y soportes actuales e

históricos a otras prácticas sobre activos de TI; Auditar los activos, e impulsar mejoras correctivas y preventivas sobre los inconvenientes detectados (Interpolados, 2020).

2.5.3. Gestión y Clasificación de Activos de TI - Ministerio TIC

El Ministerio TIC, a través del Modelo de Seguridad y Privacidad de la Información, establece lineamientos que deben ser utilizados por los responsables de la seguridad de la información, para la gestión y clasificación de activos de TI de cada entidad, determinar qué activos posee, cómo deben ser utilizados, roles y responsabilidades de los funcionarios sobre éstos y, reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe dársele, de acuerdo al nivel de confidencialidad, integridad y disponibilidad de la información gestionada por la entidad, conforme lo indican las leyes 1712 de 2014, 1581 de 2012, y según las siguientes valoraciones de criticidad del activo en cada una de sus propiedades (Ministerio TIC, 2016, pág. 7):

- Valoraciones de criticidad según confidencialidad
  - *Información Pública Reservada*: Información que estando en custodia, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento del Artículo 19 de la Ley 1712 de 2014.
  - *Información Pública Clasificada*: Información que estando en custodia, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado.
  - *Información Pública*: Información que un sujeto obligado genere, obtenga, adquiera o controle.

- Valoraciones de criticidad según integridad
  - *Alta*: Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
  - *Media*: Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen moderadas de la entidad.

- *Baja*: Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
- *No Clasificada*: Activos de información que deben ser incluidos en el inventario, y que aún no han sido clasificados, deben ser tratados como activos de información de integridad alta.

- Valoraciones de criticidad según disponibilidad
  - *Alta*: La no disponibilidad de información conlleva un impacto negativo de tipo legal o económico, retrasar funciones, o generar pérdidas de imagen severas.
  - *Media*: La no disponibilidad de información conlleva un impacto negativo de tipo legal o económico, retrasar sus funciones, o generar pérdidas de imagen moderadas.
  - *Baja*: La no disponibilidad de información afecta la operación normal de la entidad o entes externos, sin implicaciones legales, económicas o de imagen.
  - *No Clasificada*: Activos de información que deben ser incluidos en el inventario, y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad alta.

Con base en el resultado de estas valoraciones, se indica el nivel de criticidad neta del activo, teniendo en cuenta la siguiente valoración (Ministerio TIC, 2016, pág. 13):

- *Alta*: Activos en los que la clasificación de la información en mínimo dos (2) de las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
- *Media*: Activos en los que la clasificación de la información en una (1) de sus propiedades es alta o en al menos una (1) de sus propiedades es media.
- *Baja*: Activos de información en los que la clasificación de la información en todas sus propiedades es baja.

A partir de la revisión anterior, y con el ánimo de mantener idoneidad y homogeneidad, se opta por utilizar los lineamientos de gestión y clasificación de activos de TI propuestos por el Ministerio TIC en su Modelo de Seguridad y Privacidad de la Información, alineándose con el desarrollo de la Política de Gobierno Digital, y del Modelo Integral de Planeación y Gestión Institucional.

2.6. Metodologías de Gestión de Riesgos de Seguridad de la Información

Posteriormente se procede a identificar, analizar y valorar las vulnerabilidades y amenazas que pueden llegar a afectar los activos de TI de la Gobernación del Huila, analizados previamente. Para esto, se deben identificar estándares y marcos de referencia que permitan realizar la gestión de riesgos de TI, y que incluyan inicialmente identificación, análisis y valoración de vulnerabilidades y amenazas, de modo que dicha gestión sea más precisa y enfocada sobre el diagnóstico realizado a los activos de la entidad, que sobre el cumplimiento de lineamientos y estándares.

Las vulnerabilidades son el conjunto de debilidades de los activos de TI, que pueden ser explotadas por una o más amenazas (Ministerio TIC, 2016, pág. 16).. Las amenazas son las causas potenciales de incidentes no deseados que tienen afectaciones sobre las operaciones y servicios de un sistema o una organización (Ministerio TIC, 2016, pág. 11). Pueden ser naturales o humanas, y accidentales o intencionales, y uno de los objetivos de la gestión de riesgos es precisamente identificar y valorar vulnerabilidades y amenazas sobre los activos de TI, como causantes de materialización de riesgos (Ministerio TIC, 2016, pág. 19).

Ahora, una vez valoradas las vulnerabilidades y amenazas, es necesario puntualizar que los riesgos de seguridad de la información corresponden al potencial o la posibilidad de que una amenaza dada pueda explotar una vulnerabilidad, a fin de causar pérdidas o daños sobre uno o más activos de TI, en la organización (Ministerio TIC, 2016, pág. 16). Sobre este aspecto, existen estándares -como el ISO 31000, ISO 27005 y COBIT 5- y metodologías -como OCTAVE, MAGERIT, y COSO- que permiten gestionarlos de manera efectiva.

2.6.1. ISO 31000

El estándar ISO 31000 – Gestión del Riesgo- provee un marco de referencia para que las organizaciones diseñen, implementen, monitoreen, revisen y mejoren continuamente la gestión del riesgo, teniendo en cuenta principios que garantizan la eficacia del mismo, como lo son la creación y protección del valor, integración de procesos, toma de

decisiones, disponibilidad de información, adaptación, factores humanos y culturales, transparencia e inclusión, dinamismo, y orientación a la mejora continua, entre otros (ISO, 2018).

El proceso que establece ISO 31000 para la gestión de riesgos se resume en la Figura 5, en donde se observa como elemento inicial efectuar comunicación y consulta con todos los interesados dentro y fuera de la organización. Una vez establecido estos planes y/o procedimientos, se establecen los contextos, tanto internos como externos, para alinear los objetivos de la gestión de riesgo, y a su vez los objetivos de la organización. Posteriormente se realiza valoración de riesgos, mediante identificación, análisis y evaluación, y una vez finalizada esta fase, se definen los tratamientos a aplicar.

Figura 5. Proceso para gestión de riesgo

Fuente: ISO31000:2018 Gestión del riesgo - Directrices, 6. Proceso de Gestión del Riesgo (2018) - https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:es

Por último, se realiza monitoreo y revisión del proceso de gestión del riesgo, verificando controles aplicados, obteniendo información adicional para la valoración de riesgos, detectando cambios de contexto, e identificando riesgos emergentes, entre otros aspectos. Ahora, debido a que ISO 31000 no ofrece recomendaciones o procedimientos específicos sobre tratamiento de riesgos de seguridad de la información (ISOTools Excellence Colombia, 2017), se descarta su utilización.

2.6.2. COBIT 5

COBIT 5 (ISACA, 2013) también es una excelente opción para la gestión de riesgos de TI, ya que aborda estos riesgos desde la gobernanza y desde el gobierno de TI, a través de varios dominios que abarcan diferentes prácticas, como sigue:

- *EDM03 - Garantizar la Optimización del Riesgo*: busca asegurar que los riesgos de TI de la entidad no excedan el nivel de tolerancia de riesgo, que se identifican y gestionan el impacto de éstos en la generación de valor de la entidad, y que los fallos de cumplimiento en la gestión de riesgos se reduzcan al mínimo.
- *APO12 - Gestionar el Riesgo*: busca integrar la gestión de riesgos de TI con la gestión de riesgos empresariales generales, y equilibrar los costos y beneficios de gestionar riesgos de TI.
- *APO13 - Gestionar la Seguridad*: busca mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de tolerancia de riesgo de la empresa, estableciendo y manteniendo un SGSI, definiendo y administrando un plan de tratamiento de riesgos de la seguridad de la Información, y monitoreando y revisando el SGSI.
- *BAI09 - Gestionar los Activos*: busca gestionar los activos de TI durante todo su ciclo de vida, para asegurar que su uso aporta valor a un coste óptimo.
- *DSS05 - Gestionar los Servicios de Seguridad*: busca minimizar el impacto en el negocio de las vulnerabilidades operacionales de seguridad de la información y de incidentes, protegiendo la información de la empresa para mantener un nivel de riesgo de seguridad de la información aceptable para la empresa.

Como es visible, su debilidad como marco de referencia radica en la amplitud y que las practicas base tiene enfoque similar a la del estándar ISO31000, descarta su utilización para el modelo de seguridad y privacidad de la Gobernación del Huila.

2.6.3. ISO 27005

Por su parte, el estándar ISO 27005 -Gestión de Riesgos de Seguridad de la Información- se especializa en seguridad de la información, y en el tratamiento de riesgos, para lo cual aplica el proceso de valoración de riesgos, identificando los riesgos asociados a los pilares de la información: confidencialidad, disponibilidad e integridad, y sus dueños, en base a los activos de TI, amenazas, vulnerabilidades existentes. Las amenazas pueden ser de tipo deliberadas, accidentales, y ambientales. Las vulnerabilidades se asocian a cada tipo de activos de TI, y a las amenazas que pueden explotarlas, facilitando de esta forma, la identificación de los riesgos.

Posteriormente se analizan los riesgos, valorando el posible impacto de la materialización de riesgos, las probabilidades de ocurrencia y determinando niveles de riesgo, ya sea de manera cualitativa o cuantitativa, teniendo como base la identificación y valoración de escenarios de incidentes; y se evalúan los riesgos, comparando los resultados anteriores con criterios prestablecidos, para definir el nivel de riesgo residual existente, en base a la efectividad de los controles aplicados en la entidad.

Por último, se realiza el tratamiento de riesgos, seleccionando opciones apropiadas de tratamiento -ya sea reducción, aceptación, evitación y/o transferencia- y determinando los controles necesarios para aplicar los tratamientos seleccionados. Estos controles se comparan con controles predeterminados por el estándar, y se produce una declaración de aplicabilidad que contiene los controles necesarios y que sirven de base para la formulación del plan de tratamiento de riesgos de seguridad de la información (ISO, 2018).

2.6.4. MAGERIT – Metodología de Análisis y Gestión de Riesgos de TI

En cuanto a metodologías, MAGERIT es una metodología de análisis y gestión de riesgos de TI, que tiene entre sus particularidades, suministrar un método sistemático para analizar los riesgos derivados del uso de TI, dentro del cual resalta la disponibilidad de un catálogo de elementos que ofrece este estándar, para facilitar la clasificación de activos en base a cinco dimensiones de seguridad: confidencialidad, integridad, disponibilidad, autenticidad, y trazabilidad.

Igualmente facilita la identificación y clasificación de amenazas, de acuerdo con su origen: de origen natural, del entorno u origen industrial, por defectos de las aplicaciones,

causadas por las personas de forma accidental, y causadas por las personas de forma deliberada. Esta metodología también facilita la identificación y clasificación de controles según su efecto sobre los riesgos residuales. Los controles de efecto preventivo abarcan los de tipo preventivo, disuasorio, eliminatorio; los controles que acotan la degradación de activos generada por incidentes pueden ser minimizadores, correctivos, recuperativos. Y, por último, los controles que consolidan el efecto de las anteriores pueden ser de monitoreo, de detección, de concienciación, y administrativo. Esta metodología, al contar con estas herramientas y guías, permite al responsable de seguridad y privacidad de la información, enfocarse en el análisis de riesgos críticos para las entidades (PAE - Portal de Administración Electrónica, 2012).

Así las cosas, MAGERIT e ISO 27005 ofrecen el proceso para identificar activos, vulnerabilidades y amenazas, así como el impacto y probabilidades de ocurrencia de los riesgos. De esta forma, para manejar idoneidad y linealidad en el modelo de gestión que se propone, se utilizará la norma técnica ISO 27005, bajo el Modelo de Seguridad y Privacidad de la Información del Ministerio TIC, para el proceso de gestión de riesgos de seguridad y privacidad de la información en la Gobernación del Huila, integrando la metodología MAGERIT para la identificación y clasificación de amenazas según su origen.

2.7. Tratamiento de Riesgos de TI

La información antes obtenida mediante la gestión de riesgos es de vital importancia para definir los objetivos, alcance y límites para establecer el estado actual y el estado futuro de la entidad, una vez se determinen e implementen las acciones que se requieran para la mitigación de riesgos, a través de un plan de tratamiento de riesgos. Este plan se enfoca estrictamente en el establecimiento de acciones específicas para gestionar los riesgos de seguridad de la información que se deben eliminar e implantar los controles necesarios para minimizar los riesgos que persistan y proteger la información (Ministerio TIC, 2016, pág. 30).

Un plan de tratamiento de riesgos valora previamente los controles y medidas de seguridad existentes en la organización y su efectividad, para luego ser comparados con los posibles tratamientos identificados en la evaluación de riesgos, con el fin de escoger aquellos que disminuyan el riesgo, y así buscar un nivel aceptable de riesgo en cada

proceso. Posteriormente se debe diseñar el plan, tanto para seguridad como para la privacidad de la información, y este debe definir acciones a implementar, responsables, plazos, recursos, y otros aspectos que la organización pueda considerar necesarios para su cumplimiento, monitoreo y seguimiento pertinente (Ministerio TIC, 2016, pág. 36).

Revisando estándares y lineamientos relacionados, el Modelo de Seguridad y Privacidad de la Información provisto por el Ministerio TIC adopta y alinea diversos estándares, buenas prácticas, y legislaciones establecidas –como la ISO27001, Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras- para la gestión de la información en las entidades públicas, teniendo en cuenta las necesidades, requisitos de seguridad, procesos, tamaño y estructura, entre otros aspectos, a fin de garantizar el uso y la privacidad de los datos y la información que los ciudadanos brindan a las entidades para su tratamiento a través de diferentes trámites y servicios ofertados, y contribuir al cumplimiento de los objetivos estratégicos, y al incremento de los índices de transparencia en la gestión pública (Ministerio TIC, 2016, pág. 20).

De esta forma, este modelo brinda herramientas e instrumentos importantes para desarrollar y promover el mejoramiento del nivel de madurez de la gestión de la seguridad y también de la privacidad de la información, como el Instrumento de Evaluación de MSPI, con el que se pretende obtener resultados precisos, que faciliten a las entidades públicas generar y desarrollar un plan de seguridad de la información, fortaleciendo sus procesos, y dando cumplimiento a lo estipulado en el manual de implementación de la política de gobierno digital (Ministerio TIC, 2017, pág. 6).

3. Marco institucional

3.1. Reseña histórica

El 28 de abril de 1905 la Asamblea Nacional Constituyente y Legislativa, expidió la Ley 46, que fue sancionada en el 29 del mismo mes por el presidente Rafael Reyes, que en su artículo quinto expresa: "*Créase el departamento del Huila, cuya capital será la ciudad de Neiva, y lo formarán las provincias de Neiva y del sur, por los límites que hoy tienen*".

Según la Constitución Política de Colombia, el ejercicio del Poder Ejecutivo de esta región colombiana se deposita en un solo individuo, que se denomina Gobernador del Departamento del Huila, electo popularmente desde 1991, para un periodo de 4 años sin reelección inmediata. En la actualidad su sede administrativa principal se encuentra ubicada en la Carrera 4 calle 8 esquina frente al parque Santander, y se le denomina "*Palacio del Mosaico*". En el marco económico, la Gobernación del Huila se ubica en el sector económico terciario o de servicios, y contribuye a la formación del ingreso nacional y del producto nacional (Red Cultural del Banco de la República de Colombia, s.f.).

3.2. Misión y Visión

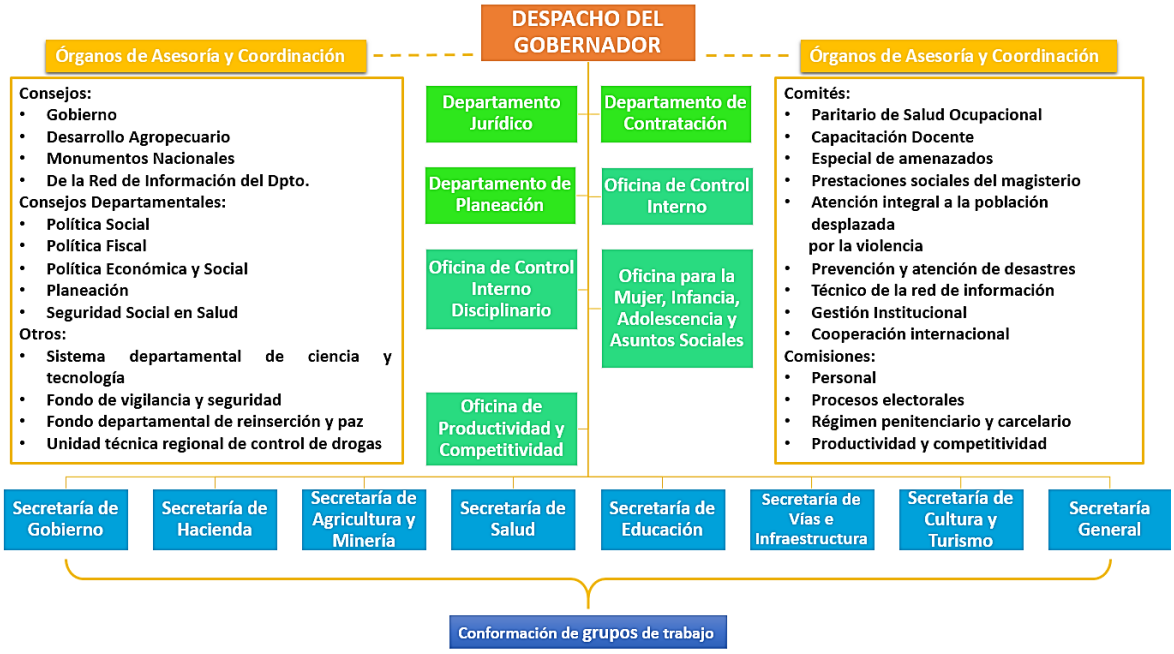
Misión: El Departamento según la Constitución Política tiene autonomía para la administración de los asuntos seccionales y la planificación y promoción del desarrollo económico y social de su territorio. Ejerce funciones administrativas de coordinación, de complementariedad de la acción municipal, de intermediación entre el Gobierno Nacional y los Municipios y prestador de los servicios determinados por la Constitución y la ley (Gobernación del Huila, 2017).

Visión: En el año 2020 el Huila será el corazón verde de Colombia, pacífico, solidario y emprendedor; líder de una región dinámica donde florecen los sueños de todos. (Gobernación del Huila, 2017).

3.3. Estructura Organizacional

Mediante Decreto departamental N° 1338 de 2008 fue definida la estructura orgánica de la Gobernación del Huila (Pajarito Sánchez García, 2008), como se describe a continuación en la Figura 6.

Figura 6. Estructura Organizacional de la Gobernación del Huila



Fuente: Estructura Organizacional, Gobernación del Huila. (2017) - https://www.huila.gov.co/general/publicaciones/7046/estructura-organizacional/

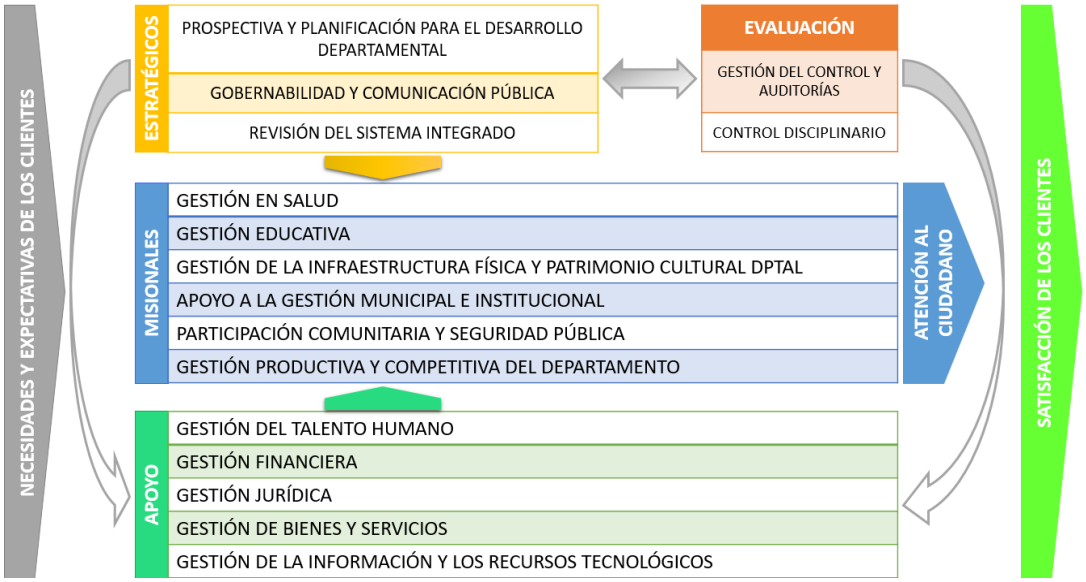
Dentro de la estructura organizacional se incluyó la **Secretaría General**, y a su vez, mediante Resolución N° 223 de 2009 se conforma el grupo interno de trabajo permanente en la Secretaría General, denominado **Grupo de Tecnología, Conectividad y Telecomunicaciones**, que, de acuerdo con la citada resolución, tiene las siguientes funciones:

- Implementar y fortalecer la capacidad organizacional y tecnológica de la Administración Central Departamental, definiendo y desarrollando las políticas, estrategias y directrices para el cumplimiento de la misión institucional.

- Planear y organizar acciones para atender requerimientos de las dependencias del nivel central en lo relacionado con recursos informáticas y de telecomunicaciones.
- Dar apoyo y soporte a todo el esquema informático (tanto hardware como software).
- Seguimiento y desarrollar el Plan Informático de la Gobernación del Huila
- Asesorar a los organismos de la Administración Central en la adquisición y actualización de tecnología y contratación de servicios informáticos.
- Contribuir y prestar mejores servicios en línea para una mayor participación ciudadana, con el fin de contribuir a la construcción de una administración pública más eficiente, más transparente, más participativa y una comunidad más informada". (Gobernación del Huila, 2009).

El Grupo de Tecnología, Conectividad y Telecomunicaciones de la Gobernación del Huila se encuentra enmarcado dentro del macroproceso de apoyo "*Gestión de la Información y de los Recursos Tecnológicos*". La figura que se presenta a continuación describe los macroprocesos que enmarcan la Gobernación del Huila, en el cual se incluye el proceso correspondiente al Grupo de Tecnología de la entidad.

Figura 7. Mapa de Macroprocesos de la Gobernación del Huila



Fuente: Mapa de Procesos, Gobernación del Huila. (2021).
https://www.huila.gov.co/publicaciones/10739/mapa-de-procesos/

3.4. Portafolio de Servicios de TI

Con relación al Grupo de Tecnología, Conectividad y Telecomunicaciones, éste presta los diferentes servicios de TI a las demás áreas, dependencias y procesos de gestión de la Gobernación del Huila, entre los que se destacan el servicio de conectividad a internet, soporte técnico a usuarios, conexión a redes Ethernet y WiFi, gestión y control de usuarios, correo electrónico, extranet, página web institucional, sistemas de información, entre otros.

Tabla 1. Servicios que presta el Grupo de Tecnología de la Gobernación del Huila

Nombre del Servicio	Descripción
Internet	Conexión a internet para el edificio central y sedes de la Gobernación del Huila
Soporte a usuarios	Asistencia técnica, de manera presencial o virtual, a equipos informáticos de puestos de trabajo
Conexión red WiFi	Acceso a la red de datos a través de conexión inalámbrica para equipos de la entidad y usuarios externos
Gestión de usuarios	Creación y administración de usuarios del domino de la entidad
Correo electrónico	Medio de intercambio externo e interno de información institucional, a través de internet de manera confiable y fácil - Creación y gestión de cuentas
Extranet	Portal de información y comunicación interno, mediante el cual se tiene acceso a información institucional y herramientas que apoyan la gestión de las diferentes dependencias
Mensajería instantánea	Medio de comunicación a través de internet, tipo chat, que permita la comunicación en tiempo real y de manera segura
Página web	Publicación de información en el portal oficial de comunicación, transparencia e interacción de la entidad, dirigido a la ciudadanía y a otras entidades ww.huila.gov.co
Sistemas de información	Gestión de requerimientos no funcionales de los diferentes sistemas de información que soportan procesos de la entidad
Soporte al sistema financiero SIFA	Apoyo técnico a la gestión de usuarios y operación del SIFA
Soporte al sistema de Comunicaciones Oficiales	Apoyo técnico a la gestión de usuarios y operación del Sistema de Comunicaciones Oficiales
Telefonía fija	Medio de comunicación por voz a través de la red de telefonía fija que permite la comunicación entre dependencias y con el exterior - Soporte y mantenimiento
Backup	Almacenamiento y respaldo de información relevante que respalde procesos de la entidad
Conceptos técnicos	Elaboración conceptos técnicos relacionados con las adquisiciones tecnológicas en hardware, sistemas de información y aplicaciones

Fuente: Catálogo de Servicios TI, Gobernación del Huila. (2020).

https://www.huila.gov.co/documentos/1382/catalogo-de-servicios-ti/

4. Diseño metodológico

De acuerdo a la formulación del problema de investigación, se establece el alcance del presente proyecto como *descriptivo*, basados en hipótesis descriptivas en las que se relacionan los conceptos de seguridad y privacidad de la información, amenazas, vulnerabilidades, riesgos y activos; también se puede establecer el alcance de este proyecto como *explicativo*, si se tiene en cuenta el establecimiento de hipótesis causales, en las que a partir de la presencia de vulnerabilidades y amenazas sobre un activo, es posible materialización de incidentes y riesgos de seguridad y privacidad de la información sobre un activo.

4.1. Tipo de investigación

Según los objetivos propuestos, el presente proyecto de investigación es de tipo *No Experimental*, partiendo del análisis de la necesidad de establecer un modelo de gestión de seguridad y privacidad de la información para la Gobernación del Huila, se analizan y valoran los activos de TI, sus vulnerabilidades y amenazas, y se identifica el impacto de los riesgos que los afectan.

Así mismo, es de tipo *Aplicada*, partiendo del análisis de que la investigación planteada tiene como fin la aplicación directa para resolver problemas prácticos, en circunstancias concretas, problemas como la mitigación de riesgos de seguridad de la información a partir de vulnerabilidades y amenazas que afectan a activos de TI de la Gobernación del Huila.

4.2. Técnicas de recolección de información

En la investigación *No Experimental* se observan fenómenos tal y como se presentan naturalmente, y permite escoger entre múltiples técnicas de recolección de datos:

- *Fuentes Primarias*: a través de la observación, documentos oficiales, formatos diseñados, y reuniones con funcionarios de cada proceso, se recopilará la información necesaria para las diferentes etapas de formulación e implementación del Modelo de Gestión de Seguridad y Privacidad de la Información.

- *Fuentes Secundarias*: a través de internet, indicadores y caracterización de los procesos de gestión de la entidad, planes de desarrollo vigentes, normatividad y reglamentación asociada, se recopilará esta información.

4.3. Enfoque investigativo

El presente proyecto de investigación presente un enfoque *Cuantitativo*, teniendo en cuenta que, planteadas las hipótesis de investigación, se trata de demostrar los conceptos que las respaldan, siguiendo un patrón predecible y estructurado (Valoración de Activos - Análisis y Tratamiento de Riesgos - Gestión de Seguridad y Privacidad de la Información).

4.3.1. Diseño de la Investigación

Según el tipo y el alcance establecido, esta investigación se plantea como *No Experimental Transeccional*, ya que las observaciones necesarias (valoración de activos - gestión de riesgos) se realizan en un solo momento dentro de dicho proceso. A su vez, la investigación se aborda de dos formas:

- *Transeccional Descriptivo*, debido a que recolectan información y datos sobre seguridad y privacidad de la información, activos de TI, amenazas, vulnerabilidades, y riesgos, reportando el análisis y resultados de esos datos.

- *Transeccional Correlacional-Causal*, debido a que, en las conclusiones de los análisis y resultados obtenidos, se pueden establecer relaciones de causalidad entre los riesgos y los activos.

4.3.2. Población / Muestra

En el presente proyecto de investigación, la población corresponde al 100% de los líderes de procesos de gestión adscritos al Sistema Integrado de Gestión de la Gobernación del Huila, conformado por 38 personas para 36 procesos. Por este motivo, y teniendo en cuenta los tamaños de muestra mínimos en estudios cuantitativos (30 casos), no se considera necesaria la utilización de ninguno método, herramienta o software de muestreo, y se aplica censo a la población establecida, utilizando las técnicas y fuentes de información antes descritas.

4.4. Análisis de la Información

Para el desarrollo del presente proyecto, y el cumplimiento de los objetivos propuestos, se realizarán las siguientes fases o actividades macro:

4.4.1. Fase 1 - Análisis y valoración de activos

Con el fin de identificar y documentar los activos de TI, a partir del inventario de la entidad, se diseñarán formatos para recopilar esta información, mediante entrevistas con cada uno de los líderes de procesos de gestión, clasificándolos y cuantificándolos según funcionalidades, y valorándolos según criterios de la metodología MAGERIT (Gutierrez Amaya, 2013). En el marco de las entrevistas a cada líder de proceso, se realizarán preguntas sobre uso de activos de TI, que permitan la evaluación acertada de las dimensiones de seguridad para cada activo, de acuerdo al contexto de cada proceso.

4.4.2. Fase 2 - Identificación de vulnerabilidades y amenazas

Una vez identificado, clasificado y cuantificado cada activo de TI, se identificarán sus vulnerabilidades y debilidades, mediante entrevistas con cada uno de los líderes de procesos de gestión de la entidad, así como también se asociarán posibles amenazas, según la metodología MAGERIT (Gutierrez Amaya, 2013), para lo cual se integrarán al

formato de análisis y valoración de activos, campos para la identificación de vulnerabilidades y amenazas de cada activo.

Además de lo anterior, se realizará la identificación de activos que correspondan a infraestructuras críticas cibernéticas – ICC, los cuales son catalogados de esta manera, si su impacto o afectación podría superar alguno de los siguientes 3 criterios: Impacto Social mayor a 250.000 personas (0,5% de Población Nacional), Impacto Económico mayor a $464.619.736 (PIB de un Día o 0,123% del PIB Anual), o Impacto Ambiental mayor a 3 años de recuperación. Esta información se integrará en el formato de análisis y valoración de activos, para disponer de toda la información de cada activo en un mismo formato.

4.4.3. Fase 3 - Análisis, evaluación y gestión de riesgos

Utilizando el formato "*Matriz de Identificación y Valoración de Riesgos"* establecido por la Gobernación del Huila a partir de la Guía para la administración del riesgo y el diseño de controles en entidades públicas (Función Pública, 2018), se identificarán, analizarán y evaluarán los riesgos que afectan los activos de TI de la Gobernación del Huila, integrando además la norma técnica ISO 27005 bajo el Modelo de Seguridad y Privacidad de la Información del Ministerio TIC, para medir el nivel de riesgo existente, identificar consecuencias y controles existentes, valorar probabilidad e impacto, y a partir de lo anterior, definir en la siguiente fase, el tratamiento a aplicar según el tipo de activo (Gutiérrez Amaya, 2013).

4.4.4. Fase 4 - Tratamiento de riesgos

Una vez identificados, analizados y evaluados los riesgos, se definirá la estrategia de tratamiento para cada uno de éstos, a partir de las siguientes: evitar, aceptar, compartir o reducir el riesgo. De esta forma y al seleccionar alguna de estas estrategias, establecidas en la Política de Operación para la Administración de Riesgos de la Gobernación del Huila (2019), se definirán las acciones necesarias para el cumplimiento de éstas.

Además de lo anterior, se diseñará un formato para la planificación del tratamiento de riesgos de seguridad de la información, adaptándose a la matriz existente, de modo que permita la diferenciación entre el control seleccionado y la acción de control establecida

para la mitigación del riesgo residual, siguiendo los lineamientos del Ministerio TIC, que sugieren utilizar el Anexo A de la norma técnica ISO/IEC 27001:2013, con el fin de seleccionar acciones de control y establecer las actividades a aplicar sobre los riesgos residuales identificados (plasmándolas en Planes de Tratamiento de Riesgos de Seguridad de la Información por procesos, y en un Plan Consolidado de Tratamiento de Riesgos de Seguridad).

4.4.5. Fase 5 - Planeación de la Seguridad y Privacidad de la Información

Además de las acciones de control establecidas a partir de la evaluación y tratamiento de riesgos, y las acciones relacionadas y derivadas de otros factores legales, organizacionales y/o normativos, se determinará el modelo de gestión adaptado a la entidad, y el plan de acción a diseñar e implementar, que incluya y abarque todas las acciones de control necesarias para la gestión de la seguridad y privacidad de la información en la Gobernación del Huila.

4.4.6. Fase 6 - Sensibilización en Seguridad y Privacidad de la Información

Posteriormente se definirá el Plan de Sensibilización de Seguridad, con el fin de ejecutar estrategias de promoción de la cultura organizacional orientada hacia la prevención de riesgos de seguridad y privacidad de la información, que abarque entre otros aspectos, la identificación de necesidades y población objetivo, roles y responsabilidades, metas, temáticas de sensibilización y capacitación, actividades e indicadores de gestión de seguridad y privacidad de la información.

5. Diagnóstico organizacional

De acuerdo con los objetivos establecidos, se hace necesario realizar el análisis de la organización, aplicando la metodología propuesta, y teniendo en cuenta cada uno de los macroprocesos de gestión que componen el Sistema Integrado de Gestión de la Gobernación del Huila, para conocer el estado actual, fortalezas, oportunidades de mejora y/o hallazgos, presentando y analizando los resultados obtenidos.

5.1. Diagnóstico de activos

Es necesario identificar los activos de TI y documentarlos mediante un inventario de activos, para saber lo que se debe proteger y garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (FrontOffice), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado. Esto, mediante encuestas y entrevistas con funcionarios líderes de procesos de gestión de la entidad. Después, estos activos se clasifican y cuantifican según funcionalidades, y se valoran según criterios de la norma técnica ISO/IEC 27001:2013, evaluando las dimensiones de seguridad para cada activo.

Esta información se recopiló en un formato denominado "*Matriz de Identificación de Activos de Seguridad de la Información*", diseñado en formato de archivo xlsx -basado en el Modelo de Seguridad y Privacidad de la Información del MinTIC, y en el que se incluyen una serie de pasos que permiten realizar una valoración de cada activo- de forma que se facilitara su integración a la metodología de gestión de riesgos de la entidad, y su uso por parte de personal de la Coordinación del Sistema Integrado de Gestión.

Figura 8. Matriz de Identificación de Activos de Seguridad de la Información – Pasos 1 al 6

1	2	3	4	5			6
Activos de seguridad digital asociados al proceso	**Tipo de activo**	**Dueño del activo**	**Custodia del activo**	**Clasificación de los activos**			**Criticidad del activo**
				Confidencialidad	Integridad	Disponibilidad	
Base de datos de calidad de datos	Información	Entidades propietarias del dato	Líder de proceso Sistemas de Información	3	1	1	**ALTA**

Fuente: MinTIC, Taller "Más seguridad, mejor región" (2019, pág. 102). https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

- **Listar activos:** Se listan los activos de Seguridad de la Información, correspondientes a los activos de TI que se identifican en cada proceso de gestión, indicando nombre y descripción breve de cada uno.
- **Identificar tipo de activo:** Cada activo se clasifica en un determinado grupo de activos según su naturaleza cómo sigue a continuación: Información, Software, Hardware, Servicios, Intangibles, Componentes de Red, Personas, Instalaciones.
- **Identificar dueño del activo:** Cada uno de los activos identificados debe tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.
- **Identificar custodio del activo:** Cada activo identificado debe tener una parte designada de la entidad, cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles que posteriormente se definan.
- **Clasificar activo según criticidad:** Se realiza la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable. Posteriormente se evalúa la criticidad de los activos, determinando el grado de importancia de cada uno, para que después, durante el análisis de riesgos tener presente esta criticidad y hacer una valoración adecuada de cada caso. Teniendo en cuenta lo anterior, se plantean las siguientes escalas valorativas para determinar la criticidad del activo en cada una de sus propiedades.

Figura 9. Escala de valoración de criticidad según disponibilidad de activos de Seguridad de la Información

CRITICIDAD SEGÚN DISPONIBILIDAD	
ALTA	La no disponibilidad de información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen **severas** de la entidad
MEDIA	La no disponibilidad de información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen **moderadas** de la entidad
BAJA	La no disponibilidad de información puede afectar la operación normal de la entidad o entes externos, per no conlleva implicaciones legales, económicas o de pérdida de imagen
NO CLASIFICADA	Activos de información que deben ser incluidos en el inventario, y que aún no han sido clasificados, deben ser tratados como activos de información de **disponibilidad ALTA**

Fuente: MinTIC, Taller “Más seguridad, mejor región” (2019, págs. 96-100).. https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

Figura 10. Escala de valoración de criticidad según integridad de activos de Seguridad de la Información

CRITICIDAD SEGÚN INTEGRIDAD	
ALTA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen **severas** de la entidad
MEDIA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen **moderadas** de la entidad
BAJA	Información cuya pérdida de exactitud y completitud conlleva un impacto **no significativo** para la entidad o entes externos
NO CLASIFICADA	Activos de información que deben ser incluidos en el inventario, y que aún no han sido clasificados, deben ser tratados como activos de información de **integridad ALTA**

Fuente: MinTIC, Taller “Más seguridad, mejor región” (2019, págs. 96-100).. https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

Figura 11. Escala de valoración de criticidad según confidencialidad de activos de Seguridad de la Información

CRITICIDAD SEGÚN CONFIDENCIALIDAD	
Información Pública Reservada	Información que estando en custodia, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento del Artículo 19 de la Ley 1712 de 2014. Ej. defensa y seguridad nacional, derechos de infancia y adolescencia, salud pública.
Información Pública Clasificada	Información que estando en custodia, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado. Ej. datos personales y secretos comerciales.
Información Pública	Información que un sujeto obligado genere, obtenga, adquiera o controle.

Fuente: MinTIC, Taller “Más seguridad, mejor región” (2019, págs. 96-100).. https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

- **Determinar nivel de criticidad neta del activo:** Se indica el nivel de criticidad neta del activo, con base en el resultado de la criticidad en cada una de sus propiedades.

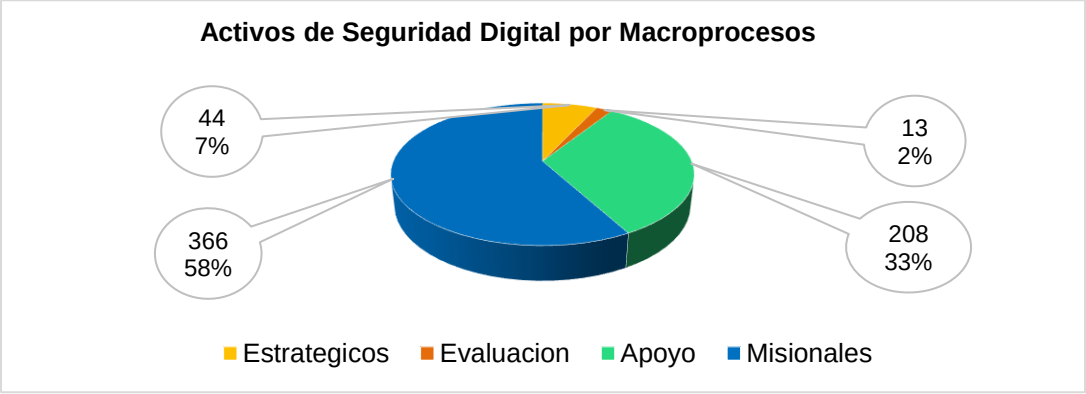
Figura 12. Escalas de valoración de criticidad de activos de Seguridad de la Información

CRITICIDAD NETA DE UN ACTIVO	
ALTA	Activos de información en los cuales la clasificación de la información en **mínimo dos (2) de las propiedades** (confidencialidad, integridad, y disponibilidad) es **ALTA**
MEDIA	Activos de información en los cuales la clasificación de la información en **una (1) de sus propiedades es ALTA** o en **al menos una (1) de sus propiedades es MEDIA**
BAJA	Activos de información en los cuales la clasificación de la información en **todas sus propiedades es BAJA**

Fuente: MinTIC, Taller "Más seguridad, mejor región" (2019, pág. 101). https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

El diagnóstico realizado a los activos de TI correspondientes a todas las áreas y procesos de gestión de la Administración Central Departamental de la Gobernación del Huila (Ver Anexo 1 "Identificación de activos de TI por macroprocesos" y Ver Anexo 2 "Matrices de Activos de Seguridad de la Información"), permitió la identificación de serias deficiencias en infraestructura tecnológica para soportar la prestación de los servicios de TI a todas las dependencias de la administración, lo que facilita el origen de eventos e incidentes de indisponibilidad de servicios, y otras implicaciones relacionadas con la ejecución de actividades y procesos misionales de la entidad, en los que se encuentra el mayor porcentaje de activos en la entidad, tal como se evidencia en la Figura 13.

Figura 13. Activos de Seguridad de la Información por Macroprocesos en la entidad



Fuente: Elaboración propia

En la tabla 2 se consolidan los principales hallazgos identificados respecto a los activos de Seguridad de la Información en la Gobernación del Huila.

Tabla 2. Hallazgos identificados por cada tipo de activo de Seguridad de la Información

HALLAZGOS POR TIPO DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN	
Información	**Hallazgos**
• Inventario de sistemas de información. • Documentos contractuales • Inventarios documentales. • Inventario de activos. • Nómina, expedientes laborales y pensionales. • Presupuesto, información financiera y de recaudo de impuestos. • Bases de datos de contribuyentes. • Información de evaluación, seguimiento, y de mejoras por procesos de la entidad. • Agenda del Gobernador. • Información del Sistema Integrado de Gestión. • Información sectorial y de necesidades poblacionales • Seguimiento al plan de desarrollo departamental. • Base de datos de grupos de valor caracterizados. • Información de carácter misional: infraestructura productiva, vial, matrícula escolar en las I.E. oficiales, documentos PQRSDF y de salida, afiliados al régimen subsidiado y contributivo de salud, historias clínicas de pacientes, programas de salud pública.	• La información de carácter misional, estratégico, de apoyo, y de evaluación, que se gestiona y aloja en equipos de cómputo, así como las bases de datos almacenadas en los servidores de los centros de datos, es asegurada mediante un servidor de respaldo de información que no cubre la totalidad de información gestionada por los funcionarios de la entidad (186 de 247 funcionarios, equivalente al 75%). Además, no se cuenta con la capacidad suficiente para almacenar y procesar los datos alojados en los servidores, ni tampoco se cuenta con lineamientos internos establecidos para promover el respaldo de la información, como parte del control A.12.3.1 "Respaldo de información" del Anexo A de la norma técnica ISO/IEC 27001:2013, que indica que "*Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada*". • Se evidencia indisponibilidad de información que se encuentra alojada en sistemas de información con entornos web, al momento en que se interrumpe la conectividad a internet, con lo que se incumplen los acuerdos de niveles de servicio establecidos al interior de la Gobernación del Huila, y los controles A.13.1.2. "Seguridad de los servicios de red" que indica que "*Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente*", y A.15.2.1. "Seguimiento y revisión de los servicios de los proveedores" que indica que "*Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores*" del Anexo A de la norma técnica ISO/IEC 27001:2013. • Se evidencia que la información de carácter misional gestionada en medio físico, no se encuentra debidamente almacenada ni asegurada, ya que se encuentra expuesta a terceros y a daños de origen natural e industrial (goteras, humedades, etc.), con lo que se incumple con el control A.9.1.1. "Política de control de acceso" que indica que "*Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información*", y con los controles del dominio A.11 "Seguridad Física y del Entorno" del Anexo A de la norma técnica ISO/IEC 27001:2013.
Red	**Hallazgos**
• Switches. • Firewall. • Cableado estructurado. • Routers. • Access point.	• Se evidencian que se presentan interrupciones de servicios de red y acceso a información en el edificio principal y sedes de la entidad, provocadas por daños en el cableado estructurado, derivados de obstrucciones con carpetas, cajas y otros elementos, incumpliendo las políticas de seguridad física del cableado, establecidas en el manual de políticas de TI de la Gobernación del Huila, el control A.11.2.3. "Seguridad en el cableado" que indica que "*El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño*", y el control A.11.2.9. "Política de escritorio y pantalla limpios" que indica que "*Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información*".
Software	**Hallazgos**
• Sistema de Información Financiera y Administrativo • Sistema de Información Tributario. • Portal Web Institucional. • Sistema de Gestión de Contratación.	• Se evidencia que no se gestionan eficientemente las contraseñas de acceso a sistemas y aplicativos, ya que los funcionarios exponen y comparten con terceros sus credenciales, incumpliendo con la política de control de acceso establecida en el manual de políticas de TI de la Gobernación del Huila. • No existen políticas de seguridad con proveedores de servicios de TI en la Gobernación del Huila, que incluyan requerimientos mínimos de servicios, SLA, gestión de cambios, entre otros aspectos incumpliendo con los controles

HALLAZGOS POR TIPO DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN	
• Sistema de Gestión Documental – Sistema de Comunicaciones Oficiales. • Sistema Integral de Salud. • Sistema de Información Regional - SIRHUILA. • Sistema de Información Turística y Cultural del Huila SITYC. • Sistema de Información de Procesos Judiciales. • Sistema de Información de Personas Jurídicas. • Sistema de Información de Control Disciplinario SIID. • Tablero Balanceado de Gestión TBG – Huila. • Licenciamiento de Software.	del dominio A.15 "Relaciones con proveedores" del Anexo A de la norma técnica ISO/IEC 27001:2013. • Se identifica la existencia de sistemas operativos sin soporte técnico de fabricante, instalados en equipos de cómputo de la entidad, incumpliendo de esta manera con los parámetros establecidos para compra de tecnología en el manual de política de TI de la Gobernación del Huila, que indican que "La reposición de software básico y de automatización de oficina tendrá en cuenta los cambios de versiones de los proveedores y los tiempos límites de soporte del proveedor a las versiones antiguas." • Se evidencia la falta de personal capacitado para administración de servidores y red de comunicaciones de la entidad, ya que la entidad requiere anualmente la disposición de recursos para contratación mediante outsourcing de personal de servicios especializados tecnológicos, con lo que se incumple el control A.7.2.2. "Toma de conciencia, educación y formación en la seguridad de la información" del Anexo A de la norma técnica ISO/IEC 27001:2013, que indica "*Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo*".
Hardware	**Hallazgos**
• Equipos de cómputo. • Servidores. • Impresoras multifuncionales. • Impresoras plotter. • Equipos de laboratorio de salud pública • Circuitos cerrados de TV • Sistema de Voz IP • Radios de comunicaciones • Videowall.	• Existen equipos de cómputo e impresoras con daños en componentes de hardware que afectan su disponibilidad en algunas dependencias de la entidad, por lo que los mantenimientos realizados anualmente son insuficientes para conservar sus funcionalidades, incumpliendo con las políticas de mantenimiento de equipos de cómputo y de administración de recursos tecnológicos, establecidas en el manual de política de TI de la Gobernación del Huila, y con el control A.11.2.4. "Mantenimiento de equipos" del Anexo A de la norma técnica ISO/IEC 27001:2013, que indica que "*Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas*". • Se evidencian interrupciones e indisponibilidad de servicios soportados por servidores de sistemas de información que no han contado con mantenimientos suficientes ni controles de cambios en sus configuraciones, incumpliendo con los controles A.11.2.4. "Mantenimiento de equipos", que indica que "*Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas*", y A.12.1.3. "Gestión de la capacidad", que indica que "*Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura*", del Anexo A de la norma técnica ISO/IEC 27001:2013.
Personas	**Hallazgos**
• Funcionarios. • Contratistas. • Contratistas de apoyo con perfil técnico misional. • Administradores de sistemas de información. • Coordinador de Grupo de Tecnología. • Personal del Grupo de Tecnología. • Alta dirección (Gabinete Departamental).	• Se evidencia que se presenta interrupción de servicios misionales en la entidad, al no contar con funcionarios de planta suficientes ni con el perfil técnico requerido para la prestación de estos servicios. Tampoco se cuenta con funcionarios capacitados para la administración de servidores y red de comunicaciones de la entidad, por lo que se requiere anualmente de recursos para contratación de personal de servicios especializados, tanto para la prestación de servicios misionales, como para la prestación de servicios tecnológicos, con lo que se incumple el control A.7.2.2. "Toma de conciencia, educación y formación en la seguridad de la información" del Anexo A de la norma técnica ISO/IEC 27001:2013, que indica "*Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo*".

Fuente: Elaboración propia

De acuerdo con los hallazgos anteriores, y en cumplimiento del primer objetivo específico del presente proyecto, se evidencia el interés de la Gobernación del Huila por disponer de lineamientos internos para gestionar sus activos de TI, partiendo del hecho de contar con un manual de políticas de TI que, aunque de manera inicial busca establecer la repetitividad de procedimientos para gestionar la seguridad de su información, resulta insuficiente al no contar con una alineación estratégica a través de una política general y la asignación de roles y responsabilidades asociados, ni con actualizaciones acorde a los últimos lineamientos y estándares establecidos por el Ministerio TIC y la norma técnica ISO/IEC 27001:2013.

Sin embargo, cabe resaltar en los hallazgos relacionados como la injerencia del factor humano en el contexto de cada uno de los procesos es clave para la identificación de fallas y debilidades, que conllevan eventualmente a la identificación de riesgos, o en su defecto a oportunidades y acciones de mejora, asociados a los lineamientos o requisitos normativos citados. Así mismo, se evidencia cómo las fallas y debilidades identificadas sobre los activos de Seguridad de la Información, afectan directamente la prestación de servicios, tanto a usuarios internos como a usuarios externos, teniendo en cuenta que, a través de la gestión de las propiedades de los activos (confidencialidad, integridad, y disponibilidad), se busca garantizar el aporte de valor a los objetivos estratégicos de la entidad.

5.1.1. Dominios a evaluar

A partir de los hallazgos identificados en el diagnóstico de activos, y según los lineamientos del Ministerio TIC y de la Norma Técnica ISO 27001, se determinan los dominios de control a evaluar, como se observa en la Tabla 3. Esto permitirá la identificación de las acciones que actualmente se desarrollan en la Gobernación del Huila en materia de seguridad y privacidad de la información, y verificar de esta forma la existencia, operación y efectividad de controles de seguridad que faciliten la implementación del Modelo de Seguridad y Privacidad de la Información en la entidad, y la medición de su nivel de madurez correspondiente.

Tabla 3. Dominios de Control de Seguridad a evaluar en la Gobernación del Huila

DOMINIOS DE CONTROL A EVALUAR SEGÚN ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN IDENTIFICADOS EN LA GOBERNACIÓN DEL HUILA	
Información	**Dominios de Control**
• Inventario de sistemas de información.	Dominio No. 12: Seguridad de las Operaciones
• Documentos contractuales	Dominio No. 11: Seguridad Física y del Entorno. Dominio No. 13: Seguridad en las Comunicaciones
• Inventarios documentales.	Dominio No. 12: Seguridad de las Operaciones
• Inventario de activos.	Dominio No. 12: Seguridad de las Operaciones
• Nómina, expedientes laborales y pensionales.	Dominio No. 11: Seguridad Física y del Entorno. Dominio No. 12: Seguridad de las Operaciones.
• Presupuesto, información financiera y de recaudo de impuestos.	Dominio No. 11: Seguridad Física y del Entorno. Dominio No. 15: Relaciones con Proveedores.
• Bases de datos de contribuyentes.	Dominio No. 11: Seguridad Física y del Entorno. Dominio No. 15: Relaciones con Proveedores.
• Información de evaluación, seguimiento, y de mejoras por procesos de la entidad.	Dominio No. 13: Seguridad en las Comunicaciones
• Agenda del Gobernador.	Dominio No. 9: Control de Acceso Dominio No. 11: Seguridad Física y del Entorno.
• Información del Sistema Integrado de Gestión.	Dominio No. 13: Seguridad en las Comunicaciones
• Información sectorial y de necesidades poblacionales	Dominio No. 12: Seguridad de las Operaciones
• Seguimiento al plan de desarrollo departamental.	Dominio No. 12: Seguridad de las Operaciones
• Base de datos de grupos de valor caracterizados.	Dominio No. 11: Seguridad Física y del Entorno. Dominio No. 12: Seguridad de las Operaciones Dominio No. 15: Relaciones con Proveedores.
• Información de carácter misional: infraestructura productiva, vial, matrícula escolar en las I.E. oficiales, documentos PQRSDF y de salida, afiliados al régimen subsidiado y contributivo de salud, historias clínicas de pacientes, programas de salud pública.	Dominio No. 9: Control de Acceso Dominio No. 11: Seguridad Física y del Entorno Dominio No. 12: Seguridad de las Operaciones Dominio No. 13: Seguridad en las Comunicaciones
Red	**Dominios de Control**
• Switches.	Dominio No. 13: Seguridad en las Comunicaciones
• Firewall.	Dominio No. 13: Seguridad en las Comunicaciones
• Cableado estructurado.	Dominio No. 11: Seguridad Física y del Entorno
• Routers.	Dominio No. 13: Seguridad en las Comunicaciones
• Access point.	Dominio No. 13: Seguridad Física y del Entorno
Software	**Dominios de Control**
• Sistema de Información Financiera y Administrativo	Dominio No.15: Relaciones con proveedores
• Sistema de Información Tributario.	Dominio No.14: Adquisición, Desarrollo y Mantenimiento de los sistemas de información Dominio No.15: Relaciones con proveedores
• Portal Web Institucional.	Dominio No.14: Adquisición, Desarrollo y Mantenimiento de los sistemas de información Dominio No.15: Relaciones con proveedores
• Sistema de Gestión de Contratación.	Dominio No. 9: Control de Acceso Dominio No.15: Relaciones con proveedores
• Sistema de Gestión Documental – Sistema de Comunicaciones Oficiales.	Dominio No. 9: Control de Acceso Dominio No.15: Relaciones con proveedores

DOMINIOS DE CONTROL A EVALUAR SEGÚN ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN IDENTIFICADOS EN LA GOBERNACIÓN DEL HUILA	
• Sistema Integral de Salud.	Dominio No. 9: Control de Acceso Dominio No.15: Relaciones con proveedores
• Sistema de Información Regional - SIRHUILA.	Dominio No.14: Adquisición, Desarrollo y Mantenimiento de los sistemas de información
• Sistema de Información Turística y Cultural del Huila SITYC.	Dominio No.14: Adquisición, Desarrollo y Mantenimiento de los sistemas de información Dominio No.15: Relaciones con proveedores
• Sistema de Información de Procesos Judiciales.	Dominio No. 7: Seguridad de los Recursos Humanos Dominio No.14: Adquisición, Desarrollo y Mantenimiento de los sistemas de información Dominio No.15: Relaciones con proveedores
• Sistema de Información de Personas Jurídicas.	Dominio No. 7: Seguridad de los Recursos Humanos Dominio No.14: Adquisición, Desarrollo y Mantenimiento de los sistemas de información Dominio No.15: Relaciones con proveedores
• Sistema de Información de Control Disciplinario SIID.	Dominio No. 7: Seguridad de los Recursos Humanos Dominio No.14: Adquisición, Desarrollo y Mantenimiento de los sistemas de información Dominio No.15: Relaciones con proveedores
• Tablero Balanceado de Gestión TBG – Huila.	Dominio No. 9: Control de Acceso
• Licenciamiento de Software.	Dominio No. 7: Seguridad de los Recursos Humanos Dominio No. 9: Control de Acceso Dominio No. 12: Seguridad de las Operaciones
Hardware	**Dominios de Control**
• Equipos de cómputo.	Dominio No. 11: Seguridad Física y del Entorno
• Servidores.	Dominio No. 11: Seguridad Física y del Entorno Dominio No. 12: Seguridad de las Operaciones
• Impresoras multifuncionales.	Dominio No. 11: Seguridad Física y del Entorno
• Impresoras plotter.	Dominio No. 11: Seguridad Física y del Entorno
• Equipos de laboratorio de salud pública	Dominio No. 11: Seguridad Física y del Entorno
• Circuitos cerrados de TV	Dominio No. 11: Seguridad Física y del Entorno
• Sistema de Voz IP	Dominio No. 11: Seguridad Física y del Entorno
• Radios de comunicaciones	Dominio No. 11: Seguridad Física y del Entorno
• Videowall.	Dominio No. 11: Seguridad Física y del Entorno
Personas	**Dominios de Control**
• Funcionarios.	Dominio No. 7: Seguridad de los Recursos Humanos
• Contratistas.	
• Contratistas de apoyo con perfil técnico misional.	
• Administradores de sistemas de información.	
• Coordinador de Grupo de Tecnología.	
• Personal del Grupo de Tecnología.	
• Alta dirección (Gabinete Departamental).	

Fuente: Elaboración propia

Además de los dominios establecidos a partir del diagnóstico de activos realizado, es necesario realizar verificación y actualización de otros dominios y controles existentes en seguridad y privacidad de la información, teniendo en cuenta que muchas de estos controles no han sido comunicados formalmente al talento humano de la Gobernación, y/o no están acorde con los lineamientos y estándares que se adoptan a través del desarrollo del presente proyecto.

De esta forma, adicional a los ya establecidos en la Tabla 3, se establece que los dominios que a continuación se indican, también requieren verificación y actualización:

- *Dominio No. 5 - Políticas de Seguridad de la Información*: Requiere generación de política general y actualización de políticas específicas de seguridad y privacidad de la información existentes.
- *Dominio No. 6 - Organización de la seguridad de la información*: Requiere establecer funciones, responsabilidades y contactos con autoridades y grupos de interés en seguridad y privacidad de la información.
- *Dominio No. 8 - Gestión de activos*: Requiere actualizar los controles relacionados con la responsabilidad de los activos, la clasificación de la información, y la gestión de soportes físicos extraíbles.
- *Dominio No. 16 - Gestión de incidentes de la seguridad de la información*: Requiere generar lineamientos y/o procedimientos para la gestión y respuesta ante incidentes de seguridad de la información en la entidad.
- *Dominio No. 17 - Aspectos de seguridad de la información en la gestión de continuidad del negocio*: Requiere verificación de lineamientos de contingencias de TI existentes y generación de lineamientos de seguridad de la información en la gestión de continuidad de los servicios de la Gobernación, ante eventos de emergencia.
- *Dominio No. 18 – Cumplimiento*: Requiere actualización de lineamientos, políticas, y procedimientos de la Gobernación, asociados al cumplimiento de políticas, normas y legislación existente, y relacionada con seguridad de la información.

5.2. Análisis y valoración de riesgos

Aplicando la matriz de identificación de activos de Seguridad de la Información diseñada, también se identificaron las amenazas y vulnerabilidades que pueden facilitar la materialización de los tres tipos de riesgos de Seguridad de la Información (pérdida de confidencialidad, pérdida de integridad, pérdida de disponibilidad) para cada activo de TI

identificado en cada uno de los procesos de gestión de la Gobernación del Huila, como sigue a continuación:

5.2.1. Amenazas detectadas

Los riesgos de Seguridad de la Información se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: integridad, confidencialidad o disponibilidad. Para cada riesgo identificado, se asocian el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. En base a esto, existen tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo, se seleccionan las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice en un activo de Seguridad de la Información.

Existen diversos lineamientos y estándares como la Norma Técnica ISO/IEC 27005 y MAGERIT, que muestran posibles amenazas, y posibles causas o vulnerabilidades que pueden materializar los tres tipos de riesgos de Seguridad de la Información (pérdida de confidencialidad, pérdida de integridad, pérdida de disponibilidad). En este caso, se utiliza el cuadro denominado "*Matriz de Identificación de Activos de Seguridad de la Información*", en el que a partir del paso 7, se identifican las diferentes amenazas que, según su origen, pueden llegar a afectar el activo identificado, y en el paso 8 las posibles causas que permitirían la materialización de estas amenazas, y las vulnerabilidades que presentan estos activos, y que pueden llegar a ser explotadas.

Figura 14. Matriz de Identificación de Activos de Seguridad de la Información–Pasos 7 al 10

7				8		9	10
Amenazas por activo				Causas / Vulnerabilidades		Infraestructura Crítica Cibernética	Observaciones
Naturales	Industriales	Errores y fallas	Ataques intencionados				
N.A.	N.A.	N.A.	Corrupción de datos	Ausencia formal para la supervisión de registro de SGSI	N.A.	N.A.	N.A.

Fuente: MinTIC, Taller "Más seguridad, mejor región" (2019, pág. 113). https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

En la Tabla 4, se observa como muestra, la aplicación del formato diseñado para la identificación de amenazas y vulnerabilidades de activos de TI en los macroprocesos misionales de la Gobernación del Huila, y en el Anexo 3 “Amenazas de activos de TI por macroprocesos”.

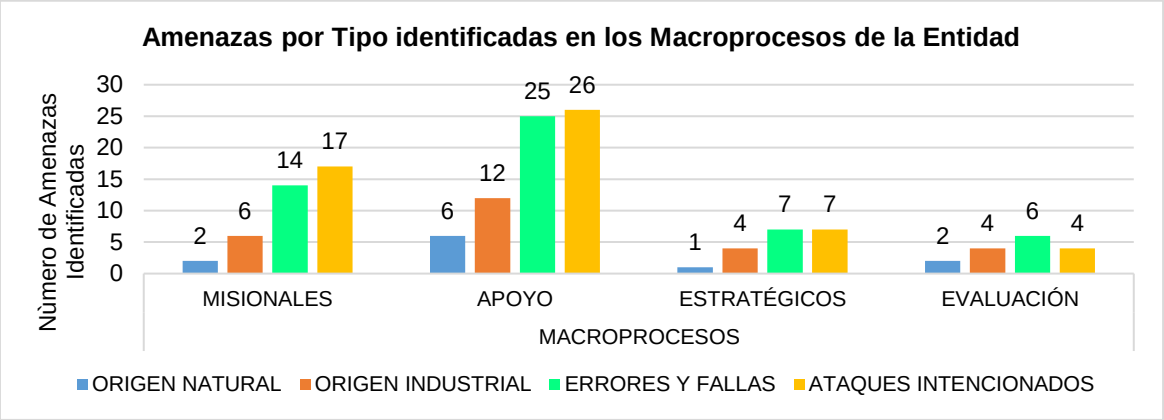
Tabla 4. Aplicación de Matriz de Identificación de Activos de Seguridad de la Información – Pasos 1, 7 y 8, en activos de Macroprocesos Misionales

PASOS							
1	7				8		
Activos de Seguridad de la Información asociados al proceso	Amenazas por activo				Causas / Vulnerabilidades		
	Naturales	Industriales	Errores	Ataques			
Sistema de Información Turística y Cultural del Huila turismo.huila.gov.co	N.A.	Daño de servidor de bases de datos del sistema de información	Alteración y destrucción accidental de la información	Modificación y destrucción deliberada de información	Fallas en servidor de base de datos del sistema de información	Falta de backup de la información y/o políticas de seguridad de la información	Falta de contratación de soporte técnico para el sistema de información
Información sobre novedades, experiencias, y formación del talento humano, para el uso y apropiación de TIC en entornos educativos	N.A.	N.A	Alteración accidental de la información	Modificación deliberada de la información	Desconocimiento de la información sobre experiencias	Uso incorrecto de software (registro adicional de participantes)	N.A
Estadísticas uso del espacio y de los libros	N.A.	N.A.	Alteración accidental de la información	Modificación deliberada de la información	Falta de backup de la información	Falta de políticas de seguridad de la información	N.A.

Fuente: Elaboración propia

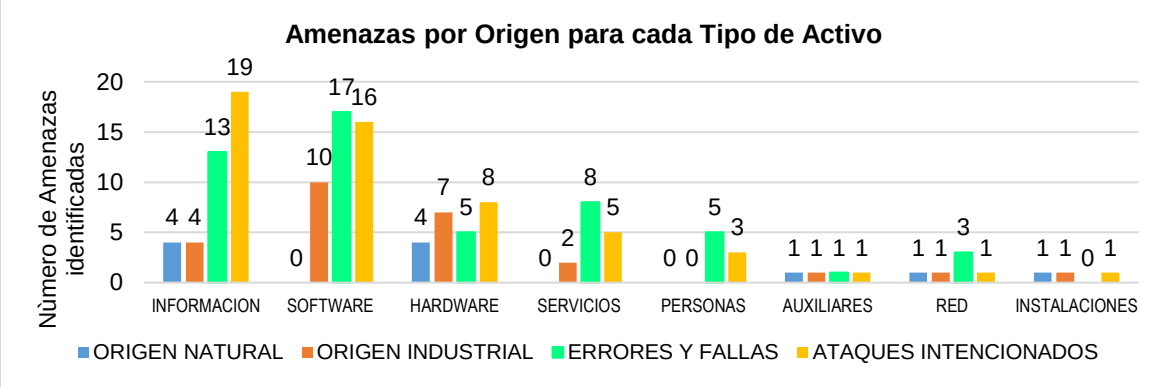
A partir de la Figura 15, en la que se observan las amenazas identificadas según su origen en los macroprocesos después de la aplicación del formato anterior, y de la Figura 16, en la que se observan las amenazas originadas según el tipo de activo que afectan, se obtiene que en la entidad los activos de tipo *información* se encuentran expuestos en mayor medida a amenazas originadas por *ataques intencionados* y los activos de tipo software se encuentran expuestos a amenazas originadas por *errores y fallas* humanas.

Figura 15. Amenazas por origen identificadas para cada macroproceso de la entidad



Fuente: Elaboración propia

Figura 16. Amenazas por origen identificadas para cada tipo de activo



Fuente: Elaboración propia

Lo anterior indica que la entidad se encuentra expuesta a amenazas que pueden configurar potenciales incidentes relacionados con seguridad de la información, y sacar provecho del ineficiente uso, gestión, apropiación y aseguramiento de los activos de TI por parte del talento humano de la entidad, entre otras vulnerabilidades existentes. Por lo tanto, es necesario fortalecer los conocimientos y competencias de los funcionarios en materia de seguridad y privacidad de la información, de acuerdo con sus roles y responsabilidades, y en el uso y gestión de las diferentes herramientas y activos de TI, para disminuir la probabilidad de ocurrencia de eventos como acceso no autorizado a sistemas e información, alteración accidental y/o modificación deliberada de información, etc.

Además, es importante tener en cuenta las amenazas de *origen industrial* en la entidad, ya que en éstas se incluyen daños y fallas ocasionados por deficiencias en infraestructura física dispuesta para archivar información en medio físico, de varias áreas y dependencias de la entidad, ya sea por no contar con espacio suficiente o por espacios en condiciones inadecuadas para albergar y resguardar este tipo de información.

Así mismo, y según lo expuesto en la Tabla 5, es posible observar que las amenazas cuyo origen radica en ataques intencionados afectan a todo tipo de activos en la Gobernación del Huila, resaltando que los que más pueden llegar a verse afectados por este tipo de amenazas son los activos de tipo Servicios. Esto, teniendo en cuenta que, a pesar de ser una menor cantidad, son dependientes de otros activos (hardware, software, información, personas), para poder tener los niveles de disponibilidad necesarios.

Tabla 5. Amenazas detectadas para cada tipo de activo según su origen

AMENAZAS DETECTADAS PARA CADA TIPO DE ACTIVO SEGÚN SU ORIGEN				
Tipo de Activo	**Origen de la Amenaza**			
	Natural	**Industrial**	**Errores y Fallas**	**Ataques Intencionados**
INFORMACIÓN (12 tipos de amenazas)	• Plagas y roedores. • Daños por lluvias, inundaciones y/o desastres naturales.	• Averías de origen físico o lógico. • Daños por actividades humanas.	• Diligenciamiento erróneo de información. • Destrucción accidental de la información. • Alteración accidental de la información.	• Modificación deliberada de información. • Destrucción deliberada de la información. • Software malicioso. • Suplantación de identidad del usuario. • Acceso no autorizado.
SOFTWARE (15 tipos de amenazas)	No aplica.	• Avería de origen físico o lógico • Mal funcionamiento del sistema. • Daño de servidor de bases de datos del sistema de información. • Vulnerabilidades del licenciamiento del software.	• Alteración accidental de la información • Destrucción accidental de la información • Diligenciamiento erróneo de la información. • Error de uso, mantenimiento, y actualización del sistema. • Error del administrador de servidor. • Error del administrador del licenciamiento del software.	• Modificación deliberada de la información. • Destrucción deliberada de información. • Manipulación con software. • Abuso de privilegios de acceso. • Uso no previsto.

AMENAZAS DETECTADAS PARA CADA TIPO DE ACTIVO SEGÚN SU ORIGEN				
Tipo de Activo	**Origen de la Amenaza**			
	Natural	**Industrial**	**Errores y Fallas**	**Ataques Intencionados**
HARDWARE (11 tipos de amenazas)	• Daños por desastres naturales, polvo, humedad, inundación, fuego, etc.	• Daños por mal uso o manipulación indebida • Daños debido a actividad humana	• Errores de mantenimiento o actualización de hardware • Errores de administración del servidor • Errores en mantenimiento de CCTV	• Acceso no autorizado. • Uso no previsto. • Incumplimiento en el mantenimiento del servidor. • Abuso de privilegios de acceso. • Daño o hurto de CCTV
COMPONENTES DE RED (8 tipos de amenazas)	• Daños por desastres naturales, polvo, humedad, inundación, fuego, etc.	• Daños por mal uso o manipulación indebida • Daños por actividades humanas.	• Error en el uso, configuración, y administración de equipos de red (switches, firewall, routers, etc.). • Errores en la instalación. • Falla de switches, routers, y access point.	• Acceso no autorizado. • Uso no previsto.
PERSONAS (7 tipos de amenazas)	No aplica.	No aplica.	• Indisponibilidad y/o ausencia del personal por accidentes. • Personal no idóneo frente al manejo de las herramientas tecnológicas del área. • Errores de usuarios y de gestión del servicio. • Ausencia de control del personal.	• Incumplimiento del personal en labores y obligaciones del personal. • Abuso sobre derechos y permisos de acceso a herramientas tecnológicas. • Repudio de solicitud de servicio.
SERVICIOS (15 tipos de amenazas)	No aplica	• Incumplimiento en el mantenimiento de sistema que soporta el servicio • Avería de origen físico o lógico del servidor • Mal funcionamiento del software	• Error en el uso, configuración, y administración de servicios • Errores de mantenimiento y actualización de programas (software) • Fugas de información • Alteración accidental de la información • Error de administrador de servidor de correo electrónico	• Abuso de privilegios de acceso • Uso no previsto • Acceso no autorizado • Suplantación de identidad del usuario • Repudio de solicitud de servicio • Falsificación de la información en validación de firmas o “apostillaje” • Modificación deliberada de la información
EQUIPOS AUXILIARES (5 tipos de amenazas)	• Daños por desastres naturales, polvo, humedad, inundación, fuego, etc.	• Daños por mal uso o manipulación indebida	• Error en el uso, configuración, y administración de UPS	• Acceso no autorizado • Uso no previsto

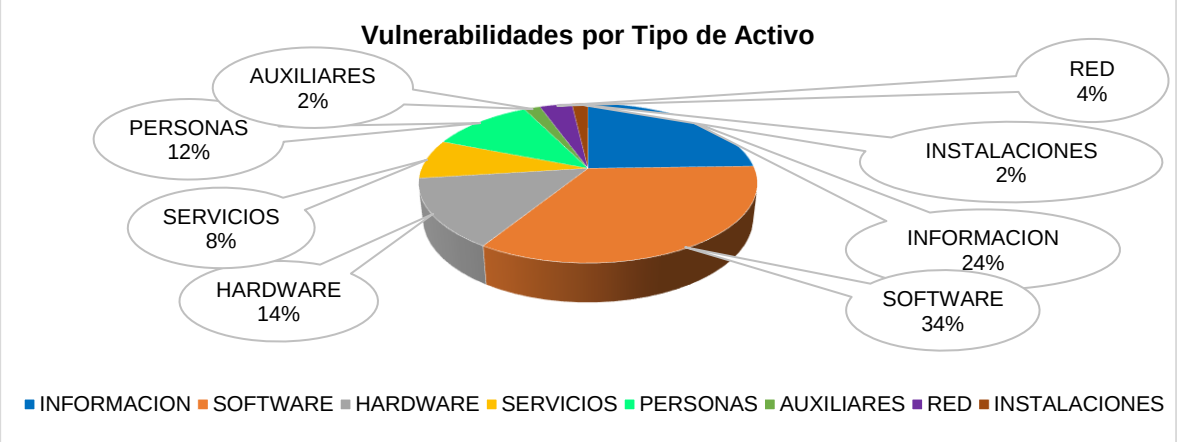
Fuente: Elaboración propia

Es importante resaltar que, de la prestación de servicios de TI, depende la prestación de varios servicios misionales de la entidad, sino todos, por lo que trasciende la importancia de identificar y analizar con detalle las posibles amenazas que afectan no solo los servicios de TI, sino a todos los activos de TI que los soportan.

5.2.2. Vulnerabilidades o posibles causas detectadas

De acuerdo con lo indicado en la Figura 17 y en el Anexo 4 “Vulnerabilidades de activos de TI por macroproceso”, los activos de tipo *software* y de tipo *información* son los que más presentan vulnerabilidades o posibles causas que permitan la materialización de riesgos, las cuales están relacionadas principalmente con la ausencia de conocimientos del personal en seguridad y privacidad de la información, fallas de sistemas de información, falta de respaldo de información, gestión ineficiente de credenciales de acceso a sistemas de información, entre otras.

Figura 17. Vulnerabilidades identificadas por cada tipo de activo



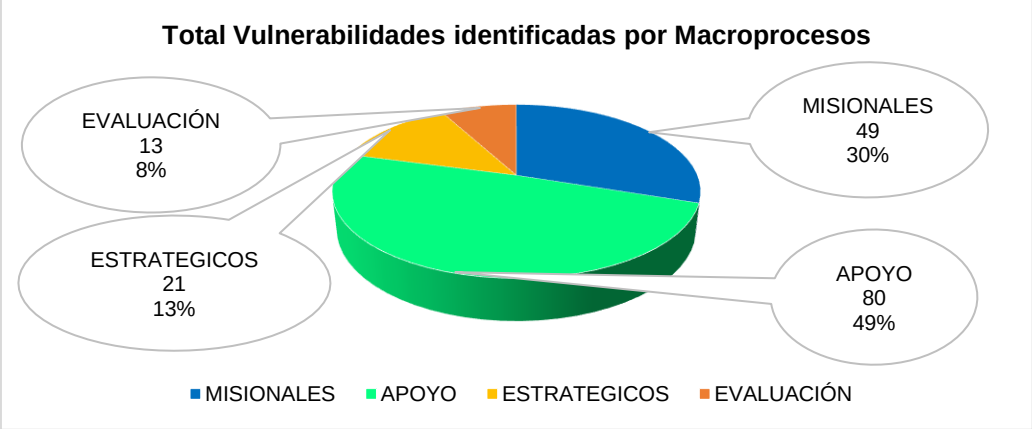
Fuente: Elaboración propia

Lo anterior, complementa uno de los planteamientos establecidos en el análisis de amenazas, incrementando la probabilidad de eventos asociados a la pérdida del aseguramiento de la información y de los sistemas que la gestionan, generando la necesidad de controles que van de la mano primordialmente con el mejoramiento de las competencias y conocimientos de los colaboradores y talento humano, en gestión y seguridad de las herramientas y servicios de TI disponibles, y que buscan disminuir tanto

vulnerabilidades presentes en sistemas de información (activos de tipo *software*), como vulnerabilidades que afectan también la información gestionada en ellos (activos de tipo *información*), y éstas deben ser tratadas efectivamente para evitar materialización de riesgos por amenazas relacionadas.

Además de lo anterior, y teniendo en cuenta lo expuesto en la Figura 18, los activos de tipo *software* de los macroprocesos de apoyo concentran la mayoría de vulnerabilidades identificadas de la entidad, ya que los sistemas de información, aplicativos y herramientas que en estos procesos se gestionan son utilizados por gran parte del resto de procesos, y así mismo presentan debilidades cuya explotación puede generar indisponibilidad en la prestación de servicios internos a las demás áreas, e interrupción de procesos y de servicios a la ciudadanía.

Figura 18. Vulnerabilidades identificadas por macroprocesos

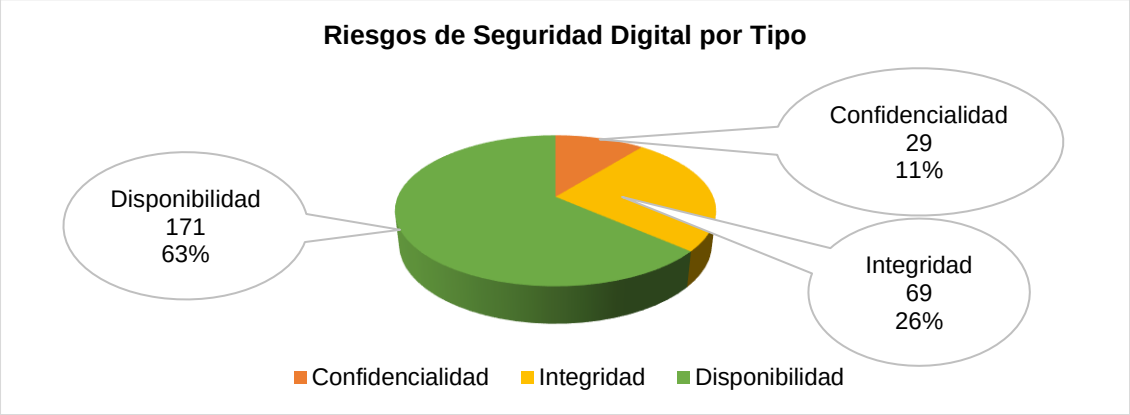


Fuente: Elaboración propia

5.2.3. Identificación de Riesgos de Seguridad de la Información

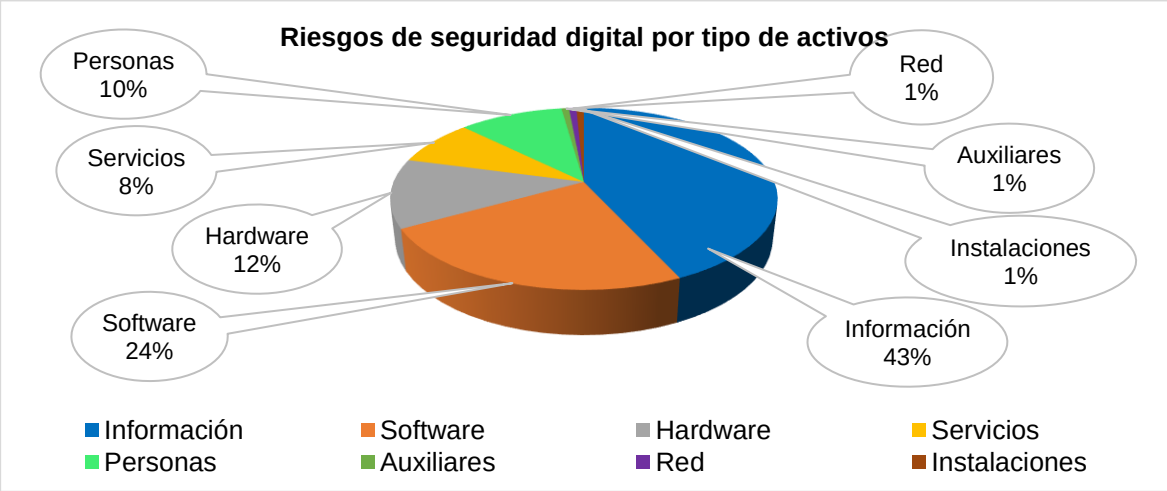
A partir de las de amenazas y vulnerabilidades asociadas a los activos de TI, se aplica el formato establecido por la entidad para identificar y valorar riesgos de Seguridad de la Información, identificando 269 riesgos, y discriminados según el tipo de riesgo, los activos y los macroprocesos afectados, como se observa en las Figuras 19, 20, y 21, respectivamente, y en el Anexo 5 “Riesgos de seguridad de la información por macroprocesos”.

Figura 19. Riesgos de Seguridad de la Información identificados en la entidad según el tipo



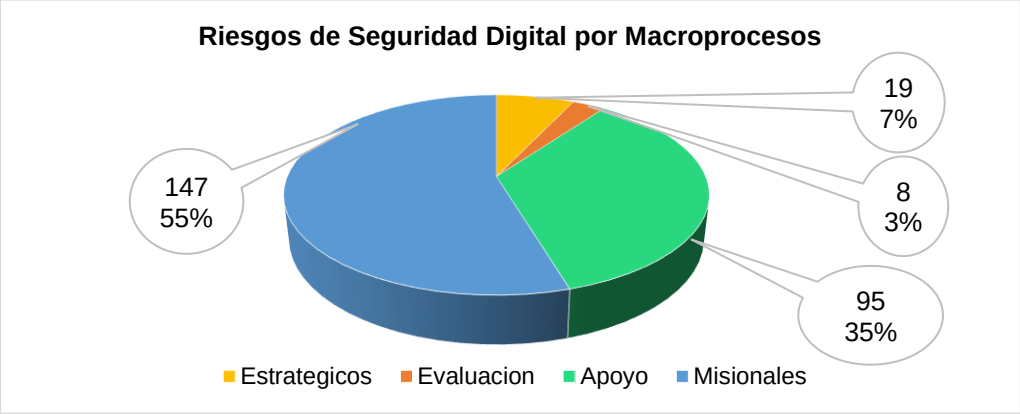
Fuente: Elaboración propia

Figura 20. Riesgos de Seguridad de la Información en la entidad por tipo de activos



Fuente: Elaboración propia

Figura 21. Riesgos de Seguridad de la Información identificados por macroprocesos



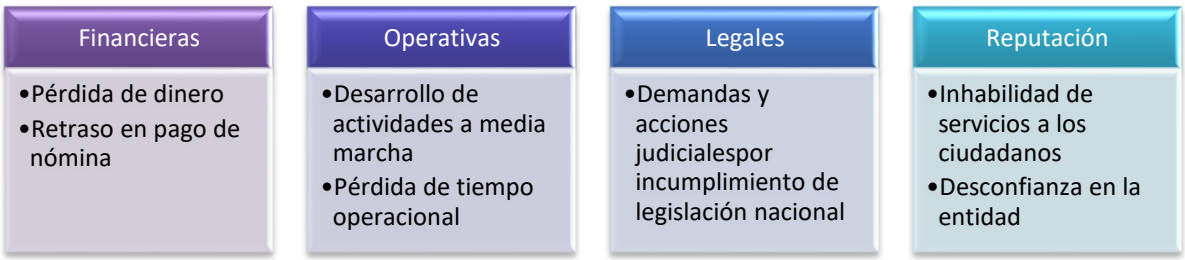
Fuente: Elaboración propia

De acuerdo con lo anterior, y teniendo como base los riesgos identificados en toda la entidad, es posible establecer que la pérdida de disponibilidad de información en macroprocesos misionales corresponde a la tipología de riesgo que más se presenta en la entidad. Esto indica que activos como información de gestión de los procesos, bases de datos gestionadas en hojas de cálculo, y alojadas en servidores de la entidad, entre otros, tienen mayor probabilidad de que se vean afectados por eventos que interrumpan su disponibilidad para el desarrollo de actividades y servicios misionales.

5.2.3.1. Consecuencias

Para cada uno de los riesgos identificados, se identifican posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputación, confianza en el ciudadano). Para esto, la Gobernación del Huila estableció el formato "*Matriz de Identificación y Valoración de Riesgos*" para generar, tanto su procedimiento de identificación y análisis de riesgos en cada uno de los procesos de gestión, como la identificación de consecuencias para cada riesgo identificado

Figura 22. Ejemplos de Consecuencias de materialización de riesgos de seguridad

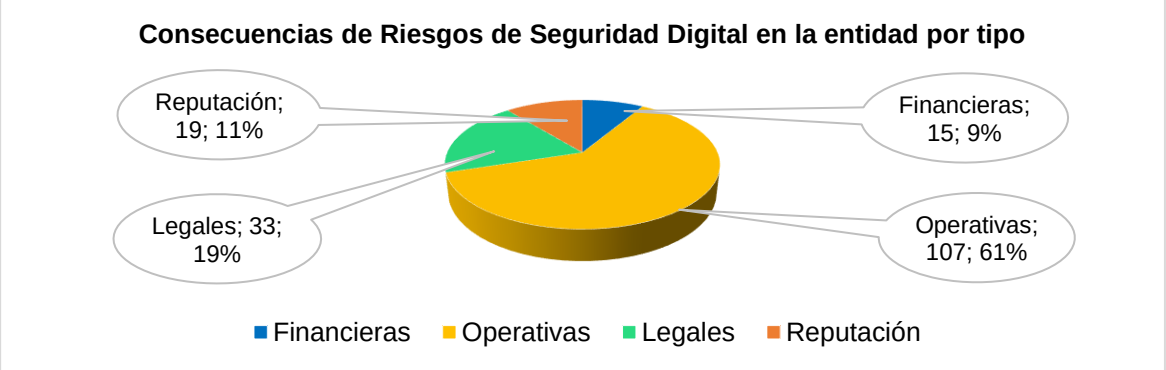


Fuente: MinTIC, Taller "Más seguridad, mejor región" (2019, pág. 113).
https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

Como se observa en las Figuras 23 y 24, en la entidad fueron identificadas un total de 174 consecuencias para los 269 riesgos de seguridad de la información identificados, destacándose las consecuencias de tipo operativo de los riesgos que afectan las actividades y servicios de carácter misional, entre las que se encuentran afectaciones en sectores productivos por la ejecución de proyectos de inversión sin planificación; proyección y asignación imprecisa de recursos en proyectos de inversión y servicios

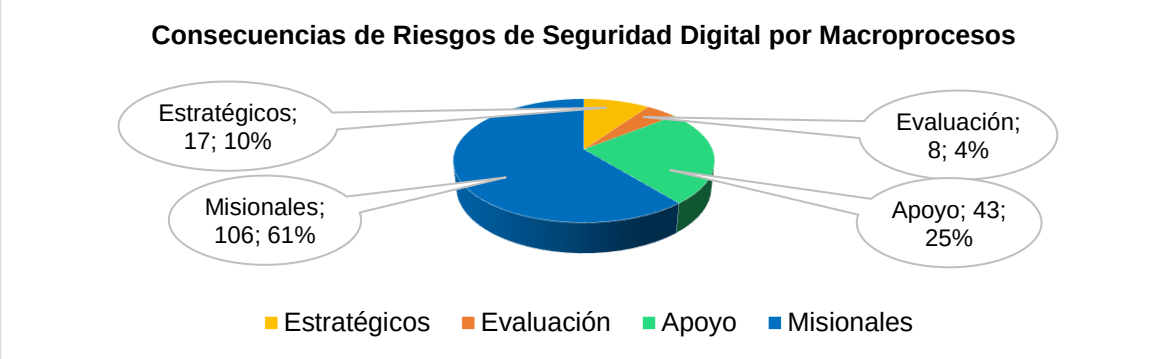
públicos esenciales bajo la responsabilidad del Estado, debido a información imprecisa de los habitantes; y la disminución de capacidades estatales a nivel regional para preservar la seguridad, la convivencia, el orden público, el respeto a los derechos humanos, la atención y prevención de emergencias y desastres.

Figura 23. Consecuencias de Riesgos de Seguridad de la Información identificados por tipo



Fuente: Elaboración propia

Figura 24. Consecuencias de Riesgos de Seguridad de la Información por macroproceso



Fuente: Elaboración propia

Igualmente se identificaron las consecuencias de tipo legal, principalmente en procesos misionales, siendo algunas de ellas: procesos judiciales por falsificación de documento público; procesos por incumplimiento en implementación de las acciones de planes de mejoramiento; investigaciones fiscales y disciplinarias, y acciones legales contra la entidad y sus funcionarios por afectaciones sobre la salud de pacientes, y sobre la financiación para prestación de servicios educativos; entre otras.

Las consecuencias identificadas relacionadas con la afectación de la reputación de la entidad están vinculadas con deficiencias en la gestión pública y rendición de cuentas de cara a la ciudadanía, por bajos resultados de eficiencia en la utilización de recursos públicos y por consiguiente, la pérdida de imagen y credibilidad de cada una de las áreas y dependencias encargadas, y en general de la Gobernación del Huila.

Por último, las consecuencias de tipo financiero identificadas son producto de los riesgos que afectan principalmente las actividades y procedimientos relacionados con la gestión de recursos financieros de la entidad, y que están a cargo de la Secretaría de Hacienda Departamental, como inconsistencias entre el presupuesto y las proyecciones financieras, lo que a su vez genera demoras en la ejecución del presupuesto; y pérdidas de recursos financieros, derivadas de disminución del recaudo de impuestos, por riesgos asociados a las bases de datos y documentación relacionada con los contribuyentes, etc.

5.2.4. Valoración de Riesgos de Seguridad de la Información

5.2.4.1. Nivel de riesgo inherente

Posterior a la identificación de los riesgos de Seguridad de la Información, sus causas y consecuencias, se procede con la valoración del nivel de riesgo inherente a partir de la valoración de la probabilidad de ocurrencia y el impacto de los riesgos identificados, para cada uno de los procesos de gestión de la Gobernación del Huila, aplicando el formato establecido por la entidad para la identificación y valoración de Riesgos.

- **Valoración de probabilidad:** La probabilidad del riesgo indica qué tan posible es que ocurra el riesgo, expresándose en términos de frecuencia, analizando el número de eventos en un periodo determinado, de hechos que se han materializado, o un historial de situaciones o eventos asociados al riesgo, si se cuenta con ello; o en términos de factibilidad, analizando factores internos y externos que pueden propiciar el riesgo, o hechos que no se han presentado, pero es posible que sucedan. Para este caso, se utiliza la escala de valoración de probabilidad de ocurrencia publicada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas (Función Pública, 2018), que está incluida en el formato "*Matriz de Identificación y Valoración de Riesgos*".

Figura 25. Valoración de la probabilidad de ocurrencia de riesgos de seguridad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
2	Improbable	Es poco probable que el evento ocurra en algún momento	Al menos 1 vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años

Fuente: MinTIC, Taller "Más seguridad, mejor región" (2019, pág. 116).
https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

- **Valoración de impacto:** El impacto se analiza y califica a partir de las consecuencias identificadas en la fase de descripción del riesgo. En el formato "*Matriz de Identificación y Valoración de Riesgos*" está incluido, dentro del procedimiento de identificación y análisis de riesgos en cada uno de los procesos de gestión, la evaluación del nivel de impacto para cada riesgo identificado.

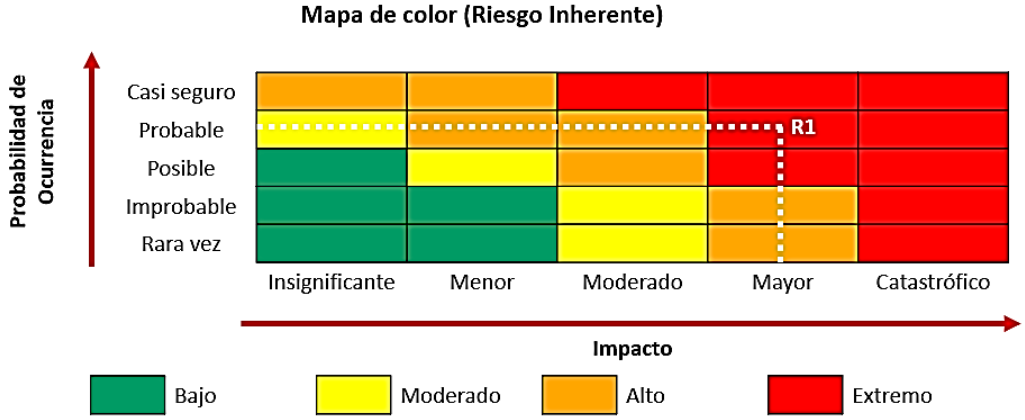
- **Determinación de riesgo inherente:** Posteriormente se procede con la identificación de los riesgos inherentes o subyacentes que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso, en base a la calificación de probabilidad resultante del paso anterior, y la calificación del nivel de impacto, aplicando mapa de color para la valoración del nivel de riesgo inherente, según el punto de intersección entre el nivel de probabilidad y de impacto. En el formato "*Matriz de Identificación y Valoración de Riesgos*" (Ver Tabla 6. Matriz de Identificación y Valoración de Riesgos – Fase 1: Identificación de Riesgos; y Tabla 7. Matriz de Identificación y Valoración de Riesgos – Fase 2: Valoración de Riesgos) se incluyó, dentro del procedimiento de identificación y análisis de riesgos en cada uno de los procesos de gestión, la determinación del riesgo inherente de seguridad, en base a la probabilidad y el nivel de impacto identificado.

Figura 26. Valoración del nivel de impacto de riesgos de seguridad

NIVEL	VALOR DE IMPACTO	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
Insignificante	1	Afectación en un valor menor al 1% de la población Afectación en un valor menor al 1% del presupuesto de la entidad No hay afectación medioambiental	Sin afectación de la integridad Sin afectación de la disponibilidad Sin afectación de la confidencialidad
Menor	2	Afectación en un valor igual o mayor al 1% y menor al 10%de la población Afectación en un valor igual o mayor al 1% y menor al 10% del presupuesto de la entidad Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación	Afectación leve de la integridad Afectación leve de la disponibilidad Afectación leve de la confidencialidad
Moderado	3	Afectación en un valor igual o mayor al 10% y menor al 20% de la población Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto de seguridad de la información en la entidad Afectación leve del medio ambiente requiere de 3 meses a 1 año de recuperación	Afectación moderada de la integridad Afectación moderada de la disponibilidad Afectación moderada de la confidencialidad
Mayor	4	Afectación en un valor igual o mayor al 20% e inferior al 50% de la población Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto de la entidad Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación	Afectación grave de la integridad Afectación grave de la disponibilidad Afectación grave de la confidencialidad
Catastrófico	5	Afectación en un valor igual o superior al 50%de la población Afectación en un valor igual o superior al 50% del presupuesto de la entidad. Afectación muy grave del medio ambiente que requiere > 3 años de recuperación	Afectación muy grave de la integridad Afectación muy grave de la disponibilidad Afectación muy grave de la confidencialidad

Fuente: MinTIC, Taller “Más seguridad, mejor región” (2019, pág. 119).
https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

Figura 27. Valoración del nivel de riesgo inherente de seguridad



Fuente: MinTIC, Taller “Más seguridad, mejor región” (2019, pág. 121).
https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

Tabla 6. Matriz de Identificación y Valoración de Riesgos – Fase 1: Identificación de Riesgos

FASE 1: IDENTIFICACIÓN DE RIESGOS							
ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos)		IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 /1.4)				ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1)	
No. De Riesgo	NOMBRE DEL PROCESO	IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida)	CLASIFICACIÓN DEL RIESGO (Gestión, Corrupción o Seguridad Digital)	TIPOLOGÍA DEL RIESGO	NIVEL DE DECISIÓN DEL RIESGO	CAUSA GENERADORA DEL RIESGO	CONSECUENCIAS DEL RIESGO
7	Gestión de la inspección y vigilancia de los establecimientos educativos	Pérdida de integridad de información pública clasificada y servicios al ciudadano del proceso	seguridad digital	Otros	Directivo y profesional	Cambios de personal directivo docente, generando falta de continuidad de lineamientos directivos y de gobierno en los establecimientos educativos	Incumplimiento en la entrega de informes de gestión a la secretaria de educación y ministerio
						Cambios normativos frecuentes en todos los procesos, generando desactualización permanente	Retrasos en la generación de actos administrativos
						Modificación de firmas, adulteración y expedición ilegal de documentos	Posible apertura de proceso disciplinario por incumplimiento en la implementación de las acciones de planes de mejoramiento
						Enfermedades de origen laboral	Incumplimiento en la entrega de informes de gestión a ministerio
8	Gestión de la inspección y vigilancia de los establecimientos educativos	Pérdida de disponibilidad de servicios, herramientas tecnológicas e información pública clasificada del proceso	seguridad digital	Otros	Nivel Directivo	Demora en la aplicación de los cambios de los procesos y documentos	Incumplimiento del plan anual de visitas de inspección y vigilancia
						Cambio del administrador del portal web	Retrasos en la publicación de actos administrativos

Fuente: Matriz de Identificación, Tratamiento y Seguimiento de Riesgos de Seguridad Digital, Gobernación del Huila. (2021). https://extranet.huila.gov.co/Site.aspx?Codigo=07DA00A4-CD98-435F-BF5E-97CAE8D8C520&p=/Descarga&ID=3814

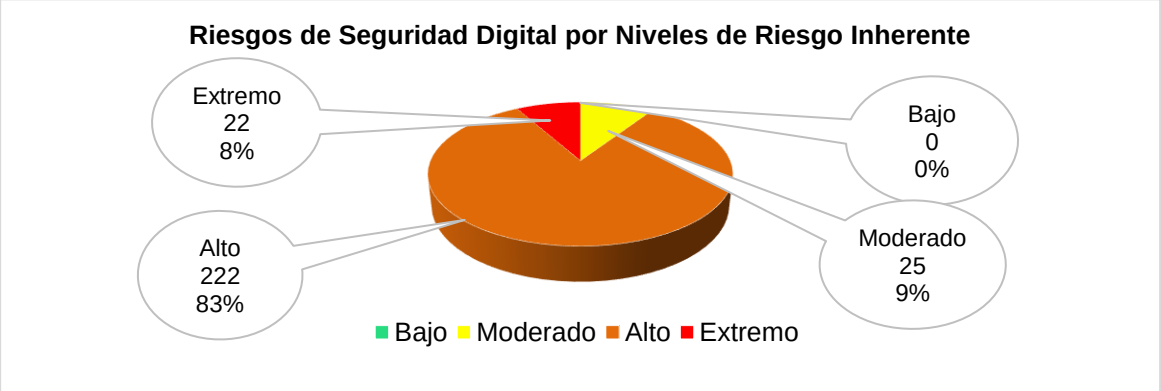
Tabla 7. Matriz de Identificación y Valoración de Riesgos – Fase 2: Valoración de Riesgos

FASE 2: VALORACIÓN DE RIESGOS																																			
ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente)														VALORACIÓN DE CONTROLES EXISTENTES (Ver hoja 3. Evaluación de controles)								EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual)													
PROBABILIDAD (ver hoja 2.1)					IMPACTO (ver hoja 2.1)					NIVEL DEL RIESGO INHERENTE												PROBABILIDAD (ver hoja 2.1)					IMPACTO (ver hoja 2.1)					NIVEL DEL RIESGO RESIDUAL			
Rara vez	Improbable	Posible	Probable	Casi seguro	Insignificante	Menor	Moderado	Mayor	Catastrófico	Extremo	Alto	Moderado	Bajo	¿Tiene Control? (Ver Hoja 3. Evaluación de controles)	Calificación del diseño del control	Calificación de la ejecución del control	Solidez individual del control:	Peso en la evaluación del diseño del control	CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	Controles ayudan a disminuir la probabilidad: Directamente o No disminuye?	¿Controles ayudan a disminuir el impacto? Directa o Indirectamente o No disminuye?	Rara vez	Improbable	Posible	Probable	Casi seguro	Insignificante	Menor	Moderado	Mayor	Catastrófico	Extremo	Alto	Moderado	Bajo
1	2	3	4	5	1	2	3	4	5						Fuerte (96-100) Moderado (86-95) Débil (0-85)	Fuerte: Siempre se ejecuta Moderado: Algunas veces se ejecuta Débil: No se ejecuta	Fuerte = 100 Moderado=50 Débil=0	SI=100 NO=0				1	2	3	4	5	1	2	3	4	5				
5					4					Extremo				No	Sin contro				Moderado	Directamente	Indirectamente	3					2					Moderado			
														No	Sin contro																				
														Si	Moderado	Fuerte	Moderado	Si																	
														No	Sin contro																				
														No	Sin contro																				
														No	Sin contro																				
														No	Sin contro																				
														No	Sin contro																				
4					4					Extremo				No	Sin contro				Débil	No disminuye	No disminuye	4					4					Extremo			
														No	Sin contro																				
														No	Sin contro																				
														No	Sin contro																				
														No	Sin contro																				
														No	Sin contro																				
														Si	Débil	Fuerte	Débil	Si																	

Fuente: Matriz de Identificación, Tratamiento y Seguimiento de Riesgos de Seguridad Digital, Gobernación del Huila. (2021).. https://extranet.huila.gov.co/Site.aspx?Codigo=07DA00A4-CD98-435F-BF5E-97CAE8D8C520&p=/Descarga&ID=3814

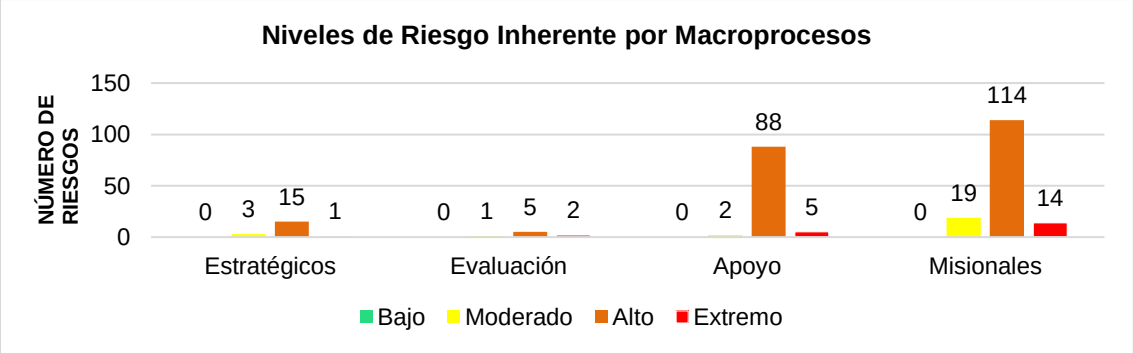
Como resultado de este proceso, y en se valoraron los 269 riesgos de Seguridad de la Información identificados, obteniendo según se muestra en la Figura 28 y en la Figura 29, que predominan los riesgos inherentes de nivel Alto, que afectan los macroprocesos misionales.

Figura 28. Valoración del nivel de riesgo inherente para riesgos de Seguridad de la Información



Fuente: Elaboración propia

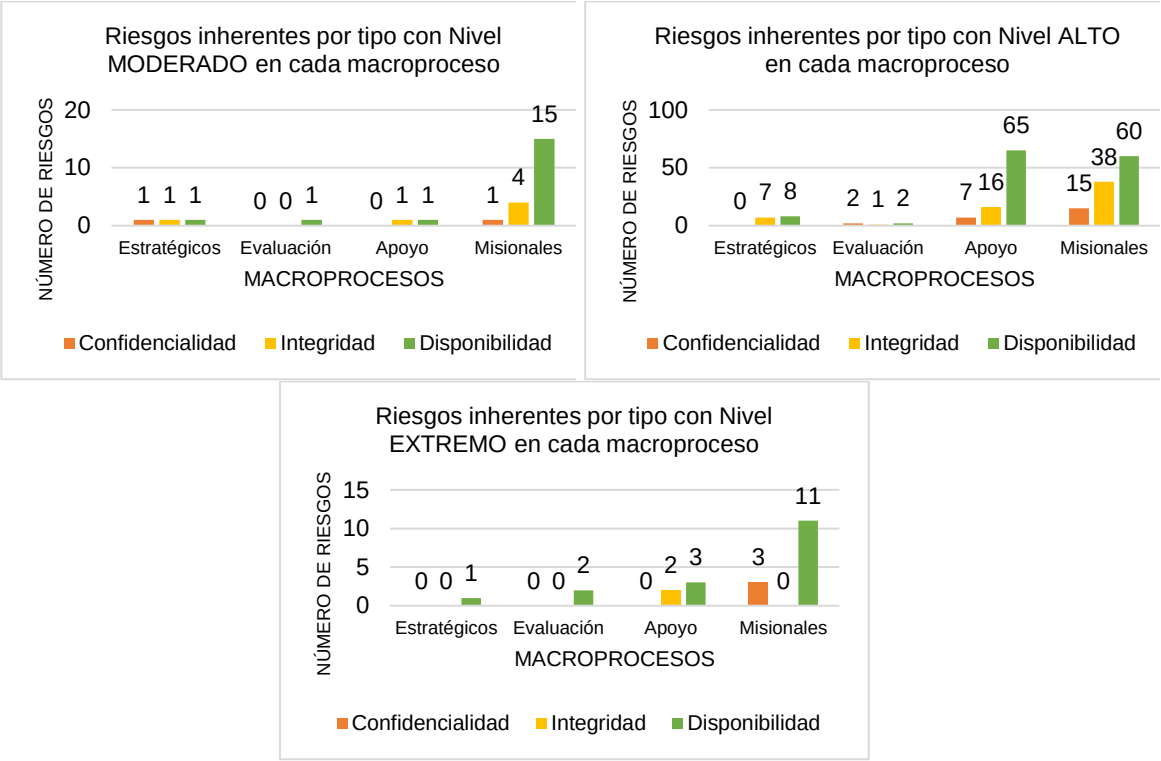
Figura 29. Valoración del nivel de riesgo inherente por macroprocesos



Fuente: Elaboración propia

De la Figura 30, en la que se muestra los tipos de riesgos para cada nivel de riesgo inherente identificado en los macroprocesos de la entidad, se obtiene que los riesgos de nivel alto afectan principalmente la disponibilidad de activos tipo software, información, hardware y equipos en los macroprocesos de apoyo y misionales, siendo estos un gran porcentaje del total de riesgos de la Gobernación (46% que equivale a 125 riesgos).

Figura 30. Riesgos de Seguridad de Información por tipo para niveles de riesgo inherente



Fuente: Elaboración propia

Lo anterior implica la necesidad de priorizar la aplicación de controles sobre activos de estos macroprocesos, buscando continuidad en la operación de servicios TI, servicios al ciudadano y a diferentes grupos de interés, fortaleciendo el uso y apropiación de controles de acceso de usuarios a los sistemas y aplicaciones, documentando las acciones y prácticas para gestionar la capacidad de la infraestructura de TI, la seguridad de las redes de comunicaciones, los requerimientos para la adquisición, mantenimiento y soporte de sistemas de información, entre otros asociados a los activos afectados.

5.2.4.2. Identificación de controles existentes

Una vez establecidos y valorados los riesgos inherentes, se procede a identificar y evaluar controles existentes para evitar trabajo o costos innecesarios. En el caso de la Gobernación del Huila, se utiliza un formato denominado "*Matriz de Evaluación de Controles*", como se observa en la Tabla 8, para valorar el impacto de controles existentes en la mitigación de riesgos o en las condiciones que contribuyen a su materialización, e identificar el nivel de riesgo residual que se presenta después de su aplicación.

Tabla 8. Matriz de Evaluación de Controles Existentes para Riesgos

¿Tiene Control?	Causa	¿Tipo de Control? (Automático o Manual)	¿Responsable asignado a la ejecución del control?	Cargo del responsable de ejecutar el control o nombre del sistema o aplicación automático	Responsable con autoridad y segregación de funciones en la ejecución del control?	La periodicidad en la ejecución del control?	Tipo de periodicidad del control (diario, semanal, quincenal, trimestral, anual, etc.)	El propósito del control ayuda (causas) a:	Describa cuál es el propósito del control	Cómo se utiliza la actividad de control?	Cómo se realiza la actividad de control	Se investigan y resuelven oportunamente las observaciones o desviaciones?	Evidencia de la ejecución del control?	PUNTAJE TOTAL DE CONTROL	Resultado - Peso en la evaluación del diseño del control
			Asignado=15 No asignado=0		Adecuado=15 Inadecuado=0	Oportuna=15 Inoportuna=0		Prevenir=15 Detectar=10 Corregir = 0		Confiable=15 No confiable=0		SI=15 NO =0	Completa=10 Incompleta=5 No existe=0		Fuerte (96-100) Moderado (86-95) Débil (0-85)
Si	Falta de backup de la información del SIG MIPG	Manual	15	Proveedor Gerente SIG	15	15	diaria semestral	15	Salvaguardar y proteger la información del SIG	15	Copia y resguardo información del SIG mediante copia en disco externo propiedad del coordinador, y mediante copia de seguridad que genera el proveedor	15	10	**100**	**Fuerte**
Si	Falta de publicación oportuna de información del SG MIPG	Manual	15	Gerente SIG	15	15	semanal	0	Garantizar la publicación oportuna de información actualizada por los responsables de los procesos	0	Control de publicación de información mediante el formato "CONTROL INFORMACIÓN ENTREGADA Y SUBIDA A LA EXTRANET"	15	5	**65**	**Débil**

Fuente: Matriz de Identificación, Tratamiento y Seguimiento de Riesgos de Seguridad Digital, Libro 3. Evaluación de Controles para Riesgos de Seguridad Digital, Gobernación del Huila. (2021). https://extranet.huila.gov.co/Site.aspx?Codigo=07DA00A4-CD98-435F-BF5E-97CAE8D8C520&p=/Descarga&ID=3814

Sin embargo, para el caso de riesgos de Seguridad de la Información, y con el fin de analizar de manera precisa las acciones relacionadas, se utiliza el Instrumento de Evaluación del Modelo de Seguridad y Privacidad de la Información, provisto por el Ministerio TIC, para realizar seguimiento al nivel de madurez de la gestión de seguridad y privacidad de la información en toda la Gobernación del Huila.

En la evaluación de cada dominio de control, el nivel mínimo es *Inexistente*, en el que no se aplica ningún tipo de control, y el nivel máximo es *Optimizado*, en el que los procesos han sido redefinidos hasta el nivel de mejores prácticas, las cuales se siguen y automatizan, según resultados de una mejora continua, como se observa en la Tabla 9.

Tabla 9. Escala de Valoración de Controles según ISO 27001:2013 - Anexo A

Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: Elaboración a partir de Instrumento de Evaluación de MSPI (Ministerio TIC, s.f.) https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx

De esta forma, aplicando el instrumento, se obtiene la valoración de dominios de control, según lo establecido en el Anexo A de la norma técnica ISO/IEC 27001:2013, tal como se observa en la Tabla 10, y en el Anexo 6 “Controles existentes según Anexo A de NTC-ISO 27001”, verificando la existencia, operación y efectividad de controles.

Tabla 10. Valoración de Dominios de Control Administrativos y Técnicos en la entidad

Tipo	Dominios de Control	Valoración
ADMINISTRATIVOS	**Políticas de Seguridad de la Información**	**20**
	• Política General	20
	• Revisión y evaluación	20
	Organización de la Seguridad de la Información	**32**
	• Organización Interna	44
	• Dispositivos móviles y teletrabajo	20
	Seguridad de los recursos humanos	**16**
	• Responsabilidades de seguridad de la información antes del empleo	40
	• Durante el empleo	7
	• Al terminar el empleo	0
	Gestión de activos	**26**
	• Responsabilidad sobre activos	30
	• Clasificación de información	27
	• Manejo de medios de almacenamiento	20
	Seguridad de la información de la Gestión de la continuidad del negocio	**30**
	• Continuidad de la seguridad de la información	60
	• Redundancias	0
	Cumplimiento de la seguridad de la información	**25**
	• Cumplimiento de requisitos legales y contractuales	50
	• Revisiones de seguridad de la información	0
	Relaciones con proveedores	**0**
	• Seguridad de la información en las relaciones con los proveedores	0
	• Gestión de la prestación de servicios de proveedores	0
TÉCNICOS	**Control de Acceso**	**50**
	• Requisitos del negocio para control de acceso	60
	• Gestión de acceso a usuarios	47
	• Responsabilidades de los usuarios	60
	• Control de acceso a sistemas y aplicaciones	32
	Criptografía	**0**
	• Controles criptográficos	0
	Seguridad física y del entorno	**33**
	• Áreas seguras	33
	• Equipos	44
	Seguridad de las operaciones	**19**
	• Procedimientos operacionales y responsabilidades	45
	• Protección contra códigos maliciosos	40
	• Copias de respaldo	40
	• Registro y seguimiento	5
	• Control de software	0
	• Gestión a la vulnerabilidad	0
	• Consideraciones sobre auditorías de sistemas de información	0
	Seguridad de la Comunicaciones	**30**
	• Gestión de la seguridad de las redes	60
	• Transferencia de información	0
	Adquisición, mantenimiento y desarrollo de sistemas	**21**
	• Requisitos de seguridad de los sistemas de información	20
	• Seguridad en los procesos de desarrollo y soporte	4
	• Datos de prueba	40
	Gestión de incidentes de seguridad de la información	**60**
	• Gestión de incidentes y mejoras en la seguridad de la información	60
	PROMEDIO EVALUACIÓN DE CONTROLES	**26**

Fuente: Elaboración propia

A partir de esta valoración para cada dominio de control establecido en el Anexo A de la norma técnica NTC-ISO 27001:2013, el Instrumento de Evaluación del Modelo de Seguridad y Privacidad de la Información brinda una valoración promedio de efectividad de controles de 26/100, que corresponde a un nivel de madurez *Repetible* que significa según la escala del instrumento, que existe repetitividad en procesos y controles, sin formación o comunicación formal de procedimientos y estándares, confiando en conocimiento de cada persona, con probabilidad de errores.

Esto indica que, a pesar de contar con buenas prácticas adoptadas por la entidad, y documentación de políticas de TI que permiten cierto nivel de gestión de seguridad y de servicios TI, éstas no están actualizadas de acuerdo con la norma técnica, ni con los lineamientos del Ministerio TIC, ni alineadas a través de una política general que oriente la gestión de seguridad de la información en la Gobernación del Huila, y que asigne roles y responsabilidades. Además, no se cuenta con procedimientos y lineamientos para gestión del centro de datos y redes de datos, planificación y procedimientos de diagnóstico, mantenimiento y retiro de equipos de cómputo y hardware en general, adquisición, mantenimiento y soporte técnico de sistemas de información.

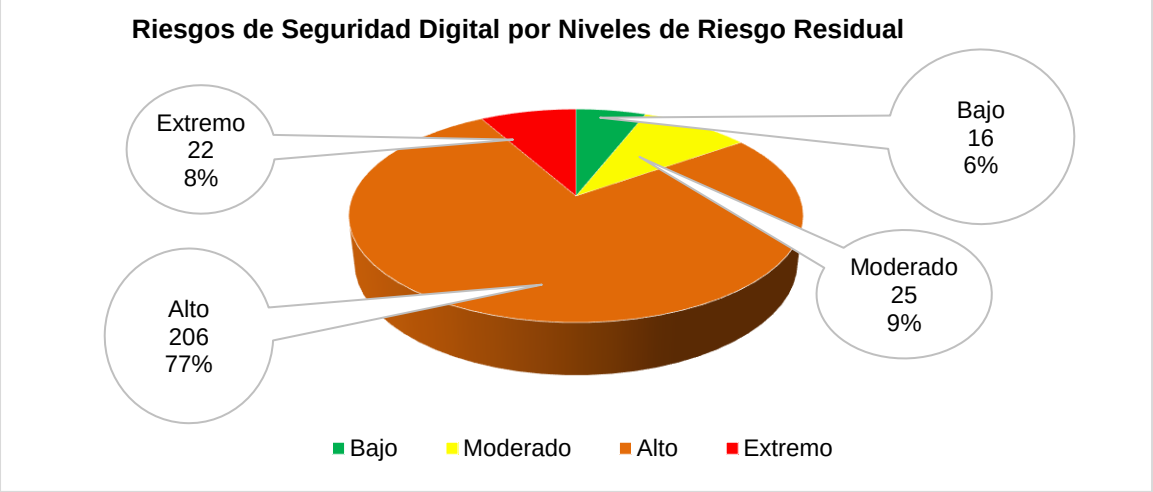
En el caso de controles asociados a redundancias y copias de respaldo, gestión de continuidad del negocio, contingencia ante desastres de TI y respuesta a incidentes, se cuenta con documentación asociada, sin verificación ni actualización con periodicidad suficiente para garantizar su efectividad ante un evento o incidente que se presente.

De los dominios mejor calificados, el control de acceso es uno de los de resaltar, teniendo en cuenta que las políticas relacionadas, aunque desactualizadas, se aplican sin novedad y se lleva registro y control de los usuarios que acceden a sistemas de información, apoyados además en ocasiones de procedimientos para el soporte técnico pertinente, o en otros de formatos que permiten los registros necesarios para tal fin. Otro aspecto para resaltar es la protección contra software malicioso que se implementa en la Gobernación del Huila, al renovar de manera bianual el licenciamiento de antivirus y antimalware, así como la implementación de restricciones y principios de mínimo privilegio aplicados en el acceso a servicios de red e instalación de software.

5.2.4.3. Nivel de riesgo residual

Una vez identificados los controles de seguridad de la información existentes en la entidad, y que están mitigando los riesgos analizados, se procede con la valoración del nivel de riesgo residual, producto de la implementación de estos controles, y como afectan la probabilidad de ocurrencia e impacto sobre los riesgos inherentes, en cada uno de los procesos de gestión de la Gobernación del Huila, aplicando el formato establecido por la entidad para la identificación y valoración de riesgos. Como resultado de este proceso, y en desarrollo del segundo objetivo específico, se obtuvo de los 269 riesgos identificados, 206 en nivel de riesgo Alto, 25 en nivel de riesgo Moderado, 22 en nivel de riesgo Extremo, y 16 en nivel de riesgo bajo (Ver Figura 31).

Figura 31. Valoración de nivel de riesgo residual para Riesgos de Seguridad de Información

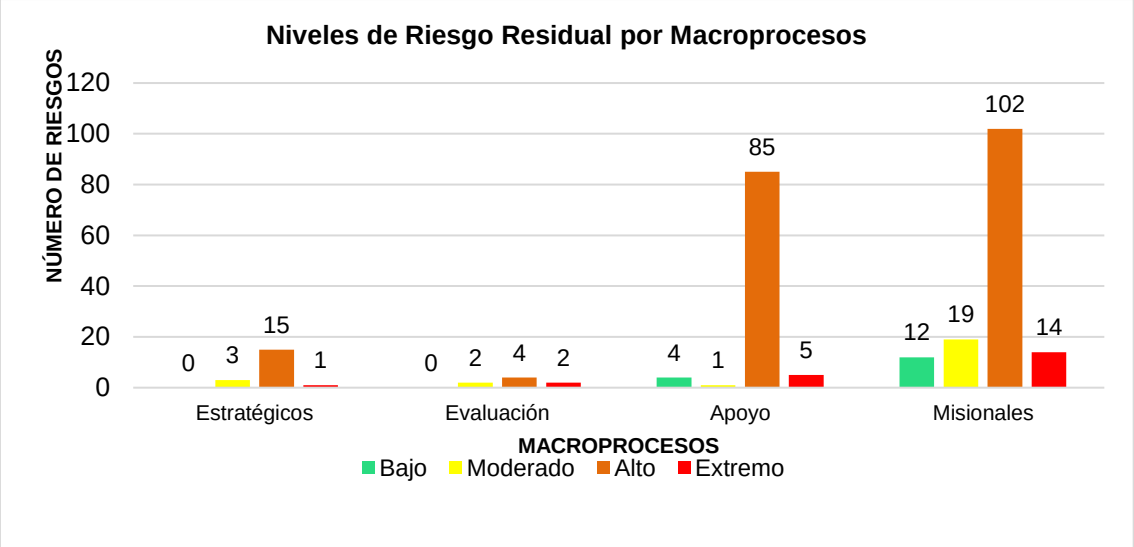


Fuente: Elaboración propia

Respecto a los riesgos inherentes identificados, se identifica una reducción de riesgos en nivel alto, pasando de 222 a 206 riesgos, y un incremento en los riesgos en nivel bajo, pasando de 0 a 16, lo cual indica un leve impacto de los controles actuales en la mitigación, sin lograr una efectividad importante, ya que se mantienen los riesgos en nivel extremo (22), en nivel moderado (25), y la reducción en nivel alto es muy baja.

Así mismo, según lo dispuesto en la Figura 32 y en la Figura 33, la disminución de riesgos de nivel alto a partir de los controles existentes y aplicados por la entidad permite mejorar la disponibilidad de activos, especialmente tipo hardware en macroprocesos misionales, y de tipo información y de tipo servicios en macroprocesos de apoyo.

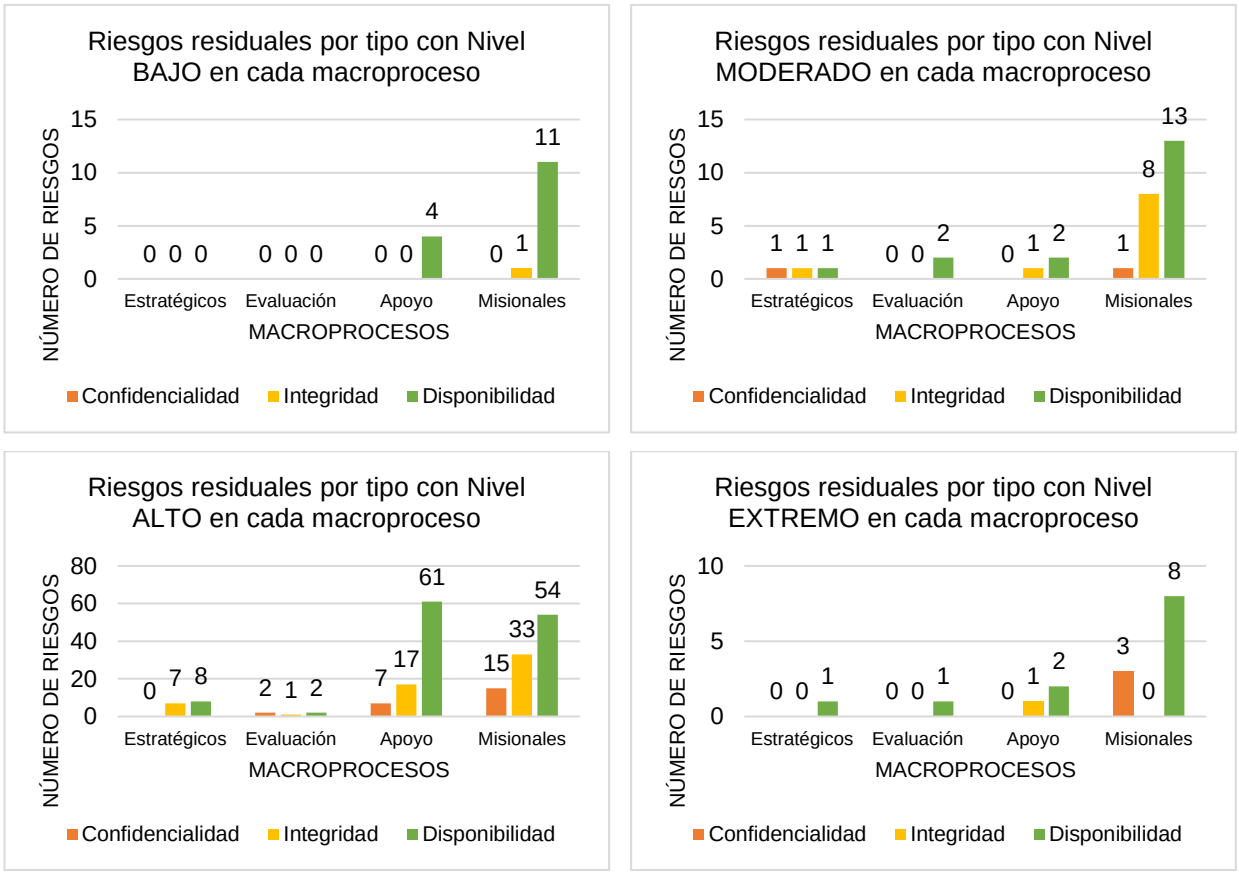
Figura 32. Valoración del nivel de riesgo residual identificados por macroprocesos



Fuente: Elaboración propia

Los controles que mostraron efectividad fueron los referentes a mantenimiento de equipos de cómputo en algunas dependencias, ya que en otras el nivel de obsolescencia es mayor (Participación Comunitaria, Control Interno de Gestión, Vías e Infraestructura, Cobertura Educativa, Talento Humano, entre otras), y por tanto el mantenimiento realizado no es suficiente para mejorar la funcionalidad de los equipos, ni la eficiencia de las actividades, procesos y servicios que allí se prestan, y por consiguiente el riesgo residual sigue siendo alto en estos casos.

Figura 33. Riesgos de Seguridad de Información por tipo para cada nivel de riesgo residual



Fuente: Elaboración propia

Además, el porcentaje de riesgos de nivel alto y extremo que afecta la disponibilidad de estos activos sigue siendo muy alto respecto al total de riesgos (42%), por lo que es importante priorizar la aplicación de controles sobre los activos, que busquen garantizar la continuidad en la operación de servicios de TI, y por consiguiente de servicios al ciudadano y a los diferentes grupos de interés, tal como se indicó al analizar los riesgos inherentes.

5.3. Tratamiento de Riesgos

Una vez se han identificado los riesgos, se define el tratamiento para cada uno de los riesgos analizados y evaluados, involucrando una selección de opciones para modificarlos, entre las que se encuentran las siguientes: evitar, aceptar, compartir o reducir el riesgo (Gobernación del Huila, 2019, pág. 14).

Figura 34. Opciones de Tratamiento de Riesgos

Fuente: MinTIC, Taller “Más seguridad, mejor región” (2019, pág. 130). https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

En base a esto, se establecen las estrategias de tratamiento, determinadas en la Política de Operación para la Administración de Riesgos de la Gobernación del Huila (2019, pág. 13), y sobre las cuales se definen acciones que permitan el cumplimiento de dicha estrategia (Ver Tabla 11. Estrategias de Tratamiento de Riesgos)

Tabla 11. Estrategias de Tratamiento de Riesgos de Seguridad de la Información

Zona de Riesgo	Estrategia de Tratamiento en la Gobernación del Huila
Baja	Se ACEPTA el riesgo y se administra por medio de las actividades propias del proceso o proyecto asociado y se realiza en el reporte mensual de su desempeño.
Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad o el impacto de ocurrencia del riesgo, se hace seguimiento BIMESTRAL y se realizan acciones para su tratamiento, registran sus avances en la matriz de seguimiento de Riesgos - SGI
Alta y Extrema	Se debe incluir el riesgo tanto en el mapa como en la matriz consolidada de riesgo y se establecen acciones de control preventivas que permitan EVITAR la materialización del riesgo. Se monitorea MENSUALMENTE y se registra en la matriz de seguimiento de Riesgos

Fuente: Matriz de Identificación, Tratamiento y Seguimiento de Riesgos de Seguridad Digital, Libro 2. Criterios para valorar Riesgos de Seguridad Digital, Gobernación del Huila. (2021). https://extranet.huila.gov.co/Site.aspx?Codigo=07DA00A4-CD98-435F-BF5E-97CAE8D8C520&p=/Descarga&ID=3814

Actualmente la entidad dispone de la Matriz de Identificación y Valoración de Riesgos para incluir allí las acciones de tratamiento y seguimiento de riesgos no controlados de gestión, corrupción, y de seguridad y privacidad de la información (Ver Tabla 12. Matriz de Identificación y Valoración de Riesgos – Fase 3: Tratamiento y Seguimiento de Riesgos). Sin embargo, en el caso de Riesgos de Seguridad y Privacidad de la Información, el modelo establecido del Ministerio TIC sugiere utilizar para ello el Anexo A de la norma técnica ISO/IEC 27001:2013, con el fin de seleccionar controles y establecer las actividades a aplicar sobre los riesgos residuales identificados (Ver Tabla 13. Esquema de Tratamiento de Riesgos de Seguridad de la Información del Ministerio TIC).

Tabla 12. Matriz de Identificación y Valoración de Riesgos de Seguridad de la Información – Fase 3: Tratamiento y Seguimiento de Riesgos

FASE 3: TRATAMIENTO Y SEGUIMIENTO									
POLÍTICAS Y OPCIONES DE TRATAMIENTO DEL RIESGO	REQUIERE PLAN DE TRATAMIENTO	PLAN DE TRATAMIENTO OBLITATORIO PARA LOS RIESGOS NO CONTROLADOS							
		ACCIÓN A IMPLEMENTAR	F - INCIIO	F - FIN	RESPONSABLE DE LA ACCIÓN	F- SEGUIMIENTO	EVIDENCIA O SOPORTE	SEGUIMIENTO DESCRIPCIÓN	PORCENTAJE DE AVANCE

Fuente: Matriz de Identificación, Tratamiento y Seguimiento de Riesgos de Seguridad Digital, Gobernación del Huila. (2021). https://extranet.huila.gov.co/Site.aspx?Codigo=07DA00A4-CD98-435F-BF5E-97CAE8D8C520&p=/Descarga&ID=3814

Tabla 13. Esquema de Tratamiento de Riesgos de Seguridad de la Información del Ministerio TIC

Opción de Tratamiento	Actividad de Control	Soporte	Responsable	Tiempo
Seleccionar entre **Aceptar, Reducir, Evitar o Compartir**	Indicar **Objetivo de Control** a aplicar según ISO 27001 Anexo A (P.E. 9.4.3. Sistema de Gestión de Contraseñas)	**Entregable o evidencia** de aplicación del Objetivo de Control (P.E. Procedimiento de gestión de contraseñas)	**Área, Oficina o Dependencia encargada** de la aplicación del Objetivo de Control (P.E. Oficina de Tecnología)	**Tiempo estimado** de ejecución del objetivo de control

Fuente: MinTIC, Taller “Más seguridad, mejor región” (2019, pág. 131). https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

Teniendo en cuenta dicha situación, en la Tabla 14 se muestra el formato diseñado para la planificación del tratamiento de riesgos de seguridad y privacidad de la información, que se adapte a la matriz existente, y que permita la diferenciación entre el control seleccionado y la acción de control establecida para mitigación del riesgo residual.

Tabla 14. Diseño de Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la Gobernación del Huila

Opción de Tratamiento	Objetivo de Control	Actividad Para Implementar	Evidencia o Soporte	Responsable	Fecha de Inicio	Fecha de Término	Fecha de Seguimiento	Descripción de Seguimiento	Porcentaje de Avance
Seleccionar entre **Aceptar, Reducir o Evitar**	Indicar **Objetivo de Control** a aplicar según ISO 27001 Anexo A (P.E. 9.4.3. Sistema de Gestión de Contraseñas)	**Descripción breve de la actividad de aplicación** del objetivo de control (P.E. Documentar, Publicar e Implementar Procedimiento de gestión de contraseñas)	**Entregable o evidencia** de aplicación del Objetivo de Control (P.E. Procedimiento de gestión de contraseñas)	**Área u Oficina encargada** de la aplicación del Objetivo de Control (P.E. Oficina de Tecnología)	**Fecha de inicio** de diseño o construcción del objetivo de control	**Fecha de entrega** del diseño o construcción del objetivo de control	**Fecha establecida para seguimiento** al diseño o construcción del objetivo de control	**Descripción breve de la actividad de seguimiento** establecida para aplicar el objetivo de control	**Porcentaje de avance en la fecha de seguimiento** del diseño o construcción del objetivo de control

Fuente: MinTIC, Taller “Más seguridad, mejor región” (2019, pág. 131). https://estrategia.gobiernoenlinea.gov.co/623/articles-102189_recurso_7.pdf

Aplicando el formato diseñado, y en cumplimiento del 3er objetivo específico del presente proyecto, se establece el plan de tratamiento para los riesgos no controlados de seguridad y privacidad de la información, para cada uno de los procesos de gestión de la Gobernación del Huila, basados en el análisis y valoración de riesgos realizados previamente, y diferenciando entre el control seleccionado para su aplicación y la actividad de control establecida para el tratamiento del riesgo residual, de los cuales se observan algunos en la Tablas 15, 16, 17 y 18, y la totalidad de ellos en el Anexo 7 “Planes de tratamiento de riesgos de Seguridad de la Información para cada proceso de la Gobernación del Huila”.

Igualmente, para facilitar la visualización de los controles seleccionados y las actividades a implementar para tratar los riesgos residuales, se ha establecido un *Plan Consolidado de Tratamiento de Riesgos de Seguridad de la Información*, como se observa en el Anexo 8 del presente documento.

Tabla 15. Plan de Tratamiento de Riesgos para el proceso misional "Atención al Ciudadano"

ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO		IDENTIFICACIÓN DEL RIESGO	ANÁLISIS DE CAUSAS Y CONSECUENCIAS		ANÁLISIS DEL RIESGO				EVALUACIÓN DEL RIESGO			
No. De Riesgo	NOMBRE DEL PROCESO	IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida)	CAUSA GENERADORA DEL RIESGO	CONSECUENCIAS DEL RIESGO	NIVEL DEL RIESGO INHERENTE				NIVEL DEL RIESGO RESIDUAL			
					Extremo	Alto	Moderado	Bajo	Extremo	Alto	Moderado	Bajo
1	Atención al ciudadano	PÉRDIDA DE CONFIDENCIALIDAD DE PQRSD RADICADOS EN LA ENTIDAD, ASÍ COMO DOCUMENTOS DE SALIDA E INTERNOS GENERADOS POR SERVIDORES PÚBLICOS	Falta de backup de la información Falta de políticas de seguridad de la información Errores en ingreso de información relacionada	Incumplimiento de términos de ley para las respuestas oportunas / Procesos disciplinarios / Seguimientos y/o Sanciones de entes de control / Baja calificación de percepción de ciudadano	Alto				Alto			
2	Atención al ciudadano	PÉRDIDA DE DISPONIBILIDAD DE REPORTES DE INDICADORES DE PQRSD	Falta de backup de la información Falta de políticas de seguridad de la información Errores en ingreso de información relacionada	Incumplimiento de términos de ley para las respuestas oportunas / Procesos disciplinarios / Seguimientos y/o Sanciones de entes de control / Baja calificación de percepción de ciudadano	Alto				Alto			
3	Atención al ciudadano	PÉRDIDA DE DISPONIBILIDAD DE SISTEMA EXTRANET (MÓDULO DE COMUNICACIONES OFICIALES)	Fallas en servidor extranet Falta de backup de la información Falta de políticas de seguridad de la información	Investigaciones, sanciones disciplinarias, pérdida de credibilidad e imagen institucional y afectación de la satisfacción del cliente	Alto				Alto			
4	Atención al ciudadano	PÉRDIDA DE DISPONIBILIDAD DE CORREO ELECTRÓNICO INSTITUCIONAL	Falta de sensibilización en seguridad de la información Suplantación de Identidad en Correo Electrónico (Phishing - Spam)	Incumplimiento de términos de ley para las respuestas oportunas / Seguimientos y/o Sanciones de entes de control / Baja calificación de percepción de ciudadano	Extremo				Extremo			
5	Atención al ciudadano	PÉRDIDA DE DISPONIBILIDAD DE EQUIPOS DE CÓMPUTO	Mantenimiento insuficiente Falta de políticas de seguridad de la información	Investigaciones, sanciones disciplinarias, pérdida de credibilidad e imagen institucional y afectación de la satisfacción del cliente	Moderado				Bajo			
6	Atención al ciudadano	PÉRDIDA DE DISPONIBILIDAD DE FUNCIONARIOS DE APOYO AL PROCESO	Ausencia del personal Falta de compromiso Falta de actualización del manual de funciones	Incumplimiento de términos de ley para las respuestas oportunas / Procesos disciplinarios / Seguimientos y/o Sanciones de entes de control / Baja calificación de percepción de ciudadano	Alto				Alto			

Fuente: Elaboración Propia

Continuación de Tabla 15. Plan de Tratamiento de Riesgos para el proceso misional "Atención al Ciudadano"

OPCIÓN DE TRATAMIENTO DEL RIESGO	REQUIERE PLAN DE TRATAMIENTO	PLAN DE TRATAMIENTO OBLIGATORIO PARA LOS RIESGOS NO CONTROLADOS								
		OBJETIVO DE CONTROL	ACTIVIDAD POR IMPLEMENTAR	EVIDENCIA O SOPORTE	RESPONSABLE DE LA ACTIVIDAD	F - INICIO	F - TÉRMINO	F- SEGUIMIENTO	DESCRIPCIÓN DE SEGUIMIENTO	PORCENTAJE DE AVANCE
REDUCIR	Si	A.12.3.1. Respaldo de Información	Actualizar e implementar políticas y procedimientos de respaldo de información	Políticas y procedimiento de respaldo de información	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
		N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
REDUCIR	Si	A.12.3.1. Respaldo de Información	Actualizar e implementar políticas y procedimientos de respaldo de información	Políticas y procedimiento de respaldo de información	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
		N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
REDUCIR	Si	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores	Establecer e implementar política de seguridad de la información en relaciones con proveedores, que incluya seguimiento y revisión de los servicios.	Política de seguridad de la información en relaciones con proveedores	Grupo de Tecnología	feb-21	dic-22	dic-22	N.A.	0%
		A.12.3.1. Respaldo de Información	Actualizar e implementar políticas y procedimientos de respaldo de información	Políticas y procedimiento de respaldo de información	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
REDUCIR	Si	A.7.2.2. Conciencia, educación y entrenamiento de seguridad de la información	Establecer, documentar e implementar Plan de capacitación y sensibilización en SPI y circulares internas	Plan de Capacitación y Sensibilización en SPI	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
		A.13.2.3. Mensajería Electrónica	Establecer, documentar e implementar políticas de uso del correo electrónico institucional	Políticas de uso del correo electrónico institucional	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
REDUCIR	Si	A.11.2.4. Mantenimiento de equipos	Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de equipos de cómputo	Plan de verificación y mantenimiento preventivo periódico de equipos de cómputo	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
REDUCIR	Si	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
		A.7.1.2. Términos y condiciones del empleo	Establecer procesos de verificación periódica de no duplicidad de funciones entre funcionarios de planta administrativa, contratistas y proveedores.	Certificado de Disponibilidad de Personal	Líder Talento Humano - Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
		N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.

Fuente: Elaboración Propia

Tabla 16. Plan de Tratamiento de Riesgos para el proceso de apoyo "Gestión de la Información Estadística y Cartográfica del Departamento del Huila"

ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO		IDENTIFICACIÓN DEL RIESGO	ANÁLISIS DE CAUSAS Y CONSECUENCIAS		ANÁLISIS DEL RIESGO				EVALUACIÓN DEL RIESGO			
					NIVEL DEL RIESGO INHERENTE				NIVEL DEL RIESGO RESIDUAL			
No. De Riesgo	NOMBRE DEL PROCESO	IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida)	CAUSA GENERADORA DEL RIESGO	CONSECUENCIAS DEL RIESGO	Extremo	Alto	Moderado	Bajo	Extremo	Alto	Moderado	Bajo
1	GESTION DE LA INFORMACIÒN ESTADISTICA Y CARTOGRÀFICA DEL DEPARTAMENTO DEL HUILA	PÉRDIDA DE DISPONBILIDAD DE SISTEMA DE INFORMACIÓN REGIONAL Y EQUIPOS DE CÓMPUTO	Ausencia formal para la supervisión de registro de SGSI	Inhabilitación de sistema de información y reacción a eventos de seguridad y contingencias	Extremo				Extremo			
			Uso incorrecto de software y hardware	Publicación de datos e información erróneos								
			Configuración incorrecta de parámetros	Inhabilidad de sistema de información								
			Almacenamiento sin protección	Acceso no autorizado a información clasificada								
			Mantenimiento insuficiente de equipos de cómputo	Dificultad en labores de administración de sistema de información y bases de datos								
			Ausencia de personal	Incumplimiento de funciones y obligaciones								
2	GESTION DE LA INFORMACIÒN ESTADISTICA Y CARTOGRÀFICA DEL DEPARTAMENTO DEL HUILA	PÉRDIDA DE INTEGRIDAD DE DATO	Ausencia formal para la supervisión de registro de SGSI	Hallazgos de los entes de control	Alto				Alto			
			Uso incorrecto de software y hardware	Deterioro de imagen institucional								

Fuente: Elaboración Propia

Continuación Tabla 16. Plan de Tratamiento de Riesgos para el proceso de apoyo "Gestión de Información Estadística y Cartográfica"

OPCIÓN DE TRATAMIENTO DEL RIESGO	REQUIERE PLAN DE TRATAMIENTO	PLAN DE TRATAMIENTO OBLIGATORIO PARA LOS RIESGOS NO CONTROLADOS								
		OBJETIVO DE CONTROL	ACTIVIDAD POR IMPLEMENTAR	EVIDENCIA O SOPORTE	RESPONSABLE DE LA ACTIVIDAD	F - INICIO	F - TÉRMINO	F- SEGUIMIENTO	DESCRIPCIÓN DE SEGUIMIENTO	PORCENTAJE DE AVANCE
REDUCIR	Si	**A.18.2.1. Revisión independiente de la seguridad de la información**	**Establecer, documentar e implementar planes de auditoría interna las políticas de SI**	Plan de Auditoría Interna y Cumplimiento de Indicadores de planes establecidos	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
		A.12.3.1. Respaldo de Información	**Actualizar e implementar políticas y procedimientos de respaldo de información**	Políticas y procedimiento de respaldo de información	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
		A.14.2.7. Desarrollo tercerizado	**Establecer, documentar e implementar políticas de desarrollo seguro de software**	Políticas de desarrollo seguro de software	Grupo de Tecnología	feb-21	dic-22	dic-22	N.A.	0%
		A.12.2.1. Controles contra software malicioso	**Adquirir y administrar aplicativo de protección contra software malicioso**	Contrato de compraventa y reportes de administración de aplicativo	Grupo de Tecnología	jun-21	dic-21	dic-21	N.A.	0%
		A.11.2.4. Mantenimiento de equipos	**Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de equipos de cómputo**	Plan de verificación y mantenimiento preventivo periódico de equipos de cómputo	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
		A.7.1.2. Términos y condiciones del empleo	**Establecer procesos de verificación periódica de no duplicidad de funciones entre funcionarios de planta administrativa, contratistas y proveedores.**	Certificado de Disponibilidad de Personal	Líder Talento Humano - Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
REDUCIR	Si	**A.18.2.1. Revisión independiente de la seguridad de la información**	**Establecer, documentar e implementar planes de auditoría interna las políticas de SI**	Plan de Auditoría Interna y Cumplimiento de Indicadores de planes establecidos	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
		A.12.3.1. Respaldo de Información	**Actualizar e implementar políticas y procedimientos de respaldo de información**	Políticas y procedimiento de respaldo de información	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%

Fuente: Elaboración Propia

Tabla 17. Plan de Tratamiento de Riesgos para el proceso estratégico "Gobernabilidad y Comunicación Pública"

ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO		IDENTIFICACIÓN DEL RIESGO	ANÁLISIS DE CAUSAS Y CONSECUENCIAS		ANÁLISIS DEL RIESGO				EVALUACIÓN DEL RIESGO			
					NIVEL DEL RIESGO INHERENTE				NIVEL DEL RIESGO RESIDUAL			
No. De Riesgo	NOMBRE DEL PROCESO	IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida)	CAUSA GENERADORA DEL RIESGO	CONSECUENCIAS DEL RIESGO	Extremo	Alto	Moderado	Bajo	Extremo	Alto	Moderado	Bajo
1	GOBERNABILIDAD Y COMUNICACIÓN PUBLICA	Pérdida de disponibilidad de página web y redes sociales corporativas de la entidad	Fallas en conectividad a internet	Deficiencia en la administración y actualización de página web y redes sociales			Alto				Alto	
			Falta de backup de la información	Desconocimiento de la gestión del Gobernante junto con la imagen institucional								
			Vulnerabilidades de página web que faciliten ataques externos	Explotación de vulnerabilidades por falta de *hardening*								
			Desconocimiento de procedimientos de gestión de claves para redes sociales	Desconocimiento de la gestión del Gobernante junto con la imagen institucional								
2	GOBERNABILIDAD Y COMUNICACIÓN PUBLICA	Pérdida de confidencialidad de la agenda general del Gobernador	Error en comunicación de la agenda	Disminución de la gestión institucional de la Gobernación			Moderado				Moderado	
			Cambios de la agenda a última hora	Pérdida de gobernabilidad credibilidad e Imagen Institucional.								
3	GOBERNABILIDAD Y COMUNICACIÓN PUBLICA	Pérdida de integridad de las bases de datos	Error en el diligenciamiento de la información en las bases de datos	Pérdida de gobernabilidad credibilidad e Imagen Institucional.			Alto				Alto	
			Errores en la edición de la información de los boletines	Pérdida de gobernabilidad credibilidad e Imagen Institucional.								
			Emisión y publicación no oportuna de los boletines	Desconocimiento de la gestión del Gobernante junto con la imagen institucional								
			Fallas en equipos tecnológicos y en red para generación de boletines	Pérdida de gobernabilidad credibilidad e Imagen Institucional.								

Fuente: Elaboración Propia

Continuación Tabla 17. Plan de Tratamiento de Riesgos para el proceso estratégico "Gobernabilidad y Comunicación Pública"

OPCIÓN DE TRATAMIENTO DEL RIESGO	REQUIERE PLAN DE TRATAMIENTO	PLAN DE TRATAMIENTO OBLIGATORIO PARA LOS RIESGOS NO CONTROLADOS								
		OBJETIVO DE CONTROL	ACTIVIDAD POR IMPLEMENTAR	EVIDENCIA O SOPORTE	RESPONSABLE DE LA ACTIVIDAD	F - INICIO	F - TÉRMINO	F- SEGUIMIENTO	DESCRIPCIÓN DE SEGUIMIENTO	PORCENTAJE DE AVANCE
REDUCIR	Si	A.15.2.1. Seguimiento y revisión de servicios de los proveedores	Establecer e implementar Política de seguridad de la información en las relaciones con el proveedor	Política de seguridad de la información en relaciones con proveedores	Grupo de Tecnología	feb-21	dic-22	dic-22	N.A.	0%
		A.12.3.1. Respaldo de Información	Actualizar e implementar políticas y procedimientos de respaldo de información	Políticas y procedimiento de respaldo de información	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
		A.12.6.1. Gestión de Vulnerabilidades Técnicas	Establecer, documentar e implementar procedimiento de gestión de vulnerabilidades técnicas para aplicativos web	Procedimiento de gestión de vulnerabilidades técnicas para aplicativos web	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
		A.9.4.3. Sistema de Gestión de Contraseñas	Establecer, documentar e Implementar política de control de contraseñas	Política de control de contraseñas	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
REDUCIR	Si	A.13.2.4. Acuerdos de confidencialidad o de no divulgación	Establecer, documentar e implementar acuerdos de confidencialidad en los procesos contractuales y de gestión de proyectos	Acuerdos de confidencialidad	Grupo de Tecnología	feb-21	dic-22	dic-22	N.A.	0%
		N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	0%
REDUCIR	Si	A.18.1.3 Protección de registros	Establecer, documentar e implementar procedimientos de protección de registros de información	Procedimiento de protección de registros de información	Grupo de Tecnología	feb-21	dic-22	dic-22	N.A.	0%
		A.12.1.2 Gestión de cambios	Establecer procedimiento de gestión de cambios en los procesos	Procedimiento de gestión de cambios	Grupo de Tecnología	feb-21	sep-23	sep-23	N.A.	0%
		N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
		A.11.2.4 Mantenimiento de equipos	Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de equipos de cómputo	Plan de verificación y mantenimiento preventivo periódico de equipos de cómputo	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%

Fuente: Elaboración Propia

Tabla 18. Plan de Tratamiento de Riesgos para el proceso de evaluación "Gestión de Control y Auditorías"

ESTABLECIMIENTO DEL CONTEXTO DONDE SE UBICA EL RIESGO (ver hojas 1.1. análisis de contexto y 1.2. Identificación activos)		IDENTIFICACIÓN DEL RIESGO (Gestión o Corrupción o Seguridad Digital) (Ver Hojas 1.1 / 1.2 / 1.3 /1.4)	ANÁLISIS DE CAUSAS Y CONSECUENCIAS (Gestión, Corrupción y seguridad digital) (Ver hoja 1.1)		ANÁLISIS PRELIMINAR DEL RIESGO (Riesgo inherente)				EVALUACIÓN DEL RIESGO VS CONTROLES (Riesgo residual)			
No. De Riesgo	NOMBRE DEL PROCESO	IDENTIFICACIÓN DEL RIESGO (Implica incertidumbre y pérdida)	CAUSA GENERADORA DEL RIESGO	CONSECUENCIAS DEL RIESGO	NIVEL DEL RIESGO INHERENTE				NIVEL DEL RIESGO RESIDUAL			
					Extremo	Alto	Moderado	Bajo	Extremo	Alto	Moderado	Bajo
1	GESTIÓN DE CONTROL Y AUDITORÍAS	PÉRDIDA DE DISPONIBILIDAD DE LA INFORMACIÓN DE EVALUACIÓN Y SEGUIMIENTO A LA GESTIÓN Y DE PLANES DE MEJORAMIENTO POR PROCESOS DE LA ENTIDAD	Uso incorrecto de software y hardware	Hallazgos de los entes de control	Extremo				Alto			
			Mantenimiento insuficiente de equipos de cómputo	Deterioro de imagen institucional								
			Ausencia de personal	Incumplimiento de funciones y obligaciones								

OPCIÓN DE TRATAMIENTO DEL RIESGO	REQUIERE PLAN DE TRATAMIENTO	PLAN DE TRATAMIENTO OBLIGATORIO PARA LOS RIESGOS NO CONTROLADOS								
		OBJETIVO DE CONTROL	ACTIVIDAD POR IMPLEMENTAR	EVIDENCIA O SOPORTE	RESPONSABLE DE LA ACTIVIDAD	F - INICIO	F - TÉRMINO	F- SEGUIMIENTO	DESCRIPCIÓN DE SEGUIMIENTO	PORCENTAJE DE AVANCE
REDUCIR	Si	A.7.1.1. Verificación de antecedentes	Elaborar e implementar procedimiento de verificación de autenticidad de documentos presentados por aspirantes a un cargo dentro de la entidad	Procedimiento de verificación de autenticidad de documentos	Talento Humano	feb-21	dic-21	dic-21	N.A.	0%
		A.11.2.4. Mantenimiento de equipos	Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de equipos de cómputo	Plan de verificación y mantenimiento preventivo periódico de equipos de cómputo	Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%
		A.7.1.2. Términos y condiciones del empleo	Establecer procesos de verificación periódica de no duplicidad de funciones entre funcionarios de planta administrativa, contratistas y proveedores.	Certificado de Disponibilidad de Personal	Líder Talento Humano - Grupo de Tecnología	feb-21	dic-21	dic-21	N.A.	0%

Fuente: Elaboración Propia

6. Modelo de Gestión de Seguridad y Privacidad de la Información diseñado para la Gobernación del Huila

El diseño del Modelo de Gestión de Seguridad y Privacidad de la Información para la Gobernación del Huila se realiza teniendo en cuenta la revisión de los diferentes modelos identificados en el marco teórico del presente documento, así como también los resultados del diagnóstico de activos de TI, del análisis y valoración de riesgos de seguridad de la información, y de la identificación de controles existentes en el marco del tratamiento de riesgos de seguridad de la información.

Así las cosas, el modelo se plantea a partir de categorías de gestión de seguridad y privacidad de la información, de forma que se alineen en un ciclo PHVA y que establezcan acciones de diagnóstico, planificación e implementación de controles, articulándose con el Plan Estratégico de Tecnologías de la Información -PETI- establecido en la entidad.

6.1. Categorías de Gestión de Seguridad y Privacidad de la Información

Como se observa en la Figura 35, el Modelo de Gestión de Seguridad y Privacidad de la Información propuesto para la Gobernación del Huila está conformado por las siguientes siete categorías de gestión:

Figura 35. Categorías del Modelo de Gestión de Seguridad y Privacidad de la Información de la Gobernación del Huila

Fuente: Elaboración propia

- **Planes de seguridad y principales políticas específicas de TI**

Tiene como finalidad documentar y actualizar los planes concernientes a cada fase de operación del modelo, principalmente la fase de planificación, para definir las acciones y herramientas que permitirán a la entidad gestionar la seguridad y privacidad de la información, registrando y consolidando sus resultados. Esto, teniendo en cuenta que estos planes deben estar alineados a los objetivos misionales, y definiendo su alcance a partir del enfoque por procesos de la entidad, y por consiguiente del impacto de los procesos y activos de TI en la estrategia institucional.

- **Contingencia, recuperación de desastres y continuidad del negocio**

Esta categoría abarca la documentación y establecimiento de planes y controles que permiten dar continuidad a los servicios de la entidad, desde la gestión de incidentes de seguridad de la información, aplicación de medidas de recuperación y contingencia ante un evento que comprometa y/o afecte la confidencialidad, integridad, y/o disponibilidad de los activos de TI la entidad.

- **Control de activos de TI (perímetros de seguridad, protección de activos de TI, mantenimiento)**

Abarca el establecimiento de lineamientos de buen uso y control de acceso a activos de TI, para su apropiación por parte del talento humano de la entidad, según sus roles y responsabilidades en materia de gestión de seguridad y privacidad de la información, disminuyendo de esta forma disminuir las vulnerabilidades y mitigando los riesgos asociados.

- **Privacidad y tratamiento de datos personales**

Incluye las políticas y medidas para el tratamiento de datos personales gestionados por la entidad, y su reporte y declaración de uso, finalidad, y medidas establecidas para garantizar el uso aceptable y autorizado de éstos, ante las autoridades competentes.

- **Adquisición y/o desarrollo de licenciamiento, software, y sistemas de información**

Esta categoría contiene las acciones y controles relacionados con la gestión de la seguridad en procesos de adquisición, desarrollo, verificación y seguimiento del licenciamiento de software y sistemas de información en la entidad, y en las relaciones con sus proveedores.

- **Seguridad de redes y servicios de red**

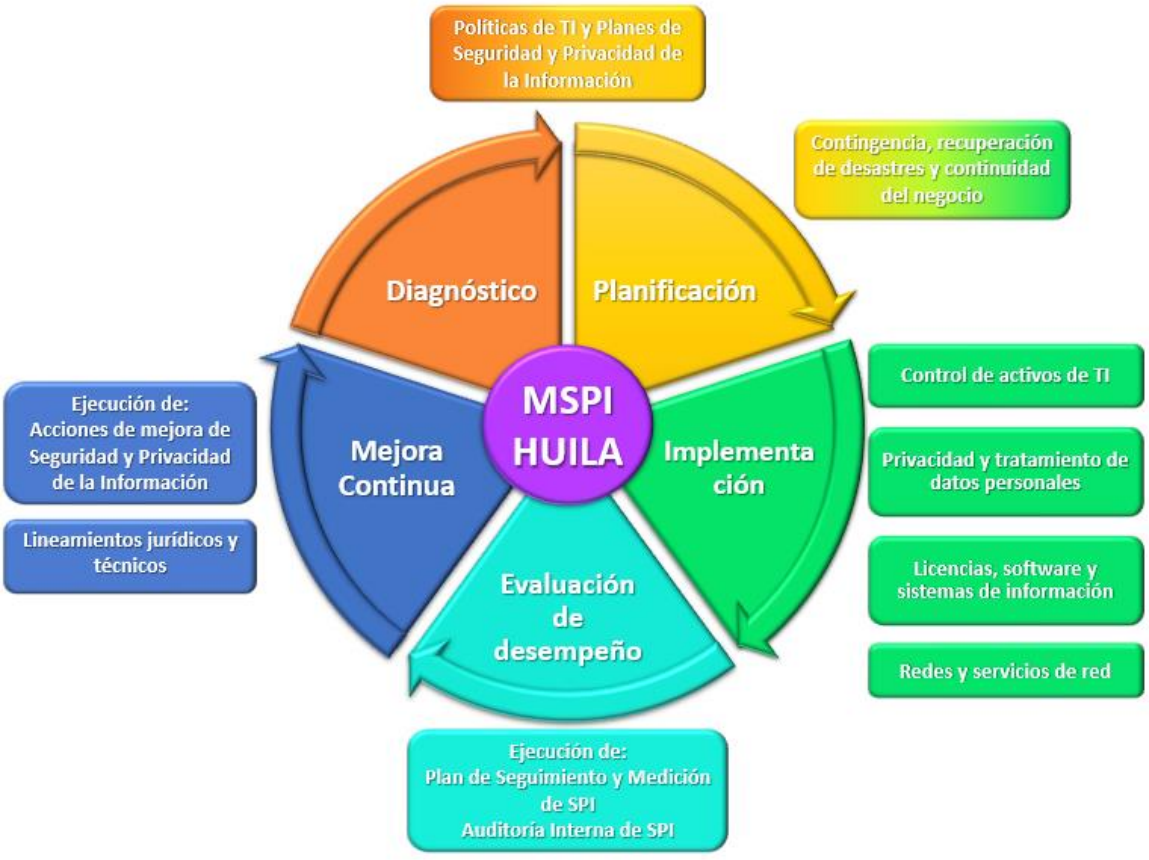
Comprende las políticas, procedimientos y en general, las acciones establecidas para garantizar la transferencia segura de información a través de las redes de comunicaciones, asegurando así los servicios de red de la entidad.

- **Lineamientos jurídicos y técnicos de seguridad de la información**

En esta categoría se incluyen las acciones asociadas a la revisión y actualización de las políticas de TI y elementos estratégicos de ésta, y de los lineamientos jurídicos y procesos de control interno disciplinario dirigido al talento humano, relacionados con la seguridad y la privacidad de la información.

Estas categorías de gestión permiten interpretar e identificar las actividades a documentar e implementar en el desarrollo de cada una de las fases del modelo propuesto, actividades que se asocian al cumplimiento de uno o más objetivos de control establecidos, así como también a la legislación y reglamentación que ha sido determinada por las entidades regulatorias del sector (Ministerio TIC, Departamento de Función Pública).

Figura 36. Ciclo PHVA del Modelo de Gestión de Seguridad y Privacidad de la Información de la Gobernación del Huila



Fuente: Elaboración propia a partir del Modelo de Seguridad del Ministerio TIC

6.2. Características del Modelo de Seguridad y Privacidad de la Información

El Modelo de Gestión de Seguridad y Privacidad de la Información propuesto para la Gobernación del Huila presenta las siguientes características:

- Busca facilitar la comprensión y aplicación de los conceptos asociados a la gestión de la seguridad y privacidad de la información, a través de la adopción y adaptación de herramientas de gestión de activos de TI, de riesgos, y de controles a aplicar en la entidad, para optimizar la operación de los procesos y la prestación de servicios.
- Permite identificar y clasificar activos tecnológicos y de información, procurando el cumplimiento de la legislación y normatividad establecida por las entidades del orden nacional y entes de control, y valorándolos de acuerdo con su nivel de importancia o criticidad para la entidad.
- Facilita la identificación y análisis de amenazas que pueden llegar a afectar a los activos de TI de la entidad, a partir de la clasificación de éstas según su origen.
- Teniendo como base el ciclo de operación PHVA, este modelo integra la gestión de riesgos de Seguridad de la Información como criterio para la selección de controles de seguridad que establece la normatividad técnica establecida por el Ministerio TIC y la norma ISO/IEC 27001:2013.
- Su implementación está asociada a los dominios de control de la norma técnica ISO/IEC 27001, estableciendo categorías de gestión que priorizan y agrupan las acciones y controles técnicos y administrativos de seguridad y privacidad de la información.
- Adopta herramientas de diagnóstico establecidas por el Ministerio TIC y el Departamento de la Función Pública, para medir el nivel de madurez de la gestión de seguridad y privacidad de la información, previo a la fase de planificación y en la fase de seguimiento y evaluación de la implementación del modelo propuesto.

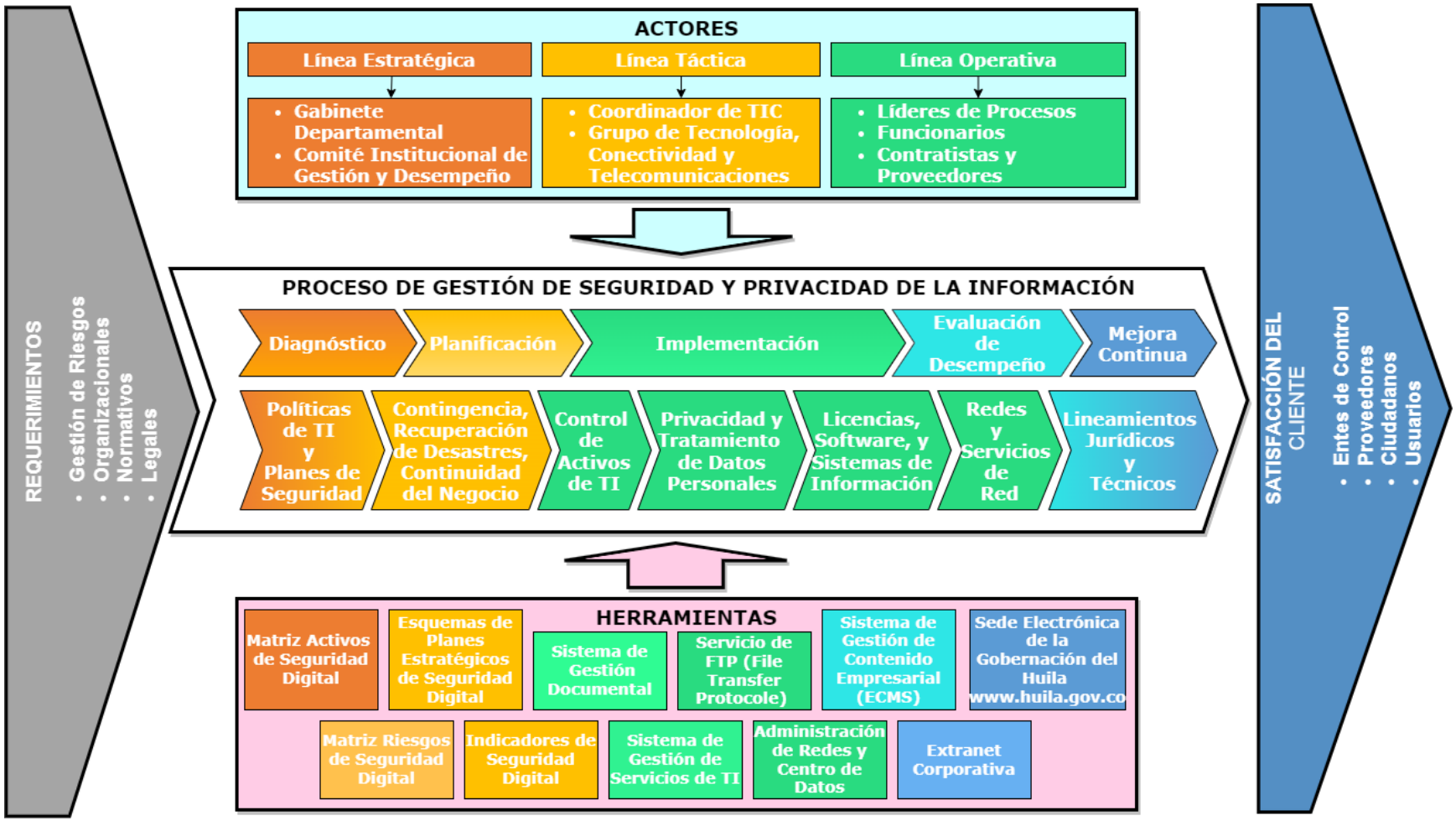
6.3. Estructura del Modelo de Gestión de Seguridad y Privacidad de la Información

El Modelo de Gestión de Seguridad y Privacidad de la Información propuesto para la Gobernación del Huila (Ver Figura 37) establece el uso de herramientas tecnológicas, partiendo desde matrices diseñadas en herramientas ofimáticas para la identificación y análisis de activos y riesgos de Seguridad de la Información, y la formulación de políticas y planes de acción relacionados, que permitan establecer las diferentes actividades a desarrollar para gestionar la seguridad de los activos de TI de la entidad, gestión que como lo indican los lineamientos técnicos del Ministerio TIC, deberá ir alineada con el Sistema de Gestión Documental de la entidad. La eficiencia de esta gestión será medida a través de indicadores de seguimiento y a su vez serán el insumo principal para la mejora continua del proceso.

Para la implementación de los diferentes controles de seguridad establecidos en los planes de acción mencionados, se requiere uso de algunos software para la gestión y administración de los servicios de TI que se prestan a partir de la infraestructura tecnológica existente, procurando su operación, integración y eficacia suficiente que permita detectar brechas, mantener el nivel de confianza requerido por los usuarios, y proporcionar así los servicios de TI que favorezcan la generación de valor en la entidad.

Los resultados de esta implementación se registrarán en primer lugar en el Sistema de Gestión de Contenido Empresarial (ECMS) en el que se administra el Sistema Integrado de Gestión, y en el que usuarios internos tienen acceso a información estratégica, políticas, planes, autoevaluaciones, auditorías, etc., que se realizan a los sistemas de gestión adoptados, y posteriormente se publicarán en la Extranet Corporativa y en la Sede Electrónica de la Gobernación del Huila, www.huila.gov.co, con el fin de que todos los interesados puedan acceder a ésta. De esta forma, los actores del modelo en sus diferentes niveles, interactúan en el desarrollo del proceso de gestión desde cada uno de los roles que se establezcan en el marco de las políticas y planes de acción que son necesarios para gestionar y apropiar la gestión de la seguridad y privacidad de la información en la cultura organizacional de la Gobernación del Huila.

Figura 37. Estructura del Modelo de Gestión de Seguridad y Privacidad de la Información de la Gobernación del Huila



Fuente: Elaboración propia

6.3.1. Proceso de gestión de seguridad y privacidad de la información

Para el desarrollo de las diferentes estrategias establecidas para el desarrollo e implementación del Modelo de Gestión de Seguridad y Privacidad de la Información en la Gobernación del Huila, se establece el siguiente flujo de actividades, enmarcadas en un ciclo PHVA, como se observa en la Tabla 19.

Tabla 19. Proceso de Gestión de Seguridad y Privacidad de la Información de la Gobernación del Huila

Actividad	Descripción	Entregables
Diagnóstico	Abarca la identificación del estado actual y el nivel de madurez, a partir de las necesidades y requerimientos de la gestión de seguridad y privacidad de la información, evaluando el cumplimiento de la legislación y normatividad técnica asociadas.	• Instrumento de Evaluación de Seguridad de la Información para la Gobernación del Huila.
Planificación	Abarca la elaboración de planes y políticas principales para la gestión de la seguridad y la privacidad de la información de la Gobernación del Huila, alineándolas con los objetivos y metas estratégicas establecidas, y definiendo acciones a implementar para gestionar los riesgos a nivel de seguridad y privacidad de la información, el cumplimiento de la legislación pertinente, normas técnicas y buenas prácticas asociadas.	• Política de Seguridad y Privacidad de Información. • Roles y responsabilidades de seguridad y privacidad de la información. • Manual de políticas de seguridad y privacidad de la información. • Matriz de activos de Seguridad de la Información. • Declaración de aplicabilidad de controles SoA. • Plan de tratamiento de riesgos de seguridad y privacidad de la información. • Plan de capacitación, sensibilización y comunicación.
Implementación	Abarca el desarrollo de las actividades establecidas en la fase de planificación del modelo de seguridad y privacidad de la información en la entidad.	• Informe de ejecución del plan de tratamiento de riesgos de seguridad y privacidad de la información. • Indicadores de gestión de seguridad y privacidad de la información.
Evaluación de Desempeño	Abarca el seguimiento y monitoreo de la implementación del modelo de seguridad y privacidad de la información, a partir de los resultados de los indicadores propuestos.	• Plan de seguimiento y revisión del modelo de seguridad y privacidad de la información. • Plan de auditorías al modelo de seguridad y privacidad de la información.

Actividad	Descripción	Entregables
Mejora Continua	Abarca el ajuste y mejoras de entregables, controles y procedimientos del modelo de gestión de seguridad y privacidad, a partir de los resultados obtenidos en la fase de evaluación y desempeño.	• Plan de mejoramiento de seguridad y privacidad de la información. • Informe de resultados del plan de mejoramiento.

Fuente: Elaboración propia

6.3.2. Actores del Modelo

En el marco de la implementación del modelo, es clave determinar la participación activa de todos los funcionarios de la entidad, resaltando la participación y compromiso de la Alta Dirección de la Gobernación del Huila, y representantes de todas las áreas y procesos de gestión, con el fin de asegurar disponibilidad de la información crítica, así como la transversalidad de las actividades de implementación. De esta forma, se establecen los actores para cada nivel de planeación del modelo (Ver Tabla 20).

Tabla 20. Actores del Modelo de Gestión de Seguridad y Privacidad de la Información

Niveles	Descripción	Actores
Línea Estratégica	En este nivel se realiza la formulación, revisión y aprobación del marco general de gestión de seguridad y privacidad de la información, alineado a la naturaleza y estrategia misional de la Gobernación del Huila	• Alta Dirección (Gabinete Departamental) • Comité Institucional de Gestión y Desempeño
Línea Táctica	En este nivel se coordina y realizan las diferentes estrategias y actividades planificadas, buscando fortalecer la gestión de la seguridad y privacidad de la información.	• Coordinador del Grupo de Tecnología (Líder de Seguridad y Privacidad de la Información). • Grupo de Tecnología y personal con funciones relacionadas con servicios de TI.
Línea Operativa	Nivel encargado de apropiar la gestión de seguridad y privacidad de la información en las actividades misionales de la entidad, generando valor en la prestación de servicios a los usuarios, ciudadanos y grupos de interés, a partir del aseguramiento de la información y los activos críticos identificados.	• Líderes de procesos de gestión de la entidad. • Funcionarios y equipos de trabajo en general, de las diferentes áreas y dependencias.
Usuarios, ciudadanos y grupos de interés	Corresponde a los clientes y/o beneficiarios de la implementación del modelo en la entidad.	• Ciudadano y usuarios de servicios de la entidad. • Entes de control. • Proveedores y/o terceros.

Fuente: Elaboración propia

6.3.3. Herramientas tecnológicas

Dentro de las herramientas diseñadas, existentes y adoptadas por la entidad para gestionar la seguridad y privacidad de la información, se tienen las disponibles en la Tabla 21:

Tabla 21. Herramientas diseñadas y adoptadas para el Modelo de Gestión de Seguridad y Privacidad de la Información de la Gobernación del Huila

Herramienta	Descripción
Matriz de identificación de activos	Matriz diseñada en formato de archivo xlsx, y en el que se incluyen una serie de pasos que permiten realizar una valoración de cada activo, de forma que se facilitara su integración a la metodología de gestión de riesgos de la entidad, y su uso por parte de personal de la Coordinación del Sistema Integrado de Gestión.
Matriz de riesgos de Seguridad de la Información	Matriz diseñada en formato xlsx para generar, tanto su procedimiento de identificación y análisis de riesgos en cada uno de los procesos de gestión, como la identificación de consecuencias para cada riesgo identificado, la evaluación del nivel de impacto para cada riesgo identificado, la determinación del riesgo inherente de seguridad, en base a la probabilidad y el nivel de impacto identificado.
Esquemas para diseño y definición de planes de seguridad, y de sensibilización en seguridad y privacidad de la información	Matrices diseñadas en formato xlsx, para la descripción y planificación de actividades de implementación y sensibilización del Modelo de Gestión y Seguridad y Privacidad de la Información en la Gobernación del Huila.
Indicadores de seguimiento a la gestión de seguridad y privacidad de la información	Indicadores orientados a la medición de efectividad, eficiencia, y eficacia de la implementación del modelo de gestión de seguridad y privacidad de la información, y que sirven de insumo para la mejora continua del modelo.
Sistema de Gestión Documental (Procesos y Documentos)	Sistema que gestiona la documentación asociada a todos los procesos de la entidad. (Planes, políticas, procedimientos, instructivos, manuales, etc.), gestión de flujos documentales, almacenamiento, clasificación y conservación de los documentos electrónicos que se gestionan en la entidad, así como también los documentos de archivos físicos que se indexen y clasifiquen a través de procesos de digitalización.
Sistema de Gestión de Servicios de TI – OTRS	Sistema de gestión de servicios de tecnologías de la información, que brinda la capacidad de realizar registro y trazabilidad de reportes de problemas, incidentes, requerimientos, solicitudes de servicios, entre otro tipo de eventos que se presentan en la entidad relacionados con la arquitectura tecnológica.
Servicio FTP (File Transfer Protocol)	Espacio dedicado en un servidor de la entidad para el intercambio de información de manera instantánea entre servidores y/o dependencias.
Herramientas de administración de redes y centro de datos	Herramientas y sistemas que permiten la gestión de redes de comunicaciones y del centro de datos, para prestar de manera eficiente servicios de TI que generen valor a la gestión estratégica de la entidad. • Servicio de directorio activo • Servidor de dominio

Herramienta	Descripción
	• Firewall UTM Sophos • Consola antivirus Kaspersky • Software de gestión de Access Point UniFi • Sistema de monitoreo de redes PRTG
Sistema ECMS (Gestión de Contenido Empresarial)	Sistema de administración de información y contenidos relacionados con el Sistema Integrado de Gestión de la entidad (Información estratégica, Políticas, Planes, Autoevaluaciones, Auditorías, etc.).
Extranet corporativa	Plataforma tecnológica que garantiza la comunicación e intercambio de información de manera oportuna entre la entidad, sus funcionarios y los ciudadanos, permitiendo el desarrollo de la gestión de comunicaciones en forma segura, eficiente, integral, oportuna y centralizada, logrando la automatización de procesos, acceso centralizado a la información, reducción de uso de papel y mejoramiento en la eficiencia en procesos misionales.
Sede electrónica de la Gobernación del Huila www.huila.gov.co	Solución enfocada a interacción, participación, trámites y servicios en línea que posibilita cambiar el modelo de comunicación ciudadano-estado.

Fuente: Elaboración propia

6.3.4. Declaración de Aplicabilidad de Controles de Seguridad (SoA)

Para determinar las actividades con las que se implementará el Modelo de Seguridad y Privacidad de la Información, se tiene en cuenta en primer lugar el nivel de madurez identificado a través del Instrumento de Evaluación del Ministerio TIC, el cual sirve de base para definir la Declaración de Aplicabilidad de Controles de Seguridad -SoA. La Declaración de Aplicabilidad -Statement of Applicability- (SoA) es un elemento para la implementación del Modelo de Seguridad y Privacidad de la Información, que indica si los objetivos de control y los controles establecidos en el Anexo A de la norma ISO 27001:2013 se encuentran implementados y en operación, o si, por el contrario, se han descartado algunos, y justificar por qué han sido excluidos.

Entre los motivos de selección se pueden encontrar: resultados, conclusiones de la evaluación y tratamiento de riesgos, requisitos legales, obligaciones contractuales y necesidades de la organización en materia de seguridad de la información. En este caso, la declaración establecida para la identificación de controles en operación y selección de controles a implementar en la Gobernación del Huila, se muestra en la Tabla 22, y en el Anexo 9.

Tabla 22. Declaración de Aplicabilidad -SOA- de controles en la Gobernación del Huila

Declaración de Aplicabilidad **Vigente hasta el: 30/12/2021**

La presente declaración se establece sobre los controles que son relevantes para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Gobernación del Huila y aplicables al mismo. Adicionalmente en ella se encuentran justificada la exclusión de algunos de los controles y se muestra el motivo de selección de los controles aplicables.

Convenciones: **RL**: requerimientos legales, **OC**: obligaciones contractuales, **RN/BP**: requerimientos del negocio/buenas prácticas adoptadas , **RVR**: resultado de la valoración de riesgos;

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control / control			LR	CO	BR/BP	RRA	
5 Políticas de Seguridad	**5.1**	**Dirección de la alta gerencia para la seguridad de la información**							
	5.1.1	Políticas de seguridad de la información	Política general de SPI publicada en el SIGC		X		X	X	Establecer y documentar políticas de SPI, y posterior inclusión en el SIG
	5.1.2	Revisión de las políticas de seguridad de la información	Revisión anual de la Política general de SPI		X		X	X	Revisión anual periódica de políticas de SPI, y posterior inclusión en el SIG
6 Organización de la Seguridad de la Información	**6.1**	**Organización interna**							
	6.1.1	Roles y responsabilidad de seguridad de la información	Política general de SPI publicada en el SIGC				X	X	Añadir las responsabilidades incluidas en las políticas, en los contratos de los funcionarios
	6.1.2	Segregación de deberes	Asignación de responsabilidad sobre activos de información				X	X	Establecer procesos de verificación periódica de no duplicidad de funciones entre funcionarios de planta administrativa, contratistas y proveedores
	6.1.3	Contacto con autoridades	Red de emergencias mediante empresa de seguridad		X		X		Establecer y documentar procedimientos
	6.1.4	Contacto con grupos de interés especial	No existe asignación de responsabilidad para contactar grupos de interés				X		Establecer y documentar procedimientos
	6.1.5	Seguridad de la información en la gestión de proyectos	No se han definido aplicación de políticas y/o procedimiento de SPI en los proyectos		X	X	X	X	Incluir cláusulas seguridad y privacidad de la información interna en los proyectos
	6.2	**Dispositivos móviles y teletrabajo**							
	6.2.1	Política de dispositivos móviles	No existe política para dispositivos móviles, pero existen directrices elevadas por talento humano		X	X	X	X	Establecer, documentar e implementar
	6.2.2	Teletrabajo	Se fomenta y aplican lineamientos de la política de teletrabajo pero no existe trazabilidad		X				Establecer, documentar e implementar procedimientos para acoger dicha estrategia al interior de la entidad

Fuente: ISO27k Statement of Applicability (2018) - https://www.iso27000.es/assets/files/ISO27k%20SOA%202013%20in%205%20languages.xlsx

6.3.5. Plan de Seguridad y Privacidad de la Información

Basado en la Declaración de Aplicabilidad de Controles de Seguridad, y según las categorías de gestión priorizadas y agrupadas del Modelo de Gestión propuesto para la Gobernación del Huila, se establece el plan de acción para la implementación del Modelo de Seguridad y Privacidad de la Información en la Gobernación del Huila, denominado *Plan de Seguridad y Privacidad de la Información*, utilizando para ello el formato que se observa en la Tabla 23 y diseñado para esta planificación, en el que cada actividad debe ser descrita y detallada de forma que se explique su objetivo y proceso de realización.

Tabla 23. Diseño de Plan de Seguridad y Privacidad de la Información para la Gobernación del Huila

Actividad	Responsable	Entrega	Presupuesto Estimado			Porcentaje de Avance	Observaciones
			Recursos Humanos	Recursos Materiales	Recursos Financieros		
Descripción de la actividad de aplicación del objetivo de control (P.E. Documentar, Publicar e Implementar Procedimiento de gestión de contraseñas)	**Área, Oficina o Dependencia encargada** de la aplicación del Objetivo de Control (P.E. Oficina de Tecnología)	**Fecha de entrega** del diseño o construcción del objetivo de control	**Talento Humano** requerido para el desarrollo de la actividad	**Equipos y materiales** requeridos para el desarrollo de la actividad	**Presupuesto** requerido para la adquisición de recursos humanos y materiales que permitan el desarrollo de la actividad	**Porcentaje de avance en la fecha de seguimiento** del diseño o construcción del objetivo de control	**Precisiones** que sean requeridas sobre la actividad

Fuente: Elaboración Propia

Este plan tiene como objetivo desarrollar estrategias y acciones que conlleven al mejoramiento de la gestión de la seguridad y privacidad de la información de la Gobernación del Huila, que fortalezcan el enfoque preventivo referente a la seguridad y privacidad de la Información, y garanticen la confidencialidad, integridad y disponibilidad de sus activos tecnológicos y de información, cumpliendo de esta forma con el cuarto objetivo específico del presente proyecto. En la Tabla 24, se observa este plan, agrupando actividades en categorías, estableciendo en primer lugar, acciones de diagnóstico, planificación e implementación de tecnologías más utilizadas en la entidad. Posteriormente, atención de eventos e incidentes de seguridad, elaboración e implementación de planes, políticas y procedimientos específicos de seguridad para diferentes tipos de activos de TI, privacidad y tratamiento de datos personales, y, por último, actualización de lineamientos jurídicos y técnicos relacionados.

Tabla 24. Plan de Seguridad y Privacidad de la Información de la Gobernación del Huila

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – GOBERNACIÓN DEL HUILA							
Actividad	**Responsable**	**Fecha de Entrega**	**Presupuesto Estimado**			**% AVANCE A 30/12/2020**	**Observaciones**
			Recurso Humano	**Materiales**	**Recursos Financieros**		
DISEÑO Y/O ACTUALIZACIÓN DE PLANES DE TI Y PRINCIPALES POLÍTICAS ESPECÍFICAS DE TECNOLOGÍAS MÁS USADAS							
Realizar **levantamiento y actualización de inventario de activos de Seguridad de la Información** de la entidad	Grupo de Tecnología	sep-20	5 técnicos	Papelería	$ 10.000.000	100%	CUMPLIDO
Realizar **análisis y evaluación de riesgos TI**, que permita la actualización del Plan de Tratamiento de Riesgos de Seguridad de la Información vigente	Grupo de Tecnología	dic-20	1 profesional especializado	Documentación	$ 12.000.000	100%	CUMPLIDO
Elaboración, aprobación de **política de seguridad de la información**, y posterior inclusión en el Sistema Integrado de Gestión de la Gobernación del Huila	Grupo de Tecnología	jun-21	3 profesionales	Documentación	$ 12.000.000	40%	Existe borrador Política General de Seguridad y Privacidad de la Información
Elaborar, publicar y divulgar **procedimientos de contacto con autoridades y grupos especiales** en relación con la seguridad de la información	Grupo de Tecnología	jun-21	1 profesional especializado	Documentación	$ 12.000.000	0%	Contacto con autoridades como colCERT, CSIRT, Centro Cibernético Policial, entre otros.
Elaborar, publicar y divulgar **procedimientos para la clasificación de la información** de la Gobernación del Huila	Grupo de Tecnología - Archivo – Calidad	jun-21	1 profesional especializado	Documentación	$ 12.000.000	60%	Según establece Ley 1712 de 2014 - Transparencia y Acceso a la Información –
Elaborar e implementar **política de gestión de dispositivos móviles** en la Gobernación del Huila	Grupo de Tecnología	jun-21	1 profesional especializado	Documentación	$ 12.000.000	0%	Gestionar conexiones de equipos portátiles, celulares y tablets, entre otros
Elaborar e implementar **políticas de transferencia de información** al interior de la Gobernación del Huila (uso del correo electrónico institucional, acuerdos de no divulgación de información)	Grupo de Tecnología	jun-21	1 profesional especializado	Documentación	$ 12.000.000	0%	N.A.
Elaborar el **plan de socialización, sensibilización y capacitación en seguridad de la información** (políticas de seguridad de la información adoptadas, Ley 1273 de 2009 - Delitos Informáticos, etc.)	Grupo de Tecnología - Talento Humano	sep-21	1 profesional especializado + 1 especialista externo	Documentación + Convenio y/o contrato para capacitación técnica	$ 50.000.000	0%	Profesional especializado para sensibilización interna + especialista externo para capacitación a personal de gestión de TI
Elaborar e implementar **procedimiento de verificación periódica de no duplicidad de funciones** entre funcionarios de planta administrativa, contratistas y proveedores	Talento Humano	dic-21	1 profesional	Documentación	N.A.	60%	Talento Humano verifica perfiles existentes en planta personal al contratar servicios profesionales

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – GOBERNACIÓN DEL HUILA							
Actividad	**Responsable**	**Fecha de Entrega**	**Presupuesto Estimado**			**% AVANCE A 30/12/2020**	**Observaciones**
			Recurso Humano	**Materiales**	**Recursos Financieros**		
Elaborar e implementar **procedimiento de verificación de autenticidad de documentos** presentados por aspirantes a un cargo dentro de la entidad	Talento Humano	dic-21	1 profesional	Documentación	N.A.	60%	Talento Humano verifica documentos de aspirantes a cargos en la entidad
Añadir **funciones, obligaciones contractuales y/o clausulas referentes a la seguridad y confidencialidad de la información**, a personal de planta administrativa, contratos de prestación de servicios, proyectos y procesos contractuales en general	Secretaría General - Departamento de Contratación - Talento Humano	dic-21	3 profesionales	Documentación	N.A.	0%	Validar inclusión con jefes de áreas relacionadas, y evaluar pertinencia de dicha inclusión en el manual de funciones
Elaborar **plan de control operativo** de seguridad y privacidad de la información	Grupo de Tecnología	dic-21	1 profesional especializado	Documentación	N.A.	0%	N.A.
Elaborar **plan de seguimiento y medición de la implementación** de seguridad y privacidad de la información	Grupo de Tecnología	dic-21	1 profesional especializado	Documentación	N.A.	0%	N.A.
Elaborar **plan de mejora continua** de seguridad y privacidad de la información	Grupo de Tecnología	dic-21	1 profesional especializado	Documentación	N.A.	0%	N.A.
Elaborar **plan de auditoría interna** a las políticas de seguridad de la información	Calidad – Grupo de Tecnología	dic-21	1 profesional especializado	Documentación	N.A.	0%	Incluir evaluación de políticas de seguridad en planes de auditoría de sistemas de gestión
Elaborar **plan de auditoría interna** a los sistemas de información de la Gobernación del Huila	Calidad – Grupo de Tecnología	dic-21	1 profesional especializado	Documentación	N.A.	0%	Incluir evaluación de sistemas de información en los planes de auditoría de cada proceso
CONTINGENCIA, RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DEL NEGOCIO							
Elaborar e implementar **políticas de respaldo de información**	Grupo de Tecnología	jun-21	1 profesional especializado	Documentación	$ 12.000.000	20%	N.A.
Elaborar **plan de continuidad del negocio** para la Gobernación del Huila	Grupo de Tecnología	dic-22	1 profesional especializado	Documentación	$ 12.000.000	0%	Recursos para contratación de Profesional TIC por prestación de servicios
Revisar y actualizar **plan de contingencia ante desastres** de Tecnologías de la Información	Grupo de Tecnología	jun-23	1 profesional especializado	Documentación	$ 12.000.000	60%	Existe plan de Contingencia para recuperación de desastres de Tecnología

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – GOBERNACIÓN DEL HUILA							
Actividad	**Responsable**	**Fecha de Entrega**	**Presupuesto Estimado**			**% AVANCE A 30/12/2020**	**Observaciones**
			Recurso Humano	**Materiales**	**Recursos Financieros**		
ELABORACIÓN E IMPLEMENTACIÓN DE POLÍTICAS DE USO Y CONTROL DE ACTIVOS DE TI EXISTENTES (INFORMACIÓN, SOFTWARE, MANTENIMIENTO)							
Elaborar e implementar **política de uso de activos TI** (hardware, software, seguimiento a responsabilidad)	Grupo de Tecnología	dic-21	1 profesional especializado	Documentación	$ 12.000.000	60%	Se cuenta con un "manual de política, uso y admón. de recursos tecnológicos"
Elaborar e implementar **política de control de acceso a información y a instalaciones** de procesamiento de información en la entidad	Grupo de Tecnología	dic-21	1 profesional especializado	Documentación	$ 12.000.000	40%	Incluye gestión de contraseñas, bloqueo de sesión de usuario, procedimientos para escritorio y pantalla limpios
Elaboración de **plan de diagnóstico, verificación y mantenimiento preventivo de activos de TI** (equipos de cómputo, impresoras, sistemas de respaldo eléctrico, dispositivos de almacenamiento de información y servicios, y cableado estructurado)	Grupo de Tecnología	dic-21	1 profesional especializado + 1 profesional + 5 técnicos	Documentación + Herramienta especializada + insumos	$ 400.000.000	0%	Contratación de personal de formulación del plan + personal de mantenimiento + materiales + herramientas
Elaboración e implementación de **lista de chequeo de mobiliario para uso de activos de TI** e inclusión en políticas de uso de activos TI	Grupo de Tecnología	dic-21	1 profesional especializado	Documentación	$ 12.000.000	0%	Recursos para contratación de Profesional TIC por prestación de servicios
Elaborar e implementar **procedimientos de trabajo en áreas seguras** de procesamiento de información (seguridad de centros de datos, oficinas y despachos).	Grupo de Tecnología - Secretaría General	dic-21	1 profesional + 1 profesional especializado	Documentación y papelería	N.A.	0%	Personal de planta administrativa + Profesional TIC por prestación de servicios
Elaborar **procedimiento para acoger la estrategia de Teletrabajo** al interior de la entidad	Talento Humano – Grupo de Tecnología	dic-21	1 profesional	Documentación	$ 25.000.000	20%	Costo de vinculación de profesional por OPS
Elaborar e implementar **procedimiento de retiro y/o traslado de activos TI**, e inclusión en políticas de uso de activos TI	Almacén - Grupo de Tecnología	jun-22	1 profesional + 1 profesional especializado	Documentación	$ 18.000.000	0%	Personal de planta administrativa + Profesional TIC por prestación de servicios
Elaborar e implementar **procedimiento para la baja, eliminación segura o reúso de activos TI**, e inclusión en políticas de uso de activos TI	Almacén - Grupo de Tecnología	jun-22	1 profesional + 1 profesional especializado	Documentación	$ 18.000.000	0%	Personal de planta administrativa + Profesional TIC por prestación de servicios

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – GOBERNACIÓN DEL HUILA							
Actividad	**Responsable**	**Fecha de Entrega**	**Presupuesto Estimado**			**% AVANCE A 30/12/2020**	**Observaciones**
			Recurso Humano	**Materiales**	**Recursos Financieros**		
Definir y aplicar el **perímetro de seguridad físico para protección de áreas** de almacenamiento y procesamiento de información crítica	Grupo de Tecnología - SGSST	dic-22	1 profesional	Documentación+ planos	N.A.	60%	Ejecución por parte de personal de planta administrativa del Grupo TIC
Realizar **verificación y aplicación de medidas de mitigación de riesgos generados por eventos físicos que afectan los activos de TI**, en el marco de implementación del SGSST	Grupo de Tecnología – Seguridad y Salud en el Trabajo	sep-23	1 profesional	Documentación	N.A.	20%	Ejecución por parte de personal de planta administrativa
TRATAMIENTO DE DATOS PERSONALES							
Actualizar **Política de Tratamiento de Datos Personales** y publicar en el portal web institucional	Grupo de Tecnología	oct-21	1 profesional especializado	Documentación	$ 12.000.000		Existe Política de Tratamiento de Datos Personal de la entidad
Actualizar **bases de datos de la Gobernación del Huila registradas en Registro Nacional de Bases de Datos** -RNBD-	Grupo de Tecnología	oct-21	1 profesional especializado	Documentación	$ 12.000.000		Existen cuatro (04) bases de datos de la entidad registradas en el RNBD
Revisar y actualizar **documentación relacionada y registrada en el Registro Nacional de Bases de Datos** -RNBD-	Grupo de Tecnología	oct-21	1 profesional especializado	Documentación	$ 12.000.000		Política de tratamiento de datos personales cargada en el RNBD
PROCEDIMIENTOS DE ADQUISICIÓN O DESARROLLO DE LICENCIAMIENTO, SOFTWARE, Y SISTEMAS DE INFORMACIÓN							
Contratar y administrar **aplicativo de protección contra software malicioso**	Grupo de Tecnología	dic-21	1 profesional	Software licenciado	$ 80.000.000	80%	Contratación de licencias de antivirus y UTM
Elaborar e implementar **políticas de desarrollo seguro de software** en la entidad (desarrollo interno, desarrollo tercerizado, seguimiento, pruebas de seguridad y aceptación)	Grupo de Tecnología	dic-22	1 profesional especializado	Documentación	$ 12.000.000	0%	Priorizar seguimiento y pruebas sobre desarrollos tercerizados existentes
Elaborar **plan de verificación y seguimiento a licenciamiento de aplicaciones y software** registrado	Grupo de Tecnología	dic-22	1 profesional especializado	Documentación	$ 12.000.000	0%	Verificar licenciamiento existente por derechos de autor y propiedad intelectual
Elaborar e implementar **procedimiento para el almacenamiento seguro de datos de prueba** de aplicativos y sistemas de información	Grupo de Tecnología	dic-22	1 profesional especializado	Documentación	$ 12.000.000	0%	Recursos para contratación de Profesional TIC por prestación de servicios
Elaborar e implementar **procedimiento de verificación de requerimientos técnicos de TI relacionados con seguridad de la información en estudios previos** de conveniencia y procesos	Secretaría General - Departamento de Contratación -	dic-22	2 profesionales +1 profesional especializado	Documentación	$ 12.000.000	0%	Personal de planta administrativa + Profesional TIC por prestación de servicios

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – GOBERNACIÓN DEL HUILA							
Actividad	**Responsable**	**Fecha de Entrega**	**Presupuesto Estimado**			**% AVANCE A 30/12/2020**	**Observaciones**
			Recurso Humano	**Materiales**	**Recursos Financieros**		
contractuales (análisis y especificación de requerimientos de seguridad, cifrado de comunicaciones de aplicaciones que trabajen sobre redes públicas)	Grupo de Tecnología						
Elaborar e implementar **política de seguridad de la información en las relaciones con proveedores** (procedimientos, monitoreo y revisión de servicios, gestión de cambios)	Grupo de Tecnología	dic-22	1 profesional especializado	Documentación	$ 12.000.000	0%	Recursos para contratación de Profesional TIC por prestación de servicios
Elaborar e implementar **procedimiento de gestión de cambios en los procesos de gestión que afecten aspectos de seguridad de la información** de la entidad	Grupo de Tecnología - Calidad	sep-23	1 profesional + 1 profesional especializado	Documentación	$ 18.000.000	0%	Personal de planta administrativa + Profesional TIC por prestación de servicios
SEGURIDAD DE REDES Y SERVICIOS DE RED							
Elaborar e implementar **política de monitoreo de usuarios** y eventos de seguridad de la información	Grupo de Tecnología	dic-22	1 profesional especializado	Documentación	$ 12.000.000	0%	Recursos para contratación de Profesional TIC por prestación de servicios
Efectuar **análisis periódicos de tráfico de red**, realizar reporte de anomalías detectadas y aplicar medidas preventivas y correctivas cuando sea el caso.	Grupo de Tecnología	dic-22	2 profesionales	Software libre de análisis tráfico + Documentación	N.A.	20%	Ejecución por parte de personal de planta administrativa y profesional especializado
Elaborar e implementar **procedimiento de transferencia segura de información y aseguramiento de servicios de red**	Grupo de Tecnología	dic-22	2 profesionales especializados	Documentación	$ 36.000.000	0%	Personal de planta administrativa + Profesional especializado externo
LINEAMIENTOS JURÍDICOS Y TÉCNICOS DE SEGURIDAD DE LA INFORMACIÓN							
Revisar y actualizar **lineamientos jurídicos y procesos de control interno disciplinario en aspectos de seguridad de la información**	Oficina de Control Disciplinario - Grupo de Tecnología	sep-23	2 profesionales	Documentación	N.A.	0%	Ejecución por parte de personal de planta administrativa
Revisión y **actualización del Sistema de Gestión Integrado**	Oficina de Control Interno	sep-23	1 profesional especializado	Documentación	N.A.	60%	Incluir en el procedimiento de revisión del SIG, seguridad de la información
				Total	**$ 919.000.000**		

Fuente: Elaboración propia

6.3.6. Plan de Sensibilización en Seguridad y Privacidad de la Información

El Plan de Sensibilización de Seguridad y Privacidad de la Información permite identificar y establecer temáticas necesarias para sensibilizar, capacitar y evaluar el nivel de gestión de seguridad y privacidad de la información en la entidad, teniendo en cuenta los diferentes públicos objetivo: usuarios finales internos, usuarios finales externos, administradores de sistemas y profesionales especializados, y personal directivo.

Siguiendo la metodología propuesta, el Plan de Sensibilización de Seguridad y Privacidad de la Información se define además para establecer y ejecutar estrategias de promoción e inclusión de la gestión y prevención de riesgos asociados en la cultura organizacional de la Gobernación del Huila, desarrollando los siguientes pasos:

6.3.6.1. Identificación de necesidades de sensibilización y capacitación

En esta fase se identifican los diferentes públicos objetivos y los objetivos de conocimiento que cada uno requiere, para posteriormente identificar las necesidades, las cuales finalmente justifican la aplicación del plan en base a los indicadores de desempeño que se planteen, mediante diferentes métodos y herramientas como encuestas, verificación de comportamientos generales del personal (sesiones abiertas, escritorios limpios etc.), verificación de los incidentes de seguridad de la información, y tendencias en el sector público, entre otros.

A partir del reporte de requerimientos de servicios tecnológicos clasificados como incidentes críticos durante la vigencia 2020, en la que se presentaron 12 incidencias de indisponibilidad de servicios tecnológicos (Gobernación del Huila, 2020), de las cuales 7 fueron incidentes de seguridad de la información, asociados a correos electrónicos de suplantación (*phishing*) y ataques de denegación de servicio de correo electrónico; se evidencia la necesidad de sensibilización para el personal de la entidad, en la identificación de correos sospechosos, spam, phishing, y demás amenazas a este servicio.

6.3.6.2. Objetivos

*Objetivo General***:** Establecer estrategias, iniciativas y métodos de comunicación, para la apropiación y uso de las tecnologías en la entidad, fortaleciendo la gestión de la seguridad y privacidad de la información e integrándola a la cultura organizacional, a partir de la construcción e implementación de acciones que permitan difundir y transferir conocimientos, beneficios, buenas prácticas, legislación, directrices, políticas y lineamientos internos del Modelo de Seguridad y Privacidad de la Información de la Gobernación del Huila.

Objetivos Específicos:

- Definir la población objetivo en la entidad, para cada estrategia y actividad de capacitación y sensibilización en seguridad y privacidad de la información.
- Establecer estrategias y actividades de capacitación, sensibilización y comunicación en seguridad y privacidad de la información, según los roles y responsabilidades de los grupos establecidos dentro de la población objetivo.
- Dar a conocer las obligaciones legales y regulatorias del estado relacionadas con la seguridad y privacidad sobre la información gestionada por la entidad.
- Fomentar el uso y apropiación de las políticas, procedimientos, y controles establecidos en el marco de la implementación del Modelo de Seguridad y Privacidad de la Información en la Gobernación del Huila.
- Disponer de los recursos necesarios para realizar las estrategias y actividades de capacitación y sensibilización en seguridad y privacidad de la información de la Gobernación del Huila.

6.3.6.3. Alcance

Abarca la definición de estrategias, recursos, materiales y contenidos necesarios para capacitar, sensibilizar y comunicar a los funcionarios y contratistas de la entidad, de acuerdo con el rol y responsabilidad establecidas en la Política General de Seguridad y Privacidad de la Información de la Gobernación del Huila.

6.3.6.4. Roles y responsabilidades

En este punto, se establecen las funciones necesarias para el desarrollo de las actividades de sensibilización y capacitación en seguridad de la información, y las responsabilidades específicas en todos los niveles: estratégico, táctico y operativo, garantizando así el liderazgo del proceso de aplicación del plan y la gestión de la cultura de seguridad de la información:

- *Alta Dirección*:
  - Identificar las necesidades de capacitación y/o sensibilización en seguridad y privacidad de la información para el personal de la entidad.
  - Garantizar la apropiación de los recursos necesarios para el desarrollo y la ejecución de las estrategias y actividades programadas en el presente plan.
  - Participar y fomentar en el personal a cargo, la participación en el desarrollo de las actividades programadas del presente plan y el cumplimiento de las políticas y procedimientos establecidas y dadas a conocer.
  - Realizar el seguimiento y mediciones de eficacia en las actividades de capacitación y sensibilización en seguridad y privacidad de la información.

- *Coordinación del Grupo de Tecnología, Conectividad y Telecomunicaciones*
  - Identificar las necesidades del personal de la entidad en materia de sensibilización y capacitación en Seguridad y Privacidad de la Información.
  - Participar en el diseño ejecución, mejora y actualización de las estrategias, actividades, jornadas para el desarrollo del presente plan.
  - Consolidar los resultados de las evaluaciones y seguimientos realizados en las actividades de sensibilización y capacitación en seguridad y privacidad de la Información, lideradas por el Grupo de Tecnología.

- *Funcionarios(as) y Contratistas*
  - Participar activamente en las estrategias, actividades y jornadas establecidas en el presente plan.
  - Aplicar en sus actividades diarias las políticas y procedimientos, relacionadas con la seguridad de la información y socializadas a través del presente plan.

- Identificar oportunidades de mejora, iniciativas y nuevas actividades a tratar en futuros programas de sensibilización y capacitación relacionados.

6.3.6.5. Metas

En este aspecto se establecen metas cuantificables de las actividades de sensibilización y capacitación en seguridad de la información:

- Adopción y apropiación por parte de los funcionarios y colaboradores de la Gobernación del Huila, de políticas y procedimientos de seguridad y privacidad de la información establecidas durante el año 2021, mediante publicaciones mensuales de difusión y promoción y jornadas semestrales de sensibilización.

- Formación y desarrollo de competencias relacionadas con gestión de seguridad de la información, análisis de vulnerabilidades, eventos y/o incidentes, en el personal del Grupo de Tecnología de la Gobernación del Huila, durante el año 2021, mediante capacitaciones técnicas relacionadas.

6.3.6.6. Audiencia objetivo

En este ítem se definen grupos objetivo de las actividades de sensibilización y capacitación en seguridad y privacidad de la información, según la caracterización del personal y de los usuarios de la entidad, para su respectiva ejecución.

Para el desarrollo del presente plan, se establecieron 4 grupos de usuarios en la Gobernación del Huila, como se muestra en la Tabla 25, y por cada uno de ellos se indican temáticas y conocimientos necesarios, con el fin de enfocar el esfuerzo de las actividades de capacitación y sensibilización.

Tabla 25. Audiencia Objetivo de Sensibilización en Seguridad y Privacidad de la Información de la Gobernación del Huila

USUARIOS	TEMÁTICAS Y CONOCIMIENTOS NECESARIOS
Alta Dirección	Legislación y directrices del Modelo de Seguridad y Privacidad de la Información -MSPI- en la entidad, generación de conciencia, compromiso y liderazgo con MSPI.
Funcionarios y Contratistas	Fortalecimiento de los niveles de concientización en seguridad y privacidad de la información, cumplimiento de las políticas, controles, recomendaciones y buenas prácticas del MSPI y responsabilidad con los sistemas a cargo y en general con el manejo de la información institucional
Administradores de Sistemas	Políticas de seguridad y privacidad de la información de la entidad, y especialmente aquellos controles de seguridad relacionados con sistemas de información, controles de acceso, gestión de contraseñas, entre otros.
Grupo de Tecnología, Conectividad y Telecomunicaciones	Fortalecimiento de competencias técnicas en seguridad informática, mediante formación en temas relacionados con la norma ISO 27001:2013, ciberseguridad, buenas prácticas de TI, para la implementación de controles de seguridad y la prevención y atención de incidentes de seguridad.

Fuente: Elaboración propia

6.3.6.7. Temáticas de sensibilización y capacitación

De acuerdo con la audiencia objetivo y las metas establecidas, se ajustan y establecen las temáticas de sensibilización y capacitación en seguridad de la información, necesarias para la generación y transferencia de conocimientos asociados, que abarquen desde aspectos legales y normativos, hasta lineamientos, directrices, políticas, buenas prácticas y controles técnicos, generando los cambios necesarios en la cultura organizacional con la inclusión de la gestión de la seguridad y privacidad de la información en la entidad. Las siguientes temáticas corresponden a las destinadas a los funcionarios y contratistas, así como la alta dirección de la entidad:

- Conocimiento general del Modelo de Seguridad y Privacidad de la Información
  - Conceptos de seguridad de la información y Norma NTC-ISO 27001:2013.
  - Generalidades sobre legislación y normatividad relacionada con seguridad de la información (Ley de transparencia, Ley de protección de datos personales, Ley de delitos informáticos, Política de Gobierno Digital y de Seguridad Digital*)*
  - Divulgación de políticas internas de seguridad y privacidad de la información.
  - Divulgación del Catálogo de Servicios TIC y de los procedimientos de gestión asociados (*Gestión Tecnológica y Servicios TIC*).

- Amenazas en Seguridad Informática (Ingeniería Social, *Phishing*, *Malware*, *Ransomware*, Robo de identidad)
- Buenas prácticas para el uso de herramientas tecnológicas (Uso adecuado del correo electrónico institucional, detección de correos sospechosos, limpieza de escritorio y puestos de trabajo, dispositivos móviles corporativos y externos, control de acceso -contraseñas, privilegios, roles- y gestión de incidentes -qué, cómo y a quién debo reportar-)

6.3.6.8. Temáticas de capacitación técnica en seguridad y privacidad de la información

Las siguientes temáticas corresponden a las destinadas a los administradores de sistemas y funcionarios del Grupo de Tecnología de la entidad, quienes requieren conocimientos sobre lineamientos y controles técnicos, para la gestión de la seguridad y privacidad de la información en la Gobernación del Huila.

- Seguridad de la Información (Seguridad de red, aplicaciones y bases de datos, Análisis forense y evidencia digital, Gestión y continuidad de negocio, Protección de datos personales, Auditoría Estándar ISO 27001).
- Hacking Ético (Pentesting, Casos típicos de ataques, Hackeo de Servidores, Aplicaciones Web, Redes Inalámbricas y de Móviles, Inyección de SQL, Criptografía).

6.3.6.9. Plan de despliegue e implementación

En el marco del presente plan, y en cumplimiento del quinto objetivo específico del presente proyecto, se establecen las actividades a realizar para sensibilizar, capacitar, y comunicar el Modelo de Seguridad y Privacidad de la Información de la Gobernación del Huila durante el año 2021, teniendo en cuenta los objetivos específicos y la audiencia objetivo, como se observa en la Tabla 26.

Tabla 26. Plan de Despliegue de Sensibilización y Capacitación en Seguridad y Privacidad de la Información en la Gobernación del Huila

#	Actividad	Responsable	Evidencia o Soporte	Fecha de inicio	Fecha de Término	Presupuesto Estimado			Observaciones
						Recursos Humanos	Recursos Materiales	Recursos Financieros	
1	Diseñar y divulgar mensajes alusivos a la seguridad y privacidad de la información a través del fondo de escritorio de los equipos de cómputo de la entidad.	**Coordinador de Grupo de Tecnología**	Fondos de escritorio establecidos en los equipos de cómputo de la entidad	**01 de julio de 2021**	**30 de diciembre de 2021**	Un (01) profesional del área de prensa + Un (01) profesional del área de Tecnología	Dos (02) equipos de cómputo	**$7'500.000**	Costo de personal para cincuenta (50) horas de trabajo y de dos equipos de cómputo.
2	Diseñar y divulgar mensajes alusivos a la seguridad y privacidad de la información, y a los lineamientos y directrices del Modelo de Seguridad de la entidad, a través de publicaciones en el sistema Extranet.	**Coordinador de Grupo de Tecnología**	Publicaciones en el sistema Extranet	**01 de julio de 2021**	**30 de diciembre de 2021**	Un (01) profesional del área de Tecnología	Un (01) equipo de cómputo	**$360.000**	Costo de personal para doce (12) horas de trabajo, y el costo del equipo de cómputo se incluyó en la primera actividad.
3	Divulgar las directrices del Modelo de Seguridad y Privacidad de la Información de la entidad, a través de reuniones de inducción o reinducción de funcionarios y/o contratistas, organizadas por el área de Talento Humano.	**Coordinador de Grupo de Tecnología**	Memorias y grabaciones de la reunión de inducción o reinducción	**01 de julio de 2021**	**30 de diciembre de 2021**	Un (01) profesional del área de Tecnología	Un (01) equipo de cómputo	**$180.000**	Costo de personal para seis (6) horas de trabajo, y el costo del equipo de cómputo se incluyó en la primera actividad.

#	Actividad	Responsable	Evidencia o Soporte	Fecha de inicio	Fecha de Término	Presupuesto Estimado			Observaciones
						Recursos Humanos	Recursos Materiales	Recursos Financieros	
4	Divulgar políticas, buenas prácticas, directrices o eventos especiales relacionados con seguridad y privacidad de la información generados por el MinTIC y la Gobernación del Huila, a través de publicaciones en el portal web institucional www.huila.gov.co.	**Coordinador de Grupo de Tecnología**	Publicaciones en el sistema Extranet	**01 de julio de 2021**	**30 de diciembre de 2021**	Un (01) profesional del área de Tecnología	Un (01) equipo de cómputo	**$360.000**	Costo de personal para doce (12) horas de trabajo, y el costo del equipo de cómputo se incluyó en la primera actividad.
5	Realizar test de phishing, con el fin de concientizar a los funcionarios y contratistas de la entidad sobre la importancia de identificar correos fraudulentos.	**Coordinador de Grupo de Tecnología**	Resultados de test realizados a funcionarios y contratistas	**01 de julio de 2021**	**30 de diciembre de 2021**	Un (01) profesional del área de Tecnología	Un (01) equipo de cómputo	**$300.000**	Costo de personal para diez (10) horas de trabajo, para socializar test gratuitos en la web, de concientización sobre phishing
6	Capacitar al personal del Grupo de Tecnología, Conectividad y Telecomunicaciones de la entidad, en la gestión de seguridad la información, análisis de vulnerabilidades, ataques informáticos, etc.	**Instituto Externo de Formación y/o Educación para el Talento Humano**	Memorias y grabaciones de capacitaciones	**01 de julio de 2021**	**30 de diciembre de 2021**	N.A.	N.A.	**$80.000.000**	Costos aproximados de capacitación técnica para diez (10) personas
							TOTAL	**$88.700.000**	

Fuente: Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información del Ministerio TIC (2016, pág. 29) https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

6.3.6.10. Indicadores de gestión de seguridad y privacidad de la información

El monitoreo al desarrollo del presente plan se realizará a través del seguimiento de los indicadores establecidos, que permitirán medir el cumplimiento en la ejecución, y contribuir al proceso de mejoramiento de este, identificando posibles desviaciones comportamentales, que significan fallas de percepción o de adaptación de los procesos y actividades relacionadas con la gestión de la seguridad y privacidad de la información, o simplemente necesidad de mejoramiento o concientización de las personas encargadas de llevarlos a cabo, y por consiguiente el nivel de gestión y apropiación de la cultura de seguridad de la información.

Para lo anterior, se plantean dos grupos de indicadores: indicadores de medición de efectividad de controles de seguridad, e indicadores de seguimiento de eventos o incidentes de seguridad, descritos tal como sigue a continuación:

- **Indicadores de efectividad de controles de seguridad de la información:** Permiten realizar seguimiento a la ejecución y actualización del Plan de Seguridad y Privacidad de la Información, como respuesta a los aspectos identificados a nivel de las revisiones y seguimientos realizados en la fase de implementación del Modelo de Seguridad y Privacidad de la Información en la entidad.
- **Indicadores de seguimiento de acciones y eventos o incidentes de seguridad:** Permiten realizar seguimiento a los registros de acciones, eventos y/o incidentes que podrían tener impacto en la eficacia o el desempeño del Modelo de Seguridad y Privacidad de la Información de la Gobernación del Huila, ya sean detectados por el personal del Grupo, o reportados por los funcionarios y contratistas de las diferentes dependencias de la entidad

De esta forma, estos indicadores se diseñarán de acuerdo con el esquema mostrado en la Tabla 27, y el detalle de cada se encuentra en el Anexo 10 "*Indicadores de Gestión de Seguridad y Privacidad de la Información de la Gobernación del Huila*" del presente documento.

Tabla 27. Indicadores de Gestión para la Seguridad y Privacidad de la Información para la Gobernación del Huila

<table>
<tr><td colspan="6">Nombre del Indicador</td></tr>
<tr><td colspan="2">Identificador</td><td colspan="4">Código de identificación del indicador</td></tr>
<tr><td colspan="6">Definición</td></tr>
<tr><td colspan="6">Definición del indicador, relacionando variables y objetivo</td></tr>
<tr><td colspan="6">Objetivo</td></tr>
<tr><td colspan="6">Indicar objetivo de la aplicación del indicador</td></tr>
<tr><td colspan="6">Tipo de indicador</td></tr>
<tr><td colspan="6">Indicar el tipo de indicador</td></tr>
<tr><td colspan="2">Descripción de variables</td><td colspan="2">Formula</td><td colspan="2">Fuente de información</td></tr>
<tr><td colspan="2">Relacionar variables utilizadas</td><td colspan="2" rowspan="2">Indicar fórmula matemática del indicador según las variables</td><td colspan="2">Indicar de donde se obtiene la información sobre la variable utilizada</td></tr>
<tr><td colspan="2">Relacionar variables utilizadas</td><td colspan="2">Indicar de donde se obtiene la información sobre la variable utilizada</td></tr>
<tr><td colspan="6">Metas</td></tr>
<tr><td>Escala valorativa 1</td><td>Valor Asignado</td><td>Escala valorativa 2</td><td>Valor asignado</td><td>Escala valorativa 3</td><td>Valor Asignado</td></tr>
<tr><td colspan="6">Observaciones</td></tr>
<tr><td colspan="6">Precisiones que sean requeridas sobre el indicador</td></tr>
</table>

Fuente: Guía de indicadores de gestión para la seguridad de la información del Ministerio TIC (2015, págs. 8-17). https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

Como ejemplo de estos indicadores, se muestran los indicadores "*Efectividad de la gestión en seguridad y privacidad de la información de la Gobernación del Huila*" (Ver Tabla 28) y "*Tratamientos de eventos relacionados en el marco de seguridad y privacidad de la información*" (Ver Tabla 29), para los indicadores de efectividad de controles de seguridad de la información, y los indicadores de seguimiento de acciones y eventos o incidentes de seguridad, respectivamente.

Tabla 28. Indicador de Efectividad de la gestión en seguridad y privacidad de la información de la Gobernación del Huila

INDICADOR 01 - EFECTIVIDAD DE LA GESTIÓN EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA GOBERNACIÓN DEL HUILA					
IDENTIFICADOR	MSPIH01				
DEFINICIÓN					
El indicador permite medir la aplicación de los controles y temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.					
OBJETIVO					
Establecer la efectividad de los controles y de la capacitación y sensibilización previamente definidos como medio para el control de incidentes de seguridad.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES (VSI)		**FORMULA**		**FUENTE DE INFORMACIÓN**	
VSI06: Número de incidentes de seguridad relacionados con temas de seguridad de la información ya sensibilizados al responsable de la ocurrencia del incidente.		1-(VSI06/VSI07)*100%		Mesa de servicios TI, Auditorías internas	
VSI07: Número total de incidentes de seguridad.				Mesa de servicios TI, Auditorías internas	
METAS					
DEFICIENTE	<80%	**ACEPTABLE**	80%-90%	**SATISFACTORIA**	>90%
OBSERVACIONES					

Fuente: Elaboración Propia a partir de Guía de indicadores de gestión para la seguridad de la información del Ministerio TIC (2015, págs. 8-17) https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

Tabla 29. Indicador de Tratamientos de eventos relacionados en el marco de seguridad y privacidad de la información

INDICADOR 08 - TRATAMIENTOS DE EVENTOS RELACIONADOS EN EL MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
IDENTIFICADOR	MSPIH08				
DEFINICIÓN					
El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.					
OBJETIVO					
El objetivo del indicador es reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES (VSI)		**FORMULA**		**FUENTE DE INFORMACIÓN**	
VSI15: Número de anomalías cerradas.		(VSI15/VSI16)*100%		Mesa de servicios TI, Auditorías internas	
VSI16: Número total de anomalías encontradas				Mesa de servicios TI, Auditorías internas	
METAS					
DEFICIENTE	<80%	**ACEPTABLE**	80%-90%	**SATISFACTORIA**	>90%
OBSERVACIONES					

Fuente: Elaboración Propia a partir de Guía de indicadores de gestión para la seguridad de la información del Ministerio TIC (2015, págs. 8-17). https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

7. Recomendaciones y conclusiones

A continuación, se presentan las recomendaciones para la implementación del modelo propuesto y las conclusiones de cierre del trabajo.

7.1. Recomendaciones

Es de suma importancia estar atentos a la normatividad y legislación nacional que se establece y socializa a través del Ministerio TIC Nacional, con el fin de adaptar y ajustar el modelo propuesto de gestión de seguridad y privacidad de la información para la Gobernación del Huila, a las modificaciones que sean necesarias, y mantenerlo alineado con la norma técnica ISO 27001 e ISO 27005.

Para la sostenibilidad del modelo establecido, es necesario vincular a diferentes áreas de la entidad, tales como el Departamento Jurídico, el Departamento de Contratación, Talento Humano, Gestión Documental, Control Interno de Gestión, y el Despacho del señor Gobernador, entre otras, con el fin de que los lineamientos que se generen tengan suficiente validación, antes de llevarse a consideración del Comité Institucional de Gestión y Desempeño de la entidad, comité que asume las funciones de asesoría en materia de Seguridad de la Información, y a su vez, realizar seguimiento permanente y detallado a su ejecución, identificando posibles deficiencias o inconvenientes que de manera particular puedan presentarse en su adopción.

El plan de sensibilización y capacitación toma una gran relevancia y es importante gestionar ante la alta dirección, los recursos necesarios para su ejecución, siendo consecuentes con el compromiso establecido en la Política General a plantear, y buscando consolidar la cultura organizacional en materia de seguridad y privacidad de la información.

Así mismo, es importante contar con un equipo de trabajo comprometido y con los conocimientos necesarios para que, desde el Grupo de Tecnología, se lidere esta implementación, teniendo en cuenta que es necesario analizar de manera constante las necesidades reales de la entidad, gestionando los recursos necesarios para realizar

adquisiciones o renovaciones que correspondan y evitar así exposición de vulnerabilidades de activos de TI de la Gobernación del Huila a las amenazas del entorno.

En materia de hardware, se considera importante la renovación del centro de datos y la red de cableado estructurado en algunos pisos y áreas del Edificio Central de la Gobernación del Huila y de sus sedes, de modo que permitan optimizar la prestación de los servicios que alojan, el rendimiento de los gestores de bases de datos, la centralización de los servicios, y el procesamiento de información a través de los aplicativos y sistemas de información correspondientes.

Igualmente, se requiere ampliar el alcance en la planeación financiera de mantenimientos preventivos y correctivos sobre los activos tecnológicos de la entidad, para cubrir la demanda existente, y ampliarla a algunos activos especiales (plotter, voz IP, videowall, radios de comunicación, entre otros), y disminuir los tiempos de atención de fallas, incidentes y recuperación de incidentes y eventos de seguridad asociados.

Con la puesta en marcha del nuevo portal web institucional de la Gobernación del Huila, se recomienda realizar verificación de accesibilidad y auditoría periódica de seguridad web, y de los diferentes aplicativos y sistemas de información que cuenten con entornos web, ya sea para uso de servidores públicos, funcionarios y contratistas, o para uso de la ciudadanía, con el fin de evitar hallazgos y subsanar vulnerabilidades existentes.

Aunque en la última vigencia se realizó la puesta en marcha de un software de respaldo de información para equipos de cómputo de la entidad, su uso ha sido priorizado para alrededor de 200 funcionarios, sin cubrir la totalidad de equipos vinculados a la red. Es por esto que es necesario establecer, difundir y fomentar la apropiación de buenas prácticas relacionadas con el respaldo de información gestionada por los funcionarios de la entidad, para garantizar así la disponibilidad de ésta ante eventos o incidentes.

En los lineamientos relacionados con adquisición de software, sistemas de información, y aplicativos, es importante definir aspectos como escalabilidad e interoperabilidad con otros sistemas, el tipo de uso y derechos de autor que contrata la entidad en dichos procesos, para que eventuales modificaciones, actualizaciones o complementos que se requieran, sean tenidas en cuenta en caso de que sea necesaria una asignación presupuestal adicional.

Teniendo en cuenta de que algunos servicios de soporte técnico especializado se prestan mediante outsourcing, es necesario que se incluyan acuerdos y cláusulas de confidencialidad para la gestión de información de carácter reservada que sea facilitada, así como diferentes controles de registro de auditoría y logs de seguridad, que permita el monitoreo de los sistemas de información, bases de datos, y demás herramientas habilitadas a este personal.

Es importante el seguimiento de los indicadores planteados del modelo de gestión de seguridad de la información, como principal herramienta para presentar, comunicar, concertar, evaluar y mejorar los resultados y gestión frente a la seguridad de la información en la Gobernación del Huila, ya que son métricas que pueden ser expresadas en lenguaje del negocio, siendo así una herramienta de gran valor para trasladar su importancia y evolución a la alta dirección de la entidad.

De igual forma, es importante resaltar la importancia de la gestión de los incidentes de seguridad en este modelo, ya que corresponde a una pieza fundamental para su buen desarrollo en la entidad, requiriendo establecer procedimientos y sensibilización adecuada a los responsables y colaboradores para gestionarlos adecuadamente, ante las causas y consecuencias que puedan generar, y teniendo en cuenta factores adicionales como el impacto, la prioridad y los tiempos de atención y respuesta necesarios.

Así mismo es importante el monitoreo de los diferentes tipos de incidentes, para generar de una base de conocimientos y lecciones aprendidas, que permita posteriormente atención y respuesta con mayor inmediatez a futuros incidentes de seguridad relacionados, y que incluso puedan surgir fuera de su entorno conocido.

Por último, y una vez el modelo de gestión de seguridad de la información planteado logre un nivel de madurez importante, es posible complementarlo en lo relacionado con la gestión de la continuidad del negocio, teniendo como base las actividades planteadas según el dominio A17 del Anexo A de la Norma ISO 27001:2013 (*Aspectos de Seguridad de la Información en la Gestión de Continuidad del Negocio*), de modo que se gestionen amenazas y riesgos potenciales y emergentes sobre los servicios críticos de la entidad, de manera que promueva la prevención y protección proactiva de la infraestructura de TI, y fortalezca y facilite los procesos de respuesta efectiva ante eventos o incidentes disruptivos de seguridad de la información.

7.2. Conclusiones

En el diagnóstico realizado a los activos de TI de la Administración, se encontraron deficiencias en la infraestructura tecnológica y prestación de servicios de TI, que facilitan y aumentan la probabilidad de materialización de riesgos relacionados con el acceso no autorizado a los sistemas y de la información gestionada en ellos, la interrupción e indisponibilidad de los sistemas de información y aplicativos de la entidad, y por consiguiente, de los servicios de TI que se ofrecen, la modificación deliberada y no autorizada de información gestionada en bases de datos a cargo de la Gobernación del Huila, y la ausencia de capacidades y conocimientos en materia de seguridad y privacidad de la información que posee el personal de la entidad.

Ante esto, la Gobernación del Huila cuenta con un manual de políticas y lineamientos asociados al desarrollo de las actividades del proceso de Gestión y Seguridad de Tecnologías de la Información, pero que requieren en algunos casos de actualización y/o modificaciones respecto a normatividad, puesta en marcha de nuevas herramientas y servicios de TI, trabajo remoto y virtualidad, entre otros aspectos.

Además de lo anterior, estos lineamientos son desconocidos por los funcionarios de la entidad, al no haber sido divulgados de manera efectiva, mediante los planes de capacitación institucional del talento humano, y, sobre todo, al no haber sido socializados ante la alta dirección de la entidad, de modo que se lidere estratégicamente la apropiación de éstos, y se garantice su continuidad

Así mismo existen otros controles que se aplican en la entidad, como la contratación de servicios especializados de soporte técnico para sistemas de información y para la administración de servidores y red de comunicaciones de la entidad ante la falta de personal capacitado, y el aseguramiento de información de equipos de cómputo vinculados a la red la entidad mediante un servidor de respaldo de información.

Respecto al talento humano, la Gobernación del Huila no cuenta con personal calificado en buenas prácticas de seguridad de la información, ya que los planes de capacitación y sensibilización internos dispuestos por el área de Talento Humano no incluyen el fortalecimiento de las competencias y habilidades específicas. Salvo iniciativas

externas y proyectos de inversión que incluyen actividades relacionadas, la destinación de recursos para capacitar el personal del área es nula.

La institucionalidad de TI en las entidades públicas del orden territorial corresponde a un factor importante al momento de establecer e implementar sistemas de gestión de TI, y la falta de ésta es un común denominador en muchas entidades. En el caso de la Gobernación del Huila, la gestión de TI no cuenta con una estructura organizacional que la respalde, ya que las actividades de dicho proceso son desarrolladas por un grupo de trabajo (Grupo de Tecnología) sin la debida asignación de recursos para el cumplimiento de las obligaciones y lineamientos que se generan a nivel nacional.

Basado en lo anterior, y para la mitigación de los riesgos identificados y valorados, es necesario el establecimiento de nuevos controles y lineamientos, analizando consecuencias y estimando el impacto frente a la gestión de la seguridad y privacidad de la información, para que en caso de que haya consecuencias operativas al presentarse un riesgo, las afectaciones en la imagen y reputación de la entidad sean mínimas.

Además de la documentación de políticas y lineamientos de seguridad y privacidad de la información, para el tratamiento de estos riesgos es necesario realizar una inversión importante en el mejoramiento de la infraestructura tecnológica y de respaldo eléctrico existente que, ante algún incidente, pueda dar oportunidades de recuperación y contingencias de servicios y procesos ante incidentes o desastres.

Igualmente es importante fortalecer las capacidades, conocimientos y habilidades del personal con funciones técnicas de TI, para que sea posible suplir la prestación de servicios especializados, en caso de que se presente una interrupción del servicio más prolongada de lo habitual, ya sea por materialización de un evento o incidente, o en caso de que la entidad decida asumir la prestación de los servicios tecnológicos asociados.

A partir de esto, es necesario el establecimiento y la documentación del modelo de gestión de seguridad y privacidad de la información y de los nuevos lineamientos asociados, para implementar controles para el aseguramiento de la información y de los activos de TI de la entidad, y de esta forma optimizar los procesos y servicios ofertados a la ciudadanía.

De esta forma, el modelo de gestión de la seguridad y privacidad de la información para la Gobernación del Huila debe estar respaldado por una estructura organizacional

que fortalezca la institucionalidad tecnológica, y que facilite y acompañe la alineación de estos lineamientos con los principios estratégicos de la Gobernación del Huila, puesto que dichas acciones quedarían sin fundamento, al no soportar o apoyar la toma de decisiones en los procesos de gestión de la entidad.

Por tal motivo, establecer esta política general es una de las primeras acciones que se plantean en la implementación del Modelo de Seguridad y Privacidad de la Información, con el fin de evitar que a futuro se requieran ajustes en las políticas, procedimientos, y demás acciones específicas establecidas en dicho plan, debido al desconocimiento de éstas por la alta dirección, al no ser precisas y relacionadas con los objetivos y actividades estratégicas y primordiales de la entidad.

Al generar este modelo de gestión, adaptándolo a las condiciones propias y necesidades del entorno en el que se encuentra la Gobernación del Huila, se facilita la apropiación, transferencia de conocimiento, y por consiguiente continuidad en su ejecución con el cambio de personal y periodo de gobierno, dada las características, normas técnicas, metodologías adaptadas, y herramientas de apoyo dispuestas para su aplicación.

Así mismo, el esquema del modelo planteado facilita el entendimiento de la gestión de seguridad y privacidad de la información en entidades públicas territoriales, categorizando la documentación necesaria para su implementación, con el fin de que desde la fase de planificación se identifiquen todas las acciones necesarias para disminuir la probabilidad de riesgos asociados, disminuir vulnerabilidades, y asegurar los activos de TI de las entidades.

A través de la implementación del presente modelo de gestión de seguridad y privacidad de la información, es clave establecer una cultura organizacional en esta materia entre los funcionarios de la entidad, para dinamizar los diferentes procesos en función del uso y apropiación de TI necesario en cada uno, disminuir el riesgo de eventos e incidentes, y generar confianza en grupos de interés de la entidad.

8. Referencias

ADALID. (Septiembre de 2018). *ANEXO TECNICO: BUENAS PRÁCTICAS Y MARCO NORMATIVO DE LA SEGURIDAD DIGITAL*. Obtenido de http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/Buenas_practicas_marco_normativo.pdf

Calvo Sánchez, J. A., & Parada Serrano, D. J. (2010). *https://repository.upb.edu.co/bitstream/handle/20.500.11912/1007/digital_19847.pdf?sequence=1.* Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/1007/digital_19847.pdf?sequence=1

Centro Cibernético Policial. (2020). *Balance Cibercrimen 2020.* Obtenido de BLSC20335DS1: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

Departamento Nacional de Planeación. (11 de Abril de 2016). *Documento CONPES 3854: Política Nacional de Seguridad Digital*. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Freshservice Inc. (s.f.). *ITIL 4.* Obtenido de https://freshservice.com/latam/itil/itil-4/

Función Pública. (Octubre de 2018). *Guía para la administración del riesgo y el diseño de controles en entidades públicas.* Obtenido de Riesgos de Gestión, Corrupción y Seguridad Digital: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual

Gobernación del Huila. (06 de 2009). *Resolución 223 de 2009 "Por medio del cual se conforma un grupo interno de trabajo permanente en la Secretaría General y se designa el Coordinador".* Obtenido de Gaceta Departamental: https://www.huila.gov.co/publicaciones/7158/gaceta-departamental

Gobernación del Huila. (2017). *Estructura Organizacional*. Obtenido de Gobernación del Huila: https://www.huila.gov.co/general/publicaciones/7046/estructura-organizacional/

Gobernación del Huila. (agosto de 2017). *Misión y Visión. Misión*. Obtenido de https://www.huila.gov.co/publicaciones/92/mision-y-vision/

Gobernación del Huila. (agosto de 2017). *Misión y Visión. Visión*. Obtenido de https://www.huila.gov.co/publicaciones/92/mision-y-vision/

Gobernación del Huila. (2018). *Indicadores de Gestión y Seguridad de Tecnologías de la Información.* Obtenido de Gobernación del Huila: https://extranet.huila.gov.co

Gobernación del Huila. (18 de 09 de 2018). *Reseña Histórica.* Obtenido de Gobernación del Huila: https://www.huila.gov.co/publicaciones/8394/resena-historica

Gobernación del Huila. (2019). *Política de Operación para la Administración de Riesgos de la Gobernación del Huila.* Obtenido de https://extranet.huila.gov.co/

Gobernación del Huila. (2020). *Catálogo de Servicios TI*. Obtenido de Gobernación del Huila: https://www.huila.gov.co/documentos/1382/catalogo-de-servicios-ti/

Gobernación del Huila. (2020). *Indicadores de Gestión y Seguridad de Tecnologías de la Información*. Obtenido de https://extranet.huila.gov.co

Gobernación del Huila. (2021). *Mapa de Procesos*. Obtenido de Gobernación del Huil: https://www.huila.gov.co/publicaciones/10739/mapa-de-procesos/

Gobernación del Huila. (2021). *Matriz de Identificación, Tratamiento y Seguimiento de Riesgos de Seguridad Digital*. Obtenido de Mejora continua y revisión del Sistema de Gestión: https://extranet.huila.gov.co/Site.aspx?Codigo=07DA00A4-CD98-435F-BF5E-97CAE8D8C520&p=/Descarga&ID=3814

Gutierrez Amaya, C. (14 de Mayo de 2013). *MAGERIT: metodología práctica para gestionar riesgos.* Obtenido de We Live Security by ESET: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

ICONTEC. (2012). *Norma Técnica NTC-ISO-IEC Colombiana 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.* Obtenido de https://tienda.icontec.org/producto/e-book-ntc-iso-iec27001-tecnologia-de-la-informacion-tecnicas-de-seguridad-sistemas-de-gestion-de-la-seguridad-de-la-informacion-requisitos/?v=42983b05e2f2

Interpolados. (22 de Septiembre de 2020). *ITIL 4: PRÁCTICAS DE GESTIÓN DE ITIL: GESTIÓN DE ACTIVOS DE TI.* Obtenido de https://interpolados.wordpress.com/2020/09/22/itil-4-practicas-de-gestion-de-itil-gestion-de-activos-de-ti/

ISACA. (2013). *Modelo de Evaluación de Procesos (PAM): Usando COBIT 5.* Obtenido de http://www.isaca.org/COBIT/Pages/COBIT-5-PAM.aspx

ISO. (2018). *ISO 31000:2018.* Obtenido de Risk management -- Guidelines: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:es

ISO. (2018). *ISO/IEC 27005:2018.* Obtenido de nformation technology - Security techniques - Information security risk management systems: https://www.iso.org/standard/75281.html

ISO27K Information Security Forum. (2018). *ISO27k SOA 2013 in 5_languages.* Obtenido de https://www.iso27000.es/assets/files/ISO27k%20SOA%202013%20in%205%20languages.xlsx

ISOTools Excellence Colombia. (2017). *Gestión de Riesgos: diferencias entre ISO 31000 e ISO 27001.* Obtenido de https://www.isotools.org/2017/06/11/gestion-de-riesgos-diferencias-entre-iso-31000-e-iso-27001/

Mantilla Guerra, A. R. (2018). *Gestión de seguridad de la información con la norma ISO 27001:2013*. Obtenido de Revista Espacios: https://www.revistaespacios.com/a18v39n18/18391805.html

Mendoza, M. Á. (2 de Marzo de 2017). *We Live Security by ESET*. Obtenido de El derecho a la privacidad en la era digital: https://www.welivesecurity.com/la-es/2017/03/02/derecho-a-la-privacidad-era-digital/

Ministerio TIC. (25 de 05 de 2015). *Guía de indicadores de gestión para la seguridad de la información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

Ministerio TIC. (2016). *Guía de Gestión de Riesgos*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

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

Ministerio TIC. (29 de Julio de 2016). *Modelo de Seguridad y Privacidad de la Información*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Ministerio TIC. (17 de 03 de 2016). *Plan de Capacitación, Sensibilización Y Comunicación de Seguridad de la Información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

Ministerio TIC. (2017). *Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información* . Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf

Ministerio TIC. (08 de 2018). *Gobierno Digital - Estrategia GEL.* Obtenido de http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html

Ministerio TIC. (2019). *Taller "Más seguridad, mejor región"*. Recuperado el 2018, de Gobierno Digital: https://www.gobiernodigital.gov.co/623/articles-102189_recurso_7.pdf

Ministerio TIC. (s.f.). *Modelo de Seguridad.* Obtenido de https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

PAE - Portal de Administración Electrónica. (2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

Pajarito Sánchez García, L. J. (noviembre de 2008). *Gobernación del Huila. Gaceta Departamental. Decreto N° 1338 de 2008 "Por el cual se define la estructura orgánica de la Administración Departamental y se dictan otras disposiciones".* Obtenido de https://www.huila.gov.co/publicaciones/7158/gaceta-departamental/

Procuraduría General. (25 de Septiembre de 2014). *PREGUNTAS FRECUENTES DE LA LEY DE TRANSPARENCIA Y DEL DERECHO AL ACCESO A LA INFORMACION 1712 DE 2014*. Obtenido de https://www.procuraduria.gov.co/portal/media/file/PREGUNTAS.pdf

Red Cultural del Banco de la República de Colombia. (s.f.). *Red Cultural del Banco de la República de Colombia - Banrepcultural. Sectores Económicos. Sector Terciario o de Servicios.* Obtenido de http://enciclopedia.banrepcultural.org/index.php?title=Sectores_econ%C3%B3micos

Rouse, M. (Junio de 2014). *TechTarget*. Obtenido de Privacidad de datos (privacidad de información): https://searchdatacenter.techtarget.com/es/definicion/Privacidad-de-datos-privacidad-de-informacion

SGSI. (21 de Mayo de 2015). *ISO 27001: ¿Qué significa la Seguridad de la Información?* Obtenido de https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

Superintendencia de Industria y Comercio. (05 de Enero de 2009). *Ley 1273 de 2009*. Obtenido de https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Universidad Distrital Francisco José de Caldas. (s.f.). *Seguridad de la Información*. Obtenido de Política para la Seguridad de la Información de la Universidad Francisco José de Caldas: https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf