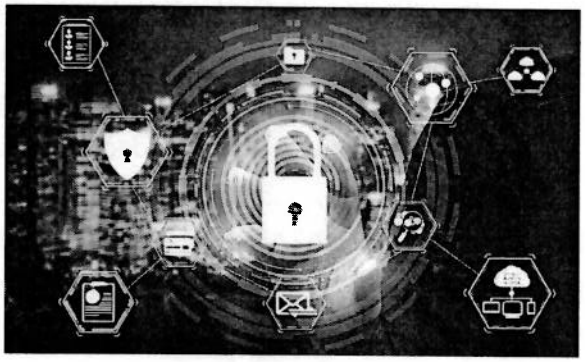
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

2024

El plan de tratamiento de riesgos de seguridad digital se formuló considerando la tecnología como herramienta transversal que soporta la prestación de servicios y ejecución de actividades misionales de cara al ciudadano, para generar valor y cumplir de manera efectiva las metas del Plan de Desarrollo Departamental.

Grupo de Tecnologías de la Información y la Comunicación



	Elaboró	Revisó	Aprobó
Firma			
Nombre	*Yesinith Varela Bonilla*	*Yesinith Varela Bonilla*	*Rodrigo Hernández Polania*
Cargo	*Líder de Proceso*	*Líder de Proceso*	*Secretaria General*

TABLA DE CONTENIDO

Introducción

El Plan de Tratamiento de Riesgos de Seguridad Digital de la GOBERNACIÓN DEL HUILA es resultado de un ejercicio de planeación estratégica realizado por el proceso GESTION Y SEGURIDAD DE TECNOLOÍGAS DE LA INFORMACIÓN, para determinar acciones específicas que permitan gestionar los riesgos de seguridad de la información que se deben mitigar, e implantar los controles necesarios para minimizar los riesgos que persistan, propendiendo por el buen uso y la privacidad de los datos y la información que los ciudadanos brindan a la entidad 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, y metas del plan de desarrollo.
El presente plan es formulado para la vigencia 2024 y se encuentra enmarcado en los planes de desarrollo nacional y departamental, así como en los lineamientos del Modelo Integrado de Planeación y Gestión y la política de Gobierno Digital.

1. OBJETIVO ESTRATÉGICO

Establecer estrategias y definir acciones que conlleven a la disminución de amenazas y vulnerabilidades asociadas a los activos de información de la GOBERNACIÓN DEL HUILA, y que pueden afectar o impedir el logro de los objetivos institucionales y estratégicos, fortaleciendo el enfoque preventivo referente a la seguridad y privacidad de la Información, y garantizando su confidencialidad, integridad y disponibilidad.

1.1 Objetivos Específicos

- Definir controles y acciones de tratamiento de riesgos inherentes de seguridad digital que puedan afectar a la GOBERNACIÓN DEL HUILA, de acuerdo a los lineamientos del Departamento Administrativo de la Función Pública -DAFP- y el Ministerio TIC.
- Proteger y preservar la confidencialidad, la integridad, y la disponibilidad de los activos de seguridad digital de la GOBERNACIÓN DEL HUILA.
- Cumplir con los lineamientos legales, reglamentarios y técnicos pertinentes y relevantes, así como también buenas prácticas y requerimientos según el contexto interno establecido en materia de seguridad digital en la entidad.
- Fortalecer, promover y apropiar conocimientos referentes a la gestión de riesgos de seguridad digital, en la cultura organizacional de la GOBERNACIÓN DEL HUILA.

2. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad Digital presenta los controles y tratamientos definidos para aplicar sobre las causas de los riesgos inherentes de seguridad digital analizados y evaluados para los 36 procesos de gestión de la GOBERNACIÓN DEL HUILA, producto de la aplicación de la Política Institucional de Gestión de Riesgo, la cual abarca para los riesgos de seguridad digital, el diagnóstico de los activos de seguridad

digital de cada uno de los procesos de gestión de la entidad, el nivel de criticidad de los mismos en base a la confidencialidad, integridad y disponibilidad de dichos activos, el análisis de los riesgos de seguridad existentes en base a causas, probabilidad de ocurrencia, nivel de impacto, vulnerabilidades, amenazas relacionadas, y por último la identificación de brechas y no conformidades.

3. MARCO NORMATIVO

- Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 415 de 2016, definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- Artículo 232 de la Ley 1450 de 2011, racionalización de trámites y procedimientos al interior de las entidades públicas.
- Decreto Ley 019 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- Decreto 2573 de 2014, reglamenta parcialmente la Ley 1341 de 2009 y que en el mismo decreto se define el componente de Privacidad y Seguridad de la información que incluye el modelo de seguridad y privacidad de la información (MSPI.
- Resolución N 2710 de 2017, por la cual se establecen lineamientos para la adopción del protocolo IPv6
- Decreto 1499 de 2017, definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.
- Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- CONPES 3701 de 2011, Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016, Política Nacional de Seguridad digital.

4. MARCO REFERENCIAL

4.1 Política de operación para la administración de riesgos de gestión, corrupción y seguridad digital

La Gobernación del Huila como ente coordinador y articulador del desarrollo sostenible del Departamento, está comprometida con la política de operación para la administración de riesgos que pudieran afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos, planes institucionales, la satisfacción de los usuarios y el manejo transparente de los recursos públicos, a partir de la elaboración y adopción de la presente política de operación y la herramienta de trabajo, documentos técnicos que facilitan la buena "Gestión y Administración de los riesgos de gestión, corrupción y seguridad digital", a través de los cuales se establecieron los lineamientos para la identificación, valoración, Diseño y ejecución de controles, tratamiento y seguimiento de dichos riesgos, tomando como referentes las directrices establecidas por el Departamento Administrativo de la Función Pública -DAFP y del Modelo Integrado de Planeación y Gestión – MIPG, conforme a la política de "Direccionamiento estratégico y planeación", de "Definir la política de administración de riesgos, identificar y valorar riesgos (operativos, corrupción, contratación y defensa jurídica), de acuerdo con la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI, la Guía para la Administración del riesgo del DAFP, el Modelo de Seguridad y Privacidad de la información de la estrategia de Gobierno Digital y la Secretaría de Transparencia de la Presidencia de la República desde su estrategia Plan Anticorrupción y de Atención al Ciudadano.

En tal sentido, la Gobernación del Huila actualizará anualmente sus mapas de Riesgos de gestión, corrupción y seguridad digital, con el fin de ajustar controles y mitigar los riesgos en el marco de la viabilidad jurídica, técnica, financiera y económica, de acuerdo con el tratamiento que se defina par cada uno de éstos: evitar, aceptar, compartir o reducir el riesgo. Los responsables de cada proceso, junto con sus equipos de trabajo, serán quienes adelanten la ejecución de los controles y las acciones preventivas y realicen el seguimiento a su cumplimiento como primera línea de defensa y mecanismo de autocontrol, conforme lo establece el Esquema de asignación de responsabilidades establecido.

Estos lineamientos, deben ser acatados por todos los servidores públicos y contratistas de la entidad en el desarrollo de sus funciones, compromisos y obligaciones, buscando que éstos conduzcan a disminuir la vulnerabilidad frente a las diferentes situaciones que puedan interferir en el logro de la misionalidad y objetivos institucionales y preparar la respuesta oportuna a amenazas externas que puedan generar eventos de riesgo.

5. METODOLOGÍA DE GESTÓN DE ACTIVOS DE SEGURIDAD DIGITAL

La Gobernación del Huila, adoptando los lineamientos establecidos por el Departamento Administración de la Función Pública, en la "*Guía para la Administración del Riesgo y el*

Diseño de Controles en Entidades Públicas", Versión 5 de diciembre de 2020, y en el anexo 4 "*Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas*", ha establecido la siguiente metodología, a fin de gestionar sus activos de seguridad digital:

5.1 Identificación, análisis y valoración de activos

Es necesario identificar los activos de TI y documentarlos mediante un inventario de activos, así podrá saber lo que se debe proteger para 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. Lo anterior se realiza mediante encuestas y entrevistas con funcionarios líderes de procesos de gestión de la entidad. Se clasifican y cuantifican según funcionalidades, y se valoran según criterios de la norma técnica ISO/IEC 27001, evaluando de manera acertada cada una de las dimensiones de seguridad para cada activo. Esta información se recopiló en un cuadro denominado "Matriz de Identificación de Activos de Seguridad Digital", 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.

PASOS PARA LA IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DIGITAL							
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

- **Paso 1 - Listar activos:** Se listan los activos de seguridad digital, correspondientes a los activos de TI que se identifican en cada proceso de gestión, indicando nombre y descripción breve de cada uno.

- **Paso 2 - 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.

- **Paso 3 - 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.

- **Paso 4 - Identificar custodio del activo:** Cada uno de los activos identificados debe tener una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que posteriormente se definan.

- **Paso 5 - 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 y demás normatividad aplicable. Posteriormente se evalúa la criticidad de los activos, determinando el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para 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.

- **Paso 6 - 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.

- **Paso 7 y 8 - Identificación de Amenazas y Vulnerabilidades:** Existen diversos lineamientos y estándares como la Norma Técnica ISO/IEC 27005 y MAGERIT, que muestran posibles amenazas y vulnerabilidades que pueden materializar los tres tipos de riesgos de seguridad digital (pérdida de confidencialidad, pérdida de integridad, pérdida de disponibilidad). En este caso, se utiliza el cuadro denominado "Matriz de Identificación de Activos de Seguridad Digital", 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.

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**

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**

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.

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**

- **Paso 9 - Identificar infraestructuras críticas cibernéticas – ICC:** Se identifican y reportan a instancias y autoridades respectivas en el Gobierno nacional si la Gobernación del Huila posee ICC. Un activo es considerado infraestructura crítica cibernética 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. Para esta identificación, se sigue utilizando el cuadro denominado "Matriz de Identificación de Activos de Seguridad Digital", en el que, en el 9no paso, se indica si el activo corresponde a un activo de infraestructura crítica cibernética, y en el paso 10 se incluyen observaciones adicionales que se consideren relevantes sobre el activo para su análisis y diagnóstico.

PASOS PARA LA IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DIGITAL							
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.

6. METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Siguiendo con la adopción de lineamientos del Departamento Administrativo de la Función Pública, la Gobernación del Huila ha establecido la "*Política de operación para la administración de riesgos de gestión, corrupción y seguridad digital*", a fin de gestionar sus riesgos de seguridad digital:

6.1 Análisis y Valoración de Riesgos de Seguridad Digital

Los riesgos de seguridad digital 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. Cabe añadir que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo. 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.

- **Identificación de 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

Financieras	Operativas	Legales	Reputación
•Pérdida de dinero •Retraso en pago de nómina	•Desarrollo de actividades a media marcha •Pérdida de tiempo operacional	•Demandas y acciones judicialespor incumplimiento de legislación nacional	•Inhabilidad de servicios a los ciudadanos •Desconfianza en la entidad

- **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, que está incluida en el formato "Matriz de Identificación y Valoración de Riesgos".

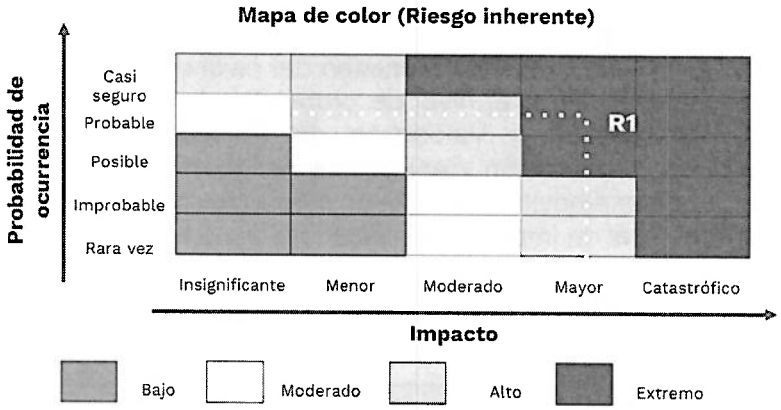
PROBABILIDAD DE OCURRENCIA DE RIESGOS DE SEGURIDAD			
NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último 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

- **Valoración de impacto:** El impacto se analiza y califica a partir de las consecuencias identificadas en la fase de descripción del riesgo. Cabe añadir que la probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades. 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" 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.

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



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

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

MATRIZ DE IDENTIFICACIÓN Y VALORACIÓN 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
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, documentos y flujos de información	Incumplimiento del plan anual de visitas de inspección y vigilancia
						Cambio del administrador del portal web	Retrasos en la publicación de actos administrativos

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

MATRIZ DE IDENTIFICACIÓN Y 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:	¿ Controles ayudan a disminuir el impacto ?	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					1	2	3	4	5	1	2	3	4	5				
5					4					Extremo				No	Sin control							3					2					Moderado			
														No	Sin control																				
														Si	Moderado	Fuerte	Moderado	Si	Moderado	Directamente	Indirectamente														
														No	Sin control																				
														No	Sin control																				
														No	Sin control																				
														No	Sin control																				
4					4					Extremo				No	Sin control							4					4					Extremo			
														No	Sin control																				
														No	Sin control																				
														No	Sin control																				
														No	Sin control																				
														No	Sin control																				
														Si	Débil	Fuerte	Débil	Si	Débil	No disminuye	No disminuye														

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.	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 mediante el formato "FORMATO CONTROL INFORMACIÓN ENTREGADA Y SUBIDA A LA EXTRANET"	15	5	65	Débil

6.2 Tratamiento de Riesgos de Seguridad Digital

Una vez se han identificados, analizados y evaluados los riesgos, a través de la aplicación de la Política de operación para la administración de riesgos de seguridad digital, la Gobernación del Huila debe definir el tratamiento para cada uno de estos riesgos analizados y evaluados, involucrando la selección de opciones para modificarlos, entre las que se encuentran las siguientes: evitar, aceptar, compartir o reducir el riesgo.

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, y sobre las cuales se definen acciones que permitan el cumplimiento de dicha estrategia.

Tabla 3. Estrategias de Tratamiento de Riesgos de Seguridad Digital

Zona de Riesgo	ESTRATEGIAS DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL 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 de riesgo del proceso 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 - SGI

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 6. Matriz de Identificación y Valoración de Riesgos – Fase 3: Tratamiento y Seguimiento de Riesgos).

Tabla 4. Matriz de Identificación y Valoración de Riesgos – Fase 3

MATRIZ DE IDENTIFICACIÓN Y VALORACIÓN 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 - INCIO	F - FIN	RESPONSABLE DE LA ACCIÓN	F- SEGUIMIENTO	EVIDENCIA O SOPORTE	SEGUIMIENTO DESCRIPCIÓN	PORCENTAJE DE AVANCE

6.3 Declaración de Aplicabilidad SOA

La Declaración de aplicabilidad es el nexo principal entre la evaluación y el tratamiento del riesgo, y la implementación del Modelo de Seguridad y Privacidad de la Información. El objetivo de este documento es definir cuáles de los controles (medidas de seguridad) sugeridos en el Anexo A de la norma ISO 27001 son los que se implementarán y, para los controles que correspondan, cómo se realizará su implementación en la Gobernación del Huila, y/o justificar por qué algunas medidas serán excluidas (las innecesarias y la razón del por qué no son requerías por la Entidad). Lo anterior, teniendo en cuenta que surgió una nueva versión de la norma, que modificó los controles a implementar, y por tanto, se debe realizar una declaración, acorde a la nueva versión de la norma técnica ISO 27001 (2022).

Tabla 5. Encabezado de Declaración de Aplicabilidad (SOA) de Controles de Seguridad Digital

Vigente hasta el: 31/12/2024
Declaración de Aplicabilidad
La presente declaración se establece sobre los controles que son relevantes para el Plan de Tratamiento de Riesgos de Seguridad Digital 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, entre los motivos de selección se pueden encontrar: resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, requisitos legales o reglamentos, obligaciones contractuales y necesidades empresariales de la organización en materia de seguridad de la información: **RL**: requerimientos legales, **OC**: obligaciones contractuales, **RN/PA**: requerimientos del negocio/mejores prácticas adoptadas , **RVR**: resultado de la valoración de riesgos;

Tabla 6. Esquema para Declaración de Aplicabilidad (SOA) de Controles de Seguridad Digital

Declaración de Aplicabilidad (SOA) de Controles de Seguridad Digital									
ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					RL	OC	RN/PA	RVR	
Cláusula	Sección	Objetivo de control / control							
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	Cumplido					
	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

6.4 Comparativo Análisis y Evaluación de Riesgos 2022-2023

Realizando un análisis comparativo del análisis, evaluación y tratamiento de riesgos de seguridad digital realizado entre las vigencias 2022 y 2023, arrojan una disminución (variación negativa) del total de riesgos de seguridad digital del 11%, teniendo como referencia que se identificaron 116 riesgos en 2023, frente a los 130 identificados en la vigencia anterior.

Total Riesgos 2022	Total Riesgos 2023	Variación Riesgos Seguridad Digital 2022-2023	
130	116	-14	-11%

Dicha variación se concentró principalmente en la disminución de riesgos de nivel extremo y de nivel alto, en áreas de gestión de información clasificada dentro de procesos misionales de la Gobernación del Huila (p.e. Secretaría de Salud, Departamento de Planeación, entre otros).

Variación Nivel de Riesgo de Seguridad Digital 2022-2023	Extremo	Alto	Moderado	Bajo
	-8	-6	-1	1

Lo anterior, refleja la ejecución de las diferentes acciones de tratamiento implementadas en los diferentes procesos de la Gobernación del Huila, para la mitigación de riesgos de seguridad digital, a partir del liderazgo del Grupo de Tecnología en la implementación del Modelo de Seguridad y Privacidad de la Información, así como también de la Coordinación del Sistema Integrado de Gestión en la Política de Administración del Riesgo de la entidad.

7. DOFA

Como resultado del análisis DOFA, se identifica la necesidad de desarrollar estrategias y acciones que permitan fortalecer la gestión de riesgos de seguridad digital en la Gobernación del Huila, a partir de políticas de administración de riesgos que actualmente se fortalecen permanentemente, aprovechando para ello los nuevos lineamientos, normatividades, nuevas tecnologías disponibles y tendencias en transformación digital para implementar controles y acciones de tratamiento que permitan mitigar los riesgos y disminuir las amenazas y vulnerabilidades que pueden afectar los activos de seguridad digital de cada uno de los procesos de la entidad.

Así mismo, es importante direccionar recursos desde entidades del orden nacional asociadas a TI (como el Ministerio TIC, el Departamento de Función Pública, entre otras) para el fortalecimiento de las capacidades y competencias del talento humano de la entidad, y de esta manera, avanzar en el cumplimiento e implementación de buenas prácticas, estándares y normatividad nacional, entre los que se destacan la Política de Gobierno Digital, la Política de Seguridad Digital, y el Índice de Desempeño Institucional del FURAG. Lo anterior, permitirá seguir fortaleciendo los conocimientos, experiencia y resultados obtenidos y documentados en el proceso de Gestión y Seguridad de TI de la entidad, y atendiendo así los riesgos que se identifiquen en la entidad.

Tabla 7. Matriz DOFA para el Plan de Tratamiento de Riesgos de Seguridad Digital

<table>
<tr><th>OPORTUNIDADES (externas)</th><th>DO</th><th>DA</th><th>AMENAZAS (externas)</th></tr>
<tr><td>Incentivos por entidades del orden nacional asociadas a TI para la formación del talento humano en seguridad de la información</td><td>Realimentación a partir de riesgos de seguridad digital identificados</td><td>Aplicación de nuevas metodologías de gestión de riesgos de seguridad digital</td><td>Incumplimiento de la normatividad establecida a nivel nacional en gestión de riesgos de seguridad digital</td></tr>
<tr><td>Tendencias de innovación y transformación digital</td><td rowspan="2">Implementación y seguimiento a controles y acciones de tratamiento de riesgos de seguridad digital establecidas, a partir de nuevas tecnologías y tendencias en transformación digital.</td><td rowspan="2">Actualización de inventario de activos de seguridad digital, incluyendo nuevas amenazas y vulnerabilidades del entorno</td><td>Rezago en la implementación de buenas prácticas y estándares de protección de datos</td></tr>
<tr><td>Asistencia y acompañamiento para implementación de nuevas tecnologías</td><td>Ataques externos de malware mediante suplantación de identidad</td></tr>
<tr><th>FORTALEZAS (Internas)</th><th>FO</th><th>FA</th><th>DEBILIDADES (Internas)</th></tr>
<tr><td>Conocimiento de la entidad y sus procesos</td><td>Implementación y seguimiento a controles y acciones de tratamiento de riesgos de seguridad digital establecidas, a partir de nuevas tecnologías y tendencias en transformación digital.</td><td>Actualización de la política, metodologías y lineamientos para la gestión de activos y riesgos de seguridad digital.</td><td>Falta de inversión en protección y seguridad de TI</td></tr>
<tr><td>Revisión y mejora continua de políticas y procedimientos de seguridad de TI</td><td rowspan="2">Oportunidades de mejora acorde al seguimiento a la ejecución de controles realizado</td><td rowspan="2">Medición, presentación y reporte de indicadores de gestión de riesgos de seguridad digital</td><td>El grupo TIC no es tenido en cuenta en el nivel estratégico de la entidad</td></tr>
<tr><td>Experiencia y buenos resultados en proyectos formulados</td><td>Falta de capacitación al personal en temás técnicos de seguridad de TI</td></tr>
</table>

8. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

A continuación, se presenta el plan de tratamiento de riesgos de seguridad digital, basado en la declaración de aplicabilidad establecida anteriormente. Cabe añadir que este plan engloba la implementación de controles para mitigación de riesgos de seguridad digital en cada uno de los procesos de la Gobernación del Huila, de modo que se facilita la visualización de los controles seleccionados y las actividades a implementar para tratar los riesgos residuales.

Tabla 8. Plan de Tratamiento de Riesgos de Seguridad Digital

Plan de Tratamiento de Riesgos de Seguridad Digital					
#	Actividad	Área Responsable	Fecha Inicial	Fecha Final	Entregable
1	Apoyar actualización de la política, metodologías y lineamientos para la gestión de activos y riesgos de seguridad digital.	Grupo de Tecnología – Coordinación Sistema de Gestión	01/feb /2024	30/nov /2024	Política, metodologías y lineamientos para la gestión de activos y riesgos de seguridad digital actualizados (si corresponde)
2	Realizar levantamiento y/o actualización de inventario de activos de seguridad digital por cada proceso en la entidad.	Líderes de proceso - Grupo de Tecnología (2da línea de defensa)	01/mar /2024	30/jun /2024	Inventario de activos de seguridad digital por cada proceso en la entidad.
3	Realizar análisis de contexto, identificación de análisis, evaluación y/o actualización de riesgos de seguridad digital por cada proceso en la entidad.	Líderes de proceso - Grupo de Tecnología (2da línea de defensa)	01/abr /2024	30/jul /2024	Versión inicial de mapas de riesgos de seguridad digital por cada proceso en la entidad.
4	Realizar realimentación, revisión y verificación de los riesgos identificados.	Grupo de Tecnología (2da línea de defensa)	01/ago /2024	30/ago /2024	Versión final de mapas de riesgos de seguridad digital por cada proceso en la entidad.
5	Aceptar y aprobar riesgos identificados y mapas de riesgos de seguridad digital por proceso.	Líderes y dueños de proceso	01/ago /2024	30/ago /2024	Mapas de riesgos de seguridad digital aprobados por líderes y dueños de cada proceso

Plan de Tratamiento de Riesgos de Seguridad Digital					
#	Actividad	Área Responsable	Fecha Inicial	Fecha Final	Entregable
6	Remitir a Coordinación del Sistema Integrado de Gestión, mapas de riesgos de seguridad digital por proceso, para su respectiva publicación.	Grupo de Tecnología (2da línea de defensa)	01/sep /2024	15/sep /2024	Correo electrónico enviado a Coordinación del Sistema de Gestión adjuntando los mapas de riesgos de seguridad digital
7	Publicar mapas de riesgos de seguridad digital de los procesos en el Sistema Integrado de Gestión.	Coordinación Sistema de Gestión	15/sep /2024	30/sep /2024	Mapas de riesgos de seguridad digital de cada proceso publicados en el Sistema Integrado de Gestión
8	Realizar seguimiento a la implementación de controles y planes de tratamiento de riesgos de seguridad digital identificados.	Líderes de proceso - Grupo de Tecnología (2da línea de defensa)	01/feb /2024	30/nov /2024	Seguimiento a acciones de tratamiento los mapas de riesgos de seguridad digital de cada proceso
9	Identificar oportunidades de mejora acorde al seguimiento a la ejecución de controles realizado.	Todas las dependencias	01/feb /2024	30/nov /2024	Planes de mejora derivados del seguimiento de riesgos de seguridad digital
10	Revisar y/o actualizar si corresponde, lineamientos de gestión de riesgos de seguridad digital, según las oportunidades de mejora identificadas y presentadas.	Grupo de Tecnología – Coordinación Sistema de Gestión	01/sep /2024	30/nov /2024	Lineamientos de gestión de riesgos de seguridad digital actualizados
11	Realizar medición, presentación y reporte de indicadores correspondientes.	Grupo de Tecnología – Coordinación Sistema de Gestión	01/feb /2024	30/nov /2024	Reporte de indicadores de cumplimiento de acciones de mejora y riesgos de seguridad digital

9. FUENTES DE INFORMACIÓN

- DAFP (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4
- DAFP (2018). Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018
- Durán Rodríguez, E., & Londoño de Perdomo, A. C. (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".
- MINTIC (2009). Ley 1273 de 2009.
- MINTIC (2016). Modelo de Seguridad – Fortalecimiento de TI.

- MINTIC (2016). Guía de Gestión de Riesgos.
- MINTIC (2016). Guía para la Gestión y Clasificación de Activos de Información.
- MINTIC (2016). Modelo de Seguridad y Privacidad de la Información.
- MINTIC (2016). Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información.
- MinTIC. (2018). Gobierno Digital - Estrategia GEL.
- MINTIC (2018). Taller "Más seguridad, mejor región". Estrategia Gobierno Digital.
- NTC ISO/IEC 27001: 2013. Sistemas de Gestión de la Seguridad de la Información
- NTC ISO/IEC 27005: 2009. Gestión del Riesgo en la Seguridad de la Información
- Pajarito Sánchez García, L. J. (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"

10. PARTICIPACIÓN CIUDADANA

Para garantizar la participación ciudadana, el presente plan se publicó el 14 de diciembre de la vigencia 2023, publicado durante un plazo de cinco (5) días hábiles en el link de transparencia de participación ciudadano de la Sede Electrónica de la Gobernación del Huila para comentarios, sugerencias y observaciones de la ciudadanía, sin observación alguna.

La Aprobación del Plan de Tratamiento de Riesgos de Seguridad Digital, se hace por parte del Comité Institucional de Gestión y Desempeño en Acta # 01 de fecha 22 de enero de 2024.

Una vez aprobado el Plan de Tratamiento de Riesgos de Seguridad Digital, por parte de los miembros del comité CIGD, éste será publicado en la Sede Electrónica de la Gobernación y en la Extranet / Sistema de Gestión MIPG / componentes estratégicos /planes integrados, para conocimiento de los servidores públicos y la ciudadanía en general.

11. SEGUIMIENTO Y CONTROL DEL PLAN

El Seguimiento y control al del Plan de Tratamiento de Riesgos de Seguridad Digital, se realizará mediante la evaluación y consolidación de resultados anuales, proceso que estará a cargo del equipo vinculado al proceso de Gestión y Seguridad de Tecnologías de la Información.

12. CONTROL DE CAMBIOS

Versión	Vigencia	Identificación de los cambios	Responsable
1	31 de enero de 2020	Primera versión	Coordinador Grupo de Tecnología, Conectividad y Telecomunicaciones y Secretario General
2	13 de mayo de 2020	Se ajustó el ítem 2, ítem 4.1 y el ítem 5 conforme al requisito de la norma ISO 27001:2013 para Controles de Seguridad digital	Coordinador Grupo de Tecnología, Conectividad y Telecomunicaciones y Secretario General
3	30 de diciembre de 2020	Se ajustó ítem 2 "Alcance", respecto al número de procesos de gestión que tienen identificación y análisis de riesgos de seguridad digital Se actualizó ítem 5.1. "Declaración de aplicabilidad SOA", respecto a la fecha de vigencia de la declaración de aplicabilidad (SoA) de controles de seguridad de la información. Se ajustó ítem 5.2."Plan de Tratamiento de Riesgos de Seguridad Digital", respecto a la actualización del porcentaje de avance de cada una de las actividades del plan, modificación de la fecha de seguimiento para éstas, y modificación de actividad asignada a objetivo de control 12.6 "Gestión de vulnerabilidades técnicas". Se ajustó ítem 6 "Conclusiones", respecto al número de procesos de los cuales se cuenta con la identificación de activos de seguridad digital.	Coordinador Grupo de Tecnología, Conectividad y Telecomunicaciones y Secretaria General

Versión	Vigencia	Identificación de los cambios	Responsable
4	21 de junio de 2021	Se incluyó en el ítem 3 "Soporte Normativo", la Resolución 500 de 2021 de Presidencia de la República. Se añadió el ítem "5. Metodología De Gestión De Activos De Seguridad Digital" y el subítem "5.1. Diagnóstico de Activos". Se ajustó numeración a 6 y se modificó ítem "Metodología de Tratamiento de Riesgos de Seguridad Digital" a "Metodología de Gestión de Riesgos de Seguridad Digital". Se añadieron los subítems 6.1. "Análisis y Valoración de Riesgos de Seguridad Digital" y 6.2. "Tratamiento de Riesgos de Seguridad Digital". Se ajustó numeración a 6.3. "Declaración de Aplicabilidad SOA", a 6.4. "Plan de Tratamiento de Riesgos de Seguridad Digital", a 7 "Conclusiones", a 8 "Recomendaciones", a 9 "Fuentes de Información", y a 10 "Control de Cambios".	Coordinador Grupo de Tecnología, Conectividad y Telecomunicaciones y Secretaria General
5	29 de enero de 2022	Se actualizó el ítem **Introducción**, el ítem No. 3 **Marco Normativo**, el ítem 5.1. **Declaración de Aplicabilidad SOA**, 5.2. **Plan Consolidado de Tratamiento de Riesgos de Seguridad Digital**. Se suprimieron los ítems 7 **Conclusiones** e ítem 8 **Recomendaciones**, al exponer vulnerabilidades de la infraestructura tecnológica de la entidad, y se modificaron numerales de ítem **Fuentes de Información** (ítem 7) y **Control de Cambios** (ítem 8).	Coordinador Grupo de Tecnología, Conectividad y Telecomunicaciones y Secretaria General

Versión	Vigencia	Identificación de los cambios	Responsable
6	13 de enero de 2023	Se actualizó el ítem 6.3. **Declaración de Aplicabilidad SOA (Diagnóstico)**, 6.4. **Plan Consolidado de Tratamiento de Riesgos de Seguridad Digital**. Se agregó ítem 8 **Participación Ciudadana.**	Coordinador Grupo de Tecnología, Conectividad y Telecomunicaciones y Secretaria General
7	22 de enero de 2024	Se actualizaron todos los ítems respecto a vigencia del plan a 2024. Se incluyó el ítem 7 "DO*FA*". Se modificó esquema y actividades del ítem 8 "*Plan de Tratamiento de Riesgos de Seguridad Digital*"	Líder de proceso y Secretaria General