PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA 2024

SIGLAS

- **ISO**: International Standard Organization.
- **MINTIC:** Ministerio de Tecnología de la Información y las Comunicaciones.
- **MOP:** Modelo de operación por procesos.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información. **SGSI:** Sistema de Gestión de Seguridad de la Información. **TI:** Tecnología de información.
- **TIC:** Tecnologías de la información y la comunicación.

NORMOGRAMA

- **Ley 909 de 2004:** "Por la cual se expiden normas que regulan el empleo público, la carrera administrativa, gerencia pública y se dictan otras disposiciones".

- **Ley 1581 de 2012:** "Por la cual se dictan disposiciones generales para la protección de datos personales".

- **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".

- **Decreto Ministerial 1078 de 2015:** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

- **Decreto Presidencial 1083 de 2015:** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

- **Decreto 612 de 2018:** "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".

- **Decreto 767 de 2022:** "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".

- **Resolución 00500 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".

- **ISO/IEC 27001:2013:** Tecnología de la información-Técnicas de seguridad-Sistemas de Gestión de la Seguridad de la Información (SGSI)- Requisitos

CONTEXTO

"**Liderar la definición, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información** de la ASAMBLEA DEPARTAMENTAL DE SANTANDER - ADS acorde al marco específico y la estrategia de la entidad."

La implementación del Sistema de Gestión de Seguridad de la Información surge en el contexto de lo expuesto en el Decreto Ministerial 1078 de 2015 referido a las obligaciones de los sujetos obligados en el artículo 2.2.9.1.1.2. para la implementación del habilitador de seguridad de la información, en atención a las orientaciones definidas en el Manual de Gobierno Digital, relacionadas con la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, refrendadas y actualizadas a través del Decreto Presidencial 767 de 2022 en lo referente al habilitador de seguridad y privacidad de la información, el cual derogo el Decreto 1008 de 2018.

De igual manera es importante resaltar que es a través del Decreto Presidencial 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", en su artículo 1, adiciona al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto Presidencial 1083 de 2015, Único Reglamentario del Sector de Función Pública, agregando al anterior Decreto el artículo 2.2.22.3.14, por medio del cual se integran los planes institucionales y estratégicos al Plan de Acción, considerando en su numeral 11 y 12 como obligación la elaboración anual del "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" y del "Plan de Seguridad y Privacidad de la Información" respectivamente de cada Entidad, y lo señalado en la Ley 1474 de 2011 por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, señala en su artículo 74 denominado "Plan de acción de las entidades públicas", indicando que a partir de la vigencia de la presente Ley, todas las entidades del Estado a más tardar el 31 de enero de cada año, deberán publicar en su respectiva página web el Plan de Acción para el año siguiente".

Coherente con lo anterior, La Corporación ha venido adelantando acciones en toda la entidad encaminadas a fortalecer las capacidades institucionales para dar cumplimiento a las disposiciones legales vigentes en materia de seguridad y privacidad de la información, atendiendo las orientaciones del Ministerio de Tecnologías de Información contenidas en la Resolución Ministerial 0500 de 2021 y sus dos respectivos anexos.

INTRODUCCIÓN

En Colombia se viene adelantando la implementación de la política de gobierno digital, tal como lo establece La Presidencia de la Republica y el Ministerio de Tecnologías de la Información y las Comunicaciones a través del Decreto 767 de 2022, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2, libro 2, como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual se ha articulado con el Modelo Integrado de Planeación y Gestión, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

El Manual de la política de Gobierno Digital expedido por el MinTIC establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Según el manual, la implementación de la política de gobierno digital se ha definido en dos componentes: TIC para el estado y TIC para la sociedad, que son habilitados por cuatro elementos transversales: Arquitectura, Cultura y Apropiación, Seguridad y Privacidad de la Información y Servicios Ciudadanos Digitales. Estos seis elementos, se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

El manual en mención, precisa que el habilitador de Seguridad y Privacidad de la Información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, tramites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

No obstante, el Artículo 2.2.9.1.2.1 del Decreto Ministerial 1078 de 2015 establece que La Política de Gobierno Digital se desarrollará a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo. En el mencionado artículo, en su numeral 3.2 recalca como habilitador, la Seguridad y Privacidad de la Información donde los sujetos obligados deben desarrollar capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El documento denominado Modelo de Seguridad y Privacidad de la Información (MSPI), expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción de este, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

La adopción, implementación y evaluación del modelo mencionado, es una actividad obligatoria según lo expresado en el artículo 2.2.9.1.3.2 del Decreto 767 de 2022. De igual manera es importante resaltar que es a través del Decreto Presidencial 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", en su artículo 1, adiciona al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto Presidencial 1083 de 2015, Único Reglamentario del Sector de Función Pública, agregando al anterior Decreto el artículo 2.2.22.3.14, por medio del cual se integran los planes institucionales y estratégicos al Plan de Acción, considerando en su numeral 11 y 12 como obligación la elaboración anual del "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" y del "Plan de Seguridad y Privacidad de la Información" respectivamente de cada Entidad.

Así mismo, la Resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, que tiene como objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información, la guía de gestión de riesgos de Seguridad de la Información y el procedimiento para la gestión de los incidentes e seguridad digital, y establecer los lineamientos y estándares para la estrategia de seguridad digital. La resolución en mención precisa la necesidad de que los sujetos obligados deban adoptar las medidas técnicas, administrativas y de talento humano para

garantizar que la seguridad digital se incorpore al Plan de Seguridad y Privacidad de la Información y así mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Es precisamente a través del artículo 5 de la resolución 0500 que se precisa la necesidad de adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, e incluirla en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos del artículo 2.22.22.3.14 del capítulo 3 del título 22 de la parte 2 del libro 2 del decreto
1083 de 2015.

Considerando que, la Resolución Ministerial 0500 de 2021, establece en su artículo 5, denominado “Estrategia de Seguridad Digital”, en especial en el numeral 2, indicando que se debe “Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos”, además, en la el anexo 1 de la misma Resolución, en su acápite “Planificación”, señala “Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo, teniendo el Plan de Tratamiento de Riesgos como el documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000), y en el mencionado anexo, en su numeral 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información, tiene como lineamiento que la Entidad debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información.

La adopción e implementación del Modelo de Seguridad y Privacidad de la información en las entidades públicas toma como sustento el estándar NTC ISO 27001:2013, así como principios regulatorios definidos por el Gobierno Nacional, tal como la Ley 1712 de 2014 o la Ley 1581 de 2012; así mismo apoyan su enfoque en la implementación de un ciclo de identificación, valoración y tratamiento de riesgos de seguridad y privacidad de la información, para lo cual se ha expedido desde el Departamento Administrativo de la Función Pública la guía para la administración del riesgo y el diseño de controles en entidades públicas, como referente para abordar los riesgos de gestión, corrupción y de seguridad de la información. La adopción de prácticas de gestión de riesgos en las entidades públicas permitirá fortalecer la toma de decisiones en cuanto a la implementación de controles de acuerdo con el plan de tratamientos definido.

Estos referentes constituyen el fundamento para la definición del plan de tratamiento de riesgos de seguridad y privacidad de la información de La Asamblea Departamental de Santander ADS sobre los activos de información que aportan al logro de los objetivos organizacionales.

CONTEXTO DEL DESARROLLO DEL PLAN 2024

En el vertiginoso escenario tecnológico que define a La Asamblea Departamental de Santander ADS, la preservación de la información emerge como una prioridad ineludible para esta entidad comprometida con impulsar los principios fundamentales de confidencialidad, disponibilidad e integridad sobre todos los activos de información que gestiona. En este contexto, el año 2023 se distingue como un momento trascendental en el fortalecimiento de la seguridad y privacidad de la información en La Corporación. Esto se logra a través del desarrollo e implementación del Plan de Seguridad y Privacidad de la Información y tratamiento de riesgos de seguridad y privacidad de la información, donde la participación de todas las dependencias de La Corporación representa un avance significativo. Esta colaboración ha permitido ampliar el alcance y mejorar la visibilidad de los activos de información que están bajo su responsabilidad.

OBJETIVO

Establecer o actualizar el marco de acción para aportar al tratamiento de riesgos de seguridad y privacidad de la información, sobre los activos de información que soportan el cumplimiento de los objetivos organizacionales, conducentes a preservar la confidencialidad, integridad y disponibilidad de la información institucional, en atención al contexto organizacional de la entidad, las capacidades y recursos disponibles, para fortalecer la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

La planeación se enfocará en fortalecer la implementación de acciones para el tratamiento de riesgos de seguridad y privacidad de la información de acuerdo a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, el departamento administrativo de la función pública, así como en atención a las observaciones que se derivan de los resultados de la auditoría realizada por la ADS de Evaluación y Control a los avances institucionales respecto de la implementación del Modelo de Seguridad y Privacidad de la Información, enfocados a la seguridad de los activos de información de La Asamblea Departamental de Santander ADS, como un aporte a las actividades que realizará la entidad en torno a la Seguridad y Privacidad de la Información institucional, teniendo en cuenta las capacidades y recursos

disponibles, para mejorar la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE INFORMACIÓN POR CATEGORÍAS

Según lo expuesto en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública, el tratamiento de riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, por lo tanto dicha planeación en este caso en particular, hace alusión al tratamiento de riesgos de Seguridad y Privacidad de la Información enfocado en la seguridad de la información sobre los activos de información a cargo de La Asamblea Departamental de Santander ADS , para lo cual se realizan un conjunto de actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados.

El primer grupo del plan está destinado a los participantes de todas las dependencias de La Asamblea Departamental de Santander ADS que no hayan llevado a cabo ninguna de las actividades contempladas en el marco de ejecución del plan de tratamiento de riesgos de seguridad y privacidad de la información durante la vigencia 2023. El segundo grupo del plan está destinado a los participantes de todas las dependencias de La Asamblea Departamental de Santander ADS que hayan llevado a cabo alguna entrega o seguimiento en la ejecución de las actividades contempladas en el marco del plan de tratamiento de riesgos de seguridad y privacidad de la información durante la vigencia 2023.

En atención a lo anterior, a continuación, se describen las actividades más relevantes orientadas al tratamiento de riesgos de Seguridad y Privacidad de la Información para cada grupo:

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - GRUPO 1													
Actividad	**Responsable**	**1 semestre 2024**						**2 semestre 2024**					
		E	**F**	**M**	**A**	**M**	**J**	**J**	**A**	**S**	**O**	**N**	**D**
Realizar la identificación de controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, Valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia.	Todas las Dependencias en caso de realizar la ejecución del plan de forma individual.								X	X	X	X	
Realizar la adquisición e implementación de controles de seguridad de la información identificados, para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia.	Todas las Dependencias en caso de realizar la ejecución del plan de forma individual.								X	X	X	X	X
Realizar la identificación, clasificación, tratamiento y divulgación de Incidentes s seguridad de la información materializados en atención a los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia de la Corporación.	Todas las Dependencias en caso de realizar la ejecución del plan de forma individual.								X	X	X	X	X
Realizar el seguimiento a las actividades de identificación, adquisición e implementación de controles de seguridad de la información, así como de tratamiento de incidentes de seguridad de la información, para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia.	Todas las Dependencias en caso de realizar la ejecución del plan de forma individual									X		X	

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - GRUPO 2													
Actividad	**Responsable**	**1 semestre 2024**						**1 semestre 2024**					
		E	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**N**	**D**
Realizar la actualización de la matriz de identificación de controles de seguridad de la información consolidada en la vigencia 2023, bajo la responsabilidad de cada dependencia, en atención a las modificaciones que puedan ser requeridas en torno al subproceso de identificación de estos.	Todas las Dependencias en caso de realizar la ejecución del plan de forma individual.								X	X	X	X	
Realizar la adquisición y/o implementación de los controles de seguridad de la información identificados en la vigencia 2023, bajo la responsabilidad de cada dependencia.	Todas las Dependencias en caso de realizar la ejecución del plan de forma individual.		X	X	X	X	X	X	X	X	X	X	X
Realizar el seguimiento a la operación de los controles de seguridad de la información implementados, para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia	Todas las Dependencias en caso de realizar la ejecución del plan de forma individual.		X	X	X	X	X	X	X	X	X	X	X
Realizar la identificación, clasificación, tratamiento y divulgación de Incidentes seguridad de la información materializados en atención a los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia	Todas las Dependencias en caso de realizar la ejecución del plan de forma individual.		X	X	X	X	X	X	X	X	X	X	X
Realizar el seguimiento a las actividades de identificación, adquisición e implementación de controles de seguridad de la información, así como de tratamiento de incidentes de seguridad de la información, para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia	Todas las Dependencias en caso de realizar la ejecución del plan de forma individual.					X			X			X	

El desarrollo de las actividades para lograr su consecución estará sujeto a la **disponibilidad de recursos** (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al apetito de riesgo institucional y a las orientaciones de la alta dirección, en cuanto al apetito de riesgo institucionales que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas.

En atención a las responsabilidades actuales de la ADS teniendo en cuenta la incompatibilidad normativa respecto del numeral 7.2.3 del anexo 1 de la resolución 0500 de 2021, así como los oficios que se han intercambiado con las diferentes áreas responsables respecto de dicha incompatibilidad, se colocará a disposición de la entidad un equipo humano dispuesto para:

✓ Apoyar a las dependencias adscritas a la Corporación, en el cumplimiento de sus responsabilidades a través de actividades específicas de sensibilización, capacitación y atención de inquietudes a través de cronogramas definidos para lo dispuesto en el “PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN”.

La Corporación ha establecido unos tiempos en los cuales se brindará y apoyará el seguimiento al desarrollo de los planes de seguridad y privacidad de la información que las dependencias presenten y así tratar las actividades pertinentes a los procesos relacionados al diligenciamiento de los planes de seguridad y privacidad de la información.