RESOLUCION No. 113
(17 DE OCTUBRE DE 2023)

"POR LA CUAL SE ADOPTA LA POLITICA DE GOBIERNO DIGITAL Y LA POLITICA DE SEGURIDAD DIGITAL (POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION (MSPI)) EN EL SISTEMA INTEGRADO DE TRANSORTE DE VALLEDUPAR SIVA SAS."

LA GERENCIA DEL SISTEMA INTEGRADO DE TRANSPORTE DE VALLEDUPAR – SIVA S.A.S

En uso de sus facultades Constitucionales, Legales, Reglamentarias y Estatutarias, y

CONSIDERANDO:

Que en virtud del Decreto Municipal N° 558 del 21 de septiembre de 2010 se crea la empresa Sistema Integrado de Transporte de Valledupar SIVA S.A.S., identificada con número de NIT. 900.404.948 – 6, como una sociedad de capital de naturaleza comercial, con personería jurídica, autonomía presupuestal, administrativa y financiera, estructura administrativa propia, sometida a las normas presupuestales y fiscales del orden municipal y cuyo objeto consiste en la gestión, organización, construcción, planeación y la vigilancia y control operativo del Sistema Estratégico de Transporte Público Colectivo de Valledupar SETPC.

Que, en virtud de lo anterior, la Junta Directiva del SIVA S.A.S eligió como Gerente a la Doctora **KATRIZZA MORELLI AROCA**, identificada con la cédula de ciudadanía número 52.993.437 expedida en Bogotá D.C., según consta en Acta de Sesión número 033 del 15 de septiembre de 2016 y Acta de Posesión del día 16 de ese mismo mes y año.

Que conforme al literal e) del artículo 28 de los Estatutos del Sistema Integrado de Transporte De Valledupar SIVA S.A.S., aprobados el 9 de julio de 2012, señala que es obligación de la Gerente de la entidad *"(…) Cumplir las demás funciones que le correspondan según lo previsto en las normas legales, en los estatutos que sean compatibles con el cargo"*

El numeral 8 del artículo 2 de la Ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC-, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones", establece como principio orientador la Masificación del Gobierno en Línea (hoy Gobierno Digital), según el cual las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones, para lo cual el Gobierno Nacional fijará los mecanismos y condiciones que garanticen el desarrollo de este principio. Asimismo, el artículo 4 ibídem establece que el Estado intervendrá en el sector TIC, entre otros, para promover su acceso, teniendo como fin último el servicio universal; así como para promover el desarrollo de contenidos y aplicaciones, la prestación de servicios que usen TIC y promover la seguridad informática y de redes para desarrollarlas:

en concordancia con el numeral 11 del artículo 2.2.22.2.1 del Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", la Política de Gobierno Digital es una Política de Gestión y Desempeño Institucional, por lo cual todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional, a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) como líder de esta Política, para su implementación.

En virtud del artículo 230 previamente citado, el MinTIC deberá contemplar como acciones prioritarias el cumplimiento de los lineamientos y estándares para la integración de trámites al Portal Único del Estado Colombiano, la publicación y el aprovechamiento de datos públicos, la adopción del modelo de territorios y ciudades inteligentes, la optimización de compras públicas de tecnologías de la información, la oferta y uso de software público, el aprovechamiento de tecnologías emergentes en el sector público, el incremento de la confianza y la seguridad digital, y el fomento a la participación y la democracia por medios digitales.

El parágrafo 3° del artículo 9 de la Ley Estatutaria 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", establece que sus sujetos obligados deberán dar cumplimiento a la estrategia de Gobierno en Línea, o la que haga sus veces, en cuanto a la publicación y divulgación de la información.

El Documento CONPES 3975 de 2019, "Política Nacional para la Transformación Digital e Inteligencia Arlificiaf', establece acciones encaminadas a impulsar la transformación digital del sector público y del sector privado mediante la disminución de barreras que impiden la incorporación de tecnologías digitales, el fortalecimiento del capital humano y la creación de condiciones habilitantes para el aprovechamiento de las oportunidades de la transformación digital.

Mediante el Decreto 620 de 2020, se subrogó el Título 17 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, con el fin de establecer los lineamientos generales en el uso y operación de los servicios ciudadanos digitales, como habilitador de la Política de Gobierno Digital.

En la Resolución 1519,de 2020 del MinTIC, se definieron los lineamientos para la publicación y divulgación de la información señalada en la Ley Estatutaria 1712 del 2014 y se establecieron los estándares de publicación y divulgación de contenidos e información, los criterios para la estandarización de contenidos e información en materia de accesibilidad web en los portales web y sedes electrónicas, las condiciones mínimas técnicas y de seguridad digital, y las condiciones mínimas de publicación de datos abiertos. En consecuencia, la

transparencia y el derecho de acceso a la información pública y las normas que la desarrollan son un pilar fundamental para la configuración y desarrollo de la línea de acción de Estado Abierto de que trata el Decreto 767 del 16 de mayo del 2022.

Mediante la Resolución 2893 de 2020 del MinTIC, se expidieron los lineamientos para estandarizar las ventanillas únicas, los portales de programas transversales y unificación de sedes electrónicas del Estado colombiano. Asimismo, el acto administrativo en mención expidió las guías técnicas para la integración al Portal Único del Estado Colombiano de las sedes electrónicas, de las ventanillas únicas, de los portales específicos de programas transversales del Estado, y de los Trámites, Otros Procedimientos Administrativos (OPAs) y Consultas de Acceso a Información Pública. En consecuencia, la estandarización de sedes electrónicas y demás canales digitales que le permitan al ciudadano ejercer su derecho al acceso a la administración pública son un pilar fundamental para la configuración y desarrollo de las líneas de acción de que trata el Decreto 767 del 16 de mayo del 2022.

La Resolución 500 de 2021, expedida por el MinTIC, estableció los lineamientos y estándares para la estrategia de seguridad digital, y la adopción del modelo de seguridad y privacidad, como habilitador de la política de Gobierno Digital. En consecuencia, la seguridad y privacidad de la información, y el Modelo de Seguridad y Privacidad de la Información adoptado. mediante el acto administrativo en mención, y las normas que lo desarrollan son un pilar fundamental para la configuración y desarrollo del habilitador de Seguridad y Privacidad de la Información de que trata el Decreto 767 del 16 de mayo del 2022.

El documento CONPES 4070 de 2021, "Lineamientos de Política para la Implementación de un Modelo de Estado Abierto", establece acciones para generar confianza ciudadana en la institucionalidad pública y avanzar en una agenda de construcción conjunta de soluciones a los problemas públicos, señalando que el uso de las Tecnologías de la Información y las Comunicaciones es un atributo esencial de la apuesta por un Estado abierto.

Mediante el Decreto 088 de 2022 se adicionó el Título 20 a la Parte 2 del Libro 2 del Decreto 1078· de 2015, para definir los lineamientos, plazos, condiciones técnicas transversales para la digitalización y automatización de los trámites y su realización en línea con el fin de facilitar, agilizar y garantizar el acceso al ejercicio de los derechos de las personas y el cumplimiento de sus obligaciones para con el Estado, a través de medios digitales

Mediante la Resolución 1117 de 2022 se establecieron los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes que definan las entidades territoriales, en el marco de la Política de Gobierno Digital. En consecuencia, se constituyen en un pilar fundamental para la configuración y desarrollo de las ciudades y territorios inteligentes como iniciativas dinamizadoras, conforme establece el Decreto 767 del 16 de mayo del 2022.

En igual sentido, se identificó la importancia del desarrollo de capacidades para la innovación pública digital en el marco de la Política de Gobierno Digital, toda vez que esta permite la adopción de tecnologías digitales emergentes para mejorar los servicios y la gestión del Estado, garantiza el derecho de acceso a la información pública e impacta la calidad de vida y la competitividad. Asimismo, se encontró que los datos constituyen un activo estratégico, en la medida en que su uso y aprovechamiento dinamiza la transformación del gobierno e impulsa la economía del país

El documento técnico aborda la Política de Gobierno Digital para el Sistema Integrado de Transporte de Valledupar SIVA SAS., establecida mediante el Decreto 1008 de 2018 (cuyas disposiciones se compilan en el Decreto 1078 de 2015, "Decreto Único Reglamentario del sector TIC", específicamente en el capítulo 1, título 9, parte 2, libro 2), además forma parte del Modelo Integrado de planeación y Gestión (MIPG) y se integra con las políticas de Gestión y Desempeño de la entidad, que busca promover una adecuada gestión interna del SIVA SAS para un buen relacionamiento con el ciudadano, a través de la participación y la prestación de servicios de calidad. En esta política se definen los procesos necesarios tendientes a garantizar la implementación de la Estrategia de Gobierno Digital, y de esta manera propender por "Garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y participativo y que preste mejores servicios con la colaboración de toda la sociedad".

Se tomará como lineamiento lo establecido en el Manual para la implementación de la Política de Gobierno Digital", se encuentra incorporado en el artículo 2.2.9.1.2.2.del DURTIC.

Que la norma internacional ISO/IEC 27001:2013 (Icontec, 2013) - Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información - Requisitos, especifica los requisitos para establecer, implantar, mantener y seguir mejorando los Sistemas de Gestión de Seguridad de la Información (SGSI) en el contexto de las organizaciones.

RESOLUCION No. 113
(17 DE OCTUBRE DE 2023)

"POR LA CUAL SE ADOPTA LA POLITICA DE GOBIERNO DIGITAL Y LA POLITICA DE SEGURIDAD DIGITAL (POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION (MSPI)) EN EL SISTEMA INTEGRADO DE TRANSORTE DE VALLEDUPAR SIVA SAS."

Que el Decreto Nacional 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones", definió la estrategia de seguridad y privacidad de la información, estableciendo que la misma no se limita a este sólo aspecto, sino que comprende la seguridad digital y los requerimientos necesarios para garantizar la continuidad en la prestación de los servicios digitales, en los siguientes términos:

"ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital. Los actores que traten información en el marco del presente título deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital, que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo. En ese sentido, deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones"

Teniendo en cuenta lo anterior, el proceso de implementación consta de cuatro grandes actividades: 1. Conocer la política, 2. Planear la política, 3. Ejecutar la política y 4. Medir la política, las cuales incorporan acciones que permitirán desarrollar la política en la entidad..

Que, en mérito de lo anteriormente expuesto,

RESUELVE:

Capitulo 1
POLITICA DE GOBIERNO DIGITAL

Artículo 1°. Adoptar la Política de Gobierno Digital y la Política de Seguridad Digital del Sistema Integrado de Transporte de Valledupar SIVA SAS.

Artículo 2° Objeto: Se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de la Entidad, a través del uso y aprovechamiento de las TIC. Hace parte del Modelo Integrado de Planeación y Gestión – MIPG Dimensión Gestion con valores y se integra con las políticas de Gestión y Desempeño Institucional.

El Marco de Acción se desarrolla a través de siete (7) pasos:

- Paso 1. Alineación con la planeación estratégica,
- Paso 2. Revisión del estado de implementación de las políticas de gestión y desempeño institucional,
- Paso 3. Revisión del estado de implementación del Marco de Referencia de Arquitectura Empresarial,
- Paso 4. Revisión del estado de implementación de la Política de Seguridad y Privacidad de la Información,
- Paso 5. Condiciones del Sistema Integrado de Transporte de Valledupar SIVA SAS para la implementación de Servicios Ciudadanos Digitales (título 17, parte 2, libro 2 del DURTIC),
- Paso 6. Priorización de Iniciativas: a partir de los proyectos, iniciativas y acciones identificadas en los pasos 1, 2, 3, 4 y 5 y
- Paso 7. Formulación o actualización del PETI y el Plan de Seguridad y privacidad de la Información.

Articulo 3° Alcance: La Política de Gobierno Digital comprende los proyectos que involucran el uso y aprovechamiento de Tecnologías de la Información y de las comunicaciones e impulsa el desarrollo de las políticas Institucionales, así como la seguridad de la información, la arquitectura de la entidad y los servicios ciudadanos digitales.

Articulo 4° Lineamientos de los elementos habilitadores. Los habilitadores transversales de la política de Gobierno Digital: Arquitectura, Seguridad de la Información y Servicios Ciudadanos Digitales; son elementos fundamentales que permiten el despliegue de los componentes de la política y tienen como objetivo, desarrollar capacidades en el Sistema Integrado de Transporte de Valledupar SIVA SAS para la implementación de la política.

Por ello, de manera paralela a la implementación de los componentes (TIC para el Estado y TIC para la Sociedad), el SIVA SAS debe trabajar en el desarrollo de los elementos habilitadores que se definen: Arquitectura, Seguridad de la Información y Servicios Ciudadanos Digitales.

Articulo 5° El responsable de proceso. Quien lidera la implementación y la mejora continua de la Política de Gobierno Digital es , o quien el gerente (a) o quien haga sus veces, las demás áreas de la entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

Cuando la entidad cuente en su estructura con una dependencia encargada del accionar estratégico de las Tecnologías y Sistemas de la Información y las Comunicaciones, hará parte del comité directivo y dependerá del nominador o representante legal, de acuerdo con lo establecido en el artículo 2.2.35.4. del Decreto Único Reglamentario de Función Pública 1083 de 2015.

Articulo 6º. Mejoramiento Continuo. Los resultados obtenidos durante el desarrollo de este proceso se constituirán en insumo para las acciones de mejoramiento del Sistema estratégico de transportes de Valledupar SIVA , con el fin de evitar la ocurrencia de cualquier hecho que pueda interferir en el trabajo e impedir el logro de los objetivos

Artículo 7. El documento técnico (ver anexo) que contiene la Política de Gobierno Digital del Sistema estratégico de transportes de Valledupar SIVA , forman parte integral de la presente Resolución, en caso de requerirse un cambio debido a ajustes, recomendaciones o cambios normativos, estos se realizarán a través de cambio de versión, el nuevo documento se anexará a la presente resolución con la anotación y firmas respectivas.

Capitulo 2
POLITICA DE SEGURIDAD DE LA INFORMACION

Artículo 8°. La Política de Seguridad y Privacidad de la Información y Seguridad Digital está conformada por estándares técnicos y generales de seguridad de la información, procesos y procedimientos, estructura organizacional y mecanismos de verificación y control para garantizar que los riesgos de seguridad de la información y los riesgos de ciberseguridad sean conocidos, asumidos, gestionados y mitigados de forma documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Artículo 9° Para El Sistema Integrado de Transporte de Valledupar – SIVA SAS, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta adopción a la política aplica al SIVA SAS según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

Articulo 10° Principios: Se establecen 12 principios de seguridad que soportan el SGSI del Sistema Integrado de Transporte SIVA SAS:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros
- protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- protegerá su información de las amenazas originadas por parte del personal.
- controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos

- protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos. implementará control de acceso a la información, sistemas y recursos de red.
- garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Articulo 11° Objetivos. La Política de Seguridad y Privacidad de la información y de Seguridad Digital en el Sistema Integrado de Transporte de Valledupar tiene los siguientes objetivos:

- Identificar, clasificar, valorar y mantener actualizados los activos de información de la Entidad.
- Gestionar los riesgos de Seguridad y Privacidad de la información que afecten la confidencialidad, integridad, disponibilidad y privacidad de los activos de información institucional.
- Gestionar los incidentes y eventos de seguridad y privacidad que pongan en riesgo la confidencialidad, disponibilidad, integridad y privacidad de los activos de información de la
- Entidad, de manera oportuna, con el fin de minimizar su impacto y propagación.
- Promover e implementar estrategias para establecer una cultura y apropiación en temas de
- Seguridad y Privacidad de la información en todos los colaboradores de la entidad.
- Establecer, implementar y mejorar el plan de continuidad del negocio para la Secretaría Distrital de
- Integración Social en cuanto a los procesos y/o actividades críticas de la entidad.
- Garantizar a través de la implementación del Modelo de Seguridad y Privacidad de la Información la continuidad de los servicios de la Entidad.
- Fomentar el uso y apropiación de las TIC en el SIVA SAS, contribuyendo en las políticas de seguridad y privacidad en los procesos de gestión, administrativos y formativos de la Entidad.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en la Entidad.

Para realizar una medición acorde con la efectividad, eficacia y eficiencia de la Seguridad de la Información en la Entidad, se deben aplicar los indicadores relacionados en la Guía de Indicadores de Gestión de la Información emitida por el Ministerio de las TIC.

Articulo 12° Responsables. La definición, implementación y mantenimiento de la Política de Seguridad y Privacidad de la Información y Seguridad Digital del Sistema Integrado de Transporte de Valledupar – SIVA SAS así como sus lineamientos específicos, tiene como responsables las siguientes instancias:

- La Gerencia, quién será la encargada de liderar las estrategias las actividades de seguridad y privacidad de la información para la Entidad.
- El Comité Institucional de Gestión y Desempeño, en representación de la Alta Dirección, quién tiene la responsabilidad de asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.
- El personal encargado de la seguridad de la información que implementará y velará por el mantenimiento del Modelo de Seguridad y Privacidad de la Información de la Entidad.
- Los funcionarios, contratistas, proveedores, operadores, entes de control y terceros, quienes deberán cumplir la Política de Seguridad y Privacidad de la Información y Seguridad Digital y sus lineamientos específicos.

Cuando la entidad cuente en su estructura con una dependencia encargada del accionar estratégico de las Tecnologías y Sistemas de la Información y las Comunicaciones, hará parte del comité directivo y dependerá del nominador o representante legal, de acuerdo con lo establecido en el artículo 2.2.35.4. del Decreto Único Reglamentario de Función Pública 1083 de 2015.

Articulo 13º. - Compromiso De La Alta Dirección. El Sistema Integrado de Transporte de Valledupar – SIVA SAS, por intermedio de su Gerente y las diferentes áreas de la entidad, se comprometen y responsabilizan con la asignación y comunicación de las funciones, obligaciones y responsabilidades de todos los colaboradores en materia de seguridad y privacidad de la información, apalancando así el establecimiento, implementación, operación, seguimiento, mantenimiento y mejora continua del SGSI.

Artículo 14. Verificación Del Cumplimiento La Gerencia y la Oficina de Control Interno propenderán por el cumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad de la información, garantizando que su implementación y operación este acorde con las políticas y procedimientos organizacionales.

El cumplimiento normativo que incluye esta política abarca normativa y requisitos contractuales, derechos de propiedad intelectual, protección de registros, privacidad y protección de información de datos personales, reglamentación de controles criptográficos, revisión independiente de la seguridad de la información, cumplimiento con las políticas y normas de seguridad y toda la revisión del cumplimiento técnico.

Las responsabilidades de ejecutar este lineamiento, cumplirlo a cabalidad y sin excepciones son para todos los funcionarios, contratistas y visitantes del SIVA SAS

Artículo 15. Vigencia. La presente Resolución rige a partir de la fecha de su expedición.

Dado en la ciudad de Valledupar, Departamento del Cesar, a los Diecisiete (17) días del mes de octubre de 2023.

KATRIZZA MORELLI AROCA
Gerente SIVA S.A.S.

Proyectó: Oficina Asesora Jurídica y Administrativa y Financiera
Revisó: Oficina Asesora Jurídica y Administrativa y Financiera
Aprobó: Gerencia
Archivo: Carpeta Resoluciones vigencia 2023.

POLITICA DE SEGURIDAD DIGITAL

SISTEMA INTEGRADO DE TRANSPORTE DE VALLEDUPAR SIVA S.A.S

KATRIZZA MORELLI AROCA
GERENTE
2023

CONTENIDO

COMPROMISO DE LA ALTA DIRECCIÓN

En el Sistema Integrado de Transporte de Valledupar SIVA S.A.S, reconocemos la importancia crítica de la seguridad de la información para el éxito continuo de nuestra organización. Como líderes de la Alta Dirección, nos comprometemos a establecer y mantener un entorno de seguridad robusto que proteja la confidencialidad, integridad y disponibilidad de la información.

Nuestro Compromiso Incluye:

Apoyo Activo: Brindaremos un respaldo continuo a la implementación y mantenimiento de medidas de seguridad de la información en todos los niveles de la organización.

Recursos Adecuados: Aseguraremos la asignación de los recursos necesarios para implementar y mantener efectivamente controles de seguridad de la información.

Cultura de Seguridad: Fomentaremos una cultura organizacional que valore y priorice la seguridad de la información, asegurándonos de que todos los miembros del personal comprendan su papel en la protección de nuestros activos digitales.

Cumplimiento Legal y Normativo: Nos comprometemos a cumplir con todas las leyes y regulaciones aplicables relacionadas con la seguridad de la información y la protección de datos.

Participación Activa: Participaremos activamente en la revisión regular del Plan de Seguridad de la Información, garantizando su alineación con los objetivos estratégicos de la organización.

Comunicación Transparente: Comunicaremos de manera transparente la importancia de la seguridad de la información a todos los niveles de la organización, asegurando una comprensión clara de los riesgos y responsabilidades asociadas.

Gestión de Riesgos: Participaremos en la identificación y evaluación de riesgos, contribuyendo a la implementación de controles efectivos para mitigar amenazas potenciales.

Liderazgo Ejemplar: Demostraremos liderazgo ejemplar al seguir y adherirnos a las prácticas de seguridad de la información en nuestra propia conducta y toma de decisiones.

Planificación para la Continuidad del Negocio: Aseguraremos la integración de la seguridad de la información en los planes de continuidad del negocio para garantizar la recuperación rápida y efectiva después de un incidente.

Mejora Continua: Promoveremos la mejora continua de las políticas, procesos y controles de seguridad de la información a través de la retroalimentación, la revisión y la adaptación a los cambios en el entorno de amenazas.

INTRODUCCION

En la era digital actual, donde la información es un activo invaluable, el Sistema Integrado de Transporte de Valledupar SIVA S.A.S reconoce la necesidad apremiante de salvaguardar la integridad, confidencialidad y disponibilidad de la información. Con el fin de establecer un marco sólido para la seguridad de la información, presentamos este Plan de Seguridad que refleja nuestro compromiso inquebrantable con la protección de los activos digitales y la garantía de la continuidad de nuestras operaciones.

En un entorno en constante evolución, las amenazas cibernéticas y los riesgos asociados a la información requieren una respuesta proactiva y una gestión eficaz. Este plan no solo busca cumplir con las regulaciones y normativas aplicables, sino que va más allá, aspirando a crear una cultura organizacional arraigada en la conciencia y práctica de la seguridad de la información en todos los niveles de nuestra entidad.

La Alta Dirección de SIVA S.A.S se compromete a liderar este esfuerzo, proporcionando los recursos necesarios, estableciendo políticas claras y promoviendo una mentalidad de seguridad en cada empleado. A través de este plan, buscamos no solo mitigar riesgos, sino también crear un ambiente donde la seguridad sea parte integral de nuestra operación diaria.

Este documento es más que una guía; es una declaración de nuestro compromiso con la excelencia, la confianza del cliente y la protección de la información que impulsa nuestra organización. Invitamos a cada miembro de nuestro equipo a adoptar este enfoque colectivo hacia la seguridad de la información, reconociendo que la responsabilidad de proteger nuestros activos digitales es un eslabón fundamental en la cadena de nuestro éxito organizacional.

Con este Plan de Seguridad de la Información, avanzamos hacia un futuro donde la seguridad no es solo un requisito, sino un principio rector que fortalece la resiliencia y la sostenibilidad de nuestro Sistema Integrado de Transporte.

OBJETIVO

El objetivo general de este Plan de Seguridad de la Información en el Sistema Integrado de Transporte de Valledupar SIVA S.A.S es establecer un marco integral y efectivo que garantice la protección, confidencialidad, integridad y disponibilidad de la información, asegurando la continuidad operativa y la confianza de las partes interesadas en un entorno digital dinámico y en constante evolución.

Objetivos Específicos

- Implementar un proceso sistemático de identificación, evaluación y tratamiento de riesgos para mitigar posibles amenazas y vulnerabilidades a los activos de información de la organización.
- Desarrollar e implementar programas de concientización y formación continuada para todos los miembros del personal, promoviendo una cultura de seguridad sólida y una comprensión clara de las mejores prácticas.
- Reforzar los controles de acceso a sistemas y datos, así como la gestión eficaz de identidades, asegurando que los usuarios tengan el nivel de acceso necesario y apropiado para llevar a cabo sus funciones.
- Desarrollar e implementar un plan integral de contingencia y continuidad del negocio que permita a la organización recuperarse de manera rápida y efectiva después de incidentes de seguridad, minimizando el impacto en las operaciones y servicios.

.

ALCANCE

Este Plan de Seguridad de la Información abarca todas las áreas y procesos operativos del Sistema Integrado de Transporte de Valledupar SIVA S.A.S. Su implementación involucra a todos los miembros del personal, contratistas, proveedores y cualquier entidad que maneje activos de información en nombre de SIVA S.A.S. El alcance se extiende a:

Activos de Información:

Todos los activos digitales y físicos que contienen, procesan o transmiten información, incluyendo sistemas de información, bases de datos, documentos impresos, y cualquier otro medio que almacene información sensible.

Personal:

Todos los empleados, contratistas y colaboradores externos que tienen acceso a los activos de información de la organización, independientemente de la forma en que se les proporcione este acceso.

Procesos Operativos:

Todas las operaciones comerciales, procesos internos y actividades que involucran el manejo, procesamiento o almacenamiento de información, desde la captura inicial hasta la eliminación segura al final de su ciclo de vida.

Sistemas y Redes:

Todos los sistemas informáticos, servidores, redes y dispositivos que respaldan las operaciones de SIVA S.A.S, incluyendo aquellos operados por terceros en nombre de la organización.

Regulaciones y Normativas:

Cumplimiento de todas las leyes, regulaciones y normativas pertinentes relacionadas con la seguridad de la información, protección de datos y privacidad, aplicables a la operación de SIVA S.A.S.

Ciclo de Vida de la Información:

Desde la creación hasta la disposición final, este plan se aplica a todas las fases del ciclo de vida de la información, abordando la seguridad en cada etapa.

Este alcance garantiza que el Plan de Seguridad de la Información sea integral, cubriendo todos los aspectos relevantes para proteger los activos de información críticos y mantener la confidencialidad, integridad y disponibilidad de la información en el entorno operativo de SIVA S.A.S.

RESPONSABLES

Todas y cada una de las dependencias de la Entidad SIVA SAS en cabeza del Comité de gestión y desempeño y la gerencia, los cuales son los responsables del pleno cumplimiento de la implementación de la Política de Gobierno Digital y la seguridad digital.

MARCO NORMATIVO

Con el propósito de dar cumplimiento al tratamiento de los datos personales, se identifica el siguiente marco normativo que articula las disposiciones de protección de datos personales

- Decreto 088 de 24 enero de 2022: "Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los articulas 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea"
- Ley 1978 de 2019: Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
- Resolución 1951 de 2022: Por la cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales; se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital.
- 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'"
- Decreto 1263 de 2022: "Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública"
- Ley 1955 de 2019: por el cual se expide el plan nacional de desarrollo 2018-2022 pacto por Colombia, pacto por la equidad. El congreso de Colombia
- Resolución 2160 de 2020: Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos
- Resolución 2893 de 2020: “Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado Colombiano, y se dictan otras disposiciones”
- 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”
- Ley estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

- Ley 1978 de 2019: Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
- Resolución 1126 de 2021: Por la cual se modifica la Resolución 2710 de 2017
- Resolución 2710 de 2017: Por el cual se establecen lineamientos para la adopción del protocolo IPV6
- Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 2052 de 2020: La presente ley tiene por objeto establecer disposiciones transversales a la Rama Ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y/o administrativas, en relación con la racionalización de trámites, con el fin de facilitar, agilizar y garantizar el acceso al ejercicio de los derechos de las personas, el cumplimiento de sus obligaciones, combatir la corrupción y fomentar la competitividad.
- Resolución 2405 de 2016: Por la cual se adopta el modelo del Sello de Excelencia Gobierno en Línea y se conforma su Comité.
- Conpes 3920 de 2018: Política Nacional de Explotación de Datos – BIG DATA
- Conpes 3975 de 2019: Política Nacional para la Transformación Digital e Inteligencia Artificial
- Decreto 415 de 2016: Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- Circula 015 de 2022: Adopción del protocolo IPV6
- Resolución 1519 de 2020: Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Resolución 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 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
- Directiva presidencial 03: Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos

DEFINICIONES

Plan de Seguridad de la Información: Un conjunto documentado de políticas, procesos, procedimientos y controles diseñados para salvaguardar la confidencialidad, integridad y disponibilidad de la información en una organización. Este plan aborda la gestión de riesgos, la concientización del personal y la implementación de medidas técnicas para proteger los activos de información.

Gestión de Riesgos de Seguridad de la Información: El proceso de identificación, evaluación y mitigación de riesgos relacionados con la seguridad de la información. Este componente del plan se centra en entender y reducir las amenazas y vulnerabilidades que podrían afectar la integridad, confidencialidad y disponibilidad de los activos de información.

Conciencia y Educación en Seguridad: Estrategias y programas diseñados para informar y educar a los miembros del personal sobre las amenazas de seguridad de la información, así como sobre las mejores prácticas y políticas de seguridad. El objetivo es desarrollar una cultura organizacional donde cada miembro sea consciente de su papel en la protección de la información.

Controles de Acceso: Medidas y políticas implementadas para gestionar y restringir el acceso a sistemas, datos y recursos. Estos controles aseguran que solo aquellos usuarios autorizados tengan la capacidad de acceder a la información según sus funciones y responsabilidades.

Plan de Contingencia y Continuidad del Negocio: Un conjunto de procesos y procedimientos detallados para mantener las operaciones críticas en caso de interrupciones o desastres. Este plan incluye la identificación de escenarios de crisis, la asignación de responsabilidades y la preparación para la recuperación rápida y efectiva después de incidentes de seguridad.

Activos de Información: Cualquier información o recurso, en formato digital o físico, que posea un valor para la organización. Esto incluye datos confidenciales, sistemas, documentos impresos, hardware, software y cualquier otro elemento que contribuya al funcionamiento y éxito de la entidad.

Cultura de Seguridad de la Información: El conjunto de valores, actitudes, percepciones y prácticas compartidas dentro de una organización en relación con la seguridad de la información. Fomentar una cultura de seguridad implica la participación activa de todos los miembros, desde la alta dirección hasta el personal de base, en la protección de los activos de información.

Gestión de Identidad: El conjunto de procesos y tecnologías utilizados para administrar y garantizar la identificación y autenticación seguras de usuarios en sistemas y redes. La gestión de identidad asegura que solo las personas autorizadas tengan acceso a los recursos de información.

Gestión de Incidentes de Seguridad: Procesos y procedimientos establecidos para identificar, gestionar y responder a incidentes de seguridad de la información. Esto incluye la detección temprana, la contención, la erradicación y la recuperación después de eventos que podrían comprometer la seguridad.

Cumplimiento Legal y Normativo: La adhesión y conformidad con las leyes, regulaciones y normativas aplicables en el ámbito de la seguridad de la información. Esto abarca aspectos como la privacidad de datos, retención de registros y otras obligaciones legales relacionadas con la gestión de la información.

Auditoría de Seguridad: Un proceso sistemático de revisión y evaluación de los controles de seguridad implementados en la organización. Las auditorías de seguridad garantizan la eficacia de las medidas de seguridad y ayudan a identificar áreas de mejora.

Mejora Continua en Seguridad de la Información: Un enfoque proactivo para perfeccionar y fortalecer constantemente las prácticas de seguridad. Esto implica la revisión regular de políticas, procedimientos y controles en respuesta a cambios en la tecnología y amenazas emergentes.

Planificación para la Recuperación de Desastres: Un componente crítico del plan de contingencia que se enfoca en la restauración de operaciones normales después de un desastre. Incluye la identificación de activos críticos, la asignación de recursos y la implementación de procesos para minimizar el tiempo de inactividad.

DESCRIPCIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

La Política de Seguridad Digital establece los principios y directrices que rigen la protección de la información, la integridad de los sistemas y la confianza en el entorno digital. Esta política refleja nuestro compromiso con la seguridad y privacidad de la información, reconociendo la importancia crítica de salvaguardar los activos digitales y mitigar los riesgos asociados con las amenazas cibernéticas en constante evolución.

Principales Elementos de la Política:

Confidencialidad: Garantizamos la confidencialidad de la información mediante la implementación de controles de acceso adecuados y la clasificación de datos según su sensibilidad. El acceso a la información confidencial se limita a personal autorizado.

Integridad de la Información: Nos comprometemos a preservar la integridad de la información, asegurando que los datos no sean alterados de manera no autorizada. Se implementarán controles para detectar y prevenir cualquier modificación no autorizada.

Disponibilidad de los Sistemas: Garantizamos la disponibilidad continua de los sistemas y servicios críticos para el funcionamiento de la organización. Se establecerán medidas para minimizar el tiempo de inactividad y responder rápidamente a incidentes que puedan afectar la disponibilidad.

Gestión de Identidad y Acceso: Implementamos controles robustos para garantizar la autenticación segura de usuarios y gestionar adecuadamente los privilegios de acceso. La gestión de identidad se basa en la necesidad de conocer y el principio de privilegios mínimos.

Cultura de Seguridad: Fomentamos una cultura organizacional arraigada en la conciencia y práctica de la seguridad digital. La educación y la concientización periódica garantizarán que cada miembro del personal comprenda las amenazas y adopte prácticas seguras.

Gestión de Riesgos: Identificamos, evaluamos y gestionamos proactivamente los riesgos de seguridad digital. La gestión de riesgos se integra en todos los procesos para anticipar y abordar posibles amenazas a la seguridad de la información.

Cumplimiento Legal y Normativo: Nos comprometemos a cumplir con todas las leyes y regulaciones aplicables relacionadas con la seguridad digital, privacidad de datos y protección de la información.

Respuesta a Incidentes: Establecemos un plan de respuesta a incidentes que permita una acción rápida y coordinada en caso de violaciones de seguridad o amenazas cibernéticas. La notificación y mitigación eficaz serán prioritarias.

Actualización y Mejora Continua: Revisamos regularmente esta política para garantizar su relevancia y eficacia. Estamos comprometidos con la mejora continua de nuestros controles y prácticas de seguridad digital.

Esta Política de Seguridad Digital es un marco sólido que guía las acciones y decisiones de todo el personal de la entidad, asegurando un entorno digital seguro y confiable para nuestros activos de información. Su cumplimiento es esencial para fortalecer nuestra resiliencia ante las amenazas digitales en constante evolución.

ANTECEDENTES EN COLOMBIA

CONPES 3995 DE 2020

El CONPES 3995 del 2020, también conocido como la Política Nacional de Confianza y Seguridad Digital, es una política nacional formulada por el Gobierno de Colombia con el objetivo de establecer medidas para ampliar la confianza digital y mejorar la seguridad digital.

Los objetivos principales de esta política son:

- Establecer las capacidades en seguridad digital: Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país.
- Actualizar el marco de gobernanza: Actualizar el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo.
- Analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital: Con énfasis en los desafíos de la Cuarta Revolución Industrial (4RI).

La política busca que Colombia sea una sociedad incluyente y competitiva en el futuro digital. Para lograr esto, se propone una serie de acciones, entre las que se incluyen la unificación de la hoja de ruta de las iniciativas para fortalecer las competencias en seguridad digital, el diagnóstico de posibles problemas existentes en el marco normativo actual, y la creación de un Sistema Nacional de Gestión de incidentes cibernéticos.

RESOLUCION 1519 DE 2020

La Resolución 1519 de 2020, emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia, establece estándares y directrices para la publicación de información conforme a la Ley 1712 del 2014. Esta resolución introduce importantes cambios con respecto a su versión anterior, la Resolución 3564 del 2015, con el objetivo de garantizar el acceso a la información, transparencia, accesibilidad web, seguridad digital y datos abiertos. Algunos de los cambios incluyen nuevas directrices de accesibilidad web, adoptando el estándar internacional WCAG para que los sitios web sean accesibles para personas con discapacidad, así como nuevas condiciones para la publicación de datos abiertos y su integración en el Portal Único de Datos Abiertos www.datos.gov.co. Las entidades públicas y sujetos obligados tienen fechas límite para

cumplir con la implementación de estas medidas, siendo el 31 de marzo del 2021 para la implementación de ciertos anexos y el 31 de diciembre del 2021 para las directrices de accesibilidad web.

LEY 1273 DE 2009

La Ley 1273 de 2009, también conocida como la "Ley de Delitos Informáticos", es una ley colombiana que modifica el Código Penal y crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos"

- Esta ley establece una serie de delitos informáticos, como el acceso abusivo a un sistema informático, la interceptación de datos informáticos, la utilización de software malicioso, entre otros
- Además, la ley establece penas de prisión y multas para aquellos que cometan estos delitos
- La ley también busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones
- Desde su promulgación, la ley ha sido objeto de análisis y discusión en cuanto a su efectividad y necesidad de reforma para adaptarse a las nuevas modalidades de delitos informáticos

LEY 1266 DE 2008

La Ley 1266 de 2008, también conocida como la "Ley de Habeas Data", tiene como objetivo desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos y archivos, y los demás derechos, libertades y garantías constitucionales relacionados con el tratamiento de datos personales

- La ley establece una serie de obligaciones para los responsables del tratamiento de datos personales, como la obtención del consentimiento previo, la verificación de la calidad de la información, la adopción de medidas de seguridad, entre otras
- Además, la ley establece sanciones para aquellos que incumplan con las obligaciones establecidas
- La ley ha sido parcialmente reglamentada por el Decreto 1081 de 2015 y ha sido objeto de modificaciones posteriores, como la Ley 1581 de 2012 y el Decreto 1377 de 2013

DECRETO 1078 DE 2015

El Decreto 1078 de 2015, expedido por el Ministerio de Tecnologías de la Información y la Comunicación, es el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Este decreto tiene como objetivo compilar y racionalizar las normas de carácter reglamentario que rigen en el sector, proporcionando un instrumento jurídico único para el mismo. Establece la estructura del sector de tecnologías de la información y las comunicaciones, así como las responsabilidades y funciones de las entidades involucradas. Además, regula aspectos

relacionados con el desarrollo administrativo, la comisión nacional digital y de información estatal, la verificación de información, entre otros aspectos relevantes para el sector. El decreto busca brindar un marco normativo claro y actualizado para el desarrollo y regulación de las tecnologías de la información y las comunicaciones en Colombia.

DIRECTIVA PRESIDENCIA 003 DE 2021

La Directiva Presidencial 003 de 2021, emitida el 15 de marzo de 2021, imparte directrices para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos por parte de las entidades públicas de la rama ejecutiva del orden nacional en Colombia. Esta directiva tiene como objetivo cumplir con el artículo 147 de la Ley 1955 de 2019, que busca disminuir los costos de funcionamiento, acelerar la innovación, brindar entornos confiables digitales para las entidades públicas y mejorar sus procedimientos y servicios. Algunas de las directrices incluyen el cumplimiento de las directrices en materia de seguridad digital y de la información emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y las que se expidan en el marco de la política nacional de confianza. La directiva busca promover el uso eficiente y seguro de las tecnologías de la información y la comunicación en el sector público, fomentando la adopción de buenas prácticas en el manejo de la información y la implementación de tecnologías emergentes como la inteligencia artificial y la computación en la nube.

DECRETO 2364 DE 2012

El Decreto 2364 de 2012, expedido por el Presidente de la República de Colombia, reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones. Este decreto establece las definiciones y requisitos necesarios para la creación de una firma electrónica que cumpla con los requisitos de la Ley 527 de 1999, así como las condiciones para su uso y validez jurídica. Además, el decreto establece la obligación de las entidades públicas de aceptar la firma electrónica en los trámites y procedimientos que se realicen por medios electrónicos. El decreto busca promover el uso de la firma electrónica en Colombia, generando mayor entendimiento sobre la misma, dando seguridad jurídica a los negocios que se realicen a través de medios electrónicos, así como facilitando y promoviendo su uso masivo en todo tipo de transacciones

DECRETO 338 DE 2022

El Decreto 338 de 2022, expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia, establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital y crear el modelo y las condiciones para la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital. El decreto busca mejorar la coordinación y la gestión de los riesgos de seguridad digital para los servicios esenciales e infraestructuras críticas cibernéticas de Colombia, así como mejorar la atención y respuesta a incidentes. Este decreto está enfocado en las entidades que conforman la Administración Pública, entendidas como los organismos de naturaleza pública

que tienen a su cargo el ejercicio de las actividades y funciones administrativas o la prestación de servicios públicos del Estado Colombiano.

CONPES 3975 DE 2019

El CONPES 3975 de 2019, titulado "Política de transformación digital e inteligencia artificial para Colombia", establece lineamientos para la transformación digital del país, promoviendo la adopción de tecnologías digitales e inteligencia artificial en diversos sectores. El plan busca impulsar la economía digital, mejorar la eficiencia del sector público, fortalecer la ciberseguridad, y fomentar la inclusión digital, entre otros objetivos. Este CONPES es relevante para el desarrollo tecnológico y la modernización del país, abordando aspectos clave para la transformación digital de Colombia

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El Modelo de Seguridad y Privacidad de la Información (MSPI) es un marco de referencia que imparte lineamientos a las entidades públicas en Colombia para la implementación y adopción de buenas prácticas en materia de seguridad de la información, tomando como referencia estándares internacionales. Este modelo tiene como objetivo orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información, permitiendo habilitar la implementación de la Política de Gobierno Digital. Está alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Administración del Riesgo y el Diseño de Controles en entidades públicas. El MSPI busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación

RESOLUCION 500 DE 2021

La Resolución 500 de 2021, emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, establece los lineamientos y estándares para la estrategia de seguridad digital. Esta resolución tiene como objetivo promover la implementación de medidas que fortalezcan la seguridad digital en el país, abordando aspectos relacionados con la protección de la información, la gestión de riesgos y la respuesta a incidentes de seguridad digital. La resolución busca garantizar la integridad, confidencialidad, disponibilidad y autenticidad de la información, así como promover la adopción de buenas prácticas en materia de seguridad digital. Este marco normativo es fundamental para el fortalecimiento de la ciberseguridad y la protección de la información en el contexto digital actual.

LEY 527 DE 1999

La Ley 527 de 1999, también conocida como la "Ley de Comercio Electrónico", es una ley colombiana que define y regula el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales. Esta ley establece la validez jurídica de los mensajes de datos y las firmas digitales, así como las condiciones para su uso y aceptación en el ámbito jurídico. Además, la ley establece la

obligación de las entidades públicas de aceptar los mensajes de datos y las firmas digitales en los trámites y procedimientos que se realicen por medios electrónicos. La ley también establece sanciones para aquellos que incumplan con las obligaciones establecidas. La Ley 527 de 1999 es una herramienta jurídica fundamental para el desarrollo del comercio electrónico y la adopción de tecnologías digitales en Colombia

RESOLUCION 746 DE 2022

La Resolución 746 de 2022, emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia, establece modificaciones a la Resolución 500 de 2021, la cual establece los lineamientos y estándares para la estrategia de seguridad digital. La Resolución 746 de 2022 adiciona dos numerales al artículo 7 de la Resolución 500 de 2021, los cuales establecen la obligación de los proveedores de servicios de seguridad digital de garantizar el cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios, así como las normas concordantes, en relación con la protección de datos personales. Además, se establece la obligación de adoptar medidas para garantizar el cumplimiento de las normas relativas a la transferencia internacional de datos personales al momento de adquirir productos y servicios de seguridad digital operados en entornos de nube. La Resolución 746 de 2022 también adiciona un anexo al Modelo de Seguridad y Privacidad de la Información.

LEY 1581 DE 2012

La Ley 1581 de 2012, conocida como la "Ley de Protección de Datos Personales", es una normativa colombiana que establece disposiciones generales para la protección de datos personales y regula el derecho fundamental que tienen todas las personas a conocer, actualizar, rectificar y suprimir la información que se haya recogido sobre ellas en bases de datos y archivos. Esta ley aplica al tratamiento de datos personales realizado en territorio colombiano, así como a aquellos realizados por responsables del tratamiento o encargados del tratamiento que se encuentren fuera del país, cuando la información sea transferida a entidades ubicadas en el extranjero. La ley establece los principios, deberes y derechos que rigen el tratamiento de datos personales, así como las obligaciones de los responsables y encargados del tratamiento. Además, regula aspectos como el manejo de datos sensibles, la seguridad de la información, la atención de consultas y reclamos por parte de los titulares de la información, entre otros aspectos relevantes para la protección de datos personales. La ley fue reglamentada parcialmente por el Decreto Nacional 1377 de 2013, el cual establece disposiciones para su aplicación.

LEY 1978 DE 2019

La Ley 1978 de 2019, conocida como la "Ley de Modernización del Sector de las Tecnologías de la Información y las Comunicaciones (TIC)", tiene como objetivo alinear los incentivos de los agentes y autoridades del sector de las TIC, promoviendo la inversión, la competencia, la innovación y el acceso a las tecnologías de la información y las comunicaciones. Esta ley distribuye competencias, crea un regulador único y dicta disposiciones para el sector de las TIC. Además, modifica el artículo

13 de la Ley 1341 de 2009, el cual se refiere a la provisión de redes y servicios de telecomunicaciones, incluyendo la provisión de redes y servicios de televisión. Asimismo, establece funciones adicionales para el Ministerio de Tecnologías de la Información y las Comunicaciones, y dispone la revisión y adopción de la estructura y la planta de personal de dicho ministerio. La ley también modifica el artículo 19 de la Ley 1341 de 2009 y establece disposiciones relacionadas con la Comisión de Regulación de Comunicaciones (CRC).

DIRECTIVA PRESIDENCIAL 002 2022

La Directiva Presidencial 02 de 2022, emitida por la Presidencia de la República de Colombia, establece directrices para las entidades públicas de la rama ejecutiva del orden nacional en el país. La directiva tiene como objetivo reiterar la política pública en materia de seguridad digital, promoviendo la adopción de medidas que fortalezcan la seguridad de la información y la ciberseguridad en el sector público. La directiva establece la obligación de las entidades públicas de adoptar medidas para garantizar la seguridad de la información, incluyendo la implementación de medidas de protección de datos personales, la adopción de medidas de seguridad en la nube, la implementación de medidas de seguridad en el desarrollo de software, entre otras. La directiva también establece la obligación de las entidades públicas de reportar los incidentes de seguridad digital al Centro Cibernético Policial (CCP) y al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). La directiva es relevante para el fortalecimiento de la ciberseguridad y la protección de la información en el sector público en Colombia.

DECRETO 767 DE 2022

El Decreto 767 de 2022, emitido en Colombia, establece los lineamientos generales de la Política de Gobierno Digital y subroga el Capítulo 1 del Título 1 de la Parte 2 del Libro 2 del Decreto 1078 de 2015. Este decreto tiene como objetivo establecer las directrices para la implementación de la Política de Gobierno Digital en el país, promoviendo la transformación digital del Estado, la prestación de servicios digitales eficientes y la protección de la información. Además, busca impulsar la adopción de tecnologías de la información y las comunicaciones en la gestión pública, así como la implementación de medidas de seguridad digital. Este marco normativo es fundamental para la modernización y eficiencia de la gestión pública a través de la implementación de soluciones digitales.

DECRETO 1263 DE 2022

El Decreto 1263 de 2022, emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia, define los lineamientos y estándares aplicables a la transformación digital pública. Este decreto establece directrices para la implementación de la Política de Gobierno Digital en el país, promoviendo la modernización y eficiencia de la gestión pública a través de la implementación de soluciones digitales. El decreto contempla aspectos como la infraestructura de datos, la interoperabilidad, los proyectos relacionados con digitalización y automatización de trámites, el uso de mecanismos de agregación de demanda, el uso de servicios

en la nube, la planeación institucional, sandbox regulatorios e inteligencia artificial. Estos lineamientos y estándares buscan impulsar los procesos de transformación digital de las entidades públicas del país, en armonía con la Política de Gobierno Digital vigente.

SEGURIDAD DE LA INFORMACIÓN EN LA POLÍTICA DE GOBIERNO DIGITAL

Es un elemento que apoya a las entidades de manera trasversal, habilitando el desarrollo de los componentes de la política de Gobierno Digital. Este componente se desarrolla, a través de lineamientos en materia de seguridad y privacidad de la información, así como de gestión de riesgos de seguridad digital, lo cuales soportan las acciones establecidas por cada entidad para proteger los activos de información, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos

ESTRATEGIAS

Se generan como apoyo para que el Gobierno Nacional logre fortalecer las capacidades de las entidades públicas para enfrentar las amenazas del entorno digital, contribuyendo en la creación de una cultura de gestión de riesgos que afiance la confianza en el uso del entorno digital. Es por esto que se considera fundamental robustecer el liderazgo del Gobierno nacional y construir una nueva visión tomando como referentes las mejores prácticas internacionales para abordar los riesgos de seguridad digital.

CSIRT Gobierno: Equipo de Respuesta a Incidentes de Seguridad Digital para las Entidades del Gobierno**.**

MGRSD: El Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD), es un conjunto de lineamientos y buenas prácticas que buscan guiar a las entidades públicas en la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad digital.

MSPI: Imparte lineamientos a las entidades públicas para la adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información**.**

Acompañamiento: El acompañamiento tiene por objetivo facilitar los procesos de adopción por parte de las diferentes Entidades de nivel nacional y territorial del modelo de seguridad y privacidad de la información, acorde con las funciones de GIT de Seguridad y Privacidad de TI.

INICIATIVAS

Facilitan las actividades de acompañamiento, apropiación, adopción e implementación de buenas prácticas, con el fin de fortalecer competencias y capacidades en la gestión de la seguridad y privacidad de la información.

Hacker Girls: Iniciativa que tiene como propósito apoyar y generar espacios de educación y oportunidad laboral para las mujeres, basados en el fortalecimiento de sus conocimientos en áreas asociadas a la ciberseguridad

Estudios impacto de incidentes de Seguridad: Instrumento elaborado por el Gobierno de Colombia, que tiene el propósito de obtener información sobre eventos e incidentes de Seguridad Digital en las organizaciones y su impacto en el país**.**

Buenas prácticas: Espacio dedicado como repositorio de consejos y buenas prácticas para que las entidades tengan una guía de cómo cumplir con normatividad específica o necesidades adicionales dentro de la implementación de la Seguridad y Privacidad de la Información.

Recursos de seguridad: Facilitan las actividades de acompañamiento, apropiación, adopción e implementación de buenas prácticas, con el fin de fortalecer competencias y capacidades en la gestión de la seguridad y privacidad de la información.

CSIRT GOBIERNO

El creciente uso de los entornos digitales y la adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC) traen consigo una serie de incertidumbres, riesgos, amenazas, vulnerabilidades que afectan la seguridad digital, lo cual exige que las entidades del gobierno cuenten con suficientes capacidades para la adecuada y oportuna gestión de los incidentes.

El CSIRT del sector Gobierno, surge como necesidad de realizar una adecuada gestión y reaccionar ante los incidentes cibernéticos de modo centralizado, para lo cual realiza seguimiento de manera unificada a las principales tipologías de ciberincidentes que atentan contra la defensa del Gobierno, para realizar de manera eficiente la gestión de sus riesgos.

El objetivo principal del CSIRT Gobierno, es ofrecer servicios proactivos, reactivos y de gestión de la seguridad básicos a todas las entidades del Estado, generando alertas y advertencias sobre amenazas y vulnerabilidades, realizando el tratamiento, análisis, respuesta y coordinación de incidentes, igualmente en el afianzamiento del conocimiento sobre seguridad, generando una cultura de seguridad digital en todos los funcionarios y encargados de seguridad digital

Las obligaciones y atribuciones que regirán cada una de las actividades que desarrollará el CSIRT Gobierno en el tratamiento de incidentes, será Autoridad Compartida, en la cual la toma de decisiones frente un incidente es conjunta entre el CSIRT Gobierno y la entidad, para lo cual el CSIRT Gobierno se apoya con los equipos de tecnología y la experiencia de la entidad cuando se presente un incidente.

El CSIRT de Gobierno brinda acompañamiento y apoyo a las entidades del estado, a través de su portafolio de servicios, con el fin de mejorar los procesos de seguridad de la infraestructura tecnológica, la gestión de los incidentes cibernéticos y generación de conciencia en seguridad digital.

Integrado por un grupo de personas técnicas especializadas, que implementan y desarrollan acciones tendientes a prevenir y gestionar los incidentes cibernéticos.

SERVICIOS PROACTIVOS

Buscan mejorar los procesos de seguridad de la infraestructura tecnológica, con el fin de prevenir incidentes de seguridad digital, reducir su impacto y alcance, cuando estos ocurran.

Generación de Alertas y Advertencias.

Difundir información sobre amenazas, vulnerabilidades de seguridad digital, con el fin de que se tomen medidas inmediatas o se realicen ajustes a la infraestructura tecnológica para evitar que un riesgo se materialice.

Difusión de Información Relacionada con la Seguridad.

Difundir información relevante sobre nuevas tecnologías, soluciones, sensibilizaciones y en general, temas relacionados con la seguridad digital, que permitan generar en los CISO´s y encargados de seguridad, conocimiento, capacidades, destrezas y habilidades.

Análisis de Vulnerabilidades WEB

Buscar en portales web del estado vulnerabilidades, con el fin de realizar ajustes y acciones de mitigación para prevenir explotaciones de estas.

Monitoreo de Eventos de Seguridad Basada en la Infraestructura de TI de las Entidades

Revisión de alertas producto de la correlación de los registros de eventos (Logs) de las plataformas de seguridad, para generación de alertas y advertencias de seguridad digital.

Monitoreo de Portales WEB del Dominio GOV.CO

Monitoreo de la disponibilidad de los portales web, informando cualquier degradación del servicio al administrador del portal, para que realice las acciones necesarias para restablecer el servicio.

SERVICIOS REACTIVOS

Son los que apoyan la Gestión, el tratamiento y el manejo de evidencias de los incidentes cibernéticos en la infraestructura tecnológica.

Gestión de incidentes

Permite realizar acompañamiento y asesoría cuando se presente un incidente cibernético en cada una de las fases de la gestión de incidentes (Detección, Evaluación, Análisis, Notificación, Contención, Erradicación y Recuperación.

Coordina las tareas de respuesta entre la entidad, los sitios relacionados con el ataque, las partes que dan soporte en TI, proveedores de servicios de Internet, a otros CSIRT (colCERT CCOCI CECIP), los administradores de redes y del sistema, igualmente realizar actividades encaminadas a facilitar el intercambio y el análisis de la información

Análisis de Malware

Consiste en determinar cuáles son las acciones adecuadas para detectar y conocer los indicadores de compromisos que permitan generar por parte de los proveedores de herramientas de seguridad firmas para su eliminación

SERVICIOS DE GESTIÓN DE CALIDAD DE LA SEGURIDAD

Son servicios diseñados para aumentar la conciencia en Seguridad Digital, especialmente en la percepción de los riesgos y amenazas cibernéticas en los funcionarios y generar conocimiento, capacidades, destrezas y habilidades a los CIO´sy CISO´s de las entidades, con el fin generar una cultura de reporte y gestión de incidentes.

MGRSD

El Modelo de Gestión de Riesgos de Seguridad Digital tiene por objetivo brindar un marco de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas y vulnerabilidades a las que una entidad pueda estar expuesta al momento de llevar a cabo actividades socio económicas en el entorno digital (prestación de trámites, servicios internos y externos, transacciones en línea entre otros) para así, fomentar y mantener la confianza de las múltiples partes interesadas (proveedores, ciudadanos, entidades públicas y privadas) en el uso del entorno digital en su interacción con Estado, impulsando así la prosperidad económica y social del país.

El MGRSD instrumentaliza sus lineamientos generales para las entidades públicas a través de la "Guía para la Administración de Riesgos y el Diseño de Controles en Entidades Públicas" y su anexo 4 denominado "Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas ". Estos lineamientos no trabajan de manera aislada, por el contrario, están alineados y articulados con otras iniciativas existentes en el gobierno nacional para facilitar su adopción e implementación.

El MGRSD deberá ser implementado por todas las entidades de la rama ejecutiva del poder público, contempladas en el ámbito de aplicación del Decreto 1008 de 2018, el Decreto 1499 de 2017 y el Decreto 1083 de 2015.

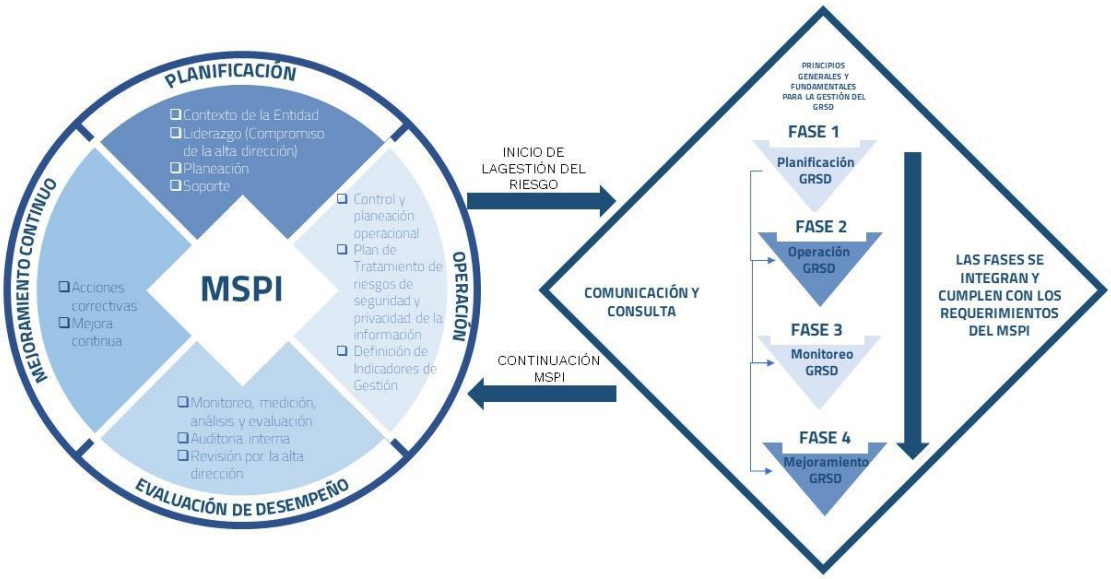

Imagen 1. MGRSD – fuente mintic.

Conforme lo indica el DAFP, las entidades públicas deben realizar la identificación del contexto interno y externo de la entidad, sin embargo, es necesario profundizar en este análisis relacionado con seguridad de la información, por lo tanto, a continuación, se dan unas directrices adicionales para realizar la actividad adecuadamente.

El contexto interno considera factores que impactan directamente a:

- La entidad pública, en general, su organización, sistemas de información o servicios, reglamentación interna, número de sedes, empleados, entre otros aspectos.
- Cada uno de los procesos sobre los cuales están soportadas sus operaciones.

Para determinar los factores de la entidad pública y los procesos se debe considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:

PARA LA ENTIDAD PÚBLICA	PARA LOS PROCESOS
✓ **Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros** ✓ **Flujos de información y los procesos de toma de decisiones** ✓ **Empleados, contratistas** ✓ **Objetivos estratégicos y la forma de alcanzarlos**	✓ Identificación de los procesos y su respectiva caracterización ✓ Detalle de las actividades que se llevan a cabo en el proceso ✓ Flujos de información ✓ Identificación y actualización de los activos en la cadena de valor de la entidad pública

✓ **La misión, visión, valores y cultura de la organización**	✓ Recursos
✓ **Sus políticas, procesos y procedimientos**	✓ Alcance del proceso
✓ **Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros)**	✓ Relaciones con otros procesos de la entidad pública
✓ **Toda la estructura organizacional**	✓ Cantidad de ciudadanos afectados por el proceso
✓ **Roles y responsabilidades**	✓ Procesos de gestión de riesgos que se tienen actualmente implementados
✓ **Sistemas de información o servicios.**	✓ Personal involucrado en la toma de decisiones

Tabla 1. Procesos a coordinar, fuente1. mintic

El alcance de la administración del riesgo de seguridad de la información debe ser extensible y aplicable a los procesos de la entidad pública que indiquen los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información3, habilitador de la Estrategia de Gobierno Digital.

Es necesario que la entidad pública establezca una política de gestión de riesgo integral, donde se incluya el compromiso en la gestión de los riesgos de seguridad de la información en todos sus niveles. Esta debe crearse como lo indica la Guía de administración del riesgo de gestión del DAFP, incluyendo la gestión de riesgos de seguridad de la información. Esta actividad es responsabilidad de la Línea estratégica dispuesta por el MIPG.

Definición de recursos para la Gestión de riesgos de seguridad de la información

La entidad pública debe disponer los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad de la información, (capital, tiempo, personal, procesos, sistemas y tecnologías), con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos de seguridad de la información.

La línea estratégica o alta dirección debe asignar entre otros, recursos tales como:

- Personal capacitado e idóneo para la gestión del riesgo de seguridad de la información.
- Recursos económicos para la implementación de controles para la mitigación de riesgos (con base al análisis de riesgo realizado, teniendo en cuenta el alcance de la política de riesgos de la entidad en cuanto a seguridad de la información), que permita ser incluido dentro de la gestión presupuestal y eficiencia del gasto público de la entidad.
- Recursos para los aspectos de mejora continua, monitoreo y auditorías.

Identificación de activos de información

Un activo de información es cualquier elemento que participe en el tratamiento de información que tenga valor para la organización, sin embargo, en el contexto de seguridad de la información son activos elementos tales como: hardware, software, aplicaciones de la entidad pública, servicios Web, redes, información digital, personal, ubicación, organización, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.

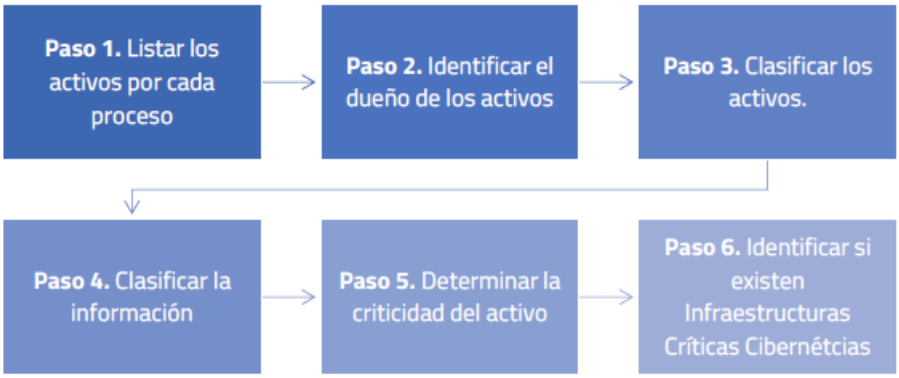

Imagen 2. Identificación de activos de información – fuente: mintic

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública.

Identificar los riesgos inherentes de seguridad de la información

la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas" emitida por el DAFP, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

Identificación de Amenazas:

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

• Deliberadas (D), fortuitas (F) o ambientales (A).

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
	Fenómenos climáticos	A

Tabla 2 Tabla de Amenazas

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	• Reto • Ego • Rebelión • Estatus • Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	• Destrucción de la información • Divulgación ilegal de la información • Ganancia monetaria • Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	• Chantaje • Destrucción • Explotación • Venganza • Ganancia política • Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	• Ventaja competitiva • Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica • Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	• Curiosidad • Ego • Inteligencia • Ganancia monetaria • Venganza • Errores y omisiones no intencionales (ej.	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto

Tabla 3. Tabla de amenazas dirigidas al hombre – fuente: mintic

Identificación de vulnerabilidades: la entidad pública puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla

Tabla 4. Tabla de vulnerabilidades comunes. Fuente: mintic

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
HARDWARE	• Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento • Ausencia de esquemas de reemplazo periódico • Susceptibilidad a la humedad, el polvo y la suciedad • Sensibilidad a la radiación electromagnética • Ausencia de un eficiente control de cambios en la configuración	• Incumplimiento en el mantenimiento del sistema de información. • Destrucción de equipos o medios. • Polvo, corrosión y congelamiento • Radiación electromagnética • Error en el uso
	Susceptibilidad a las variaciones de voltaje Susceptibilidad a las variaciones de temperatura Almacenamiento sin protección física	Pérdida del suministro de energía Fenómenos meteorológicos Hurtos medios o documentos. Hurtos medios o documentos. Hurtos medios o documentos. Abuso de los derechos

SOFTWARE	Falta de cuidado en la disposición final	Abuso de los derechos
	Copia no controlada	Abuso de los derechos
	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	Corrupción de datos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Corrupción de datos
	Ausencias de pistas de auditoria	Error en el uso
	Asignación errada de los derechos de acceso	Error en el uso
	Software ampliamente distribuido	Error en el uso
	En términos de tiempo utilización de datos errados en los programas de aplicación	Falsificación de derechos
	Interfaz de usuario compleja	Falsificación de derechos
	Ausencia de documentación	Falsificación de derechos
	Configuración incorrecta de parámetros	Procesamiento ilegal de datos
	Fechas incorrectas	Mal funcionamiento del software
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Mal funcionamiento del software
	Tablas de contraseñas sin protección	
	Gestión deficiente de las contraseñas	
	Habilitación de servicios innecesarios	
	Software nuevo o inmaduro	
	Especificaciones incompletas o no claras para los desarrolladores	
RED	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
		Uso no autorizado del equipo
		Negación de acciones
		Escucha encubierta

	Fallas en la producción de informes de gestión Ausencia de pruebas de envío o recepción de mensajes Líneas de comunicación sin protección Tráfico sensible sin protección Conexión deficiente de los cables Punto único de fallas Arquitectura insegura de la red Transferencia de contraseñas en claro Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento) Conexiones de red pública sin protección	Escucha encubierta Fallas del equipo de telecomunicaciones Fallas del equipo de telecomunicaciones Falsificación de derechos Espionaje remoto Espionaje remoto Saturación del sistema de información Uso no autorizado del equipo
PERSONAL	Ausencia del personal Procedimientos inadecuados de contratación Entrenamiento insuficiente en seguridad Uso incorrecto de software y hardware Falta de conciencia acerca de la seguridad Ausencia de mecanismos de monitoreo Trabajo no supervisado del personal externo o de limpieza	Incumplimiento en la disponibilidad del personal Destrucción de equipos y medios Error en el uso Error en el uso Error en el uso Procesamiento ilegal de los datos Hurto de medios o documentos.
LUGAR	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos Ubicación en área susceptible de inundación Red energética inestable Ausencia de protección física de la edificación (Puertas y ventanas)	Uso no autorizado del equipo Hurto de medios o documentos Destrucción de equipos o medios Falla en equipo de telecomunicaciones

ORGANIZACIÓN	Ausencia de protección física de la edificación (Puertas y ventanas)	
	Ausencia de procedimiento formal para el registro y retiro de usuarios	
	Ausencia de proceso formal para la revisión de los derechos de acceso	
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	
	Ausencia de auditorias	Hurto de medios o documentos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
		Abuso de los derechos
		Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
		Abuso de los derechos
		Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de estos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	
	Ausencia de procedimiento formal para la documentación del MSPI	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
		Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
		Negación de acciones
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Falla del equipo
		Error en el uso
		Error en el uso
	Ausencia de planes de continuidad	Error en el uso
		Error en el uso
	Ausencia de políticas sobre el uso de correo electrónico	Hurto de equipo
		Hurto de equipo
		Hurto de equipo

	Ausencia de procedimientos para introducción del software en los sistemas operativos Ausencia de registros en bitácoras Ausencia de procedimientos para el manejo de información clasificada Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información Ausencia de política formal sobre la utilización de computadores portátiles Ausencia de control de los activos que se encuentran fuera de las instalaciones Ausencia de política sobre limpieza de escritorio y pantalla Ausencia de autorización de los recursos de procesamiento de información Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad Ausencia de revisiones regulares por parte de la gerencia Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Hurto de medios o documentos Hurto de medios o documentos Hurto de medios o documentos Uso no autorizado de equipo Uso no autorizado de equipo Uso de software falsificado o copiado

Tabla 5. Tabla de Amenazas y Vulnerabilidades

Identificación del riesgo inherente de seguridad de la información

Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.

Adicionalmente, se debe identificar el dueño del riesgo, es decir, "quien tiene que rendir cuentas sobre el riesgo o quien tiene la autoridad para gestionar el riesgo".

La identificación de riesgos, amenazas y vulnerabilidades puede ser realizada a través de diferentes metodologías. Como ejemplo, se citan las siguientes:

- Lluvia de ideas: mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas asociadas al manejo de la información digital y los activos de información se pueden presentar o casos ocurridos que los participantes conozcan que se hayan dado en la entidad pública o en el sector. Deben existir un orden de la sesión, un líder y personas que ayuden con la captura de las memorias.
- Juicio de expertos: a través de este esquema se reúnen las personas con mayor conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad de la información se pueden presentar. Para emplear esta técnica, se requiere disponer de una agenda con un orden de temas, establecer reglas claras y contar con la participación de un orientador o moderador, así como personas que tomen notas de los principales conceptos expuestos. Al finalizar, se retoman los principales riesgos identificados y se procede a hacer una valoración
- Análisis de escenarios: en este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse: explosión de un pozo, sobrecarga de un nodo, pérdida de control de una unidad operada remotamente; y con base en estas posibilidades, se determina qué puede llegar a suceder, desde la perspectiva digital, a los activos de información y las consecuencias de la afectación.
- Otras técnicas que pueden ser empleadas son: entrevistas estructuradas, encuestas o listas de chequeo.

Posterior a la identificación de los riesgos de seguridad de la información con sus respectivas amenazas y vulnerabilidades enunciadas en este documento, se deberá continuar con el Paso 3. Valoración del Riesgo, de la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas" del DAFP.

Identificación del nivel de confianza para la autenticación digital

Se deben identificar aquellos tramites y servicios ciudadanos digitales que deben contar con autenticación digital de acuerdo con lo señalado en la guía de lineamientos para los Servicios Ciudadanos Digitales, en la que se establece que inicialmente, para el acceso al servicio de Autenticación Digital, las entidades deben identificar y determinar el grado de confianza requerido para los procesos relacionados con el trámite acorde con la siguiente clasificación:

- Bajo: Ofrece un nivel de confianza mínimo en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es mínimo.

- Medio: Ofrece cierto nivel de confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es moderado.
- Alto: Ofrece una gran confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea implica un riesgo alto.
- Muy alto: Ofrece más confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea implica un riesgo extremo

Identificación y evaluación de los controles existentes

Para determinar si existen uno o varios controles asociados a los riesgos inherentes identificados se en los OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA (Tomados del Anexo A de la Norma ISO/IEC 27001:2013) como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad.

Tratamiento de los riesgos de seguridad de la información

Una vez se han identificado los riesgos, se debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos previamente en la Política de Administración de Riesgos Institucional.

El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, se puede tener en cuenta las opciones planteadas en la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas" del DAFP: Evitar, aceptar, compartir o mitigar el riesgo.

Planes de Tratamiento de Riesgos de Seguridad de la información e Indicadores para la Gestión del Riesgo

Aquí la Línea Estratégica debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos.

El responsable de seguridad digital deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes (Primer Línea de Defensa y la Oficina de Tecnologías de la Información -TI- generalmente)

Monitoreo y revisión

a través de las Tres Líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, Componente Actividades de control, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.

- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad de la información para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles

En esta fase se deben evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles propuestos, de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad pública. Así mismo, también deberán tenerse en cuenta los incidentes de seguridad de la información que hayan afectado a la entidad y también las métricas o indicadores definidos para hacer seguimiento a las medidas de seguridad implementadas. Todo lo anterior contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la línea estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y las partes interesadas.

Registro y reporte de incidentes de seguridad de la información

Es importante que cuente con el registro de los incidentes de seguridad de la información que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

Reporte de la gestión del riesgo de seguridad de la información al interior de la entidad pública

El responsable de seguridad digital debería reportar periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:

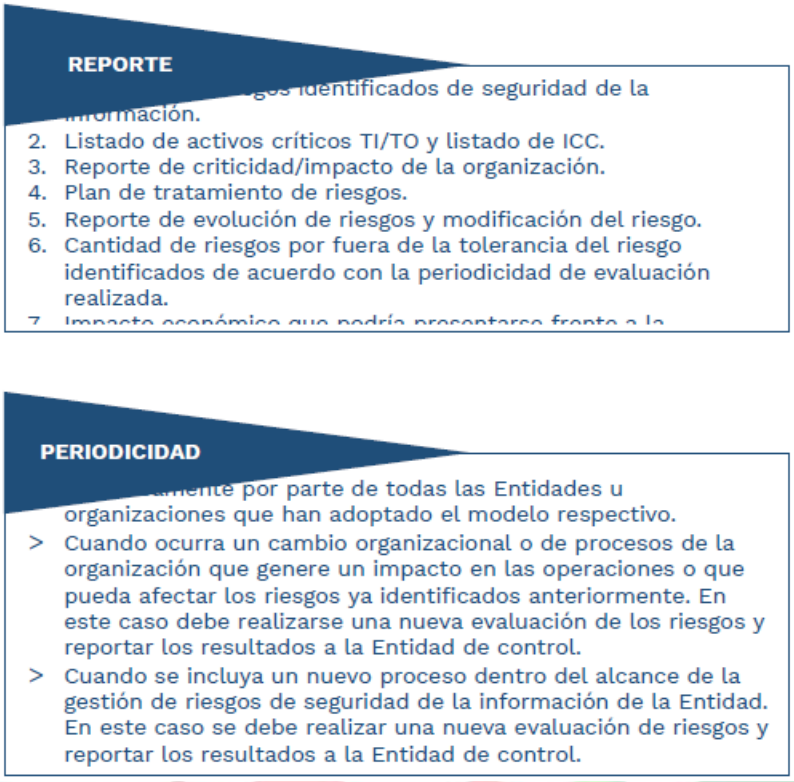

Imagen 3. Reporte de información fuente: mintic

Reporte de la gestión del riesgo de seguridad de la información a autoridades o entidades especiales

Una vez se obtenga los resultados de la gestión de riesgos de seguridad de la información, se debería consolidar información (previamente obtenida con la aplicación del modelo) con el fin de reportarla a futuro a las autoridades o instancias encargadas del tema y que el Gobierno defina.

La finalidad del reporte de esta información es que el Gobierno Nacional pueda identificar posibles oportunidades para la generación de política pública, generación de capacidades o asignación de recursos que permita ayudar a la mejora de la seguridad de la información.

Información por consolidar para generar el reporte de información:

Se propone que las entidades públicas consoliden la siguiente información puntual para poder llevar a cabo el reporte respectivo:

- Riesgos con nivel crítico
- Amenazas críticas

- Vulnerabilidades críticas
- Tipos de Activos afectados por los riesgos críticos (incluyendo servicios digitales o que delimitan con internet)
- Planes de tratamiento propuestos para la mitigación y si han sido ejecutados
- Servicios digitales críticos en la entidad pública (Servicios o trámites para los ciudadanos o sistemas de información críticos para la entidad).

Esta información tiene por objetivo permitir la construcción de un panorama de riesgos de seguridad de la información de todo el país, para poder tomar decisiones estratégicas para la construcción de política pública, generación de capacidades o planes de acción con base a la información que pueda analizarse.

Mejoramiento continuo de la gestión del riesgo de seguridad de la información
La entidad pública debe garantizar la mejora continua de la gestión de riesgos de seguridad de la información, por lo tanto, debe establecer que cuando existan hallazgos, falencias o incidentes de seguridad de la información se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.

Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad de la información de la siguiente forma:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

CONCLUSION

En la conclusión de este Plan de Seguridad de la Información, se destaca la importancia crítica de la seguridad digital en el contexto dinámico y desafiante en el que operamos. Reconocemos que la protección de la información no es simplemente una responsabilidad, sino un imperativo estratégico que resguarda la integridad de nuestros servicios y la confianza de nuestras partes interesadas. Este plan, elaborado con atención a los principios de confidencialidad, integridad y disponibilidad, sienta las bases para una cultura organizacional donde la seguridad digital no es solo una medida de cumplimiento, sino una expresión tangible de nuestro compromiso con la excelencia y la protección de los activos digitales de SIVA S.A.S.

Al implementar esta política, nos embarcamos en un viaje hacia la resiliencia digital, donde la gestión proactiva de riesgos, la conciencia del personal y la mejora continua se entrelazan para fortalecer nuestra postura frente a amenazas emergentes. Este plan no es estático; es un documento vivo que evolucionará con el panorama de seguridad digital. Con la participación activa de cada miembro de la organización, nos aseguramos de que la seguridad de la información sea no solo un conjunto de medidas, sino una parte integral de nuestra identidad corporativa, impulsando la confianza y la sostenibilidad a medida que avanzamos hacia un futuro digital.

NOMBRE	ELABORADO POR:	REVISÓ:	APROBÓ	VERSIÓN
POLITICA DE GOBIERNO DIGITAL	JOSÉ LUIS PEÑARANDA TORO ING - ELECTRÓNICO			1.0