PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2026

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

JAIME ANDRÉS GONZÁLEZ MEJÍA
GERENTE
2026

COMPROMISO DE LA ALTA DIRECCIÓN

En SIVA SAS, reconocemos que la seguridad y privacidad de la información son pilares fundamentales para el éxito sostenible de nuestra organización y la confianza de quienes confían en nosotros. Este compromiso se refleja en nuestro Plan de Seguridad y Privacidad de la Información (PSPI) - Versión 4, una manifestación de nuestra dedicación a salvaguardar los datos de manera integral y respetar la privacidad de todas las partes involucradas.

Nos comprometemos a:
Confidencialidad: Garantizar la confidencialidad de la información, protegiendo los datos contra accesos no autorizados y asegurando que solo aquellos con los derechos correspondientes tengan acceso a la información.

Integridad: Salvaguardar la integridad de los datos, implementando controles que aseguren la exactitud y consistencia de la información a lo largo de su ciclo de vida.

Disponibilidad: Garantizar la disponibilidad de la información crítica, adoptando medidas proactivas para prevenir interrupciones y asegurar la continuidad de los servicios.

Privacidad de la Información: Respetar y proteger la privacidad de los individuos, aplicando prácticas y controles específicos para el manejo de datos personales en conformidad con las leyes y regulaciones aplicables.

Cumplimiento Legal: Cumplir con todas las leyes y regulaciones relacionadas con la seguridad y privacidad de la información en todas las jurisdicciones en las que operamos.

Mejora Continua: Buscar constantemente la mejora continua en nuestras prácticas de seguridad y privacidad, adaptándonos a los cambios tecnológicos y evaluando activamente los riesgos emergentes.

Transparencia y Educación: Fomentar la transparencia en nuestras prácticas de seguridad y privacidad, proporcionando información clara y educación a todas las partes interesadas sobre sus derechos y responsabilidades.

Gobernanza Efectiva: Establecer y mantener una gobernanza efectiva de la seguridad y privacidad de la información, con roles y responsabilidades claros para garantizar una implementación coherente de nuestro PSPI.

A través de este compromiso, buscamos no solo cumplir con estándares y regulaciones, sino superar las expectativas de seguridad y privacidad de aquellos que confían en nosotros. Este PSPI no es solo un documento; es una promesa de responsabilidad y respeto hacia la información y la privacidad de cada individuo y entidad que forma parte de nuestro ecosistema.

CONTENIDO

NTRODUCCIÓN

En la era digital actual, donde la información se ha convertido en uno de los activos más valiosos, salvaguardar la seguridad y privacidad de los datos es imperativo para la sostenibilidad y confianza de cualquier entidad. El Sistema Integrado de Transporte de Valledupar (SIVA SAS), consciente de la importancia crítica de la protección de la información, presenta la versión 4 de su Plan de Seguridad y Privacidad de la Información (PSPI).

Este documento refleja la evolución continua de nuestras prácticas y políticas para asegurar la confidencialidad, integridad y disponibilidad de la información, así como para respetar y proteger la privacidad de nuestros usuarios y partes interesadas. La versión 4 del PSPI se forja en la experiencia acumulada, la evaluación constante de riesgos y el compromiso inquebrantable con los estándares más elevados de seguridad y privacidad.

En un mundo digital en constante cambio, el PSPI no solo se presenta como un marco estático, sino como un documento dinámico que refleja nuestra adaptabilidad a las amenazas emergentes y a las expectativas cambiantes de privacidad. A través de este plan, reafirmamos nuestro compromiso de ser custodios responsables de la información confiada a nosotros, buscando el equilibrio adecuado entre la innovación tecnológica y la protección de la privacidad.

Este PSPI no solo es un compromiso con el cumplimiento de regulaciones y normativas, sino un reflejo de nuestra dedicación a la construcción y fortalecimiento de la confianza. Invitamos a todas las partes interesadas, internas y externas, a sumergirse en este documento, entender nuestras políticas y colaborar en la creación de un entorno digital seguro y confiable para todos.

Con este propósito en mente, presentamos la versión 4 del Plan de Seguridad y Privacidad de la Información de SIVA SAS, confiados en que sirva como un faro que guíe nuestra organización hacia un futuro digital más seguro y respetuoso de la privacidad.

DEFINICIONES

Seguridad de la Información: La seguridad de la información se refiere a la protección de datos contra accesos no autorizados, la prevención de la alteración de la información y la garantía de su disponibilidad cuando sea necesario. Incluye prácticas, políticas y tecnologías diseñadas para gestionar y mitigar los riesgos asociados con el manejo de la información.

Privacidad de Datos: La privacidad de datos se refiere al control que una persona tiene sobre la información relacionada con ella. Incluye el derecho a saber qué datos se recopilan, quién los recopila y con qué propósito. La privacidad de datos implica proteger la información personal de usos no autorizados y garantizar su manejo ético.

Plan de Continuidad del Negocio (BCP): Un Plan de Continuidad del Negocio es un conjunto de procedimientos y políticas diseñadas para garantizar que una organización pueda mantener operaciones críticas en caso de interrupciones significativas, como desastres naturales, ataques cibernéticos o emergencias.

Cifrado de Datos: El cifrado de datos es el proceso de transformar información legible en un formato ilegible utilizando algoritmos matemáticos. Este proceso protege la confidencialidad de la información y garantiza que solo aquellos con la clave correcta puedan acceder y comprender los datos cifrados.

Riesgo de Seguridad de la Información: El riesgo de seguridad de la información se refiere a la probabilidad de que un evento no deseado o una amenaza impacte negativamente en la confidencialidad, integridad o disponibilidad de la información. La gestión de riesgos es esencial para identificar, evaluar y mitigar estos riesgos.

Gestión de Incidentes de Seguridad: La gestión de incidentes de seguridad implica la preparación, detección, respuesta y recuperación de eventos de seguridad no deseados. Esto incluye la identificación y mitigación de amenazas, así como la restauración de sistemas y datos afectados.

Auditoría de Seguridad: La auditoría de seguridad es un proceso sistemático de revisión y evaluación de los controles de seguridad de una organización. Se realiza para garantizar el cumplimiento de políticas y estándares, identificar vulnerabilidades y mejorar la postura general de seguridad.

Conformidad Normativa: La conformidad normativa implica cumplir con las leyes, regulaciones y estándares relacionados con la seguridad y privacidad de la información. Esto puede incluir normativas gubernamentales, leyes de protección de datos y estándares de la industria.

Firewall: Un firewall es una barrera de seguridad que controla y monitorea el tráfico de red entre redes confiables e no confiables. Su objetivo es prevenir accesos no autorizados y proteger contra amenazas cibernéticas.

Phishing: El phishing es un tipo de ataque cibernético en el que los delincuentes intentan engañar a las personas para que revelen información confidencial, como contraseñas o datos financieros, a menudo haciéndose pasar por entidades de confianza.

Token de Seguridad: Un token de seguridad es un dispositivo físico o aplicación que genera códigos temporales utilizados en la autenticación de dos factores. A menudo se utiliza para agregar una capa adicional de seguridad a las cuentas en línea.

Vulnerabilidad: Una vulnerabilidad es una debilidad en un sistema o proceso que podría ser explotada para comprometer la seguridad. Identificar y remediar vulnerabilidades es esencial para proteger sistemas contra posibles amenazas.

Gestión de Identidad y Acceso (IAM):
La gestión de identidad y acceso es un conjunto de procesos y tecnologías que aseguran que solo usuarios autorizados tengan acceso a los recursos de la organización. Incluye la gestión de credenciales, autenticación y autorización.

Hacking Ético: El hacking ético es la práctica de utilizar habilidades de hacking de manera ética para identificar vulnerabilidades en sistemas y redes con el objetivo de mejorar la seguridad. Se realiza de manera autorizada y legal.

Resiliencia Cibernética: La resiliencia cibernética se refiere a la capacidad de una organización para resistir, recuperarse y adaptarse a eventos cibernéticos adversos. Incluye la planificación de la continuidad del negocio y la respuesta a incidentes.

OBJETIVOS

Objetivo general

El objetivo general de este Plan de Seguridad y Privacidad de la Información (PSPI) es establecer un marco integral y dinámico que garantice la confidencialidad, integridad y disponibilidad de la información crítica de SIVA SAS, al tiempo que salvaguarda la privacidad de los datos de todas las partes interesadas. Este plan tiene como meta fundamental fortalecer la postura de seguridad y privacidad de la entidad, promoviendo una cultura organizacional proactiva y comprometida con las mejores prácticas en el manejo de la información.

Componentes Clave del Objetivo General:

- Confianza y Credibilidad: Construir y mantener la confianza y credibilidad de clientes, empleados y partes interesadas a través de prácticas sólidas de seguridad y privacidad.
- Protección Integral de la Información: Asegurar la protección integral de la información, abordando tanto los aspectos de seguridad como de privacidad para garantizar un enfoque holístico.
- Adaptabilidad a Riesgos Emergentes: Desarrollar la capacidad de adaptarse a los riesgos emergentes mediante la evaluación continua y la actualización proactiva de medidas de seguridad y privacidad.
- Cultura Organizacional: Fomentar una cultura organizacional que valore la seguridad y privacidad de la información como un elemento clave en todas las operaciones y decisiones.
- Cumplimiento Normativo: Garantizar el cumplimiento de leyes, regulaciones y estándares relacionados con la seguridad y privacidad de la información, tanto a nivel nacional como internacional.
- Resiliencia y Continuidad: Reforzar la resiliencia de la entidad frente a incidentes de seguridad y garantizar la continuidad de las operaciones críticas en todo momento.
- Concientización y Educación: Promover la concientización y educación continua sobre seguridad y privacidad entre empleados y colaboradores para fomentar la responsabilidad compartida.

- Innovación Responsable: Facilitar un entorno que promueva la innovación tecnológica de manera responsable, considerando siempre los aspectos de seguridad y privacidad desde la fase inicial de los proyectos.
- Mejora Continua: Establecer un ciclo de mejora continua, donde las lecciones aprendidas, los cambios en el entorno de amenazas y las innovaciones en seguridad y privacidad se integren en políticas y prácticas de manera oportuna.
- Protección de Datos Personales: Garantizar un manejo ético y responsable de los datos personales, respetando los derechos individuales y cumpliendo con las expectativas de privacidad de los usuarios.

Objetivos Específicos

- Aumentar la participación en programas de concientización y capacitación en seguridad en un 30% en comparación con el año anterior.
- Desarrollar e implementar módulos de capacitación interactivos y relevantes.
- Realizar auditorías periódicas de políticas de privacidad para identificar posibles brechas.
- Mejorar la capacidad de monitoreo y detección de amenazas cibernéticas.
- Mantenerse informado sobre cambios en leyes y regulaciones relevantes para la privacidad de datos.

MARCO NORMATIVO

El Plan Estratégico de las Tecnologías de Información – PETI, aplicado al Sistema Integrado de Transporte de Valledupar SIVA S.A.S se encuentra directamente relacionado a la normativa nacional colombiana, por tal razón es compromiso de esta entidad seguir detalladamente las pautas que presenta el MINTIC para las entidades del estado.

En la siguiente tabla, se presentan las normas a considerar aplicables con respecto a la elaboración del documento PETI y otras regulaciones relevantes del Sistema Integrado de Transporte de Valledupar SIVA S.A.S en el tema tecnológico.

Norma	Descripción
Directiva Presidencial No. 10 de 2002	Programa de renovación de la Administración Pública: hacía un Estado Comunitario.
Ley 790 de 2002	Programa de Reforma de la Administración Pública.
Conpes 3248 de 2003	Renovación de la Administración Pública.
Decreto 3816 de 2003	Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública.
Decreto Nacional 1151 del 14 de abril de 2008	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
Ley 1341 2009	Define principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional de Espectro
Decreto 235 de 2010	Intercambio de información entre entidades para el cumplimiento de funciones públicas.
Decreto 2693 2012	Establece los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011
Ley 1551 de 2012	Por el cual se establece las funciones del Municipio.

Decreto 2573 del 12 de diciembre de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Resolución 3564 2015	Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)
Decreto 1078 del 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Resolución 2405 2016	Adopta el modelo del Sello de Excelencia Gobierno en Línea y se conforma su comité
Decreto 728 2016	Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico
Decreto 415 de 2016	Por el cual se establece que el director de TI, conocido como Chief Information Officer (CIO) es el encargado de coordinar y alinear la ejecución de los procesos relacionados con tecnología en todas las organizaciones.
Decreto 1413 de 2017	Actualiza el Decreto Único Reglamentario del sector de las TIC, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales
Decreto 1008 2018	Establece los lineamientos generales de la política de Gobierno Digital y actualizando el Decreto Único Reglamentario del sector de las TIC
NTC / ISO 27001:2018	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC / ISO 31000 - 2018	Gestión del Riesgo. Principios y directrices.
CONPES 3975 2019	Política Nacional Para La Transformación Digital E Inteligencia Artificial

Directiva 02 2019	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones
Ley 1955 2019	Simplificación de interacción digital los ciudadanos y el Estado
Ley 1978 del 2019	Plan de desarrollo 2018-2022. "pacto por Colombia, pacto por la equidad¨
Decreto 2106 del 2109	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Publica Efectiva
Decreto 620 mayo 2020	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
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.
Resolucion 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
Conpes 3995 de 2020	Este documento CONPES busca fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.
Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública diciembre de 2020
Resolución 2893 de 2020	Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPA, 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
Ley 2080 de 2021	por medio de la cual se reforma el código de procedimiento administrativo y de lo contencioso administrativo -ley 1437 de 2011- y se dictan otras disposiciones en materia de descongestión en los procesos que se tramitan ante la jurisdicción
Directiva Presidencial 03 de 2021	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
Decreto 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Resolución 1117 de 2022	Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital
Resolución 746 de 2022	por el cual se modifica la estructura de la Agencia Nacional de Infraestructura y se determinan las funciones de sus dependencias.
Decreto 338 de 2022	Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones
Directiva Presidencial 02 de 2022	Reiteración de la política pública en materia de seguridad digital.

Resolución 460 de 2022	or la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
Decreto 088 de 2022	Por el cual se adiciona el Titulo 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 artículos 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
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	Política de Gobierno Digital

Tabla 1. Marco normativo

ROLES Y RESPONSABILIDADES

Definición de roles y responsabilidades

Todas las entidades deben definir internamente las responsabilidades para ejecutar las actividades específicas de seguridad de la información designando a las personas apropiadas.

El Sistema Estratégico de transporte de Valledupar SIVA SAS tiene como responsables de la implementación, seguimiento y mantenimiento de la Política del Plan de Seguridad y Privacidad de la información lo siguiente:

- El Profesional de Gestión administrativa, quien velara por el cumplimiento de la Política de Seguridad y privacidad de la Información
- El Profesional de planeación quien será el delegado para velar la formulación e implementación de la Política de seguridad y privacidad de la información.
- El profesional Universitario encargado de la gestión de TICS, será el encargado de desarrollar la implementación de la Política de seguridad y privacidad de la información.
- Todos los funcionarios y/o contratistas y demás partes interesadas del Sistema Estratégico de transporte de Valledupar SIVA SAS son responsables del cumplimiento obligatorio de la Política de seguridad y Privacidad de la Información y en caso de no cumplir se reserva el derecho de tomar las medidas correspondientes según el caso.

Para comunicar esta política se hará mediante socialización con todos los funcionarios, contratista y partes interesadas del Sistema Estratégico de transporte de Valledupar SIVA SAS, el cual dará a conocer la existencia, contenido y obligatoriedad de dicho documento. La custodia y ubicación física del documento estará a cargo del Sistema Integrado de Gestión y el líder de TIC.

Responsable de Seguridad de la Información (RSI):

Responsabilidades:

- Desarrollar, implementar y supervisar políticas y procedimientos de seguridad de la información.
- Coordinar la respuesta a incidentes de seguridad y liderar las investigaciones correspondientes.
- Evaluar y mitigar riesgos de seguridad y privacidad en colaboración con otros departamentos.
- Mantenerse actualizado sobre las amenazas y tendencias de seguridad para adaptar estrategias y controles.

Oficial de Privacidad de Datos:

Responsabilidades:

- Supervisar la conformidad con las leyes y regulaciones de privacidad de datos.
- Desarrollar y mantener políticas de privacidad y procedimientos internos.
- Actuar como punto de contacto para consultas relacionadas con la privacidad de datos.
- Colaborar con el RSI para garantizar una protección integral de la información.

Equipo de Gestión de Incidentes:

Responsabilidades:

- Detectar, investigar y responder a incidentes de seguridad.
- Coordinar la implementación de medidas correctivas después de un incidente.
- Mantener registros detallados de los incidentes y las acciones tomadas.
- Realizar análisis pos-tincidente para mejorar las estrategias de seguridad.

Personal de Tecnologías de la Información (TI):

Responsabilidades:

- Implementar y mantener medidas de seguridad técnica, como firewalls y cifrado.
- Supervisar la integridad y disponibilidad de sistemas y datos.

- Colaborar con el RSI en la identificación y mitigación de vulnerabilidades.
- Participar en programas de concientización y capacitación en seguridad.

Usuarios Finales:

Responsabilidades:

- Cumplir con las políticas y procedimientos de seguridad de la información.
- Informar de inmediato cualquier incidente o actividad sospechosa al equipo de gestión de incidentes.
- Participar activamente en programas de concientización y capacitación en seguridad.
- Contribuir a la protección de datos y la privacidad mediante prácticas seguras.

Auditor Interno de Seguridad:

Responsabilidades:

- Realizar auditorías regulares de conformidad con políticas y procedimientos.
- Evaluar la efectividad de los controles de seguridad implementados.
- Proporcionar informes detallados de hallazgos y recomendaciones.
- Colaborar con el RSI en la mejora continua de políticas y prácticas de seguridad.

Estas definiciones de roles y responsabilidades establecen una estructura organizativa clara para la implementación y gestión efectiva del PSPI. Cada rol contribuye de manera única a la protección integral de la información y la promoción de una cultura organizacional comprometida con la seguridad y privacidad.

Comité Institucional de Gestión y Desempeño Institucional – Comité de Seguridad y privacidad de la información

Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:

- Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad y privacidad de la información.
- Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad.
- Aprobar acciones y mejores prácticas que en la implementación del MSPI.
- Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.

Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

Oficina Jurídica y Contratación

- Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.
- Representar a la entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente

Gestión del Talento Humano

- Controlar y salvaguardar la información de datos personales del personal de planta de la entidad, en concordancia con la normatividad vigente.

- Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

Control Interno

Dentro de la definición de responsables en cada uno de los Dominios entregados en el Marco de Arquitectura Empresarial, está contemplado el papel del responsable de seguridad y privacidad de la información de la entidad, de esta forma se tienen las siguientes responsabilidades específicas de acuerdo con el Dominio:

DOMINIO	RESPONSABILIDADES
SERVICIOS TECNOLÓGICOS	• Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. • Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. • Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. • Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. • Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. • Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar

	vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
ESTRATEGIA TI	Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.
GOBIERNO TI	Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información
SISTEMAS DE INFORMACIÓN	• Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. • Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. • Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. • Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.

	• Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio
DE INFORMACIÓN	• Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. • -Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información
USO Y APROPIACIÓN	• Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. • Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. • Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

Tabla 1: Responsabilidad - MRAE

METODOLOGIA

El Sistema Estratégico de transporte de Valledupar SIVA SAS divulga los objetivos y alcances de la seguridad de la información dentro de la entidad, que son efectivos por medio de controles de seguridad, con el fin de mantener, gestionar y mitigar el riesgo como se estable en el Plan de Tratamiento de Riesgos, garantizando así la continuidad de los servicios y disminuyendo la probabilidad de amenazas que puedan afectar los procesos internos para el cumplimiento de la prestación del servicio.

Identificación, clasificación y valoración de activos de información.

Cada proceso, bajo supervisión y con base en el inventario de activos del Sistema Estratégico de transporte de Valledupar SIVA SAS siempre se debe estar actualizando en donde se incorpore la clasificación, valoración, ubicación y acceso de la información y demás características identificas por la Alta dirección permitiendo así la administración eficiente de cada proceso garantizando la disponibilidad, integridad y confidencialidad de dicha información.

Seguridad de la información en el Talento Humano

Todas y todos los servidores públicos del Sistema Estratégico de transporte de Valledupar SIVA SAS, independiente del tipo de vinculación laboral o contractual, o de los procesos al que pertenezca y del nivel de funciones o actividades que desempeñe deben contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. Por ende, se debe contar con un directorio completo y actualizado de los perfiles creados.

La responsabilidad de custodia de cualquier documento o archivo generado dentro de la entidad, usado o producido por algún funcionario y/o contratista que se retira, o cambia de cargo, recae en jefe dependencia o supervisor del contrato; Aclarando que el proceso de cadena de custodia de la información debe hacer parte integral de un procedimiento de terminación de la relación contractual o de cambio de cargo.

Usuarios invitados y servicios de acceso público.

El acceso de usuarios no registrados solo debe estar autorizado por la Alta dirección, de manera de información institucional, igualmente el servicio de internet al que puedan acceder debe estar protegido con una contraseña, contando con una restricción de sitios web no autorizados. Si los usuarios invitados no realizaron el debido proceso de registro, no se permitirá el acceso a cualquier otro tipo de recursos de información, aplicación y/o herramientas TIC.

Seguridad Física y del entorno

Seguridad en los equipos, los servidores o equipos de cómputo que contengan informaciones institucionales deben estar en un ambiente seguro y protegido por lo menos con:

- Controles de acceso y seguridad física.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Además, toda información institucional en formato digital debe ser mantenida en los servidores y/o unidades extraíbles aprobados por Gestión administrativa.

También se debe asegurar que la infraestructura esté cubierta, con mantenimiento y soporte adecuados tanto para el hardware como para el software y las estaciones de trabajo deben ser operadas por funcionarios de la institución el cual deben estar capacitados acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional. Se deben incluir los medios que alojan copias de seguridad el cual deben ser conservados de forma correcta de acuerdo a las políticas y estándares establecidos.

Administración de las comunicaciones y operaciones

Reporte y revisión de incidentes de seguridad, el personal vinculado del Sistema Estratégico de transporte de Valledupar SIVA SAS, debe realizar el reporte de una manera eficiente y con responsabilidad de las presuntas violaciones de seguridad

detectadas y se deben reportar a través de su jefe de dependencia o su supervisor a la Secretaria General y de las TIC o cuando la ocasión lo amerite si es un caso especial y podrá realizarse la directamente por la persona que encuentre el incidente o novedad.

Se debe diseñar, mantener y difundir las normas, procesos y guías para el reporte y revisión de incidentes de seguridad el cual se mantendrá procedimientos escritos para la operación de dichas actividades sin afectar el desarrollo normal de la prestación del servicio y asegurando la confiabilidad de la información.

Protección contra software malicioso y hacking.

Se debe proteger todos los sistemas de información que involucre los controles humanos, físicos técnicos y administrativos para no incurrir en daños, se elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking que pueda afectar la prestación del servicio.

Como control básico, todas las estaciones de trabajo del Sistema Estratégico de transporte de Valledupar SIVA SAS, deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus.

Copias de Seguridad

Toda información que se encuentre contenida en el inventario de activos de información o que sea de interés para un proceso siempre debe estar ser respaldada con copias de seguridad tomadas de acuerdo con los procedimientos documentados y probados por el Sistema Integrado de Gestión El procedimiento debe incluir actividades de almacenamiento, administración y custodia de las copias de seguridad incluyendo lugares seguros y control de registros de dichas copias. Dentro del procedimiento debe quedar claro que se deben efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

Tener en cuenta que la creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios, es decir la responsabilidad de realizar las copias y mantenerlas

actualizadas, recae directamente sobre cada dueño de los activos de la información de la Entidad.

Intercambio de Información con Entidades Externas.

Las peticiones o solicitudes de información por parte de entes externos deben ser aprobadas por la Alta dirección, y ser redireccionados a los responsables del manejo y custodia dicha información. Tener en cuenta que la información solicitada por parte de los entes externos debe ser realizada por un medio valido que permita el registro de la solicitud, donde se pueda identificar el remitente, el asunto y la fecha aclarando que toda información institucional debe ser manejada de acuerdo con la normatividad legal vigente.

Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas operativos previamente instalados del Sistema Estratégico de transporte de Valledupar SIVA SAS, deben ser aprobadas por la Alta dirección, de acuerdo con los procedimientos establecidos para tal fin.

El funcionario encargado en la Gestión de las TIC debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad para su respectiva investigación además debe tener un inventario del software autorizado para su uso institucional.

Control de Claves y Nombres de Usuario

Las claves de administrador de los diferentes sistemas deben ser conservadas por la Gestión administrativa y el funcionario encargado en la Gestión de las TIC y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie. Adicionalmente se debe elaborar, mantener y actualizar el procedimiento para la correcta definición, uso y complejidad de las claves de usuario.

Una vez se termine la relación contractual o laboral del personal con del Sistema Estratégico de transporte de Valledupar SIVA SAS, se debe expedir un certificado de

suspensión y/o cancelación de las cuentas creadas al respectivo usuario, en todos y cada uno de los sistemas de información en los cuales estuviera activo (correo electrónico, sistemas de información automatizados, entre otros); se determinara cualquier será el tiempo prudencial por la posible renovación de la relación contractual o laboral, o una vez transcurrido el tiempo se dará de baja las cuentas si no hay renovación ninguna.

Uso adecuado de Internet

Del Sistema Estratégico Transporte de Valledupar SIVA SAS es consciente de la importancia del servicio de Internet como una herramienta fundamental para el desempeño de labores que proporcionará los recursos necesarios para asegurar su disponibilidad a los servidores públicos y demás partes de interés que así lo requieran.

- El proceso de Gestión de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- El proceso de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- El proceso de TIC debe monitorear continuamente el canal o canales del servicio de Internet.
- El proceso de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

PLAN DE TRABAJO Y CRONOGRAMA DE ACTIVIDADES

Para dar cumplimiento al Plan de Seguridad y Privacidad de la Información, se tiene prevista la ejecución de las actividades según el siguiente cronograma:

Actividad No.	Acción o Actividad	Producto	Responsable	Fecha de inicio	Fecha Fin
1	Actualizar las Políticas de Seguridad de la Información (Si aplica)	Documento Actualizado	Profesional de gestión de TIC	17/02/2026	30/12/2026
2	Gestionar los activos de información en cada dependencia y/o proceso (si aplica)	Informe Administrativo	Profesional de gestión de TIC	17/02/2026	30/12/2026
3	Gestionar los Capacitaciones Seguridad TI	Capacitaciones	Profesional de gestión de TIC	17/02/2026	30/12/2026
4	Socializar la Guía de gestión de incidentes de seguridad de la información	Socialización realizada	Profesional de gestión de TIC	17/02/2026	30/12/2026
5	Elaborar plan de concientización, formación, socialización en seguridad de la información y apropiación del SGSI.	Documento Administrativo	Profesional de gestión de TIC	17/02/2026	30/12/2026
6	Implementar las estrategias y campañas incluidas en el plan de concientización, formación, socialización en seguridad de la información y apropiación del SGSI.	Estrategias y campañas	Profesional de gestión de TIC	17/02/2026	30/12/2026
7	Realizar pruebas de vulnerabilidades y pen test de acuerdo con el alcance y la metodología establecida	Documento Administrativo	Profesional de gestión de TIC	17/02/2026	30/12/2026
8	Elaborar Plan de copias de respaldo de la información para la vigencia 2026	Plan de copias de respaldo de la información	Profesional de gestión de TIC	17/02/2026	30/12/2026
9	Adquisición de Cuentas de Correo Electrónico Institucional	cuentas de correos adquiridas	Profesional de gestión de TIC	17/02/2026	30/12/2026
10	Definir Mantenimiento preventivo y correctivo	Plan de mantenimiento de equipos ejecutado	Profesional de gestión de TIC	17/02/2026	30/12/2026

	periódicos de Hardware y software				
11	Elaborar y/o Actualizar el Inventario de Activos (activos informáticos) de la información	Inventario de activos informáticos actualizados	Profesional de gestión de TIC	17/02/2026	30/12/2026
12	Realizar mantenimiento correctivo y preventivo a la UPS de la red eléctrica regulada de la entidad	Plan de mantenimiento de UPS y redes eléctricas ejecutado	Profesional de gestión de TIC	17/02/2026	30/12/2026
13	Definir un Plan de capacitación, sensibilización y comunicación en seguridad de la información	Plan de capacitación ejecutada	Profesional de gestión de TIC	17/02/2026	30/12/2026
14	Adquirir licencias de antivirus e instalar y hacer seguimiento desde la consola o central	Licencias adquiridas	Profesional de gestión de TIC	17/02/2026	30/12/2026

Fin del documento

CONTROL DE CAMBIOS

VERSION	FECHA	DESCRIPCION DEL CAMBIO
1	30/12/2021	Elaboración del documento
2	27/01/2023	Actualización del documento
3	22/01/2024	Actualización del documento
4	24/01/2025	Actualización del documento
5	30/01/2026	Actualización del documento

ELABORADO POR	REVISADO POR	APROBADO POR
Profesional contratista administrativa	JAIME ANDRÉS GONZÁLEZ MEJÍA GERENCIA	JAIME ANDRÉS GONZÁLEZ MEJÍA GERENCIA