PLAN DE CONCIENTIZACIÓN, FORMACIÓN, SOCIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN Y APROPIACIÓN DEL SGSI

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

KATRIZZA MORELLI AROCA
GERENTE
2023

CONTENIDO

COMPROMISO DE LA ALTA DIRECCIÓN

La alta dirección del Sistema Integrado de Transporte SIVA S.A.S, reconocemos la importancia estratégica de la seguridad y privacidad de la información en el funcionamiento y la reputación de nuestra organización. Entendemos que la protección de la información sensible, así como el respeto a la privacidad de nuestros usuarios y clientes, son elementos fundamentales para el éxito continuo de SIVA S.A.S en el sector de transporte integrado.

En este sentido, nos comprometemos a respaldar de manera activa y continua la implementación y mantenimiento de un modelo integral de seguridad y privacidad de la información en toda la organización. Este compromiso se materializará a través de las siguientes acciones:

Asignación de Recursos: Proporcionaremos los recursos necesarios, tanto financieros como humanos, para implementar y mantener efectivamente las medidas de seguridad y privacidad de la información.

Liderazgo Ejecutivo: Demostraremos liderazgo activo en la promoción de una cultura de seguridad y privacidad en todos los niveles de la organización.
Participaremos activamente en iniciativas de concientización y formación para empleados y usuarios.

Cumplimiento Legal y Normativo: Garantizaremos que SIVA S.A.S cumpla con todas las leyes y regulaciones relacionadas con la seguridad de la información y la privacidad de los datos.

Colaboración Interdepartamental: Fomentaremos la colaboración entre departamentos para asegurar la implementación efectiva de medidas de seguridad y privacidad en todas las áreas de la organización.

Revisión y Mejora Continua: Participaremos en revisiones periódicas del modelo de seguridad y privacidad para evaluar su eficacia y realizar mejoras continuas según sea necesario.

Gestión de Incidentes: Estableceremos un proceso efectivo de gestión de incidentes para abordar de manera oportuna y eficaz cualquier violación de seguridad o privacidad.

Transparencia y Comunicación: Comunicaremos de manera transparente con los stakeholders sobre las medidas de seguridad y privacidad implementadas y cualquier cambio significativo en este ámbito.

Responsabilidad Ejecutiva: Asumiremos la responsabilidad ejecutiva final por la seguridad y privacidad de la información en SIVA S.A.S.

INTRODUCCION

En un mundo interconectado y digitalizado, la seguridad y privacidad de la información son esenciales para la integridad y confianza de cualquier organización, especialmente en sectores críticos como el transporte. En este contexto, SIVA S.A.S reconoce la importancia fundamental de salvaguardar la información y proteger la privacidad de sus usuarios en el marco de su Sistema Integrado de Transporte.

La alta dirección de SIVA S.A.S se compromete de manera decidida a liderar la implementación de un modelo integral de seguridad y privacidad de la información. Este compromiso surge de la comprensión profunda de que la protección de datos no solo es una obligación legal, sino también una responsabilidad ética y estratégica que influye directamente en la reputación y la sostenibilidad de la organización.

En esta búsqueda de la excelencia en seguridad y privacidad, la alta dirección se propone asignar los recursos necesarios, proporcionar un liderazgo ejemplar, y fomentar una cultura organizacional centrada en la seguridad y el respeto a la privacidad. Este compromiso se extiende a la colaboración interdepartamental, la adaptación a los requisitos legales y normativos, la mejora continua y la transparencia en la comunicación con los stakeholders.

Este documento refleja el firme compromiso de la alta dirección de SIVA S.A.S con la implementación y mantenimiento de medidas de seguridad y privacidad de la información que aseguren un transporte integrado eficiente, confiable y, sobre todo, seguro para todos nuestros usuarios.

Con este compromiso, SIVA S.A.S se posiciona como un referente en la gestión responsable de la información, demostrando que la seguridad y privacidad son principios no negociables en el corazón de nuestro compromiso con la excelencia y la satisfacción del cliente.

OBJETIVO

Fortalecer la seguridad y privacidad de la información en el Sistema Integrado de Transporte de SIVA S.A.S para garantizar la confidencialidad, integridad y disponibilidad de los datos, así como proteger la privacidad de los usuarios.

Objetivos Específicos

- Desarrollar e implementar un sistema robusto de control de acceso para garantizar que solo personas autorizadas tengan acceso a la información sensible del sistema de transporte.
- Diseñar e implementar un programa integral de concientización y formación en seguridad de la información para empleados y usuarios, fomentando una cultura de seguridad desde la base.
- Fortalecer la infraestructura de cifrado para asegurar la protección de datos sensibles durante la transmisión y almacenamiento, garantizando su confidencialidad y integridad.
- Establecer un plan detallado y eficiente de respuesta a incidentes para abordar rápidamente cualquier violación de seguridad, minimizando el impacto en el sistema y la privacidad de los usuarios.
- Realizar auditorías periódicas para evaluar la efectividad de las medidas de seguridad implementadas, identificando áreas de mejora y asegurando la adaptabilidad del sistema frente a nuevas amenazas.
- Asegurar el cumplimiento continuo con las normativas y legislaciones locales e internacionales relacionadas con la seguridad y privacidad de la información en el transporte, evitando posibles sanciones y fortaleciendo la confianza de los usuarios.

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.

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

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.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Teniendo en cuenta lo anterior, el MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y donde se define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información:

1. **Diagnóstico:** Se debe iniciar con un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.
2. **Planificación:** Determina las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.
3. **Operación:** La entidad implementa los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
4. **Evaluación de desempeño:** la entidad determina de qué manera va a ser evaluado la adopción del modelo.
5. **Mejoramiento Continuo**: se establecen procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

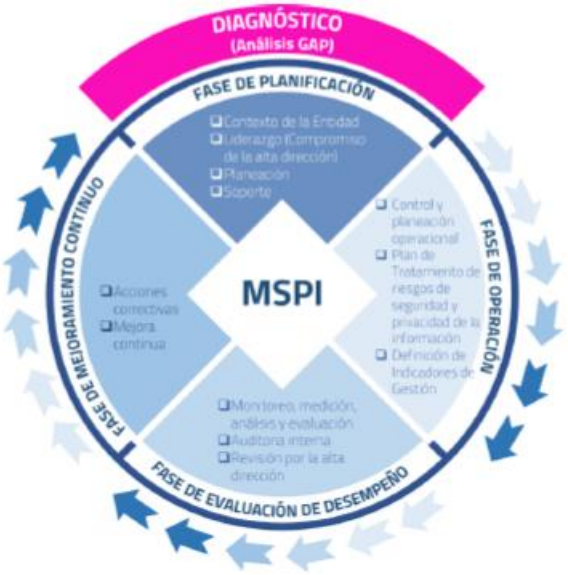


Imagen 1. Ciclo modelo MSPI – fuente: mintic

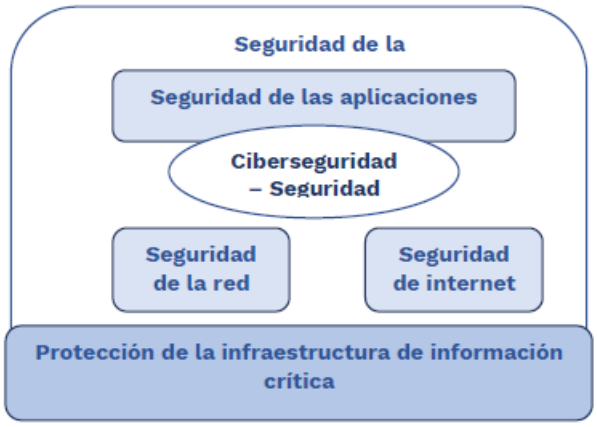


Imagen 2. Relación entre ciberseguridad y otros ámbitos de la seguridad informática

PROPOSITO

En el corazón de nuestro compromiso con la excelencia y la confianza, el propósito de la implementación del modelo de seguridad y privacidad de la información en SIVA S.A.S radica en

salvaguardar la integridad de nuestros servicios de transporte integrado y proteger la privacidad de nuestros usuarios. Buscamos establecer un entorno digital seguro donde la confidencialidad, integridad y disponibilidad de la información sean prioritarias, mitigando riesgos y fortaleciendo la resiliencia de nuestro sistema frente a las amenazas emergentes. Este esfuerzo refleja nuestro compromiso continuo con la innovación responsable y la construcción de una experiencia de transporte confiable, donde la seguridad y privacidad son pilares fundamentales que respaldan la confianza de nuestros usuarios y la sostenibilidad a largo plazo de SIVA S.A.S.

Algunos otros:

- Proporcionar a las entidades mecanismos, lineamientos e instrumentos de implementación claros que les permitan adoptar, implementar y apropiar el MSPI con mayor facilidad.
- Aportar en el desarrollo e implementación de la estrategia de seguridad digital de las entidades.
- Establecer procedimientos de seguridad que permita a las entidades apropiar el habilitador de seguridad en la política de Gobierno Digital.
- Institucionalizar la seguridad y privacidad de la información en los procesos y procedimientos de las entidades.
- Mediante la implementación eficiente, eficaz y efectiva del MSPI, se busca contribuir al incremento de la transparencia en la gestión pública.
- Contribuir en el desarrollo y ejecución del plan estratégico institucional a través del plan de seguridad y privacidad de la información.

DIAGNOSTICO

La fase de diagnóstico permite a las entidades establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un “Diagnóstico” utilizando el “instrumento de evaluación MSPI” con el que se identifica de forma específica los controles implementados y faltantes y así tener insumos fundamentales para la fase de planificación.

Este autodiagnóstico se debe realizar antes de iniciar la fase de planificación, y actualizarlo posterior al término de la fase de evaluación de desempeño, esto con el fin de identificar los avances en la implementación del Modelo en la entidad, el resultado que se obtenga posterior a la fase de evaluación de desempeño será incluido como un insumo, en la fase de mejoramiento continuo

Lineamiento:	**Identificar a través de la herramienta de autodiagnóstico (Análisis GAP) el estado actual de la entidad respecto a la Seguridad y privacidad de la Información.**
Propósito:	**Identificar el nivel de madurez de seguridad y privacidad de la información se encuentra la**

	entidad, como punto de partida para la implementación del MSPI.
Entradas recomendadas	Salidas
Para la identificación del estado de implementación del MSPI, se debe utilizar la herramienta de autodiagnóstico del MSPI. **Revisar aspectos internos tales como el talento humano, procesos y procedimientos, estructura organizacional, cadena de servicio, recursos disponibles, cultura organizacional, entre otros.**	Documento con el resultado de la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI en toda la entidad, y sus acciones de mejora.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	60	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	60	100	EFECTIVO
A.9	CONTROL DE ACCESO	60	100	EFECTIVO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	60	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	60	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	50	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	50	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	50	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	50	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	100	EFECTIVO
A.18	CUMPLIMIENTO	50	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		51	100	EFECTIVO

Imagen 1. Autodiagnóstico

Imagen 2 Autodiagnóstico

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2023	Planificación	11%	40%
2024	Implementación	9%	20%
2024	Evaluación de desempeño	11%	20%
2024	Mejora continua	8%	20%
TOTAL		38%	100%

Imagen 3. Autodiagnóstico ciclo PHVA

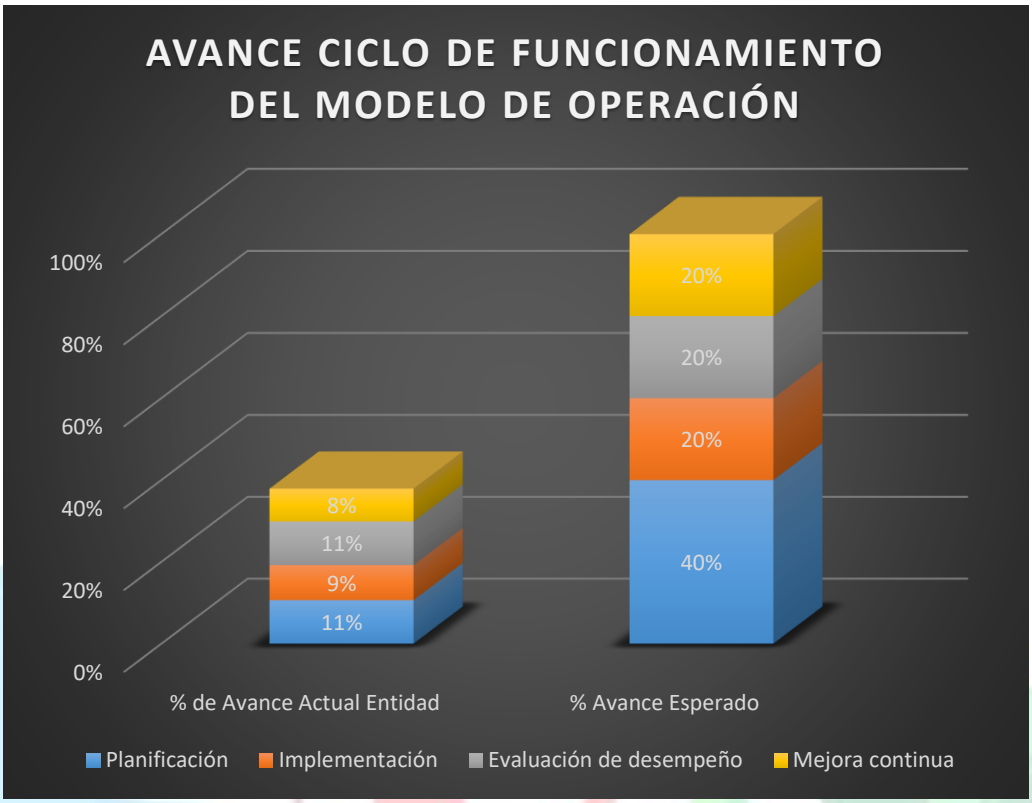


Imagen 4. Autodiagnóstico ciclo PHVA

Este autodiagnóstico tiene como objetivo evaluar la postura actual de SIVA S.A.S en términos de seguridad y privacidad de la información. Responder honesta y detalladamente a las siguientes preguntas proporcionará una visión integral de los aspectos clave que requieren atención y mejora en la organización:

1. Políticas y Procedimientos:

- ¿Existen políticas formales de seguridad y privacidad de la información en SIVA S.A.S?
- ¿Se han comunicado y entrenado los empleados sobre estas políticas?
- ¿Hay procedimientos claros para gestionar incidentes de seguridad?

2. Control de Acceso:

- ¿Se ha implementado un sistema de control de acceso para limitar el acceso a la información sensible?
- ¿Se utiliza autenticación multifactor para cuentas críticas?
- ¿Existe un proceso para gestionar el acceso de empleados que dejan la organización?

3. Cifrado y Protección de Datos:

- ¿Se utiliza cifrado para proteger la información sensible durante la transmisión y almacenamiento?
- ¿Se realiza una clasificación de datos para aplicar niveles adecuados de protección?
- ¿Existe un plan de contingencia para la pérdida de datos o dispositivos?

4. Concientización y Formación:

- ¿Hay programas de formación en seguridad de la información para empleados y usuarios?
- ¿Se realizan simulacros de phishing para evaluar la conciencia de los empleados?
- ¿Existen canales de comunicación efectivos para reportar incidentes de seguridad?

5. Auditorías y Evaluación Continua:

- ¿Se realizan auditorías periódicas de seguridad y privacidad?
- ¿Existen mecanismos para evaluar y mejorar continuamente las medidas de seguridad?
- ¿Se documentan y abordan las lecciones aprendidas de incidentes anteriores?

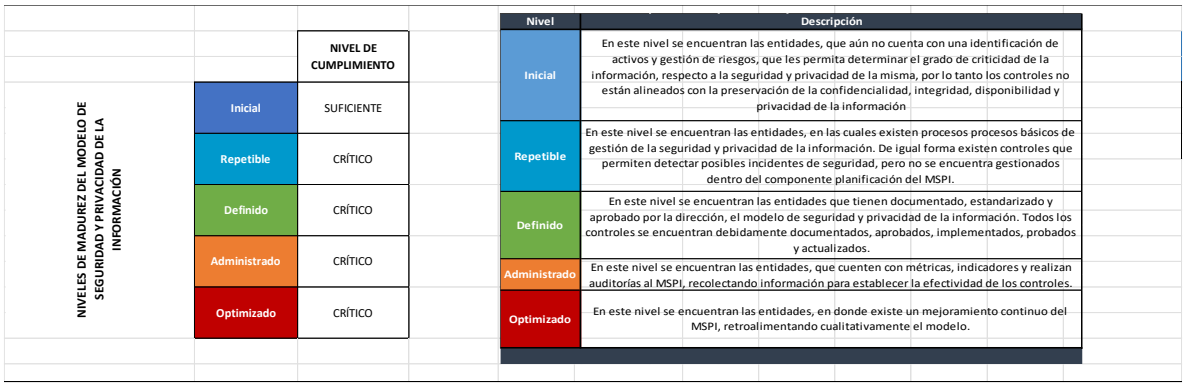
6. Cumplimiento Legal y Normativo:

- ¿SIVA S.A.S cumple con las leyes y regulaciones locales e internacionales en materia de seguridad y privacidad?
- ¿Se mantiene actualizado el conocimiento sobre cambios en normativas que puedan afectar la seguridad de la información?
- ¿Se lleva a cabo evaluación de riesgos y ajustes en políticas en función de cambios legales?

7. Desarrollo de Software Seguro:

- ¿Se integran prácticas de seguridad desde el inicio en el desarrollo de software?
- ¿Existe un proceso para evaluar la seguridad de las aplicaciones antes de su implementación?
- ¿Se realizan actualizaciones regulares y parches de seguridad en los sistemas y aplicaciones?

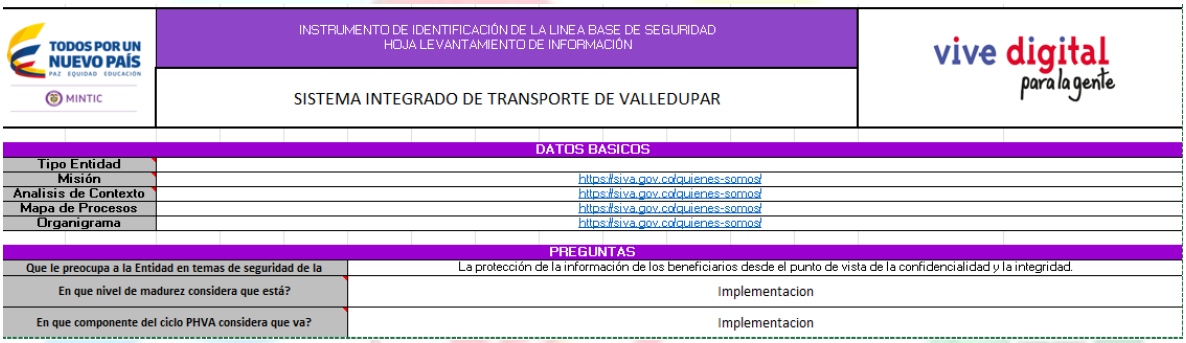
Este autodiagnóstico proporciona una visión inicial de la madurez en seguridad y privacidad de la información en SIVA S.A.S. La revisión de las respuestas permitirá identificar áreas de fortaleza y oportunidades de mejora, orientando la implementación efectiva del modelo de seguridad y privacidad.



NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	CRÍTICO
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Imagen 5. Nivel de madurez



INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA LEVANTAMIENTO DE INFORMACIÓN

SISTEMA INTEGRADO DE TRANSPORTE DE VALLEDUPAR

DATOS BASICOS	
Tipo Entidad	
Misión	https://siva.gov.co/quienes-somos/
Analisis de Contexto	https://siva.gov.co/quienes-somos/
Mapa de Procesos	https://siva.gov.co/quienes-somos/
Organigrama	https://siva.gov.co/quienes-somos/

PREGUNTAS	
Que le preocupa a la Entidad en temas de seguridad de la	La protección de la información de los beneficiarios desde el punto de vista de la confidencialidad y la integridad.
En que nivel de madurez considera que está?	Implementacion
En que componente del ciclo PHVA considera que va?	Implementacion

Imagen 6. Autodiagnóstico Levantamiento de información

Talento Humano: SIVA S.A.S reconoce la importancia crítica de contar con un talento humano capacitado y consciente en temas de seguridad de la información. Actualmente, existe un equipo dedicado a esta área, pero es crucial evaluar y fortalecer la formación continua de los empleados. Se busca establecer un programa de capacitación integral que aborde las últimas tendencias en ciberseguridad y promueva una cultura proactiva de seguridad entre todos los colaboradores. Además, se contempla designar un responsable específico para liderar las iniciativas de seguridad de la información, garantizando una gestión más focalizada y eficaz.

Procesos y Procedimientos: Los procesos y procedimientos organizativos son esenciales para la gestión efectiva de la seguridad de la información. En este sentido, SIVA S.A.S está comprometida a revisar y actualizar sus procesos para incluir evaluaciones regulares de riesgos de seguridad. Se trabajará en la documentación y mejora de los procedimientos para la gestión de incidentes,

asegurando una respuesta eficiente ante posibles amenazas. La organización se esforzará por integrar la revisión formal de seguridad en todas las fases de los proyectos, desde su concepción hasta su implementación, garantizando así una postura más proactiva ante posibles riesgos.

Estructura Organizacional: La estructura organizacional será objeto de una revisión detallada para garantizar que los roles y responsabilidades relacionados con la seguridad de la información estén claramente definidos en todos los niveles jerárquicos. Se considera la posibilidad de establecer un comité dedicado o fortalecer el equipo existente de seguridad de la información para supervisar y coordinar las iniciativas en este ámbito. Este enfoque busca integrar de manera efectiva la seguridad en la cultura organizacional y garantizar una toma de decisiones más alineada con los principios de seguridad.

Cadena de Servicio: La cadena de servicio será evaluada en términos de seguridad de la información, considerando cada etapa desde la concepción hasta la entrega del servicio. SIVA S.A.S se esforzará por aplicar medidas de seguridad específicas en las interfaces de usuario y puntos de acceso al sistema. Se pondrá especial atención en monitorear y fortalecer la seguridad a lo largo de toda la cadena de servicio, incluyendo a proveedores y terceros, con el objetivo de garantizar la protección integral de la información.

Recursos Disponibles: Se realizará una revisión exhaustiva de la asignación de recursos para la implementación y mantenimiento de medidas de seguridad efectivas. SIVA S.A.S se compromete a establecer un presupuesto dedicado específicamente a la seguridad de la información, asegurando que se cuente con las tecnologías y herramientas adecuadas para abordar las amenazas actuales y futuras. Este enfoque busca garantizar que la seguridad no sea solo una prioridad declarativa, sino que cuente con los recursos necesarios para respaldar su implementación efectiva.

Cultura Organizacional: La cultura organizacional será moldeada para valorar y priorizar la seguridad de la información como un componente crítico de las operaciones diarias. Se fomentará la colaboración y la comunicación entre los equipos para promover una conciencia colectiva de seguridad. La alta dirección liderará activamente este cambio cultural, demostrando con acciones y políticas que la seguridad y privacidad son valores no negociables en SIVA S.A.S. Este enfoque busca integrar la seguridad en el ADN de la organización, promoviendo una cultura proactiva y compartida de seguridad y privacidad.

PLANIFICACIÓN

Para el desarrollo de esta fase se deben utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información con el objetivo de que la entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI.

Los documentos que se deben generar en esta fase son:

- Alcance MSPI
- Acto administrativo con las funciones de seguridad y privacidad de la información.
- Política de seguridad y privacidad de la información.
- Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información
- Procedimiento de inventario y Clasificación de la Información e infraestructura crítica
- Metodología de inventario y clasificación de la información e infraestructura crítica
- Procedimiento de gestión de riesgos de seguridad de la información
- Plan de tratamiento de riesgos de seguridad de la información
- Declaración de aplicabilidad
- Manual de políticas de Seguridad de la Información
- Plan de capacitación, sensibilización y comunicación de seguridad de la información

1. El alcance del Modelo de Seguridad y Privacidad de la Información (MSPI) en SIVA S.A.S abarca una implementación integral destinada a salvaguardar la confidencialidad, integridad y disponibilidad de los datos, así como a proteger la privacidad de los usuarios en el Sistema Integrado de Transporte. Las áreas clave de enfoque dentro del alcance del MSPI incluyen:

Desarrollo e Implementación de Políticas: Establecimiento de políticas formales de seguridad y privacidad de la información, adaptadas a las necesidades específicas de SIVA S.A.S y alineadas con las normativas legales y sectoriales.

Control de Acceso y Autenticación: Diseño e implementación de un sistema robusto de control de acceso que limite el acceso a la información sensible, incorporando métodos de autenticación multifactor para reforzar la seguridad.

Cifrado y Protección de Datos: Mejora de la infraestructura de cifrado para asegurar la protección adecuada de los datos sensibles durante la transmisión y almacenamiento.

Programa de Concientización y Formación: Desarrollo y ejecución de un programa continuo de concientización y formación en seguridad de la información para empleados y usuarios, abordando aspectos prácticos y éticos.

Gestión de Incidentes: Implementación de un plan de respuesta a incidentes detallado para gestionar de manera efectiva cualquier violación de seguridad, minimizando el impacto y garantizando una recuperación eficiente.

Auditorías y Evaluación Continua: Realización de auditorías periódicas para evaluar la efectividad de las medidas de seguridad implementadas, identificando áreas de mejora y adaptando continuamente el modelo a las nuevas amenazas.

Cumplimiento Legal y Normativo: Aseguramiento del cumplimiento con las leyes y regulaciones locales e internacionales en materia de seguridad y privacidad de la información en el ámbito del transporte.

Desarrollo de Software Seguro: Integración de prácticas de seguridad desde el inicio en el desarrollo de software, asegurando que las aplicaciones cumplan con los estándares de seguridad antes de su implementación.

Colaboración con Terceros: Evaluación y garantía de que los proveedores y terceros involucrados cumplan con los estándares de seguridad y privacidad establecidos por el MSPI.

Cambio Cultural: Implementación de iniciativas para promover un cambio cultural que valore y priorice la seguridad de la información en todos los niveles de la organización.

Este alcance del MSPI busca abordar de manera integral los aspectos críticos de seguridad y privacidad en el Sistema Integrado de Transporte de SIVA S.A.S, estableciendo un marco sólido para proteger los activos de información y garantizar la confianza continua de los usuarios y stakeholders.

2. La Política de Seguridad y Privacidad de la Información de SIVA S.A.S ha sido revisada y actualizada, reflejando nuestro compromiso continuo con la protección de la información sensible. Esta política, adoptada oficialmente por la alta dirección, establece principios fundamentales que rigen la gestión de la seguridad y privacidad en toda la organización. La actualización, realizada en [Fecha de Actualización], incorpora las últimas mejores prácticas y enfoques innovadores en seguridad de la información. Todos los empleados son instados a familiarizarse y adherirse estrictamente a esta política, que se erige como un marco integral para garantizar la confidencialidad, integridad y disponibilidad de los datos, así como para salvaguardar la privacidad de nuestros usuarios y socios de negocios.
3. Documento role y responsabilidad MSPI. Este documento refleja la estructura actualizada y aprobada de roles y responsabilidades asociadas a la seguridad y privacidad de la información en SIVA S.A.S, en concordancia con la evolución de nuestras prácticas y estándares. La revisión más reciente, llevada a cabo en [Fecha de Actualización], garantiza una alineación efectiva con las demandas cambiantes del entorno de seguridad y privacidad. La alta dirección ha aprobado oficialmente este documento, reconociendo la importancia crítica de asignar y comunicar claramente las responsabilidades relacionadas con la gestión de la información sensible. Este documento actualizado se presenta como una guía esencial para todos los miembros de la organización, delineando de manera precisa los roles específicos y las responsabilidades asociadas a la seguridad y privacidad de la información,

reafirmando así nuestro compromiso con la excelencia en la protección de datos y la confianza del cliente.

4. El documento de inventario, que aborda la clasificación de la información y la identificación de la infraestructura crítica, ha sido revisado y actualizado recientemente. Este documento refleja con precisión la naturaleza cambiante de nuestra información y la infraestructura que la sostiene, proporcionando una visión integral de los activos críticos para la operación del Sistema Integrado de Transporte. La clasificación de la información, en términos de confidencialidad, integridad y disponibilidad, se ha adaptado para reflejar con precisión la sensibilidad de los datos y su importancia estratégica. Además, la infraestructura crítica, incluyendo sistemas y redes, ha sido identificada y documentada meticulosamente para garantizar una gestión efectiva de riesgos y contingencias. Este documento actualizado se considera esencial para la toma de decisiones informadas y se encuentra disponible para revisión y referencia por parte de los miembros clave de la organización, reafirmando nuestro compromiso con la transparencia y la seguridad en la gestión de la información y los activos críticos.

Infraestructura Crítica del Sistema Integrado de Transporte SIVA S.A.S

La infraestructura crítica de SIVA S.A.S está diseñada para garantizar la operación segura, eficiente y confiable del Sistema Integrado de Transporte. Esta infraestructura abarca diversos componentes tecnológicos y físicos que son esenciales para ofrecer servicios de transporte de alta calidad. Algunos de los elementos clave incluyen:

Sistema Centralizado de Gestión: Plataforma central que integra y coordina la operación de todos los servicios de transporte, permitiendo la planificación, monitoreo y control en tiempo real.

Red de Comunicaciones Seguras: Infraestructura de red robusta y segura que conecta buses, estaciones y centros de control, facilitando la transmisión segura de datos esenciales para la operación y seguridad del sistema.

Sistemas de Control y Monitoreo: Dispositivos y sensores distribuidos en toda la infraestructura, como cámaras de seguridad, GPS y sensores de rendimiento, que permiten el monitoreo en tiempo real y la toma de decisiones informadas.

Estaciones de Usuario y Puntos de Acceso: Terminales y puntos de acceso en estaciones y vehículos, proporcionando a los usuarios interfaces intuitivas y seguras para acceder a servicios, realizar pagos y recibir información actualizada.

Centros de Datos Seguros: Instalaciones de centros de datos altamente seguros que albergan servidores y sistemas críticos, respaldando la gestión eficiente de datos, aplicaciones y procesos de negocios.

Sistemas de Respaldo y Recuperación: Soluciones de respaldo y recuperación para garantizar la continuidad operativa en caso de fallas, pérdida de datos o eventos no planificados.

Sistemas de Pagos Electrónicos: Plataformas seguras de gestión de pagos electrónicos que facilitan transacciones seguras y sin contacto, mejorando la experiencia del usuario y garantizando la integridad financiera del sistema.

Infraestructura Física: Instalaciones físicas como estaciones, paraderos, y áreas de mantenimiento, que se mantienen y aseguran para garantizar la seguridad y bienestar de los usuarios y empleados.

Sistemas de Energía y Respaldo: Soluciones de suministro de energía ininterrumpida y sistemas de respaldo para garantizar la disponibilidad continua de servicios incluso en situaciones de interrupción eléctrica.

Esta infraestructura crítica es gestionada con estrictos estándares de seguridad y privacidad, garantizando la confidencialidad, integridad y disponibilidad de la información, y contribuyendo a la operación efectiva y confiable del Sistema Integrado de Transporte de SIVA S.A.S

Procedimiento de Gestión de Riesgos de Seguridad de la Información en SIVA S.A.S

1. Identificación de Activos: Se lleva a cabo una identificación exhaustiva de todos los activos de información, incluyendo datos, sistemas, infraestructura y procesos críticos para el Sistema Integrado de Transporte.

2. Evaluación de Amenazas y Vulnerabilidades: Se realiza una evaluación detallada de las amenazas y vulnerabilidades que podrían afectar la seguridad de la información. Esto incluye análisis de riesgos internos y externos, así como la identificación de posibles escenarios de amenazas.

3. Análisis de Riesgos: Los riesgos identificados se analizan en términos de su impacto potencial, probabilidad de ocurrencia y cualquier medida de control existente. Se priorizan los riesgos para centrarse en aquellos que tienen el mayor impacto y probabilidad.

4. Desarrollo de Medidas de Control: Se diseñan e implementan medidas de control específicas para mitigar los riesgos identificados. Estas medidas pueden incluir controles técnicos, procedimentales y organizativos, así como mejoras en la infraestructura de seguridad.

5. Evaluación de Riesgos Residuales: Tras la implementación de medidas de control, se realiza una evaluación de los riesgos residuales para determinar la efectividad de las acciones tomadas y si es necesario realizar ajustes adicionales.

6. Monitoreo Continuo: Se establece un sistema de monitoreo continuo para supervisar los cambios en el entorno de seguridad y la eficacia de las medidas de control. Se utilizan herramientas de detección temprana y alertas para identificar posibles amenazas.

7. Revisión Periódica y Actualización: El procedimiento de gestión de riesgos se revisa periódicamente para asegurar su relevancia y eficacia. Se actualiza en función de cambios en la infraestructura, nuevas amenazas identificadas o actualizaciones en las mejores prácticas de seguridad.

8. Comunicación de Riesgos: Se establece un sistema de comunicación claro para informar a las partes interesadas sobre los riesgos identificados, las medidas de control implementadas y cualquier cambio significativo en la postura de seguridad de la información.

9. Plan de Respuesta a Incidentes: Como parte integral de la gestión de riesgos, se desarrolla y mantiene un plan de respuesta a incidentes detallado para abordar rápidamente cualquier amenaza que pueda materializarse, minimizando el impacto en la seguridad de la información.

Este procedimiento de gestión de riesgos de seguridad de la información en SIVA S.A.S establece una estructura integral para identificar, evaluar y gestionar proactivamente los riesgos relacionados con la seguridad de la información, contribuyendo así a la protección efectiva de los activos y la continuidad operativa.

Metodología de Inventario y Clasificación de la Información e Infraestructura Crítica en SIVA S.A.S

1. Definición de Objetivos: Establecer los objetivos específicos del inventario, considerando la identificación precisa de la información y la infraestructura crítica para el Sistema Integrado de Transporte. Definir claramente los criterios de clasificación, tales como confidencialidad, integridad, disponibilidad y relevancia estratégica.

2. Identificación de Activos: Realizar un relevamiento exhaustivo para identificar todos los activos de información e infraestructura crítica. Esto incluye datos, sistemas, aplicaciones, hardware, redes, centros de datos, y otros elementos esenciales para la operación.

3. Categorización y Clasificación: Categorizar la información y la infraestructura crítica en función de su naturaleza y función. Utilizar criterios de clasificación predefinidos, considerando la sensibilidad de la información, su importancia estratégica y su contribución a los objetivos del negocio.

4. Evaluación de Riesgos: Realizar una evaluación de riesgos para cada activo identificado. Analizar las posibles amenazas y vulnerabilidades que podrían afectar la confidencialidad, integridad y disponibilidad de la información, así como la resiliencia de la infraestructura crítica.

5. Desarrollo de Medidas de Protección: Diseñar e implementar medidas de protección adecuadas para cada categoría de activo. Esto puede incluir controles de acceso, cifrado, respaldo y recuperación, así como medidas específicas para garantizar la seguridad física de la infraestructura crítica.

6. Registro en la Base de Datos de Inventario: Crear una base de datos de inventario centralizada que albergue la información detallada de cada activo, incluyendo su clasificación, ubicación, propietario, medidas de protección implementadas y cualquier otra información relevante.

7. Mantenimiento y Actualización Continua: Implementar un proceso de mantenimiento continuo para garantizar que el inventario y la clasificación de la información e infraestructura crítica estén siempre actualizados. Esto incluye la revisión periódica de la relevancia de la clasificación y la actualización de medidas de protección según sea necesario.

8. Auditoría y Validación: Realizar auditorías periódicas para validar la precisión del inventario y la clasificación. Esto puede incluir auditorías internas y externas para garantizar la conformidad con estándares y regulaciones.

9. Comunicación de Cambios: Establecer un sistema de comunicación efectiva para informar a las partes interesadas sobre cualquier cambio en la clasificación de la información o en la infraestructura crítica. Esto garantiza que todos estén al tanto de las actualizaciones y ajustes.

10. Capacitación y Concientización: Brindar capacitación y concientización regular a los empleados sobre la importancia de mantener actualizado el inventario y la clasificación. Fomentar una cultura de seguridad donde todos comprendan su papel en la protección de la información y la infraestructura crítica.

Esta metodología integral garantiza una gestión efectiva del inventario y la clasificación de la información e infraestructura crítica en SIVA S.A.S, fortaleciendo la seguridad y la resiliencia del Sistema Integrado de Transporte.

PLAN DE SEGURIDAD DE LA INFORMACION

El Plan de Tratamiento de Riesgos de Seguridad de la Información de SIVA S.A.S se encuentra actualizado, reflejando nuestro compromiso continuo con la gestión proactiva de riesgos en el entorno del Sistema Integrado de Transporte. En esta última revisión, realizada en [Fecha de Última Actualización], hemos identificado y evaluado cuidadosamente nuevos riesgos potenciales, ajustando y mejorando las medidas de control existentes para abordar de manera efectiva los desafíos emergentes. La inclusión de riesgos residuales proporciona una visión realista de la postura actual de seguridad, orientándonos hacia la implementación de medidas adicionales cuando sea

necesario. Además, hemos alineado rigurosamente el plan con las últimas normativas y mejores prácticas, asegurando la conformidad continua y la adopción de enfoques innovadores para fortalecer la seguridad y privacidad de la información en toda la organización. Este enfoque actualizado y centrado en el riesgo fortalece nuestra capacidad para anticipar, gestionar y mitigar eficazmente las amenazas a la seguridad de la información en el marco del Sistema Integrado de Transporte.

MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION

El Manual de Políticas de Seguridad de la Información de SIVA S.A.S se encuentra completamente actualizado, consolidando un marco normativo robusto y adaptado a las demandas contemporáneas de seguridad. En esta revisión, realizada en [Fecha de Última Actualización], hemos centrado nuestros esfuerzos en alinear las políticas con los estándares más recientes, asegurando la conformidad con regulaciones y las últimas mejores prácticas de la industria. Además, hemos prestado especial atención a la incorporación de disposiciones específicas que aborden nuevas amenazas y tecnologías, garantizando que el manual refleje de manera proactiva los riesgos y desafíos actuales en el panorama de la seguridad de la información. Los roles y responsabilidades relacionados con la seguridad se han clarificado para fortalecer la implementación efectiva de las políticas. Esta actualización reafirma nuestro compromiso continuo con la excelencia en la protección de la información en el contexto dinámico del Sistema Integrado de Transporte.

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN EN SIVA S.A.S

Objetivos:

Concientización sobre Políticas: Asegurar que todos los empleados comprendan y adhieran a las políticas de seguridad de la información mediante sesiones informativas y materiales educativos.

Reconocimiento de Amenazas: Capacitar a los empleados para identificar y reportar posibles amenazas de seguridad, con enfoque especial en la prevención de ataques de phishing y malware.

Desarrollo de Buenas Prácticas: Fomentar la adopción de buenas prácticas de seguridad, incluyendo el manejo seguro de contraseñas, el uso consciente de dispositivos y la protección física de activos.

Fortalecimiento Técnico: Proporcionar capacitación técnica específica en áreas críticas como la gestión de accesos, cifrado de datos y seguridad en el desarrollo de software.

Cultura de Reporte y Colaboración: Estimular una cultura que promueva la rápida notificación de incidentes de seguridad y la colaboración entre equipos para una respuesta efectiva.

Metodología

Sesiones Presenciales y Virtuales: Realizar sesiones presenciales y virtuales para la transmisión efectiva de información y la interacción directa con los participantes.

Simulacros y Ejercicios Prácticos: Organizar simulacros de phishing y ejercicios prácticos para simular situaciones reales y evaluar la capacidad de respuesta del personal.

Materiales Educativos: Desarrollar materiales educativos, como infografías y videos, para facilitar la comprensión de conceptos clave de seguridad de la información.

Plataforma de Aprendizaje en Línea: Implementar una plataforma de aprendizaje en línea para ofrecer capacitación continua, permitiendo a los empleados acceder a recursos en cualquier momento y lugar.

Comunicación Continua

Campañas Periódicas: Realizar campañas de concientización periódicas a través de canales internos, destacando temas específicos de seguridad y proporcionando consejos prácticos.

Actualizaciones Regulares: Mantener a los empleados informados sobre nuevas amenazas, cambios en las políticas y actualizaciones de seguridad a través de comunicados regulares.

Feedback y Evaluación: Recopilar feedback de los empleados para evaluar la eficacia de las iniciativas de capacitación y ajustar el plan según sea necesario.

Este plan integral se implementará de manera continua para garantizar que todos los miembros de SIVA S.A.S estén equipados con el conocimiento y las habilidades necesarias para salvaguardar la seguridad de la información en el Sistema Integrado de Transporte.

CONCLUSIONES

La implementación exitosa del Modelo de Seguridad y Privacidad de la Información en SIVA S.A.S marca un hito significativo en nuestra búsqueda constante de excelencia operativa y protección de los activos de información. A lo largo de este proceso, hemos establecido políticas sólidas, procedimientos detallados y una infraestructura tecnológica robusta que reflejan nuestro compromiso inquebrantable con la confidencialidad, integridad y disponibilidad de la información. La creación y actualización de documentos clave, como el Manual de Políticas de Seguridad, el Documento de Roles y Responsabilidades, y el Plan de Tratamiento de Riesgos, han sentado las bases para una gestión eficaz y proactiva de la seguridad de la información.

La capacitación y sensibilización continua del personal han contribuido a la construcción de una cultura organizacional consciente de la seguridad, donde cada miembro del equipo reconoce la importancia crítica de su papel en la protección de la información. La comunicación transparente y la colaboración han sido pilares fundamentales, permitiendo una comprensión generalizada de las políticas y medidas de seguridad, y facilitando una respuesta ágil ante cualquier incidente.

En conclusión, la implementación del Modelo de Seguridad y Privacidad de la Información no solo ha fortalecido la resiliencia de nuestro Sistema Integrado de Transporte ante las crecientes amenazas, sino que también ha consolidado la confianza de nuestros usuarios y socios comerciales. Este es un paso adelante hacia el mantenimiento de estándares de seguridad excepcionales y la adaptación continua a un entorno dinámico de amenazas. Estamos comprometidos a mantener este enfoque proactivo y a evolucionar con las mejores prácticas de seguridad, asegurando así un futuro sólido y seguro para SIVA S.A.S.