PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TRANSCARIBE S.A.

ENERO DE 2024

CARTAGENA DE INDIAS

1. HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	31/12/2018	Versión uno del documento
1.0.1	25/01/2022	Versión dos del documento
1.0.2	25/01/2023	Versión tres del documento
1.0.3	19/01/2024	Versión cuatro del documento

2. OBJETIVO

Establecer las actividades del Plan de Seguridad y Privacidad de la Información para la implementación, gestión, verificación y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI de TRANSCARIBE S.A.

3. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información se aplica a las diferentes dependencias que conforma la entidad, estas son: (Gerencia, Secretaria General, Planeación e Infraestructura, Operaciones, Administrativa y Financiera, Asesora Jurídica y Control Interno), en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información – SGSI.

4. TERMINOS Y DEFINICIONES

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE TRANSCARIBE

La Secretaria General, se compromete a administrar los riesgos de seguridad de la información para generar, implementar y monitorear los controles que permitan mantener la confidencialidad, integridad y disponibilidad de sus activos de información en cumplimiento de los requisitos aplicables. De igual manera, promoverá la cultura de la seguridad informática para mitigar y administrar incidentes que no contribuyan a la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI.

6. OBJETIVOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

a) Supervisar y validar los eventos de seguridad de la información de todo lo que ocurra en la Red de área local y demás servicios tecnológicos de TRANSCARIBE S.A.
b) Mantener y fortalecer la seguridad y disponibilidad de la información en las diferentes plataformas tecnológicas de la entidad acorde con las políticas de seguridad implementadas
c) Velar por el cumplimiento de los requisitos legales aplicables a la naturaleza de la nuestra Entidad en materia de Seguridad de la Información.
d) Promover una cultura de seguridad de la información en los servidores públicos (empleados oficiales, funcionarios, contratistas etc.)
e) Fortalecer el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

7. ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN - SGSI

EL SGSI es aplicable a los todos los sistemas de información, equipo de cómputo, y servidores activos en todos los procesos del TRANSCARIBE S.A, verificándolo y aplicándolo a las diferentes dependencias en el entendimiento de comprender las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con las normas que rigen las políticas de seguridad de la información y que serán validadas por el Comité Institucional de Gestión y Desempeño de Transcaribe S.A.

8. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité Institucional de Gestión y Desempeño de Transcaribe S.A., se creará como una instancia orientadora del Modelo Integrado de Planeación y Gestión, a través del cual se discutirán todos los temas referentes a las políticas de gestión y desempeño institucional y demás componentes del modelo y el cual tiene también como propósito impulsar y hacer seguimiento y/o verificación de la implementación del Sistema de Gestión de Seguridad de la Información SGSI de TRANSCARIBE S.A.

Esté estaría conformado por:

- El Gerente General.
- La Secretaria General.
- El Director de Planeación e Infraestructura, quien ejercerá la secretaría técnica.
- Jefe de la Oficina Asesora Jurídica.
- Director Administrativo y Financiero.
- Director de Operaciones.

Invitados:

- El Jefe de la Oficina de Control Interno.
- Designado del Equipo de Respuesta a Incidentes de Seguridad Informática de TRANSCARIBE S.A.
- Designado del Coordinador del Grupo de Gestión Documental electrónica de TRANSCARIBE S.A.

Las funciones del Comité de Seguridad de la Información son:

- Impulsar la implementación del Sistema de Gestión de Seguridad de la información SGSI de TRANSCARIBE S.A.
- Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SGSI de TRANSCARIBE S.A.
- Supervisar la integración del Sistema de Gestión de Seguridad de la Información - SGSI con el Sistema de Calidad.
- Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información de TRANSCARIBE S.A.
- Adoptar las medidas y acciones a que haya lugar, de conformidad con los resultados de los diagnósticos de la seguridad de la información determinados por El Comité Institucional de Gestión y Desempeño de Transcaribe S.A. y cuyo fin es tomar y establecer las medidas necesarias para corregir lo identificado.

- Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual que puedan generar pérdidas patrimoniales o afectar los recursos de Información de la entidad.
- Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información.
- Revisar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.
- Recomendar la investigación de los incidentes de seguridad de la información ante las instancias necesarias cuando haya lugar a ello.
- Evaluar los planes de acción para mitigar y/o eliminar riesgos en seguridad de la información.
- Alinear sus acciones y decisiones a la normatividad vigente en materia de tecnologías y seguridad de la información.
- Las demás funciones inherentes a la naturaleza de este Comité.

9. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A partir del desarrollo e implementación del Sistema de Gestión de Seguridad de la Información – SGSI de TRANSCARIBE S.A., el cual hace parte del Sistema de calidad de la entidad. Se definieran a futuro las actividades para la vigencia 2023 con las cuales se establece los procesos que se deberán surtir para implementar EL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, permitiendo así la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI.

10. POLÍTICAS QUE AMPARAR LA ESTRUCTURA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

POL - 01 ACCESO A LA INFORMACION

Todos los funcionarios que laboran para el SISTEMA INTEGRADO DE TRANSPORTE MASIVO DE CARTAGENA DE INDIAS TRANSCARIBE S.A. deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la entidad, la Coordinación u Oficina responsable de generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación del jefe inmediato.

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Entidad la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Entidad.

El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

PO-02 ADMINISTRACION DE CAMBIOS

Todo cambio a un componente de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.
Todo cambio que afecte la plataforma tecnológica debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración del componente tecnológico, Jefe de la dependencia o Coordinador del Área o a quienes estos formalmente deleguen.

Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona o área.

Para la administración de cambios se efectuará el procedimiento correspondiente definido por TRANSCARIBE S.A., de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

PO-03 ADMINISTRACION DE LA SEGURIDAD

La función de administración de la seguridad será realizada por los Ingenieros de TI y por los administradores de la seguridad informática para cada sistema aplicativo.

Los funcionarios de la sub área de Sistemas son los responsables de velar por la implantación de las medidas relativas a esta. Igualmente, son responsables de desarrollar las tareas necesarias para el mantenimiento de estas medidas.

La Coordinación de Sistemas se encargará de la definición y actualización de las políticas, normas, procedimientos y estándares relacionados con la seguridad informática, igualmente velará por la implantación y cumplimiento de las mismas.

Con base en análisis de riesgos el área Sistemas participará en la planeación de los controles requeridos en la plataforma tecnológica.

Para realizar la función de administración de la seguridad los responsables se apoyarán en herramientas tecnológicas que permitan una adecuada administración, monitoreo y control de los recursos informáticos.

PO-04 ALMACENAMIENTO Y RESPALDO DE LA INFORMACION

La información que es soportada por la infraestructura de tecnología informática del SISTEMA INTEGRADO DE TRANSPORTE MASIVO DE CARTAGENA DE INDIAS TRANSCARIBE S.A. es almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

Existe una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.

El almacenamiento de la información deberá realizarse interna y/o externamente a la Entidad, esto de acuerdo con la importancia de la información para la operación de TRANSCARIBE S.A.

El área dueña de la información en conjunto con la Coordinación de Sistemas definirá la estrategia a seguir para el respaldo de la información.

POL – 05 COMUNICACIONES ELECTRONICAS

Las comunicaciones electrónicas dentro TRANSCARIBE S.A. y hacia el exterior, deben establecerse de acuerdo con las normas de seguridad informática definidas y con los mecanismos que aseguren tanto la autenticidad de quienes realizan la conexión, como la confidencialidad, integridad y disponibilidad de la misma.

Las comunicaciones electrónicas deben tener la característica de cordialidad y respeto, siguiendo los conductos regulares de ética y manuales de convivencia de la entidad, respetando el fuero y ámbito de decisión de las diferentes instancias.

Las comunicaciones electrónicas tendrán la misma validez que las comunicaciones realizadas en forma impresa.

Existen parámetros de seguridad a nivel de los diversos componentes tecnológicos involucrados en el flujo de comunicaciones electrónicas.

POL – 06 CONFIDENCIALIDAD DE LA INFORMACION

Toda la información del SISTEMA INTEGRADO DE TRANSPORTE MASIVO DE CARTAGENA DE INDIAS TRANSCARIBE S.A. es de propiedad y uso del área que la genera. Es potestad y obligación de dicha área clasificar la información dentro de los criterios que la entidad establezca en sus normas de seguridad.

Para la clasificación de la información se deberá tener en cuenta el grado de confidencialidad requerido en su manejo, entendiéndose por confidencial aquella información cuyo conocimiento por parte de usuarios no autorizado implique riesgos para la entidad.

El carácter de confidencialidad de la información, es una cualidad requerida para que los procesos se den en un ambiente de control adecuado que garantice una correcta segregación de funciones. En este sentido la confidencialidad no debe asimilarse a la no disponibilidad de la información. La entidad deberá poner a disposición la información en el evento que sea requerida por personal interno o externo a la misma, cuya solicitud atienda al proceso formal de requisición de la información por los diferentes entes de control que supervisan la operación.

POL – 07 CONTRATOS, ALIANZAS O CONVENIOS CON TERCEROS

Cualquier contrato, alianza o convenio con terceros no debe vulnerar en forma alguna el contenido de las políticas de seguridad informática definidas, ni las normas emitidas para su implantación.

Toda conexión requerida por entidades externas, socios, clientes y proveedores, para compartir información con la Transcaribe S.A. deberá ser analizada y aprobada por el área responsable de la información, profesional especializado de la secretaria general - Sistemas y los Ingenieros de soporte TI.

Esta conexión debe establecerse de acuerdo con el estándar existente en la entidad involucrando los controles que aseguren tanto la identidad de quien realiza la conexión como la confidencialidad, integridad, oportunidad y disponibilidad de la misma.

Las actividades de instalación y/o conexión deben ser coordinadas previamente por el área responsable de la información en conjunto con la Coordinación de Sistemas para garantizar la asistencia técnica informática necesaria.

POL – 08 NORMAS Y PROCEDIMIENTOS OPERATIVOS

El área que genera la información necesaria para el desarrollo de sus procesos, es responsable de definir dentro de los aplicativos que soporten su operación, el flujo del proceso, la administración de la información generada, los parámetros de

administración de seguridad, el esquema de accesos a la información por parte de los usuarios y los controles que deben existir en el proceso y flujo de la información.

En la definición de las normas y procedimientos operativos participa la directiva de la entidad. Para la documentación se deberán atender los estándares definidos en la entidad.

La Coordinación de Sistemas y su grupo de colaboradores garantizaran la eficiencia de los controles implantados en los procesos operativos de la entidad con el objeto de garantizar la integridad, confidencialidad y veracidad de la información manejada.

POL – 09 PROCESAMIENTO DE LA INFORMACION

El procesamiento de la información que se realice sobre cualquier componente de la plataforma tecnológica, propiedad del SISTEMA INTEGRADO DE TRANSPORTE MASIVO DE CARTAGENA DE INDIAS TRANSCARIBE S.A. o de terceros, debe cumplir con todas las políticas, normas y procedimientos de seguridad y contingencia que garanticen los principios de confidencialidad, integridad y disponibilidad de la información.

Para atender eventos que pongan en riesgo el adecuado procesamiento de la información existen procedimientos que en forma rápida permiten recuperar la operación normal de la información dentro de los niveles de control estipulados por la entidad.

Para el procesamiento adecuado de la información se cuenta con adecuadas condiciones de seguridad física y ambiental.

POL – 10 PROCESAMIENTO DE LA INFORMACION

La información que es soportada por la infraestructura de tecnología informática de Transcaribe S.A. Pertenece a la entidad a menos que en una relación contractual se establezca lo contrario. Sin embargo, la facultad de otorgar acceso a la información es del responsable del área que genera esa información, a nivel de Jefe de área.

La propiedad de la información no va en contra del carácter público de la misma, esto significa, que la información generada por la entidad deberá estar disponible en el evento que sea requerida por personal interno o externo a la esta, y cuya solicitud atienda al proceso formal de requisición de la información por parte de los organismos de control.

Para efectos de control del flujo de la información de los procesos de la entidad, se asignarán responsables de la información, quienes deben asegurar y otorgar acceso a la información que genere su área, con el fin de lograr un adecuado ambiente de control y un buen nivel de segregación de funciones.

En caso de divulgación no autorizada de la información de propiedad de la entidad se generarán sanciones a las personas que lo realicen.

POL – 11 RESPONSABILIDAD DE LOS FUNCIONARIOS EN EL CUMPLIMIENTO DE LA NORMATIVIDAD REFERENTE A SEGURIDAD INFORMÁTICA

Todas las personas que laboran para TRANSCARIBE S.A., son responsables por el cumplimiento de las políticas, normas, procedimientos y estándares vigentes con respecto a la seguridad informática.

Todos los usuarios de la información son responsables del manejo adecuado de la información y mediante el cumplimiento de las políticas, procedimientos y estándares de los procesos operativos y de seguridad informática, se comprometen a respetar su carácter de confidencialidad e integridad.

Los responsables de la información se encargarán de definir los accesos a la información y aprobar cambios a los aplicativos en concordancia con la normatividad de seguridad informática vigente.

Existen roles definidos en el esquema de seguridad informática adoptado por la TRANSCARIBE S.A, que garantizan una adecuada segregación de funciones para la realización de las actividades de administración y operación de la seguridad informática**.**

POL – 12 SEGURIDAD FISICA

Todo recurso informático, ya sea propio o de terceros, que procese información de TRANSCARIBE S.A. debe cumplir con todas las normas de seguridad física que se

emitan con el fin de restringir el acceso a personas no autorizadas y asegurar la protección de los recursos informáticos.

El personal ubicado en áreas de procesamiento y/o almacenamiento de información debe cumplir con normas básicas de higiene y cuidado de los componentes tecnológicos ubicados en las instalaciones.

Cualquier cambio a las instalaciones donde se realice procesamiento o almacenamiento de la información deberá ser analizado por el profesional especializado de la secretaria general con el objeto de validar el posible impacto en la seguridad de la información de la entidad.

Existe documentación del diseño de las instalaciones donde se ubican los componentes tecnológicos de TRANSCARIBE S.A con el fin de poder realizar una adecuada planeación y toma de decisiones en la implementación de controles para la seguridad de la información.

POL – 13 SOFTWARE UTILIZADO

Todo software que utilice TRANSCARIBE S.A será adquirido de acuerdo con las leyes vigentes y siguiendo las normas y procedimientos específicos de la entidad.

Todo el software de manejo de datos que utilice TRANSCARIBE S.A dentro de su infraestructura informática, cuenta con las técnicas más avanzadas de la industria para garantizar la integridad de los datos.

Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios de las implicaciones que tiene el instalar software ilegal en los computadores de la TRANSCARIBE S.A.

Existe un inventario de las licencias de software de la entidad que permite su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

Existe una reglamentación de uso para los productos de software instalado en los computadores de la entidad.

Todo software adquirido por la TRANSCARIBE S.A debe contar con la aprobación previa del profesional especializado de la secretaria general.

Todo proceso de adquisición que incluya software debe ser analizado y aprobado previamente por el área responsable de la información y el profesional especializado de la secretaria general.

El software instalado en los componentes tecnológicos de TRANSCARIBE S.A. que no esté respaldado por un concepto previo del profesional especializado de la secretaria general no se le brindará ningún tipo de soporte.

11. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

12. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.