TABLA DE CONTENIDO

LISTA DE FIGURAS

PRESENTACIÓN

La implementación del sistema de gestión de seguridad de la información-SGSI, busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de la Superintendencia de Transporte, garantizando su buen uso y la privacidad de los datos, a través del Modelo de Seguridad y Privacidad de la Información – MSPI.

En ese sentido la Superintendencia de Transporte considera indispensable actualizar la Política de Seguridad y Privacidad de la Información donde se establecen los lineamientos, reglas y condiciones generales que todos los actores internos y externos deben cumplir para garantizar la seguridad y privacidad de los activos de información.

Por lo antes expuesto la Oficina de Tecnologías de la Información y las Comunicaciones, en este documento define los lineamientos y procedimientos de la política de Seguridad y privacidad de la Información, y liderará su implementación, capacitación y ejecución, a fin de mitigar las vulnerabilidades de la información durante el ciclo de vida del dato, a través de herramientas y mecanismos que permitan garantizar la confidencialidad, integridad, confiabilidad y disponibilidad de los datos e información, a fin de que la entidad, los ciudadanos y demás partes interesadas cuenten con información relevante, accesible, precisa, oportuna y comparable.

Este documento de Política se estructura teniendo en cuenta la guía técnica colombiana ISO 27001:2013 y las recomendaciones y buenas prácticas del estándar ISO 27002:2013, así mismo se consideran los lineamientos y recomendaciones efectuadas por el Ministerio de Telecomunicaciones – MINTIC desde el Modelo de Seguridad y Privacidad de la Información - MSPI. La política de seguridad y privacidad de la Información de la Superintendencia de Transporte está estructurada en 4 capítulos, en el primero se realiza una Introducción, en el segundo capítulo se describe el Contexto de la entidad, en el tercero se detallan los lineamientos, procedimientos, excepciones y sanciones definidos por esta Política de seguridad y privacidad de la información.

1 CONTEXTO

1.1 COMPORTAMIENTO DEL CIBERCRIMEN

El Informe Global de Riesgos 2019 realizado por Foro Económico Mundial, estableció que la tecnología sigue desempeñando una función fundamental en la configuración del panorama global de riesgos, en este informe se evidenció que en el 2018 se produjeron nuevas filtraciones masivas de datos, que revelaron nuevas debilidades de hardware y la investigación señaló los usos potenciales de la inteligencia artificial para diseñar ciberataques más potentes. Este mismo informe, demostró que los ciberataques plantean riesgos para las infraestructuras críticas, lo que llevó a los países a reforzar el control de las asociaciones transfronterizas por motivos de seguridad nacional.

Las preocupaciones sobre el fraude de datos y los ataques cibernéticos volvieron a ser prominentes en la Encuesta de Percepción de Riesgos Globales - GRPS, que también puso de relieve otras vulnerabilidades tecnológicas: alrededor de dos tercios de los encuestados esperan que los riesgos asociados con las noticias falsas y la suplantación de identidad aumenten en 2019, mientras que tres quintas partes dijeron lo mismo sobre la pérdida de la privacidad de las sociedades y los gobiernos. Según el informe global del riesgo 2019, los ciberataques se ubican dentro de los diez principales riesgos globales con mayor grado de probabilidad de ocurrencia.

Adicional a lo expuesto, es necesario tener en cuenta el Índice Nacional de Seguridad Cibernética - NCSI[1], el cual es un índice global que mide la preparación de los países para prevenir las amenazas cibernéticas y gestionar los incidentes cibernéticos. El NCSI también es una base de datos con materiales de evidencia disponible al público y una herramienta para el desarrollo de capacidades nacionales de seguridad cibernética.

Los indicadores del NCSI se han desarrollado de acuerdo con el marco nacional de seguridad cibernética y se tienen en cuenta las amenazas cibernéticas fundamentales que afectan directamente el funcionamiento normal de los sistemas nacionales de información y comunicación:

- Denegación de servicios electrónicos: los servicios no son accesibles.

[1] El Índice Nacional de Seguridad Cibernética (NCSI), es generado anualmente por la Academia de Gobierno Electrónico en Estonia, el cual es un marco para comprender el riesgo cibernético y evalúa a los países interesados en participar y Colombia participa en éste.

- Infracción de la integridad de los datos: modificación no autorizada.
- Infracción de la confidencialidad de los datos: el secreto está expuesto.

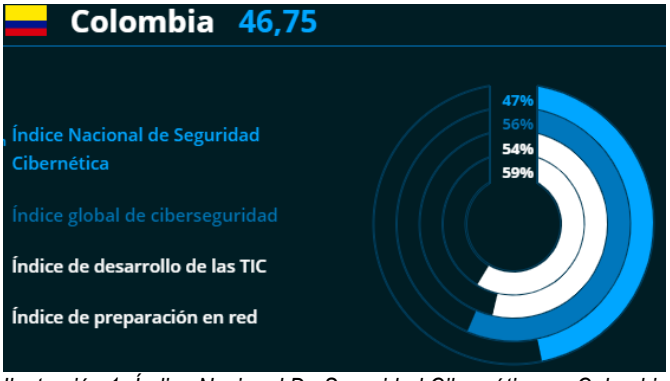
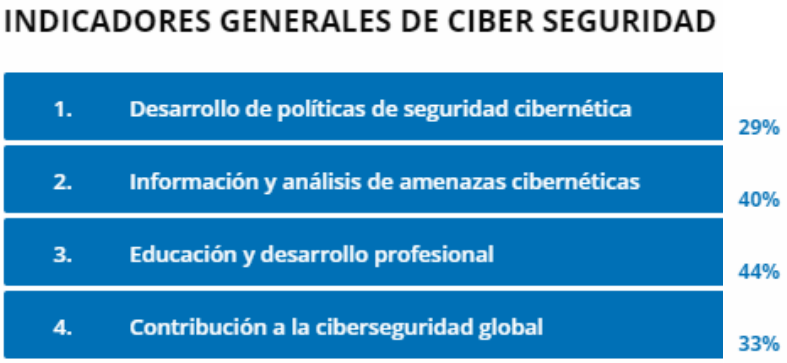


Ilustración 1- Índice Nacional De Seguridad Cibernética en Colombia

Fuente: NCSI - e-Governance Academy Foundation

En los resultados de dicho índice Colombia obtiene un puntaje global de 46,75 sobre un total de 100, lo que muestra una baja preparación en seguridad digital.

Teniendo en cuenta los resultados del 13 de febrero de 2019, de los 12 indicadores evaluados, 8 presentan un avance menor al 60%, solo 3 indicadores presentan un avance importante: Identificación electrónica y servicios de confianza y operaciones cibernéticas militares se logra un avance del 67% y para el indicador lucha contra el cibercrimen el avance es del 78%, sin embargo, para el caso de índice de protección de datos personales se logra un avance del 100%.



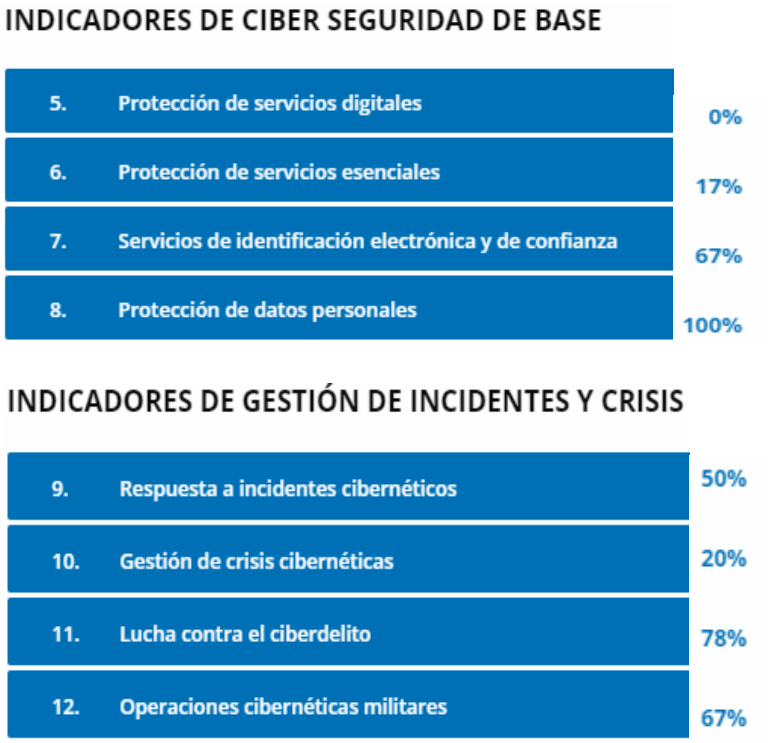


Ilustración 2- Indicadores Generales de Seguridad Cibernética-2019

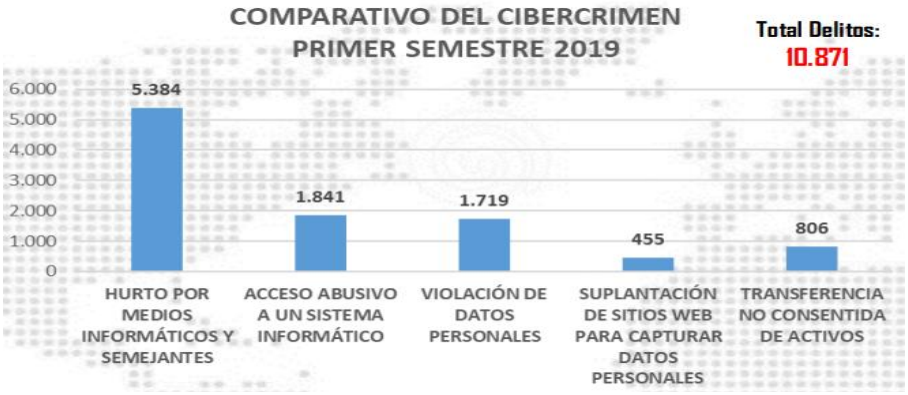
Fuente: NCSI - e-Governance Academy Foundation

1.2 CIBERCRIMEN EN COLOMBIA

De acuerdo con el Foro Económico Mundial, el cibercrimen actúa de una manera coordinada y dispone de recursos económicos ilimitados provenientes de las ganancias derivadas de actividades criminales previas. Por ejemplo, el fraude BEC (por sus siglas en inglés Business Email Compromise) – hace referencia a correos electrónicos comprometidos, y consiste en suplantar a los gerentes generales y financieros de las compañías para tener acceso a las finanzas y conseguir que se transfieran grandes sumas de dinero a cuentas bancarias. Otro de los ataques cibernéticos que han cobrado relevancia en los últimos años son los ataques como ransomware, el malware, las ciberextorsiones las amenazas que más han afectado la cadena productiva de las empresas en Colombia, por lo cual se hace necesario conocer las tipologías y modalidades que utiliza el cibercrimen en Colombia, para poder combatirlas.

De otro lado el informe de Tendencias del Cibercrimen en Colombia 2019 – 2020, realizado por la Policial -Dijin, detalla cada una de las modalidades de mayor afectación e impacto señalando los actores que intervienen en la cadena criminal e

identificando cuáles son los principales métodos de engaño que emplean los criminales a la hora de facilitar y acometer los ataques. La dinámica actual del cibercrimen en Colombia refleja un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades del ecosistema de ciberseguridad.



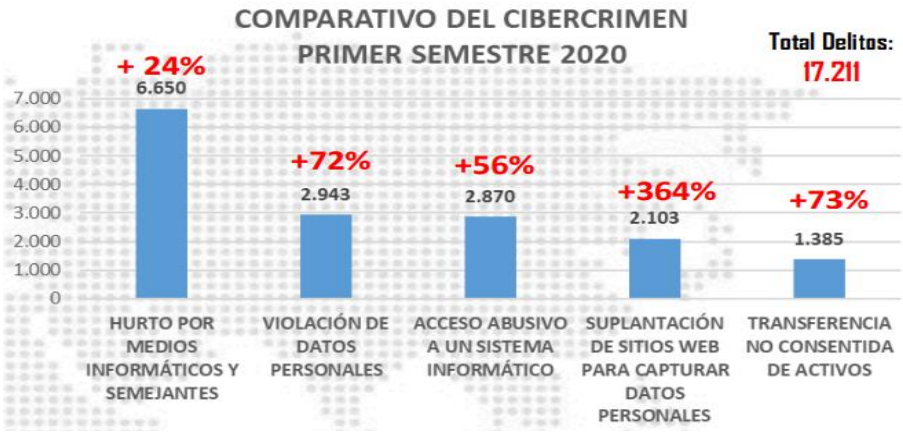


Ilustración 3-Comparativos Cibercrimen Primer Trimestre 2019 Vs Primer Trimestre 2020

Fuente: Centro Cibernéticos Policial

Como se ilustra anteriormente en Colombia hubo un aumento de 364% en la suplantación de sitios web, portales falsos que buscan apoderarse de información personal.

El 91% de incremento en el delito de daños informáticos, a causa de la viralización en internet de páginas con contenido malicioso.
El 73% de incremento en el delito de transferencia no consentida de activos.
El 72% de incremento en el delito de violación de datos personales.
El 59% de incremento por delitos informáticos.
El 56% de incremento en el delito de acceso abusivo a un sistema informático.
El 24% de incremento en el delito de hurto por medios informáticos y semejantes.

Así mismo, de acuerdo con el reporte entregado por el Centro Cibernético Policial – C4, durante el 2020 los incidentes más reportados en Colombia han sido los casos de phishing con un 42%, la suplantación de identidad 28%, el envío de malware 14% y los fraudes en medios de pago en línea con 16%.

1.3 SUPERINTENDENCIA DE TRANSPORTE

La Superintendencia de Transporte vigila, inspecciona y controla la prestación del servicio público de transporte marítimo, fluvial, terrestre, férreo y aéreo en el país, en cuanto a calidad de infraestructura y prestación del servicio se refiere. Estas funciones primordialmente se realizan a través de lo que se denominan procesos misionales, actividades que le permiten cumplir con su razón de ser.

La entidad está conformada por 27 dependencias, con un total 479 colaboradores,[2]. Para apoyar las labores diarias la entidad cuenta con equipos de escritorio y portátiles, buzones de correo electrónico habilitados y un centro de datos para el procesamiento de información, dotado de equipos de seguridad, comunicaciones, servidores, sistema de almacenamiento y backups.

Para desarrollar sus labores administrativas y de supervisión la entidad cuenta a la fecha de elaboración de esta política con veinte (20) aplicaciones de software y sistemas de información misionales y de apoyo entre los cuales se destaca, el sistema misional Vigía que es el Sistema nacional de supervisión al transporte a través del cual se registra la información de los 8.783 vigilados actualmente activos. El catálogo completo y actualizado de aplicaciones y sistemas de información se encuentra disponible en la herramienta de trabajo colaborativo de la entidad.

De acuerdo con lo expuesto la entidad cuenta con un programa de gestión documental el cual debe estar alineado con el MSPI y la Política de Seguridad y privacidad de la Información.

1.3.1 MISIÓN

Ejercer la vigilancia, inspección y control de la prestación del servicio público de transporte, su infraestructura y servicios afines en sus medios, modos y nodos dentro de la cadena logística del transporte, para el cumplimiento de las políticas públicas y normatividad nacional e internacional, de tal forma que se generen condiciones de competitividad, bienestar y desarrollo económico y social del país.

[2] Información suministrada por el grupo de Talento humano el 27 de septiembre de 2020.

1.3.2 VISIÓN

En 2022 seremos reconocidos en el País, como la Superintendencia que de manera efectiva y transparente ejerce sus funciones de supervisión, protege a los usuarios y contribuye al fortalecimiento del sector transporte.

1.3.3 PROCESOS

En la siguiente gráfica se ilustra la cadena de valor de la Superintendencia de Transporte y se identifican los diferentes procesos que la integran, entre los que se encuentra el de **Gestión de TIC** como proceso estratégico e integra el proceso Gestión estratégica de la información, los cuales estaban separados en la anterior cadena de valor.

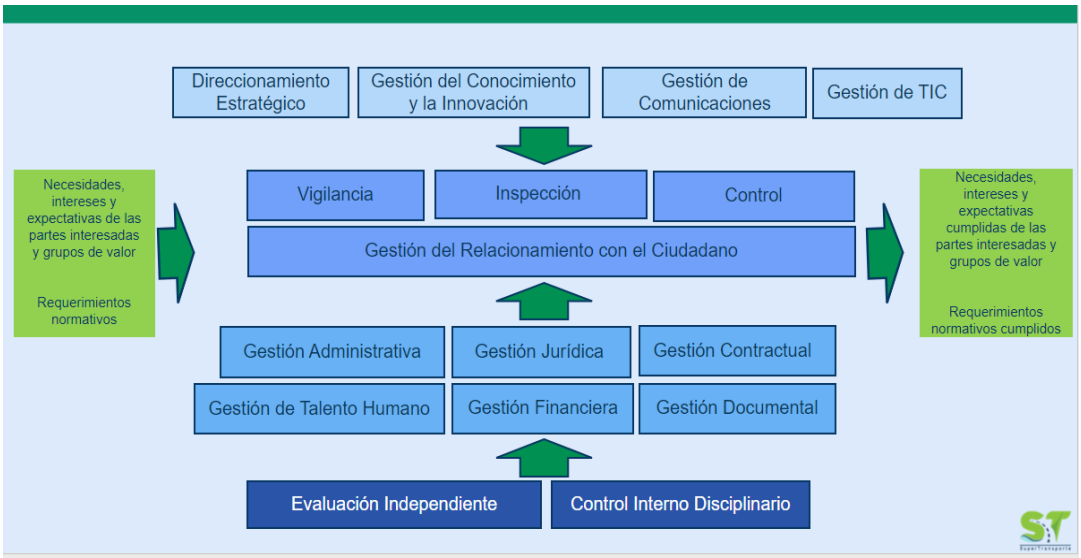


Ilustración 4- Procesos Cadena de valor Superintendencia de Transporte

1.3.3.1 Gestión de tecnologías de la información y las comunicaciones -TIC

En el 2018, a través del decreto 2409 se modifica y renueva la estructura de la entidad, se crea la Oficina de Tecnologías de la Información y las Comunicaciones (en adelante OTIC) y se establecen los objetivos que debe cumplir, dando

cumplimiento a los lineamientos de Gobierno Digital emitidos por MINTIC. A través de la implementación del MSPI y la Política de Seguridad y privacidad de la Información se busca contribuir en el logro del siguiente objetivo general de la OTIC:

Transformar con el uso de Tecnologías de la Información y las Comunicaciones los procesos, trámites y servicios de la Superintendencia de Transporte, haciendo uso de tecnologías innovadoras y mejores prácticas de la industria.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer las reglas, lineamientos y principios para la gestión de la seguridad de los activos de información, con el fin de preservar la confidencialidad, integridad y disponibilidad durante todo el ciclo de vida de la información en la Superintendencia de Transporte.

2.2 OBJETIVOS ESPECÍFICOS

- Gestionar y mantener la seguridad de la información que se gestiona y procesa dentro de la entidad y de los servicios y trámites dispuestos para los grupos de interés externos.
- Establecer, implementar y mantener la protección adecuada de los activos de información de la entidad.
- Asegurar que los funcionarios, contratistas, y empresas prestadoras de servicios en la entidad, conozcan sus responsabilidades y deberes, además que estén informados de las amenazas respecto a la seguridad de la información con el fin de reducir los riesgos de seguridad.
- Evitar el acceso no autorizado a los sistemas de información, servicios de información e infraestructura tecnológica de la entidad, así como el daño o interceptación no autorizada a la información de la entidad.
- Impedir pérdida, daño, robo o puesta en riesgo de los activos de información y la interrupción de las actividades de la entidad.
- Asegurar la operación correcta y segura de los servicios de almacenamiento y de procesamiento de la información.
- Establecer la inclusión de controles de seguridad en los sistemas de información desarrollados por la entidad o por terceros, o adquiridos.
- Dar directrices para contrarrestar las interrupciones en las actividades de la entidad y proteger los procesos más críticos en caso de fallas importantes de los sistemas de información o la infraestructura tecnológica y asegurar su recuperación oportuna.
- Definir los roles y perfiles dentro de la entidad para la gestión y seguridad de la información.

3 ALCANCE

- La política de seguridad y privacidad de la información aplica a todos los procesos de la Superintendencia de Transporte y la deben cumplir todos sus funcionarios, contratistas, vigilados y los terceros que presten algún servicio a la entidad.

- La política de seguridad y privacidad de la información estará alineada al marco de referencia de Arquitectura TI y a la Política de Gobierno Digital, así mismo contribuirá en el desarrollo del Plan Estratégico Institucional y del Plan Estratégico de Tecnologías de la Información y de las Comunicaciones.

- La política de seguridad y privacidad de la información estará alineada a la política de tratamiento de datos personales que defina la entidad, mas no da lineamientos en esta materia.

- La política de seguridad y privacidad de la información deberá estar articulada con la política de administración del riesgo, en lo relacionado con los riesgos de seguridad digital.

4 DEFINICIONES

Activo: Aquello que tenga valor para la organización. (Base de datos, sistemas de información, servicios, documentos, personas). Los activos los podemos separar en dos grandes grupos: tangibles e intangibles. Los activos tangibles son aquellos activos materiales que contienen información. Los activos intangibles son aquellos que soportan la información dentro de un activo material, y pueden inutilizar la información, pese a que el activo físico no haya sufrido daño alguno.

Activos de información: es: “algo que una organización valora y por lo tanto debe proteger”. Se puede considerar como un activo de información a: los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios. Es importante precisar que el concepto de activos de información definido en la ley 1712 de 2014 es diferente al concepto que maneja el MSPI – ISO 27001.

Acuerdo de confidencialidad: es el mecanismo mediante el cual regulamos los aspectos relativos a la seguridad de la información en una prestación de servicios, acorde a las funciones a desempeñar en la entidad.

Arquitectura empresarial: es un marco conceptual que explica la estructuración y funcionamiento de una organización e incluye los siguientes elementos: Mapa de organización, Mapa de procesos de negocio, Mapa de sistemas, Mapa de Información

Backup de la información: se refiere a la copia y archivo de datos de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

Cadena de mensajes: consiste en un mensaje que intenta inducir al receptor a realizar algún número de copias de este para luego pasarlos o propagarlos a nuevos receptores.

Centro de datos: es la ubicación física donde se concentran los recursos necesarios de computación de una organización o proveedor de servicios.

Centro de procesamiento: al espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

Certificado SSL: (Secure Sockets Layer o capa de conexión segura) es un estándar de seguridad global que permite la transferencia de datos cifrados entre un navegador y un servidor web, la capa SSL permite que dos partes tengan una comunicación privada.

CISO (Chief Information Security Officer). El oficial de seguridad es el director de seguridad de la información. Básicamente es un rol desempeñado a nivel ejecutivo y su función principal es la de alinear la seguridad de la información con los objetivos de negocio.

Ciberataques: es un intento de exponer, alterar, desestabilizar, destruir, eliminar para obtener acceso sin autorización o utilizar información, se intenta obtener el control de un sistema informático para utilizarlo con fines maliciosos o robo de información.

Ciberamenazas: Una amenaza digital es un acto malicioso que busca hacer daño a datos, robar datos, o afecta la vida digital en general. Los ciber ataques incluyen amenazas cómo virus.

Ciberdelincuente: Persona que realiza actividades delictivas en internet como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad.
Ciberseguridad: Es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.

CIO: (Chief Information Officer) Líder de la gestión estratégica de Tecnologías de Información, encargado de planificar, organizar, coordinar, gestionar y controlar la estrategia de uso y apropiación de TI.

Código quemado: Hace referencia a una mala práctica en el desarrollo de software que consiste en incrustar datos directamente en el código fuente del programa como usuario, contraseña, dirección ip, entre otros.

ColCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

Confidencialidad: asegura que el acceso a la información está adecuadamente autorizado. prevenir la divulgación no autorizada de la información sobre nuestra organización.

Cortafuego: conocido en inglés como firewall, es un sistema que bloquea cualquier intento de uso y acceso no autorizado a equipos de cómputo o portátiles. Los cortafuegos pueden ser de software, hardware, o una combinación de ambos.

Correos masivos: Es él envió simultaneo de correo a varias personas a través de un solo buzón de correo.

Criticidad: Es un indicador proporcional al riesgo que permite establecer la jerarquía o prioridades de procesos, sistemas y equipos, creando una estructura

que facilita la toma de decisiones acertadas y efectivas y permite direccionar el esfuerzo y los recursos a las dependencias donde es más importante y/o necesario mejorar la confiabilidad y administrar el riesgo.

Custodio de la información: Es un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. intenta obtener el control de un sistema informático para utilizarlo con fines maliciosos, robo de información.

Disponibilidad: Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan.

GRPS: Encuesta de Percepción de Riesgos Globales. (Global Risks Perception Survey -GRPS)

Información sensible: se usa este término para designar datos privados relacionados con Internet o informática, como contraseñas de correo electrónico, conexión a Internet, IP privada, así como la información personal privada de un individuo como datos personales y bancarios.

Integridad: Supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.

Malware: Es un término general para referirse a cualquier tipo de software malicioso, diseñado para infiltrarse en un dispositivo (PC, móviles, tabletas) sin conocimiento, del que hace uso de este.

Modelo Integrado de Planeación y gestión- MIPG: el Sistema de Gestión, integra los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad y lo articula con el Sistema de Control Interno, siendo MIPG el mecanismo que facilitará dicha integración y articulación.

NCSI: Índice Nacional de Seguridad Cibernética.

OTIC: Oficina de las Tecnologías de la Información y las Comunicaciones.

Perfiles: Permite definir los permisos a que tiene derecho un grupo de usuarios.

Phishing: es un método para suplantación de Identidad, que recopila información personal utilizando una llamada telefónica, correos electrónicos y sitios web engañosos, logrando que un usuario comparta contraseñas, números de tarjeta de crédito, y cualquier otra información confidencial.

Política de Gobierno Digital: consiste en poner a disposición de los ciudadanos, usuarios y grupos de interés, los trámites y servicios del Estado haciendo uso de las TIC, garantizando el uso de esquemas de autenticación, la interoperabilidad y el almacenamiento y conservación electrónica de la información.

Política de Seguridad de la información: es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene el conjunto de lineamientos y procedimientos que deben ser implementados para gestionar la seguridad de la información.

Propietario de la Información: Es un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente y de definir y revisar periódicamente las restricciones y clasificaciones del acceso.

Ransomware: Es un software malicioso que al infectar un equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar los archivos quitando el control de toda la información y datos almacenados. El atacante a cambio de desencriptar la información solicita una cantidad de dinero.

Roles: es una colección de permisos definida para todo el sistema que Usted puede asignar a usuarios específicos.

Seguridad de la información: es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

Seguridad Digital: es la dependencia de una empresa u organización enfocada en procesos informáticos y telemáticos para proteger toda la infraestructura física y digital relacionada con la tecnología computacional.

Servicios Ciudadanos Digitales: son un conjunto de soluciones tecnológicas que buscan facilitar a los usuarios, y en específico a los ciudadanos, su interacción con las entidades públicas y optimizar la labor del Estado.

Sistema de Seguridad Digital SGDI: busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

Tecnologías de la Información y de la Comunicación: son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y

medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes.

TIC: Tecnologías de la Información y de la Comunicación.

TI: Tecnologías de la información

TOGAF: Es un marco de trabajo de arquitectura empresarial desarrollado por el Open Group que proporciona un enfoque para el diseño, planificación, implementación y gobierno de una arquitectura empresarial. Este marco plantea la estructuración de la arquitectura cuatro dominios o dimensiones: Negocio, Tecnología (TI), Datos y Aplicaciones.

5 RESPONSABILIDADES

A fin de ejecutar la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, así como la política de seguridad y privacidad de la Información, se establecen los diferentes roles, asignación de responsabilidades y principales actividades a ejecutar así:

	ROLES				
ACTIVIDADES	**SUPERINTENDENTE**	**OTIC**	**DIRECTORES O JEFES DE DEPENDENCIA**	**FUNCIONARIOS/ CONTRATISTAS**	**PROVEEDORES DE SERVICIOS**
Estructurar la política de seguridad y privacidad de la Información	A-I	R	C	C	
Aprobar la política de seguridad y privacidad de la información	A	I	I	I	
Implementar y socializar la política de seguridad y privacidad de La Información	I	R	R	R	R
Actualizar la política de seguridad y privacidad de la Información	I	R	C	C	
Efectuar diagnóstico y estado actual del MSPI	I	R	R	C	C
Identificar vulnerabilidades de los activos de información de la entidad.	I	R	R	C	C
Identificar avance y efectividad de los controles para la gestión de riesgos de seguridad de la información	I	R	R	C	C
Documentar, socializar y ejecutar los procedimientos de seguridad de la información	I	R	R	C	C
Identificar y actualizar los activos de información		R	R	C	C
Efectuar la valoración y tratamiento de los riesgos de seguridad de la información.	I	R	R	C	C
Estructurar y ejecutar el plan de sensibilización y capacitación.	I	R	R	C	C
Establecer los indicadores de Gestión del MSPI para la entidad.	I	R	R	C	C

Responsable (R): es la persona que realiza el trabajo hasta completar la tarea.
Aprobador (A): es el encargado de designar a la persona responsable de la tarea, además será el responsable de que la tarea se realice con éxito.
Consultado (C): se refiere a las personas que expresan su opinión sobre una actividad en concreto.

Informado (I): designa a aquellos que buscan mantenerse al día sobre el progreso de la actividad

Responsables de la información:

Administradores o custodios: Se denomina así a las personas o dependencias que proporcionan información o servicios de información. Los custodios no necesitan conocer la información para la realización de su trabajo, solamente procesarla, gestionar su almacenamiento y hacerla accesible.

Propietario: el término propietario identifica a un individuo o una entidad que tiene responsabilidad aprobada por el nivel directivo para la creación, el desarrollo, mantenimiento, uso y seguridad de los activos de información.

Usuario, es aquella persona que introduce, modifica, borra o lee la información almacenada en los Sistemas de información o aplicaciones. Para adquirir un perfil de usuario es necesaria autorización previa del propietario de la información.

Roles y Responsabilidades: La elaboración, actualización y manejo de los instrumentos de información Pública, estará a cargo de cada dependencia bajo la orientación de la Oficina Asesora de Planeación así:

ACTIVIDAD	RESPONSABLE
Reporte y registro de activos de Información en los formatos y herramientas definidas	Directores o jefes de dependencia
Revisar y consolidar todos los activos de información de las dependencias.	Oficina de Tecnologías de la información y las Comunicaciones, Grupo de Gestión Documental
Índice de Información Clasificada y Reservada	Oficina Asesora Jurídica
Esquema de publicación de información	Equipo de Comunicaciones
Programa de Gestión Documental	Grupo de Gestión Documental

6 MARCO NORMATIVO Y REGULATORIO

La Superintendencia de Transporte por ser una entidad pública del orden Nacional de la rama ejecutiva, debe cumplir con la regulación y la normativa que establece el Estado colombiano en materia de Tecnologías de la Información. En ese sentido y para dar cumplimiento de la Política pública de Gobierno Digital, la cual hace parte de las 18 políticas de gestión y desempeño institucional, que se establecen en el Modelo Integrado de Planeación y Gestión MIPG, se requiere trabajar e implementar los tres habilitadores trasversales de la Política de Gobierno Digital: Arquitectura empresarial, Seguridad de información y Servicios ciudadanos Digitales.
Para implementar el habilitador de seguridad de la información, así como el SGSI y la Política se seguridad y privacidad la Información se requiere dar cumplimiento a los decretos, leyes, normas que se enuncian a continuación:

Normas regulatorias

- Conpes 3995 de 2020, Política Nacional De Confianza y Seguridad Digital.
- Conpes 3975 de 2019, Política Nacional Para la Transformación Digital e Inteligencia Artificial.
- Conpes 3920 de 2018, Política Nacional De Explotación De Datos (Big Data).
- Conpes 3701 de 2011, Lineamientos de política para la Ciberseguridad y Ciberdefensa.
- Decreto 620 de 2020, "Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 1008 de 2018, por el cual se establecen los lineamientos generales de la Política de Gobierno Digital.
- Decreto 1499 de 2017,Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema *de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.* Modelo Integrado de Planeación y gestión- cap 3.
- Decreto 1078 de 2015, Reglamenta el Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1377 de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Ley 2052 de 2020. Por medio de la cual se establecen 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 y se dictan otras disposiciones. Se crean las condiciones para racionalizar, automatizar y digitalizar trámites con el Estado. - La norma rige que los trámites que se creen a partir de su entrada en vigor deberán realizarse totalmente en línea por parte de los ciudadanos.

- Ley 1955 de 2019, Por el cual se expide el Plan Nacional de Desarrollo 2018-2022.
- Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de acceso a la Información Pública Nacional.
- Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Protección de datos y privacidad de la información.
- 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, es decir, regula el manejo de la información contenida en bases de datos personales.
- Ley 594 de 2000, Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
- Ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Resolución 3564 de 2015 expedida por MinTIC, Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
- Normas internas de la Superintendencia de Transporte: Resolución 57481 de 2017. Por la cual se adoptan los siguientes instrumentos de la gestión de información pública: el registro de activos de información, el índice de información clasificada y reservada, el esquema de publicación de información y el programa de gestión documental

Normas Técnicas

- Norma NTC ISO IEC 27001-2013, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información – SGSI.
- Norma NTC ISO IEC 27002-2013, Técnicas de Seguridad, Código de practica para la gestión de la seguridad de la Información.
- Norma NTC ISO IEC 27005–2009, Técnicas de Seguridad, Gestión del Riesgo en la Seguridad de la Información.

7 ATRIBUTOS DE SEGURIDAD DE LA INFORMACIÓN

Los siguientes atributos de calidad descritos son los definidos por la ISO 27001 y la entidad se alinea con ellos con la implementación de la política de seguridad y privacidad de la información.

Confidencialidad de la información: hace referencia a que la información sólo debe ser conocida por las personas que han sido autorizadas para ello, es decir, controlar el acceso a los datos para evitar su divulgación no autorizada.
La confidencialidad puede romperse a través de ataques directos diseñados para obtener acceso no autorizado a sistemas, aplicaciones y bases de datos con el fin de robar o manipular datos, o también puede violarse involuntariamente, a través de errores humanos, descuidos o controles de seguridad inadecuados.

Integridad de la información: Se refiere a que la información que se encuentra almacenada en los dispositivos o la que se ha transmitido por cualquier canal de comunicación no ha sido manipulada por terceros de manera malintencionada, es decir, garantizar que la información no será modificada por personas no autorizadas, por lo tanto, es confiable.

Disponibilidad de la información: hace referencia a que la información debe estar disponible siempre para las personas autorizadas según los roles definidos, es decir que la disponibilidad implica que las redes, los sistemas, las aplicaciones y servicios estén en funcionamiento. Ello garantiza que los usuarios autorizados tengan acceso oportuno y fiable a los recursos cuando los necesiten.

8 POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.1 Declaración de la política de seguridad y privacidad de la información

La Superintendencia de Transporte adopta como su Política de Seguridad y Privacidad de la Información enmarcada en el modelo de seguridad y privacidad de la información con el fin de asegurar la protección, confidencialidad, integridad, disponibilidad de los activos de información (procesos, hardware, software, infraestructura, información, funcionarios, contratistas, terceros) que soportan los procesos de la entidad mediante la implementación de los lineamientos, procedimientos e instructivos, y la asignación de responsabilidades generales y específicas, los cuales están orientados a preservar la continuidad del negocio, la prevención de incidentes de seguridad y la reducción de su impacto potencial dentro de un proceso de mejora continua.

La Superintendencia de Transporte considera la información como un elemento importante e indispensable en el cumplimiento de los objetivos organizacionales, razón por la cual define la Política de Seguridad y Privacidad de la Información para salvaguardar la seguridad y privacidad de la información de manera adecuada durante su ciclo de vida, además de definir los lineamientos o directrices que permitan desarrollar estrategias para la gestión de los activos de información que garanticen pertinencia, calidad, oportunidad, seguridad e intercambio de datos e información.

La Superintendencia de Transporte cuenta con el proceso de Gestión de TIC'S con el fin de contribuir al cumplimiento de sus funciones de la vigilancia, inspección y control de la prestación del servicio público de transporte, su infraestructura y servicios afines en sus medios, modos y nodos dentro de la cadena logística del transporte.

Aunado a lo anterior la Superintendencia de Transporte es consciente de la importancia de la implementación del Sistema de Gestión de Seguridad de la Información-SGSI, razón por la cual la Política de Seguridad y privacidad de la Información se constituyen como parte fundamental de éste.

En ese sentido el Superintendente de Transporte se compromete a implementar el SGSI en cada uno de sus procesos a fin de identificar y gestionar la seguridad de los activos de información y adicionalmente a:

- Divulgar y verificar el cumplimiento de la Política de seguridad y privacidad de la información a los funcionarios y contratistas de la entidad.
- Promover la cultura en Ciberseguridad y privacidad de la información al interior de la Superintendencia.

- Aprobar la asignación de funciones, roles y responsabilidades de cada dependencia en el sistema de gestión de seguridad de la información.
- Asignar los recursos para la implementación y mejora continua del sistema de gestión de seguridad de la información.
- Apoyar la innovación tecnológica acorde con los lineamientos del Ministerio de las Tecnologías y las Comunicaciones MINTIC, con el fin de contribuir en la implementación de la Política de Gobierno Digital.
- Minimizar y mitigar los riesgos de seguridad digital, acorde con lo establecido en la política de administración del riesgo de la entidad.

8.2 Consideraciones Generales

1. La implementación, ejecución y seguimiento de la Política, procedimientos, funciones de software y hardware e instructivos en materia de seguridad y privacidad de la información estará a cargo de la OTIC con la colaboración de las demás dependencias de la entidad acorde con los procesos y procedimientos en los cuales interactúen.
2. Todos los funcionarios y contratistas que laboran en la Superintendencia de Transporte se comprometen a cumplir con la política de Seguridad y privacidad de la Información y dar el manejo adecuado a los activos de información a su cargo.
3. La política de seguridad y privacidad de la información de la Superintendencia de Transporte describe los lineamientos, reglas, normas y procedimientos que se deben cumplir para la adecuada gestión y uso los de activos de información de la entidad.

El incumplimiento de la política de seguridad y privacidad de la información por parte de los funcionarios y contratistas de la entidad acarreará sanciones disciplinarias y sanciones legales a las que haya lugar, de acuerdo con lo definido en el numeral 11 y 12 de este documento.

9 LINEAMIENTOS DE SEGURIDAD

Proteger la información significa garantizar el cumplimiento de los tres principios fundamentales de la seguridad de la información, es decir, que la entidad debe asegurar la confidencialidad, la integridad y la disponibilidad de la información, además de establecer los lineamientos que deben cumplir los funcionarios, contratistas y terceros. Para lograr este propósito se definen los lineamientos que permitirán garantizar la seguridad de los activos de información de la Superintendencia de Transporte.

9.1 LINEAMIENTOS PARA LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. El comité institucional de gestión y desempeño deberá revisar y aprobar las actualizaciones efectuadas a la política de seguridad y privacidad de la información.
2. El CIO (jefe de la oficina de tecnologías de la información y las comunicaciones), el oficial de seguridad y el asesor de TIC del despacho del superintendente, tendrán la responsabilidad de proyectar, actualizar y/o modificar la Política de Seguridad y Privacidad de la Información, como mínimo una vez al año, si a ello hubiere lugar y ser presentada al comité institucional de gestión y desempeño para su aprobación.
3. El comité institucional de gestión y desempeño deberá aprobar la asignación de un facilitador por dependencia o por procesos para establecer las mesas de trabajo con el fin de identificar los activos de información de la entidad, así como la matriz de riesgos.
4. La Secretaria General y Oficina Asesora Jurídica con el acompañamiento de la OTIC deben establecer un acuerdo de confidencialidad o clausula en los contratos según corresponda, así como la aceptación de la política, procedimientos y lineamientos del manejo adecuado de información, tanto para funcionarios, contratistas, estudiantes en práctica empresarial o cualquiera que desarrolle proyectos para la entidad de tipo académico.
5. La OTIC deberá establecer el canal de comunicación con los entes gubernamentales y privados, que apoyen las labores de seguridad en temas de prevención y atención de incidentes de seguridad.
6. La entidad debe contar con una política de protección y privacidad de datos personales que deberá ser comunicada a todos los involucrados cuando se recolecte y almacene información personal a través de formatos físicos, digitales o sistemas de información. La Secretaria General será la encargada de estructurar la política y presentarla al comité institucional de gestión y desempeño para su aprobación.
7. El representante legal y el ordenador del gasto de la entidad deberán programar las auditorías internas a través de la oficina de control interno,

previa asignación de los recursos requeridos (humanos, económicos y técnicos) o a través de un tercero especializado, para verificar el cumplimiento de los lineamientos de la política de seguridad en los sistemas de información y plataforma tecnológica de la entidad.

8. La OTIC deberá validar los controles de los procesos más críticos para la continuidad del negocio o de mayor impacto para la entidad en caso de fallo.
9. La política de seguridad y Privacidad de la información deberá estar alineada con el Programa de Gestión Documental – PGD de la entidad y deberán cumplir con lo establecido en la resolución interna de la Superintendencia 57481 de 2017, relacionada con la gestión de activos de información de que trata la Ley 1712 de 2014.

9.2 LINEAMIENTOS PARA LA GESTIÓN DE ACTIVOS DE INFORMACIÓN.

1. La entidad a través de la OTIC debe identificar, clasificar y mantener actualizados todos los activos de información por dependencia y por procesos, estableciendo los más críticos y sensibles para la entidad, se deberá documentar la importancia que tienen para cada dependencia en los formatos o herramientas tecnológicas definidas por la OTIC, la cual debe crear un repositorio de activos de información, con control de acceso.
2. Cada dependencia, deberá actualizar el inventario de activos de información, cada vez que se elimine, modifique o actualice un activo de información que se encuentre a su cargo de acuerdo con el procedimiento establecido por la OTIC.
3. El grupo de gestión documental y la OTIC establecerán el procedimiento de identificación y clasificación de activos, así como la definición de reglas de uso de los activos de información, además del formato de levantamiento de información para cada activo y crear el repositorio de la información inherente a seguridad de la información con roles y perfiles para el control de acceso. Se deberá detallar para cada activo: Información básica del activo (nombre, observaciones, proceso), nivel de clasificación de la información, ubicación, tanto física como electrónica, propietario, custodio, usuarios y derechos de acceso (roles) y demás que se requieran.
4. Cada dependencia de la entidad deberá clasificar los activos de información analizando la confidencialidad, integridad y disponibilidad, acorde con el nivel de criticidad para cada dependencia o proceso, y establecer el grado de importancia, estimación y mitigación de los riesgos asociados. Se deberá cumplir con lo establecido en la resolución interna de la Superintendencia de transporte 57481 de 2017, relacionada con la gestión de activos de información de que trata la ley 1712 de 2014. Así mismo debe definir el propietario, custodio, usuario y responsable para cada activo de información que maneje.

5. La entidad a través de la OTIC debe establecer el procedimiento de asignación y devolución de los activos de información asignados a los funcionarios y a los contratistas, así como a terceros que presten algún servicio e interactúen con la entidad, el cual deberá estar disponible en la cadena de valor.
6. La OTIC y el oficial de seguridad deben definir y revisar máximo cada tres (3) meses las restricciones y clasificaciones de acceso a activos de información importantes, teniendo en cuenta las políticas de control de acceso.
7. La Oficina asesora jurídica y la Oficina Asesora de planeación deberán establecer el procedimiento para realizar la transferencia y envió de información pública reservada o información pública clasificada por correo, copia impresa o electrónica a entidades o personas fuera de la entidad.
8. La OTIC debe definir el procedimiento para eliminar, destruir o borrar de forma segura información de unidades de almacenamiento, estaciones de trabajo, servidores, portátiles a fin de realizar la gestión adecuada a los activos de información.
9. La OTIC y el grupo de gestión documental debe definir el procedimiento de clasificación de la información tanto para activos en formato físico como electrónicos y/o metadatos, acorde con el esquema de clasificación definida por el grupo de Gestión documental.
10. La OTIC, deberá establecer todos los procedimientos asociados al proceso de gestión de TIC relacionados con el procesamiento, almacenamiento, gestión y transferencia información a través de medios y canales electrónicos.
11. Toda la información que sea creada o procesada, por los funcionarios, contratistas o prestadores de servicios es propiedad de la entidad y deberá ser entregada a la entidad una vez culmine su relación contractual en los medios y formatos definidos por la OTIC o la dependencia según corresponda.
12. La Superintendencia de Transporte no se hace responsable de la información personal que los funcionarios y contratistas almacenen en los equipos de cómputo asignados para las labores o funciones diarias en la entidad.
13. La OTIC debe definir los lineamientos para el manejo adecuado de directorio activo y asignación de licencias de software ofimático y de BackOffice de funcionarios y contratistas.
14. La Superintendencia de Transporte a través de la OTIC en su proceso misional de gestión estratégica de la información debe incluir la definición e implementación del proceso o procedimiento de anonimización, con el fin de impedir que, a partir de un dato o de una combinación o correlación de datos, se logren identificar sujetos individuales ya sean individuos o empresas vigiladas a partir de la información publicada por la entidad.
15. Todos los manuales y procedimientos que complementen la Política de Seguridad y privacidad de la Información deberán ser aprobados y

publicados en la cadena de valor, y estarán disponibles para todos los contratistas y funcionarios de la entidad a través de la Intranet.

9.3 LINEAMIENTOS DE SEGURIDAD DE LOS FUNCIONARIOS Y CONTRATISTAS

1. Solo tendrá acceso a la información de la entidad los funcionarios y contratistas que estén autorizados por los jefes de dependencia, con el fin de evitar accesos no autorizados, modificación o eliminación de esta, para lo cual cada dependencia deberá diligenciar la matriz de acceso a la información y sistemas de información a la que el funcionario tendrá acceso; el jefe de cada dependencia deberá autorizar el acceso mediante la herramienta de mesa de servicio de la entidad. El formato de la matriz se estructurará con el apoyo de la OTIC.
2. La OTIC y las dependencias deberán capacitar a los funcionarios y contratistas cuando ingresen por primera vez a la entidad, en el manejo de las aplicaciones misionales y demás aplicativos que utilicen los diferentes procesos.
3. La OTIC deberá habilitar el acceso a los aplicativos y herramientas de la entidad según los roles, de acuerdo con la solicitud realizada por la dependencia a través de la herramienta de mesa de servicio de la entidad.
4. La OTIC deberá estructurar y ejecutar el plan de sensibilización y capacitación en temas de ciberseguridad, política de seguridad y transformación digital para toda la entidad, durante todo el año.
5. La Secretaria General y la Dirección Administrativa durante el proceso de vinculación de contratistas y funcionarios deben verificar la hoja de vida con todos los soportes tanto académicos como laborales, así como la verificación de antecedentes penales y profesionales.
6. Cuando la vinculación sea específica para la OTIC, dependiendo del rol a desempeñar y las actividades a ejecutar se deberá establecer un formato especial acorde con los activos de información a su cargo. Así mismo cuando se produzca la terminación del contrato o culmine la relación laboral con la entidad, se deberá realizar la transferencia de conocimiento y la entrega formal de la documentación e información que procesó y generó durante sus labores en las herramientas y repositorios definidos según corresponda.
7. Dentro de las cláusulas generales de los contratos de prestación de servicios que se realicen deberán definir e incluir las responsabilidades y deberes en temas de seguridad de la información. así como el acuerdo de confidencialidad. Esta actividad estará a cargo de la Secretaria General y la Oficina Asesora Jurídica.
8. El Superintendente, a través de los jefes de dependencia y supervisores de contratos, verificarán el cumplimiento de la política de seguridad y privacidad de la información sus lineamientos y procedimientos.

9. Los funcionarios y contratistas deberán asistir a las charlas y talleres de ciberseguridad y transformación digital que programe la entidad. La no participación de estas actividades acarreara afectación en los acuerdos de gestión del jefe de cada dependencia.
10. Los funcionarios y contratistas tienen el deber de reportar a la OTIC las novedades de seguridad si estas son evidenciadas, con el fin de tomar las medidas correctivas necesarias, a través de la herramienta de mesa de servicio de la entidad.
11. La OTIC mensualmente se deben generar tips o píldoras informativas de seguridad y privacidad de la información para los usuarios de la entidad, con el fin de ir generando conciencia en la gestión y uso de los activos de información y los temas de ciberseguridad. Así como la generación de comunicados de forma inmediata y masiva para prevención, teniendo en cuenta los informes generados por los entes gubernamentales y entidades privadas.
12. El incumplimiento de la política por parte de los funcionarios, contratistas, estudiantes en práctica empresarial o cualquiera que desarrolle proyectos para la entidad de tipo académico, así como de los lineamientos y procedimientos de seguridad de información de la entidad, así como la divulgación de información no autorizada y/o el manejo inadecuado de activos de información, acarreará acciones o sanciones de acuerdo con el numeral 3.7 de esta política.
13. El Grupo de Talento humano deberá reportar a la OTIC las novedades de los funcionarios: (Vacaciones, Licencia, incapacidad), a través de la herramienta de mesa de servicio, con el fin de realizar el bloqueo de los usuarios en el directorio activo, para el acceso a los sistemas de información, equipo de seguridad perimetral, servidores y base de datos.
14. La OTIC debe efectuar backup de la de información del perfil del usuario que se encuentre almacenada en el equipo de cómputo, cuando exista alguna de las siguientes novedades de los funcionarios: (Vacaciones, Licencia, cambio de dependencia o finalice el vínculo laboral con la entidad)
15. La OTIC deberá bloquear automáticamente los usuarios de los funcionarios y contratistas que soliciten la firma del formato “Paz y Salvo de Funcionarios y Contratistas”, cuando estos finalizan su vinculación con la entidad y una vez se tenga el VoBo del Grupo de Gestión documental.
16. Todos los funcionarios y contratistas de la entidad deben firmar el acuerdo de confidencialidad, así como la aceptación de la Política, procedimientos y lineamientos del manejo adecuado de información.
17. Los funcionarios y contratistas que tengan asignados portátiles de la entidad deberán dejarlo con el cable de seguridad (guaya) cuando termine la jornada laboral o se ausenten de su puesto de trabajo, de lo contrario estos deberán ser recogidos y guardados por el personal de vigilancia.

9.4 LINEAMIENTOS PARA LA SEGURIDAD FÍSICA Y DEL ENTORNO

1. La Superintendencia de transporte a través de Dirección Administrativa implementará control de acceso a las instalaciones de la entidad a través de tecnologías de punta que permitan tener el registro de ingreso y salida del personal autorizado. Todos los funcionarios y contratistas solo podrán ingresar a la entidad si poseen carné y deberán pasar por el control de acceso establecido, de lo contrario deberán registrarse como un visitante.
2. La autorización de parametrización del usuario al control de acceso se deberá realizar a través de la herramienta de mesa de servicio por el jefe inmediato o supervisor del contrato.
3. La OTIC deberá almacenar los registros de ingreso y salida de las instalaciones de la entidad y deberán estar disponibles para su consulta cuando lo requieran la dependencia de talento humano.
4. El ingreso del personal de la OTIC o personal externo que preste un servicio a los centros de datos y procesamiento deberán ser autorizados por el jefe de la OTIC a través de formulario electrónico, y se debe llevar registro físico y digital. El personal externo deberá estar siempre acompañado de un funcionario de la OTIC.
5. El centro de datos y de procesamiento debe ser un espacio cerrado y con acceso restringido y controlado, el cual debe contar con sistema de control de incendios y cumplir con las normas técnicas vigentes.
6. Se dispondrá de personal de seguridad para gestionar el ingreso a las instalaciones, para el caso de visitantes, estos deben ser anunciados y autorizados por un funcionario de la entidad. Deberá quedar el registro físico en el libro de los ingresos, con la información del visitante y de la persona que autoriza el ingreso. Los visitantes no pueden ingresar y salir solos, un funcionario deberá acompañarlos al ingreso y salida de la entidad.
7. La Superintendencia deberá contar con un centro de datos, de procesamiento y almacenamiento alterno en nube, para asegurar y resguardar la información sensible de la entidad y de los procesos críticos a fin de garantizar la continuidad del negocio.
8. La Dirección administrativa debe establecer el procedimiento para que el personal de seguridad verifique los elementos que ingresan o salen de la institución, así como el soporte de autorización para salida de elementos emitido por el responsable de cada dependencia.
9. Las áreas de archivo deberán tener asignado un responsable y tener el control adecuado para acceder a la documentación y evitar manipulación de información, especialmente la información crítica de la entidad, para esta información se deberá establecer el procedimiento para dar un manejo especial.
10. El jefe de OTIC verificará periódicamente las listas de los controles de acceso al centro de datos de la entidad.

11. Los funcionarios y contratistas deberán portar en un lugar visible el carné que los identifique dentro de la entidad.

9.5 LINEAMIENTOS DE SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO

1. La entidad debe contar con un centro de datos interno o externo, que cumpla con el estándar ANSI/TIA-942 que permita garantizar y facilitar los procedimientos de: administración, gestión y control de forma óptima para la ejecución de todos los servicios de tecnologías de la información (TI), a fin de mantener siempre condiciones de: eficiencia, seguridad, confiabilidad y disponibilidad.
2. La OTIC debe garantizar que cada puesto de trabajo cuente con un punto de corriente normal y corriente regulada, para evitar daños en los equipos y daño o pérdida de la información. Cumplir con la norma TIA 568.
3. La entidad debe contar con un plan de mantenimiento preventivo de todos los equipos de cómputo, el cual debe ser actualizado cada año y ejecutado por la OTIC.
4. La OTIC deberá definir una herramienta digital (aplicación) para autorizar salida de equipos de las instalaciones de la entidad, esta autorización de salida debe estar visada por el jefe de cada dependencia o supervisor del contrato y validada en el momento de la salida por los funcionarios de la empresa de seguridad de la entidad.
5. La entidad a través de la OTIC debe documentar los procedimientos de operación de todos los servicios de procesamiento de información (encendido y apagado de los equipos del centro de datos, copias de respaldo, mantenimiento de los equipos del centro de datos, manejo de cuartos de cableado, reinicio y recuperación de los sistemas, gestión de registro de auditorías y del sistema), y disponerlos en formato digital en el repositorio de la OTIC y la cadena de valor de la entidad según la confidencialidad definidos para estos.
6. La OTIC debe establecer los procedimientos de reutilización, eliminación y borrado de información de equipos no funcionales.
7. Los equipos asignados a los funcionarios y contratistas solo podrán ser usados para cumplir con sus funciones y/u obligaciones contractuales.
8. Los funcionarios y contratistas no tienen permitido abrir o desmontar las CPU o los monitores de los equipos.
9. Los funcionarios y contratistas no podrán ingerir bebidas y alimentos mientras estén utilizando los equipos de cómputo.
10. Todos los puertos USB y unidades ópticas deben estar inhabilitados de todos los equipos de la entidad, con el fin de mitigar la propagación de virus, robo y eliminación de información sensible para la entidad. Si se requiere el uso de medios extraíbles es necesario justificar el uso y el periodo por el cual se debe habilitar el puerto, previa autorización y justificación del jefe de cada

dependencia o supervisor, esto con el fin de evitar fuga de información. El soporte de la autorización debe quedar en formato digital y firmado.

11. Todas las novedades que se presenten con el equipo de cómputo asignado al funcionario y/o el contratista deberán ser reportados y solicitar el soporte técnico a través de la herramienta de mesa de servicio.
12. Todos los equipos de cómputo (PCs) deben tener restringido la instalación de software con el fin de evitar el uso de software ilegal en la entidad, cuando se requiera habilitar o instalar algún software que tenga licenciado la entidad, el jefe de la Dependencia realizará la solicitud a la OTIC a través del aplicativo de mesa de servicio de la entidad.
13. La OTIC debe validar mensualmente las actualizaciones de los parches de seguridad de toda la plataforma tecnológica como bases de datos, aplicaciones o software instalados. Deberá realizar de forma oportuna las actualizaciones una vez se publiquen o estén disponibles, especialmente las de los sistemas operativos, navegadores y programas antivirus, no obstante, previamente se deberá identificar el efecto de estas actualizaciones.
14. Todas las estaciones de trabajo de la entidad deben contar con un antivirus. La OTIC deberá parametrizar la configuración de actualizaciones de forma automática de los equipos de cómputo (PCs), relacionados con antivirus.
15. La entidad a través de la OTIC debe actualizar y no poseer aplicaciones o sistemas operativos obsoletos, que no dispongan de actualizaciones de seguridad o no cuenten con soporte por parte del fabricante, por consiguiente, se deberán identificar y clasificar los más críticos, para migrarlos a plataformas actualizadas.
16. Cada funcionario y contratista deberá hacer backups periódicos de la información a su cargo en el servicio de nube contratado por la entidad. Cada funcionario y contratista contará con un límite de espacio de almacenamiento. Cuando la información almacenada supere la capacidad de almacenamiento limite asignado en la nube, el usuario deberá revisar y depurar su información y en caso estrictamente necesario solicitar a OTIC la generación del backup a través de la herramienta de mesa de servicio.

9.6 LINEAMIENTOS PARA LA GESTIÓN DE COMUNICACIONES Y OPERACIONES

1. La OTIC debe definir los lineamientos para la gestión de cambios y requerimientos, en infraestructura tecnológica, sistemas de información, base de datos y repositorios de información.
2. La OTIC debe establecer los procedimientos para la gestión y operación de todos los servicios de procesamiento de información y establecer los accesos para el almacenamiento y procesamiento de información en el servicio contratado de nube.
3. La OTIC definirá los lineamientos de creación y uso de carpetas compartidas en la entidad.

4. La OTIC debe establecer los procedimientos para el procesamiento y manejo de información, como encendido y apagado de los equipos, copias de respaldo, plan de mantenimiento de equipos, manejo de medios, gestión de usuarios, gestión de correo electrónico, programación y desarrollo, interoperabilidad, manejo de errores, contactos de soporte en caso de fallas técnicas, recuperación y reinicio del sistema, servicios de red y demás propios del proceso de gestión de TI, los cuales deben estar disponibles en la cadena de valor e intranet, según el grado de confidencialidad que se defina para cada uno de ellos.
5. La OTIC debe establecer los procedimientos para las pruebas de restauración de las copias de respaldo de todos los sistemas de información y toda la infraestructura tecnológica que respalda todos los servicios y trámites de la entidad.
6. La entidad a través de la OTIC y demás dependencia involucradas, deberán estructurar, implementar y realizar pruebas del plan para la continuidad del negocio de los sistemas y plataformas de comunicación y procesos más críticos.
7. El jefe de OTIC debe definir funciones, roles y perfiles para cada integrante de la OTIC, así como la autorización de acceso a los activos de información.
8. La OTIC debe garantizar que ninguna solución tecnología o aplicativo de software sea desplegado y puesto en producción sin antes haber pasado las pruebas funcionales y no funcionales en el ambiente de pruebas y/o preproducción, que incluyan pruebas de seguridad.
9. La OTIC debe contar con ambientes independientes para desarrollo, pruebas y puesta en producción de las aplicaciones.
10. La OTIC debe definir los requerimientos mínimos de los entornos de desarrollo, pruebas y producción, así como la data que se podrá manejar en cada entorno, además de los permisos y roles de forma restringida a los funcionarios y contratistas encargados de los sistemas de información y desarrollo.
11. La OTIC deberá asegurar la protección de la información en las redes y la protección de la infraestructura que soporta las operaciones y el procesamiento de la información de la entidad, a través del monitoreo del tráfico de la red y la verificación de reportes de la infraestructura de seguridad perimetral.
12. La OTIC activará el acceso remoto a la red de la entidad, siempre y cuando exista una solicitud registrada en la plataforma de mesa de servicio autorizada por el jefe de cada dependencia o supervisor del contrato, donde indique el tiempo por el cual se debe parametrizar el ingreso.
13. Ningún funcionario o contratista de la entidad podrá prestar su usuario y credenciales de acceso a la plataforma tecnológica de la entidad.
14. No se podrán conectar a la red cableada equipos personales y/o que no sean propiedad de la entidad. Para poder conectar estos equipos a la red, deberá ser revisado por el personal de la OTIC, este procedimiento se debe solicitar

a la mesa de servicio y contar con autorización del jefe de cada dependencia o supervisor del contrato.

15. La OTIC creará un perfil invitado para proveer de servicio de internet a los visitantes de la entidad a través de la red wifi, el cual será suministrado en el momento que se requiera.
16. El jefe de OTIC y el grupo de gestión documental deberán definir los lineamientos para la creación de repositorios de información dentro las herramientas que dispone la entidad, con el fin de establecer como se debe almacenar la información generada y procesada de cada dependencia.
17. La OTIC implementará la propuesta del framework de TOGAF, para el versionamiento de la documentación de procesos y procedimientos de la dependencia cuando surjan modificaciones, actualizaciones o acciones de mejora.
18. Todos los sistemas de información y bases de datos deben tener activados las opciones y log de auditoria para garantizar el registro de todas las transacciones y la no manipulación de los datos de entrada, los datos procesados y de salida, además la OTIC deberá definir los roles y perfiles de acceso.
19. El jefe de la OTIC definirá y estructurará repositorios especiales de almacenamiento con la documentación de los Sistemas de Información y/o aplicaciones y/o base de datos, Servidores, Switche, Router, Seguridad, y en general de toda la arquitectura de TI de la entidad con restricción de acceso acorde con los roles y perfiles autorizados.
20. La OTIC deberá implementar controles de detección y prevención contra códigos maliciosos, así como los procesos de capacitación para concientizar a los usuarios de la entidad.
21. La OTIC deberá implementar el uso de técnicas criptográficas, para proteger la confidencialidad, integridad, la autenticidad y no repudio de la información confidencial y sensible de la entidad para garantizar el intercambio de información seguro entre diferentes actores.
22. La entidad debe disponer de una política de protección de datos personales tanto para gestión interna como para la publicación e intercambio de información en formatos y portales de información de la entidad. La Secretaria General será la encargada de estructurar la política y presentarla al comité institucional de gestión y desempeño para su aprobación.
23. La entidad prohíbe el envío de correos masivos o réplicas de cadenas de información al interior y al exterior de la entidad desde cuentas no autorizadas para este fin.
24. La entidad a través de un trabajo coordinado entre la OTIC, el Grupo de Gestión Documental y la Oficina Asesora Jurídica, con la participación de los jefes de dependencia deberán clasificar la información en el catálogo de activos de información de que habla la ley 1712 de 2014, así como definir el procedimiento para el manejo de la información más sensible o crítica, es decir la información de mayor riesgo.

25. La OTIC implementará de manera gradual el uso de firmas digitales, para el tratamiento de los procesos de gestión documental, expedientes electrónicos, resoluciones, correos electrónicos relevantes, así como de los demás procesos de la entidad que lo requieran.
26. La OTIC deberá establecer los lineamientos para la actualización de parches de seguridad de todos los aplicativos o software implementados en la entidad.
27. La entidad a través de la OTIC deberá definir los lineamientos y articularse con las dependencias responsables para el manejo de la mensajería electrónica y el intercambio de datos electrónicos., así como la integridad y disponibilidad de la información publicada electrónicamente a través de sistemas disponibles al público.
28. La entidad a través del oficial de seguridad y la Oficina Asesora Jurídica determinará el acceso y manejo de la información clasificada y más sensible para la entidad.
29. La OTIC deberá establecer el control para registrar las actividades tanto de los operadores como de los administradores de los sistemas y de la plataforma tecnológica de la entidad, a través de los registros de auditoria, donde se puedan monitorear las acciones y deje el registro del usuario, fecha y hora, inicio y cierre, registro de intentos de rechazo al sistema, a los datos, cambios de configuración del sistema, uso de utilidades y aplicaciones, alarmas del sistema.
30. La Secretaría General, con el apoyo de La OTIC debe establecer los lineamientos para el almacenamiento de la información relacionada con los procesos de contratación de la entidad de tal forma que se guarde los documentos fuente para su posterior utilización.
31. La entidad a través de la OTIC debe garantizar que las pasarelas de pago dispuestas por la entidad para los pagos realizados por los vigilados a través de comercio electrónico (pagos por PSE) cumpla con los protocolos de seguridad como lo son SSL/TLS.
32. La OTIC debe disponer de herramientas de monitoreo de los sistemas de información y base de datos, que permitan realizar monitoreo preventivo y reactivo.
33. La OTIC deberá monitorear el uso de los servicios de procesamiento de información, de cuentas privilegiadas, administradores, supervisores, acciones fallidas, fecha y hora de eventos, tipo de evento, archivos accesados, alertas o fallas del sistema, cambios en seguridad del sistema.
34. La OTIC debe generar el registro de las fallas reportadas por los usuarios, o novedades de procesamiento de información y de los sistemas de comunicación, y procedimiento, además deberá documentar la solución a fallos y restauración, para la aplicación de buenas prácticas y de lecciones aprendidas.
35. La OTIC deberá sincronizar todos los relojes de todos los sistemas de procesamiento de información, con la hora legal colombiana, para garantizar

los registros de auditoria que pueden ser necesarios para investigaciones o evidencias en casos disciplinarios o legales.

9.7 LINEAMIENTOS DE COPIAS DE SEGURIDAD

1. La OTIC debe generar backup y copia de seguridad de la información de la entidad, además deberá generar backup de las aplicaciones incluyendo, del código fuente, en las diferentes versiones, manuales de usuario final, de administración, operación y de instalación.
2. La OTIC debe definir los procedimientos de restauración y copias de respaldo de toda la información que maneja la entidad, además es importante identificar la información más crítica de la operación y definir periodicidad de respaldo, así como el tiempo de resguardo del backup.
3. La OTIC definirá un estándar para la rotulación y reutilización de cintas de backups, lo cual deberá quedar establecido en el procedimiento de respaldo y backups de la entidad.
4. La OTIC deberá realizar un análisis de la información que se genera y se procesa para definir la periodicidad con la que se realizará la copia de seguridad incremental, completa o diferencial, y se deberá establecer el procedimiento respectivo.
5. La OTIC deberá efectuar análisis periódico de los sistemas de información críticos y de la data que se debe procesar, para implementar el procedimiento de backup, así como el repositorio de los sistemas de información en caso de restauración de los sistemas.
6. La OTIC definirá el procedimiento de recuperación de fallas y restauración de backup.
7. La OTIC junto con cada dependencia deberá identificar los activos más críticos para la entidad y dar un tratamiento especial, el cual será definido en el Plan de Continuidad del Negocio.
8. La OTIC deberá generar respaldos de la información más crítica para la entidad adicionales a la copia de respaldo en cinta o unidades de almacenamiento en un servicio de nube como plan de contingencia y continuidad del negocio.
9. La OTIC deberá etiquetar las copias de seguridad y llevará un registro de los soportes sobre los que se ha realizado alguna copia, de acuerdo con el procedimiento establecido.
10. La OTIC definirá el procedimiento de restauración de la información a partir de copias de seguridad, el cual deberá ser probado y revisado cada 6 meses.
11. La OTIC debe controlar el acceso a las copias de seguridad, solo podrá tener acceso a los backups de la información el personal autorizado definido en el procedimiento para tal fin.

9.8 LINEAMIENTOS PARA EL CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN. SERVICIOS DE INFORMACIÓN E INFRAESTRUCTURA TECNOLÓGICA DE LA ENTIDAD.

1. La OTIC debe definir los perfiles, roles y permisos de acceso, a los activos de información de la entidad. La solicitud y autorización de acceso se debe enviar a través de la plataforma de mesa de servicio autorizando a los encargados de cada dependencia, indicando: periodo autorizado, función, perfil y roles.
2. El jefe de la OTIC y el oficial de seguridad deben establecer las funciones y reglas de control de acceso tanto para solicitud, autorización, administración y retiro de estas; en los Sistemas de información, base de datos, servidores, y toda la plataforma tecnológica de la entidad.
3. La OTIC definirá el procedimiento para el registro y cancelación de usuarios. El jefe de cada dependencia a través de la herramienta mesa de servicio realizará la autorización de los usuarios y el rol que manejan para que la OTIC otorgue o elimine los permisos de acceso según sea el caso.
4. El jefe de la OTIC y el Oficial de Seguridad deberán restringir y controlar la asignación de roles y privilegios, al grupo de funcionarios y contratistas de la OTIC, y deberá quedar documentado por qué se les autoriza el acceso a sistemas operativos, base de datos, sistemas de información e infraestructura y hacerlos efectivos a través del directorio activo.
5. El oficial de seguridad de la entidad y el jefe de OTIC, deberán efectuar una revisión detallada en los activos de información respecto a permisos y roles asignados a los integrantes de la OTIC. Los permisos y roles asignados a los integrantes de la OTIC deben quedar registrados como solicitud a través de la herramienta de mesa de servicio y aprobados por este medio.
6. La OTIC deberá efectuar un análisis de actividad de los usuarios, realizar la actualización mensual de novedades, retiros y cambios a través del directorio activo.
7. El jefe de OTIC y el oficial de seguridad deben definir lineamientos para autorización, revisión, cambios y retiro de derechos de acceso a la información.
8. La OTIC debe estructurar un procedimiento de gestión y asignación de contraseñas, así como la parametrización de caducidad de las claves de acceso.
9. La OTIC debe establecer el procedimiento de revisión máximo cada seis meses de los derechos de acceso de los usuarios de toda la entidad.
10. La OTIC debe concientizar a los usuarios sobre sus responsabilidades con relación al uso de contraseñas y la seguridad del equipo de trabajo asignado, así como exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en el uso de las contraseñas.
11. Los funcionarios y contratistas deberán bloquear la sesión al ausentarte del puesto de trabajo y apagar el equipo al finalizar la jornada laboral.

12. Los funcionarios y contratistas deben conservar su escritorio libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento, con el fin de reducir el riesgo de acceso no autorizado, daño o eliminación de información.
13. La OTIC debe programar el bloqueo automático, bloqueo de pantallas de los equipos de trabajo después de un periodo de 5 minutos de inactividad.
14. La OTIC a través del administrador del Directorio Activo debe generar reportes periódicos de inactividad de equipos o de no logueo en el directorio activo y deberá actualizar los derechos de acceso a la red periódicamente, así como la lista de usuarios, periodo de activación, roles y perfiles, y autorización de acceso. Dichos reportes deberán ser analizados por el Oficial de Seguridad para tomar las acciones correspondientes.
15. La gestión de contraseñas deberá tener en cuenta los siguientes lineamientos:
    - El usuario debe cambiar la contraseña en la primera vez de uso.
    - La contraseña debe tener como mínimo 8 caracteres.
    - Se generará a través del directorio activo de manera automática la solicitud de renovación de credencial de acceso cada 60 días.
    - No deben contener el nombre de cuenta del usuario o partes del nombre
      completo del usuario en más de dos caracteres consecutivos.
    - La contraseña debe incluir: mayúsculas, minúsculas, dígitos del 0 al 9 y caracteres especiales o alfanuméricos. (!, $, #, %).
16. La OTIC debe conservar un registro de contraseñas de usuarios y evitar su reutilización antes de 6 meses.
17. Los funcionarios y contratistas deben mantener la confidencialidad de las contraseñas, y no deben compartir los usuarios y contraseñas, estos son de uso personal. Los usuarios deberán evitar conservar registros de las contraseñas en papel, post it en los escritorios y/o archivos digitales dentro del equipo.
18. La OTIC debe definir las reglas de acceso y conectividad, así como los riesgos del uso de los dispositivos móviles (portátiles, teléfonos móviles).
19. Los funcionarios y contratistas deberán guardar la copia de seguridad de la información en el servicio de nube contratado por la entidad.
20. Los funcionarios y contratistas deberán evitar mantener información de la entidad en los dispositivos móviles.
21. Los funcionarios y contratistas deberán evitar el uso de redes públicas desde equipos asignados por la entidad.
22. La OTIC debe implementar el doble factor de autenticación para el ingreso a la plataforma tecnológica de la entidad o servicios contratados.
23. Los jefes de dependencia deben informar a la OTIC los cambios de dependencia de sus funcionarios y contratistas para modificar los roles y permisos de los aplicativos y carpetas compartidas a los que tiene acceso.

24. Los funcionarios y contratistas tendrán acceso solo a las aplicaciones y recursos que requiera para realizar su trabajo, dependiendo del rol que desempeñe en la entidad. Se detallarán las aplicaciones colaborativas y de teleconferencia permitidas, así como sus condiciones de uso evitando utilizar programas no autorizados.

9.9 LINEAMIENTOS PARA EL TRABAJO REMOTO

La entidad para la gestión de trabajo remoto establece los siguientes lineamientos, con el fin de garantizar la seguridad de la información:

1. La OTIC debe establecer métodos apropiados de autenticación para controlar el acceso de usuarios remotos, a través de soluciones de red privada virtual VPN y garantizar el trabajo remoto desde casa.
2. Los funcionarios y contratistas si hacen uso de equipos personales para acceder a la información o aplicaciones de la entidad deberán contar con un antivirus en sus equipos y mantenerlo actualizado, además de habilitar el cortafuegos de los equipos personales (firewall) y dar consentimiento para la instalación del software necesario para establecer la conexión (VPN).
3. La OTIC deberá tener la capacidad de conocer la trazabilidad de la información que se acceda a través de la conexión (VPN), mediante una herramienta especializada para tal fin.

9.10 LINEAMIENTOS DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

1. La OTIC debe definir la arquitectura de seguridad de referencia la cual contiene lineamientos que debe ser tenidos en cuenta en el diseño, desarrollo, implementación o adquisición de cualquier sistema de información.
2. La OTIC debe implementar los controles apropiados para los sistemas de información, para garantizar el procesamiento correcto de los datos de entrada, procesamiento interno y datos de salida.
3. La OTIC deberá exigir o implementar el cifrado de contraseñas y prácticas de hardcode (código quemado) de contraseñas dentro del código de las aplicaciones.
4. Todos los códigos fuentes de las soluciones de software de la entidad deben estar en un repositorio de control de versiones, al cual solo tiene acceso el líder de desarrollo, el arquitecto de software y los desarrolladores de la OTIC, para garantizar la seguridad de los archivos del sistema.
5. La actualización de software operativo, las aplicaciones y las librerías de los programas solo podrán ser actualizadas por la OTIC.

6. Todas las aplicaciones de cara al ciudadano o aplicaciones web deben poseer certificados de seguridad digital, certificado SSL.
7. La OTIC debe conservar en el repositorio de control de versiones, las versiones anteriores del software de aplicación como medida de contingencia.
8. La entidad no utilizará data con información sensible.
9. La OTIC debe definir e implementar un procedimiento para gestión de cambios.
10. La para la ejecución de pruebas de software la OTIC deberá supervisar y monitorear el desarrollo de software contratado externamente, se deberán definir los acuerdos sobre licencias, propiedad del código fuente y propiedad intelectual.
11. La OTIC deberá definir las certificaciones de calidad del trabajo realizado y la definición de las pruebas de seguridad antes de la instalación, para detectar código maliciosos y troyanos.
12. La OTIC deberá efectuar como mínimo una vez al año prueba de vulnerabilidad técnicas de los sistemas de información que tenga en uso la entidad y para los sistemas de información de terceros adquiridos por la entidad o que presten algún servicio y definir las acciones para tratar los riesgos identificados.
13. La OTIC debe establecer el inventario actual de los activos de información (sistemas de Información y Bases de datos) el cual debe incluir la siguiente información: proveedor, versiones, estado actual, responsables.
14. Todos los sistemas de información y bases de datos deben poseer opciones de auditorías habilitadas incluyendo: validación periódica de logueo de usuarios, cambios realizados, intrusiones no autorizadas, atención de novedades.

9.11 LINEAMIENTOS PARA LA GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

Se deberán establecer los lineamientos para detectar, prevenir, reportar y gestionar los incidentes de seguridad y privacidad de la información que se presenten en la entidad.

1. El Oficial de seguridad en conjunto con las dependencias de la entidad será el encargado de identificar los roles y responsabilidades en la detección, evaluación, prevención y gestión de los incidentes de seguridad de la información para garantizar la continuidad de los servicios más importantes de la entidad.
2. De acuerdo con el plan de gestión de incidentes de la entidad, la OTIC creará el equipo de trabajo de seguridad para la atención de incidentes; conformado por las siguientes personas: Un (1) representante del grupo de infraestructura y telecomunicaciones, un (1) representante del grupo de sistemas de información y desarrollo, el jefe de la OTIC, el oficial de seguridad con el fin

de detectar, evaluar y gestionar los riesgos, amenazas y vulnerabilidades de los activos de seguridad de la información más críticos para la operación de la entidad (OTIC).

3. La OTIC establece como canal de comunicación el correo electrónico con los centros especializados (Csirt, Colcert, centro cibernético policial C4, CCOC) y ejecutará las recomendaciones efectuadas en temas de seguridad con el fin de prevenir y mitigar los riesgos; así como el manejo adecuado de los activos más críticos para la entidad.
4. La OTIC Implementará lecciones aprendidas y retroalimentación de los casos más frecuentes y comunes de ciberataques y ciberamenazas como mecanismos de prevención.
5. El oficial de seguridad de la entidad o el que haga sus veces reportara al Csirt cualquier ataque que se presente en un lapso no mayor a 3 horas a través de los canales dispuestos para tal fin.

9.12 LINEAMIENTOS PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

1. La OTIC con la participación de los jefes de dependencia deberá definir e implementar un Plan de gestión de continuidad del negocio, el cual incluirá el tema de seguridad de la información.
2. Todas las dependencias de la entidad con la orientación y liderazgo de la OTIC deben identificar los riesgos que puede enfrentar en términos de probabilidad de ocurrencia e impacto en el tiempo, determinando los procesos más críticos de la entidad.
3. La OTIC debe construir un matriz de riesgos donde se visualicen los impactos que puede generar las interrupciones causadas por incidentes de seguridad de la información.
4. La entidad a través de la OTIC debe identificar e implementar controles preventivos y de mitigación de incidentes de seguridad.
5. La OTIC debe estructurar los procedimientos para la continuidad de los servicios de operación y servicios de procesamiento de información.
6. La OTIC deberá desarrollar e implementar los procedimientos para mantener o recuperar las operaciones y asegurar la información, después de la interrupción o falla de los procesos críticos de la entidad.
7. La OTIC será la encargada de documentar el plan de continuidad del negocio para la OTIC, efectuar pruebas y actualizaciones periódicas como mínimo una vez al año.
8. La OTIC debe fijar las condiciones para activación del plan, los procedimientos de emergencia que se deben iniciar, los procedimientos de respaldo, procedimientos operativos, procedimientos de reanudación y los responsables de la ejecución de estos.

9.13 LINEAMIENTOS DE INTEROPERABILIDAD E INTERCAMBIO DE INFORMACIÓN

1. La OTIC debe establecer e implementar las características de seguridad que debe cumplir los servicios de información, para interactuar con la Plataforma de Interoperabilidad del Estado colombiano.
2. La entidad deberá tener como referencia la arquitectura sugerida por MINTIC para la implementación de los servicios de intercambio de información mediante servicios web, es decir deberá estar orientada a la exposición y consumo de servicios de intercambio de información mediante servicios WEB tipo SOAP o REST.
3. La entidad a través de la OTIC deberá realizar el intercambio de los conjuntos de datos susceptibles a interoperar mediante servicios de intercambio de información integrados a la plataforma de interoperabilidad del Estado (PDI), con la herramienta X-Road para garantizar la seguridad en el intercambio de información de los servicios que se exponen a otras entidades.
4. La OTIC debe documentar y definir el diagrama de interoperabilidad con otras entidades el cual debe contener: Servicios que expone el sistema, y su relación con los sistemas internos y externos que lo usan, así como los Servicios expuestos por otros sistemas internos o externos, y su relación con el sistema de información que se está diseñando.
5. Para cada servicio expuesto o usado, la OTIC debe definir el tipo de integración: archivos planos, webservices, acceso a base de datos, ETL, EAI.
6. Se deberá garantizar a través de la OTIC la calidad, seguridad, disponibilidad, accesibilidad, e interoperabilidad de la información y de los servicios de información expuestos y/o publicados por la entidad.
7. La OTIC debe definir el procedimiento para intercambio de información a través de la plataforma X-Road u otros mecanismos, definir los lineamientos y protocolos para la interoperabilidad con las entidades. Estructurar los acuerdos con las entidades del sector, esquema de comunicación y de intercambio de información.
8. La OTIC debe documentar y definir el diagrama de interoperabilidad con otras entidades, para sistemas de información, establecer la vista de los servicios que expone la entidad y que son consumidos por otras entidades, incluyendo el nombre de la entidad que expone el servicio y la entidad que lo usa, los nombres del sistema que expone el servicio y el sistema que lo usa, el nombre del servicio y el tipo de integración.

9.14 LINEAMIENTOS PARA TERCEROS U OUTSOURCING

1. La entidad a través de la OTIC con la participación de los jefes de dependencia deberá controlar y gestionar toda relación con proveedores, en particular aquellos que tienen acceso a la información y garantizar que estará suficientemente protegida con base a los acuerdos de confidencialidad y contratos correspondientes.
2. La protección de la información debe contemplarse antes, durante y a la finalización del servicio prestado.
3. La entidad a través de los jefes de dependencia debe asegurar que los productos y servicios contratados cumplen con la política de seguridad y privacidad de la Información definida y aprobada por la entidad.
4. La entidad a través de la OTIC con la participación de los jefes de dependencia deberá definir los requisitos mínimos de seguridad que deben cumplir los productos que se adquieren y los servicios que se contratan.
5. Se deberán establecer cláusulas contractuales en materia de seguridad de la información en los contratos celebrados con proveedores o terceras personas. Esta actividad estará a cargo de la Secretaria General y la Oficina Asesora Jurídica.
6. Para los servicios contratados, la superintendencia de Transporte a través de la Secretaria General o la OTIC según el servicio que se adquiera, debe establecer los acuerdos de nivel de servicio – ANS.
7. La OTIC determinará los controles de seguridad de obligatorio cumplimiento por parte de los proveedores de servicios tecnológicos.
8. La superintendencia de transporte a través de la OTIC deberá garantizar la seguridad de la información tras la finalización de un servicio o contrato.
9. En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios o sanciones, por el no cumplimiento de las políticas de seguridad de la información. Esta actividad estará a cargo de la Secretaria General y la Oficina Asesora Jurídica.
10. La OTIC deberá identificar los riesgos de la información y los servicios de procesamiento de información, así como mitigar los riesgos de seguridad referente al acceso de los proveedores y/o contratistas a los sistemas de información.
11. Los proveedores y/o contratistas deben informar de manera inmediata al supervisor del contrato de cualquier brecha o incidente de seguridad, que pueda comprometer los activos de información de la entidad.

9.15 LINEAMIENTOS PARA CORREO Y DOCUMENTOS ELECTRÓNICOS

1. La OTIC debe establecer los lineamientos de uso permitido y seguro del correo electrónico corporativo y generación de documentos electrónicos que

sirva para impedir errores, incidentes, usos ilícitos y para evitar ataques cibernéticos por esta vía.

2. La OTIC deberá crear campañas y capacitaciones de concientización para todos los empleados de la entidad para que hagan uso seguro de los correos y documentos electrónicos.
3. La OTIC instalará y activará aplicaciones antimalware y filtros antispam en la plataforma tecnológica que utiliza la entidad.
4. La OTIC deberá implementar una tecnología de cifrado y firma digital que se pueda usar con los documentos y correos electrónicos para proteger la información confidencial y asegurar la autenticidad del funcionario y/o contratista que por su rol requiera firmar documentos y estén autorizados.
5. La OTIC deberá desactivar el formato HTML y la ejecución de macros para una protección adicional de las cuentas de correo electrónico.
6. Los funcionarios y contratistas no deben usar el correo electrónico con fines personales.
7. Los funcionarios y contratistas deben revisar cuidadosamente los adjuntos de correos de remitentes desconocidos antes de abrirlos. Si sospechan de su autenticidad, no lo deben descargar ni abrir y deben reportarlo a OTIC.
8. Los funcionarios y contratistas tienen prohibido remitir información confidencial o sensible de la entidad a sus correos personales.
9. Toda información y documentos generados por la entidad y que sean distribuidos en los canales de comunicación, deben ser autorizados por los jefes de dependencia para ser socializadas y con un vocabulario institucional.
10. La asignación de cuentas de correo electrónico deberá ser autorizado por el jefe inmediato o supervisor del contrato a través de la herramienta de mesa de servicio.
11. La OTIC, deberá establecer el tamaño para cada buzón de correo electrónico, es decir un espacio en el servidor de correo, destinado al almacenamiento de mensajes electrónicos de cada usuario. Se deberá informar a los usuarios la capacidad asignada.
12. Todos los documentos y correos electrónicos enviados por funcionarios y contratistas deben contener una firma de acuerdo con el estándar y la información definido por la dependencia de comunicaciones.
13. Cuando un funcionario requiere ausentarse de la entidad por un periodo superior de tiempo vacaciones, incapacidad) debe programar el correo electrónico para que automáticamente responda a los remitentes indicando fecha de llegada, nombre y dirección de correo electrónico de la persona encargada durante su ausencia.
14. Solo el jefe de la OTIC podrá autorizar él envió de correos masivos, los jefes de cada dependencia deberán efectuar las coordinaciones respectivas con OTIC.

10 PROCEDIMIENTO PARA ACTUALIZAR LA POLÍTICA

1. La actualización de la política de seguridad y privacidad de la información estará a cargo de la oficina de tecnologías de la información y las comunicaciones en cabeza del oficial de seguridad con la colaboración de las demás dependencias de la entidad.
2. Los jefes de dependencia o líderes de los procesos deberán informar la necesidad de ajustar algún lineamiento o procedimiento de seguridad y privacidad de la información al jefe de la OTIC a través de herramienta de mesa de servicio.
3. El comité institucional de gestión y desempeño tendrá la potestad de aprobar la actualización y/o modificación de la política de seguridad y privacidad de la Información y una vez sea aprobada ésta deberá quedar aprobada y en firme por el director de la entidad.

11 SANCIONES E INCUMPLIMIENTO

La política de seguridad y privacidad de la información y sus lineamientos deberán ser adoptadas como herramienta de obligatorio cumplimiento, estas declaran la información necesaria que permite a los funcionarios y contratistas hacer un acceso y uso apropiado de los recursos informáticos de la Superintendencia de Transporte.

EL incumplimiento de la política de seguridad y privacidad de la Información y los lineamientos establecidos dará lugar a la aplicación acciones disciplinarias incluyendo la terminación del contrato, acción civil y penal, que, en su caso, puedan resultar aplicables.

El Grupo de Talento Humano y/o Control Interno Disciplinario definirá y hará cumplir la respectiva sanción administrativa para los funcionarios y contratistas que incurran en cualquiera de los siguientes delitos y/o violaciones de seguridad informática utilizando la información y los recursos tecnológicos de la entidad. Las sanciones según la tipificación del delito serán publicados y socializados a toda la entidad e incorporados en esta política, cuando se definan:

1. Acceso no autorizado a la información.
2. Destrucción de Datos o archivos o informes.
3. Infracción de los derechos de autor.
4. Interceptación de e-mail.
5. Estafas electrónicas.
6. Transferencias de fondos en forma ilegal.
7. Delitos convencionales como espionaje, terrorismo, narcotráfico, proselitismo de sectas, propaganda de grupos extremistas.
8. Uso indebido de los activos de información asignados.
9. Accesos a páginas de contenido no apto, o promueva el uso de éstas desde los equipos de la entidad.
10. Participar de juegos en línea a través de la red.
11. No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
12. Dejar información pública reservada y privada, en carpetas compartidas.
13. No guardar de forma segura o extraviar la información en formato físico o digital que se le entrega a un funcionario o contratista en el ejercicio de sus funciones.
14. Dejar los computadores (de escritorio y portátiles) encendidos una vez finalizada la jornada laboral, sin que medie una justificación.
15. Enviar información pública reservada o información pública clasificada por correo, copia impresa o electrónica sin la debida autorización.

16. Usar dispositivos de almacenamiento externo en los computadores y extraer información sin autorización otorgada por la OTIC.
17. Compartir con otros funcionarios o personal externo a la entidad las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la entidad.
18. Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
19. Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas
20. Realizar cambios no autorizados en la plataforma tecnológica de la entidad o manipular datos o cifras que alteren la información oficial.
21. Acceder, almacenar o distribuir pornografía infantil.
22. Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por la OTIC.

La Superintendencia de Transporte deberá ejecutar las acciones disciplinarias para los funcionarios y contratistas que violen la política de protección de datos personales y los lineamientos de la política de seguridad y privacidad de la información.

12 EXCEPCIONES

Toda solicitud de excepción de alguno de los lineamientos establecidos en la política de seguridad y privacidad de la información debe ser solicitada por los jefes de dependencia, al jefe de la OTIC, con la debida justificación y documentación conforme a la naturaleza de su cargo.

El jefe de OTIC y el oficial de seguridad deberán realizar la evaluación del alcance solicitado y el impacto de dicha excepción, la cual deberá quedar documentada y aprobada por las partes involucradas donde asumen el riesgo que conlleva la aceptación de la excepción.

En caso ser necesario la evaluación de la excepción puede incluir a la Oficina Asesora Jurídica, la Oficina Asesora de Planeación y la Secretaría General. En estos casos la Oficina OTIC definirá la necesidad del acompañamiento de las dependencias.

1. Control de cambios

Versión	Fecha	Descripción del cambio
1	13-Oct-2020	Versión Original en Formato del Sistema de Gestión creado para tal efecto.

5. Aprobación del documento

Etapa	Nombres y apellidos	Cargo
Elaboró	Milena Katherine Malagón	Contratista -Oficina de Tecnologías de la información y las Comunicaciones
Revisó	Claudia Milena Rodríguez	Asesor Despacho del Superintendente de Transporte
Aprobó	Javier Pérez Pérez	Jefe Oficina de Tecnologías de la Información y las Comunicaciones