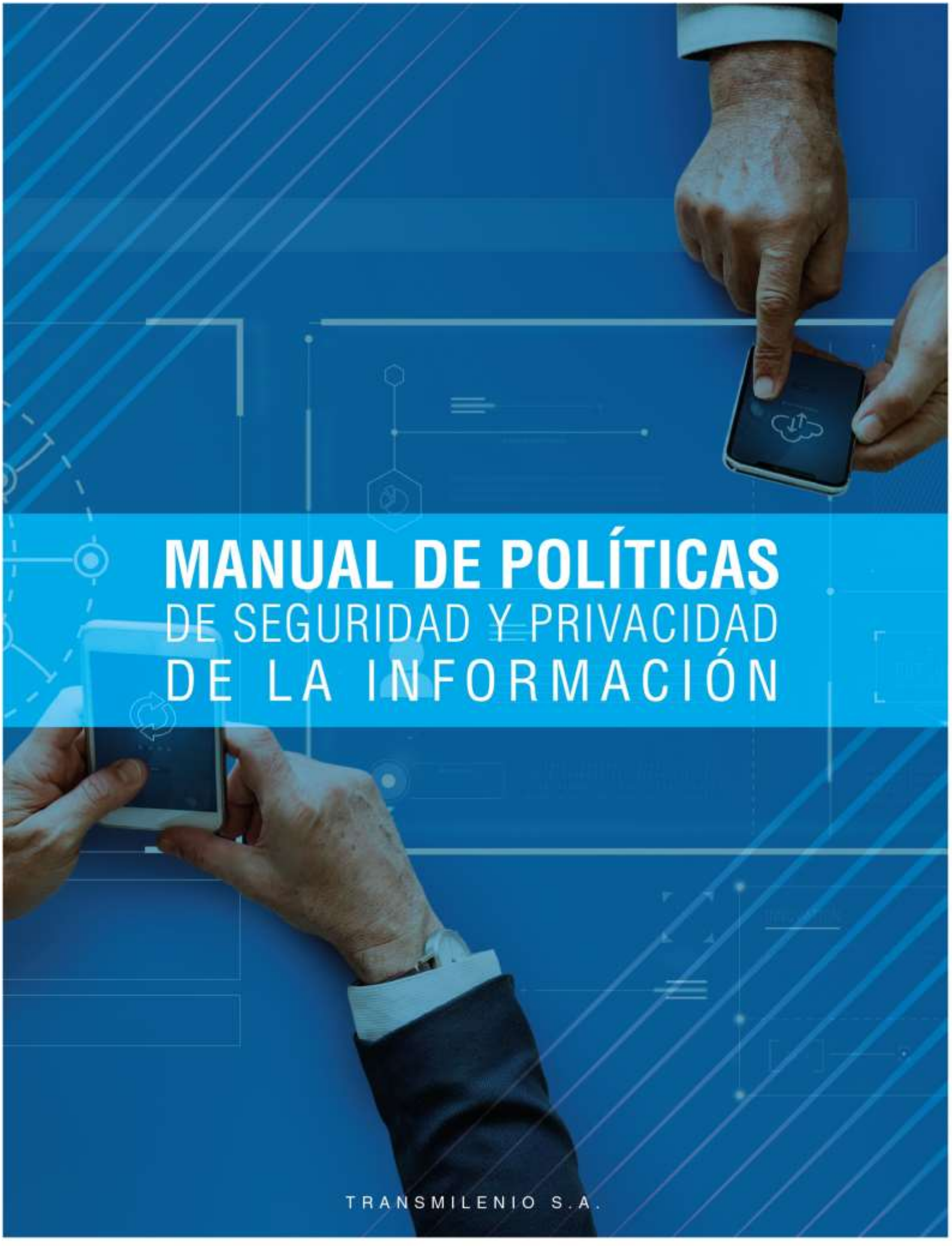

MANUAL DE POLÍTICAS
DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TRANSMILENIO S.A.

TABLA DE CONTENIDO

MODIFICACIONES:

VERSION	FECHA	CAMBIO	SOLICITO
0	01-05-2016	Primera versión Oficial del documento	N/A
1	30-03-2017	Se eliminan No. 6.3 Compromisos de la dirección y No. 6.5.2. "Normas que rigen para la estructura organizacional de seguridad de la información". Se realiza la construcción de procedimientos que complementen y fortalezcan el manual respecto a los numerales "8.6.1.3 Proceso disciplinario" "8.7 Gestión de activos" "8.7.5 Manejo de los soportes de almacenamiento"	Dirección de TICs
2	25-07-2018	Se cambia el título de manual de políticas de seguridad de la información, por políticas de seguridad y privacidad de la información. Se realiza cambio estructural y de contenido, al Manual de políticas de seguridad y privacidad de la información, de acuerdo con la normatividad vigente y los riesgos existentes en las organizaciones	Dirección de TICs
3	26-03-2019	Se incluyen las referencias a los siguientes Procedimientos y Protocolos. • Procedimiento: P-DT-012: Procedimiento para el Intercambio Seguro de la Información Electrónica • Protocolo: T-DT-001: Protocolo para la Revisión de Informes de Interventoría al Contrato de Concesión SIRCI. • Protocolo: T-DT-003: Protocolo a Seguir para Gestionar el Uso de los Medios Removibles Se realiza el ajuste del Numeral 9.2.2.4 Eliminación de los medios. Donde se elimina la referencia al nivel 7 dado que esto excede los tiempos de respuesta y el borrado puede efectuarse con herramientas más rápidas.	Dirección de TICs

VERSION	FECHA	CAMBIO	SOLICITO
		Se realizó el ajuste del numeral 9.5 Política de seguridad en las operaciones. donde se agregaron las políticas relacionadas con los registros de auditoria. Numerales n) al r). Lo anterior de acuerdo con lo requerido por la Norma ISO 27001:2013.	

INTRODUCCIÓN

La adopción de políticas, y procedimientos en TRANSMILENIO S.A., obedece a una decisión estratégica que cumple con las normas de seguridad y privacidad de la información. Éstas deben analizarse, diseñarse e implementarse para satisfacer las necesidades, los objetivos, los requisitos de seguridad, los procesos, el tamaño, la tecnología y la estructura de la entidad.

En la actualidad, TRANSMILENIO S.A. identifica la información como uno de los activos indispensables en la conducción y consecución de los objetivos definidos en el Plan Estratégico de la Entidad, razón por la cual es necesario establecer un marco en el cual se asegure que la información es protegida de manera adecuada independientemente del medio en la que ésta sea manejada, procesada, transportada o almacenada. Adicional a lo expuesto, en la medida en que los sistemas de información se constituyen en un apoyo de los procesos de la Entidad, se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de la información.

El presente documento describe la política institucional de seguridad de la información y las políticas generales definidas por TRANSMILENIO S.A., las cuales se constituyen en un insumo fundamental del Sistema de Gestión de Seguridad de la Información y se convierten en la base para la implantación de los controles, procedimientos, guías y estándares definidos.

Este documento es de propiedad de TRANSMILENIO S.A., las actualizaciones se publicarán internamente en la herramienta de Gestión documental y cuando existan cambios, oficializados y aprobados por la Oficina Asesora de Planeación y por el profesional especializado grado 06 de Seguridad de la Información de la Dirección de TICs, éste último realizará el cambio siguiendo el procedimiento establecido para tal fin. Dicha información se hará conocer a cada uno de los funcionarios y contratistas a través de los sistemas de divulgación establecidos para tal fin. (Intranet, correo electrónico, charlas de sensibilización).

1. OBJETIVO

Establecer y comunicar las políticas complementarias alineadas a la política de alto nivel del Sistema de Gestión de Seguridad de la Información - SGSI de TRANSMILENIO S.A., en pro de gestionar adecuadamente la integridad, confidencialidad y disponibilidad de los activos de información, en el marco de la norma NTC/ISO 27001:2013 y su Anexo A.

2. APLICACION

El presente Manual de políticas complementarias de seguridad de la información hace parte integral del modelo de seguridad adoptado por TRANSMILENIO S.A., y establecido en el Manual del SGSI.

Las políticas de Seguridad de la Información definidas por la Entidad han sido orientadas para todos los funcionarios públicos, oficiales, proveedores, contratistas y terceras partes que dependan o interactúen con la entidad, que desarrollen labores de asesoría, consultoría, implementación en términos de seguridad de la información.

3. RESPONSABLES

El Profesional Especializado (06) de Seguridad de la Información de la Dirección de Tics es el responsable por la elaboración y mantenimiento de este documento y el director(a) de la Dirección Técnica de Tics de TRANSMILENIO S.A. de su cumplimiento, implementación y mantenimiento.

Todos los funcionarios públicos adscritos a TRANSMILENIO S.A., en sus diferentes procesos y dependencias, son responsables por la aplicación y cumplimiento del presente manual de políticas de seguridad y privacidad de la información, en cuanto tengan bajo su custodia o responsabilidad de información y los medios de procesamiento de información (sistemas de información o aplicativos) de la Entidad.

4. DEFINICIONES

Acción correctiva: acción tomada para eliminar la causa de una no conformidad detectada u otra situación no deseable.

Activo de información: todo aquel recurso del Sistema de Seguridad de la Información ISO 27001, necesario para que la empresa funcione alineado con las políticas de seguridad de la información. Es

referido a todo aquel software o hardware o recurso humano en el que procesa, almacena o transmite información y que tiene un valor para la organización. Ejemplo: bases de datos, programas de computación, plataforma tecnológica (procesamiento de datos o comunicaciones), documentos impresos.

Administrador de bases de datos: un administrador de base de datos (DBA) dirige o lleva a cabo todas las actividades relacionadas con el mantenimiento de un entorno de base de datos y dentro de sus responsabilidades se incluyen el diseño, implementación y mantenimiento del sistema de base de datos; el establecimiento de políticas y procedimientos relativos a la gestión, la seguridad, el mantenimiento y el uso del sistema de gestión de base de datos; y la capacitación de los empleados en la gestión y el uso de las bases de datos.

Administración de usuarios: actividad mediante la cual se desarrollan las labores de creación, modificación, consulta, bloqueo, desbloqueo y eliminación de la cuenta de un usuario.

Análisis de riesgos: es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir en el desarrollo de una determinada actividad, abordándose una clasificación de los mismos y construyendo unos planes de acción para su tratamiento.

Almacenamiento: Se refiere a la forma en la que se almacena el activo, como en medios magnéticos, salas, cajas, PC's, Servidores, CD's, DVD's, USBs, Cintas magnéticas, etc.

Auditoría al sistema de gestión de seguridad de la información: examen sistemático e independiente para determinar sí las actividades y los resultados relacionados con la seguridad de la información cumplen disposiciones preestablecidas, y sí estas disposiciones se aplican en forma efectiva y son aptas para alcanzar los objetivos.

Autenticidad: es la propiedad de garantizar la identidad de un sujeto o recurso declarado, la autenticidad se aplica a entes tales como usuarios, procesos, sistemas e información.

Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.

Backup: es la copia total o parcial de información importante del disco duro, CD, bases de datos u otro medio de almacenamiento, la cual puede recuperarse en caso de pérdida de la copia original.

Cifrado: Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación (letras, símbolos o números) del contenido que solo pueden comprenderse si se dispone de la clave necesaria para descifrarlos).

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado. La información debe clasificarse en términos de sensibilidad e importancia para la entidad.

Complementario: hace referencia a todo aquel elemento, objeto, individuo o fenómeno que se caracteriza por unirse a otro elemento para completarlo y, en lo posible, mejorarlo.

Comité de seguridad: cuerpo integrado por representantes de todas las áreas de la Entidad, destinado a garantizar el apoyo a las iniciativas de seguridad de la información, para lograr un trabajo eficaz y seguro al interior de TRANSMILENIO S.A.

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Contraseña o palabra clave: serie secreta de caracteres que permite a un usuario tener acceso, a un archivo, computador o programa.

Cultura de seguridad de la información: es aquella red de significados, acciones, creencias y comportamientos que se asocian con la seguridad y control de la información, la cual define en sí misma la forma como una persona cuida y protege ese activo que representa esa figura valiosa para él y por ende para la organización.

Custodio: Persona delegada para ejercer el cuidado o vigilancia sobre un activo que le ha sido encargado.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Destrucción: Se refiere a la actividad para la destrucción de la información que se maneja sobre el activo en el momento en el que este finaliza su ciclo de vida:

- Incineración: Destrucción de información exponiéndola a altas temperaturas para quemarla.

- Borrado Seguro: Aplica solo para medio magnéticos, es un borrado a bajo nivel.
- Trituración: Esto aplica más que todo a la destrucción de papel por medio de máquinas trituradoras.

Dependencia: oficina o área de la entidad.

Directorio activo: es un repositorio que contiene información sobre las propiedades y la ubicación de los diferentes tipos de recursos dentro de la red distribuida de una empresa.

Dominio: Áreas en las que se desarrolla la NTC/ISO 27001.

Disponibilidad: es la característica o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Etiquetado: Colocar una etiqueta o rótulo para identificar un elemento.

Evento de Seguridad de la Información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Excepciones: Todo aquello que se excluye de la generalidad o regla común.

Firewall: es un computador, software o dispositivo físico que se conecta en una red con salida a internet con el fin de impedir el acceso no autorizado, incorporando elementos que garantizan la privacidad, autentificación y filtraje de contenidos, conforme a las políticas de seguridad de la información, de la entidad donde se instala.

Hardware (HW): son las partes físicas y tangibles de una computadora, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Incidente de seguridad de la Información: Un evento o serie de eventos de seguridad de la Información no deseados o inesperados, que tiene una la probabilidad significativa de comprometer las operaciones del negocio o amenazar la seguridad de la información de los activos críticos que almacenen, procesen y/o gestionen información.

Infraestructura de procesamiento de información: es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica o instalación física que los contenga.

Información: es un conjunto de datos acerca de un suceso, hecho, fenómeno o situación, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo. Información impresa, escrita, hablada y almacenada.

Integridad: es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización.

Intranet: red de computadores que utiliza la tecnología del protocolo de internet (IP) para compartir información, sistemas operativos o servicios de computación dentro de una organización, es de carácter interno, por lo que solo los miembros de esa organización tienen acceso a ella.

Inventario de activos: Listado de recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.)

Logs: registro de actividad del sistema, que permite referenciar información e indicadores sobre sesiones iniciadas, procesos ejecutados en equipos, conexiones externas, accesos y utilización de los recursos del sistema, intentos de violación de las políticas de seguridad, detección de ataques sistémicos o intentos de intrusión.

Medio de procesamiento de información: denominación genérica para todo aquel software o conjunto de aplicaciones de software, que hace de una computadora un elemento útil, debido a que posibilita al sistema para manejar una tarea específica. Pueden ser aplicaciones de propósito general, que pueden ser utilizados para una amplia variedad de tareas, como contabilidad, gestión documental, administración, procesamiento de texto, bases de datos, entre otros. Otros tipos de software se ajustan a la computadora para acoplarse a necesidades y operaciones específicas, como bancarias, de seguros, hospitales, manufactura, entre otros.

Misión crítica: se entiende por sistemas de misión crítica a aquellos servidores que ejecutan aplicaciones esenciales que, sí fallan, tienen un impacto significativo en el funcionamiento de cualquier empresa, organización o institución que dependa de su información.

Partes interesadas: son aquellos individuos o entes que influyen en el proceso de gestión de la seguridad de la información o son influenciados por él. Dentro del contexto del sistema de gestión de seguridad de la información se consideran como partes interesadas (stakeholders), usuarios internos, clientes, directivos, entre otros.

Perfil: conjunto de características que permiten establecer la identidad, así como las restricciones o permisos a que tiene derecho cada usuario cuando ingresa al sistema. Esta utilidad permite que el administrador del sistema asigne acciones, reportes u opciones del sistema que estarán visibles o disponibles para cada usuario o grupo de usuarios.

Personal: funcionarios, empleados contratados, consultores y contratistas.

Políticas: es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una Entidad teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

Política de seguridad de la información: establece a alto nivel los objetivos y metas relacionados con la seguridad de la información.

Propietario de la información: individuo, entidad o unidad de negocio que tiene la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información que le han sido asignados o de los que hace uso.

Proveedor: persona natural o jurídica que abastece a otras empresas o personas, con existencias de bienes o servicios, necesarios para el normal desarrollo de las actividades propias de esas personas o empresas.

Registro: documento que suministra evidencia objetiva de las actividades efectuadas o de los resultados alcanzados.

Rollback: en tecnologías de base de datos, un rollback o reversión es una operación que devuelve a la base de datos a algún estado previo.

Sistema de gestión de seguridad de la información (SGSI): conjunto de políticas, procedimientos, procesos y recursos, basado en un enfoque de riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión

incluye organigrama, políticas, planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos relacionados con la seguridad de la información.

Sistema integrado de gestión: es una herramienta de gestión que contribuye a aumentar el desempeño institucional a través de sus procesos, lo cual se ve reflejado en el mejoramiento continuo de la calidad de los servicios de la Entidad, en el cumplimiento de los objetivos institucionales con eficiencia, eficacia y efectividad, y en la satisfacción de las necesidades, intereses y expectativas de los clientes - usuarios, partes interesadas y grupos de interés.

Sistema integrado para la gestión de los organismos y entidades públicas, adoptado mediante el Decreto 652 de 2011 y el cual lo conforman el subsistema de gestión de la calidad (SGC), subsistema de control interno (SCI), subsistema de gestión ambiental (SGA), subsistema de seguridad y salud ocupacional (S&SO), subsistema de gestión de seguridad de la información (SGSI), subsistema interno de gestión documental y archivo (SIGA) y el subsistema de responsabilidad social (SRS).

Seguridad de la información: conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Sistema de información: “es aquel conjunto de componentes interrelacionados que capturan, almacenan, procesan y distribuyen la información para apoyar la toma de decisiones, el control, análisis y visión de una organización" (K y J Laudon).

Software: es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación. (Extraído del estándar 729 del IEEE5).

SSL: secure socket layer es un protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet.

Teletrabajador: Es la persona que utiliza las tecnologías de la información y comunicación como medio para realizar su actividad laboral fuera del local del empleador, en el marco de un contrato de trabajo o de una relación laboral dependiente, en la cual le sean garantizados todos sus derechos laborales.

Teletrabajo: Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo

Tercero o subcontratista: es el proveedor de un producto o servicio que afecta la calidad del servicio prestado por la empresa o que desarrolla labores de asesoría, consultoría, implementación, soporte o mantenimiento y demás personas que, sin ser de planta de la Entidad, tienen un nivel de vinculación o brindan algún tipo de servicio dentro de las instalaciones de TRANSMILENIO S.A.

TIC (tecnologías de la información y las comunicaciones): Es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las tecnologías de la información y las comunicaciones. Dentro de sus funciones está incrementar y facilitar el acceso de los usuarios de la organización a las tecnologías de la información, las comunicaciones y a sus beneficios.

UPS: sistema de alimentación ininterrumpida - uninterruptible power supply (UPS), es un dispositivo que gracias a un conjunto de baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica a todos los dispositivos que tenga conectados por un tiempo limitado y durante un corte del fluido eléctrico.

VPN: (Virtual Prívate Network) Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

Vulnerabilidad: debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

WEB: significa “red”, “telaraña” o “malla”. El concepto se utiliza en el ámbito tecnológico para nombrar a una red informática y, en general a Internet.

5. DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia de 1991:

Artículo 2.	Fines esenciales del Estado.
Artículo 6.	Responsabilidad de los servidores públicos.
Artículo 15.	Derecho a la Intimidad. Hábeas data.

Artículo 20.	Derecho a la información.
Artículo 74.	Libre acceso a documentos públicos.
Artículo 122	Desempeño de funciones públicas.
Artículo 123	Desempeño de funciones de los servidores públicos.
Artículo 209	Fines de la función administrativa.
Artículo 269	Métodos y procedimientos de control interno.
Artículo 284	Acceso a información reservada.

- **Ley 1273 de 2009:** por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
- **Ley 23 de 1982:** ley emitida por el Congreso de la República de Colombia, acerca de la Propiedad Intelectual y los Derechos de autor.
- **Ley 734 de 2002:** por la cual se expide el Código Disciplinario Único.
- **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
- **Ley 603 del 2000:** Por la cual se modifica el artículo 47 de la Ley 222 de 1.995**.**
- **Ley 1266 de 2008:** por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contendida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1581 de 2012:** por la cual se dictan disposiciones generales para la protección de datos personales, habeas data
- **Ley 1341 de 2009:** por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones acerca de la protección de los derechos de los usuarios.
- **Ley 1712 de 2014:** ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

- **Reglamento interno de trabajo de TRANSMILENIO S.A.:** documento que se establece como norma reguladora de las relaciones internas de la Empresa con los trabajadores adscritos a ella.
- **Decreto 2573 de 2014:** por el cual se reglamentan los lineamientos generales de la estrategia de gobierno en línea.
- **Decreto 1360 de 1989**: por el cual se reglamenta la inscripción de soporte lógico (software) en el registro nacional del derecho de autor.
- **Decreto 460 de 1995:** por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el depósito legal
- **Decreto 162 de 1995:** por el cual se reglamenta en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos.
- **Sentencia T-444 de 1992:** recolección de información por parte de los organismos de seguridad del Estado.
- **NTC- ISO-IEC-27001:** Sistema de Gestión de Seguridad de la Información "SGSI".
- **NTC- ISO-IEC-27002.** Técnicas de Seguridad. Código de prácticas para controles de la información".
- **NTC- ISO-IEC- 27005.** Guías sobre la gestión de riesgos".
- **NTC 5450-1-2006:** tecnología de la información, técnicas de seguridad, criterios de evaluación para la seguridad de tecnologías de la información (TI) "introducción y modelo general".
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL

6. POLITICA DE ALTO NIVEL DEL SGSI

La Política General de Seguridad de la Información enuncia el compromiso de la Alta Dirección de TRANSMILENIO S.A., de generar la estrategia corporativa a partir de lineamientos para la protección de la información involucrando tanto la información digital como física, a fin de ser conocidos, divulgados y cumplidos de forma obligatoria por todos los funcionarios públicos, oficiales, contratistas y stakeholders de TRANSMILENIO S.A., en la procura de prevenir, detectar y neutralizar de forma oportuna una posible fuga, pérdida o alteración no autorizada de información.

La política general de seguridad de la información tiene como objetivo la consolidación de una cultura de Seguridad de la Información al interior de la Entidad, que permita a su vez, brindar un apoyo directo al desarrollo e integración de los sistemas de transporte público masivo intermodal de pasajeros de la ciudad de Bogotá D.C., en cuanto al cuidado de la información como su activo más valioso.

Armonizados con el Plan Estratégico Institucional, la Entidad establece como Política de alto nivel del SGSI, la siguiente:

> ***"La información es reconocida por TRANSMILENIO S.A. como uno de los activos más importantes para lograr su objetivo fundamental de contribuir al desarrollo sostenido del sector movilidad , mediante la prevención, vigilancia y control , es por eso que se compromete a disponer sus recursos tanto físicos, tecnológicos, financieros, informativos, de conocimiento y humanos para liderar y fortalecer la seguridad de la información a través del establecimiento, implementación y mejora continua de un Sistema de gestión de seguridad de la información (SGSI); cuyo fin es el aseguramiento de la integridad, disponibilidad y confidencialidad de la información mediante la gestión y tratamiento adecuado de los riesgos, en el marco de los requisitos de la entidad, los legales o reglamentarios, y las obligaciones de seguridad contractuales; con servidores públicos, proveedores y partes interesadas, comprometidos a participar activamente en el desarrollo de la cultura de seguridad de la información"***.

6.1 COMPROMISO DE LA DIRECCIÓN

La Dirección de TICs y la Alta Dirección de la Entidad demuestran su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Entidad a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad. a través de la ejecución de programas de sensibilización.
- Facilitar la divulgación del Manual de Políticas de Seguridad a todos los funcionarios de la entidad.

- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.
- Asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la Entidad.

7. AUTORIDADES Y ROLES DE SEGURIDAD DE LA INFORMACIÓN

Para asegurar el adecuado entendimiento de cada una de las políticas, a continuación, se presentan las autoridades y los roles establecidos en el modelo de seguridad de la información adoptado por la entidad[1] e insumo para la definición de cada uno de los lineamientos:

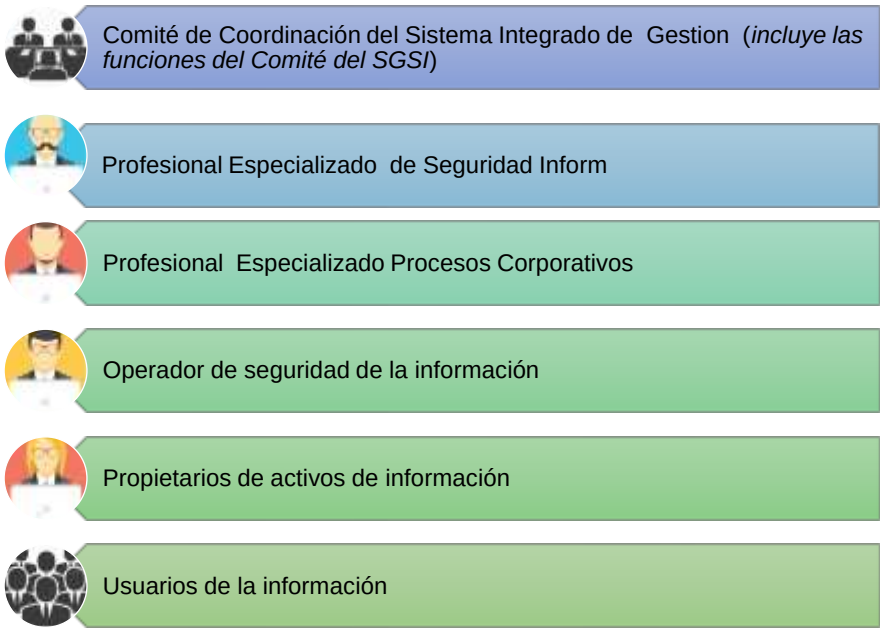

Ilustración 1. Autoridades y Roles de seguridad de la información de TRANSMILENIO S.A.

8. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información conceptualizan el modelo de manejo de los recursos tecnológicos, humanos, datos y físicos de TRANSMILENIO S.A., en los roles de funcionarios públicos,

[1] NTC ISO 27001:2013

oficiales, proveedores, contratistas y terceras partes que manejan administran y custodian la información.

Las herramientas tecnológicas con las que cuenta TRANSMILENIO S.A., y los recursos asignados a cada uno de sus usuarios (hardware y software), acceso, información, almacenamiento de datos, consulta y modificación de la información, internet, intranet, correo institucional y los demás que sean pertinentes con base en las funciones de cada área, se constituyen en un activo de propiedad exclusiva de la Entidad, por ende a la naturaleza de los bienes públicos, por lo cual podrá ser objeto de verificación, control y monitoreo.

Las políticas definidas a continuación se encuentran estructuradas y orientadas con base en cada dominio o control del Anexo A de la NTC ISO 27001:2013, y están alineadas con las prácticas de gestión de la norma NTC-ISO 27002:2015.

8.1 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La Alta Dirección de TRANSMILENIO S.A. apoya activamente la seguridad de la información dentro de la organización, con un rumbo claro, un compromiso demostrado y el conocimiento de las responsabilidades de la seguridad de información, para ello cuenta con el Comité de Seguridad de la Información o un organismo de dirección, en el cual participan representantes de todos los procesos según lo considere pertinente.

8.2 POLÍTICA PARA DISPOSITIVOS MÓVILES

Dominio/ Control: A.6.2.1 Política para Dispositivos Móviles

Objetivo: garantizar la seguridad en el uso de los dispositivos móviles.

Alcance: la presente política aplica para todos funcionarios públicos, oficiales, proveedores, contratistas y terceras partes. o que, por su rol, hagan uso de dispositivos móviles en la entidad.

Lineamientos:

a. La Dirección de TICs efectuará labores de monitoreo tanto a los dispositivos móviles propios de la Entidad como a los personales conectados a la red de TRANSMILENIO S.A., (cuando a ello haya lugar) con el objeto de adoptar los mecanismos de protección de la información y aplicar las medidas correctivas cuando se requieran.

b. La Dirección de TICs establece las configuraciones definidas para el manejo tanto de los dispositivos móviles propios de la entidad como de aquellos que sean personales y se encuentren conectados en la red del de la entidad siguiendo, para ello, las reglas generales de la Guía para el uso aceptable de activos previamente adoptada.

c. Todos los usuarios que tengan autorizado el uso de dispositivos móviles personales deben cumplir con las reglas generales establecidas en la guía para el uso aceptable de activos.

Excepciones:

Cualquier excepción a los lineamientos precedentes, debe ser autorizada por la Dirección de TICs y/o el Líder u oficial de Seguridad de la Información de la entidad.

8.3 POLÍTICA DE TELETRABAJO

Dominio/ Control: A.6.2.2 Teletrabajo

Objetivo: establecer los lineamientos para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

Alcance: la presente política aplica para todos funcionarios públicos, oficiales, proveedores, contratistas y terceras partes.

Lineamientos:

TRANSMILENIO S.A. establece los siguientes lineamientos, en el marco de la Ley 1221 de 2008 y la Resolución 420 de 2016 al interior de la Entidad: “Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones”:

TRANSMILENIO S.A., como empleador debe:

- Autorizar la utilización de equipos personales a los teletrabajadores para la ejecución de sus obligaciones y/o funciones (cuando a ello haya lugar), en los cuales se deben implementar todas las medidas de seguridad definidas por la entidad.
- Facilitar los mecanismos para que los trabajadores conozcan los lineamientos impartidos a través de la presente política y con ello los riesgos que se derivan del uso de los equipos tecnológicos en el proceso de seguridad de la información de la entidad.

- Definir los tipos de usuarios que dispondrán de modalidad de teletrabajo y los permisos de acceso remoto pertinentes.
- Establecer procedimientos para la solicitud y autorización del teletrabajo.
- Establecer un procedimiento de conexión remota de emergencia para solventar problemas e incidencias puntuales.
- Establecer un compromiso por parte del Teletrabajador (en el documento que defina la entidad), frente al cumplimiento de los lineamientos adoptados a través de la presente política, así como lo relacionado al uso exclusivo del equipo que se destine para la ejecución de sus obligaciones y/o funciones (según sea el caso), aceptando y cumpliendo para tales efectos con las medidas de seguridad de la información implementadas por la entidad.
- Definir los derechos y obligaciones de cada una de las partes que intervienen en el teletrabajo.
- Llevar un seguimiento de las conexiones remotas a los servicios corporativos de teletrabajo. Especialmente se debe prestar atención a los intentos de conexión sospechosos.
- Los Teletrabajadores no deben almacenar en los equipos asignados o personales información sensible o reservada. En lo que respecta a la información que se encuentre contenida en medios digitales, los teletrabajadores están en la obligación de dar estricto cumplimiento a los lineamientos de seguridad de la información establecidos por la entidad y que a continuación se relacionan:
  - ✓ Si los equipos son personales, el Teletrabajador debe instalar el sistema operativo desde una fuente fiable, mantener el sistema operativo y las aplicaciones actualizadas.
  - ✓ Instalar un software de antivirus.
  - ✓ Utilizar el control de acceso definido por la entidad con sus correspondientes permisos.
  - ✓ Mantener configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc.), parametrizando el bloqueo automático por inactividad y en lo posible, utilizar un cifrado de disco.
- Los equipos portátiles no deben dejarse desatendidos, el Teletrabajador debe evitar transportar el equipo si no es necesario.
- Guardar bajo llave en el sitio o sitios en los que se ejecuten las funciones de teletrabajo, el dispositivo mientras no se utiliza.

- Manejar cuentas de usuario independientes o incluso el uso de sistemas operativos o máquinas virtuales separadas.
- No utilizar conexiones poco confiables (conexiones Wi-Fi abiertas, redes públicas de hoteles, bibliotecas, locutorios, aeropuertos, entre otros) sin algún tipo de cifrado punto a punto como puede ser VPN o conexiones a sitios web protegidos con SSL (los que empiezan por HTTPS).
- Verificar que en el acceso a los servidores corporativos se utilicen certificados reconocidos y que la figura del “candado” de la conexión SSL no indique sobre la existencia de posibles de peligros o errores.
- Utilizar contraseñas seguras siguiendo los lineamientos de la Política de control de acceso de TRANSMILENIO S.A.
- Borrar el histórico de navegación, las cookies y otros datos del navegador web.
- Por políticas de seguridad de la Información, el Teletrabajador, no debe usar el cuadro de dialogo en el que se sugiera recordar contraseña.
- Al finalizar el trabajo, cerrar todas las conexiones con servidores y páginas web utilizando cuando sea posible la opción “desconectar” o “cerrar sesión”.
- Eliminar la información temporal alojada en carpeta de descargas, papelera de reciclaje, escritorio virtual u otras que se encuentren en diferentes carpetas del dispositivo.
- Solicitar a la mesa de ayuda de la entidad, cuando sea necesario, la aplicación de las herramientas de borrado seguro sobre la información institucional alojada en el dispositivo con el que se ejecuten las labores de teletrabajo, previa autorización cuando sea el caso.
- Asegurarse de retirar cualquier memoria USB, CD o DVD que se haya utilizado en el equipo.
- En lo que respecta a la información que se encuentre contenida en medios físicos, los teletrabajadores están en la obligación de dar estricto cumplimiento a los lineamientos de seguridad de la información establecidos por la entidad y que a continuación se relacionan: Almacenar los documentos bajo llave mientras no se estén utilizando.
- Llevar a cabo la destrucción de los documentos, para lo cual será necesario romperlo o triturarlo con el objeto de evitar que la pieza documental se arroje de manera completa al contenedor o papelera y sea reutilizada para labores domésticas que de alguna manera ponga en riesgo la información institucional.

- No dejar las copias impresas desatendidas en la bandeja de la impresora.
- No dejar los documentos en tránsito desentendidos en el lugar o lugares en los que se ejecutan las funciones de teletrabajo.

Excepciones

Cualquier forma de teletrabajo debe estar aprobada formalmente por la Dirección Administrativa, toda excepción a los lineamientos debe ser justificada por el Teletrabajador y autorizada por el Líder u oficial de Seguridad de la información de la entidad.

8.4 POLÍTICA DE CONTROL DE ACCESO

Dominio: A.9 Control de Acceso

Objetivo: establecer los lineamientos para evitar el acceso no autorizado a la información y a las instalaciones de procesamiento de información de TRANSMILENIO S.A.

Alcance: la presente política aplica para todos los funcionarios públicos, oficiales, proveedores, contratistas y terceras partes, o que, por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información de TRANSMILENIO S.A.

Lineamientos:

8.4.1 Requisitos del negocio para control de acceso

a) Los sistemas de información de TRANSMILENIO S.A. deben contar con mecanismos y procedimientos para el control de acceso a sus sistemas de información y a las instalaciones de procesamiento de información tales que la autorización para el acceso a estos sistemas debe ser definida y aprobada por cada dependencia o propietario de la información, e implementada por la Dirección TICs y supervisada por el Profesional Especializado (06) de Seguridad de la Información de la Dirección de TICs, de acuerdo con la funcionalidad de cada sistema, según el procedimiento de gestión de usuarios y contraseñas.

b) TRANSMILENIO S.A., proporcionará a los funcionarios de planta y contratistas los recursos tecnológicos necesarios para que puedan desempeñar las funciones de una manera eficaz, por tal motivo no se permite conectar o instalar, de manera cableada o inalámbrica, a la red LAN de la Entidad, cualquier dispositivo fijo o móvil, del tipo computadores portátil, Tablet, enrutador ,

agenda electrónica, Smartphone, Access point, amplificadores de señal, que no sean autorizados por la dirección de TICs.

c) Quien (es) ejecute (n) el rol de Administrador de control de acceso lógico debe (n) establecer las medidas de control de acceso de los funcionarios públicos, oficiales, proveedores, contratistas y terceras partes, a través de mecanismos de identificación, autenticación y autorización de acceso, a nivel de red, sistemas de información, bases de datos, instalaciones de procesamiento de información y servicios de TI de acuerdo con los perfiles y cargos establecidos en la entidad.

d) Quien (es) ejecute (n) rol de Administrador de control de acceso lógico debe (n) dar cumplimiento a la aprobación o rechazo de los permisos de conexión remota o VPN, previamente otorgada por la dirección de TICs o por el líder u Oficial de seguridad de la Información de la entidad o quien haga sus veces, En lo que respecta a la solicitud de acceso lógico que efectúen los funcionarios públicos, oficiales, proveedores, contratistas y terceras partes, esta debe ir respaldada, soportada y avalada por el jefe inmediato o supervisor del contrato según sea el caso.

e) Quien (es) ejecute (n) el rol de Administrador de recursos informáticos debe (n) velar por el cumplimiento del procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red. Quien (es) ejecute (n) El rol de Administrador de control de acceso lógico podrá (n) realizar una verificación de los controles de acceso de los funcionarios públicos, oficiales, proveedores, contratistas y terceras partes en la periodicidad que se establezca para ello, a fin de cerciorarse que dichos usuarios acceden solamente a los recursos autorizados para la realización de sus tareas, funciones u obligaciones; así mismo debe realizar la deshabilitación o suspensión de aquellos usuarios que contando con acceso activo, presenten cualquier tipo de novedad que así lo amerite.

f) Quien(es) ejecute(n) el rol de Administrador del control de acceso lógico debe (n) asegurar que las redes inalámbricas cuenten con métodos de autenticación que eviten accesos no autorizados.

g) Es responsabilidad de funcionarios públicos, oficiales, proveedores, contratistas y terceras partes, el buen manejo y uso de los recursos, así como de las claves que le han sido asignadas.

h) Los perfiles y derechos de acceso serán revisados periódicamente (anualmente) por el área de soporte de la dirección de TICs y los propietarios de la información. Adicionalmente, es responsabilidad del usuario, informar cualquier privilegio que no corresponda con su perfil para que sea ajustado.

i) Los privilegios se asignarán a los usuarios de acuerdo con a los roles y responsabilidades. Los privilegios se deben extender sólo cuando sea necesario y deben contar con autorización del profesional especializado 06 de seguridad de la información de la Dirección.

j) Los derechos de acceso a la información de todos los funcionarios de planta, contratistas y usuarios externos a la Entidad se deben cancelar al terminar su vinculación como empleado, contrato o acuerdo, o se deben ajustar cuando se requieran cambios, previamente solicitados por el área o profesional responsable.

k) Siempre que los usuarios dejen el puesto de trabajo, deben bloquear el equipo, en caso de ausencia de las instalaciones, el computador debe permanecer apagado, con el fin de evitar el acceso no autorizado a cualquier aplicación de la organización.

8.4.2 Identificación y autenticación

a) Todos los funcionarios públicos, oficiales, proveedores, contratistas y terceras partes, que, con ocasión a sus tareas u obligaciones con la entidad, tengan acceso a los sistemas de información, deben utilizar un nombre de usuario de dominio TRANSMILENIO S.A, asignándole para ello una contraseña que cumpla con las políticas de seguridad adoptadas por la entidad, la cual deberá ser personal e intransferible.

b) El acceso a los sistemas de información y servicios tecnológicos de la entidad, a través del uso de usuario de dominio TRANSMILENIO, debe estar restringido y delimitado a las tareas, funciones, responsabilidades u obligaciones que ejecuten los funcionarios públicos, oficiales, proveedores, contratistas y terceras partes en la entidad.

c) La creación del usuario seguirá el modelo: nombre.apellido@transmilenio.gov.co

d) Para la creación de contraseñas seguras funcionarios públicos, oficiales, proveedores, contratistas y terceras partes, deben:

- Escoger contraseñas que sean difíciles de descifrar y que no contengan información relacionada con su trabajo o vida personal, por lo cual no se debe utilizar la siguiente información: Números de identificación personal, números de teléfono, nombres de los conyugues, direcciones postales, nombres propios, lugares conocidos o términos técnicos.
- Combinar palabras (Mayúsculas o minúsculas), puntuación y números, de tal modo que arroje como resultado una contraseña alfanumérica con símbolos especiales.
- Transformar una palabra común utilizando un método especifico.

- ❖ Crear acrónimos (siglas que forman una palabra)
- ❖ Crear contraseñas que contengan como mínimo 8 dígitos y cambiarla en intervalos de 30 días.
- ❖ Las contraseñas no deberán ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.
- ❖ Cambiar las contraseñas temporales al primer acceso.
- ❖ No debe contener el nombre de usuario.
- ❖ Las contraseñas temporales deben ser entregadas a los usuarios de una manera segura, con expiración en el primer uso. Se debe evitar la entrega de la clave a una tercera persona.
- ❖ Las contraseñas por omisión que vienen en los sistemas y software deben ser modificadas enseguida de su instalación.
- ❖ Los Intentos no exitosos de ingreso de la contraseña, después de un número veces determinadas y previamente establecidas por la entidad, traerá consigo el bloqueo del usuario de manera inmediata para lo cual se deberá solicitar el desbloqueo a quien ejecute el rol de Administrador de control de acceso lógico.

e) Las contraseñas que sean suministradas a través de correo electrónico por quien ejecute el rol de administrador de un determinado sistema, deben ser cambiadas de manera inmediata tan pronto como la misma sea recibida por parte de la persona a quien se le han asignado los permisos, siguiendo para ello con los protocolos de seguridad de la información y las buenas prácticas de uso de contraseña aludidas.

8.4.3 Almacenamiento de contraseñas

a) Las contraseñas no deben ser almacenadas en formato legible, papeles, agendas de trabajo, computadores sin sistemas de control de acceso o cualquier otro lugar donde las personas no autorizadas puedan encontrarlas.

b) Si algún funcionario público, oficiales, proveedores, contratistas y terceras partes, sospecha (n) de la pérdida de confidencialidad de alguna de sus claves, debe (n) notificar de manera escrita el evento y/o incidente de seguridad de la información (según sea el caso) a la mesa de ayuda de la entidad , a fin de tomar las medidas pertinentes de cuidado de la información y supervisar la generación de nuevas credenciales siguiendo los lineamientos del Procedimiento Gestión de Incidentes de seguridad de la información.

c) El acceso a los recursos de la red será controlado por medio de la creación de usuarios y contraseñas correspondientes, a fin para prevenir accesos no autorizados. Los usuarios tendrán solamente acceso a los servicios de red y sistemas de información para los cuales fueron autorizados y que son necesarios para realizar su trabajo.

d) El acceso por parte de un proveedor a la red interna se debe realizar por medio de un mecanismo seguro y con previa autorización de la Dirección de TICs de TRANSMILENIO S.A.

e) El tiempo de inactividad del computador debe activar el control de bloqueo de la máquina. Dicha política se establece por plantilla del directorio activo para un tiempo igual o superior a 5 minutos de inactividad. El tiempo de inactividad definido debe reflejar los riesgos de seguridad del área, la aplicación que esté siendo usada, la información que esté siendo manejada y los riesgos relacionados a los usuarios de los equipos.

f) Todas las contraseñas de los súper-usuarios (privilegios de administrador) deben ser protegidas y almacenadas en una bóveda por el líder u oficial de seguridad de la información.

g) Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece, al correo soportetecnico@transmilenio.gov.co.

8.4.4 Control de acceso a sistemas y aplicaciones

TRANSMILENIO S.A., deberá asegurar, preservar y garantizar el control de acceso a los sistemas y aplicaciones institucionales, cumpliendo los siguientes parámetros de seguridad:

a) El propietario de la aplicación y de la información, deberá identificar y documentar explícitamente la sensibilidad o confidencialidad de la información contenida en los sistemas y aplicaciones de la entidad.

b) Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos, las necesidades de uso y la clasificación de la información.

c) No está permitido para ningún funcionario público, oficiales, proveedores, contratistas y terceras partes, acceder a la información y a las aplicaciones de un sistema de información para el cual no haya sido autorizado.

d) Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico en la entidad debe (n) asegurar que los grupos de servicios de información, usuarios y sistemas de información sean segmentados en redes.

e) Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurar que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.

f) Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) establecer los controles de acceso a los ambientes de producción de los sistemas de información.

g) Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

h) En lo que respecta a la autorización y continuidad en el uso de los usuarios de los aplicativos de la entidad, será deber de cada una de las dependencias de la entidad, informar a los Administradores de las aplicaciones la novedad o novedades que surjan en funcionario público, oficiales, proveedores, contratistas y terceras partes, con el objeto de que dichos usuarios sean deshabilitados o suspendidos oportunamente, según fuere el caso.

Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

i) Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurar que en lo que respecta a los sistemas operativos de la entidad, se bloquee la sesión automáticamente, después de determinados minutos de inactividad, previamente establecidos.

j) Quien (es) ejecute (n) el rol de desarrollador de sistemas de información debe (n) garantizar que se cierre la sesión en las aplicaciones, después de determinados minutos de inactividad previamente establecidos.

k) El Director de TIC’s o a quien este designe como encargado del Equipo de Desarrollo debe asignar el rol del Administrador de programas fuentes, quien tendrá la responsabilidad de custodiar dichos programas y por virtud de su función no deberá pertenecer al equipo de desarrollo.

l) Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe (n) llevar un registro actualizado de todos los programas fuentes en uso, indicando entre otros, el nombre del

programa, programador, analista responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).

m) Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe (n) restringir el acceso a los códigos fuente de los programas, asegurándose de que solamente los ingenieros desarrolladores tengan acceso.

n) Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe (n) mantener los códigos fuente de los programas en el servidor o repositorio de fuentes. El mantenimiento y copiado de las bibliotecas fuentes del programa está sujeto a procedimientos estrictos de control de cambios.

o) La actualización de las bibliotecas de fuentes del programa, así como la emisión de las fuentes para los programadores sólo se deben realizar después de haber recibido la autorización del Profesional encargado del Equipo de Desarrollo.

p) Quien (es) ejecute (n) el rol de administrador de programas fuentes debe (n) mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes del programa.

q) Los desarrolladores deben aplicar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.

r) Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe(n) asegurarse de que los programas fuentes cuenten con una copia de respaldo actualizada, conforme a lo estipulado en el procedimiento de backup.

s) No está permitido facilitar el usuario o la contraseña a otra persona para adelantar cualquier labor en los sistemas de información.

Excepciones:

Cualquier excepción a los lineamientos, debe ser justificada por quien (es) ejecute (n) el rol de Administrador de control de acceso lógico o Administrador de programas fuentes, según aplique; debidamente validada por el líder u oficial de seguridad de la información de la entidad y aprobada por la Dirección de Tecnologías de la Información o quien haga sus veces.

8.5 POLÍTICA DE SEGURIDAD EN LAS TELECOMUNICACIONES

Dominio: A.13 Seguridad de las comunicaciones.

Objetivo: establecer los lineamientos para la gestión segura de las redes de TRANSMILENIO S.A., la cual puede abarcar los límites organizacionales, que requieren de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

Alcance: la presente política aplica para todos los funcionarios públicos, oficiales, proveedores, contratistas y terceras partes, o que, por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información de TRANSMILENIO S.A.

Lineamientos:

8.5.1 Gestión de la seguridad en las redes

TRANSMILENIO S.A, debe Asegurar y controlar los accesos a los servicios Internos y externos con el fin de proteger la información en sistemas y aplicaciones, dando cumplimiento a los siguientes lineamientos:

a) Se deben controlar los accesos a servicios internos y externos conectados en red.

b) La Dirección de TICs debe mantener el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad).

c) La Dirección de TICs de TRANSMILENIO S.A., como responsable de las redes de datos y los recursos de red de la entidad (internos y externos), debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

d) La Dirección de TICs de TRANSMILENIO S.A., debe asegurar que las redes inalámbricas de la Entidad cuenten con procedimientos de autenticación que eviten accesos no autorizados, dichos procedimientos están soportados en técnicas de segmentación de redes y restricción de uso de las redes inalámbricas solo a funcionarios autorizados.

e) Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de TRANSMILENIO S.A., deben contar con la autorización previa para la creación de cuentas de usuario, solicitada a la Dirección de TICs por medio escrito o electrónico. y el Acuerdo de Confidencialidad firmado previamente.

f) Se deben identificar e incluir en los acuerdos de niveles de servicio (ANS) (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de

red, independientemente de si estos servicios se entregan de manera interna o están externalizados.

g) Se deben segmentar las redes en función de los grupos de servicios, usuarios y sistemas de información.

h) TRANSMILENIO S.A., provee los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios inadecuados sobre los sistemas operacionales.

i) No deben realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción.

Excepciones:

Cualquier excepción a los lineamientos, debe ser justificada por quien (es) ejecute (n) el rol de Administrador de redes, según aplique; debidamente validada por el líder u oficial de seguridad de la información de la entidad y aprobada por la Dirección de Tecnologías de la Información o quien haga sus veces.

8.6 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

Dominio/ Control: A.13.2Transferencia de información

Objetivo: establecer los lineamientos para mantener la seguridad de la información transferida dentro de la entidad y con cualquier entidad externa.

Alcance: la presente política aplica para funcionarios públicos, oficiales, por su rol, transfieran información dentro de la entidad y con cualquier entidad externa.

Lineamientos:

La transferencia de Información por cualquier medio debe realizarse protegiendo la confidencialidad e integridad de los datos con los mecanismos que se encuentren establecidos en el Modelo de Seguridad y Privacidad de la Información- MSPI de acuerdo con la clasificación del activo de información involucrado.

La Entidad deberá dar cumplimiento a los siguientes lineamientos de seguridad:

a. TRANSMILENIO S.A. cuenta con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, soportada en su infraestructura de telecomunicaciones. Ver procedimiento P-DT-012 Procedimiento para el Intercambio seguro de la Información Electrónica.

b. Cuando se trate de intercambios periódicos, se debe privilegiar la transmisión de datos a través de vías seguras. La situación más evidente en este sentido surge con entes distritales, con los cuales se establecen convenios o nexos de diferente naturaleza, y que involucran de alguna forma el intercambio de información.

c. Para acceso a sitios web se debe implementar herramientas de seguridad perimetral seguros (firewalls) y el uso de protocolos seguros.

8.6.1 Mensajería electrónica

TRANSMILENIO S.A. debe asignar una cuenta de correo electrónico como herramienta de trabajo para cada uno de los funcionarios que lo requieran para el desempeño de sus funciones y en algunos casos a terceros previa autorización; su uso se encuentra sujeto a lo establecido en la presente política.

Los mensajes y la información contenida en los buzones de correo son de propiedad de TRANSMILENIO S.A y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

El tamaño de los buzones de correo está determinado por la Dirección de TIC's de acuerdo con las necesidades de cada usuario y previa autorización del Jefe Inmediato de cada Dirección o Dependencia. Para el uso del correo electrónico, se deberá dar cumplimiento a los siguientes lineamientos:

a. No Enviar o recibir mensajes con un tamaño superior al autorizado (20 Mbps) y configurado entre: cuentas de correo corporativas o entre una cuenta de correo corporativa y una externa.

b. No Enviar o recibir cadenas de correo, mensajes con contenido religioso, juegos, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar

prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos. Si un usuario encuentra este tipo de material deberá reportarlo a su jefe inmediato con copia al buzón soportetecnico@transmilenio.gov.co.

c. El envío de archivos que contengan extensiones como .mp3, wav, .exe, .com, .dll, .bat. o cualquier otro archivo ejecutable; en caso de que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por la Dirección de TICs de TRANSMILENIO S.A.

d. El uso del correo electrónico en cadenas o mensajes enviados a un número de destinatarios para que estos a la vez se reenvíen a otros, enviado a un gran número de receptores sin un propósito relacionado con la misión de la TRANSMILENIO S.A., estos tipos de mensajes degradan el desempeño del sistema y consumen recursos valiosos en disco y memoria. El usuario debe borrar los correos de cadena y masivos (no relacionados con la misión de la Entidad) y abstenerse de reenviarlos a otras personas. Así mismo, no debe reenviar correo a otra persona sin el previo consentimiento del remitente.

e. No se debe alterar la línea “De” (autor del correo) u otra información relacionada con los atributos de origen del correo electrónico.

f. El envío de mensajes anónimos y la gestión con este tipo de mensajes está prohibida.

g. El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la Dirección de Tics de TRANSMILENIO S.A. y deberá incluir un mensaje que le indique al destinatario cómo ser eliminado de la lista de distribución.

h. Toda información de TRANSMILENIO S.A., generada con los diferentes procesadores de texto (Ej. Herramientas de Oficina como Word, Excel, PowerPoint, Project, Access, WordPad, Open Office, entre otras), que requiera ser enviada fuera de la Organización, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables, utilizando una herramienta que evite la modificación de la información. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

i. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la Dirección de Tics de TRANSMILENIO S.A. y deben conservar en todos los casos el mensaje legal institucional de confidencialidad.

j. El correo electrónico, deberá tener al final del mensaje el siguiente texto:

"Este mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley. Sólo puede ser utilizada por la persona o compañía a la cual está dirigido. Si usted no es el receptor autorizado, o por error recibe este mensaje, favor borrarlo inmediatamente. Cualquier retención, difusión, distribución, copia o toma de cualquier acción basada en ella, se encuentra estrictamente prohibido ".

"This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message. Any disclosure, copying, or distribution of this message, or the taking of any action based on it, is strictly prohibited ".

k. La información enviada por correo electrónico, clasificada como confidencial, debe ser protegida con contraseña de acceso o cifrado según corresponda.

l. Se prohíbe falsificar el encabezado de los mensajes con el objeto de esconder su verdadero contenido, las fechas de su recepción o los remitentes o destinatarios incluidos en ellos.

m. Se prohíbe al usuario, además, hospedar sitios que sean publicitados por medio de mensajes de correo electrónico no solicitados o sitios que generen este tipo de mensajes no solicitados, aunque los mismos no se generen directamente desde ese sitio. Hospedar, publicitar, comercializar o de cualquier manera poner a disposición de terceros cualquier software, programa, producto o servicio diseñados para violar de alguna forma la presente política o las políticas de uso aceptable de otro proveedor de acceso a internet, lo que incluye, pero no está limitado a, programas diseñados para enviar mensajes con publicidad no solicitados ("spamware"), los que se encuentran prohibidos por este documento.

n. Las cuentas o servicios de TRANSMILENIO S.A., no podrán ser utilizadas para recibir respuestas a mensajes enviados desde otro proveedor de servicio de internet si dichos mensajes violan la presente política o la de otro proveedor.

o. Se prohíbe comunicar, publicar, circular, enviar o allegar a instancias o entidades diferentes a aquellas que lo requieren, información que en la Entidad se considera confidencial o de uso interno exclusivamente.

p. TRANSMILENIO S.A., se reserva el derecho de monitorear y supervisar la información tramitada y transmitida a través de sistemas, servicios y equipos, por todos los usuarios de acuerdo con lo establecido en este manual y la legislación vigente.

Excepciones:

Cualquier excepción a los lineamientos, debe ser justificada por quien (es) ejecute (n) el rol de Administrador, según aplique; debidamente validada por el líder u oficial de seguridad de la información de la entidad y aprobada por la Dirección de Tecnologías de la Información o quien haga sus veces.

8.7 POLÍTICA DE CONFIDENCIALIDAD

Dominio: A.7.1.2 Términos y condiciones del empleo.

Objetivo: asegurar que los empleados y contratistas comprendan sus responsabilidades y son idóneos en los roles para los que se consideran.

Alcance: la presente política establece que todos los funcionarios públicos, oficiales, contratistas y terceras partes, deben dar cumplimiento a las Políticas de Seguridad y Privacidad de TRANSMILENIO S.A.

Lineamientos:

La presente Política de Confidencialidad, tiene por objeto informarles a todos los funcionarios públicos, oficiales, contratistas y terceras partes vinculados con TRANSMILENIO S.A; sobre el compromiso frente a la no divulgación de la información relacionada con las funciones que desempeña en la entidad, a personal interno o externo de la misma. Concluyendo que en ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcial sin contar con previa autorización.

Todos los funcionarios, contratistas y clientes deben firmar la cláusula y/o acuerdos de confidencialidad definidos por TRANSMILENIO S.A. y este deberá ser parte integral de cada uno de los contratos. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de la Entidad a personas o entidades externas. Su aplicación se llevará a cabo en coordinación con la subgerencia jurídica de TRANSMILENIO S.A.

TRANSMILENIO S.A., firmará acuerdos de confidencialidad con los clientes y terceros o contratistas, que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Institución. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio

de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

El acuerdo de confidencialidad deberá formalizarse en cada uno de los contratos celebrados con terceros y que en la prestación del servicio puedan tener acceso a la información restringida o confidencial de TRANSMILENIO S.A. De dicho acuerdo deberá derivarse una responsabilidad tanto civil como penal para la tercera parte que TRANSMILENIO S.A. contrata.

Todos los funcionarios públicos, oficiales, contratistas de TRANSMILENIO S.A. deben Guardar absoluta reserva en relación con la información a la que tenga acceso con ocasión de la ejecución del contrato, aun después de finalizada su ejecución, por el tiempo establecido por la normatividad legal vigente y aplicable para cada caso en particular.

Excepciones:

Las excepciones establecidas por Ley en caso de aplicar.

8.8 POLÍTICA DEL RECURSO HUMANO

Dominio: A.7. Seguridad del recurso Humano.

Objetivo: asegurar que los empleados y contratistas comprendan sus responsabilidades y son idóneos en los roles para los que se consideran.

Alcance: la presente política establece que todos los funcionarios públicos, oficiales, contratistas y terceras partes, deben dar cumplimiento a las Políticas de Seguridad y Privacidad de TRANSMILENIO S.A.

Lineamientos:

TRANSMILENIO S.A., reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos funcionarios se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

Antes de la contratación

Asegurar que los empleados y contratistas comprendan sus responsabilidades y sean idóneos en los roles para los que se consideran.

a) El Grupo de Talento Humano debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en TRANSMILENIO S.A., antes de su vinculación definitiva.

b) El Grupo de Talento Humano debe certificar que los funcionarios de la Entidad firmen un Acuerdo y/o Cláusula de Confidencialidad y de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

c) El personal provisto por terceras partes que realice labores en o para TRANSMILENIO S.A., debe firmar un Acuerdo y/o Cláusula de Confidencialidad y de Aceptación de Políticas de Seguridad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

d) El personal provisto por terceras partes debe garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad y de aceptación de las Políticas de Seguridad de la Información de la Entidad.

e) Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes y deben ser proporcionales a los requisitos de la entidad, a la clasificación de la información a que va a tener acceso, y a los riesgos percibidos.

Durante la ejecución del empleo:

Asegurar que todos los funcionarios públicos, oficiales, contratistas y terceras partes, tomen conciencia de sus responsabilidades de seguridad de la información, considerando el cumplimiento de los siguientes lineamientos:

a. La Dirección de Tics debe diseñar y ejecutar de manera periódica (mínimo una vez al año) un plan de cultura y sensibilización en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.

b. Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información de TRANSMILENIO S.A.

c. El grupo de talento humano debe convocar a los funcionarios a las charlas y eventos programados como parte del desarrollo del plan de cultura y sensibilización en seguridad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas, aplicando las sanciones pertinentes por la falta de asistencia no justificada.

Excepciones:

Las excepciones establecidas por Ley en caso de aplicar.

8.9 POLÍTICA DE ÀREAS SEGURAS

Dominio/ Control: A.11.1 Áreas Seguras

Objetivo: prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de TRANSMILENIO S.A.

Alcance: la presente política aplica para todos los funcionarios públicos, oficiales, contratistas y terceras partes, o que por su rol tengan acceso físico a las instalaciones y áreas seguras de TRANSMILENIO S.A.

Los servicios de procesamiento de información críticos de TRANSMILENIO S.A., deben estar instalados en áreas seguras, con protección de perímetro y controles de entrada. Se deben proteger físicamente de acceso no autorizado, daño e interferencia.

Lineamientos:

8.9.1 Perímetros de seguridad física – controles físicos de entrada

Las áreas y dependencias de TRANSMILENIO S. A, deben encontrarse protegidas por barreras y controles físicos, para lo cual deben estar monitoreadas y supervisadas, las áreas seguras serán por lo menos las siguientes:

a) **Datacenter:** corresponde al centro de procesamiento de datos en donde se albergan los sistemas de información (aplicaciones, bases de datos), los componentes de telecomunicaciones y los sistemas de almacenamiento (servidores físicos y virtuales).

b) **Centros de Cableado:** áreas de unión central que se usan para conectar los dispositivos de la red del área local (LAN) el cual alberga paneles de conexión y equipos activos, entre otros.

c) **Cuartos de suministro:** áreas en donde se ubican los servicios de suministro como: las UPS y la planta eléctrica.

d) **Archivo físico central:** áreas en donde se administran, custodian y conservan los documentos físicos con valor administrativo, legal, permanente, histórico entre otros**.**

e) **Archivo físico de gestión:** Hace referencia a aquella documentación todavía en trámite que conserva TRANSMILENIO S.A así como a aquella que aun después de finalizado el procedimiento administrativo, está sometida a uso continuo y consulta administrativa, aplicando para ello lo dispuesto en las tablas de retención documental. Y todas aquellas dependencias y áreas de la entidad que por sus competencias funcionales manejen información reservada o sensible, serán consideradas áreas seguras.

TRANSMILENIO S.A debe adoptar los mecanismos tendientes para asegurar dicha información y se debe dar cumplimiento a los siguientes lineamientos:

- El perímetro de la construcción o sitio que contiene instalaciones de procesamiento de información debe ser físicamente sólido. Los muros externos del sitio deben ser de construcción sólida y todas las puertas externas deben estar protegidas contra el acceso no autorizado, ejemplo alarmas, cerraduras, etc.
- Debe definirse un área de recepción u otro medio para el control del acceso físico al sitio o edificio.
- Impedir que aquellas áreas cuyas ventanas den al exterior por su ubicación, permitan de alguna manera (al menos mínima) la visibilidad hacia el interior de la entidad.
- Implementar el uso de sistemas de control de acceso físico de proximidad en las áreas seguras.
- Los privilegios de acceso a las áreas seguras de TRANSMILENIO S.A deben ser definidos y otorgados por el profesional u oficina encargada del área segura, para ello debe tener en cuenta los siguientes tipos de usuario:

- Profesionales que trabajan regularmente en las áreas seguras.
- Profesional de soporte que requiere acceso periódico.
- Visitantes (servidores públicos, contratistas, proveedores o terceras partes) que requieren acceder muy rara vez.

Teniendo en cuenta lo anterior, los únicos que deben tener privilegios de acceso permanente a las áreas seguras son los profesionales que trabajan regularmente en ellas. Los demás usuarios deben solicitar autorización para el acceso y portar un documento que demuestre su identidad. En este tipo de casos, se debe asignar por parte del área responsable del área segura un profesional que acompañe y supervise la labor de dicho visitante, hasta su salida.

- El acceso al Datacenter está restringido y su ingreso es únicamente por medio biométrico.
- Para el ingreso de los visitantes, en las áreas seguras se debe llevar un registro de ingreso previamente este autorizado por el funcionario correspondiente.
- Para el ingreso de funcionarios, proveedores y terceras partes al Datacenter y/o centros de cableado, se debe diligenciar el formato de ingreso al Datacenter o centro de cableado, con la autorización del responsable correspondiente.
- Las actualizaciones a los derechos de acceso pueden ser efectuadas cuando ello así se requiera por parte de la dirección Administrativa de TRANSMILENIO S.A., para lo cual, si es del caso, se revocarán aquellos permisos que ya no sean necesarios.
- Deben mantenerse pistas de auditoría de todos los accesos a las áreas restringidas.

8.9.2 Seguridad de oficinas, recintos e instalaciones

Con el propósito de mantener la confidencialidad, integridad y disponibilidad en la oficinas, recintos e instalaciones, es necesario establecer la guía de uso de este para funcionarios públicos, oficiales, contratistas y terceras partes. Las directrices a este respecto estarán a cargo de la Dirección Administrativa y el Área de Seguridad Física de TRANSMILENIO S.A. Se debe considerar el cumplimiento de los siguientes lineamientos:

a. Todos los servidores públicos, contratistas, proveedores y terceras partes deben portar visiblemente el carné o documento que los acredite como tal, mientras se encuentren en las instalaciones de TRANSMILENIO S.A.

b. El personal que ingrese o salga de las instalaciones de la entidad y porte los dispositivos tecnológicos institucionales o personales, deberá registrarse en la bitácora de vigilancia.

c. Todo visitante debe notificar en la recepción, la oficina o área a la que se dirige y su ingreso debe estar previamente autorizado.

d. Todas las oficinas de la entidad que procesen almacenen y/o gestionen información reservada o sensible deben implementar y adoptar las medidas tendientes a asegurar dicha información.

e. Para aquellas oficinas cuyo acceso físico, se de a través de puertas, es deber del Jefe de Oficina correspondiente, salvaguardar las llaves de esta y asegurar una copia en un lugar diferente y seguro.

f. Los directorios telefónicos internos que identifican lugares o instalaciones de procesamiento de información sensible no deben ser fácilmente accesibles por el público.

g. Los materiales peligrosos o combustibles deben ser almacenados de manera segura a una distancia prudente de las áreas seguras. Los suministros como papelería no deben almacenarse en áreas seguras hasta que sea requerido.

h. Se deben utilizar circuitos cerrados de televisión (CCTV) para monitorear las actividades dentro y alrededor de los sitios críticos. Dicha labor está a cargo de la Dirección administrativa de TRANSMILENIO S.A.

i. Las salidas de emergencia deben tener alarma.

8.9.3 Protección contra amenazas externas y ambientales

TRANSMILENIO S.A debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de la infraestructura física, así como de la seguridad de la información y de las personas de la entidad, ante posibles eventos como incendios, inundaciones, terremotos, explosiones, ataques maliciosos, entre otros. Se debe dar cumplimiento de los siguientes lineamientos:

a. La Dirección de TICs debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

b. El propietario del activo de información debe propender porque éste se almacene en un ambiente protegido y seguro.

8.9.4 Trabajo en áreas seguras

a. En el centro de cómputo, deben existir sistemas de control ambiental de temperatura, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

b. La Dirección de TICs debe velar porque los recursos de la plataforma tecnológica de TRANSMILENIO S.A., ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

c. La Dirección de TICs debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

d. Cualquier cambio, modificación, actualización, ajuste o soporte que se realice sobre los procesos, áreas seguras y sistemas de procesamiento de información, que puedan afectar alguno o todos los pilares de seguridad de la información (integridad, confidencialidad y disponibilidad) deben pasar por la aprobación del Comité de cambios antes de su ejecución.

e. Se debe hacer uso de enrutamiento y/o medios de transmisión alternativos.

8.9.5 Áreas de despacho y carga

Las áreas de carga, descarga, entrega de mercancías y demás puntos de acceso a las instalaciones de TRANSMILENIO S.A., deben estar controladas y supervisadas con circuito cerrado de TV (CCTV), y en lo posible separadas de las áreas seguras para evitar el acceso no autorizado a éstas últimas. Se debe dar cumplimiento de los siguientes lineamientos:

a. El área de carga debe estar diseñada de tal manera que los suministros puedan ser descargados sin que el personal de entrega acceda a áreas críticas del edificio de TRANSMILENIO S.A.

b. El material entrante debe ser revisado por peligros potenciales antes de ser movido del área de carga al punto de utilización.

Excepciones:

Cualquier excepción a los lineamientos, debe ser justificada por quien (es) ejecute (n) el rol de Administrador o responsable, según aplique; debidamente validada por el líder u oficial de seguridad de la información de la entidad y aprobada por la Dirección de Tecnologías de la Información o quien haga sus veces.

9.0 POLÍTICA DE SEGURIDAD DE LOS EQUIPOS

Dominio/ Control: A.11.2 Equipos

Objetivo: prevenir la perdida, daño, o compromiso de activos, y la interrupción de las operaciones de TRANSMILENIO S.A.

Alcance: la presente política aplica para todos los funcionarios públicos, oficiales, contratistas y terceras partes, o que por su rol sean responsables de los equipos y activos de TRANSMILENIO S.A.

Lineamientos:

La seguridad de los Equipos y Activos de TRANSMILENIO S.A., permite prevenir pérdidas, daño o compromiso de los activos y la interrupción de las actividades del negocio. Se debe dar cumplimiento de los siguientes lineamientos:

a. La infraestructura tecnológica de TRANSMILENIO S.A. tal como, servidores, equipos activos, PBX's y otro tipo de hardware de computador que no resida típicamente en escritorios de usuario o en un área de trabajo común como laboratorios, call, centers, etc., deben estar ubicados físicamente en un área segura, y se deben implementar los controles necesarios para la prevención contra riesgos ambientales y no ambientales, que puedan afectar la disponibilidad de los datos.

b. Los computadores portátiles asignados a los funcionarios de TRANSMILENIO S.A., deben ser entregados con guaya de seguridad, para permitir su anclaje en el puesto de trabajo del usuario, a fin de mitigar el criterio de riesgo de robo

c. El hardware de computador debe estar protegido contra problemas eléctricos que puedan causar una falla o mal funcionamiento del equipo.

d. La Dirección TIC's debe garantizar que el cableado de energía eléctrica y de telecomunicaciones que transporta los datos o soporta los servicios de información de la entidad se encuentren adecuadamente protegidos para evitar daño o mala manipulación.

e. Las áreas de distribución de redes deben estar físicamente aseguradas para prevenir la modificación o el acceso no autorizado.

f. La instalación de cualquier tipo de software en los equipos de cómputo de TRANSMILENIO S.A., es responsabilidad de la Dirección de TICs y por tanto son los únicos autorizados para realizar o autorizar esta labor.

g. Los equipos deben ser mantenidos acorde con las especificaciones e intervalos de servicio recomendados por los Fabricantes y se deben mantener los registros de todas las fallas reales o sospechosas.

h. Se deben asegurar los equipos fuera de las instalaciones de la organización y su salida debe estar autorizada por el responsable del área a la cual esté asignada la máquina.

i. Toda la información de TRANSMILENIO S.A. tendrá que ser removida del equipo antes de su disposición o reutilización.

j. Antes de cualquier venta o donación, todos los medios de almacenamiento deben ser borrados de acuerdo con los mecanismos de eliminación de información que adopte la entidad.

k. Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla definido por la Entidad. Estos cambios pueden ser realizados únicamente por la Dirección de TICs, para ello se debe disponer de un estándar de seguridad para estaciones de trabajo independientemente del sistema operativo.

l. La Dirección de TICs, define e informa la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realiza el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

m. La Dirección de TICs será la única dependencia encargada de la adquisición de software y hardware. El resto de las dependencias podrán a través de dicha dependencia realizar las debidas adquisiciones.

n. El acceso a unidades CD, DVD y dispositivos USB debe ser restringido, solamente podrá ser utilizado por el personal autorizado por la Dirección de TIC's.

o. El área de soporte de la Dirección de TICs no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de TRANSMILENIO S.A.

Excepciones:

Cualquier excepción a los lineamientos, debe ser justificada por quien (es) ejecute (n) el rol de Administrador o responsable, según aplique; debidamente validada por el líder u oficial de seguridad de la información de la entidad y aprobada por la Dirección de Tecnologías de la Información o quien haga sus veces.

9.1 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

Dominio/ Control: A.11.2.9 Política de escritorio limpio y pantalla limpia

Objetivo: establecer los lineamientos para prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de TRANSMILENIOS S.A.

Alcance: la presente política aplica para todos los funcionarios públicos, oficiales, contratistas y terceras partes, o que por su rol sean responsables de los equipos, activos y que tengan acceso a la información, en medio digital o físico de TRANSMILENIO S.A.

Lineamientos:

9.1.1 Escritorio limpio

La política de escritorio limpio aplica para toda la información de la entidad, para cual debe tenerse en cuenta la clasificación de información, requerimientos legales y contractuales y los correspondientes riesgos y aspectos culturales de la organización. Se debe dar cumplimiento de los siguientes lineamientos:

a. No se deben dejar documentos con información calificada como información pública reservada y pública clasificada. al alcance de personal no autorizado, en caso de tener este tipo de información en físico ésta debe ser guardada bajo llave en archivadores.

b. Ningún dispositivo móvil o documento que se encuentre en tránsito y que almacene información institucional debe dejarse al alcance de personal no autorizado.

c. No se debe consumir líquidos o alimentos cerca de dispositivos que procesen o almacenen información, así como en aquellos en los cuales se archive información de la entidad.

d. Documentos con información clasificada o sensitiva deben removerse de impresoras tan pronto como sea posible.

e. Información sensitiva o crítica del negocio en papel o en medios de almacenamiento electrónico debe estar protegida (idealmente en una caja o gabinete) cuando no se requiera, especialmente cuando no hay nadie en la oficina.

9.1.2 Equipo informático de usuario desatendido

Los usuarios deben asegurar que el equipo desatendido tiene una adecuada protección y están obligados a:

a. Terminar las sesiones activas cuando finalicen, a menos que puedan ser aseguradas por un mecanismo de bloqueo, por ejemplo, el protector de pantalla protegido con contraseña.

b. Usar el protector de pantalla con contraseña, el cual debe ser activado dentro del tiempo límite de inactividad. Este complementa el anterior mecanismo de bloqueo, pero no actúa como un reemplazo.

c. Cierre la sesión de usuario en computadores centrales y servidores cuando finalice la tarea (no es correcto apagar la pantalla o el equipo sin salir de la sesión de usuario).

d. Los computadores y terminales se deben dejar con las sesiones terminadas o protegidas con un mecanismo de bloqueo de pantalla y teclado controlado por una contraseña, cuando están desatendidos.

Excepciones:

Cualquier excepción a los lineamientos, debe ser justificada por quien (es) ejecute (n) el rol de Administrador o responsable, según aplique; debidamente validada por el líder u oficial de seguridad de la información de la entidad y aprobada por la Dirección de Tecnologías de la Información o quien haga sus veces.

9.2 POLÍTICA DE GESTIÓN Y CLASIFICACIÓN DE ACTIVOS

Dominio: A.8 Gestión de Activos

Objetivo: establecer los lineamientos para identificar los activos Institucionales y definir las responsabilidades de protección apropiadas.

Alcance: la presente política aplica para todos los funcionarios públicos, oficiales, contratistas y terceras partes, o que por su rol tengan bajo su propiedad o custodia, activos de información.

Lineamientos:

9.2.1 Responsabilidad por los activos

9.2.1.1 Inventario de activos

El Líder u oficial de seguridad de la información o quien haga sus veces, es el encargado de llevar a cabo funciones de orientación y apoyo en cada uno de los procesos institucionales a través de las actividades para la identificación de activos de información, con el objeto de contribuir a que los inventarios de activos de cada una de las dependencias de TRANSMILENIO S.A se encuentren alineados tanto con las Tablas de Retención Documental como con los criterios establecidos en el procedimiento de Identificación, Valoración y Clasificación de Activos de Información, asegurando que:

a. Toda la información contenida en los activos sea clasificada por su criticidad, valor y disposiciones normativas legales, atendiendo para ello lo indicado tanto por los propietarios de la información como por TRANSMILENIO S.A.

b. La Matriz de identificación y clasificación de activos de información permanezca en un repositorio seguro con acceso restringido.

c. La matriz de identificación y clasificación de activos de información se actualice por lo menos una vez al año y/o cuando se presenten retiros, adquisiciones o reemplazos en los activos identificados.

d. Mantener actualizado el inventario de los activos de información tecnológicos incluyendo redes, servidores, aplicaciones, dispositivos de red, estaciones de trabajo, portátiles y licencias de software, así como aires acondicionados, generadores de energía, unidades de potencia (UPS).

e. Los activos de Hardware deben ser marcados con un ID único de acuerdo con los métodos de etiquetado de TRANSMILENIO S.A.

f. Cada uno de los activos debe estar identificado como:

- Misión Crítica.
- No-Crítica

9.2.1.2 Propiedad de los activos de información

Quien ejerza las funciones de propietario de activos de información en TRANSMILENIO S.A deberá:

a. TRANSMILENIO S.A. debe identificar a los propietarios para todos los activos de información y asignar la responsabilidad del mantenimiento de los controles para la adecuada protección de estos.

b. Procurar que todos los activos de información bajo su propiedad se encuentren debidamente inventariados.

c. Verificar que los activos de información sean clasificados y protegidos de acuerdo con el nivel de criticidad, valoración y disposiciones normativas legales.

d. Revisar al menos una vez al año o cuando ocurra un cambio significativo, las restricciones y clasificaciones de acceso a los activos de información.

e. Verificar que los procesos de eliminación o destrucción no permitan la exposición de los activos de información a terceros.

9.2.1.3 Uso aceptable de los activos de información

Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información y todos los servidores públicos, contratistas, proveedores, terceras partes, deben acatar y dar estricto cumplimiento a lo prescrito en la Guía de Uso Aceptable de los Activos de Información.

9.2.1.4 Devolución de los activos de información

Todos los empleados, contratistas y usuarios de terceras partes deben retornar todos los activos que posean de TRANSMILENIO S.A., a la terminación de su empleo o contrato. Se debe dar cumplimiento de los siguientes lineamientos:

a. El proceso de terminación debe ser formalizado e incluir el retorno de todo el software emitido previamente, documentos corporativos y equipos. Esto incluye dispositivos de computación móvil, tarjetas de acceso, carné, manuales, información almacenada en medios electrónicos, dispositivos de autenticación, entre otros.

b. La Dirección de TICs debe asegurar que sobre todo activo de información, que sea devuelto o vaya a ser traspasado o destruido, se ejecute un borrado seguro a fin de evitar que la información sea conocida por personal no autorizado.

c. Una vez finalizado el vínculo con la entidad, el Superior Inmediato o Supervisor contractual (según sea el caso) deberá solicitar a la mesa de ayuda de la entidad, la aplicación de las herramientas de borrado seguro sobre la información institucional alojada en el activo de información utilizado para la ejecución de las funciones u obligaciones contractuales.

9.2.2 Clasificación de la información

La información de TRANSMILENIO S.A. se debe clasificar de acuerdo con las siguientes 4 categorías:

a. Información pública. Es toda información no sensible para la divulgación al público que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

b. Información pública clasificada. Es aquella información que es sensible o confidencial dentro de la Entidad y destinada a uso de TRANSMILENIO S.A., solo la pueden acceder algunos funcionarios de acuerdo con sus funciones y responsabilidades.

c. Información pública reservada. Es aquella información que es extremadamente sensible o privada del más alto valor para la entidad y destinada para un grupo de personas de confianza de la Organización; cualquier violación a este tipo de información puede ocasionar daño a intereses públicos.

d. Información publicada o divulgada. Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión.

Los dueños de los procesos están obligados a clasificar y dar el tratamiento adecuado a la información de acuerdo con estos niveles y siguiendo los lineamientos de la Guía de Clasificación y Rotulado de Información.

La eliminación y destrucción de la información debe realizarse de acuerdo con su nivel de clasificación y siguiendo los lineamientos establecidos por Gestión Documental.

9.2.2.1 Etiquetado de la información

Cada activo debe poseer un etiquetado en donde se identifique el nivel de clasificación asignado. El etiquetado debe ser utilizado para aquella información que se encuentre contenida tanto en medio físico como en medio electrónico.

9.2.2.2 Manejo de activos de información

Para el manejo, procesamiento, almacenamiento y comunicación de la información se debe considerar la clasificación anteriormente definida.

9.2.2.3 Gestión de medios removibles

a. Cualquier dispositivo de almacenamiento de información (cintas, discos, casetes, unidades USB y reportes impresos entre otros) de propiedad de TRANSMILENIO S.A., se constituye en un activo de información, por tanto, el ingreso, uso, movilización y salida, debe ser previamente autorizado por la (s) dependencia (s) competentes. Lo anterior de acuerdo con el Protocolo T-DT-003: Protocolo a seguir para gestionar el uso de los medios removibles.

b. No se deben utilizar dispositivos de almacenamiento de información personales para guardar información de la entidad.

c. Se debe mantener un inventario actualizado de los dispositivos de almacenamiento de información de la entidad y de sus propietarios.

d. Se deben implementar mecanismos de cifrado, cuando sea requerido, en cada uno de los dispositivos de almacenamiento de información de la entidad.

e. Los propietarios de medios deben asegurar que éstos no queden desatendidos debido a que pueden ser susceptibles de pérdida o robo de la información. El propietario es el único

responsable de mantener la confidencialidad, integridad y disponibilidad de la información contenida en el medio a su cargo.

f. La protección a los medios debe hacerse de acuerdo con el nivel de clasificación de la información contenida en ellos.

g. Si ya no se requieren los contenidos previos de cualquier medio reutilizable, que será removido de la organización, deben ser borrados (eliminados). Para tal efecto se debe realizar solicitud al correo soportetecnico@transmilenio.gov.co.

h. Todos los medios deben ser almacenados en un ambiente seguro de acuerdo con las especificaciones de los fabricantes.

9.2.2.4 Eliminación de los medios

a. Una vez terminado el ciclo de vida útil de un determinado medio de almacenamiento, la información allí contenida, debe ser eliminada de manera segura de acuerdo con los procedimientos formales previamente establecidos por la Entidad.

b. Para eliminar activos de información sensible se debe garantizar mantener un registro mediante acta donde sea posible con el fin de mantener una pista de auditoría.

c. Para la destrucción de Disco contenedores de información se debe realizar un borrado a bajo nivel garantizando la eliminación total de esta. Se debe dejar registro de esto.

9.2.2.5 Transferencia de medios físicos

La información puede ser vulnerable a acceso no autorizado, uso indebido y pérdida o corrupción durante el transporte físico.

El transporte de los medios de almacenamiento de la entidad debe darse de acuerdo a la clasificación de la información contenida en éstos, para ello se deben utilizar servicios de mensajería confiables, verificarlos tipos de monitoreo, las técnicas de embalaje y llevar un registro correspondiente a los medios de almacenamiento transportados.

Excepciones:

Cualquier excepción a los lineamientos, debe ser justificada por quien (es) ejecute (n) el rol de Administrador o responsable, según aplique; debidamente validada por el líder u oficial de seguridad de la información de la entidad y aprobada por la Dirección de Tecnologías de la Información o quien haga sus veces.

9.3 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

Dominio/ Control: A.10.1.1 Política sobre el uso de controles criptográficos

Objetivo: establecer los lineamientos para asegurar el uso apropiado y eficaz de la criptografía a fin de proteger la confidencialidad, la autenticidad y/o la integridad de la información.

Alcance: la presente política aplica para todos los funcionarios públicos, oficiales, contratistas y terceras partes, o que por su rol hagan uso de controles criptográficos, cuando se requiera.

Lineamientos:

Quien (es) ejecute (n) el rol de administrador de herramientas criptográficas debe (n) identificar los sistemas y aplicaciones en los que se considere necesario hacer uso de controles criptográficos para proteger la información. El uso de controles criptográficos quedará determinado por el análisis de riesgos del sistema, así como el nivel o fortaleza de los mecanismos de cifrado a utilizar (algoritmos, longitudes de clave mínimas, etc.).

Se debe dar cumplimiento de los siguientes lineamientos:

a. Utilizar Las herramientas y mecanismos de cifrado (simétricos y asimétricos) estandarizados en la entidad.

b. Determinar el uso de mecanismos de cifrado de acuerdo la sensibilidad de la información y su nivel de clasificación, así como los sistemas y líneas de comunicaciones por los que se almacena, procesa o transmite la información. Así como los requisitos legales.

c. Se debe realizar una gestión segura de todas las claves criptográficas, por parte de quienes requieran su uso, con el objeto de garantizar la eficacia de los controles criptográficos.

d. Quien (es) ejecute (n) el rol de Administrador debe(n) documentar los pasos necesarios para el registro, generación, distribución, almacenamiento, recuperación, renovación, revocación y

destrucción de las claves criptográficas y debe mantener un registro de actividad que evidencie su cumplimiento y permita su posterior revisión o auditoría.

e. Cuando se utilicen mecanismos de cifrado simétrico o de clave privada (compartida), se debe garantizar la confidencialidad en el intercambio de las claves (por un canal seguro o cifradas mediante mecanismos de cifrado asimétrico).

f. Cuando se utilicen mecanismos de cifrado asimétricos o de clave pública/privada, se debe:

g. En el intercambio de claves públicas, la autenticidad e integridad de las mismas deben quedar avaladas por una autoridad de certificación de confianza, bien sea interna (PKI interna) o externa

h. En el caso de uso de servicios criptográficos de terceros, los acuerdos de prestación de servicios deben cubrir aspectos de responsabilidad civil, fiabilidad y seguridad del servicio y tiempos de provisión.

i. Los tokens de seguridad suministrados a los servidores públicos y/o contratistas, para realizar consulta, modificación, trasmisión de información, pagos, entre otros fines, deberán ser guardados en un lugar seguro bajo llave, libre de acceso al mismo.

Excepciones:

Cualquier excepción debe ser autorizada por la dirección de Tecnologías de la Información y/o el Líder u oficial de Seguridad de la información de la entidad.

9.4 POLÍTICA DE DESARROLLO SEGURO

Dominio/ Control: A.14.2.1 Política De Desarrollo seguro

Objetivo: asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

Alcance: la presente política aplica para los sistemas informáticos, tanto desarrollos propios como de terceros, que integren cualquiera de los ambientes administrados por TRANSMILENIO S.A (desarrollo, producción y/o pruebas).

Lineamientos:

9.4.1 Confidencialidad

a. La protección de la confidencialidad de los activos de información de la Entidad se encuentra delimitada por el nivel al que pertenezca dicha información conforme a su clasificación y al nivel de evaluación de riesgo, para lo cual se debe considerar lo siguiente: TRANSMILENIO S.A., debe contar con ambientes tecnológicos separados:

- Se deben definir y documentar las reglas para la transferencia de software del ambiente de pruebas al ambiente de producción.
- Los cambios en los sistemas operativos y aplicaciones se deben poner a prueba en un entorno de pruebas antes de aplicarlos a los ambientes de producción.
- Las pruebas no se deben llevar a cabo en el ambiente de producción;
- Los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no deben ser accesibles desde los ambientes de producción cuando no se requiera.
- Los usuarios deben usar diferentes perfiles de usuario para los ambientes de producción y los ambientes de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error.

b. Los datos sensibles no se deben copiar en el ambiente de pruebas, salvo que se suministren controles equivalentes al ambiente de producción.

c. La ejecución del análisis de vulnerabilidades tiene como fin, identificar las brechas de seguridad con las que cuenta un sistema de información, por lo tanto, la Entidad debe ejecutar análisis de vulnerabilidades a los sistemas activos de información, para lo cual se debe:

- Documentar los resultados.
- Priorizar las vulnerabilidades.
- Documentar el plan de acción para corregir o mitigar (según sea el caso) las brechas identificadas.
- Entregar los resultados de las pruebas realizadas a cada uno de los responsables del desarrollo del sistema de información o aplicación, quién es el encargado de definir y aplicar el debido plan de remediación.

d. Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Dirección de Tecnología de la Información y las Comunicaciones con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.

e. El software que se adquiera a través de los proyectos o programas debe quedar a nombre de TRANSMILENIO S.A.

9.4.2 Ciclo de vida del software - SDLC

La entidad debe garantizar que los criterios de seguridad de la información se cumplan en todas las etapas de desarrollo y durante todo el ciclo de vida de un determinado software, con el objeto de incluir los requisitos de seguridad de la información en la metodología utilizada para tal fin en el que se establezcan las directrices de codificación seguras para cada lenguaje de programación usado. y se apliquen los siguientes pasos:

a. Análisis de requerimientos.
b. Análisis arquitectónico.
c. Tipo de desarrollo (propio o a terceros).
d. Pruebas (funcionales, no funcionales y de seguridad)
e. Producción
f. Mantenimiento

TRANSMILENIO S.A., asegurará que el software adquirido y desarrollado tanto al interior de la Entidad, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por ésta.

La Dirección de TICs incluirá requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

En caso de desarrollos propios de la entidad se debe verificar que están completamente documentados, que las diferentes versiones se preservan adecuadamente en varios medios y se guarda copia de respaldo externa a la entidad y que sean registrados ante la Dirección General de Derechos de Autor del Ministerio del Interior y de Justicia.

9.4.3 Migración a ambiente de producción

En el ambiente de producción se ubicarán todos los servidores y aplicativos que prestarán los servicios a los usuarios finales internos y/o externos a la entidad. Luego que la etapa de pruebas llegue a su fin y se tenga un aplicativo estable en ambiente de pruebas donde se haya probado la instalación y la funcionalidad, el responsable de la aplicación desarrollada, debe hacer una solicitud de cambio al Comité de cambios para migrar de manera controlada dicho aplicativo hacia producción. Para poder recibir un software en el ambiente de Producción se debe tener en cuenta las siguientes condiciones:

a) Tipo y clasificación de la información que maneja.

b) Características del respaldo y restauración (cantidad de información, periodicidad, crecimiento esperado, tiempo de retención, tiempo aceptable de recuperación, desde cuándo se debe recuperar).

c) Plan de contingencia (preferiblemente alineado con el plan de continuidad de la entidad).

d) Documento de control de cambios o documentación de implementación.

e) Resultado del plan de pruebas detallado y exhaustivo (con pruebas de desempeño y funcionales).

f) Pruebas de seguridad y controles aplicados a la mitigación o respuesta al riesgo.

g) Manual de diseño.

9.4.4 Cifrado de datos sensibles

Se debe contar con un algoritmo criptográfico para el cifrado de datos sensibles, siempre que se garanticen los tres pilares de la seguridad de la información.

Se debe contar con mecanismos de autenticación por usuario y contraseña siguiendo la Política de control de acceso a la información de TRANSMILENIO S.A.

Se debe contar con mecanismos de parametrización para generar pistas de auditoría de eventos tales como accesos a la información y con el objeto de evidenciar potenciales violaciones a la confidencialidad de la información.

9.4.5 Integridad

En lo que respecta a todas las aplicaciones de TRANSMILENIO S.A., se deben implementar mecanismos cuyo objeto sea el de propender por la integridad del activo de información con base en el nivel de clasificación y el nivel de evaluación de riesgo identificado.

El área de soporte de la Dirección de Tics de TRANSMILENIO S.A., será la única dependencia autorizada para realizar copia de seguridad del software original.

El software proporcionado por TRANSMILENIO S.A. no pueden ser copiados o suministrados a terceros.

Excepciones:

Cualquier excepción debe ser autorizada por la dirección de Tecnologías de la Información y/o el Líder u oficial de Seguridad de la información de la entidad.

9.5 POLÍTICA DE SEGURIDAD EN LAS OPERACIONES

Dominio: A.12. Seguridad de las operaciones.

Objetivo: establecer los lineamientos para las operaciones correctas y seguras de las instalaciones de procesamiento de información de TRANSMILENIO.

Alcance: la presente política aplica para todas las operaciones que se desarrollen en TRANSMILENIO S.A. a través de todos los funcionarios públicos, oficiales, contratistas y terceras partes.

Lineamientos:

Se debe dar cumplimiento de los siguientes lineamientos:

a) Los procedimientos operativos se deben documentar y poner a disposición de los funcionarios públicos, oficiales, contratistas y terceras partes que los necesitan.

b) Los procedimientos operativos específicos de TRANSMILENIO S.A., deben ser tratados como documentos formales y los cambios autorizados por el equipo de administración apropiado.

c) Se debe mantener un diagrama actualizado de la red de la Entidad.

d) TRANSMILENIO S.A., debe implementar un proceso documentado para la gestión de cambios, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

e) TRANSMILENIO S.A., debe realizar un análisis de capacidades y proyecciones de procesamiento y almacenamiento disponible. Estas proyecciones deben tener en cuenta los nuevos negocios y los requerimientos de sistemas y tendencias proyectadas y actuales en el procesamiento de la información.

f) Los ambientes de desarrollo, pruebas y producción deben estar separados para reducir los riesgos de accesos o cambios no autorizados a los sistemas en producción, así como posibles inconvenientes en la operación de estos.

g) La Dirección de TICs debe mantener una lista documentada y actualizada de los servicios, protocolos y puertos utilizados, incluyendo la justificación pertinente en los casos que se estén utilizando protocolos no seguros. En el caso de detectar protocolos inseguros, se debe contar con contramedidas para cerrar las vulnerabilidades encontradas.

h) El líder u oficial de seguridad de la información debe coordinar con la Dirección de TICs, una revisión semestral de la configuración de los dispositivos de seguridad.

i) Deben habilitarse sólo los servicios y protocolos necesarios y seguros según lo requiera la función del sistema.

j) Todo acceso administrativo a sistemas críticos de la Entidad que no sea por consola debe ser cifrado.

k) Todos los sistemas (servidores, equipos activos de red y máquinas de usuarios) deben contar con sincronización de reloj a nivel de sistema operativo, teniendo como referencia la Hora Legal Colombiana. No está permitida la desactivación del sistema de sincronización o la manipulación manual de la hora.

l) Se deben implementar controles de detección y prevención para proteger contra el software malicioso, así mismo se deben realizar procedimientos de concientización para el usuario.

m) Todos los equipos de cómputo de la Entidad deben tener instalados los parches de seguridad más recientes proporcionados por los fabricantes. La aplicación de los parches debe realizarse dentro de un periodo máximo de un mes a partir de su liberación.

n) Se deben generar y mantener registros de auditoría sobre las actividades de los usuarios, excepciones, fallas y eventos de seguridad de información para soportar futuras investigaciones y monitoreo del control de acceso.

o) Registrar las actividades realizadas por los usuarios administradores y operadores del sistema, con el fin de realizar revisiones de comportamiento y uso del acceso privilegiado por parte de los usuarios administradores y operadores, a intervalos planeados o cuando la Dirección de TIC's lo requiera.

p) Los registros de auditoría deberán revisarse y monitorearse de acuerdo con lo requerido por la Dirección de TICs, cuando ocurra un incidente de seguridad o por demanda. Lo anterior con el fin de identificar posibles eventos, incidentes, amenazas a la seguridad de la información o problemas de capacidad, entre otros. Los incidentes que sean detectados a partir de la revisión de los registros de auditoría deberán ser notificados de acuerdo con lo definido en los lineamientos de gestión de Incidentes.

q) Los registros de información se deben proteger contra intentos de alteración y/o acceso no autorizado.

r) La retención de los registros de auditoría dependerá de la capacidad de los sistemas de información o aplicaciones que tiene actualmente TRANSMILENIO S.A. Dependiendo de esto, la Dirección de TIC's dispondrá los recursos que estén a su alcance para su respectivo almacenamiento.

s) TRANSMILENIO S.A., debe implementar procedimientos para la gestión de vulnerabilidades técnicas.

t) TRANSMILENIO S.A., debe implementar procedimientos para controlar la instalación de software en sistemas en producción.

u) Está totalmente prohibida la instalación de software no autorizado en los equipos de TRANSMILENIO S.A.

v) Las herramientas de auditoría deben estar separadas de desarrollo y sistemas en producción y no permanecer en bibliotecas de cintas o áreas de usuarios, a menos que se le dé un nivel adecuado de protección adicional y que cuente con autorización para esto.

w) Se deben segregar funciones y áreas de responsabilidad con el fin de reducir las posibilidades de modificaciones no autorizadas o uso indebido de la información o servicios. Se debe tener

especial cuidado para que una persona no pueda ejecutar fraudes en las áreas de responsabilidad individual sin ser detectada.

x) Los registros y auditorias de TRANSMILENIO S.A. deben garantizar la evaluación de los controles, la eficiencia de los sistemas y el cumplimiento de los lineamientos establecidos por la entidad, así como las recomendaciones de las deficiencias o hallazgos detectados.

y) De igual forma la entidad, define los responsables de gestionar las auditorias de forma periódica a los activos de información críticos y no críticos de la entidad, de acuerdo con los parámetros establecidos por el área o proceso responsable para tal fin; los cuales deben estar alineada a los objetivos estratégicos, a los procesos y a la normatividad legal vigente de la entidad.

z) Todas las evidencias que se recolecten como resultado de las auditorías practicadas, deben contar con un lugar para el almacenamiento de los registros y monitoreo de los eventos de seguridad.

aa) El profesional especializado 06 de seguridad de la información de la Dirección de TICs tiene la responsabilidad de mantener el contacto con las autoridades y verificar el cumplimiento de la ley, así como las normas expedidas relacionadas con la seguridad de la información y que podría impactar la seguridad de la información de TRANSMILENIO S.A.

Excepciones:

Cualquier excepción debe ser autorizada por la Dirección de Tecnologías de la Información y el Líder u oficial de Seguridad de la información de la entidad.

9.6 POLÍTICA DE COPIAS DE RESPALDO

Dominio: A.12.3 Copias de Respaldo.

Objetivo: definir las pautas generales para garantizar en TRANSMILENIO S.A., la preservación, mantenimiento y verificación de copias de respaldo de la información.

Alcance: la presente política aplica para todos los todos los funcionarios públicos, oficiales, contratistas que hacen parte de la dirección de Tecnologías de la Información y que son responsables de las copias de respaldo.

Lineamientos:

Se debe dar cumplimiento de los siguientes lineamientos:

a) TRANSMILENIO S.A. debe seguir un procedimiento definido para las actividades de backup, teniendo en cuenta la criticidad y las necesidades de disponibilidad de los datos. Este procedimiento debe estar debidamente documentado para seguimiento y control.

b) TRANSMILENIO S.A. deberá proporcionar almacenamiento seguro a largo plazo fuera del sitio principal para sus backup. La información pertinente a las bases de datos administrativas se replica en un sitio en la nube dispuesto para tal fin por el fabricante Microsoft.

c) La información de backup debe tener un adecuado nivel de protección física y ambiental, acorde con los estándares aplicados al sitio principal. Los controles aplicados a los medios del sitio principal deben ser extendidos al sitio de respaldo externo. Estos controles deben tener en cuenta los estándares de clasificación de datos.

d) Es responsabilidad de quien (es) ejecute (n) el rol de administrador de cada sistema de información, realizar la solicitud de copia a quien (es) ejecute (n) el rol de administrador de backup, validar y asegurar que su sistema de información se encuentre contemplado en el cronograma de copias de seguridad, además de hacer seguimientos regulares a su ejecución.

e) Quien (es) ejecute (n) el rol de Administrador de backup debe validar el resultado de la ejecución de las copias de seguridad y registrar las novedades en la bitácora establecida para ello.

f) Es responsabilidad de quien (es) ejecute (n) el rol de Administrador de backup realizar pruebas de restauración de copias de seguridad de manera trimestral siguiendo los lineamientos del Procedimiento Backup y Recuperación de la Información.

g) Cada copia de seguridad debe quedar registrada en la máquina donde son realizados (logs de servidor) y en un archivo externo (texto, planilla, etc.) que permita mantenerla disponible para controles o auditoría.

h) Los medios de respaldo removibles deben ser trasladados a un lugar externo que garantice el catálogo, la fiabilidad, seguridad y disponibilidad de estos. Para ello se debe asegurar un transporte o un servicio de mensajería fiable que cuente con todas las medidas de seguridad.

Excepciones:

Toda excepción debe ser validada por el líder u oficial de seguridad de la información y posteriormente aprobada por la dirección de la Oficina de Tecnologías de la Información o quien haga sus veces.

9.7 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES

Dominio: A.15 Relaciones con los proveedores

Objetivo: establecer los lineamientos para asegurar la protección de los activos de la entidad que sean accesibles a los proveedores.

Alcance: la presente política aplica para todos los proveedores o terceras partes que requieran acceso a los activos de información de TRANSMILENIO S.A y para los funcionarios públicos, oficiales y contratistas que establezcan dichos accesos.

Lineamientos:

a. Durante la etapa precontractual, desde la construcción de los estudios previos, el Área solicitante de la contratación, debe identificar los riesgos de seguridad de la información con el apoyo del líder u oficial de seguridad de la información, los cuales deben ser parte de la estimación y cobertura de los riesgos del proceso de contratación. De acuerdo con lo anterior, el análisis de riesgos de seguridad de la información debe incluir la identificación de los mismos en la respectiva contratación, su clasificación, probabilidad de ocurrencia estimada, su impacto, la determinación de la parte que debe asumirlos, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.

b. Así mismo, el Comité evaluador debe identificar sí el objeto de la propuesta u oferta evaluada, requiere del acceso de los proveedores a la información reservada o sensible de la entidad, sistemas de información y/o áreas seguras de la entidad; de ser así, el Comité evaluador debe contar con la participación del Líder u oficial de seguridad de la información a fin de determinar los requisitos mínimos de seguridad y los controles necesarios por parte del proveedor para ejecutar dicho contrato.

c. En medio de la Etapa Contractual, se debe asegurar la inclusión de la cláusula de confidencialidad, protección de datos, derechos de propiedad intelectual, las políticas de seguridad y privacidad de la información y derechos de autor, en la suscripción y

perfeccionamiento del contrato que se celebre entre la entidad y aquellos proveedores que tendrán acceso a la información reservada o sensible de TRANSMILENIO S.A.

d. Antes de iniciar la ejecución del contrato, el supervisor debe socializar a los proveedores las políticas, normas y procedimientos de seguridad de la información de TRANSMILENIO S.A., a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, así como el Procedimiento para la gestión de incidentes de seguridad de la información y acordar el canal para su debido reporte.

e. Como parte de la supervisión a la ejecución del contrato, se debe contemplar procesos de auditoria a proveedores cuyo objetivo sea validar el cumplimiento de los requisitos de seguridad de la información estipulados en la etapa contractual, dichos resultados deben quedar consignados también en los informes presentados por el supervisor del contrato.

f. Durante la Etapa Post Contractual, es función del supervisor y/o interventoría asignada, monitorear y hacer seguimiento a los controles pactados para asegurar la confidencialidad, integridad y disponibilidad de la información, frente a los riesgos previamente identificados.

g. Para los servicios de tecnología y de comunicaciones contratados externamente, se debe exigir que los proveedores divulguen los requisitos y prácticas de seguridad de la entidad, a lo largo de la cadena de suministro.

h. Toda gestión del proveedor que represente una modificación, mantenimiento, revisión al servicio de tecnología de la información, comunicaciones o equipos de suministros, debe pasar por el Procedimiento Gestión de Cambios y seguir las directrices del Líder u oficial de seguridad de la información, antes de su ejecución.

i. Para la contratación de servicios o componentes de la infraestructura de TI y/o áreas seguras, se debe exigir a los proveedores la presentación de los planes de contingencia que aseguren la disponibilidad de la información, suministrada y procesada entre las partes.

j. Para lo relacionado con la revisión de informes de interventoría al contrato de concesión del SIRCI y para la generación de informes de supervisión, se debe seguir el protocolo T-DT-001: Protocolo para revisión de informes de interventoría al contrato de concesión del SIRCI y generación del informe de supervisión.

k. Los demás lineamientos deben aplicarse de acuerdo con el Manual de Contratación GRFT-GC-MP-001 establecido por la entidad.

Excepciones:

Cualquier excepción a los lineamientos, debe ser justificada por el Área solicitante, el comité evaluador o el supervisor del contrato, según aplique; y aprobada por el Líder u oficial de seguridad de la información de la entidad.

9.8 POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

Dominio: A.18.1.4 Privacidad y Protección de Información de Datos Personales

Objetivo: evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

Alcance: la presente política aplica para todos los funcionarios públicos, oficiales, contratistas y terceras partes, o que, por su rol, tengan bajo su responsabilidad o suministren datos personales a la entidad. Adicional es de libre consulta para los TITULARES.

Lineamientos:

TRANSMILENIO S.A. en cumplimiento a lo establecido por las normas vigentes**:** Ley 1266 de 2008, Ley 1581 de 2012 y el Decreto 1377 de 2013, actúa como responsable de los datos personales que se encuentren en sus bases de datos y cada de una de las dependencias de la entidad actúa como Encargado del tratamiento.

Por tanto, TRANSMILENIO S.A. podrá dar tratamiento a los datos personales de TITULARES con los cuales tiene, ha tenido o espera tener algún tipo de relación, cualquiera sea su naturaleza (civil, comercial y/o laboral, etc.) y entre los cuales se incluyen, pero sin limitarse, los grupos de interés (usuarios directos, usuarios indirectos, terceros relacionados y entidades externas)[2] Salvo en los casos exceptuados por la ley, la entidad solicitará a más tardar en la recolección de la información, autorización del TITULAR para capturar, almacenar, procesar y tratar los datos personales que hayan sido suministrados a la entidad por cualquier medio, bien sea digital o físico, y en desarrollo de su objeto social o con ocasión de cualquier tipo de relación civil o comercial que llegue a surgir en virtud de sus actividades conexas o propias de su naturaleza; dicha autorización deberá estar contenida en un documento físico o electrónico, como se ilustra a continuación:

[2] Ver Art. 10 Ley 1581 de 2012

TRANSMILENIO S.A. en calidad de Responsable del tratamiento de los datos personales suministrados por sus beneficiarios, funcionarios, contratistas, proveedores, terceros, usuarios y otros interesados, de conformidad con el artículo 9 de la Ley 1581 de 2012 , solicita la autorización de dichos TITULARES para que de manera libre, previa, expresa, voluntaria, y debidamente informada permitan a la Entidad, efectuar o continuar con el almacenamiento, uso, circulación y tratamiento de sus datos, información que es y será utilizada en el desarrollo de las funciones propias de la Entidad, de acuerdo con la política de Privacidad y protección de información de datos personales la cual se encuentra publicada para consulta en la página web: http://www.transmilenio.gov.co/Publicaciones/la_entidad/transparencia_y_acceso_a_la_informacion_publica_transmilenio.

Ilustración 2. Modelo Solicitud de autorización

Para todos los efectos, se entiende que la autorización por parte de los TITULARES a favor de TRANSMILENIO S.A., para el suministro y/o tratamiento de sus datos personales, realizada a través de los canales físicos o electrónicos, o por escrito o mediante conductas inequívocas, es:

Expresa y voluntaria, lo que implica que EL TITULAR y/o sus representantes, según sea el caso, acepta todo el contenido de la presente y le concede(n) a la entidad su autorización para que utilice dicha información personal conforme a las estipulaciones de la presente política, la cual también está publicada en la página web *www.transmilenio.gov.co*, obligándose a leerla, conocerla y consultarla en desarrollo del derecho que le asiste como TITULAR de datos personales.

En el evento en que desee manifestar su negativa frente a la mentada autorización o solicitar la supresión de la información, podrá ejercer su derecho a través del correo contactenos@transmilenio.gov.co o en cualquiera de los puntos de atención al ciudadano, dentro de los 30 días hábiles siguientes a la implementación y publicación de la Política de Privacidad y Protección de Datos Personales de TRANSMILENIO S.A.
Una vez vencido el periodo señalado anteriormente, la entidad podrá mantener un tratamiento sobre los datos suministrados con anterioridad a esta legislación, en atención a lo consagrado en el numeral

cuarto del artículo 10° del Decreto 1377 de 2013, sin perjuicio de la facultad que tiene en calidad de Titular de la Información de ejercer en cualquier momento su derecho.

No obstante, se hace la salvedad que de conformidad al artículo 9 del decreto 1377 del año 2013, la solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular de esta, tenga un deber legal o contractual de permanecer en la base de datos de la entidad.

Por su parte, TRANSMILENIO S.A. asegura un manejo adecuado de los datos personales recolectados en sus bases de datos, registros de Ingreso a las instalaciones, registro fotográfico, firmas de asistencia, y de más medios de recolección, con el fin de proteger la privacidad de la misma y conservarla bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, así como el respeto de los derechos del TITULAR, según lo estipulado en la ley. De esta manera la entidad manifiesta que garantiza los derechos de privacidad, la intimidad, el buen nombre y la autonomía en el tratamiento de los datos personales, en consecuencia, todas sus actuaciones se regirán por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

Todas las personas que, en desarrollo de diferentes actividades, contractuales, laborales, entre otras, sean permanentes u ocasionales, llegaran a suministrar a TRANSMILENIO S.A cualquier tipo de información o dato personal, podrá conocerla, actualizarla y rectificarla. En efecto, TRANSMILENIO S.A.:

a. Garantiza al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b. Conserva la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
c. Realiza oportunamente la actualización, rectificación o supresión de los datos en los términos que estipula la ley.
d. Actualiza la información reportada por los Encargados del Tratamiento en los términos que estipula ley.
e. Tramita las consultas y los reclamos formulados por los TITULARES en los términos señalados en la ley.

f. Se abstiene de circular información que esté siendo controvertida por el TITULAR y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

g. Permite el acceso a la información únicamente a las personas que pueden tener acceso a ella.

h. Informa a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los TITULARES.

i. Cumple las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Cualquier consulta, reclamo o requisito debe ser dirigido a través de los diferentes sitios y canales de atención dispuestos por TRANSMILENIO S.A. para tal fin, los cuales se pueden consultar en la página web www.transmilenio.gov.co

Excepciones:

Las excepciones establecidas por Ley.

9.9 POLÍTICA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Dominio: A.17.1 Continuidad de Seguridad de la Información.

Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización, TRANSMILENIO S.A. proporcionará los recursos suficientes para dar una respuesta efectiva a los procesos en caso de contingencia o eventos catastróficos que se presenten en la Entidad y que afecten la continuidad de su operación.

Alcance: La presente política establece que TRANSMILENIO S.A debe determinar sus requisitos para la Continuidad del negocio, basados en la planificación, implementación y verificación de los mismos, para todos los procesos de la entidad.

Lineamientos:

Se debe dar cumplimiento de los siguientes lineamientos:

a. La política debe determinar sus requisitos para la Seguridad de la Información y la Continuidad de la Gestión de la Información en situaciones adversas, por ejemplo, durante una crisis o desastres.

b. La entidad a través de la dirección de planeación debe liderar el plan de continuidad del negocio.

c. La Dirección de Tics, debe elaborar el plan de recuperación ante desastres y retorno a la normalidad, para cada uno de los servicios y sistemas de información que tengan un impacto alto en los procesos de la entidad.

d. Debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

e. Debe verificar a intervalos regulares los controles de Continuidad de la Seguridad de la Información, implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

f. Se debe establecer, documentar y mantener procesos, procedimientos para asegurar el nivel de Continuidad requerido para la Seguridad de la Información durante una situación adversa.

9.9.1 Redundancia

Se debe asegurar la disponibilidad de instalaciones de procesamiento de información. TRANSMILENIO S.A propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la entidad. Se debe dar cumplimiento de los siguientes lineamientos:

a. Analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la entidad y la plataforma tecnológica que los apoya.

b. Evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de TRANSMILENIO S.A.

c. A través de sus funcionarios, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la entidad.

Excepciones:

Toda excepción debe ser validada por el líder u oficial de seguridad de la información y posteriormente aprobada por la dirección de la Oficina de Tecnologías de la Información o quien haga sus veces.

10.0 POLITICA GESTIÓN DE INCIDENTES DE LA INFORMACIÓN

Dominio: A.16.1 Gestión de incidentes y mejoras en la Seguridad de la Información.

Objetivo: asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Alcance: la presente política aplica para todos los funcionarios públicos, oficiales, contratistas y terceras partes, deben reportar todo evento o incidente de seguridad de la información a la Mesa de ayuda, a través de los canales oficiales establecidos por la entidad, y estos a su vez, deben ser gestionados por los responsables de acuerdo con el procedimiento establecido para tal fin.

Lineamientos:

Se debe dar cumplimiento de los siguientes lineamientos:

a) TRANSMILENIO S.A , promoverá entre los Funcionarios, Contratistas, Proveedores y Terceras partes, ante la existencia de una anomalía, evento o incidente de seguridad de la información (informáticos y no informáticos) en el cual se comprometa los recursos tecnológicos, sistemas de información, información física, demás medios en el que se encuentre información institucional y las personas, y que a su vez se afecte uno (1) o todos los pilares fundamentales de seguridad como son: Confidencialidad, Integridad y Disponibilidad de la información; ellos deberá reportar dicha novedad de manera inmediata, a través de los canales de comunicación oficiales definidos por la entidad.

b) De tal forma que dichos incidentes deben ser atendidos a través de una serie de normas, reglamentos, procedimientos y/o protocolos a seguir, donde se definen las distintas medidas a tomar para identificar, prevenir, priorizar los incidentes identificados los cuales se les debe documentar, solucionar, realizar seguimiento y posterior cierre por las responsables del equipo de manejo de incidentes al interior de la entidad o personal externo según sea el caso; al igual se debe tener en cuenta los aspectos legales a los cuales se debe dar cumplimiento.

c) Los propietarios de los activos de información deben informar a la Dirección de Tics de TRANSMILENIO S.A., a través de la mesa de ayuda (soportetecnico@transmilenio.gov.co), los incidentes de seguridad que identifiquen o que reconozcan ante su posibilidad de materialización.

d) La Alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

e) Se debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.

f) Se debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

g) En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios deben notificarlo a la Dirección de Tics para que se registre y se le dé el trámite necesario.

Excepciones:

Toda excepción debe ser validada por el líder u oficial de seguridad de la información y posteriormente aprobada por la dirección de la Oficina de Tecnologías de la Información o quien haga sus veces.

10.1 POLÍTICA DE CULTURA Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Dominio: A.7.2.2 Toma de conciencia, educación y formación en la Seguridad de la Información.

Objetivo: asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

Alcance: la presente política aplica para todos los servidores públicos, contratistas, proveedores, terceras partes, los cuales deben participar activamente en los programas de sensibilización que realiza la entidad para SGSI.

Lineamientos:

Se debe dar cumplimiento de los siguientes lineamientos:

a) Se debe sensibilizar y divulgar a través de los medios establecidos por la entidad sobre la Seguridad de la Información, en donde a cada servidor público, contratista, proveedor y terceras partes deben participar activamente en los Programas o Planes de Cultura y Sensibilización en Seguridad de la Información desarrollados por la Dirección de Tecnología de Información – TICS,

y de acuerdo al contenido debe ser interiorizado y aplicado según corresponda su rol y responsabilidad dentro de la entidad.

b) Para realizar el contenido de los Programas o Planes de Cultura y Sensibilización de Seguridad de la Información deben enmarcarse en tres (3) fases:

- **Diseño.** Deben ser diseñados teniendo en cuenta la misión de la entidad, identificación de las necesidades y prioridades (verificación de Incidentes de Seguridad), elaboración de indicadores o métricas de desempeño que permitan generar resultados.
- **Desarrollo.** Elaborar material de entrenamiento en el que se pueda emplear una buena pedagogía para la difusión de los temas de Seguridad y este debe ser sometido aprobación por el comité integrado de Gestión SIG, antes de la puesta en marcha.
- **Implementación.** Socializar el programa o Plan de Cultura Sensibilización de Seguridad de la Información de la entidad que fue diseñado y desarrollado al igual que emplear los indicadores o métricas para evaluar el desempeño del Programa o Plan.

c) Se debe incorporar dentro del ciclo de vida del Programa o Plan los nuevos avances tecnológicos, nuevas amenazas y vulnerabilidades, modalidades de ingeniería social, nueva normatividad vigente y actualizar el plan de cultura y sensibilización anualmente.

Excepciones:

Toda excepción debe ser validada por el líder u oficial de seguridad de la información y posteriormente aprobada por la dirección de la Oficina de Tecnologías de la Información o quien haga sus veces.

10.2 POLÍTICA DE CUMPLIMIENTO

Dominio: A.18.1 Cumplimiento de requisitos legales y contractuales.

Objetivo: evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

Alcance: la presente política establece que se debe dar cumplimiento a los requisitos estatutarios, reglamentarios y contractuales pertinentes, establecidos por TRANSMILENIO S.A a través de las políticas de seguridad y privacidad de la información.

Lineamientos:

a. TRANSMILENIO S.A. implementará los procedimientos a que haya lugar para asegurar el cumplimiento de ley y requerimientos regulatorios y contractuales acerca de la propiedad intelectual, patentes, secretos de comercio y marcas.
b. El incumplimiento a la Política de Seguridad y Privacidad de la información de TRANSMILENIO S.A, traerá consigo, las consecuencias legales que aplique a la normativa vigente de la entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

10.2.1 Sanciones para las violaciones de las políticas de seguridad de la información

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre todos los servidores públicos, contratistas, proveedores y terceras partes de TRANSMILENIO S.A. Por tal razón, el incumplimiento del presente manual podrá presumirse como causa de responsabilidad administrativa, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, sí así lo ameritan.

Excepciones:

Las excepciones establecidas por Ley.

10.3 REVISIÓN DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACION

Dominio: A.18.2 Revisión de Seguridad de la Información.

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

Alcance: La presente política establece revisiones necesarias al SGSI, para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque de la entidad para gestionar la seguridad de la información.

Lineamientos:

a. La definición, actualización y mantenimiento del documento de Políticas de Seguridad de la Información de TRANSMILENIO S.A es responsabilidad del Líder u oficial de seguridad de la información, quien debe revisar las políticas de seguridad de la información al menos una vez al año o cuando ocurran cambios significativos, para asegurar su conveniencia, adecuación y eficacia continua, con la debida aprobación del comité de seguridad de la información y/o Comité Integrado de Gestión y deberá seguir los lineamientos definidos en el procedimiento de control de documentos.

b. En las revisiones periódicas se deben tener en cuenta factores como: Prioridades del negocio, costos e impacto de los controles sobre la eficiencia del negocio, incidentes de seguridad, nuevas vulnerabilidades detectadas, Cambios en los requerimientos regulatorios y /o legales. cambios en la infraestructura tecnológica u organizacional, cambios en los objetivos del sistema o de la organización, entre otros.

Excepciones:

Las excepciones establecidas por Ley.

10.4 VIGENCIA DE LAS POLÍTICAS

Las políticas descritas en este documento regirán a partir de la fecha de aprobación y publicación de este documento.

La versión oficial de este documento será la que se encuentre publicada y aprobada en la Intranet de TRANSMILENIO S.A.