Resolución Número 317
(Julio 6 de 2017)

"Por la cual se modifica el Manual de políticas de seguridad de la información (M-DT-001)"

EL JEFE DE LA OFICINA ASESORA DE PLANEACIÓN DE LA EMPRESA DE TRANSPORTE DEL TERCER MILENIO "TRANSMILENIO S.A.", en ejercicio de sus facultades delegadas mediante la Resolución 143 del 2 de marzo de 2016 y

CONSIDERANDO:

Que de conformidad con lo señalado en el artículo segundo del Acuerdo 4 de 1999, corresponde a TRANSMILENIO S.A., la gestión, organización y planeación del servicio de transporte público masivo urbano de pasajeros en el Distrito Capital y su área de influencia, bajo la modalidad de transporte terrestre automotor.

Que cumpliendo con lo ordenado en el parágrafo único del artículo 1º de la Ley 87 de 1993, se adoptó el Manual de Procedimientos de TRANSMILENIO S.A.

Que siendo TRANSMILENIO S.A., el ente gestor del Sistema Integrado de Transporte Público, considera necesario actualizar el Manual de Procedimientos de la Entidad, con el objeto de ajustarlo a los nuevos parámetros documentales, necesidades y desarrollo del Sistema.

Que una vez socializado el protocolo para la cuantificación de la inversión realizada por concepto de overhaul con los concesionarios, se hace necesario ajustar dicho documento acorde con las observaciones presentadas en esta actividad.

Que en mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: Actualizar el siguiente documento con la versión registrada a continuación

Código	Versión	Nombre
M-DT-001	1	Manual de políticas de seguridad de la información

ARTÍCULO SEGUNDO: Derogar en su totalidad la Resolución 4 del 2016, mediante la cual se había adoptado la versión 0 del documento M-DT-001

ARTÍCULO TERCERO: La presente Resolución rige a partir de su publicación en la Gaceta Distrital.

Dada en Bogotá, a los seis (6) días del mes de julio de dos mil diecisiete (2017).

PUBLÍQUESE Y CÚMPLASE.

CARLOS ARTURO FERRO ROJAS
Jefe de Oficina Asesora de Planeación

TRANSMILENIO	**TÍTULO:** **MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**			**ALCALDÍA MAYOR DE BOGOTA**
	Código **M-DT-001**	**Versión** **1**	**Fecha** **Julio de 2017**	

TABLA DE CONTENIDO

MODIFICACIONES

VERSION	FECHA	CAMBIO	SOLICITÓ
0	01-05-2016	Primera versión Oficial del documento	N/A
1	30-03-2017	Las modificaciones realizadas entre otros aspectos son : Se eliminan No. 6.3 Compromisos de la dirección 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 tecnologías de la información y comunicaciones

1 OBJETIVO

Comunicar los lineamientos establecidos por la Dirección de TIC´s y la Alta Dirección de TRANSMILENIO S.A., para la gestión de la seguridad de la Información, los cuales se constituyen como guía para la ejecución de las actividades de la Entidad, de forma que mitiguen los riesgos de pérdida de confidencialidad, disponibilidad e integridad de la información.

2 ALCANCE

Este documento describe las políticas de Seguridad de la Información definidas por TRANSMILENIO S.A. y aplica para todos los funcionarios públicos y oficiales, terceros y contratistas que desarrollen labores de asesoría, consultoría, implementación, soporte o mantenimiento.

Para la elaboración del mismo, se toma como base la normatividad vigente leyes y demás regulaciones aplicables, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

3 DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad (statement of applicability - SOA) referenciado en la cláusula 4.2.1j del estándar ISO 27001 es un documento que lista los objetivos y controles objeto de aplicación en la Entidad.

Para el caso específico de TRANSMILENIO S.A., este tipo de análisis se hará evaluando el cumplimiento de

la norma ISO 27002, para cada uno de los controles establecidos con la gestión de la seguridad de la información, y una vez se complete, se publicará y oficializará la declaración de aplicabilidad.

4 RESPONSABLES

El Profesional Especializado (06) de Seguridad de la Información de la Dirección de TIC´s es el responsable por la elaboración y mantenimiento de este documento y el Director(a) de la Dirección Técnica de TIC´s 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 en cuanto tengan bajo su custodia o responsabilidad información y los medios de procesamiento de información (sistemas de información o aplicativos) de la Entidad.

Las actualizaciones se realizarán de acuerdo a las necesidades de la Entidad o cuando haya un cambio de la legislación y normatividad vigente aplicable.

5 DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia de 1991:

ARTICULO	REFERENCIA
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: “el informe de gestión deberá contener una exposición fiel sobre la evolución de los negocios y la situación económica, administrativa y judicial de la sociedad”.
- 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.
- ISO-IEC-27000: "vocabulario sistema de gestión de la seguridad de la información".
- ISO-IEC-27002: "por el cual se establece el código de buenas prácticas para la gestión de la seguridad de la información".
- ISO-IEC-27003: "por la cual se determina el proceso de planificación e implementación de los procesos del SGSI".
- ISO-IEC-27004: "por el cual se estipula el sistema de medición de la eficacia de los SGSI implementados".
- ISO-IEC- 27005: "por el cual se estandarizan las guías sobre la gestión de riesgos".
- ISO-IEC-27006: "por el cual se informa sobre cómo los organismos de certificación deben interpretar la ISO 17021-1 en el contexto de auditorías a SGSI, en cumplimiento con la norma ISO 27001".
- ISO-IEC- 27007: "por el cual se estandarizan las auditorías según la norma ISO 27001, el alcance y la complejidad, la gestión de riesgos, la selección de controles y la competencia de los auditores de SGSI".
- ISO-IEC-27008: "por el cual se manejan los aspectos técnicos de los controles de seguridad definidos en el anexo A de la ISO27001".
- NTC- 5411-1-2006: tecnología de la información, técnicas de seguridad, gestión de la seguridad de la tecnología de la información y las comunicaciones, "conceptos y modelos para la gestión de la tecnología de la información y las comunicaciones".
- 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".
- NTC GP 1000:2009: norma técnica que describe las generalidades y los requisitos mínimos para establecer, documentar, implementar y mantener un sistema de gestión de la calidad en los organismos, entidades y agentes obligados, conforme al artículo 2 de la Ley 872 de 2003.
- NTC ISO 9001:2008: norma técnica que determina los requisitos para un sistema de gestión de la calidad (SGC), que pueden utilizarse para su aplicación interna por las organizaciones, sin importar si el producto o servicio lo brinda una organización pública o empresa privada, cualquiera que sea su tamaño, para su certificación o con fines contractuales.
- NTD-SIG 001:2011: norma técnica distrital que determina los requisitos del sistema integrado de gestión para las entidades y organismos distritales adoptada mediante el decreto 652 de 2011 por la Alcaldía de Bogotá.

6 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.

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.

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.

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.

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.

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.

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: acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la política de seguridad de la información de TRANSMILENIO S.A. independiente de su origen.

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.

ISO (international organization for standardization): deriva del griego isos, que significa "igual"; esta organización fue creada el 23 de febrero de 1947 en Ginebra, Suiza, con el fin de "facilitar la coordinación internacional y unificación de normas industriales", actualmente hay 165 países miembros.

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.

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 la 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.

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..

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.

7 CONDICIONES GENERALES

Este documento describe la política institucional de seguridad de la información y las políticas generales y específicas definidas por TRANSMILENIO S.A.

Las políticas incluidas en este manual se constituyen en un insumo fundamental del Sistema de Gestión de Seguridad de la Información de TRANSMILENIO S.A. y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La seguridad de la información es una prioridad para TRANSMILENIO S.A. y por lo tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

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 06 de Seguridad de la Información de la Dirección de TIC´s, 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).

7.1 Vigencia y actualización del manual de políticas

El Manual de Políticas de Seguridad, como conjunto de medidas preventivas y reactivas de la Entidad permite establecer lineamientos en aras de resguardar y proteger la información corporativa, buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Por lo tanto, debe ser materia de estudio, de conocimiento y de vigencia permanente para todas aquellas personas que directamente o a través de empresas formalicen contractualmente relación con TRANSMILENIO S.A.

La definición, actualización y mantenimiento del manual de políticas de seguridad de la información de TRANSMILENIO S.A., es responsabilidad de la Dirección Técnica de TIC’s de TRANSMILENIO S.A., con la debida aprobación del comité de seguridad de la información y deberá seguir los lineamientos definidos en el procedimiento de control de documentos. En las revisiones periódicas se deben tener en cuenta factores como: incidentes de seguridad, nuevas vulnerabilidades detectadas, cambios en la infraestructura tecnológica u organizacional, en los objetivos del sistema o de la organización, entre otros.

La versión oficial de este documento para funcionarios, será la que se encuentre publicada y aprobada en la Intranet de TRANSMILENIO S.A. o en su defecto la versión impresa que se encuentre bajo custodia de la Dirección de TIC’s.

El Manual de Políticas de Seguridad debe ser revisado cada vez que se presenten cambios significativos en:

- Efectividad demostrada por la naturaleza, número y el impacto de los incidentes de seguridad registrados.
- Vulnerabilidades y amenazas emergentes.
- Prioridades del negocio, costos e impacto de los controles sobre la eficiencia del negocio.

- Cambio de la infraestructura organizacional y/o técnica
- Cambios en los requerimientos regulatorios y /o legales.
- Transferencia de la responsabilidad o la propiedad tal como adquisiciones y/o escisiones.
- Costos e impacto de los controles sobre la eficiencia de la entidad.
- Requerimientos regulatorios y /o legales.

7.2 Compromiso de la dirección

La Dirección de TIC´s de TRANSMILENIO S.A. aprueba la Política de Seguridad de la Información, como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Entidad.

La Dirección de TIC´s y la Alta Dirección de la Entidad demuestran su compromiso 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.

7.3 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 los funcionarios, personal externo y de TRANSMILENIO S.A. Por tal razón, se hace necesario que las violaciones a las Políticas de Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información.

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.

8 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

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.

8.1 Políticas de seguridad de la información

Las políticas de seguridad de la información, conceptualizan el modelo de manejo de los recursos tecnológicos y físicos de TRANSMILENIO S.A., tanto en el rol de proveedor como de usuario de la información; teniendo en cuenta que la seguridad de la información de una entidad del Estado, sugiere la capacidad del ente para acceder y disponer de sus medios, generando a la vez la oportunidad para gestionar la disponibilidad, confidencialidad e integridad de la información.

De acuerdo a lo anterior, la aplicación de las registradas en el presente manual, se constituyen en la plataforma doctrinal de TRANSMILENIO S.A., para proteger su 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 de la Entidad, se constituyen en un activo de propiedad exclusiva de TRANSMILENIO S.A., por ende a la naturaleza de los bienes públicos, por lo cual podrá ser objeto de verificación, control y monitoreo por parte del profesional especializado 06 de seguridad de la información de la dirección de TIC's.

8.2 Directrices de dirección en seguridad de la información

Frente al presente Manual de Seguridad de la información la Dirección de TIC´S y la Alta Dirección de TRANSMILENIO S.A., son responsables de lo enunciado a continuación y de velar por su estricto cumplimiento:

- Divulgar el presente manual a cada uno de los funcionarios, con el fin de generar y consolidar una cultura de seguridad de la información al interior de la entidad.
- Velar por el cumplimiento de las políticas y lineamientos para el manejo y administración de la información de TRANSMILENIO S.A. registradas en el presente manual.
- Promover e impulsar el uso de la información de TRANSMILENIO S.A., de manera segura.
- Socializar las acciones de control y supervisión frente al adecuado uso de la información de TRANSMILENIO S.A.
- Aplicar el manual de políticas de seguridad de la información en el desarrollo de todas las actividades diarias y propias, en cada una de las dependencias de TRANSMILENIO S.A.
- Evitar la difusión no autorizada de información clasificada como confidencial, perteneciente a TRANSMILENIO S.A.
- Orientar a los funcionarios de TRANSMILENIO S.A., en el cumplimiento de las obligaciones y deberes establecidos para salvaguardar la seguridad de la información y la seguridad informática.
- Fortalecer los niveles de seguridad de TRANSMILENIO S.A. en relación con la administración y uso de la información, de tal forma que se disminuya el riesgo frente a la pérdida, alteración o difusión no autorizada de información.

8.2.1 Políticas para la seguridad de la información.

Propender por la divulgación y cumplimiento de las políticas para la seguridad de la información, aprobadas por la Dirección, publicadas y comunicadas a los empleados y partes interesadas.

8.2.2 Revisión de las políticas para la seguridad de la información

Las políticas de seguridad de la información serán proyectadas y evaluadas por el profesional especializado (06) de Seguridad de la Información de la Dirección de TIC´s y revisadas por el Director de TIC's.

Una vez se conforme oficialmente el comité de seguridad de información de la Entidad, se redefinirán otros protocolos de evaluación.

Los cambios a los lineamientos, políticas o directrices existentes pueden ser efectuados por cualquiera de los siguientes aspectos:

- Efectividad demostrada por la naturaleza, número y el impacto de los incidentes de seguridad registrados.
- Vulnerabilidades y amenazas emergentes.
- Prioridades del negocio, costos e impacto de los controles sobre la eficiencia del negocio.
- Cambio de la infraestructura organizacional y/o técnica
- Cambios en los requerimientos regulatorios y /o legales.
- Transferencia de la responsabilidad o la propiedad tal como adquisiciones y/o escisiones.
- Prioridades de TRANSMILENIO S.A.
- Costos e impacto de los controles sobre la eficiencia de la entidad.
- Requerimientos regulatorios y /o legales.

8.3 Aspectos organizativos de la seguridad de la información

8.3.1 Organización interna

TRANSMILENIO S.A., ha establecido un esquema de seguridad de la información a partir de la creación de usuarios en el directorio activo de la plataforma de servidores de la Entidad, en donde existen roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

8.3.1.1 Asignación de responsabilidades para la seguridad de la información

Normas dirigidas a: la alta dirección

- La Alta Dirección debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.
- La Alta Dirección debe promover activamente una cultura de seguridad de la información en TRANSMILENIO S.A.
- La Alta Dirección de TRANSMILENIO S.A., debe asignar los recursos, la infraestructura física y el

personal necesario para la gestión de la seguridad de la información de la Entidad.

Normas dirigidas al: comité de seguridad de la información

- El comité de seguridad de la información debe actualizar y presentar ante la Subgerencia General de TRANSMILENIO S.A., las políticas de seguridad de la información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- El comité de seguridad de la información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- El comité de seguridad de la información debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.
- La Oficina de Control Interno contribuirá a la generación de lineamientos para gestionar la seguridad de la información de TRANSMILENIO S.A. y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.

Normas dirigidas a: Dirección de Tecnologías de la Información y las Comunicaciones

- La Dirección de Tecnología debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica de la Entidad.
- Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

8.3.1.2 Segregación de tareas

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. Lo siguiente debe ser establecido:

- Es importante segregar las funciones que requieran colusión, por ejemplo revisar una orden de compra y verificar que los bienes han sido recibidos.
- Si hay riesgo de colusión, entonces los controles necesitan ser concebidos de tal modo que dos o más personas necesiten ser partícipes, reduciendo la posibilidad de conspiración.
- Las pistas de auditoría son esenciales como mecanismo de control e investigación.

8.3.1.3 Contacto con autoridades

El profesional especializado 06 de seguridad de la información de la Dirección de TIC´s tiene la responsabilidad de mantener el contacto con las autoridades y verificar el cumplimiento de la ley, que podría impactar la seguridad de la información de TRANSMILENIO S.A., además, estar atento a normas expedidas relacionadas con la seguridad de la información, ya sea por entidades privadas nacionales o internacionales para promover y verificar su cumplimiento o impacto al interior de la Entidad.

8.3.1.4 Contacto con grupos de interés especial

Se debe mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales como por ejemplo:

CONTACTO	DESCRIPCION DEL CONTACTO	ENLACE
Anti phishing working group	El Grupo de Trabajo Anti-Phishing (APWG) es una organización internacional sin ánimo de lucro para la aplicación en entornos industriales y de cumplimiento de la ley con el objeto de eliminar el fraude, el crimen y el robo de identidad como resultado de las actividades de phishing, pharming, malware y suplantación de correo electrónico de cualquier tipo.	AWPG
CWE	De alcance internacional y libre uso público, CWE™ ofrece un conjunto unificado y medible de las debilidades de software que permite una más eficaz discusión, descripción, selección y uso de herramientas de seguridad de software y servicios que se podrían contener estas debilidades en su código fuente y los sistemas operativos. Permite una mejor comprensión y manejo de las debilidades de software relacionados con la arquitectura y el diseño.	CWE
ESET	Consejos de seguridad para el uso seguro del ordenador y de la información sensible y personal.	http://www.eset.es/centro-de-alertas/consejos-seguridad

CONTACTO	DESCRIPCION DEL CONTACTO	ENLACE
Laboratorios independientes de evaluación antivirus	En la selección de un buen AV se debe consultar a los laboratorios que están probando varios antivirus contra las últimas amenazas de malware y comprobar su actualización periódica. Varios enlaces a laboratorios disponibles.	http://www.virusbtn.com/vb100/latest_comparative/index AV-TEST Instituye AV Comparative
McAfee	Alertas de amenazas al Consumidor de McAfee le advertirá sobre las descargas más peligrosas, pop-ups y el spam sospechoso para que pueda mantenerse a la vanguardia de las actividades de delincuentes y mantener su PC y la información personal segura y protegida. Permite suscripción gratuita a las alertas.	http://resources.mcafee.com/content/ConsumerThreatAlerts
Microsoft	Centro de descargas de soluciones.	http://www.microsoft.com/downloads/es-es/default.aspx
Oficina de seguridad del internauta	La "Oficina de Seguridad del Internauta" (OSI) es un servicio del Gobierno para proporcionar la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden afectarnos al navegar por Internet. Su objetivo es elevar la cultura de seguridad, prevenir, concienciar y formar proporcionando información clara y concisa acerca de la tecnología y el estado de la seguridad en Internet. Al mismo tiempo impulsamos la detección y denuncia de nuevas amenazas en la red, de fraudes, estafas online o de cualquier otro tipo de ataque de seguridad informática.	http://www.osi.es
Securelist	Información actualizada y muy completa sobre aquellas amenazas de Internet que están activas, y explica cómo evitarlas. El portal incluye diferentes secciones con artículos informativos y análisis, blogs, una enciclopedia de seguridad informática y descripciones de malware, así como un amplio glosario de términos.	http://www.securelist.com/
Secure database	Panel de información con las vulnerabilidades en productos y que se actualiza constantemente. La sección de herramientas permite consultar posibles soluciones de manera extensa y en materia de seguridad.	http://www.security-database.com/

8.3.1.5 Seguridad de la Información en la Gestión de Proyectos.

Los supervisores de contratos o profesionales encargados de la ejecución de proyectos deben monitorear periódicamente las actividades realizadas por los contratistas a fin de garantizar la protección de la información de acuerdo a las políticas establecidas por la entidad a través del manual de políticas de seguridad de la información.

Los supervisores de contratos o profesionales encargados deben realizar una auditoría periódica sobre la información almacenada y tramitada por los contratistas en el desarrollo de sus labores.

Para la ejecución de los proyectos los contratistas deben informar y registrar cualquier dispositivo de información que se requiera ingresar a las instalaciones de Transmilenio como material de apoyo de su trabajo.

Todo dispositivo ingresado a TRANSMILENIO S.A., debe surtir el proceso de sanitización de medios establecido por el profesional especializado 06 de Seguridad de la Información. Dicho proceso será realizado por personal de soporte de la Dirección de TIC´s de TRANSMILENIO S.A.

Para tal efecto el profesional a cargo del contrato, informará, a través del correo electrónico soportetecnico@transmilenio.gov.co al área de soporte para que se lleve a cabo la gestión.

8.3.2 Dispositivos para movilidad y teletrabajo

8.3.2.1 Política de uso de dispositivos para la movilidad

TRANSMILENIO S.A. establece las siguientes medidas de seguridad para la protección contra los riesgos de usar computación y dispositivos móviles:

- No conectar los dispositivos móviles a redes WIFI abiertos sin contraseña.
- Proteger contraseñas, en lugares públicos se debe tener cuidado para evitar el riesgo de miradas "sobre el hombro" por personas no autorizadas que puedan poner en riesgo la seguridad de la información.
- Los protocolos para la protección contra software malicioso deben aplicarse y mantenerse al día.
- Los equipos deben estar disponibles para permitir el rápido y fácil backup de la información. A estos backups se les debe proporcionar la adecuada protección contra robo o pérdida de información.
- El acceso remoto a la información de TRANSMILENIO S.A., a través de la red pública usando dispositivos móviles de cómputo debe solamente ocurrir después de una identificación y autenticación exitosas, y con mecanismos de control de acceso adecuados.
- Los dispositivos de cómputo móviles deben además estar físicamente protegidos contra robo,

especialmente cuando sean dejados, por ejemplo, en carros u otras formas de transporte, habitaciones de hotel, centros de conferencias y lugares de reuniones. Los equipos que contengan datos confidenciales y restringidos deben ser guardados en forma segura o se deben usar candados especiales para asegurar los equipos.

- Los portátiles de TRANSMILENIO S.A. deben ser cifrados por disco.

8.3.2.2 Teletrabajo

Se deben desarrollar e implementar planes y procedimientos para actividades de teletrabajo.

La protección conveniente de los sitios de teletrabajo debe estar en funcionamiento para minimizar el riesgo por robo de los equipos y la información, la divulgación no autorizada de información, el acceso remoto no autorizado a los sistemas internos o instalaciones de TRANSMILENIO S.A.

La Entidad debe autorizar las actividades de teletrabajo solamente, sí se satisfacen los acuerdos de seguridad y los controles se encuentran en marcha de acuerdo con las políticas de seguridad de TRANSMILENIO S.A. Dicha actividad está reglamentada a través de la resolución 420 de 2016 al interior de la Entidad.

Las siguientes medidas deben ser aplicadas:

- Seguridad Física
- Autorización del jefe o encargado del área que postula al candidato de teletrabajo.
- Protocolo de soporte y mantenimiento de hardware y software.
- Los procedimientos para backup y continuidad del negocio.
- Mecanismos de seguridad en comunicaciones, para el acceso remoto a los sistemas de TRANSMILENIO S.A.
- Revocación de derechos de acceso y la devolución de los equipos cuando cesen las actividades de teletrabajo.
- Capacitación y sensibilización en Seguridad de la Información.
- Firma de Acuerdos de confidencialidad y reserva de la información.
- Protocolos de auditoría y monitoreo de la seguridad.
- Protección antivirus y requerimientos de firewall.
- Conexiones vía VPN a los sistemas de información de TRANSMILENIO S.A.

8.4 Control de acceso

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, la autorización para el acceso a los sistemas de información debe ser definida y aprobada por cada dependencia o propietario de la información, e implementada por la Dirección TIC's y supervisada por el Profesional Especializado (06) de Seguridad de la Información de la Dirección de TIC´s, de acuerdo con la funcionalidad de cada sistema, según el procedimiento de gestión de usuarios y contraseñas.

Objetivo: limitar el acceso a la información y a las instalaciones de procesamiento de información de TRANSMILENIO S.A.

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 o switch, agenda electrónica, Smartphone, access point, amplificadores de señal, que no sean autorizados por la dirección de TIC´s.

8.4.1 <u>Política de control de accesos</u>

Definir las pautas generales para asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática del TRANSMILENIO S.A., así como el uso de medios de computación móvil, teniendo en cuenta lo siguiente:

- La dirección de TIC´s de TRANSMILENIO S.A., suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información para los cuales tengan autorización de uso, bajo la premisa de que las claves son de uso personal e intransferible. Es responsabilidad de cada usuario el tratamiento que se le dé a la clave que le ha sido asignada.
- Solo funcionarios del área de soporte designados por la dirección de TIC´s estarán autorizados para instalar software o hardware en la infraestructura tecnológica de TRANSMILENIO S.A.
- Cualquier actividad que involucre el establecimiento de una conexión remota a la red de área local de TRANSMILENIO S.A., deberá ser implementada a

través de una conexión VPN segura suministrada por la entidad, la cual debe ser previamente aprobada y registrada por la dirección de TIC´s.

- El área de soporte de la Dirección de TIC´s de TRANSMILENIO S.A., revisará periódicamente el estado de actividad de los usuarios, a fin de llevar a cabo las actualizaciones a que haya lugar. En caso de remoción de derechos de acceso se coordinará con el área de recursos humanos de la Dirección Administrativa.

8.4.2 Control de acceso a las redes y servicios asociados

- Permitir únicamente el acceso de los usuarios, que hayan sido previamente autorizados por la Dirección TIC's de TRANSMILENIO S.A. a los recursos de la red LAN corporativa.

- Todo acceso remoto debe ser configurado con la siguiente información: responsable, tiempo de acceso permitido, número de sesiones autorizadas y fecha de expiración.

De igual forma, el área de soporte de la Dirección de TIC's, controlará el vencimiento de las conexiones de acceso remoto trimestralmente.

- Todos los funcionarios de la organización tienen acceso a Internet para desempeñar su labor. Es responsabilidad de la Dirección de TIC's implementar un sistema de control de navegación para filtrar los sitios Web previniendo acceso a categorías definidas de alto riesgo, o que redunden en la degradación del ancho de banda utilizado.

- Para acceso a correo electrónico externo o páginas web restringidas, se debe realizar una solicitud justificada a través de correo electrónico a la Dirección de TIC´s, y al Profesional Especializado (06) de Seguridad de la información, quien evaluará el requerimiento y determinará la viabilidad de la misma en un tiempo no mayor a 8 horas.

8.4.3 Gestión de acceso de usuario

De acuerdo a los perfiles, se debe asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios de TRANSMILENIO S.A., gestión de altas/bajas en el registro de usuarios.

El proceso formal del registro y cancelación del registro es fundamental para posibilitar la asignación de los derechos de acceso que incluya:

Altas:

- Usar ID de usuario únicos de tal manera que puedan ser identificados y responsabilizados por sus acciones.

- El uso de ID´s de grupo solamente se permitirán donde sea necesario por razones operacionales o de negocio, y deben ser aprobados y documentados.

- Verificar que el nivel de acceso concedido es adecuado al propósito del negocio y es consistente con la política de seguridad organizacional, por ejemplo no comprometer la segregación de funciones.

- Proporcionar a los usuarios un documento escrito, que contenga una lista y descripción de sus derechos de acceso, así como de sus obligaciones.

Bajas:

- Inactivar o bloquear los derechos de acceso de los usuarios que han cambiado de área o ya no laboran en TRANSMILENIO S.A.

- Suspender los derechos de acceso de los usuarios que se encuentran en vacaciones o en periodos de licencia.

8.4.3.1 Gestión de los derechos de acceso asignados a usuarios

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

- Los derechos y privilegios necesarios para el desarrollo de sus funciones se asignarán a los usuarios únicamente.

- El nivel de acceso a la información debe ser autorizado por el jefe del área responsable de la información, para un funcionario o grupo de funcionarios, acorde a las funciones a desempeñar, mediante documento escrito o correo electrónico enviado a la Dirección de TIC´s de TRANSMILENIO S.A.

- En caso de personal ajeno a TRANSMILENIO S.A., el área responsable de la información debe autorizar el acceso a la misma atendiendo la clasificación de la información, así como las normas y procedimientos definidos para tal fin.

8.4.3.2 Gestión de los derechos de acceso con privilegios especiales

- Las transacciones realizadas y los accesos a los aplicativos o programas, a la red o a los sistemas de TRANSMILENIO S.A., son registrados de manera que se pueden llevar a cabo auditorías.
- Las transacciones realizadas y los accesos a los aplicativos o programas, a la red o a los sistemas de TRANSMILENIO S.A., son registrados de manera que se pueden llevar a cabo auditorías.
- Los privilegios deben 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 de TIC's.
- Se debe implementar un procedimiento que garantice conceder privilegios adecuados y efectivos a los usuarios.

8.4.3.3 Revisión de los derechos de acceso de los usuarios

Para mantener un control efectivo sobre el acceso a datos y servicios de información, el área de soporte de la dirección de TIC´s, revisará los derechos de acceso de los usuarios periódicamente (trimestralmente), valiéndose además de la información suministrada por el área de recursos humanos de la dirección administrativa de TRANSMILENIO S.A.

La revisión debe tener en cuenta:

- Los usuarios que han dejado TRANSMILENIO S.A. ya no tengan cuentas activas.
- Los usuarios con cuentas privilegiadas solo tengan acceso a lo que necesiten con el fin de realizar sus responsabilidades de trabajo.
- Los privilegios asociados con cada aplicación, sistema o servicio deben ser identificados por los propietarios o usuarios encargados responsables de la información o recursos.
- Los cambios a cuentas privilegiadas deben ser registrados para revisión periódica (trimestralmente).
- La Dirección TIC's y el personal de Soporte, implementará los perfiles de los usuarios por solicitud del área o profesional a cargo, de acuerdo con lo establecido por el propietario o usuarios encargados responsables del activo de información.

8.4.3.4 Cancelación o ajuste de los derechos de acceso

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.

8.4.4 <u>Responsabilidades del usuario</u>

Objetivo: hacer que los usuarios rindan cuentas por la custodia de información de autenticación a los sistemas de información y servicios de TRANSMILENIO S.A.

Los usuarios son responsables de cualquier actividad realizada con las credenciales otorgadas para su acceso a los sistemas de información de TRANSMILENIO S.A.

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

8.4.4.1 Uso de información confidencial para la autenticación

Todos los usuarios deben tener un único identificador (ID de usuario), correspondiente al user creado en la estructura de directorio activo en los servidores de la entidad.

- El procedimiento de creación de usuarios debe ser aplicado a todo tipo de usuarios incluyendo contratistas, funcionarios de planta, pasantes., etc.
- Los usuarios de TRANSMILENIO S.A., deben cumplir con las buenas prácticas que la Entidad ha dispuesto para el uso de información y de procedimiento de autenticación a través de la contraseña de usuario, implementadas por la Dirección TIC's y el personal de soporte.
- El acceso a los recursos de la red será controlado por medio de la creación de usuarios y password correspondiente, 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.
- Todos los accesos remotos deben ser autorizados por el propietario de la información y la Dirección TIC's.
- Todo acceso remoto a la red de TRANSMILENIO S.A., debe contar con mecanismos de autenticación, autorización, registros de auditoría y de

cifrado, para reducir el riesgo de divulgación de información sensible y accesos no autorizados.

- El acceso a la red interna por parte de los funcionarios autorizados se debe realizar a través de una conexión segura con un certificado de seguridad SSL (secure sockets layer).

- 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 TIC´s de TRANSMILENIO S.A.

- Todos los accesos de los usuario deben contar con un ID identificable que permita dejar pistas de las actividades y fijar responsabilidades individuales.

8.4.5 Control de acceso a sistemas y aplicaciones

Objetivo: la Dirección TIC's debe prevenir el uso no autorizado de sistemas y aplicaciones.

8.4.5.1 Procedimientos seguros de inicio de sesión

Mediante un procedimiento de conexión segura se debe controlar el acceso a sistemas y aplicaciones.

- Los responsables de la administración de la red deben realizar una evaluación periódica de los riesgos de seguridad existentes, y definir los controles para minimizarlos. El intercambio de información hacia o desde redes externas debe ser controlado por sistemas de control de acceso, tales como Firewall.

- Al cuarto intento fallido de ingreso al dominio y/o aplicaciones asignadas, el usuario será bloqueado.

- Si el bloqueo de usuario es repetitivo, es responsabilidad del área de soporte de la Dirección de TIC's, analizar el motivo del bloqueo para tomar las medidas pertinentes.

- 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.

- Los computadores deben apagarse después de un periodo definido de inactividad para prevenir el acceso por personas no autorizadas y debe ser una condición obligatoria al terminar la jornada laboral.

- 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.

- Controlar el tiempo de conexión, se debe implementar para aplicaciones sensibles especialmente en localizaciones de alto riesgo, ejemplo áreas externas o públicas que están fuera de la administración de seguridad de TRANSMILENIO S.A., ejemplos de tales restricciones incluyen:

    - El uso de ventanas de tiempo predeterminadas por ejemplo trasmisiones de lotes de archivos o sesiones interactivas regulares de corta duración.

    - Restricción de los tiempos de conexión para las horas de oficina normales, si no hay requerimiento de horas extras u operaciones de horario extendido.

8.4.5.2 Gestión de contraseñas de usuario

Las contraseñas brindan el medio de validar la autenticidad del usuario y así establecer derechos de acceso a los servicios y facilidades de procesamiento de información. Los funcionarios de TRANSMILENIO S.A. son responsables de asegurar que las credenciales de autenticación permanecen bajo su control. Credenciales de grupo o compartidas no son permitidas. Las cuentas deben ser únicas para cada funcionario de TRANSMILENIO S.A, excepto donde sea imposible (cuentas "root" o "administrador"), de igual forma las credenciales para estos usuarios deben ser cambiadas y guardadas bajo protocolo de administración de usuarios privilegiados.

Sí se requiere el uso de estos perfiles se debe crear un nuevo usuario y asignarle estos permisos, de la misma manera, las contraseñas deben ser tratadas como información confidencial de TRANSMILENIO S.A. y no deben ser transmitidas en texto claro en el inicio de sesión de una aplicación o sistema.

Todos los usuarios deben:

- Mantener la confidencialidad de las contraseñas. Son personales e intransferibles por lo tanto, no se pueden compartir.

- Evitar mantener un registro (por ejemplo papel, archivo de programa, dispositivo de mano) de contraseñas, a menos que puedan ser almacenadas en forma segura y el método de almacenamiento haya sido aprobado.

- La política de creación de usuario y contraseña, de acuerdo al manual de políticas de seguridad de la información de TRANSMILENIO S.A., establecidas por la Dirección TIC's , está diseñada de forma segura donde:
    - La creación del usuario seguirá el modelo: nombre.apellido@transmilenio.gov.co
    - La creación de la contraseña debe ser de (08) caracteres, alfanumérica, debe contener una letra mayúscula y un número, ejemplo [Ejemplo5]
    - No estén compuestas por caracteres idénticos consecutivos o caracteres seguidos (12345, abcdefg).
    - No estén basadas en información de la persona o personas cercanas: nombres, números de teléfono, fechas de nacimiento, nombres de mascotas, etc.
    - No sean palabras que aparezcan en diccionarios así sean de otro idioma.
    - No debe contener el nombre de usuario.
- Los usuarios deberán seguir las siguientes políticas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados.
- Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
- Las contraseñas no deberán ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.
- Las contraseñas no se deberán escribir en ningún medio, excepto cuando son entregadas en custodia.
- Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.
- Las contraseñas se deberán cambiar según los requerimientos de la infraestructura de procesamiento de información.
- Los usuarios deberán cambiar las contraseñas la primera vez que usen las cuentas asignadas
- Cambiar las contraseñas a intervalos regulares o basados en el número de accesos.
- Cambiar las contraseñas temporales al primer acceso.
- Evitar el uso de contraseñas anteriormente usadas.
- Las aplicaciones y sistemas de información deben utilizar un sistema de control de acceso basado en contraseñas interactivas y de calidad.
- La Dirección TIC's y el personal soporte, deben verificar el cumplimiento de la política asociada a la periodicidad con la cual las contraseñas deben ser cambiadas y las cuentas deshabilitadas de TRANSMILENIO S.A., este requerimiento aplica a sistemas, bases de datos o aplicaciones
- Las aplicaciones y sistemas de información deben utilizar un sistema de control de acceso basado en contraseñas interactivas y de calidad.
- Requerir a los usuarios mantener la confidencialidad de las contraseñas personales.
- Las contraseñas temporales proporcionadas cuando los usuarios olviden su contraseña deben ser suministradas solamente cuando se haya hecho una validación positiva de la identidad del 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 temporales deben ser únicas para un individuo y no deben ser previsibles.
- Las contraseñas nunca deben ser almacenadas sin protección en los sistemas de computador.
- Las contraseñas por omisión que vienen en los sistemas y software deben ser modificadas enseguida de su instalación.
- Todas las contraseñas de los súper-usuarios (altos privilegios) deben ser protegidas y almacenadas de una manera coherente con los planes de continuidad del negocio y/o el de recuperación.
- Asegurar que las contraseñas son revisadas periódicamente (trimestralmente), para verificar el cumplimiento de los lineamientos establecidos para creación de contraseñas y llevar a cabo los ajustes correspondientes de ser necesarios.
- La asignación de autenticación secreta o confidencial se debe controlar por medio de un procedimiento de gestión formal, implementada por la Dirección de TIC's de TRANSMILENIO S.A., que es parametrizada a través del directorio activo de la plataforma de servidores.
- Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que

no le pertenece al correo soportetecnico@transmilenio.gov.co.

- No visualizar contraseñas legibles en la pantalla del computador cuando éstas se estén digitando.

8.4.5.3 Caducidad de la Contraseña

Las contraseñas reutilizables para cualquier aplicación deben caducar por lo menos cada 90 días. Los sistemas y aplicaciones se deben programar para que automáticamente controlen la frecuencia de cambio según sea necesario. En los sistemas donde no sea posible la programación automática el usuario tiene la responsabilidad de cambiar la contraseña con la frecuencia que se le indique como estándar para el sistema.

8.4.5.4 Uso de herramientas de administración de sistemas

- La Dirección TIC's de TRANSMILENIO S.A., controlará el uso de programas utilitarios que podrían tener la capacidad de anular el sistema y los controles de las aplicaciones.
- Los usuarios finales no deben tener acceso a la ejecución de comandos del sistema operativo; en caso que sea necesario, se debe restringir el acceso por medio de herramientas que sólo permitan las funciones que han sido autorizados a ejecutar.
- La Dirección TIC's de TRANSMILENIO S.A. y el área responsable del cada sistema de información deben determinar las actividades mínimas realizadas por cada usuario sobre cada una de las aplicaciones en las cuales está autorizado a trabajar. Esto con el fin de que se parametricen los accesos respectivos, a fin de detectar fallas o prevenir violaciones a la política de seguridad.

8.4.5.5 Control de acceso al código fuente de los programas

La Dirección TIC's a través de su área de soporte, controla el acceso a códigos fuente de programas, por medio de la configuración de perfiles.

8.5 <u>Seguridad en las telecomunicaciones</u>

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

8.5.1 <u>Gestión de la Seguridad en las Redes</u>

Objetivo: asegurar la operación correcta y segura de los puntos de red instalados y operativos al interior de la Entidad.

- Se deben controlar los accesos a servicios internos y externos conectados en red.
- El acceso de los usuarios a redes y servicios en red no debe comprometer la seguridad de los servicios en red si se garantizan:
- Que existen interfaces adecuadas entre la red de la Entidad y las redes públicas o privadas de otras entidades;
- El cumplimiento del control de los accesos de los usuarios a través de la aplicación del registro (logging) y el seguimiento adecuado que posibiliten el registro y detección de acciones que puedan afectar la seguridad de los servicios de información.
- La Dirección de TIC's 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).

8.5.1.1 Controles de red

Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

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

Se deben establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan sobre redes públicas, y para proteger los sistemas conectados. Controles especiales pueden ser además requeridos para mantener la disponibilidad de los servicios de red y los computadores conectados.

Las actividades de administración deben ser estrechamente coordinadas para optimizar el servicio a la entidad y para asegurar que los controles están aplicados consistentemente a través de la infraestructura de procesamiento de información.

Normas dirigidas a: Dirección de Tecnologías de la Información y Comunicaciones

- La Dirección de TIC's 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.

- La Dirección TIC's de TRANSMILENIO S.A., en conjunto con el área de Soporte, deberá validar con los supervisores de contrato o áreas encargadas la identificación de los usuarios provistos por terceras partes, que requieran autenticarse en las redes o recursos de red de la entidad, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las políticas de seguridad de la información por parte de estos.

Normas dirigidas a: todos los usuarios

- 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 TIC´s por medio escrito o electrónico. y el Acuerdo de Confidencialidad firmado previamente.

- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la Entidad deben cumplir con todos los requisitos o controles para autenticarse en ellas referidos a la asignación de usuario válido o autorizado y únicamente podrán realizar las tareas para las que fueron autorizados.

8.5.1.2 Mecanismos de seguridad asociados a servicios en red

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.

8.5.1.3 Segregación de redes o separación de redes

- Se deben segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.

- 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, así mismo, TRANSMILENIO S.A. controlará el paso de software y aplicaciones de un ambiente a otro.

- TRANSMILENIO S.A., se asegura mediante controles de acceso adecuados, que los usuarios utilicen perfiles con diferentes modalidades de autorización en caso de necesitar hacer uso de los ambientes de desarrollo y/o de producción.

- No deben realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno.

- Sistemas de Información o aplicaciones que se encuentran en estado de pruebas no podrán pasar al ambiente de producción sin antes haber sido aprobado el cambio o cambios por el funcionario o área responsable.

- Queda prohibida la copia de información sensible desde el ambiente de producción al ambiente de pruebas; en caso contrario, en el cual las pruebas requieran de esta información, la copia debe ser solicitada por el funcionario designado y autorizada por el propietario o administrador de la aplicación y por la Dirección de TIC's de TRANSMILENIO S.A.

- Periódicamente, la Dirección de TIC's de TRANSMILENIO S.A., podrá verificar las versiones instaladas tanto en ambiente de pruebas como en producción y confrontará esta información con las revisiones pasadas y con las versiones de programas fuentes almacenadas en los repositorios de TRANSMILENIO S.A.

8.5.2 <u>Intercambio/trasferencia de información con partes externas</u>

Objetivo: mantener la seguridad de la información trasferida al interior de la Entidad y de aquella transferida o intercambiada con cual cualquier entidad externa.

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 Intercambio seguro de Información.

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.

Para establecer dicha transmisión se debe consultar el concepto técnico de la Dirección de TIC's de TRANSMILENIO S.A., área que además coordinará la verificación de los requerimientos para el proceso de transmisión. También se debe privilegiar este mecanismo o similares técnicamente, cuando el intercambio de información se produzca con otros organismos

nacionales con los que exista intercambio regular de información. La información a intercambiar debe estar previamente definida y formalizada a través de una petición institucional.

Para acceso a sitios web se debe implementar herramientas de seguridad perimetral seguros (firewalls) y para acceso a portales institucionales, se debe realizar asegurándose que sean implementados desarrollos seguros.

8.5.2.1 Mensajería electrónica

Definir las pautas generales para asegurar una adecuada protección de la información de TRANSMILENIO S.A, en lo referente al uso del servicio de correo electrónico por parte de los usuarios autorizados.

Correo electrónico

TRANSMILENIO S.A asigna 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 el presente manual:

- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de TRANSMILENIO S.A.
- 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.

No se permite:

- 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.
- 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.
- El envío de archivos que contengan extensiones como .mp3, wav, .exe, .com, .dll, .bat. o cualquier otro archivo ejecutable; en caso que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por la Dirección de TIC's de TRANSMILENIO S.A.
- Se prohíbe el uso de correo en cadena 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.
- No se debe alterar la línea "De" (autor del correo) u otra información relacionada con los atributos de origen del correo electrónico.
- No se permite el envío de mensajes anónimos y la gestión con este tipo de mensajes está prohibida.
- El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la Dirección de TIC's de TRANSMILENIO S.A. y deberá incluir un mensaje que le indique al destinatario cómo ser eliminado de la lista de distribución.
- 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.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido

por la Dirección de TIC's de TRANSMILENIO S.A. y deben conservar en todos los casos el mensaje legal institucional de confidencialidad.

- Todo correo electrónico que deba ser transmitido hacia Internet, 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.
- La información enviada por correo electrónico, clasificada como confidencial, debe ser protegida con contraseña de acceso o cifrado según corresponda.
- Se prohíbe el envío de mensajes no solicitados para el desarrollo de la misión de la Entidad, incluyendo él envió de "correo basura", mensajes cadena u otro material de publicidad a personas que específicamente no lo hayan solicitado (por ejemplo, "inundación con mensajes de e-mail" o "spam") y que se materialicen en la queja reiterada del receptor, harán presumir los mensajes como "no solicitados", así como su requerimiento expreso de no continuar recibiendo dicho material.
- Se incluye, sin limitación, el envío de masivos de publicidad comercial, anuncios informativos y comunicaciones políticas. También se incluye la publicación de un mismo mensaje o similar en uno o más grupos de noticias (exceso de publicación cruzada o múltiple publicación).
- 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. .
- 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.
- 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 mensaje violan la presente política o la de otro proveedor.
- 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.
- 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.

Internet

Internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias de TRANSMILENIO S.A., por lo cual el uso adecuado de este recurso se controla, verifica y monitorea, considerando para todos los casos las siguientes políticas:

- No se permite:
- Navegación o publicación en sitio de contenido pornográfico, basado en sentimientos de odio o segregación, de delincuencia computacional (hackers o crackers) o cualquier otro sitio que la Dirección de TIC's considere fuera de los límites permitidos.
- Dirección de publicación o envío de información confidencial hacia fuera de la Entidad sin la autorización de los dueños respectivos. (repositorios externos, redes sociales, páginas web, etc.)
- Utilización de otros servicios disponibles a través de Internet, como por ejemplo FTP y Telnet.
- Publicación de anuncios comerciales o material publicitario.

- Promover o mantener asuntos o negocios personales en horario laboral y haciendo uso de los equipos suministrados por TRANSMILENIO S.A. que pongan en riesgo el descargue de Malware en los equipos de la entidad.

- Recepción de noticias o actualización de datos, a menos que el material sea requerido para actividades de TRANSMILENIO S.A.

- Utilización de programas de aplicación o software no relacionados con la actividad laboral y que ocupen excesivamente el tiempo de procesamiento de la estación de trabajo o de la red, por ejemplo aplicaciones que se ejecutan mientras está activo el protector de pantalla.

- La Dirección de TIC's realiza monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, puede inspeccionar, registrar e informar de las actividades realizadas durante la navegación en caso de percibir degradaciones del ancho de banda que maneja la entidad.

- Cada uno de los usuarios es responsable de dar un uso adecuado de este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, entre otros.

- Los funcionarios y contratistas no pueden asumir en nombre de TRANSMILENIO S.A., posiciones personales en encuestas de opinión, foros u otros medios similares.

- El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de TRANSMILENIO S.A.

Recursos tecnológicos

TRANSMILENIO S.A., asigna diferentes recursos tecnológicos como herramientas de trabajo para uso exclusivo de sus funcionarios y terceros autorizados. El uso adecuado de estos recursos se reglamenta bajo las siguientes políticas:

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

- 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 organización. Estos cambios pueden ser realizados únicamente por la Dirección de TIC´s en coordinación con la Subgerencia de Comunicaciones y atención al Usuario.

- La Dirección de TIC's, 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.

- Únicamente los usuarios autorizados por la Dirección de TIC's y previa solicitud por parte del jefe inmediato, pueden conectarse a la red inalámbrica de TRANSMILENIO SA.

- La Dirección de TIC's será la única dependencia encargada de la adquisición de software y hardware. El resto de dependencias podrán a través de dicha oficina realizar las debidas adquisiciones.

- Los funcionarios no deben realizar cambios en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física y además, sólo podrán ser realizados por la Dirección de TIC's en coordinación con personal autorizado por la Dirección Administrativa de TRANSMILENIO S.A.

- El acceso a unidades CD, DVD y dispositivos USB debe ser restringido, solamente podrá ser utilizado por personal autorizado por la Dirección de TIC's y funcionarios del área de soporte.

8.5.2.2 Acuerdos de confidencialidad y secreto

- 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 funcionarios, 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.

- Todo funcionario de TRANSMILENIO S.A. es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.
- Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad requeridos.
- Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la 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.
- Sí es aplicable para cada uno de los contratos, el acuerdo de confidencialidad deberá incluir aspectos como:
    - Duración del acuerdo.
    - Definición de la información que deberá ser protegida.
    - Definición de responsabilidades de cada una de las partes para evitar que se presente divulgación de la información.
    - Asignación de permiso para que el tercero o contratista haga uso de la información que para TRANSMILENIO S.A., es sensible o crítica.
    - Definición del propietario de la información que el tercero o contratista va a manipular.
    - Inclusión de aspectos como secretos de mercado.
    - Inclusión de aspectos como propiedad intelectual, derechos de autor relacionados con desarrollos de software, licencias, manuales, etc.
    - Definición de las responsabilidades de cada una de las partes, mientras la información se encuentra fuera de las instalaciones de TRANSMILENIO S.A. o del tercero.
    - Inclusión del derecho a auditar y monitorear actividades que involucren información sensible o crítica, en aquellos casos que aplique y sea esencial.
    - Definición de acciones a tomar sí el acuerdo se incumple.
    - Definición de términos de tiempo en que la información manejada por el tercero debe ser devuelta cuando el contrato se finalice.

Así mismo y en el caso que se requiera, el tercero o contratista, deberá tener acuerdos de confidencialidad con los empleados que estén directamente relacionados con el manejo de la información de TRANSMILENIO S.A.

8.6 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

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.

8.6.1 Antes de la contratación

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

Normas dirigidas a: grupo de talento humano

- 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.
- El grupo de talento humano debe certificar que los funcionarios de la entidad firmen un acuerdo y/o

cláusula de confidencialidad y un documento de aceptación de políticas de seguridad de la información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

Normas dirigidas a: personal provisto por terceras partes

- 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 un documento de aceptación de políticas de seguridad de la información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.
- El personal provisto por terceras partes, debe garantizar el cumplimiento de los acuerdos y/o cláusulas de confidencialidad y aceptación de las políticas de seguridad de la información de la Entidad.

8.6.1.1 Términos y condiciones del empleo

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.

8.6.1.2 Sensibilización, educación y capacitación en seguridad de la información

La Dirección de TIC´s debe diseñar y ejecutar de manera periódica (mínimo una vez al año) un programa de 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.

8.6.1.3 Proceso disciplinario

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.

Normas dirigidas a: **grupo de talento humano**

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

8.7 Gestión de activos

Objetivo: lograr y mantener la protección adecuada de los activos de información mediante la asignación de estos a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Los responsables de procesos y dependencias de TRANSMILENIO S.A. deben observar que:

- La instalación de software en los computadores suministrados por TRANSMILENIO S.A., es una función exclusiva del área de soporte de la Dirección de TIC´s. Se mantendrá una lista actualizada del software autorizado para instalar en los computadores.
- Los usuarios no deben mantener almacenados en los discos duros, de las estaciones cliente o discos virtuales de red, archivos de vídeo, música y fotos que no sean de carácter institucional.
- En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a éstos archivos.
- Los usuarios podrán trabajar sus documentos institucionales en borrador en la estación cliente asignada por el DAPRE y deberán ubicar copias y documentos finales en las carpetas virtuales centralizadas que se establezcan para tal fin por la Dirección de TIC´s.
- El préstamo de equipos de cómputo, computadores portátiles y vídeo proyectores se debe tramitar a través de la mesa de ayuda con anticipación y se proveerá de acuerdo a la disponibilidad.
- Los equipos que ingresan temporalmente a TRANSMILENIO S.A., que son de propiedad de terceros: deben ser registrados en las porterías de la entidad para poder realizar su retiro sin autorización. Dicha labor es realizada por personal de vigilancia a cargo de la Dirección administrativa de TRANSMILENIO S.A.
- La Entidad no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.
- El área de soporte de la Dirección de TIC´s no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de TRANSMILENIO S.A.

8.7.1 Inventario de activos

TRANSMILENIO S.A., debe 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.

Adicionalmente, se debe mantener actualizado el inventario de los activos de información de infraestructura tecnológica tal como aires acondicionados, generadores de energía, unidades de potencia (UPS) y circuitos. Cada uno de los activos debe estar clasificado como:

- Misión crítica.
- No-Crítica

Para identificar, clasificar el nivel de protección y respuesta ante incidentes, TRANSMILENIO S.A. debe clasificar los sistemas de computación así:

- Servidores de producción – sistemas que proveen funciones de negocio en operación.
- Servidores de desarrollo – sistemas de información usados para la creación de software
- Servidores de pruebas – sistemas de información usados para ambientes de pruebas.
- Computadores de usuario final – PCs, portátiles, y estaciones de trabajo utilizadas como cliente para acceder a los servidores de desarrollo y producción.

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

Las auditorías al hardware deben verificar la ubicación y el etiquetamiento, las auditorías periódicas al inventario de software se deben efectuar para dar cumplimiento a la ley sobre software licenciado.

8.7.2 Propiedad de los activos de información

- Todos los activos de información deben ser justificados y tener asignado un propietario.
- 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.
- El propietario de los activos debe implementar los controles necesarios para asegurar la protección de los activos que se encuentran bajo su responsabilidad.
- Se debe elaborar y mantener el inventario de activos identificando los propietarios y custodios de los activos, directivos o gestores responsables de proteger los activos, ubicación, número de serie, número de versión, estado de desarrollo / pruebas / producción.

8.7.3 Devolución de activos

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.

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.

8.7.4 Clasificación de la información

Objetivo: asegurar que la información recibe protección en función del nivel de sensibilidad o criticidad para TRANSMILENIO S.A.

TRANSMILENIO S.A. debe llevar a cabo un proceso para clasificar y proteger los datos de acuerdo con estándares de clasificación.

8.7.4.1 Directrices de clasificación

La información se debe clasificar de acuerdo con las siguientes 4 categorías:

- **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.
- **Información pública clasificada:** es aquella información que es sensible o confidencial dentro de la entidad y destinada a uso de TRANSMILENIO. Solo la pueden acceder algunos funcionarios de acuerdo con sus funciones y responsabilidades.
- **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.
- **Publicar o divulgar:** 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.

8.7.5 Manejo de los soportes de almacenamiento

Objetivo: prevenir revelación, modificación, remoción o destrucción no autorizada de activos, e interrupciones a las actividades de la entidad. Los medios deben ser controlados y físicamente protegidos.

8.7.5.1 Gestión de soportes extraíbles

- Debe haber procedimientos para la administración de medios removibles tales como cintas, discos, casetes, unidades USB y reportes impresos entre otros.

Los siguientes controles deben ser implementados:

- 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
- Todos los medios deben ser almacenados en un ambiente seguro de acuerdo con las especificaciones de los fabricantes.
- Todos los datos almacenados en medios removibles deben ser evaluados contra los estándares de clasificación de datos y protegidos de la manera indicada en el presente Manual.

8.7.5.2 Eliminación de soportes.

- La información confidencial debe destruirse por medio de destructoras de papel que garanticen que no se reconstruirá.
- Los medios deben ser eliminados de una manera segura cuando ya no sean requeridos. La información sensible podría ser filtrada a personas externas a través del descuido en la eliminación de medios.
- Muchas organizaciones ofrecen servicios de recolección y eliminación para papeles, equipos y medios. Cuando se evalúe un proveedor para este propósito, evalúelo contra los requerimientos de eliminación segura y reutilización de equipos.
- 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.
- Para la destrucción de Disco contenedores de información se debe realizar un borrado a bajo nivel 7 garantizando la eliminación total de esta. Se debe dejar registro de esto.
- Para la destrucción de información confidencial se debe considerar por lo menos los siguientes protocolos:
- Borrado por software o Hardware a bajo nivel (nivel 7)
- Eliminación magnética o destrucción del disco.
- Destrucción física del disco.
- Cuando se dé acumulación de medios para eliminación, debe darse la consideración del efecto agregación, que puede causar que una gran cantidad de información no clasificada pueda llegar a ser más sensible que una pequeña cantidad de información clasificada.

8.7.5.3 Soportes físicos en tránsito

La información puede ser vulnerable a acceso no autorizado, uso indebido y pérdida o corrupción durante el transporte físico, cuando se envían medios a través del servicio postal o empresas de mensajería.

Los siguientes controles deben ser aplicados cuando sea posible para salvaguardar los medios de computador que son trasportados entre sitios:

- Se deben usar empresas de transporte confiables.
- El embalaje debe ser lo suficientemente robusto para proteger los contenidos de cualquier daño físico.
- Se deben utilizar métodos de cifrado de los datos confidenciales o restringidos para prevenir perdidas de datos si los medios son robados o extraviados.
- Controles especiales deben ser adoptados, donde sea necesario, para proteger la información sensible de modificación o divulgación no autorizada, los ejemplos incluyen:
    - o Uso de contenedores con llave.
    - o Entrega a la mano.
    - o Evidencia de manipulación del empaque (que revele cualquier intento de acceso).

En casos excepcionales, división del envío en más de una entrega y envío por diferentes rutas.

8.8 Cifrado o criptografía

Objetivo: asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.

8.8.1 Política sobre el uso de controles criptográficos

Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.

TRANSMILENIO S.A. velará porque la información de la entidad, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

8.9 Seguridad física y ambiental

8.9.1 Áreas seguras

Objetivo: prevenir el acceso no autorizado, daño e interferencia a la información.

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.

8.9.1.1 Perímetro de seguridad física

TRANSMILENIO S.A., proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes.

Así mismo, controlará y mitigará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.

Las siguientes pautas y medidas de control se deben implementar donde sea necesario:

- 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.

8.9.1.2 Controles físicos de entrada

Las áreas seguras de TRANSMILENIO S.A., deben estar protegidas por controles de entrada para prevenir que únicamente el personal autorizado tiene permitido el acceso. Los siguientes controles se consideran medidas de protección adecuadas:

- Los visitantes a las áreas seguras deben ser supervisados o aprobados, y se debe registrar la fecha y hora de entrada y salida, y la razón de ingreso.
- Los visitantes a las áreas seguras deben portar en forma visible la identificación.
- El acceso a información sensible y a las instalaciones de procesamiento de información requieren medios secundarios de control de acceso y estar restringido únicamente al personal autorizado. Se deben usar controles de autenticación para validar y autorizar todo acceso.
- Deben mantenerse pistas de auditoría de todos los accesos a las áreas restringidas.
- No se debe ingresar dispositivos de almacenamiento a las áreas de procesamiento de información, si existe la necesidad de ingresar dispositivos de almacenamiento es necesario realizar un proceso de sanitización a los dispositivos de almacenamiento.
- El personal debe portar su carné de identificación todo el tiempo y estar dispuesto a retar o confrontar a los extraños sin acompañante y cualquiera que no porte la identificación de forma visible.
- Los derechos de acceso a las áreas seguras deben ser regularmente revisados y actualizados por parte de la Dirección Administrativa de TRANSMILENIO S.A.
- Se deben registrar todas los ingresos y salidas de equipos de cómputo a la Entidad.

8.9.1.3 Seguridad de oficinas, despachos y recursos

La selección y el diseño de las áreas seguras debe contemplar la posibilidad de daño por fuego, inundación, explosión, accidentes, ataques y otras formas de desastre natural o provocados por el hombre. Las directrices a este respecto estarán a cargo de la Dirección Administrativa y el Área de Seguridad Física de TRANSMILENIO S.A.

Los siguientes controles son consideraciones esenciales:

- Las instalaciones clave deben estar ubicadas donde se pueda evitar el acceso público.
- Las construcciones deben ser discretas y dar una indicación mínima de su propósito.

- Puertas y ventanas tendrán que estar cerradas cuando no estén vigiladas y efectuar la protección externa para ventanas, particularmente a nivel del suelo.
- Las instalaciones de procesamiento de la información administradas por TRANSMILENIO S.A., deben estar físicamente separadas de otras administradas por terceros.
- Los directorios telefónicos internos que identifican lugares o instalaciones de procesamiento de información sensible, no deben ser fácilmente accesibles por el público.
- 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.
- Debe ubicarse un área de recepción para el control del acceso físico al centro de proceso de datos. El acceso debe restringirse únicamente al personal autorizado.
- Los visitantes a las áreas seguras deben estar siempre acompañados, registrarse fecha y hora de entrada y salida. Ellos solo deben acceder a lugares específicos con propósitos autorizados. Se debe establecer un registro de control de visitantes. Los empleados responsables de los visitantes acompañados, deben mantener el control sobre ellos en todo momento.
- 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.
- Las salidas de emergencia deben tener alarma.

8.9.1.4 Protección contra las amenazas externas y ambientales

- La Dirección de TIC's debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados 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.
- La Dirección de TIC's 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.
- La Dirección de TIC's 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.
- La Dirección de TIC's 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.

8.9.1.5 Áreas de acceso público, carga y descarga

Las áreas de carga y de entrega deben ser controladas y, si es posible, aislarse de las instalaciones de procesamiento de datos para evitar el acceso no autorizado.

Deben aplicarse los siguientes controles:

- El acceso al área de carga desde fuera del edificio debe estar restringida a personal autorizado e identificado.
- 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.
- Las puertas externas del área de carga deben estar aseguradas cuando las puertas internas estén abiertas.
- El material entrante debe ser revisado por peligros potenciales antes de ser movido del área de carga al punto de utilización.

8.9.2 <u>Seguridad de los equipos</u>

Garantizar la seguridad de los equipos de TRANSMILENIO S.A., permite prevenir pérdidas, daño o compromiso de los activos y la interrupción de las actividades del negocio.

Los equipos deben estar físicamente protegidos contra amenazas físicas y ambientales.

8.9.2.1 Instalación y protección de los equipos

La infraestructura tecnológica de TRANSMILENIO S.A. tal como, servidores, enrutadores, equipos de proceso central, PBX's y otro tipo de hardware de computador que no resida típicamente en escritorios

de usuario o en una 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.

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. Es responsabilidad de los funcionarios de la Entidad propender por el buen uso y cuidado del computador asignado.

8.9.2.2 Instalaciones de suministro

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

Las siguientes opciones para fuentes de poder continuas deben ser usadas:

- Múltiples fuentes para evitar puntos de fallo en una fuente de poder. Esquema presentado en dispositivos activos y servidores del centro de cómputo.
- Fuentes de poder ininterrumpidas (UPS).
- Generadores de respaldo.

8.9.2.3 Seguridad del cableado

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.

Deben aplicarse los siguientes controles:

- Las líneas de energía y telecomunicaciones dentro de las instalaciones de procesamiento de la información deben estar ocultas donde sea posible o sujetas a protección alternativa.
- El cableado de redes debe estar protegido de daño o interceptación no autorizada, por ejemplo usando conductos o rutas para evitar pasar a través de áreas públicas.
- Los cables de potencia deben estar separados de los de comunicaciones para prevenir interferencias.
- Los cables se deben marcar e identificar claramente para evitar errores en su manipulación.
- Las áreas de distribución de redes deben estar físicamente aseguradas para prevenir la modificación o el acceso no autorizado.
- Para los sistemas sensibles o críticos además de los controles anteriores se debe tener en cuenta:
    - Instalación de conductos blindados y cuartos bloqueados o cajas para puntos de inspección y terminación.
    - Uso de enrutamiento alternativo y/o medios de transmisión.
    - Uso de cableado de fibra óptica. Iniciación de barrido técnico e inspección física para dispositivos no autorizados que estén conectados a los cables.

8.9.2.4 Mantenimiento de Equipos

Los equipos deben ser mantenidos acorde con las especificaciones e intervalos de servicio recomendados por los Fabricantes.

Deben mantenerse los registros de todas las fallas reales o sospechosas y todo el mantenimiento preventivo y correctivo. Dichos registros tienen trazabilidad en la herramienta Aranda.

8.9.2.5 Salida de activos fuera de las dependencias de la empresa

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.

Los siguientes controles deberán ser aplicados:

- Los equipos no se deben dejar desatendidos en lugares públicos.
- Los equipos portátiles se deben llevar como equipaje de mano cuando se esté viajando.
- Se deben seguir los hábitos de seguridad comunes del lugar de trabajo: seguridad de equipo desatendido, escritorio limpio, control de acceso para usuarios autorizados.

8.9.2.6 Reutilización o retirada segura de dispositivos de almacenamiento

Eliminación de la información

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

Los procedimientos de eliminación adecuados son:

- Eliminar a bajo nivel la información por aplicaciones de software o hardware.
- Sobrescribir los datos almacenados para evitar su posible recuperación.
- Desmagnetizar medios de almacenamiento.
- Destruir físicamente los medios de almacenamiento – evitar la posibilidad de su lectura usando hardware estándar.

Donación / venta de equipos

Existen varios factores a tener en cuenta sí TRANSMILENIO S.A., opta por donar el equipo para caridad o venderlo a un tercero:

- Antes de cualquier venta o donación, todos los medios de almacenamiento deben ser borrados de acuerdo con los mecanismos de eliminación de información mencionados anteriormente.
- Cualquier marca que pudiera identificar el equipo como propiedad de TRANSMILENIO S.A., o asociado con él, debe ser eliminada.
- Se debe asegurar que no exista garantía o responsabilidad de TRANSMILENIO S.A., para la función u operación del equipo.

8.9.2.7 Equipo informático de usuario desatendido

Los usuarios deben asegurar que el equipo desatendido tiene una adecuada protección y están obligados 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.
- 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.
- 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).

8.9.2.8 Política de puesto de trabajo despejado y bloqueo de pantalla

La política de escritorio limpio y pantalla limpia aplica para toda la información de la TRANSMILENIO S.A., para cual debe tenerse en cuenta la clasificación de información, requerimientos legales y contractuales y los correspondientes riesgos y aspectos culturales de la organización.

- 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.
- 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.
- Uso no autorizado de fotocopiadoras y otra tecnología de reproducción como escáner y cámaras digitales.
- Documentos con información clasificada o sensitiva deben removerse de impresoras tan pronto como sea posible.

8.10 Adquisición desarrollo y mantenimiento de los sistemas de información

8.10.1 Requisitos de Seguridad de los sistemas de Información

Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida, esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.

- 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. Las áreas propietarias de sistemas de información, la Dirección de TIC's incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán 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.
- Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica de

TRANSMILENIO S.A., gestionado por cualquier dependencia o proyecto de la Entidad, deberá ser aprobado por la Dirección de TIC´s.

- Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.
- El área de soporte de la Dirección de TIC´s de TRANSMILENIO S.A., será la única dependencia autorizada para realizar copia de seguridad del software original.
- La instalación del software en computadores de la Entidad, se llevará a cabo únicamente por funcionarios del área de Soporte o por terceros autorizados y supervisados por la Dirección de TIC´s.
- Los softwares proporcionados por TRANSMILENIO S.A. no pueden ser copiados o suministrados a terceros.
- En los equipos de TRANSMILENIO S.A solo se podrán utilizar los softwares licenciados por la Dirección de Tecnología de la Información y las Comunicaciones.
- 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.
- El software que se adquiera a través de los proyectos o programas, debe quedar a nombre de TRANSMILENIO S.A.
- Se encuentra prohibido el uso e instalación de juegos en los computadores de TRANSMILENIO S.A.

8.11 Seguridad en la operación

8.11.1 Responsabilidades y procedimientos de operación

Objetivo: asegurar y garantizar que los cambios sobre la infraestructura de tecnología de información, los servicios prestados por terceras partes, procedimientos, controles y comunicaciones en TRANSMILENIO S.A. se realicen e implementen adecuadamente siguiendo procedimientos estándar.

8.11.1.1 Procedimientos operativos documentados

Los procedimientos son uno de los elementos dentro de la documentación del Manual de Políticas de Seguridad de la Información. Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso, en él se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso.

También es recomendable el uso de instructivos para detallar aún más las tareas y acciones puntuales que se deben desarrollar dentro de un procedimiento, como son los instructivos de trabajo y de operación; los primeros para la ejecución de la tarea por la persona y los segundos para la manipulación o la operación de un equipo.

Los funcionarios de TRANSMILENIO S.A., pueden consultar las descripciones detalladas de cada procedimiento a través del sistema integrado de gestión disponible en la Intranet de la Entidad o en la Dirección de TIC´s de TRANSMILENIO S.A.

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

Ver los procedimientos siguientes:

- P-DT-002-1 Administración bases de datos administrativas.
- P-DT-003 Especificación y gestión de requerimientos para solicitud.
- P-DT-004 Gestión ambiente de pruebas de software.
- P-DT-005 Compra y actualización de software.
- P-DT-007 Administración de usuarios.
- P-DT-008 Mantenimiento de los equipos de cómputo.
- P-DT-009 Soporte técnico a usuarios finales.
- P-DT-010 Monitoreo del uso de medios.
- P-DT-011 Otorgar acceso a los medios.
- P-DT-012 Intercambio de información.

8.11.1.2 Control de cambios

TRANSMILENIO S.A., debe implementar un proceso documentado para realizar el control de cambios. Las solicitudes de control de cambios deben incluir:

- Nombre del Solicitante
- Área y cargo del solicitante
- Motivo del cambio

- Nombre del autorizador.
- Configuraciones de software – ejemplo actualizaciones de aplicaciones.
- Requerimientos de servicio – ejemplo ventana de tiempo para mantenimiento del sistema.
- Parches de sistema operativo – ejemplo parches de Windows
- Evaluación de Impacto.

El proceso de control de cambios debe contener los siguientes elementos:

- Administración de activos - identificación de sistemas en producción.
- Administración de la configuración – tiempo de los cambios, autor de los cambios, razones para los cambios.
- Aprobación del flujo de trabajo – procesos documentados para la aprobación de los cambios.
- Proceso de versiones – pruebas, ventana de cambios, respaldo de los procesos.

El profesional especializado 06 de seguridad de la información de TRANSMILENIO S.A., debe estar incluido en el proceso de control de cambios para asegurar que los cambios implementados no comprometen la seguridad, ni permitan materializar incidentes de seguridad de la información.

8.11.1.3 Gestión de Capacidades

Las demandas de capacidad deben ser monitoreadas y las proyecciones de los requerimientos de capacidad deben asegurar el poder 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 de TRANSMILENIO S.A.

Los recursos del sistema tales como procesadores, almacenamiento, impresoras y otros dispositivos de salida y sistemas de comunicación deben ser monitoreados para identificar las tendencias de uso de estos recursos.

La Dirección de TIC's debe usar esta información para identificar y evitar posibles cuellos de botella que puedan presentar una amenaza para la seguridad del sistema o los servicios del usuario, y planear adecuadamente las medidas correctivas.

8.11.1.4 Separación de entornos de desarrollo, pruebas y producción

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 los mismos.

Controles que deben implementarse:

- Las reglas para la transferencia de software de desarrollo a producción deben estar definidas y documentadas.
- Planeación y pruebas de cambios.
- Evolución de impactos potenciales, incluyendo impactos de seguridad.
- Procedimientos de aprobación formal.
- Comunicación de detalles de cambios a todas las personas relevantes.
- Procedimientos de retorno incluyendo responsabilidades para abortar y recuperarse de cambios no satisfactorios y eventos imprevistos.

8.11.2 Protección contra código malicioso

Objetivo: la presente política promueve la protección de la integridad, disponibilidad y confidencialidad del software y la información almacenada en él.

Se requieren precauciones para prevenir y detectar la introducción de software malicioso. El software y los servicios de procesamiento de información son vulnerables a la introducción de software malicioso, tal como virus informático, gusanos de red, caballos troyanos, software espía y bombas lógicas, entre otros.

8.11.2.1 Controles contra el código malicioso

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. Esto incluye los siguientes requerimientos:

- Es obligatorio usar un software de detección y remoción de código malicioso (antivirus) en todos los computadores, dispositivos móviles, teléfonos inteligentes y cualquier tipo de equipo de cómputo empleado para acceder a los servicios y sistemas de información de TRANSMILENIO S.A.
- Todos los ambientes de correo electrónico deben desplegar la detección de virus.

- El antivirus debe ser instalado con su respectiva licencia para todas las estaciones de trabajo de TRANSMILENIO S.A (servidores, computadores de escritorio y portátiles) y debe ser desplegado a todos los sistemas de usuario final.
- El antivirus corporativo debe mantenerse actualizado en todos los PC y servidores de TRANSMILENIO S.A.
- Los parches se deben aplicar periódicamente a las estaciones y servidores para garantizar que se mantienen protegidos. La periodicidad es definida por el fabricante del software quien los libera para su uso.
- Los usuarios finales de los computadores no deben detener, desinstalar o alterar el funcionamiento del software de antivirus. Las modificaciones sobre el software de antivirus solo deben ser realizadas por personal formalmente por la Dirección de TIC's.
- Es obligatorio realizar verificaciones periódicas automáticas a los computadores de la Entidad, de acuerdo con el estándar que defina Comité de Seguridad dela Información de TRANSMILENIO S.A.
- No se puede usar software no instalado y autorizado por la Dirección de TIC's.

8.11.3 Copias de seguridad

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

El respaldo de la información busca reducir el impacto de los riesgos asociados a la pérdida de información y es un mecanismo para soportar los planes de contingencia, recuperación ante desastres y atención a incidentes de seguridad de la información adoptados por la Entidad, aportando a el cumplimiento de la integridad y disponibilidad de la información.

Se deben establecer procedimientos de rutina llevar a cabo la estrategia de copias de seguridad tomando copias de backup de datos y ensayando su oportuna restauración, registrando eventos, incidentes y fallas.

8.11.3.1 Copias de Seguridad de la Información

Las copias de seguridad de la información y software esencial de la Entidad deben ser tomadas regularmente de acuerdo con las necesidades de TRANSMILENIO S.A.

Frecuencia del backup

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. Ver procedimiento P-DT-002-1 Administración bases de datos Administrativas.

Almacenamiento de backup

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.

Seguridad del almacenamiento de backup

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.

En los casos donde la confidencialidad de la información es importante, los datos deben ser protegidos por medio de cifrado.

Restauración y pruebas

Los procedimientos de restauración deben ser regularmente verificados y controlados para asegurar que son efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operativos para la recuperación.

La solicitud de restauración de información deberá ser solicitada a través de correo electrónico dirigido al área de soporte técnico de la siguiente dirección (soportetecnico@transmilenio.gov.co)

Las copias de respaldo de la información deben ser preservadas por el tiempo definido en las tablas de retención documental y aprobadas por los responsables de los procesos a los que pertenece la información.

8.11.4 <u>Registro de Actividad y supervisión.</u>

Objetivo: garantizar la Integridad y confidencialidad de la información almacenada y procesada en los sistemas de información de TRANSMILENIO S.A. Con el fin de detectar actividades de procesamiento de información no autorizadas y prevenir la perdida de servicios y cumplir con requerimientos legales.

8.11.4.1 Registro y gestión de eventos de actividad

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

Los registros de eventos (event logs) establecen las bases para los sistemas de seguimiento automatizados que están en capacidad de generar informes consolidados y alertas sobre la seguridad del sistema.

Los registros de auditoría deben incluir en lo posible:

- Identificación de usuarios.
- Fechas, horas y detalles de los eventos claves, por ejemplo acceso al sistema (log-on) y salida del sistema (log-off).
- Identificación de terminal.
- Registros de intentos de accesos satisfactorios y rechazados.
- Cambios a la configuración del sistema.
- Uso de utilitarios y aplicaciones.
- Archivos accedidos.
- Activación y desactivación de protecciones del sistema.

8.11.4.2 Protección de los Registros de información

Los registros de información se deben proteger contra intentos de alteración y acceso no autorizado.

Los controles deben fortalecer la protección contra cambios no autorizados y problemas operacionales:

- Alteración a los tipos de mensajes que son registrados.
- Archivos de log que estén siendo editados o eliminados.
- La capacidad de almacenamiento medio del archivo de log que esté siendo excedida y resultado de ello se presenten fallas al registrar eventos o sobrescriba registros recientes.

Los logs de auditoría deben ser archivados y retenidos por el tiempo fijado y establecido en las tablas de retención documental las cuales deben ser acordadas con los propietarios de la información.

8.11.4.3 Registro de actividad del administrador y operador del sistema.

Se deben establecer procedimientos e implementación de controles que permitan registrar las actividades y operaciones realizadas por el administrador y operador del sistema, para lo cual se debe como mínimo contemplar lo siguiente:

- Implementar registros que muestren las actividades realizadas por los administradores o los operadores de los equipos o servicios a su cargo.
- Procedimiento de mantenimiento de los registros de las fallas sobre los equipos o servicios a su cargo.
- Implementar registros de los usuarios a los cuales se les ha otorgado acceso privilegiado a cada activo, servicio o componente.
- Realizar una revisión periódica de los privilegios de acceso otorgados a los usuarios de los servicios o componentes a su cargo.

8.11.4.4 Sincronización de relojes

Los relojes de todos los sistemas de información relevantes de TRANSMILENIO S.A., deben estar sincronizados contra una fuente de tiempo exacto.

La política en TRANSMILENIO S.A., es que todos los servidores de su data center administrativo deben estar sincronizados contra el servidor de referencia internacional.

8.11.5 <u>Control del software en explotación</u>

Las siguientes directrices deben tenerse en cuenta para la instalación de software en TRANSMILENIO S.A.:

- La actualización de software, aplicaciones y bibliotecas de programas solo debe ser ejecutada por ingenieros de la Dirección de TIC´s o por personal técnico designado por terceros responsables de las aplicaciones.
- Una estrategia de retorno (rollback) debe definirse antes que los cambios sean implementados.
- Se debe mantener un registro de auditoría de todas las actualizaciones a las bibliotecas de programas en producción.
- Versiones previas del software de aplicación se deben retener como una medida de contingencia.
- El software usado en sistemas debe ser mantenido en un nivel soportado por el proveedor.

- Toda decisión de actualizar a una nueva versión (release) debe tener en cuenta los requerimientos de la Entidad para el cambio y la seguridad de la nueva versión como la introducción de nueva funcionalidad de seguridad o el número y severidad de problemas de seguridad que afectan esta versión.
- Los parches de software deben aplicarse cuando puedan ayudar a remover o reducir amenazas de seguridad.

8.11.6 Gestión de la vulnerabilidad técnica

8.11.6.1 Gestión de las vulnerabilidades técnicas

TRANSMILENIO S. A., debe implementar procedimientos para la gestión de vulnerabilidades técnicas que como mínimo deben contemplar:

- Inventario de activos de información, identificando para cada uno de ellos si son elementos tecnológicos, su sistema operativo y aplicaciones instaladas.
- Acceso a fuentes de información técnica que notifiquen sobre las vulnerabilidades descubiertas.

8.11.6.2 Restricciones en la instalación de software

Objetivo: garantizar que las restricciones para la instalación de software en los equipos tecnológicos de TRANSMILENIO S.A. se realicen e implementen adecuadamente siguiendo procedimientos estándar que incluyan.

- No se deben realizar cambios sin la previa autorización de TRANSMILENIO S.A.
- No se debe poner en peligro la integridad de la información debido a la falta de revisión de los cambios.
- No se deben realizar cambios por usuarios no autorizados.
- No se pueden realizar cambios que atenten o vayan en contra de las estrategias de continuidad y seguridad definidas por TRANSMILENIO S.A.
- Está totalmente prohibida la instalación de software no autorizado en los equipos de TRANSMILENIO S.A.
- Si se requiere la instalación de algún tipo de herramienta colaborativa esta debe ser revisada y autorizada por el profesional especializado 06 de Seguridad de la Información.
- Todo software a instalar debe pasar por un proceso de sanitización.
- El personal de TRANSMILENIO S.A debe reportar mediante los conductos aprobados la solicitud de cambios o nuevos requerimientos tecnológicos, de servicios o sistemas de información.

8.11.7 Consideraciones de las auditorías de los sistemas de información

8.11.7.1 Controles de auditoria de los sistemas de información

Los requerimientos de auditoría y las actividades que involucran pruebas sobre los sistemas, deben ser cuidadosamente planeados y aprobados para minimizar el riesgo de interrupciones en la Entidad.

- Los requerimientos de auditoría deben ser acordados y aprobados en conjunto con las áreas involucradas.
- El alcance de las pruebas debe ser acordadas y controladas.
- Las pruebas deben ser limitadas a solo acceso de lectura para software y datos.
- Acceso diferente a solo lectura debe solo ser permitido para copias aisladas de archivos del sistema, que deben ser borradas cuando la auditoría sea completada o dársele la adecuada protección si es necesario mantener los archivos como evidencia de la auditoría.
- Los recursos de TI para la realización de las pruebas deben ser explícitamente identificados solicitados.
- Todos los accesos deben ser monitoreados y registrados para generar pistas de referencia.
- Todos los procedimientos, requerimientos y responsabilidades deben ser documentados.

8.11.7.2 Protección de las herramientas de auditoría de sistemas de información

- Las herramientas de auditoría de sistemas de información deben ser protegidas para prevenir el uso indebido o manipulación.
- 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.

8.12 Politicas que rigen la relacion con terceras partes

Objetivo: establecer mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

8.12.1 Normas de inclusión de condiciones de seguridad en la relación con terceras partes

Normas dirigidas a: **Dirección de Tecnologías de la Información y las Comunicaciones**

- La Dirección de TIC's debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de TRANSMILENIO S.A.
- La Dirección de TIC´s debe establecer las condiciones de comunicación segura, cifrado si es pertinente y transmisión de información desde y hacia los terceros proveedores de servicios.
- La Dirección de TIC´s debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de TRANSMILENIO S.A.

Normas dirigidas a: **supervisores de contratos con terceros**

- Los Supervisores de contratos con terceros deben divulgar 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, por parte de los terceros se realice de manera segura.

8.12.1.1 Tratamiento del riesgo dentro de acuerdos de proveedores

Los riesgos de acceso a través de una conexión de red son diferentes de los riesgos resultantes de acceso físico. Por lo tanto, ambos accesos físico y lógico deben ser protegidos.

Todos los accesos de las terceras partes deben pasar por un análisis de riesgos de seguridad con estrategias de mitigación que deben ser implementadas antes que la conexión esté operativa.

8.12.1.2 Cadena de suministro en tecnología de la información y las comunicaciones

El profesional especializado 06 de seguridad de la información de la Dirección de Tecnología de la Información y las Comunicaciones y la Subgerencia Jurídica, deben identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.

Los supervisores de contratos con terceros, con el apoyo del profesional especializado 06 de seguridad de la información, deben administrar los cambios en el suministro de servicios por parte de los, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

8.12.2 Gestión de la prestación de servicios por proveedores

8.12.2.1 Supervisión y revisión de los servicios prestados por terceros

Los servicios, reportes y registros provistos por el tercero deben ser regularmente monitoreados y revisados y se deben adelantar auditorías con regularidad.

El monitoreo y la revisión tiene como propósito asegurar que los términos y condiciones de seguridad de la información del acuerdo están siendo cumplidos y los incidentes y problemas de seguridad son manejados apropiadamente. Se debe poner especial atención en el control cuando el servicio tercerizado implica el manejo de información sensitiva o crítica para TRANSMILENIO S.A.

8.12.2.2 Gestión de cambios en los servicios tercerizados

Cambios a la provisión de servicios, incluyendo mantenimiento y mejoras a las políticas de seguridad existentes, procedimientos y controles, deben ser manejados teniendo en cuenta la criticidad de los sistemas y procesos de la Entidad involucrados y la re-evaluación de riesgos.

Se debe tener en cuenta:

Cambios hechos por TRANSMILENIO S.A. para implementar:

- Ampliaciones a los servicios y procesos ofrecidos actualmente.
- Desarrollo de nuevas aplicaciones y sistemas.

- Modificaciones o actualizaciones a las políticas y procedimientos de TRANSMILENIO S.A.

Cambios del tercero para implementar:

- Cambios y ampliaciones a las redes.
- Uso de nuevas tecnologías.
- Nuevas herramientas de desarrollo y ambientes.
- Cambios de la localización física o instalaciones de servicio.

8.13 Politica de gestión de incidentes de seguridad de la información

8.13.1 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 debilidad.

8.13.1.1 Política para el reporte y tratamiento de incidentes de seguridad

TRANSMILENIO S.A. promoverá entre los funcionarios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

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.

8.13.1.2 Normas para el reporte y el tratamiento de incidentes de seguridad.

Normas dirigidas a: **propietarios de los activos de información**

Los propietarios de los activos de información deben informar a la Dirección de TIC´s 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.

Normas dirigidas a: **Dirección de Tecnologías de la Información y las Comunicaciones**

- Debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- Debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad de la Información aquellos en los que se considere pertinente.
- 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.
- 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.

Normas dirigidas a: **comité de seguridad de la información**

El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Normas dirigidas a: **todos los usuarios**

Es responsabilidad de los funcionarios del TRANSMILENIO S.A. y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

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 TIC´s para que se registre y se le dé el trámite necesario.

8.14 Aspectos de seguridad de la información en la gestión de la continuidad de negocio

8.14.1 Continuidad de seguridad de la información.

Objetivo: la Continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.

8.14.1.1 Política de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

TRANSMILENIO S.A. proporcionará los recursos suficientes para dar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la Entidad y que afecten la continuidad de su operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. TRANSMILENIO S.A., mantendrá canales de comunicación adecuados hacia funcionarios, y terceras partes interesadas.

8.14.1.2 Normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

Normas dirigidas a: Dirección de Tecnología de la Información y las Comunicaciones

- Debe elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.
- Debe participar activamente en las pruebas de recuperación ante desastres y notificar los resultados al Comité de Seguridad de la Información.
- Debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
- Debe liderar los temas relacionados con la continuidad del negocio y la recuperación ante desastres.
- Debe realizar los análisis de impacto a la entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

Debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

- 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.
- La Dirección de TIC´s debe elaborar un plan de recuperación ante desastres para el centro de cómputo administrativo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.

Normas dirigidas a: **gerente, subgerentes, directores y jefes de oficina**

El gerente, subgerentes, directores y jefes de oficina deben identificar al interior de sus áreas los posibles escenarios de riesgo y generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, en lo referente a seguridad de la información. Estos procedimientos deben someterse a las pruebas correspondientes para validar su efectividad.

8.14.2 Redundancia

Objetivo: asegurarse de 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.

8.14.2.1 Normas de Redundancia

Normas dirigidas a: **Dirección de Tecnología de la Información y las Comunicaciones**

- Debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la entidad y la plataforma tecnológica que los apoya.
- Debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de TRANSMILENIO S.A.
- 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.

8.15 Cumplimiento

8.15.1 Cumplimiento de los requisitos legales y contractuales.

8.15.1.1 Identificación de la legislación aplicable

TRANSMILENIO S.A velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

8.15.1.2 Derechos de propiedad Intelectual

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.

8.15.1.3 Protección de los registros de la Organización

Los registros críticos de TRANSMILENIO S.A deben ser protegidos de pérdida, destrucción, acceso no autorizado, duplicación no autorizada, manipulación, alteración y falsificación y se debe establecer las tablas de retención documental descritas, establecidas por la entidad y requeridas por la ley.

8.15.1.4 Protección de datos y privacidad de la información personal

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, TRANSMILENIO S.A. a través de la Subgerencia De Comunicaciones y Atención al Usuario, propenderá por la protección de los datos personales de sus beneficiarios, y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales el TRANSMILENIO S.A., como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la Entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, TRANSMILENIO S.A. exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que TRANSMILENIO S.A. conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la Entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

8.15.1.5 Regulación de controles criptográficos

- Está expresamente prohibido cifrar información con mecanismos no autorizados por el sistema de gestión de seguridad de la información de TRANSMILENIO S.A.
- Está expresamente prohibido cifrar información sin la autorización del custodio de la información.
- Está expresamente prohibido revelar las claves privadas de cifrado de información a personal no autorizado.

8.15.2 Revisiones de la Seguridad de la Información

El gerente, subgerentes, directores, jefes de oficina y en general funcionarios que por su grado de responsabilidad y funciones tengan personal a cargo, deben asegurar que todos los procedimientos de seguridad dentro de sus áreas, son llevados a cabo correctamente para cumplir con los estándares y políticas de seguridad. Todas las áreas de la organización deben ser objeto de revisiones regulares con el fin de verificar el cumplimiento con las políticas y estándares de seguridad.

El profesional especializado 06 debe establecer procedimientos de validaciones de cumplimiento para las políticas expresadas en el presente manual, a fin de que todos los funcionarios de TRANSMILENIO S.A. cumplan a cabalidad con las políticas y lineamientos descritos esto debe incluir verificaciones físicas y digitales.