Políticas de Seguridad y Privacidad de la Información.

TRANSMILENIO S.A.

TABLA DE CONTENIDO

INTRODUCCIÓN **7**

1. OBJETIVO **8**

2. ALCANCE **8**

3. RESPONSABLES **8**

4. DEFINICIONES **8**

ELABORÓ:	APROBÓ:	
Daniel Leonardo Beltrán Gonzalez **Contratista de la Dirección de TIC** Javier Alfonso Castañeda Parra **Profesional Especializado Grado 06 - Seguridad de la Información** **Vo.Bo.** Rafael Felipe Valdez Laguado **Director de TIC**	COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO: Maria Fernanda Ortiz Carrascal **Gerente General** Gina Alexandra Vaca Linares **Directora Corporativa** Rafael Felipe Valdez Laguado **Director Tecnologías de la Información y Comunicaciones** Xiomara Sined Romero Aguirre **Jefe Oficina Asesora de Planeación** Yolima Pérez Ariza **Subgerente de Atención al Usuario y Comunicaciones** Camilo Ernesto Forero Barrera **Subgerente Jurídico** Claudia Cecilia Puentes Riaño **Subgerente de Negocios Colaterales** Candelaria Gonzalez **Subgerente Técnico y de Servicios** Marcos Antonio Ataya Saray **Subgerente Económico** Carmen Yanneth Rosales Suarez **Directora Técnica de Infraestructura** Lucy Cucaita Cruz **Directora Técnica de Buses** Natalia Tinjaca Mora **Directora Técnica de Seguridad** Jaime Enrique Monroy Garavito **Director Técnico de BRT** Janneth Johana Buriticá Rodriguez **Jefe Oficina de Control Disciplinario Interno**	

5. DOCUMENTOS DE REFERENCIA 16
6. AUTORIDADES Y ROLES DE SEGURIDAD DE LA INFORMACIÓN 18
7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 19
7.1. Política de alto nivel del sistema de gestión de seguridad de la información (SGSI) 20
7.1.1. Compromiso de la Dirección 20
7.2. Políticas De Seguridad Organizacional 21
7.2.1. Política de control de acceso 21
7.2.2. Política de transferencia de información 29
7.2.3. Política de gestión y clasificación de activos de información 33
7.2.4. Política de seguridad en las operaciones 38
7.2.5. Política de seguridad de la información con los proveedores 42
7.2.6. Política de privacidad y protección de datos personales 43
7.2.7. Política de gestión de continuidad del negocio 44
7.2.8. Política gestión de incidentes de seguridad 45
7.2.9. Política de cumplimiento 46
7.3. Políticas de seguridad del personal 47
7.3.1. Política de teletrabajo 47
7.3.2. Política de confidencialidad 49
7.3.3. Política del recurso humano 50
7.3.4. Política de cultura y sensibilización en seguridad de la información 52
7.4. Políticas de seguridad física 53
7.4.1. Política de áreas seguras 53
7.4.2. Política de seguridad de los equipos 57
7.4.3. Política de escritorio y pantalla limpia 59
7.5. Políticas de seguridad tecnológica 60
7.5.1. Política para dispositivos móviles 60
7.5.2. Política de seguridad en las telecomunicaciones 61
7.5.3. Política sobre el uso de controles criptográficos 63
7.5.4. Política de desarrollo seguro 64
7.5.5. Política de copias de respaldo 68
7.5.6. Política de seguridad en la nube 69
8. EXCEPCIONES EN LAS POLÍTICAS 70
9. REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 70

MODIFICACIONES:

VERSIÓN	FECHA	CAMBIO	SOLICITO
0	01-may-2016	Primera versión Oficial del documento	No Aplica
1	30-mar-2017	Se eliminan No. 6.3 Compromisos de la dirección y No. 6.5.2. “Normas que rigen para la estructura organizacional de seguridad de la información”. Se realiza la construcción de procedimientos que complementen y fortalezcan el manual respecto a los numerales: “8.6.1.3 Proceso disciplinario”, “8.7 Gestión de activos” y “8.7.5 Manejo de los soportes de almacenamiento”	Dirección de TIC
2	25-jul-2018	Se cambia el título de manual de políticas de seguridad de la información, por políticas de seguridad y privacidad de la información. Se realiza cambio estructural y de contenido, al Manual de políticas de seguridad y privacidad de la información, de acuerdo con la normatividad vigente y los riesgos existentes en las organizaciones	Dirección de TIC
3	26-mar-2019	Se incluyen las referencias a los siguientes Procedimientos y Protocolos. • Procedimiento: P-DT-012: Procedimiento para el Intercambio Seguro de la Información Electrónica • Protocolo: T-DT-001: Protocolo para la Revisión de Informes de Interventoría al Contrato de Concesión SIRCI. • Protocolo: T-DT-003: Protocolo a Seguir para Gestionar el Uso de los Medios Removibles Se realiza el ajuste del Numeral 9.2.2.4 Eliminación de los medios. Donde se elimina la referencia al nivel 7 dado que esto excede los tiempos de respuesta y el borrado puede efectuarse con herramientas más rápidas. Se realizó el ajuste del numeral 9.5 Política de seguridad en las operaciones. donde se agregaron las políticas relacionadas con los	Dirección de TIC

VERSIÓN	FECHA	CAMBIO	SOLICITO
		registros de auditoría. Numerales n) al r). Lo anterior de acuerdo con lo requerido por la Norma ISO 27001:2013.	
4	27-abr-2021	Incorporación en el numeral 8.4.2 Identificación y autenticación, del literal d), correspondiente al uso de cuentas genéricas o de servicio. Se ajusto el numeral 9.8 aclarando que se aplicaran los lineamientos establecidos en el Manual M-SC-006 “Política de tratamiento y protección de datos personales” de TRANSMILENIO S. A.	Dirección de TIC
5	8-oct-2021	Se ajusta el literal f) del numeral 9.6, a fin de articular la periodicidad de pruebas de restauración con el procedimiento de backup P-DT-019.	Dirección de TIC
6	1-dic-2022	Se crea el numeral 10.4. Excepciones a las políticas de seguridad, en el marco del cual se incorpora el Anexo 1. Excepciones de Seguridad de la Información.xlsx. Se modifica el numeral “9.6 Política de copias de respaldo” agregando el numeral i).	Dirección de TIC
7	01-abr-2025	Se cambia de codificación del documento según tipología establecida en el sistema de gestión pasando de Manual (M-DT-001) a políticas (L-DT-002). Se reorganizan las políticas de seguridad y se distribuyen según los dominios de control de la norma ISO/IEC 27001:2022, por lo tanto, se renumera el documento. Se realiza el ajuste de redacción de políticas y se agregan nuevas políticas según la norma ISO/IEC 27001:2022. Dentro de estas políticas se encuentran: 1. Uso del formato de autorización de servicios (Seguridad en las operaciones), 2. Tiempo de uso de las memorias usb, temporal. (Gestión de medios removibles), 3. Política de uso de las redes: Conexión a la red por cable, uso de las wifi. (Política de seguridad en las	Dirección de TIC

VERSIÓN	FECHA	CAMBIO	SOLICITO
		telecomunicaciones), 4. Manipulación de equipos: abrir equipos, retirar cables, desconectar. (Política de seguridad de los equipos), 5. Uso de equipos personales de los funcionarios. (Seguridad en las operaciones), 6. Restricciones de acceso al correo electrónico por país. (Política de transferencia de información), 7. IMAP restringido únicamente a equipos dentro del dominio. (Política de transferencia de información), 8. Inicio de sesión de OneDrive restringido únicamente a los equipos dentro del dominio. (Seguridad en las operaciones), 9. Acta de asignación de los usuarios administradores (política de control de acceso), 10. Política de creación de usuarios administradores (política de control de acceso), 11. Políticas de contraseñas: longitud, complejidad, etc. (política de control de acceso), 12. Política de uso del Multifactor MFA (política de control de acceso), 13. Gestor de aplicaciones permitidas en la entidad con InTune (Seguridad en las operaciones), 14. Política de acceso remoto por VPN (Política de seguridad en las telecomunicaciones), 15. Bloquear la navegación a internet de los controladores de dominio y restringir correspondencia (Política de seguridad en las telecomunicaciones), 16. Políticas de Ciberseguridad (objetivo y alcance), 17. Políticas de IoT (Aplicación), 18. Enmascaramiento de datos (política de desarrollo seguro), 19. Borrado seguro (devolución de activos), 20. Gestión de la configuración (Seguridad en las operaciones), 21. Monitoreo de la seguridad física (Política de seguridad física), 22. Seguridad en la nube, 23. Inteligencia de amenazas (Gestión de incidentes), 25. Política de uso aceptable de equipos: qué equipos son aceptados dentro de la Entidad, 26. Política de uso aceptable de firmas digitales, 27. Uso del correo electrónico para fines de trabajo y dentro del territorio	

VERSIÓN	FECHA	CAMBIO	SOLICITO
		colombiano, 28. Envío de correos masivos, 29. Creación de grupos de correo electrónico, 30. Excepciones de Multifactor Se retira la política de 8.3.1.5. Áreas de despacho y carga, debido a que el control no aplica para la Entidad.	

INTRODUCCIÓN

La adopción de políticas y procedimientos de seguridad y privacidad de la Información en TRANSMILENIO S. A., obedece a una decisión estratégica que se alinea con la Política de Gobierno digital y su habilitador de Seguridad y Privacidad de la Información[1]. Estas políticas son diseñadas e implementadas teniendo en cuenta los objetivos, los requisitos de seguridad, los procesos, el tamaño, la tecnología y la estructura organizacional de la Entidad, con el fin de satisfacer las necesidades de los usuarios y procesos en materia de seguridad y privacidad de la información.

En la actualidad, TRANSMILENIO S. A. identifica la información como uno de los activos indispensables en la conducción y consecución de los objetivos definidos en el Plan Estratégico[2] de TRANSMILENIO S. A., razón por la cual es necesario establecer un marco en el cual se asegure que la información es protegida de manera adecuada independientemente del medio en la que ésta sea manejada, procesada, transportada o almacenada. Adicional a lo expuesto, en la medida en que los sistemas de información se constituyen en un apoyo de los procesos de la Entidad, se requiere contar con estrategias de alto nivel que permitan garantizar la protección de la información.

El presente documento describe la política institucional de seguridad de la información y las políticas específicas definidas por TRANSMILENIO S. A., las cuales se constituyen como un insumo fundamental del Sistema de Gestión de Seguridad de la Información (SGSI)[3], y se convierten en la base para la implantación de los controles, procedimientos, guías y estándares definidos para la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI).

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 la alta dirección de la Entidad. Dicha información se hará conocer a cada uno de los funcionarios y contratistas a través de los sistemas de divulgación establecidos para tal fin. (Intranet, correo electrónico, charlas de sensibilización).

[1] https://gobiernodigital.mintic.gov.co/692/w3-multipropertyvalues-533221-533236.html?__noredirect=1
[2] Acuerdo 5 de 2024
[3] Adoptado mediante la resolución 355 de 2022

1. OBJETIVO

Establecer y comunicar las políticas de seguridad, ciberseguridad y privacidad de la información de TRANSMILENIO S. A., como parte integral de su sistema de gestión de seguridad de la información (SGSI), con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información de la Entidad, en el marco de la norma ISO/IEC 27001:2022.

2. ALCANCE

La presente política es de obligatorio cumplimiento y aplicación por parte de todos los trabajadores oficiales, empleados públicos, contratistas, proveedores, y terceras partes que dependan o interactúen con la Entidad, y que tengan acceso a cualquier componente de la infraestructura tecnológica (TI y TO), sistema de información o dato/información de la Entidad o sus colaboradores que se encuentre al interior de la Entidad, nube, centros alternos o ciberespacio.

3. RESPONSABLES

El Profesional Especializado grado 06 de Seguridad Informática de la Dirección de TIC es el responsable de la elaboración y actualización del presente documento.

El Director de TIC velará por su estricto cumplimiento, implementación y mantenimiento.

La revisión o actualización de este documento deberá realizarse cuando se considere pertinente por parte de los responsables de elaboración y cumplimiento.

4. DEFINICIONES

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

Activo de información: todo aquel recurso del sistema de seguridad de la información ISO 27001, necesario para que la empresa funcione alineada con las políticas de seguridad de la información. Es referido a todo aquel software o hardware o recurso humano en el que procesa, almacena o transmite información y que tiene un valor para la organización. Ejemplo: bases de datos, programas de

computación, plataforma tecnológica (procesamiento de datos o comunicaciones), documentos impresos.

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

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

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

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

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

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

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

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

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.

Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

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

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

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

Comité de seguridad: cuerpo integrado por representantes de todas las dependencias 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.

Comunicación oficial: documento de carácter oficial que emite la Entidad a nivel interno y externo.

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

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

Cultura de seguridad de la información: es aquella red de significados, acciones, creencias y comportamientos que se asocian con la seguridad y control de la información, la cual define en sí

misma la forma como una persona cuida y protege ese activo que representa esa figura valiosa para él y por ende para la organización.

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

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

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

- Incineración: destrucción de información exponiéndola a altas temperaturas para quemarla.
- Borrado Seguro: aplica solo para medio magnéticos, es un borrado a bajo nivel.
- Trituración: esto aplica más que todo a la destrucción de papel por medio de máquinas trituradoras..

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Medio de procesamiento de información: denominación genérica para todo aquel software o conjunto de aplicaciones de software, que hace de una computadora un elemento útil, debido a que posibilita al sistema para manejar una tarea específica. Pueden ser aplicaciones de propósito general, que pueden ser utilizados para una amplia variedad de tareas, como contabilidad, gestión documental,

administración, procesamiento de texto, bases de datos, entre otros. Otros tipos de software se ajustan a la computadora para acoplarse a necesidades y operaciones específicas, como bancarias, de seguros, hospitales, manufactura, entre otros.

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

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

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

Personal: empleados públicos, trabajadores oficiales vinculados, contratistas o colaboradores.

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

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

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

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

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

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 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 esta.

Sistema de información: es aquel conjunto de componentes interrelacionados que capturan, almacenan, procesan y distribuyen la información para apoyar la toma de decisiones.

Software[4]: 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..

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

[4] Tomado del estándar 729 del IEEE5

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

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

Tercero: 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.

Tecnologías de la Información (TI): es el proceso de creación, almacenamiento, transmisión y percepción de la información y los métodos de aplicación de dichos procesos.

Tecnologías de la Operación (TO): software o hardware para controlar los equipos industriales, e incluye sistemas especializados que se utilizan en los sectores de fabricación, energía, medicina y gestión de los edificios, transporte, entre otros.

Tecnologías de la información y las comunicaciones (TIC): 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.

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

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

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

5. DOCUMENTOS DE REFERENCIA

- **Constitución Política de Colombia de 1991:**

Artículo 2.	Fines esenciales del Estado.
Artículo 6.	Responsabilidad de los servidores públicos.
Artículo 15.	Derecho a la Intimidad. Hábeas data.
Artículo 20.	Derecho a la información.
Artículo 74.	Libre acceso a documentos públicos.
Artículo 122	Desempeño de funciones públicas.
Artículo 123	Desempeño de funciones de los servidores públicos.
Artículo 209	Fines de la función administrativa.
Artículo 269	Métodos y procedimientos de control interno.
Artículo 284	Acceso a información reservada.

- **Ley 23 de 1982:** ley emitida por el Congreso de la República de Colombia, acerca de la propiedad intelectual y los derechos de autor.
- **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 de 2000:** Por la cual se modifica el artículo 47 de la Ley 222 de 1995**.**

- **Ley 734 de 2002:** por la cual se expide el código disciplinario único.
- **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 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 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 1581 de 2012:** por la cual se dictan disposiciones generales para la protección de datos personales, habeas data
- **Ley 1712 de 2014:** ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
- **Decreto 1360 de 1989**: por el cual se reglamenta la inscripción de soporte lógico (software) en el registro nacional del derecho de autor.
- **Decreto 162 de 1996** por el cual se reglamenta en relación con las sociedades de gestión colectiva de derecho de autor o de derechos conexos.
- **Decreto 460 de 1995:** por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el depósito legal.
- **Decreto 2573 de 2014:** por el cual se reglamentan los lineamientos generales de la estrategia de gobierno en línea.
- **Documento CONPES 3854 de 2016:** Política Nacional de Seguridad digital.
- **Resolución 500 de 2021:** por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital, expedida por el Ministerio de las TIC.

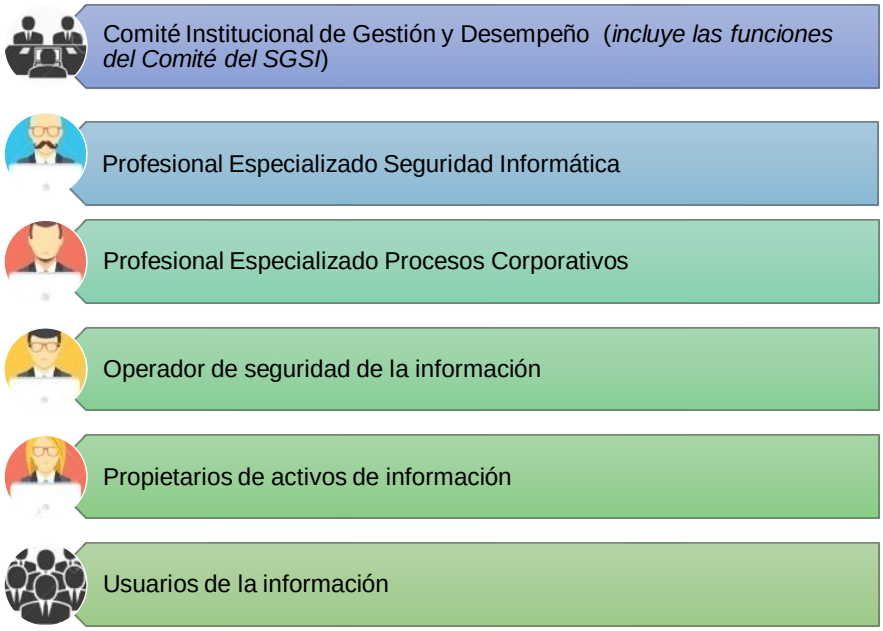
- **Resolución 746 del 2022:** por la cual se fortalece el modelo de seguridad y privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021, expedida por el Ministerio de las TIC.
- **Sentencia T-444 de 1992:** recolección de información por parte de los organismos de seguridad del Estado.
- Modelo nacional de gestión de riesgos de seguridad Digital del Ministerio de las TIC
- Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de las TIC.
- **Norma ISO/IEC 22301:** seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos.
- **Norma ISO/IEC 27001:** seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos.
- **Norma ISO/IEC 27002:** seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información
- **Norma ISO/IEC 31000:** gestión del riesgo.
- Demas normativa interna o externa.

6. AUTORIDADES Y ROLES DE SEGURIDAD DE LA INFORMACIÓN

Para asegurar el adecuado entendimiento de cada una de las políticas, a continuación se presentan las autoridades y los roles establecidos en el modelo de seguridad de la información adoptado por la entidad[5] e insumo para la definición de cada uno de los lineamientos enmarcados en el comité de seguridad de la información que hace parte de los equipos transversales del comité institucional de gestión y desempeño de la Entidad.

[5] Tomado de la NTC ISO 27001:2013

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



7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad y privacidad de la información conceptualizan el modelo de manejo de los recursos tecnológicos, humanos, datos y físicos de TRANSMILENIO S. A., en los roles de empleados públicos, trabajadores oficiales, proveedores, contratistas y terceras partes que manejan administran y custodian la información.

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

Las políticas definidas a continuación se encuentran estructuradas y orientadas con base en cada dominio o control del Anexo A de la ISO/IEC 27001:2022, y están alineadas con las prácticas de gestión de la norma ISO/IEC 27002:2022.

7.1. Política de alto nivel del sistema de gestión de seguridad de la información (SGSI)

La política de alto nivel del SGSI enuncia el compromiso de la alta dirección de TRANSMILENIO S. A., de construir la estrategia corporativa a partir de los lineamientos para la protección de la información, involucrando tanto la información digital como física, de tal forma que sean conocidos, divulgados y cumplidos de forma obligatoria por todos los funcionarios, contratistas y partes interesadas. Lo anterior, tiene como fin prevenir, detectar y mitigar de forma oportuna los riesgos de seguridad frente a una posible fuga, pérdida o alteración no autorizada de la información.

De igual manera, la política tiene como objetivo la formación de una cultura de seguridad de la información al interior de la Entidad, que permita 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.

De acuerdo con la política de alto nivel del SGSI y en articulación con el plan estratégico institucional, la entidad establece:

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

7.1.1. Compromiso de la Dirección

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

- La revisión y aprobación de las políticas de seguridad de la información contenidas en este documento.
- La promoción activa de una cultura de seguridad. a través de la ejecución de programas de sensibilización.
- Facilitar la divulgación del Manual de políticas de seguridad y privacidad de la información a todos los funcionarios de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

Asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la Entidad.

7.2. Políticas de seguridad organizacional

7.2.1. Política de control de acceso

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

7.2.1.1. Requisitos del negocio para control de acceso

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

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

señal, que no sean autorizados por la Dirección de TIC. Cualquier permiso se deberá solicitar dirección de TIC por los canales y formatos autorizados.

c) Quienes ejecuten el rol de administrador de control de acceso lógico de la Dirección de TIC deben implementar las medidas de control de acceso de los empleados públicos, trabajadores oficiales, proveedores, contratistas y terceras partes, a través de mecanismos de identificación, autenticación y autorización de acceso, a nivel de red, sistemas de información, bases de datos, instalaciones de procesamiento de información y servicios de TI de acuerdo con los perfiles y cargos establecidos en la Entidad.

d) Quienes ejecuten rol de Administrador de control de acceso lógico de la Dirección de TIC deben dar cumplimiento a la aprobación o rechazo de los permisos de conexión remota o VPN, previamente otorgada por la Dirección de TIC o por el líder u oficial de seguridad de la Información de la entidad o quien haga sus veces, En lo que respecta a la solicitud de acceso lógico que efectúen los empleados públicos, trabajadores oficiales, proveedores, contratistas y terceras partes, esta debe ir respaldada, soportada y avalada por el jefe inmediato o supervisor del contrato según sea el caso.

e) Quienes ejecuten el rol de administrador de recursos informáticos deben velar por el cumplimiento del procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red. Quienes ejecuten el rol de administrador de control de acceso lógico de la Dirección de TIC podrá realizar una verificación de los controles de acceso de los empleados públicos, trabajadores oficiales, proveedores, contratistas y terceras partes en la periodicidad que se establezca para ello, a fin de cerciorarse que dichos usuarios acceden solamente a los recursos autorizados para la realización de sus tareas, funciones u obligaciones; así mismo debe realizar la des habilitación o suspensión de aquellos usuarios, que contando con acceso activo, presenten cualquier tipo de novedad que así lo amerite. Esto aplica para todas las aplicaciones corporativas.

f) Quienes ejecuten el rol de administrador del control de acceso lógico deben asegurar que las redes inalámbricas cuenten con métodos de autenticación que eviten accesos no autorizados.

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

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

i) Los privilegios se asignarán a los usuarios de acuerdo con a los roles y responsabilidades. Los privilegios se deben extender sólo cuando sea necesario y deben contar con autorización del Profesional Especializado Grado 06 - Seguridad Informática de la Dirección de TIC, en caso de que haya lugar.

j) Los derechos de acceso a la información de todos los empleados públicos, trabajadores oficiales, 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 director, subgerente o jefe de área responsable.

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

l) La creación o asignación de usuarios administradores sobre la infraestructura tecnológica de la Entidad deberán ser realizada por los funcionarios de la Dirección de TIC responsables de los servidores, aplicaciones, sistemas de información, equipos de cómputo, redes, comunicaciones y seguridad respectivamente, a través de actas de creación, asignación o entrega según corresponda.

7.2.1.2. Identificación y autenticación

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

b) Todas las cuentas de la Entidad, a excepción de las cuentas de servicio, deberán tener habilitado de manera obligatoria el servicio de autenticación multifactor (MFA).

c) El acceso a los sistemas de información y servicios tecnológicos de la entidad, a través del uso de usuario de dominio TRANSMILENIO, debe estar restringido y delimitado a las tareas,

funciones, responsabilidades u obligaciones que ejecuten los empleados públicos, trabajadores oficiales, proveedores, contratistas y terceras partes en la entidad.

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

e) Cuentas genéricas o de servicio: son aquellas que son utilizadas para la gestión o administración de un servicio o sistema dentro de la red de TRANSMILENIO S.A y que pueden utilizarse por más de un usuario. Por lo tanto, este tipo de cuentas se crearán con un nombre genérico asociado al servicio prestado y deberán cumplir con los siguientes lineamientos específicos:

- El grupo de soporte técnico deberá realizar la entrega formal de la cuenta genérica o de servicio a los empleados públicos, trabajadores o contratistas encargados de dicha cuenta, de modo que se formalice la entrega y las responsabilidades asociadas al uso de esta.
- El responsable de la cuenta genérica deberá reportar a la dirección de TIC cuando dicha cuenta ya no se encuentre en uso, para que el Grupo de soporte técnico realice la desactivación.
- El grupo de seguridad de la información de la Dirección de TIC programará y realizará las charlas de sensibilización a los responsables de las cuentas genéricas o de servicio, donde se indiquen los riesgos de seguridad relacionados con el uso de estas cuentas.
- El grupo de seguridad de la información realizará el monitoreo frecuente del uso de dichas cuentas, con el fin de detectar incidentes de seguridad o eventos que permitan mejorar la seguridad frente al uso de estas.
- Cambiar mensualmente la contraseña de las cuentas genéricas o de servicio, sin embargo, se definen las siguientes aclaraciones:

  (i) Para el caso de las cuentas genéricas que son tipo administrador se deberán cambiar por lo menos cada seis meses.

  (ii) Para el caso de las cuentas de los usuarios de la Entidad que tienen asignado el rol de administrador, se deberá realizar el cambio mensualmente.

  (iii) Para el caso de cuentas genéricas que tengan el rol de integrar aplicaciones, se cambiarán por lo menos una vez al año.

  (iv) Cambiar la contraseña de cualquier cuenta de acuerdo con los requisitos o condiciones técnicas exigidas por los fabricantes de la infraestructura, en la instancia pertinente.

- Aplicar controles compensatorios en caso de que se identifiquen nuevos riesgos relacionados con cuentas genéricas o de servicio.
- El grupo de soporte técnico realizará una revisión y depuración anual de las cuentas genéricas para detectar aquellas que ya no se estén utilizando.

f) Las contraseñas de cualquier otra cuenta que utilice la Entidad deberán cumplir las siguientes políticas:

- Tener una longitud mínima de 14 caracteres.
- Utilizar una complejidad que incluya: letras mayúsculas, letras minúsculas, números y caracteres especiales.
- Tener una periodicidad de cambio de 2 meses calendario o menos.
- Mantener una restricción de historial de 3 contraseñas utilizadas anteriormente.
- Solicitar el cambio de la contraseña para el primer acceso.
- Bloquear la cuenta después de 5 intentos fallidos de autenticación.
- Escoger contraseñas que sean difíciles de descifrar y que no contengan información relacionada con el trabajo o vida personal, por lo cual no se debe utilizar la siguiente información: Números de identificación personal, números de teléfono, nombres de los conyugues, el mismo nombre usuario, direcciones postales, nombres propios, lugares conocidos, nombre de la Entidad, siglas de la Entidad o términos técnicos.
- Las contraseñas no deberán ser reveladas por ningún medio, tal como vía telefónica, correo electrónico o escritas.
- Las contraseñas deberán entregarse de manera segura al responsable.
- Se deberán cambiar las contraseñas que vienen definidas por defecto en los sistemas operativos, software, aplicaciones o equipos.

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

h) La responsabilidad de garantizar la implementación de estas políticas dentro de cada aplicación o sistema de información es de los administradores propios de cada aplicación o sistema.

7.2.1.3. Almacenamiento de contraseñas

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

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

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

d) El acceso por parte de un proveedor a la red interna se debe realizar por medio de un mecanismo seguro y con previa autorización de la Dirección de TIC de TRANSMILENIO S. A., utilizando los formatos definidos para tal fin.

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

f) Todas las contraseñas de los súper-usuarios (privilegios de administrador) deben ser protegidas y almacenadas en una bóveda por el Profesional Especializado Grado 06 – Seguridad Informática o el Profesional Especializado Grado 06 - Coordinación de Procesos Corporativos.

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

7.2.1.4. Control de acceso a sistemas y aplicaciones

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

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

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

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

d) Quienes ejecuten el rol de administrador del control de acceso lógico en la entidad deben asegurar que los grupos de servicios de información, usuarios y sistemas de información sean segmentados en redes.

e) Quienes ejecuten el rol de administrador del control de acceso lógico deben asegurar que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.

f) Quienes ejecuten el rol de administrador del control de acceso lógico deben establecer los controles de acceso a los ambientes de producción de los sistemas de información.

g) Quienes ejecuten el rol de administrador del control de acceso lógico deben asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

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

i) Quienes ejecuten el rol de administrador del control de acceso lógico deben restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

j) Quienes ejecuten el rol de administrador del control de acceso lógico deben asegurar que en lo que respecta a los sistemas operativos de la entidad, se bloquee la sesión automáticamente, después de determinados minutos de inactividad, previamente establecidos.

k) Quienes ejecuten el rol de desarrollador de sistemas de información deben garantizar que se cierre la sesión en las aplicaciones, después de determinados minutos de inactividad previamente establecidos.

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

m) Quienes ejecuten el rol de administrador de programas fuentes deben llevar un registro actualizado de todos los programas fuentes en uso, indicando entre otros, el nombre del programa, programador, analista responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).

n) Quienes ejecuten el rol de administrador de programas fuentes deben restringir el acceso a los códigos fuente de los programas, asegurándose de que solamente los ingenieros desarrolladores tengan acceso.

o) Quienes ejecuten el rol de administrador de programas fuentes deben mantener los códigos fuente de los programas en el servidor o repositorio de fuentes. El mantenimiento y copiado de las bibliotecas fuentes del programa está sujeto a procedimientos estrictos de control de cambios.

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

q) Quienes ejecuten el rol de administrador de programas fuentes deben mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes del programa.

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

s) Quienes ejecuten el rol de administrador de programas fuentes deben asegurarse de que los programas fuentes cuenten con una copia de respaldo actualizada, conforme a lo estipulado en el procedimiento de backup.

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

7.2.2. Política de transferencia de información

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

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

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

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

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

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

7.2.2.1. Mensajería electrónica

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

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

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

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

b. No Enviar o recibir cadenas de correo, mensajes con contenido religioso, juegos, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos. Si un usuario encuentra este tipo de material deberá reportarlo a su jefe inmediato con copia al buzón soportetecnico@transmilenio.gov.co.

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

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

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

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

g. La creación de las cuentas para el envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la Dirección de TIC de TRANSMILENIO S. A. y deberá incluir un mensaje que le indique al destinatario cómo ser eliminado de la lista de distribución.

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

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

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

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

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

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

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

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

limitado a, programas diseñados para enviar mensajes con publicidad no solicitados ("spamware"), los que se encuentran prohibidos por este documento.

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

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

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

q. El acceso a la plataforma de correo electrónico, se permitirá únicamente a las direcciones IP u orígenes que pertenezcan a Colombia. No se permite el acceso al correo electrónico ni demás servicios colaborativos desde fuera del país.

r. La sincronización del correo electrónico con aplicaciones de escritorio (IMAP, POP3) únicamente se permitirá en los equipos de escritorio, portátiles o celulares que son propiedad de TRANSMILENIO S.A y en aquellos de propiedad de los usuarios que sean autorizados por la Dirección de TIC.

s. El envío de correos masivos está permitido en primera instancia para los siguientes roles:

   i) Dirección de TIC: Representante de infraestructura tecnológica y representante de Seguridad y privacidad de la información, así como el Director de TIC o quien haga sus veces.

   ii) Dirección corporativa: Representante de la dirección corporativa y Representante de Seguridad y Salud en el trabajo, así como el Director Corporativo o quien haga sus veces.

   iii) Subgerencia de Atención al Usuario y Comunicaciones (SAUC): Representante a cargo de la Intranet. Así como el Subgerente o quien haga sus veces.

t. Si por algún motivo se presenta la necesidad de creación de una nueva cuenta a un funcionario, dependencia o área diferente a las mencionadas anteriormente, se deberá realizar la solicitud a la Dirección de TIC a través de los formatos definidos y conforme a los procedimientos establecidos, la cual deberá ser aprobada en última instancia por parte del Director de TIC. De

igual manera, la cuenta de envío de correos masivos que se cree es responsabilidad del subgerente, director o jefe de oficina de la dependencia, quien podrá designar su uso a la persona que considere necesaria. No obstante, tanto para la designación como para el cambio de personal que utilice la cuenta de correos masivos, el subgerente, director o jefe de oficina del área deberá informar a la Dirección de TIC la solicitud o el retiro de los permisos asignados cuando estos ya no se requieran.

7.2.3. Política de gestión y clasificación de activos de información

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

7.2.3.1. Inventario de activos de información

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

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

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

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

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

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

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

- Misión Crítica.
- No Crítica.

7.2.3.2. Propiedad de los activos de información

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

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

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

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

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

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

7.2.3.3. Uso aceptable de los activos de información

Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información y todos los empleados públicos, trabajadores oficiales, contratistas, proveedores, terceras partes, deben acatar y dar estricto cumplimiento a lo prescrito en la siguiente relación de políticas para el uso aceptable de los activos de información.

a. Para conectarse a la red cableada de la Entidad los equipos aceptados deben:

- Ser propiedad de TRANSMILENIO S. A.
- Estar registrados dentro del dominio de Windows de la Entidad.
- Tener instalado el software de antivirus licenciado y adquirido por la Entidad

- Tener instalado el software de XDR o EDR licenciado y adquirido por la Entidad.
- Tener instalado un sistema operativo Windows licenciado, actualizado y con soporte por parte del fabricante.
- Tener instalado únicamente el software autorizado definido por la Entidad.
- Accederse a través de cuentas del dominio.
- Tener solo un administrador local que estará a cargo de la Dirección de TIC.

b. Para conectarse a la red inalámbrica de la Entidad los equipos aceptados deben:

- Conectarse únicamente a la red inalámbrica destinada para equipos BYOD.
- Tener instalado un software de antivirus.
- Tener instalado un sistema operativo licenciado, actualizado y con soporte por parte del fabricante.
- Estar protegido por usuario y contraseña.

7.2.3.4. Devolución de los activos de información

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

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

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

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

7.2.3.5. Clasificación de la información

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

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

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

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

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

Los dueños de los procesos están obligados a clasificar y dar el tratamiento adecuado a la información de acuerdo con estos niveles y siguiendo los lineamientos de la guía de clasificación y rotulado de información.

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

7.2.3.6. Etiquetado de la información

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

7.2.3.7. Manejo de activos de información

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

7.2.3.8. Gestión de medios removibles

a. Cualquier dispositivo de almacenamiento de información (cintas magnéticas, discos extraíbles, memorias USB y reportes impresos entre otros) de propiedad de TRANSMILENIO S. A., se constituye en un activo de información, por tanto, el ingreso, uso, movilización y salida, debe ser previamente autorizado por las dependencias competentes.

b. No se permite la conexión o uso de cualquier medio removible en los equipos de la Entidad a excepción de aquellos que son propiedad de la Entidad o que son autorizados a través de los formatos definidos por la Dirección de TIC. En todo caso, cualquier medio removible autorizado tendrá una vigencia de uso de tres meses, momento en que el usuario deberá solicitar nuevamente la autorización.

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

d. El grupo de soporte debe mantener una relación de los dispositivos de almacenamiento de información de la Entidad y de sus propietarios.

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

f. Los propietarios de medios deben asegurar que éstos no queden desatendidos debido a que pueden ser susceptibles de pérdida o robo de la información. El propietario es el único responsable de mantener la confidencialidad, integridad y disponibilidad de la información contenida en el medio a su cargo.

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

h. Si ya no se requieren los contenidos previos de cualquier medio reutilizable, que será removido de la organización, deben ser borrados (eliminados).

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

7.2.3.9. Eliminación de los medios

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

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

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

7.2.3.10. Transferencia de medios físicos

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

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

7.2.4. Política de seguridad en las operaciones

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

Se debe dar cumplimiento de los siguientes lineamientos:

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

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

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

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

e) TRANSMILENIO S. A., debe implementar la gestión de configuraciones sobre la infraestructura tecnológica de tal forma que se mantenga actualizada la información de línea base de configuraciones de cada elemento tecnológico.

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

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

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

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

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

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

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

m) 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.

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

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

p) Registrar las actividades realizadas por los usuarios administradores y operadores del sistema, con el fin de realizar revisiones de comportamiento y uso del acceso privilegiado por parte de los usuarios administradores y operadores, a intervalos planeados o cuando la Dirección de TIC lo requiera. Las actividades deberán quedar registradas en los registros de auditoría de cada equipo tecnológico o en un repositorio centralizado para la recolección de logs.

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

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

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

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

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

v) Está totalmente prohibida la instalación de software no autorizado en los equipos de TRANSMILENIO S. A. Toda instalación de software que no se encuentre registrado dentro de la lista de software autorizado de la Entidad deberá solicitarse a la Dirección de TIC para su respectiva validación de seguridad y autorización.

w) 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.

x) 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.

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

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

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

bb) El Profesional Especializado Grado 06 - Seguridad de la Información de la Dirección de TIC tiene la responsabilidad de mantener el contacto con las autoridades y verificar el cumplimiento de la ley, así como las normas expedidas relacionadas con la seguridad de la información y que podría impactar la seguridad de la información de TRANSMILENIO S. A.

cc) Las solicitudes relacionadas con seguridad y privacidad de la Información realizadas por parte de los usuarios de la Entidad deberán realizarse a través de los formatos de solicitud o autorización definidos por la Dirección de TIC.

dd) Todos los funcionarios de la Entidad deberán utilizar los equipos de cómputo entregados por la Entidad para el desarrollo de sus actividades. En ningún momento se podrán utilizar equipos personales de funcionarios para conectarse a la red de la Entidad a excepción de aquellos que están definidos para las actividades de teletrabajo, trabajo en casa o trabajo remoto según corresponda.

ee) La sincronización del repositorio de almacenamiento (OneDrive) con aplicaciones de escritorio únicamente se permitirá en los equipos de escritorio o portátiles que son propiedad de TRANSMILENIO S. A.

7.2.5. Política de seguridad de la información con los proveedores

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

a. El supervisor del contrato y el contratista deben identificar los riesgos de seguridad de la información del contrato. De acuerdo con lo anterior, el análisis de riesgos de seguridad de la información debe incluir la identificación de los mismos en la respectiva contratación, su clasificación, probabilidad de ocurrencia estimada, su impacto, la determinación de la parte que debe asumirlos, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.

b. El supervisor del contrato debe identificar sí el objeto del contrato requiere del acceso de los proveedores a la información reservada o sensible de la entidad, sistemas de información o áreas seguras de la entidad; de ser así, se deben determinar los requisitos mínimos de seguridad y los controles necesarios por parte del proveedor para ejecutar dicho contrato.

c. En medio de la etapa contractual, se debe asegurar la inclusión de la cláusula de confidencialidad, protección de datos, derechos de propiedad intelectual, las políticas de seguridad y privacidad de la información y derechos de autor, en la suscripción y perfeccionamiento del contrato que se celebre entre la Entidad y aquellos proveedores que tendrán acceso a la información reservada o sensible de TRANSMILENIO S. A.

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

e. Como parte de la supervisión a la ejecución del contrato, se deben contemplar procesos de validación de controles de seguridad de la información a proveedores, cuyo objetivo es validar el cumplimiento de los requisitos de seguridad de la información asociadas al contrato. Dichos resultados deben quedar consignados en los informes presentados por el supervisor del contrato.

   El supervisor del contrato deberá realizar la solicitud de validación de seguridad de la información al grupo de seguridad de la información por lo menos una vez durante la ejecución del mismo y preferiblemente dentro de mes siguiente a la suscripción del acta de inicio. Con esta solicitud el grupo de seguridad de la información entregará al supervisor el instrumento de autodiagnóstico

para diligenciamiento por parte del proveedor, el cual será objeto de validación. Como resultado de la validación, el grupo de seguridad de la información determinará la eventual necesidad de realizar la auditoría.

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

g. Para los servicios de tecnología y de comunicaciones contratados externamente, es responsabilidad del supervisor del contrato exigir que los proveedores socialicen los requisitos y prácticas de seguridad de la Entidad, a lo largo de su cadena de suministro. Es decir, con sus contratistas, terceros y demás personal que tenga acceso a la información de la Entidad dentro del marco del contrato.

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

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

j. Los demás lineamientos deben aplicarse de acuerdo con el Manual de contratación M-DA-013 y con el Manual de supervisión e interventoría M-DA-015 establecidos por la entidad.

7.2.6. Política de privacidad y protección de datos personales

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

TRANSMILENIO S. A. en cumplimiento a lo establecido por las normas vigentes**:** Ley 1266 de 2008, Ley 1581 de 2012 y el Decreto 1377 de 2013, actúa como responsable de los datos personales que se encuentren en sus bases de datos y cada de una de las dependencias de la entidad actúa como encargado del tratamiento. Los lineamientos se seguirán acorde con lo establecido en el M-SC-006 Política de tratamiento y protección de datos personales.

7.2.7. Política de gestión de continuidad del negocio

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

Se debe dar cumplimiento de los siguientes lineamientos:

a. La entidad a través de la Oficina Asesora de Planeación debe liderar la definición e implementación del plan de continuidad del negocio de la Entidad.

b. La Entidad debe definir una política de continuidad del negocio que determine los requisitos para la seguridad de la información y la continuidad de la gestión de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.

c. La Dirección de TIC, debe elaborar el plan de recuperación de desastres, para cada uno de los servicios y sistemas de información críticos de la Entidad.

d. La Dirección de TIC, debe asegurar la ejecución de pruebas periódicas del plan de recuperación ante desastres, verificando la seguridad de la información durante su ejecución y la documentación de dichas pruebas.

e. La Dirección de TIC debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información, implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

f. La Dirección de TIC debe establecer, documentar y mantener procesos, procedimientos para asegurar el nivel de continuidad requerido para la Seguridad de la Información durante una situación adversa.

7.2.7.1. Redundancia

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

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

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

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

7.2.8. Política gestión de incidentes de seguridad

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

Se debe dar cumplimiento de los siguientes lineamientos:

a) TRANSMILENIO S. A., promoverá entre los empleados públicos, trabajadores oficiales, contratistas, proveedores y terceras partes, ante la existencia de una anomalía, evento o incidente de seguridad de la información (informáticos y no informáticos) en el cual se comprometa los recursos tecnológicos, sistemas de información, información física, demás medios en el que se encuentre información institucional y las personas, y que a su vez se afecte uno o todos los pilares fundamentales de seguridad como son: confidencialidad, integridad y disponibilidad de la información; ellos deberá reportar dicha novedad de manera inmediata, a través de los canales de comunicación oficiales definidos por la entidad.

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

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

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

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

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

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

h) La Entidad deberá realizar monitoreo frecuente de los eventos de seguridad detectados por las herramientas de tal forma que le permita desarrollar la inteligencia de amenazas y descubrimiento de nuevos tipos de ataque.

7.2.9. Política de cumplimiento

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

a. TRANSMILENIO S. A. implementará los procedimientos a que haya lugar para asegurar el cumplimiento de ley y requerimientos regulatorios y contractuales acerca de la propiedad intelectual, patentes, secretos de comercio y marcas.

b. El incumplimiento a la política de seguridad y privacidad de la información de TRANSMILENIO S. A., traerá consigo, las consecuencias legales que aplique a la normativa vigente de la entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la Información se refiere.

7.2.9.1. Sanciones para las violaciones de las políticas de seguridad de la información

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

7.3. Políticas de Seguridad del Personal

7.3.1. Política de teletrabajo

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

TRANSMILENIO S. A. establece los siguientes lineamientos, en el marco de la Ley 1221 de 2008 y la Resolución 420 de 2016 emitida por de la Entidad, por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones:

TRANSMILENIO S. A., como empleador debe:

- Autorizar la utilización de equipos personales a los teletrabajadores para la ejecución de sus funciones (cuando a ello haya lugar), en los cuales se deben implementar todas las medidas de seguridad definidas por la entidad.
- Facilitar los mecanismos para que los trabajadores conozcan los lineamientos impartidos a través de la presente política y con ello los riesgos que se derivan del uso de los equipos tecnológicos en el proceso de seguridad de la información de la entidad.
- Definir los tipos de usuarios que dispondrán de modalidad de teletrabajo y los permisos de acceso remoto pertinentes.
- Establecer procedimientos para la solicitud y autorización del teletrabajo.
- Establecer un procedimiento de conexión remota de emergencia para solventar problemas e incidencias puntuales.
- Establecer un compromiso por parte del teletrabajador (en el documento que defina la entidad), frente al cumplimiento de los lineamientos adoptados a través de la presente política, así como lo relacionado al uso exclusivo del equipo que se destine para la ejecución de sus funciones (según sea el caso), aceptando y cumpliendo para tales efectos con las medidas de seguridad de la información implementadas por la entidad.
- Definir los derechos y obligaciones de cada una de las partes que intervienen en el teletrabajo.
- Llevar un seguimiento de las conexiones remotas a los servicios corporativos de teletrabajo. Especialmente se debe prestar atención a los intentos de conexión sospechosos.

- Los teletrabajadores no deben almacenar en los equipos asignados o personales información sensible o reservada. En lo que respecta a la información que se encuentre contenida en medios digitales, los teletrabajadores están en la obligación de dar estricto cumplimiento, por sus propios medios, a los lineamientos de seguridad de la información establecidos por la entidad y que a continuación se relacionan:

  a) Si los equipos son personales, el teletrabajador debe instalar el sistema operativo desde una fuente fiable, mantener el sistema operativo y las aplicaciones actualizadas.

  b) Instalar un software de antivirus debidamente licenciado.

  c) Utilizar el control de acceso definido por la entidad con sus correspondientes permisos.

  d) Mantener configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc.), parametrizando el bloqueo automático por inactividad y en lo posible, utilizar un cifrado de disco.

- Los equipos portátiles no deben dejarse desatendidos, el Teletrabajador debe evitar transportar el equipo si no es necesario.
- Guardar bajo llave en el sitio o sitios en los que se ejecuten las funciones de teletrabajo, el dispositivo mientras no se utiliza.
- Manejar cuentas de usuario independientes o incluso el uso de sistemas operativos o máquinas virtuales separadas.
- No utilizar conexiones poco confiables (conexiones WiFi abiertas, redes públicas de hoteles, bibliotecas, locutorios, aeropuertos, entre otros) sin algún tipo de cifrado punto a punto como puede ser VPN o conexiones a sitios web protegidos con SSL (los que empiezan por HTTPS).
- Verificar que en el acceso a los servidores corporativos se utilicen certificados reconocidos y que la figura del “candado” de la conexión SSL no indique sobre la existencia de posibles de peligros o errores.
- Utilizar contraseñas seguras siguiendo los lineamientos de la Política de control de acceso de TRANSMILENIO S. A.
- Borrar el histórico de navegación, las cookies y otros datos del navegador web.
- Por políticas de seguridad de la Información, el Teletrabajador, no debe usar el cuadro de dialogo en el que se sugiera recordar contraseña.

- Al finalizar el trabajo, cerrar todas las conexiones con servidores y páginas web utilizando cuando sea posible la opción “desconectar” o “cerrar sesión”.
- Eliminar la información temporal alojada en carpeta de descargas, papelera de reciclaje, escritorio virtual u otras que se encuentren en diferentes carpetas del dispositivo.
- Solicitar a la mesa de ayuda de la entidad, cuando sea necesario, la aplicación de las herramientas de borrado seguro sobre la información institucional alojada en el dispositivo con el que se ejecuten las labores de teletrabajo, previa autorización cuando sea el caso.
- Asegurarse de retirar cualquier memoria USB, CD o DVD que se haya utilizado en el equipo.
- En lo que respecta a la información que se encuentre contenida en medios físicos, los teletrabajadores están en la obligación de dar estricto cumplimiento a los lineamientos de seguridad de la información establecidos por la entidad y que a continuación se relacionan: Almacenar los documentos bajo llave mientras no se estén utilizando.
- Llevar a cabo la destrucción de los documentos, para lo cual será necesario romperlo o triturarlo con el objeto de evitar que la pieza documental se arroje de manera completa al contenedor o papelera y sea reutilizada para labores domésticas que de alguna manera ponga en riesgo la información institucional.
- No dejar las copias impresas desatendidas en la bandeja de la impresora.
- No dejar los documentos en tránsito desentendidos en el lugar o lugares en los que se ejecutan las funciones de teletrabajo.

7.3.2. Política de confidencialidad

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

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

Todos los funcionarios, contratistas y clientes deben firmar la cláusula 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 o a los recursos de la Entidad a personas o entidades externas. Su aplicación se llevará a cabo en coordinación con la subgerencia jurídica de TRANSMILENIO S. A.

TRANSMILENIO S. A., firmará acuerdos de confidencialidad con los clientes y terceros o contratistas, que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Entidad. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

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

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

7.3.3. Política del recurso humano

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

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

Antes de la contratación

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

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

b) El Grupo de Talento Humano debe asegurar que los funcionarios de la Entidad firmen un acuerdo o cláusula de confidencialidad y de aceptación de políticas de seguridad de la información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

c) El personal provisto por terceras partes que realice labores en o para TRANSMILENIO S. A., debe firmar un acuerdo o cláusula de confidencialidad y de aceptación de políticas de seguridad de la información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

d) El personal provisto por terceras partes debe garantizar el cumplimiento de los acuerdos o cláusulas de confidencialidad y de aceptación de las políticas de seguridad de la Información de la Entidad.

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

Durante la ejecución del empleo:

Se debe asegurar que todos los empleados públicos, trabajadores oficiales, contratistas y terceras partes, tomen conciencia de sus responsabilidades de seguridad de la información, considerando el cumplimiento de los siguientes lineamientos:

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

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

c. El grupo de talento humano debe convocar a los funcionarios a las charlas y eventos programados como parte del desarrollo del plan de cultura y sensibilización en seguridad de la

información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas, aplicando las acciones pertinentes por la falta de asistencia no justificada.

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

e. El sistema de información de nómina vigente deberá generar una notificación con las novedades administrativas, vacaciones y licencias (remuneradas y no remuneradas), de los empleados públicos y trabajadores oficiales, previamente autorizadas por la Dirección Corporativa, a los administradores del control de acceso a las aplicaciones corporativas y la mesa de ayuda de la Entidad según sea el caso.

7.3.4. Política de cultura y sensibilización en seguridad de la información

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

Se debe dar cumplimiento de los siguientes lineamientos:

a) Se debe sensibilizar y divulgar a través de los medios establecidos por la entidad sobre la Seguridad de la Información, en donde a cada servidor público, contratista, proveedor y terceras partes deben participar activamente en los programas o planes de cultura y sensibilización en seguridad de la información desarrollados por la Dirección de TIC, y de acuerdo al contenido debe ser interiorizado y aplicado según corresponda su rol y responsabilidad dentro de la entidad.

b) Para realizar el contenido de los programas o planes de cultura y sensibilización de seguridad de la información deben enmarcarse en tres fases:

- **Diseño:** deben ser diseñados teniendo en cuenta la misión de la entidad, identificación de las necesidades y prioridades (verificación de Incidentes de Seguridad), elaboración de indicadores o métricas de desempeño que permitan generar resultados.
- **Desarrollo:** elaborar material de entrenamiento en el que se pueda emplear una buena pedagogía para la difusión de los temas de seguridad y este debe ser sometido aprobación por el comité institucional de gestión y desempeño , antes de la puesta en marcha.

- **Implementación:** socializar el programa o plan de cultura sensibilización de seguridad de la información de la entidad que fue diseñado y desarrollado al igual que emplear los indicadores o métricas para evaluar el desempeño del programa o plan.

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

7.4. Políticas de seguridad física

7.4.1. Política de áreas seguras

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

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.

7.4.1.1. Perímetro de seguridad física – controles físicos de entrada

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

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

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

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

d) Archivo físico de gestión: Hace referencia a aquella documentación todavía en trámite que conserva TRANSMILENIO S. A. así como a aquella que aun después de finalizado el procedimiento administrativo, está sometida a uso continuo y consulta administrativa, aplicando para ello lo dispuesto en las tablas de retención documental.

e) Centro de monitoreo de seguridad la Dirección Técnica de Seguridad: área utilizada por la dirección técnica de seguridad para el monitoreo de seguridad y cámaras de vigilancia.

f) Centro de control de BRT: Centro de monitoreo y control de flota troncal de la Entidad.

g) Centro de Control de Buses: Centro de monitoreo y control de flota zonal de la Entidad.

h) Archivo físico central: áreas en donde se administran, custodian y conservan los documentos físicos con valor administrativo, legal, permanente, histórico entre otros. Esta área segura, aunque resguarda información de la Entidad, corresponde a las instalaciones de un tercero que son administradas y gestionadas por este a través de contratos públicos.

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

- El perímetro de la construcción o sitio que contiene instalaciones de procesamiento de información debe ser físicamente sólido. Los muros externos del sitio deben ser de construcción sólida y todas las puertas externas deben estar protegidas contra el acceso no autorizado, ejemplo alarmas, cerraduras, etc.
- Debe definirse un área de recepción u otro medio para el control del acceso físico al sitio o edificio.
- Impedir que aquellas áreas cuyas ventanas den al exterior por su ubicación, permitan de alguna manera (al menos mínima) la visibilidad hacia el interior de la entidad.
- Implementar el uso de sistemas de control de acceso físico de proximidad en las áreas seguras.
- Los privilegios de acceso a las áreas seguras de TRANSMILENIO S. A. deben ser definidos por el director del área o por el personal que este asigne, encargada del área segura, para ello debe tener en cuenta los siguientes tipos de usuario:
  - Profesionales que trabajan regularmente en las áreas seguras.
  - Profesional de soporte que requiere acceso periódico.
  - Visitantes (empleados públicos, trabajadores oficiales contratistas, proveedores o terceras partes) que requieren acceder muy rara vez.

Teniendo en cuenta lo anterior, los únicos que deben tener privilegios de acceso permanente a las áreas seguras son los profesionales que trabajan regularmente en ellas. Los demás usuarios deben solicitar autorización para el acceso y portar un documento que demuestre su identidad. En este tipo

de casos, se debe asignar por parte del área responsable del área segura un profesional que acompañe y supervise la labor de dicho visitante, hasta su salida.

- El acceso al centro de datos está restringido y su ingreso es únicamente por medio de tarjeta de proximidad o biométrico.
- Para el ingreso de los visitantes a las áreas seguras se debe llevar una bitácora de ingreso donde se registre la información del personal que previamente haya sido autorizado por el funcionario correspondiente.
- Las actualizaciones a los derechos de acceso pueden ser efectuadas cuando ello así se requiera por parte de la Dirección Corporativa de TRANSMILENIO S. A. en consenso con la Dirección de TIC, para lo cual, si es del caso, se revocarán aquellos permisos que ya no sean necesarios.
- Deben mantenerse registros de auditoría de todos los accesos a las áreas restringidas. Estos registros podrán mantenerse dentro del software del control de acceso o en un repositorio centralizado para la recolección de logs.

7.4.1.2. Seguridad de oficinas, recintos e instalaciones

Con el propósito de mantener la confidencialidad, integridad y disponibilidad en la oficinas, recintos e instalaciones, es necesario establecer la guía de uso de este para empleados públicos, trabajadores oficiales, contratistas y terceras partes. Las directrices a este aspecto estarán a cargo de la Dirección Corporativa y quien se encargue de la seguridad física de TRANSMILENIO S. A. Se debe considerar el cumplimiento de los siguientes lineamientos:

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

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

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

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

e. 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.

f. Se deben utilizar circuitos cerrados de televisión (CCTV) para monitorear las actividades dentro o alrededor de las áreas seguras. Dicha labor está a cargo de la Dirección Corporativa de TRANSMILENIO S. A.

7.4.1.3. Protección contra amenazas externas y ambientales

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

a. La Dirección de TIC en conjunto con la Dirección Corporativa deben certificar que el centro de datos y los centros de cableado se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

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

7.4.1.4. Trabajo en áreas seguras

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

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

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

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

7.4.1.5. Monitoreo de la seguridad física

TRANSMILENIO S.A deberá realizar monitoreo periódico de la seguridad física del edificio principal con el fin de identificar eventos de acceso no autorizados y tomar de manera oportuna las acciones de mitigación.

7.4.2. Política de seguridad de los equipos

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

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

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

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

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

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

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

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

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

h. Se deberán proteger los equipos fuera de las instalaciones de la organización y su salida debe realizarse en el marco de lo establecido por la Dirección Corporativa.

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

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

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

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

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

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

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

p. No se permite la manipulación no autorizada de los equipos de la Entidad ni de sus componentes, tales como apertura, traslado, cambio de componentes, apagado o desconexión de cables a menos de que sea realizada por el personal de soporte técnico.

7.4.3. Política de escritorio y pantalla limpia

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

7.4.3.1. Escritorio limpio

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

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

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

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

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

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

7.4.3.2. Equipo informático de usuario desatendido

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

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

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

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

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

7.5. Políticas de seguridad tecnológica

7.5.1. Política para dispositivos móviles

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

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

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

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

7.5.2. Política de seguridad en las telecomunicaciones

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

7.5.2.1. Gestión de la seguridad en las redes

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

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

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

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

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

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

f) Se deben identificar e incluir en los acuerdos de niveles de servicio (ANS)os mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.

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

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

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

j) Se debe restringir la navegación a internet de los controladores de dominio únicamente a los servicios de actualización y parches.

k) Se deben aplicar restricciones de navegación adicionales para los equipos pertenecientes al personal de archivo y correspondencia, en lo relacionado con el acceso a correos electrónicos personales, redes sociales, WhatsApp Web y sitios de transferencia de información que puedan ser vector de fuga de información.

l) Los únicos equipos que pueden conectarse con cable a la red de la Entidad, son los equipos de escritorio o portátiles que sean propiedad de TRANSMILENIO S.A y que se encuentren vinculados dentro del dominio.

m) Cualquier equipo que no sea propiedad de TRANSMILENIO S. A., como por ejemplo equipos personales de funcionarios, contratistas u otros deberán conectarse únicamente a la red inalámbrica de tipo BYOD definida por la Dirección de TIC.

n) Las conexiones VPN tipo cliente, para el acceso a la red de la Entidad únicamente se crearán y asignarán a los funcionarios o contratistas responsables de efectuar labores de administración de la infraestructura tecnológica o soporte técnico de la misma, de manera remota. Estas conexiones se deberán solicitar a través de los formatos de autorización definidos por la Dirección de TIC. Los nombres de las VPN de cliente deberán incluir el nombre del funcionario o contratista responsable y no con solo nombres genéricos. No obstante, podrán existir excepciones para personal administrativo, según se autorice por la Dirección de TIC. La continuidad de las VPN se revisará al interior de la Dirección de TIC, con fin el de realizar la depuración correspondiente por lo menos una vez al año.

o) La navegación a internet deberá controlarse a través de reglas de filtrado de contenido que restrinjan categorías que no están relacionadas con el trabajo, tales como pornografía, hacking, abuso de drogas, entretenimiento, grupos extremistas, violencia implícita, discriminación, contenido ilegal o no ético, plagio, entre otras. De igual manera, si se requiere acceso a páginas

especiales por parte de alguna dependencia de la Entidad, esta se deberá solicitar a través de los formatos de autorización definidos por la Dirección de TIC.

p) Con el fin de evitar movimientos laterales, las redes de la Entidad implementarán restricciones de conexión entre VLAN de usuarios y también conexiones entre equipos dentro de la misma VLAN. Los únicos permisos de red que se habilitarán son la navegación a internet y la conexión con los servidores de la Entidad, siendo este último solo permitido para los equipos propiedad de TRANSMILENIO conectados por cable.

q) No está permitida la conexión a los servidores de la Entidad a través de la red inalámbrica. El acceso al directorio activo, servicios de almacenamiento y aplicaciones internas solo se podrá brindar a los equipos propiedad de TRANSMILENIO S. A. que se encuentran conectados a través de la red cableada.

7.5.3. Política sobre el uso de controles criptográficos

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

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

Se debe dar cumplimiento de los siguientes lineamientos:

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

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

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

d. Quienes ejecuten el rol de Administrador deben documentar los pasos necesarios para el registro, generación, distribución, almacenamiento, recuperación, renovación, revocación y

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

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

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

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

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

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

j. Los funcionarios que tengan asignada una firma digital deberán usarla siempre que se requiera firmar una comunicación oficial.

7.5.4. Política de desarrollo seguro

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

7.5.4.1. Confidencialidad

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

- Se deben definir y documentar las reglas para la transferencia de software del ambiente de pruebas al ambiente de producción.
- Los cambios en los sistemas operativos y aplicaciones se deben poner a prueba en un entorno de pruebas antes de aplicarlos a los ambientes de producción.

- Las pruebas no se deben llevar a cabo en el ambiente de producción.
- Los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no deben ser accesibles desde los ambientes de producción cuando no se requiera.
- Los usuarios deben usar diferentes perfiles de usuario para los ambientes de producción y los ambientes de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error.

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

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

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

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

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

f. Se deben definir y aplicar reglas de enmascaramiento de los datos para la información almacenadas en bases de datos de los sistemas de información, de tal forma que no pueda se accedida o visualizada de forma no autorizada. El enmascaramiento se debe definir de acuerdo con la clasificación de la información.

7.5.4.2. Ciclo de vida del software - SDLC

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

a. Análisis de requerimientos.

b. Análisis arquitectónico.

c. Tipo de desarrollo (propio o a terceros).

d. Pruebas (funcionales, no funcionales y de seguridad).

e. Producción.

f. Mantenimiento.

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

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

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

7.5.4.3. Migración a ambiente de producción

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

producción. Para poder recibir un software en el ambiente de Producción se debe tener en cuenta las siguientes condiciones:

a) Tipo y clasificación de la información que maneja.

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

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

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

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

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

g) Manual de diseño.

7.5.4.4. Cifrado de datos sensibles

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

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

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

7.5.4.5. Integridad

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

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

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

7.5.5. Política de copias de respaldo

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

Se debe dar cumplimiento de los siguientes lineamientos:

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

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

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

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

e) Quienes ejecuten el rol de administrador de backup debe validar el resultado de la ejecución de las copias de seguridad y registrar las novedades que se presenten en el proceso.

f) Es responsabilidad de quienes ejecuten el rol de Administrador de backup realizar pruebas de restauración de copias de seguridad por lo menos dos veces al año, siguiendo los lineamientos del procedimiento backup y recuperación de la información P-DT-019 Procedimiento para realizar copias de respaldo y restauración de información.

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

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

i) Toda la información generada, procesada y almacenada por los sistemas de información y aplicaciones de la Entidad, así como por los equipos asignados a los funcionarios y contratistas es propiedad de TRANSMILENIO S. A. Por lo tanto, los archivos de backup generados sobre esta información solo podrán ser solicitados y consultados por funcionarios y contratistas activos con previa autorización de la Dirección de TIC. Ningún archivo de backup o copia de respaldo podrá entregarse a terceros que no hagan parte de la Entidad.

7.5.6. Política de seguridad en la nube

Objetivo: definir las directrices para garantizar que se apliquen medidas de seguridad sobre la infraestructura que TRANSMILENIO S. A. tiene actualmente desplegada en la nube.

Se debe dar cumplimiento de los siguientes lineamientos:

a) TRANSMILENIO S. A. debe aplicar un proceso de identificación, análisis, evaluación y valoración de riesgos de seguridad para los servicios de la Entidad que se encuentren contratados en la nube.

b) Se debe monitorear la seguridad de los servicios de nube que la Entidad tenga contratados.

c) La información clasificada, reservada, pública clasificada e información de carácter personal que se almacene o procese en la infraestructura de la Nube debe permanecer cifrada para evitar su divulgación o acceso no autorizado.

d) El uso de los servicios de computación en la nube dentro de la Entidad debe ser exclusivo para el cumplimiento de las funciones de las labores dentro de la Entidad, no está autorizado el uso de servicios de computación en la nube para fines personales.

e) En los contratos celebrados en Colombia con proveedores de servicios de computación en la nube, se debe incluir el cumplimiento de las políticas de seguridad de la información de la Entidad, el cumplimiento de los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual vigentes sobre la información, leyes y regulaciones sobre la protección de la información de la Entidad e información de carácter personal.

f) Los servicios de computo en la nube deben cumplir con los procedimientos de capacidad, disponibilidad, cambios y backup de la Entidad.

g) Los usuarios de administración de la plataforma deben mantener en estricta confidencialidad las contraseñas para acceso a los servicios de computación en la nube y el acceso a la plataforma debe ser con doble factor de autenticación.

h) El aprovisionamiento de servicios en la nube de la Entidad deberá ser aprobado por la Dirección de TIC a través de los formatos de solicitud o autorización definidos.

8. EXCEPCIONES EN LAS POLÍTICAS

Las excepciones sobre las políticas son aquellas que se encuentren dentro del marco de la ley colombiana. Sin embargo, cualquier excepción específica o particular que se genere sobre las políticas debe ser autorizada por el Director de TIC o Profesional Especializado Grado 06 - Seguridad Informática o quien desempeñe el rol de líder u oficial de seguridad de la información de la Entidad.

Por lo anterior, las excepciones asociadas a las políticas de seguridad de la información se registran por parte del grupo de seguridad de la información, en un documento de excepciones, el cual está clasificado como confidencial y es actualizado por la Dirección de TIC a medida que se considere pertinente. Dicho documento se encuentra ubicado en el repositorio del grupo de seguridad de la información de la Dirección de TIC.

9. REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

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

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

b. En las revisiones periódicas se deben tener en cuenta factores como: Prioridades del negocio, costos e impacto de los controles sobre la eficiencia del negocio, incidentes de seguridad, nuevas

vulnerabilidades detectadas, Cambios en los requerimientos regulatorios y /o legales, cambios en la infraestructura tecnológica u organizacional, cambios en los objetivos del sistema o de la organización, entre otros.