



| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACIÓN ELECTRÓNICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |



TABLA DE CONTENIDO

1. OBJETO
2. ALCANCE
3. RESPONSABLES
4. DOCUMENTOS DE REFERENCIA
5. DEFINICIONES
6. CONDICIONES GENERALES
 - 6.1 Política de intercambio de información con partes externas
 - 6.1.1. Transferencia de Información
 - 6.1.2 Políticas y procedimientos de transferencia de información
 - 6.1.3 Acuerdos sobre transferencia de información
 - 6.1.4 Mensajes electrónicos
 - 6.1.5 Acuerdos de confidencialidad o de no divulgación
7. DESCRIPCIÓN DE ACTIVIDADES
8. TABLA DE FORMATOS

MODIFICACIONES:

| VERSION | FECHA | CAMBIO | SOLICITO |
|---------|------------|--|-------------------|
| 0 | 01-12-2015 | Primera versión Oficial del documento | N/A |
| 1 | 26-03-2019 | Se realizaron los siguientes ajustes: <ul style="list-style-type: none"> • Revisión y actualización de los documentos de referencia • Roles y nombres de cargos. • Cambio en nombre de normas ISO 27001 e ISO 27002 dado que ya no se requiere el prefijo "BS" • Eliminación de política relacionada con medios removibles puesto que ya existe en el documento de Políticas de seguridad y privacidad de la información de TRANSMILENIO S.A. • Ajuste del nombre del formato R-DT-008. | Director de TIC's |

| | | |
|--|--|-----------------------|
| ELABORÓ: PROFESIONAL ESPECIALIZADO GRADO 06 - SEGURIDAD INFORMATICA | APROBÓ: DIRECTOR DE TIC'S | Página 1 de 19 |
|--|--|-----------------------|

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

1. OBJETO

Determinar las políticas, responsables y las actividades necesarias para que el intercambio de información se efectúe en forma segura contando y aplicando los pilares de confidencialidad, integridad y disponibilidad de la información en TRASMILENIO S.A.

2. ALCANCE

Todas las Dependencias, funcionarios, contratistas que desarrollen labores de asesoría, consultoría, implementación, soporte o mantenimiento y demás personas que sin ser de planta, tienen un nivel de vinculación o brindan algún tipo de servicio dentro los procesos y dependencias de las instalaciones de TRANSMILENIO S.A., que en cumplimiento de la misión de la entidad, tengan cualquier tipo de interacción con la información y medios de procesamiento (sistemas de información o aplicativos).

3. RESPONSABLES



El responsable por la elaboración, mantenimiento, implementación y cumplimiento de este documento es el Profesional Especializado Grado 06 de Seguridad de la Información de la Dirección de TIC's.

Por los niveles de cumplimiento e implementación del procedimiento velará el Director de Tecnologías de la Información y las Comunicaciones.

Por el desarrollo, ejecución y monitoreo del procedimiento será responsable el área de Soporte de la Dirección de TIC's.

Por su aplicación, todos los usuarios funcionales que interactúen directa o indirectamente en el intercambio de la información electrónica de TRASMILENIO S.A.

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



| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

4. DOCUMENTOS DE REFERENCIA



- **Constitución Política de Colombia de 1991**

| | |
|---------------|--|
| Artículo 2. | Fines Esenciales del Estado. |
| Artículo 6. | Responsabilidad de los servidores públicos. |
| Artículo 15. | Derecho a la Intimidad. Hábeas Data. |
| Artículo 20. | Derecho a la Información. |
| Artículo 74. | Libre Acceso a Documentos Públicos. |
| Artículo 122. | Desempeño de Funciones Públicas. |
| Artículo 123. | Desempeño de funciones de los Servidores Públicos. |
| Artículo 209. | Fines de la Función Administrativa. |
| Artículo 269. | Métodos y Procedimientos de Control Interno. |
| Artículo 284. | Acceso a Información Reservada. |

- **Ley 1273 de 2009:** por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, el cual establece en su “Capítulo I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” así:
 - Artículo 269A: Acceso abusivo a un Sistema Informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático
 - Artículo 269B: Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático.
 - Artículo 269C: Interceptación de Datos Informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático.
 - Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos.
 - Artículo 269E: Uso de Software Malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

- Artículo 269F: Violación de Datos Personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes
- Artículo 269G: Suplantación de Sitios Web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.
- **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, se establecen las entidades de certificación y se dictan otras disposiciones
- **Ley 603 del 2000:** ley emitida por el Congreso de la República de Colombia, acerca del cumplimiento de las Normas de Propiedad Intelectual
- **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 1266 de 2008:** por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **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 1520 de 2012:** por medio de la cual se implementan compromisos adquiridos por virtud del "Acuerdo de Promoción Comercial", suscrito entre la República de Colombia y los Estados Unidos de América y su "Protocolo Modificatorio, en el Marco de la Política de Comercio Exterior e Integración Económica"
- **Ley 1581 de 2012:** por la cual se dictan disposiciones generales para la protección de datos personales, habeas data
- **Decreto 1360 de 1989:** por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

- **Decreto 460 de 1995:** por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal
- **Decreto 162 de 1995:** por el cual se reglamenta en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos
- **ISO/IEC 27001:2013** Norma técnica que describe los requerimientos del Sistema de Seguridad de la Información (*Information technology - Security techniques - Information security management systems - Requirements*) aprobado y publicado por la ISO International Organization for Standardization y por la IEC International Electrotechnical Commission.
- **ISO/IEC 27002:2013** Documento que recopila el código de práctica y los controles para la gestión de la seguridad de la información (*Information technology - Security techniques - Code of practice for information security management*) aprobado y publicado por la ISO International Organization for Standardization y por la IEC International Electrotechnical Commission.
- **Reglamento Interno de trabajo de TRANSMILENIO S.A.** documento que se establece como norma reguladora de las relaciones internas de la Entidad con los trabajadores adscritos a ella.

5. DEFINICIONES

Activo: cualquier cosa que tiene valor para la Entidad.

Aplicativos: software, programa informático diseñado como herramienta.



Autenticidad: propiedad de garantizar la identidad de un sujeto o recurso declarado. Se aplica a entidades tales como usuarios, procesos, sistemas e información.

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

Bases de datos: es un “almacén” que nos permite guardar grandes cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente. Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

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

Datos: es un elemento aislado, recabado para un cierto fin, pero que no ha pasado por un proceso que lo interrelacione con otros de manera funcional para el fin previsto.

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

Disponibilidad: es la propiedad de la información de ser accesible y utilizable por solicitud de una Entidad o funcionarios autorizados.

Firewall: es un ordenador, 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, autenticación, etc., conforme a las políticas de seguridad.

Formularios electrónicos: herramienta que permite la identificación de información, estructura y diseño de los formularios web a presentar en el portal del Usuario final. Dicha configuración se almacena en el repositorio de datos de uso los cuales tratan y gestionan la inclusión y configuración de diversos componentes, como por ejemplo bloques, secciones, objetos de formulario, etc.

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: causa potencial que puede producir daño a un sistema o la Entidad.

Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.



Integridad: es la propiedad de salvaguardar la exactitud y estado completo de los activos.

Intranet: red privada de computadoras que permite compartir recursos entre ellas y se encuentra enlazada. Puede o no tener acceso a Internet.

ISO (International Organization for Standardization): deriva del griego ISOS, que significa "igual"; Organización creada el 23 de Febrero de 1947, en Ginebra, Suiza, con el fin de "facilitar la coordinación internacional y unificación de normas industriales". Actualmente son miembros 165 países.

Políticas: actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos. Acción elegida como guía en el proceso de toma de decisiones al poner en práctica o ejecutar las estrategias, programas y proyectos específicos del nivel institucional.

Riesgo: potencial de que una amenaza determinada aproveche las vulnerabilidades de una activo o grupo de activos y produzca daño a la Entidad. Se mide en términos de la combinación de la probabilidad de un evento y sus consecuencias.

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

Seguridad informática: consiste en preservar la confidencialidad, integridad y disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Sistema de gestión de la seguridad de la información - SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Terceros: personal que pertenece a empresas que proveen servicios a TRASMILENIO S.A.

TICs (Tecnologías de la Información y las Comunicaciones): es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. Dentro de sus funciones está incrementar y facilitar el acceso de los usuarios de la Entidad a las Tecnologías de la Información, las Comunicaciones y a sus beneficios.

Usuarios: Funcionarios, empleados contratados, consultores y contratistas.

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.

6. CONDICIONES GENERALES

TRASMILENIO S.A., asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán acuerdos de confidencialidad y/o de intercambio de información con las terceras partes con quienes se realice dicho intercambio. La Dirección TIC's propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo dicho proceso; sin embargo, establecerá directrices para el intercambio de información en medio físico.

Aplica para todos los medios de intercambio de información que la Entidad emplee, así como:

- El correcto uso de los medios.

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

- Controles para evitar la modificación, la interceptación, el copiado o la destrucción de la información.
- Controles de protección contra el código malicioso.
- Técnicas de ingeniería social.
- Uso de cifrado en datos que se consideren necesarios.

6.1 Política Intercambio de Información con partes externas¹

TRASMILENIO S.A., entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

6.1.1. Transferencia de Información²

Objetivo: TRASMILENIO S.A. debe mantener la seguridad de la información transferida dentro de la organización y con cualquier entidad externa.

6.1.2 Políticas y procedimientos de transferencia de información³

TRASMILENIO S.A. debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante todo tipo de instalaciones de comunicaciones.

6.1.3 Acuerdos sobre transferencia de información⁴



Los acuerdos de TRASMILENIO S.A. deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.

¹ ISO/IEC 27001:2013 Clausula A.13.2

² ISO/IEC 27001:2013 Clausula A.13.2.1

³ ISO/IEC 27001:2013 Clausula A.13.2.2

⁴ ISO/IEC 27001:2013 Clausula A.13.2.3

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

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 las cuales se establecen convenios o nexos de diferente naturaleza y que involucran de alguna forma el intercambio de información.

Para establecer dicha transmisión se debe consultar el concepto técnico de la Dirección de TIC’s de TRANSMILENIO S.A. a través del Profesional Especializado Grado 06 Seguridad Informática, quien coordinará la verificación de los requerimientos para el proceso de transmisión. También se debe privilegiar este mecanismo o similares técnicamente, cuando el intercambio de información se produzca con otros Organismos Nacionales con los que exista intercambio regular de información. La información a intercambiar debe estar previamente definida y formalizada a través de una petición institucional.

Para acceso a sitios web se debe implementar herramientas de seguridad perimetral seguros (firewalls)

Para acceso a portales institucionales se debe realizar asegurándose que sean implementados desarrollos seguros.

6.1.4 Mensajes electrónicos⁵



Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.

Para dar un uso adecuado a la mensajería electrónica, se deberán observar los siguientes lineamientos:



Correo Electrónico

TRANSMILENIO S.A asigna una cuenta de correo electrónico como herramienta de trabajo para cada uno de los funcionarios que lo requieran para el desempeño de sus funciones y en algunos casos a terceros previa autorización; su uso se encuentra sujeto a las siguientes políticas:

⁵ ISO/IEC 27001:2013 Clausula A.13.2.4

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |



- a) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de TRASMILENIO S.A.
- b) Los mensajes y la información contenida en los buzones de correo son de propiedad de TRASMILENIO S.A y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- c) El tamaño de los buzones de correo está determinado por la Dirección de TIC's de acuerdo con las necesidades de cada usuario y previa autorización del Jefe Inmediato de cada Dirección o Dependencia.
- d) No se permite:
 - i) Enviar o recibir mensajes con un tamaño superior al autorizado y configurado entre cuentas de correo corporativas.
 - ii) Enviar o recibir mensajes con un tamaño superior al autorizado y configurado entre una cuenta de correo corporativa y una externa.
 - iii) 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.
 - iv) 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's de TRASMILENIO S.A.
 - v) No se podrá enviar información clasificada como Restringida sin la autorización previa de la Dirección de TIC's de TRASMILENIO S.A.
 - vi) Se prohíbe el uso de correo en cadena o mensajes enviados a un número de destinatarios para que estos a la vez se reenvíen a otros, enviado a un gran número de receptores sin un propósito relacionado con la misión de la TRASMILENIO 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.

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

- vii) No se debe alterar la línea "De" (autor del correo) u otra información relacionada con los atributos de origen del correo electrónico.
- viii) No se permite el envío de mensajes anónimos y la gestión con este tipo de mensajes está prohibida.
- e) El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la Dirección de TIC's de TRASMILENIO S.A. y deberá incluir un mensaje que le indique al destinatario cómo ser eliminado de la lista de distribución.
- f) Toda información de TRASMILENIO 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.
- g) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la Dirección de TIC's de TRASMILENIO S.A. y deben conservar en todos los casos el mensaje legal institucional de confidencialidad.
- h) Todo correo electrónico que deba ser transmitido hacia Internet, deberá tener al final del mensaje el siguiente texto:

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

This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message. Any disclosure, copying, or distribution of this message, or the taking of any action based on it, is strictly prohibited.
- i) La información enviada por correo electrónico, clasificada como confidencial, debe ser protegida con contraseña de acceso o cifrado según corresponda.



| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

- j) Se prohíbe el envío de mensajes no solicitados para el desarrollo de la misión de la Entidad, incluyendo el envío de “correo basura”, mensajes cadena u otro material de publicidad a personas que específicamente no lo hayan solicitado (por ejemplo, “inundación con mensajes de e-mail” o “spam”) y que se materialicen en la queja reiterada del receptor, harán presumir los mensajes como “no solicitados”, así como su requerimiento expreso de no continuar recibiendo dicho material.

Se incluye, sin limitación, el envío de masivos de publicidad comercial, anuncios informativos y comunicaciones políticas. También se incluye la publicación de un mismo mensaje o similar en uno o más grupos de noticias (exceso de publicación cruzada o múltiple publicación).

- k) 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.
- l) Se prohíbe al usuario además, hospedar sitios que sean publicitados por medio de mensajes de correo electrónico no solicitados o bien sitio 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.
- m) Se encuentra prohibido el mantenimiento de cualquier red de servicios que permita, sin restricciones, el envío de mensajes o correos electrónicos por terceras personas. 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.
- n) Comunicar, publicar, circular, enviar o allegar a Instancias o Entidades diferentes a aquellas que lo requieren información que en la Entidad se considera confidencial o de uso interno exclusivamente.



TRANSMILENIO S.A. se reserva el derecho de monitorear y supervisar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en esta Política y la legislación vigente.

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

Internet

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

- a) No se permite:
 - i) Navegación en sitios de contenido pornográfico, basado en sentimientos de odio o segregación, de delincuencia computacional (hackers o crackers) o cualquier otro sitio que la Dirección de TIC's considere fuera de los límites permitidos.
 - ii) Publicación, envío o adquisición de material sexualmente explícito u orientado, basado en sentimientos de odio o segregación, de delincuencia computacional o de cualquier otro contenido que la Dirección de TIC's considere fuera de los límites permitidos.
 - iii) Publicación o envío de información confidencial hacia fuera de la Dirección de TIC's sin la autorización de los dueños respectivos.
 - iv) Utilización de otros servicios disponibles e inseguros a través de Internet, como por ejemplo FTP y Telnet.
 - v) Publicación de anuncios comerciales o material publicitario.
 - vi) Promover o mantener asuntos o negocios personales.
 - vii) Recepción de noticias o actualización de datos, a menos que el material sea requerido para actividades de TRASMILENIO S.A.
 - viii) Utilización de programas de aplicación o software no relacionados con la actividad laboral y que ocupen excesivamente el tiempo de procesamiento de la estación de trabajo o de la red, por ejemplo aplicaciones que se ejecutan mientras está activo el protector de pantalla.
- b) La Dirección de TIC's realiza monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.
- c) Cada uno de los usuarios es responsable de dar un uso adecuado de este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, entre otros.
- d) Los funcionarios, contratistas de éstos, no pueden asumir en nombre de TRASMILENIO S.A., posiciones personales en encuestas de opinión, foros u otros medios similares.



| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

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

Recursos Tecnológicos

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

- a) La instalación de cualquier tipo de software en los equipos de cómputo de TRASMILENIO S.A., es responsabilidad de la Dirección de TIC's y por tanto son los únicos autorizados para realizar o autorizar esta labor.
- b) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla definido por la Organización. Estos cambios pueden ser realizados únicamente por la Dirección de TIC's y el personal que presta sus servicios a TRASMILENIO S.A.
- c) La Dirección de TIC's, define e informa la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realiza el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
- d) Únicamente los usuarios autorizados por la Dirección de TIC's y previa solicitud por parte del jefe inmediato, pueden conectarse a la red inalámbrica de TRASMILENIO SA.
- e) Los equipos de cómputo deberán ser bloqueados por los funcionarios cada vez que se retiren del lugar de trabajo.
- f) La Dirección de TIC's, 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.
- g) Los funcionarios no deben realizar cambios en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física y además, sólo podrán ser realizados por la Dirección de TIC's

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

El acceso a dispositivos removibles como CDs, DVDs, USBs, entre otros, se encuentra restringido. Sin embargo, la Dirección de TIC's manejará la posibilidad de conceder excepciones para el uso de estos dispositivos de acuerdo a las siguientes políticas:

- La Dirección de TIC's podrá aprobar conjuntamente aquellas excepciones que considere en beneficio de TRASMILENIO S.A.

NOTA: Esta es una aprobación que realiza un grupo de personas dependiendo del rol o la aplicación que pueda verse afectada

- El personal responsable de la Seguridad de Información, Tecnología de Información y Auditoría de Sistemas de la Dirección de TIC's, podrá estar eximido, previa autorización escrita de la dirección correspondiente, de las prohibiciones a las que estará sujeto el resto del personal, siempre y cuando sea para beneficio del desarrollo de sus responsabilidades y de las actividades de TRASMILENIO S.A.

De otra forma, para el uso de medios removibles, todos los usuarios deberán seguir el Protocolo T-DT-003 Protocolo a seguir para gestionar el uso de los medios removibles.

6.1.5 Acuerdos de confidencialidad o de no divulgación.⁶



Todos los funcionarios, contratistas y clientes deben firmar la cláusula y/o acuerdo de confidencialidad definido por TRASMILENIO S.A. y este deberá ser parte integral de cada uno de los contratos.

Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de la Entidad a personas o entidades externas.

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

Todos los funcionarios y contratistas de TRASMILENIO S.A. son responsables por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes

⁶ ISO/IEC 27001:2013 Clausula A.13.2.44

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.



Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de esta y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad requeridos.

Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

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

Si es aplicable para cada uno de los contratos, el acuerdo de confidencialidad deberá incluir aspectos como:

- a) Duración del acuerdo.
- b) Definición de la información que deberá ser protegida.
- c) Definición de responsabilidades de cada una de las partes para evitar que se presente divulgación de la información.
- d) Asignación de permiso para que el tercero o contratista haga uso de la información que para TRASMILENIO S.A., es sensible o crítica.
- e) Definición del propietario de la información que el tercero o contratista va a manipular.
- f) Inclusión de aspectos como secretos de mercado.
- g) Inclusión de aspectos como propiedad intelectual, derechos de autor relacionados con desarrollos de software, licencias, manuales, etc.
- h) Definición de las responsabilidades de cada una de las partes, mientras la información se encuentra fuera de las instalaciones de TRASMILENIO S.A. o del tercero.

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |



- i) Inclusión del derecho a auditar y monitorear actividades que involucren información sensible o crítica, en aquellos casos que aplique y sea esencial.
- j) Definición de acciones a tomar si el acuerdo se incumple.
- k) Definición de términos de tiempo en que la información manejada por el tercero debe ser devuelta cuando el contrato se finalice.




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



7. DESCRIPCIÓN DE ACTIVIDADES

El siguiente procedimiento abarca las etapas del ciclo de INTERCAMBIO DE INFORMACIÓN a los usuarios y terceros de todos los niveles que tengan acceso a la información y sistemas de TRASMILENIO S.A.

| ETAPA | ACTIVIDAD | RESPONSABLE |
|-------|---|---|
| 10 | INICIO | |
| 20 | <p>Aplicar la política y actividades necesarias para el intercambio seguro de la información electrónica al interior de la Entidad y con otras Entidades, descritas en este documento</p> <p>En caso de requerirse, debe utilizarse el formato: R-DT-008 Autorización de Uso y Acceso a Redes, Aplicaciones y Herramientas</p> | <p>Profesional Especializado Grado 06 Seguridad Informática</p> |
| 30 | <p>Monitorear el cumplimiento de las políticas y actividades necesarias para el intercambio seguro de la información electrónica al interior de la Entidad y con otras Entidades. Este monitoreo podrá realizarse a través de auditorías por demanda, pruebas de vulnerabilidad y hacking ético, así como pruebas de ingeniería social, entre otras técnicas de verificación.</p> | <p>Profesional Especializado Grado 06 Seguridad Informática</p> |

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

| ETAPA | ACTIVIDAD | RESPONSABLE |
|--|---|--|
| ¿15?  | ¿Se cumplen las políticas y actividades para el intercambio seguro de la información electrónica al interior de la Entidad y con otras Entidades? Si: ir a etapa 40 No: ir a etapa 20 | Profesional Especializado Grado 06 Seguridad Informática |
| 40 | Generar un plan de revisión periódico de la política y actividades de intercambio seguro de la información electrónica al interior de TRANSMILENIO S.A. y con otras Entidades. | Profesional Especializado Grado 06 Seguridad Informática |
| 50 | Formular acciones preventivas, correctivas o de mejora para el intercambio seguro de la información electrónica al interior de TRANSMILENIO S.A. y con otras Entidades y generar una bitácora que permita llevar un registro de los eventos presentados. | Responsable del proceso |
| ¿25?  | ¿Aprobar las acciones preventivas, correctivas o de mejora propuestas? Si: ir a etapa 60 No: ir a etapa 35 | Director de TIC's |
| 60 | Implementar actividades y surtir las acciones correctivas, preventivas y de mejora necesarias para el cumplimiento de las políticas y actividades. En caso de requerirse, debe utilizarse el formato: R-DT-008 Autorización de Uso y Acceso a Redes, Aplicaciones y Herramientas | Responsable del proceso |
| ¿35?  | ¿Se identificaron eventos o incidentes de seguridad? Si: ir a etapa 70 No: ir a etapa 80 | Profesional Especializado Grado 06 Seguridad Informática |
| 70 | Aplicar la política de gestión de incidentes que se encuentra descrita dentro del M-DT-001 Manual de Políticas de Seguridad y Privacidad de la Información. | Profesional Especializado Grado 06 Seguridad Informática |
| 80 | FIN | |

| | | | | |
|---|--|-----------------------------|---------------------------------------|--|
|  | TÍTULO: PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACION ELECTRONICA | | |  ALCALDÍA MAYOR DE BOGOTÁ |
| | Código: P-DT-012 | Versión: 1 | Fecha: Abril de 2019 | |

8. TABLA DE FORMATOS

| CÓDIGO | NOMBRE | UBICACIÓN | RESPONSABLE |
|----------|---|-----------|---|
| R-DT-008 | Autorización de Uso y Acceso a Redes, Aplicaciones y Herramientas | Intranet | Profesional Especializado Grado 06 - Seguridad de la Información |

COPIA NO CONTROLADA