AÑO 50
NÚMERO 5750
2016 · ENERO · 7

REGISTRO DISTRITAL

DECRETOS DE 2016

ALCALDÍA MAYOR DE BOGOTÁ D.C.

Decreto Número 013
(Enero 4 de 2016)

"Por el cual se designan los miembros que representan al Distrito Capital en la Junta Administradora Regional de la Sociedad Canal Capital Ltda.".

EL ALCALDE MAYOR DE BOGOTÁ, D.C.
En ejercicio de sus atribuciones legales y de conformidad con lo dispuesto en los estatutos de la Sociedad Canal Capital Ltda., y,

CONSIDERANDO:

Que Canal Capital Ltda. es una sociedad entre entidades públicas, organizada como empresa industrial y comercial del Estado, con carácter de entidad descentralizada indirecta y constituida bajo las leyes colombianas.

Que de conformidad con lo dispuesto en el Acuerdo Distrital 257 de 2006 *"Por el cual se dictan normas básicas sobre la estructura, organización y funcionamiento de los organismos y de las entidades de Bogotá, Distrito Capital, y se expiden otras disposiciones"*, la Sociedad Canal Capital Ltda., pertenece, como entidad vinculada, al Sector Cultura, Recreación y Deporte.

Que de conformidad con el Acuerdo 005 de 2010, por medio del cual se adoptan los estatutos de la Sociedad Canal Capital Ltda., su Junta Administradora Regional estará integrada por 8 miembros principales con sus respectivos suplentes, de los cuales (5) miembros con sus suplentes representarán al Distrito Capital.

Que de conformidad con lo establecido en el inciso 2°, del numeral 1°, del artículo 10 de los referidos Estatutos, la designación de los miembros con sus respectivos suplentes, que representarán al Distrito Capital, será efectuada por el Alcalde Mayor de Bogotá, mediante acto administrativo que así lo disponga.

Que en mérito de lo anterior,

DECRETA:

ARTÍCULO 1°. Los miembros principales y suplentes de la Junta Administradora Regional de la Sociedad Canal Capital Ltda., en representación del Distrito Capital de delegación del Alcalde Mayor, son:

* El Alcalde Mayor quien la presidirá o su suplente que será el/la Secretario/a Privado/a.
* El/la Secretario/a Distrital de Hacienda o su suplente que será el/la Subsecretario/a General.
* El/la Secretario/a Distrital de Educación o su suplente que será el/la Jefe/a de la Oficina Asesora de Comunicaciones y Prensa.
* El/la Secretario/a Distrital de Cultura, Recreación y Deporte o su suplente que será el/1a Subsecretario/a General y de Control Interno Disciplinario.
* El/la Secretario/a Distrital de Desarrollo Económico o su suplente que será el/la Subsecretario/a de Desarrollo Económico y Control.

ARTÍCULO 2°. Los miembros que representen al Instituto Distrital para la Recreación y el Deporte, serán designados por la citada entidad descentralizada.

ARTÍCULO 3°.- El presente Decreto rige a partir de la fecha de su expedición y deroga las disposiciones que le sean contrarias, en especial el Decreto Distrital 539 de 2007.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dado en Bogotá, D.C., a los cuatro (4) días del mes de enero de dos mil dieciséis (2016).

ENRIQUE PEÑALOSA LONDOÑO
Alcalde Mayor

Decreto Número 020
(Enero 5 de 2016)

"Por medio del cual se hace un nombramiento".

EL ALCALDE MAYOR DE BOGOTÁ, D.C.
En uso de sus facultades legales, en especial las conferidas por el Decreto Ley 1421 de 1993, el Decreto 1083 de 2015

DECRETA:

ARTÍCULO 1°.- Nombrar a partir de la fecha, a la doctora ADRIANA MARCELA GUTIÉRREZ CASTAÑEDA, identificada con la cédula de ciudadanía Nro. 39.573.449, en el cargo de Directora General de Entidad Descentralizada Código 050 Grado 02 del Instituto Distrital de Turismo - IDT.

ARTÍCULO 2°.- Notificar a la doctora ADRIANA MARCELA GUTIÉRREZ CASTAÑEDA, el contenido del presente Decreto, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 3°.- Comunicar al Instituto Distrital de Turismo - IDT y a la Subdirección de Talento Humano de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., el contenido del presente Decreto, a través de la Subdirección de Gestión Documental de la misma Secretaría.

ARTÍCULO 4°.- El presente Decreto rige a partir de la fecha de su expedición.

NOTIFÍQUESE, COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE.

Dado en Bogotá, D.C., a los cinco (5) días del mes de enero de dos mil dieciséis (2016).

ENRIQUE PEÑALOSA LONDOÑO
Alcalde Mayor

RESOLUCIONES

SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, D.C.

Resolución Número 005
(Enero 4 de 2016)

"Por la cual se hace un nombramiento"

LA SECRETARIA GENERAL DE LA ALCALDÍA MAYORDE BOGOTÁ, DISTRITO CAPITAL (E)
En ejercicio de sus fucultades legales, en especial de las conferidas en el Decreto 101 de 2004.

RESUELVE:

ARTÍCULO 1°-: Nombrar a la doctora ÁNGELA BEATRIZ ANZOLA DE TORO, identificada con la cédula de ciudadanía Nro. 53.905.271, en el cargo de Jefe de Oficina Código 006 Grado 08 de la Oficina de Alta Consejería para los Derechos de las Víctimas, la Paz y la Reconciliación, de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 2°-: Notificar a la doctora ÁNGELA BEATRIZ ANZOLA DE TORO, el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 3°-: Comunicar a la Subdirección de Talento Humano de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., para los trámites legales correspondientes.

ARTÍCULO 4°-: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE, NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los cuatro (4) días del mes de enero de dos mil dieciséis (2016).

GISELE MANRIQUE VACA
Secretaria General (E)

Resolución Número 007
(Enero 5 de 2016)

"Por la cual se hace un nombramiento".

LA SECRETARIA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, DISTRITO CAPITAL (E)
En ejercicio de sus facultades legales, en especial de las conferidas en el Decreto 101 de 2004.

RESUELVE:

ARTÍCULO 1°-: Nombrar a la doctora ADRIANA DEL PILAR ACOSTA ROA, identificada con la cédula de ciudadanía Nro. 52.839.123, en el cargo de Jefe Oficina Asesora Código 115 Grado 06 de la Oficina Asesora de Planeación de la Subsecretaría General de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 2°-: Notificar a la doctora ADRIANA DEL PILAR ACOSTA ROA, el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 3°-: Comunicar a la Subdirección de Talento Humano de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., para los trámites legales correspondientes.

ARTÍCULO 4°-: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE, NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los cinco (5) días del mes de enero de dos mil dieciséis (2016).

GISELE MANRIQUE VACA
Secretaria General (E)

Resolución Número 009
(Enero 5 de 2016)

"Por la cual se hace un nombramiento".

LA SECRETARIA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, DISTRITO CAPITAL (E)
En ejercicio de sus facultades legales, en especial de las conferidas en el Decreto 101 de 2004.

RESUELVE:

ARTÍCULO 1°-: Nombrar a la doctora AURA ELVIRA GÓMEZ MARTÍNEZ, identificada con la cédula de ciudadanía Nro. 52.375.911, en el cargo de Subdirector Técnico Código 068 Grado 06 de la Subdirección de Contratación de la Dirección de Gestión Corporativa, de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 2°-: Notificar a la doctora AURA ELVIRA GÓMEZ MARTÍNEZ, el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 3°-: Comunicar a la Subdirección de Talento Humano de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., para los trámites legales correspondientes.

ARTÍCULO 4°-: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE, NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los cinco (5) días del mes de enero de dos mil dieciséis (2016).

GISELE MANRIQUE VACA
Secretaria General (E)

Resolución Número 012
(Enero 5 de 2016)

"Por la cual se hace un nombramiento".

LA SECRETARIA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, DISTRITO CAPITAL (E)
En ejercicio de sus facultades legales, en especial de las conferidas en el Decreto 101 de 2004.

RESUELVE:

ARTÍCULO 1°-: Nombrar a la doctora YANET PATRICIA RODRÍGUEZ CAMARGO, identificada con

la cédula de ciudadanía Nro. 51.770.771. en el cargo de Subdirector Técnico Código 068 Grado 06 de la Subdirección de Talento Humano de la Dirección de Gestión Corporativa, de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 2°-: Notificar a la doctora YANET PATRICIA RODRÍGUEZ CAMARGO, el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 3°-: Comunicar a la Subdirección de Talento Humano de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., para los trámites legales correspondientes.

ARTÍCULO 4°-: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE, NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los cinco (5) días del mes de enero de dos mil dieciséis (2016).

GISELE MANRIQUE VACA
Secretaria General (E)

Resolución Número 017
(Enero 5 de 2016)

"Por la cual se hace un nombramiento".

LA SECRETARIA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, DISTRITO CAPITAL (E)
En ejercicio de sus facultades legales, en especial de las conferidas en el Decreto 101 de 2004.

RESUELVE:

ARTÍCULO 1º-: Nombrar a la doctora LUZ ÁNGELA MARÍA GÓMEZ GÓMEZ, identificada con la cédula de ciudadanía Nro. 52.866.113, en el cargo de Subdirector Técnico Código 068 Grado 06 de la Subdirección Administrativa de la Dirección de Gestión Corporativa, de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 2º-: Notificar a la doctora LUZ ÁNGELA MARÍA GÓMEZ GÓMEZ, el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 3º-: Comunicar a la Subdirección de Talento Humano de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., para los trámites legales correspondientes.

ARTÍCULO 4º-: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE, NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los cinco (5) días del mes de enero de dos mil dieciséis (2016).

GISELE MANRIQUE VACA
Secretaria General (E)

Resolución Número 018
(Enero 5 de 2016)

"Por la cual se hace un nombramiento".

LA SECRETARIA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, DISTRITO CAPITAL (E)
En ejercicio de sus facultades legales, en especial de las conferidas en el Decreto 101 de 2004.

RESUELVE:

ARTÍCULO 1º-: Nombrar a la doctora DIANA ALEJANDRA OSPINA MORENO, identificada con la cédula de ciudadanía Nro. 52.218.248, en el cargo de Subdirector Técnico Código 068 Grado 06 de la Subdirección de Calidad del Servicio de la Dirección Distrital de Servicio al Ciudadano, de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 2º-: Notificar a la doctora DIANA ALEJANDRA OSPINA MORENO, el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 3º-: Comunicar a la Subdirección de Talento Humano de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., el contenido de la presente

Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., para los trámites legales correspondientes.

ARTÍCULO 4º-: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE, NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los cinco (5) días del mes de enero de dos mil dieciséis (2016).

GISELE MANRIQUE VACA
Secretaria General (E)

Resolución Número 019
(Enero 5 de 2016)

"Por la cual se hace un nombramiento".

LA SECRETARIA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, DISTRITO CAPITAL (E)
En ejercicio de sus facultades legales, en especial de las conferidas en el Decreto 101 de 2004.

RESUELVE:

ARTÍCULO 1º-: Nombrar a la doctora IRMA NATHALIA KENGUAN HENAO, identificada con la cédula de ciudadanía Nro. 1.088.261.658, en el cargo de Asesor Código 105 Grado 05 de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 2º-: Notificar a la doctora IRMA NATHALIA KENGUAN HENAO, el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 3º-: Comunicar a la Subdirección de Talento Humano de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., para los trámites legales correspondientes.

ARTÍCULO 4º-: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE, NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los cinco (5) días del mes de enero de dos mil dieciséis (2016).

GISELE MANRIQUE VACA
Secretaria General (E)

Resolución Número 020
(Enero 5 de 2016)

"Por la cual se hace un nombramiento".

LA SECRETARIA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, D.C. (E)
En ejercicio de sus facultades legales, en especial de las conferidas en el Decreto 101 de 2004

RESUELVE:

ARTÍCULO 1º-: Nombrar a la doctora BEATRIZ CASTILLO TRUJILLO, identificada con la cédula de ciudadanía Nro. 41.707.191, en el cargo de Asesor, Código 105, Grado 05 de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 2º-: Notificar a la doctora BEATRIZ CASTILLO TRUJILLO el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

ARTÍCULO 3º-: Comunicar a la Subdirección de Talento Humano de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., el contenido de la presente Resolución, a través de la Subdirección de Gestión Documental de la misma Secretaría, para los trámites correspondientes.

ARTÍCULO 4º-: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE, NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los cinco (5) días del mes de enero de dos mil dieciséis (2016).

GISELE MANRIQUE VACA
Secretaria General (E)

Resolución Número SDH-000007
(Enero 6 de 2016)

"Por la cual se efectúa un nombramiento ordinario".

LA SECRETARIA DISTRITAL DE HACIENDA en ejercicio de las facultades legales y en especial las conferidas por el artículo 1º del decreto 101 del 13 de abril de 2004, y

CONSIDERANDO:

Que mediante memorando remitido por la Secretaria Distrital de Hacienda, se solicitó en la Subdirección del Talento Humano el nombramiento ordinario de LUIS FELIPE RIVERA GARCÍA en el cargo de Director Técnico código 009 grado 08, Despacho del Director de Informática y Tecnología.

Que una vez revisados los requisitos establecidos en el manual de funciones de la Secretaría Distrital de Hacienda, la Subdirección del Talento Humano, certifica que Luis Felipe Rivera García, los cumple.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1°. Nombrar a LUIS FELIPE RIVERA GARCÍA, identificado con cédula de ciudadanía 91.239.655, en el cargo de Director Técnico código 009 grado 08, Despacho del Director de Informática y Tecnología, de la planta de personal de la Secretaría Distrital de Hacienda, con una asignación básica mensual de $ 5.873.764 y gastos de representación de $ 2.349.506.

ARTÍCULO 2°. La presente resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D. C., a los seis (6) días del mes de enero de dos mil dieciséis (2016).

BEATRIZ ELENA ARBELÁEZ MARTÍNEZ
Secretaria Distrital de Hacienda

Resolución Número SDH-000008
(Enero 6 de 2016)

"Por la cual se efectúa un nombramiento ordinario".

LA SECRETARIA DISTRITAL DE HACIENDA

en ejercicio de las facultades legales y en especial las conferidas por el artículo 1º del decreto 101 del 13 de abril de 2004, y

CONSIDERANDO:

Que mediante memorando remitido por la Secretaria Distrital de Hacienda, se solicitó en la Subdirección del Talento Humano el nombramiento ordinario de LEONARDO ARTURO PAZOS GALINDO, en el cargo de Director Técnico código 009 grado 08, Despacho del Director Jurídico.

Que una vez revisados los requisitos establecidos en el manual de funciones de la Secretaría Distrital de Hacienda, la Subdirección del Talento Humano, certifica que Leonardo Arturo Pazos Galindo, los cumple.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1°. Nombrar a LEONARDO ARTURO PAZOS GALINDO, identificado con cédula de ciudadanía 79.374.245, en el cargo de Director Técnico código 009 grado 08, Despacho del Director Jurídico, de la planta de personal de la Secretaría Distrital de Hacienda, con una asignación básica mensual de $ 5.873.764 y gastos de representación de $ 2.349.506.

ARTÍCULO 2°. La presente resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D. C., a los seis (6) días del mes de enero de dos mil dieciséis (2016).

BEATRIZ ELENA ARBELÁEZ MARTÍNEZ
Secretaria Distrital de Hacienda

Resolución Número SDH-000009
(Enero 6 de 2016)

"Por la cual se efectúa un nombramiento ordinario".

LA SECRETARIA DISTRITAL DE HACIENDA en ejercicio de las facultades legales y en especial las conferidas por el artículo 1º del decreto 101 del 13 de abril de 2004, y

CONSIDERANDO:

Que mediante memorando remitido por la Secretaria Distrital de Hacienda, se solicitó en la Subdirección del Talento Humano el nombramiento ordinario de MARÍA ALEJANDRA VIDAL SAMBONI en el cargo de Jefe Oficina código 006 grado 06, Oficina de Análisis y Control de Riesgo.

Que una vez revisados los requisitos establecidos en el manual de funciones de la Secretaría Distrital de Hacienda, la Subdirección del Talento Humano, certifica que María Alejandra Vidal Samboni, los cumple.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1°. Nombrar a MARÍA ALEJANDRA VIDAL SAMBONI, identificada con cédula de ciudadanía 52.715.990, en el cargo de Jefe de Oficina código 006 grado 06, Oficina de Análisis y Control de Riesgo, de la planta de personal de la Secretaría Distrital de Hacienda, con una asignación básica mensual de $ 4.784.819 y gastos de representación de $ 1.913.928.

ARTÍCULO 2°. La presente resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D. C., a los seis (6) días del mes de enero de dos mil dieciséis (2016).

BEATRIZ ELENA ARBELÁEZ MARTÍNEZ
Secretaria Distrital de Hacienda

Resolucion Núero SDH-000046
(Diciembre 23 de 2015)

"Por la cual se reglamenta el trámite interno de las peticiones, quejas, reclamos y sugerencias -PQRS- en la Secretaría Distrital de Hacienda".

EL SECRETARIO DISTRITAL DE HACIENDA (E)
En uso de sus facultades constitucionales y legales, en especial las conferidas por el artículo 22 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, sustituido por la Ley 1755 de 2015 y el artículo 4° del Decreto 601 de 2014, modificado por el Decreto 364 de 2015 y

CONSIDERANDO:

Que la Constitución Política establece en el artículo 23 el derecho fundamental de petición, el cual permite que toda persona presente peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta respuesta dentro de los términos legales.

Que de conformidad con lo dispuesto en el artículo 22 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, sustituido por la Ley 1755 de 2015, las autoridades deben reglamentar el trámite interno de las peticiones que les corresponda resolver y la manera de atender las quejas para garantizar el buen funcionamiento de los servicios a su cargo, observando en especial las disposiciones legales consagradas en los artículos 13 a 33 de la Ley 1437 de 2011, sustituidos por la Ley 1755 de 2015, en el inciso 3 del artículo 6 de la Ley 962 de 2005, en el artículo 55 de la Ley 190 de 1995 y en su Decreto Reglamentario 2232 de 1995, compilado en el Decreto Único Reglamentario del Sector de la Función Pública N° 1083 de 2015 o las normas que las modifiquen adicionen o sustituyan .

Que el Decreto Nacional 2573 de 2014, compilado en el Decreto Único Reglamentario del Sector de Tecnología de la Información y las Comunicaciones N° 1078 de 2015, establece los lineamientos, instrumentos y plazos para implementar la Estrategia de Gobierno en Línea y así contribuir al incremento de la transparencia en la gestión pública y promover la participación ciudadana haciendo uso de los medios electrónicos en concordancia con lo dispuesto por el artículo 76 de la Ley 1474 de 2011 y el artículo 1° del Decreto Ley 019 de 2012 o las normas que las modifiquen, adicionen o sustituyan.

Que la Ley 1712 de 2014, *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"*, regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía de tal derecho y las excepciones a la publicidad de información.

Que el Secretario Distrital de Hacienda, mediante resoluciones SDH-000083 del 11 de abril de 2014 y SDH-000192 del 19 de agosto de 2014, reglamentó el trámite interno de las peticiones, quejas, reclamos y sugerencias en la Secretaría Distrital de Hacienda.

Que el 30 de junio de 2015 fue expedida la Ley estatutaria 1755, *"Por medio de la cual se regula el derecho de petición y se sustituye un título del Código de Procedimiento y de lo Contencioso Administrativo"*, y en virtud de esto se hace necesario modificar la reglamentación interna del trámite de las peticiones, quejas, reclamos y sugerencias –PQRS- que le corresponden atender, responder o resolver a la Secretaría Distrital de Hacienda.

Que en mérito de lo expuesto,

RESUELVE:

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO 1°. Objeto. El objeto de la presente Resolución es reglamentar y adoptar el trámite interno de las –PQRS- presentados por la ciudadanía ante la Secretaría Distrital de Hacienda a través de los canales oficiales definidos por la Entidad, de conformidad con lo establecido en la normativa vigente aplicable a la materia.

ARTÍCULO 2°. Canales Oficiales. Los canales oficiales definidos por la Entidad para la recepción de las –PQRS- presentadas por la ciudadanía son los siguientes:

- **Puntos de Radicación:** Corresponden a las ventanillas de radicación dispuestas por la Entidad para la recepción de comunicaciones escritas presentadas por la ciudadanía.
- **Sistema Distrital de Quejas y Soluciones (SDQS):** Herramienta informática de acceso público dispuesta por la Alcaldía Mayor de Bogotá D.C., administrada por la Secretaría General, la cual permite a los ciudadanos del Distrito Capital formular de manera virtual sus PQRS, sobre temas relacionados con cualquier entidad del Distrito, para que éstas sean resueltas por cada una de ellas en lo de su competencia.
- **Correo Electrónico:** La Secretaría Distrital de Hacienda dispone del correo electrónico contactenos@shd.gov.co, el cual es administrado por la Oficina de Atención al Ciudadano de la Subsecretaría General, por medio del cual, la ciudadanía puede registrar de manera virtual y electrónica sus –PQRS-.
- **Atención Telefónica:** Medio de comunicación directo con el que cuenta la ciudadanía, a través del cual puede formular verbalmente las –PQRS- ante la Oficina de Atención al Ciudadano de la Subsecretaría General.
- **Atención Presencial:** Punto de atención directa y personalizada dispuesto en la Oficina de Atención al Ciudadano de la Subsecretaría General, para la recepción de las –PQRS-.
- **Buzón de Sugerencias:** Buzones ubicados en puntos de atención dispuestos por la Entidad, a través de los cuales la ciudadanía puede formular por escrito las –PQRS-.

PARÁGRAFO PRIMERO. El Secretario Distrital de Hacienda por necesidades del servicio y para los fines que determine, podrá establecer otros canales oficiales para la recepción de las –PQRS- en la Entidad, previa recomendación de la Oficina de Atención al Usuario.

PARÁGRAFO SEGUNDO. Las –PQRS- que se reciban por un medio diferente a los establecidos en el presente artículo deberán ser remitidos por el(la) servidor(a) que las reciba al correo electrónico contactenos@shd.gov.co para que éstas sean registradas en el aplicativo CORDIS y surtan el trámite respectivo, de conformidad con el procedimiento establecido para ello.

CAPÍTULO II
PETICIONES

ARTÍCULO 3°. Derecho de Petición. Toda persona tiene derecho a presentar peticiones respetuosas verbales o escritas a las autoridades por motivos de interés general o particular y a obtener resolución completa y de fondo sobre las mismas. Toda actuación que inicie cualquier persona ante las autoridades implica el ejercicio del derecho de petición consagrado en el artículo 23 de la Constitución Política, sin que sea necesario invocarlo.

El derecho de petición ante la Secretaría Distrital de Hacienda puede ser ejercido a través de modalidades tales como:

- **Solicitud de Información:** Cuando una persona demanda el acceso a documentos, actos o actuaciones de la entidad.
- **Solicitud de Copias:** Cuando se solicita(n) copia(s) de documento(s) que reposa(n) en los archivos de la entidad, ya sea en interés particular o general.
- **Consulta:** Cuando ante la entidad se presenta una solicitud para que se exprese una opinión, un parecer o un criterio sobre determinada materia, relacionada con sus funciones o con situaciones de su competencia.
- **Queja:** Cuando ante la Entidad se presenta una manifestación de protesta, censura, descontento o inconformidad que formula una persona en relación con una conducta

que considera irregular de uno o varios servidores públicos o contratistas, en desarrollo de sus funciones o durante la prestación de sus servicios.

- **Reclamo:** Cuando una persona exige, reivindica o demanda ante la Entidad una solución, ya sea por motivo de interés general o particular, referente a la indebida prestación de un servicio o falta de atención de una solicitud.

- **Sugerencia:** Cuando se presenta a la entidad la manifestación de una idea o propuesta para mejorar la prestación de un servicio o la gestión institucional.

Mediante el derecho de petición, la ciudadanía podrá solicitar, entre otras actuaciones: el reconocimiento de un derecho, la intervención de una entidad o servidor, la resolución de una situación jurídica, la prestación de un servicio e interponer recursos.

PARÁGRAFO PRIMERO. La recepción de las PQRS verbales estará a cargo de la Oficina de Atención al Ciudadano de la Subsecretaría General, a través de los canales de atención telefónica o presencial, de conformidad con la reglamentación que para el efecto se establezca para ello por la autoridad nacional.

Cuando al recibir una PQRS verbal se encuentre que el objeto de la solicitud no es competencia de la Secretaría Distrital de Hacienda se le informará inmediatamente al peticionario con la indicación de cuál es la Entidad a la que debe dirigir su requerimiento. Si el peticionario insiste en formular su solicitud ante la Secretaría Distrital de Hacienda, se recibirá dejando constancia de ello y se procederá a remitir la misma a la entidad competente a través del SDQS.

PARÁGRAFO SEGUNDO. La Secretaría Distrital de Hacienda no podrá negarse a la recepción y radicación de las –PQRS-.

ARTÍCULO 4°. Peticiones Análogas: Cuando más de diez (10) personas formulen peticiones análogas de información, de interés general o de consulta, la Secretaría Distrital de Hacienda, además de responder directamente a los peticionarios, podrá emitir una única respuesta que publicará en un diario de amplia circulación, la pondrá en su página web y entregará copias de la misma a quienes la soliciten.

ARTÍCULO 5°. Contenido de las Peticiones. Toda petición deberá contener por lo menos:

1. La designación de la autoridad a que se dirige.

2. Los nombres y apellidos completos del solicitante y de su representante y/o apoderado si es el caso, con indicación de su documento de identidad y de la dirección donde recibirá correspondencia. El peticionario podrá agregar el número de fax o la dirección electrónica. Si el peticionario es una persona privada que deba estar inscrito en el registro mercantil, estará obligada a indicar su dirección electrónica.

3. El objeto de la petición.

4. Las razones en las que fundamenta su petición.

5. La relación de los documentos que desee presentar para iniciar el trámite.

6. Firma del peticionario cuando fuere el caso.

PARÁGRAFO PRIMERO. La dependencia responsable del trámite dentro de la Secretaría Distrital de Hacienda tiene la obligación de examinar integralmente la petición, y en ningún caso la estimará incompleta por falta de requisitos o documentos que no se encuentren dentro del marco jurídico vigente, que no sean necesarios para resolverla o que se encuentren dentro de sus archivos.

PARÁGRAFO SEGUNDO. En ningún caso podrá ser rechazada la petición por motivos de fundamentación inadecuada o incompleta.

PARÁGRAFO TERCERO. Cuando la petición no se acompañe de los documentos necesarios para resolverla, al momento de la recepción y radicación, la persona competente deberá indicar al peticionario los documentos que faltan. Si éste insiste en que se radiquen así, se hará dejando constancia de los requisitos o documentos faltantes.

PARÁGRAFO CUARTO. Cuando se actúe a través de mandatario, éste deberá acompañar el respectivo poder en los términos señalados en el artículo 74 de la Ley 1564 de 2012 y demás normas concordantes o las normas que las modifiquen, adicionen o sustituyan.

PARÁGRAFO QUINTO. El ejercicio del Derecho de Petición es gratuito y puede realizarse sin necesidad de representación a través de abogado, o de persona mayor cuando se trate de menores para el pleno ejercicio de sus derechos fundamentales.

ARTÍCULO 6°. Información General. Los asuntos de información general de la entidad tales como: la misión, funciones y estructura; organigrama y funciones generales; procesos y procedimientos; normatividad asociada a la gestión; mecanismos para la formulación de quejas y reclamos; entre otros, estarán disponibles en el portal web de la Entidad. No obstante, cualquier persona tiene derecho a pedir y obtener copia de documentos relacionados con dichos asuntos, de conformidad con lo establecido en la presente Resolución.

ARTÍCULO 7°. Información Especial o Particular. Las peticiones dirigidas a consultar y obtener acceso a información diferente a la señalada en el artículo anterior, sobre asuntos de la Entidad, así como aquellas tendientes a obtener copia de los documentos que reposen en la Entidad, serán atendidas por la dependencia o servidor(a)s competente(s), conforme al procedimiento y plazos señalados en esta Resolución. Sin embargo, la petición se negará si la solicitud se refiere a alguno de los documentos que la Constitución Política o la ley prescriben como de carácter reservado o clasificado.

ARTÍCULO 8°. Examen de Documentos. El examen de documentos se facilitará en horas de atención al público con la autorización del Jefe de la respectiva dependencia, o del servidor(a) en quien éste haya delegado dicha facultad, previa verificación que los documentos no tienen carácter reservado o clasificado|.

ARTÍCULO 9°. Solicitud de Copias. La solicitud de copias o fotocopias de documentos que reposen en la Secretaría Distrital de Hacienda se tramitará por los responsables de su custodia de acuerdo con las Tablas de Retención Documental de la Entidad, previo el pago por parte del peticionario del costo de las mismas conforme a la Resolución 340 de 2002 de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. o sus modificatorios.

Ningún servidor(a) podrá suministrar copia o fotocopia de documentos que según la Constitución o la Ley tengan el carácter de clasificado o reservado. El suministro de copia o fotocopia de documentos sin tal carácter, o de cualquier otro documento, requiere de orden del Jefe del área responsable de la custodia de los mismos.

PARÁGRAFO: En ningún caso el precio de las copias o fotocopias podrá exceder el valor de la reproducción determinado según el inciso primero del presente artículo.

ARTÍCULO 10°. Extensión de la jurisprudencia del Consejo de Estado a terceros. El interesado en que se aplique a su caso la jurisprudencia del Consejo de Estado presentará petición ante la Entidad para reconocer el derecho, siempre que la pretensión judicial no haya caducado. Petición que además de los requisitos generales contendrá los señalados en el artículo 102° de la Ley 1437 de 2011 o la norma que la modifique, adicione o sustituya.

La Secretaría Distrital de Hacienda extenderá los efectos de las sentencias de unificación jurisprudencial dictadas por el Consejo de Estado, en las que se haya reconocido un derecho a quienes lo soliciten y acrediten los mismos supuestos fácticos y jurídicos, debiéndose observar con preferencia los precedentes de la Corte Constitucional que interpreten las normas constitucionales aplicables a la resolución de los asuntos.

ARTÍCULO 11°. Términos para resolver las PQRS presentadas ante la Entidad. Salvo norma legal especial, la Secretaría Distrital de Hacienda tendrá un plazo máximo de quince (15) días hábiles siguientes a la recepción del requerimiento en la Entidad, para atender o resolver las –PQRS- que le sean asignadas a las dependencias de acuerdo con sus competencias; tiempo dentro del cual el peticionario deberá recibir la respuesta.

Sin perjuicio de lo anterior, estará sometido a término especial en la presente Resolución, las siguientes peticiones:

1. Las peticiones de información y copias o fotocopias de documentos deberán resolverse dentro de los diez (10) días siguientes a su recepción. Si en este lapso no se ha dado respuesta al peticionario se entenderá, para todos los efectos legales, que la respectiva solicitud ha sido aceptada y, por consiguiente, la Administración ya no podrá negar la entrega de la información o de dichos documentos al peticionario, y como consecuencia, las copias o fotocopias se entregarán dentro de los tres (3) días siguientes.

2. Las peticiones de documentos y de información provenientes de otras entidades o autoridades públicas, deberán resolverse dentro de los diez (10) días siguientes a su recepción.

3. Las peticiones mediante los cuales se eleva una consulta a las autoridades en relación con las materias a su cargo deberán resolverse dentro de los treinta (30) días siguientes a su recepción.

4. Las solicitudes a que se refiere el inciso 2° del artículo 8° de la Ley 393 de 1997 (Acción de Cumplimiento), o la norma que la modifique, adicione o sustituya, dentro de los diez (10) días hábiles siguientes a su recepción en la entidad.

PARÁGRAFO PRIMERO. Cuando la –PQRS- corresponda a un trámite enmarcado en una norma especial que establezca un término mayor de respuesta, dentro de los quince (15) días hábiles siguientes a la recepción del requerimiento en la Entidad, la dependencia o el(la) servidor(a) responsable deberá informar por escrito al ciudadano el plazo en el cual será dada respuesta de fondo, situación que debe quedar registrada en el aplicativo CORDIS.

PARÁGRAFO SEGUNDO. En el evento de que la Entidad no cuente con los datos necesarios para allegar la respuesta al peticionario o quejoso, a causa de que la –PQRS- recibida no relacione la información de contacto del remitente, y no sea posible establecerla conforme a información que reposa en la Entidad, se debe publicar en la cartelera de la Oficina de Atención al Ciudadano de la Subsecretaría General y en la página web de la Entidad, la contestación producida por la dependencia o servidor(a) competente para resolver o atender el requerimiento.

A su vez, cuando la respuesta emitida por la Secretaría Distrital de Hacienda a una –PQRS- haya sido enviada a la dirección informada por el peticionario o quejoso y ésta sea devuelta a la Entidad por imposibilidad de su entrega, dicha respuesta debe ser comunicada mediante publicación en la página web de la Entidad, reportando los datos generales que identifiquen la recepción del requerimiento, así como la información de salida de la respuesta dada por la dependencia o servidor(a) competente de responder o resolver, y la causal de la devolución.

ARTÍCULO 12. Excepción términos para resolver las PQRS presentadas ante la Entidad. Cuando excepcionalmente no sea posible resolver las –PQRS- en los plazos señalados, se deberá informar de inmediato esta circunstancia al interesado, y en todo caso antes del vencimiento de los términos establecidos anteriormente, expresando los motivos de la demora e indicando el plazo razonable en que se resolverá o dará respuesta, el cual no podrá exceder el doble del tiempo inicialmente previsto.

Cuando no se dé cumplimiento a los términos establecidos en el presente artículo, el Jefe Inmediato, tan pronto tenga conocimiento de dicha circunstancia, deberá compeler al servidor (a) responsable para que atienda la –PQRS- y dé respuesta en forma inmediata a dicho requerimiento, sin perjuicio de los procesos disciplinarios cuando a ello haya lugar.

ARTÍCULO 13°. Trámite Interno de las PQRS. El trámite interno a las –PQRS- peticiones presentadas por la ciudadanía ante la Secretaría Distrital de Hacienda inicia con su recepción a través de los canales oficiales definidos por la Entidad, continúa con su radicación y asignación de trámite en el aplicativo CORDIS a las dependencias competentes de responder, resolver o atender las mismas, y prosigue con su distribución y entrega al área correspondiente. Frente a esta gestión se debe tener en cuenta lo siguiente:

a. Las quejas, reclamos y sugerencias recibidas en los puntos de radicación dispuestos por la Secretaría Distrital de Hacienda, por correo electrónico, a través de atención telefónica o presencial y en los buzones de sugerencias, deberán ser registrados en el SDQS por la Oficina de Atención al Ciudadano de la Subsecretaría General.

b. Las –PQRS- que ingresen de manera directa por el SDQS y por los demás canales oficiales diferentes al punto de radicación, deberán ser registradas en el aplicativo CORDIS.

PARÁGRAFO PRIMERO. En cuanto a las quejas recibidas, la Oficina de Atención al Ciudadano de la Subsecretaría General deberá informar por escrito al ciudadano el área responsable de atenderlas al interior de la Secretaría Distrital de Hacienda de acuerdo con su competencia legal.

PARÁGRAFO SEGUNDO: A su vez la Oficina de Atención al Ciudadano de la Subsecretaría General en cumplimiento de las funciones asignadas por el artículo 60 del Decreto 601 de 2014 o la norma que la modifique, adicione o sustituya, le corresponderá administrar el Sistema de Quejas y Soluciones para garantizar un control eficaz de las respuestas ofrecidas por las diferentes dependencias a los ciudadanos y comunicar a los responsables del proceso para que se tomen las medidas correctivas necesarias para propiciar las mejoras pertinentes en los procesos.

Así mismo dicha Oficina realizará el seguimiento y controlar de manera integral el trámite y análisis de las respuestas de quejas formuladas por los ciudadanos en relación con los servidores públicos y servicios que presta la Secretaría Distrital de Hacienda, para que sean resueltos con calidad y dentro de los términos previstos.

Adicionalmente, la atención de las quejas presentadas contra servidores públicos será efectuada por la Oficina de Control Interno Disciplinario de conformidad con lo establecido en la Ley 734 de 2002, sus normas modificatorias o concordantes.

PARÁGRAFO TERCERO. Las quejas formuladas en relación con los servicios prestados por contratistas de la Entidad, deben ser atendidas por el supervisor o interventor del contrato de acuerdo con la guía 37-G-03 "Guía para el ejercicio de las funciones de Supervisor y obligaciones de la Interventoría" o el documento que haga sus veces.

ARTÍCULO 14°. Competencia para dar respuesta, resolver o atender las –PQRS- presentadas ante la Entidad. De conformidad con las competencias propias al interior de la entidad en relación directa con las –PQRS- presentadas, a través del aplicativo CORDIS se asignará trámite a las dependencias competentes para responder, resolver o atender las mismas.

El(la) servidor(a) de la dependencia a la que le es asignado el trámite, debe verificar que la –PQRS- reúne la información o documentos necesarios para responder o resolver la misma, y determinar si efectivamente tiene la competencia para atenderla.

PARÁGRAFO. Cuando la competencia para resolver una PQRS recaiga en diferentes dependencias de la Entidad, deberá darse cumplimiento a las directrices impartidas para garantizar la coordinación y consolidación de la integralidad de la respuesta.

ARTÍCULO 15°. Falta de Competencia. Si la dependencia a quien se le asigna el trámite de la PRQS no es competente para resolver o atender la misma, dentro de los cinco (5) días hábiles siguientes al de la recepción en la Secretaría Distrital de Hacienda - SDH, deberá dar traslado de la petición a la entidad competente, expresando las razones por las cuales no es de su competencia la respuesta y enviar copia del oficio al peticionario.

Si encuentra que la competencia para resolver las –PQRS- recae en otro(a) servidor(a) de la Secretaría Distrital de Hacienda, debe dar traslado motivado al competente dentro de los dos (2) días hábiles siguientes a la recepción de la asignación del trámite, lo cual deberá ser registrado en el aplicativo CORDIS. En este evento, deberá tenerse en cuenta que el plazo con que cuenta la Secretaría Distrital de Hacienda para responder la –PQRS- se contabiliza a partir del día siguiente a la radicación en la Entidad.

En caso de no existir servidor(a) competente para dar respuesta, dentro del mismo término legal señalado, se deberán comunicar por escrito al peticionario las razones por las cuales se considera que no hay autoridad competente.

PARÁGRAFO. Si el(la) servidor (a) de la dependencia a la que le es asignada la –PQRS- considera que no es competente para su trámite, debe informar de esta circunstancia en el momento de la entrega por parte del personal de correspondencia para que se efectúe el redireccionamiento respectivo a través del aplicativo CORDIS. Cuando se produzca la asignación y recepción de la PQRS, el(la) servidor(a) definido(a) como competente para dar respuesta, resolver o atender la misma, estará obligado(a) a realizar el trámite de traslado correspondiente mediante su registro en el aplicativo CORDIS, de conformidad con las disposiciones consagradas en la presente Resolución.

ARTÍCULO 16°. Peticiones Incompletas y Desistimiento Tácito. En virtud del principio de eficacia, cuando la dependencia o servidor(a) al que le ha sido asignado el trámite constate que una petición ya radicada está incompleta o que el peticionario deba realizar una gestión de trámite a su cargo, necesaria para adoptar una decisión de fondo, y que la actuación pueda continuar sin oponerse a la ley, requerirá al peticionario dentro de los diez (10) días hábiles siguientes a la fecha de radicación para que la complete en el término máximo de un (1) mes.

A partir del día siguiente en que el interesado aporte los documentos o informes requeridos se reactivará el término para resolver la petición.

Se entenderá que el peticionario ha desistido de su solicitud o de la actuación cuando no satisfaga el requerimiento, salvo que antes de vencer el plazo concedido solicite prórroga hasta por un término igual.

Vencidos los términos establecidos en este artículo, sin que el peticionario haya cumplido el requerimiento, la dependencia o el(la) servidor(a) al que le ha sido asignado(a) la –PQRS- decretará el desistimiento y el archivo del expediente, mediante acto administrativo motivado que se notificará personalmente, contra el cual únicamente procede recurso de reposición, sin perjuicio de que la respectiva solicitud pueda ser nuevamente presentada con el lleno de los requisitos legales.

ARTÍCULO 17°. Desistimiento Expreso de la Petición. Los interesados podrán desistir en cualquier tiempo de sus peticiones, sin perjuicio de que la respectiva solicitud pueda ser nuevamente presentada con el lleno de los requisitos legales, pero la dependencia o el(la) servidor(a) al que le ha sido asignado la –PQRS- podrá continuar de oficio la actuación si la considera necesaria por razones de interés público, en tal caso expedirá Resolución motivada.

ARTÍCULO 18°. Peticiones Irrespetuosas, Oscuras o Reiterativas. Toda petición debe ser respetuosa so pena de rechazo por parte de la dependencia o servidor(a) competente, lo que debe producirse por acto debidamente motivado y contra lo cual procede Recurso de Reposición. Sólo cuando no se comprenda la finalidad u objeto de la petición, ésta se devolverá al interesado para que la corrija o aclare dentro de los diez (10) días hábiles siguientes a su recepción. En caso de no corregirse o aclararse, se archivará la petición. En ningún caso se devolverán peticiones que se consideren inadecuadas o incompletas.

Respecto de peticiones reiterativas ya resueltas, la Entidad podrá remitirse a las respuestas anteriores, salvo que se trate de derechos imprescindibles, o de peticiones que se hubieren negado por no acreditar requisitos, siempre que en la nueva petición se subsane.

ARTÍCULO 19°. Prueba de recepción y envío de mensajes de datos por la autoridad. Para efectos de

demostrar el envío y la recepción de comunicaciones, se aplicarán las siguientes reglas:

1. El mensaje de datos emitido por la autoridad para acusar recibo de una comunicación, será prueba tanto del envío hecho por el interesado como de su recepción por la autoridad. En este caso la respuesta podrá ser emitida por esta misma vía, cumpliendo con el procedimiento de "Quejas y Soluciones".

2. Cuando fallen los medios electrónicos de la Entidad, que impidan a las personas enviar sus escritos, peticiones o documentos, el remitente podrá insistir en su envío dentro de los tres (3) días hábiles siguientes, o remitir el documento por otro medio dentro del mismo término, siempre y cuando exista constancia de los hechos constitutivos de la falla en el servicio.

PARÁGRAFO: En caso de que la –PQRS- sea enviada a través de cualquier medio idóneo para la comunicación o transferencia de datos, esta tendrá como fecha y hora de radicación, así como el número y clase de documentos recibidos, los registrados en el medio por el cual se han recibido los documentos.

ARTÍCULO 20°. Informaciones y Documentos Reservados o Clasificados. Tendrán carácter de reservado o clasificado aquellos documentos sometidos a reserva por la Constitución Política y la Ley, así como los contenidos en el Índice de Información Clasificada y Reservada definido por la Entidad.

PARÁGRAFO. Para efecto de la solicitud de información de carácter reservada o clasificada, solo podrá ser solicitada por el titular de la información, por sus apoderados o por las personas autorizadas con facultad expresa para acceder a esa información.

ARTÍCULO 21°. Denegación o Rechazo de las Peticiones de Información por Motivo de Clasificación o Reserva. Toda decisión que rechace la petición de informaciones o documentos será motivada, indicará en forma precisa el fundamento constitucional que deniega o rechaza la solicitud de información por razón de clasificación o reserva, señalando expresamente la norma, artículo, inciso o párrafo de la calificación, la identificación de la excepción, el tiempo por el que se extiende la clasificación o reserva, contado a partir de la fecha de generación de la información, la determinación del daño presente, probable y específico que causaría la divulgación de la información y la relación de las razones y las pruebas, en caso de que existan, que acrediten la amenaza del daño. Dicha respuesta deberá notificarse al peticionario y contra la decisión que rechace la petición de informaciones o documentos por motivos de clasificación o reserva legal no procede recurso alguno, salvo lo previsto en el artículo siguiente.

La restricción por reserva legal no se extenderá a otras piezas del respectivo expediente o actuación que no estén cubiertas por ella.

PARÁGRAFO. El carácter reservado de una información o de determinados documentos, no será oponible a las autoridades judiciales, legislativas, ni a las autoridades administrativas que siendo constitucional o legalmente competentes para ello, los soliciten para el debido ejercicio de sus funciones. Corresponde a dichas autoridades asegurar la reserva de las informaciones y documentos que lleguen a conocer.

ARTÍCULO 22°. Insistencia del Solicitante en caso de Reserva. Si la persona interesada insistiere en su petición de información o de documentos ante la autoridad que invoca la reserva, corresponderá al Tribunal Administrativo de Cundinamarca decidir en única instancia si se niega o se acepta, total o parcialmente, la petición formulada.

Para ello, el(la) servidor(a) respectivo(a) enviará la documentación correspondiente al Tribunal Administrativo de Cundinamarca, el cual decidirá dentro de los términos de su competencia, de conformidad con lo previsto en el artículo 26 de la Ley 1437 de 2011, sustituido por la Ley 1755 de 2015 o la norma que la modifique, adicione o sustituya.

PARÁGRAFO. El recurso de insistencia deberá interponerse por escrito y sustentado en la diligencia de notificación, o dentro de los diez (10) días siguientes a ella.

CAPÍTULO III
SEGUIMIENTO Y CONTROL DE LAS -PQRS- , INFORME Y EVALUACIÓN DEL SISTEMA

ARTÍCULO 23°. Seguimiento y Control al trámite de las –PQRS-. La Oficina de Atención al Ciudadano de la Subsecretaría General, conforme a su competencia y de acuerdo con lo establecido en el procedimiento definido, deberá efectuar seguimiento y control a las -PQRS- recibidas en la Entidad.

ARTÍCULO 24°. Informe de las -PQRS-. El(la) servidor(a) designado(a) por la Oficina de Atención al Ciudadano de la Subsecretaría General, deberá elaborar el "Informe Mensual de Peticiones, Quejas, Reclamos y Sugerencias" o el documento que corresponda, de acuerdo con el formato establecido para ello, como instrumento que evidencie el seguimiento y control al trámite de las –PQRS- recibidas en la Entidad.

ARTÍCULO 25°. Evaluación del Sistema. De acuerdo con sus funciones y competencias, la Oficina de Con-

trol Interno deberá evaluar de manera permanente el "Sistema de Quejas y Soluciones" de la Entidad o el mecanismo que haga sus veces y rendirá informe semestral sobre el particular al Despacho del Secretario Distrital de Hacienda.

CAPÍTULO IV
DISPOSICIONES FINALES

ARTÍCULO 26°. Procedimientos Regulados por Normas Especiales. Los procedimientos administrativos regulados por normas especiales se regirán por ellas, y en lo no previsto se aplicarán las disposiciones contenidas en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo y en la presente Resolución, en cuanto resulten compatibles, y las normas que las modifiquen, adicionen o sustituyan.

ARTÍCULO 27°. Sanciones. La falta de atención a las –PQRS-, a los términos para resolverlas y el desconocimiento de los derechos de las personas, serán sancionados disciplinariamente por la Entidad de conformidad con los procesos y procedimientos definidos para ello, sin perjuicio de la acción prevalente de los entes de control competentes, de conformidad con las normas legales vigentes.

ARTÍCULO 28°. Legislación Complementaria. Las situaciones no previstas en la presente Resolución se regirán por las disposiciones contenidas en las leyes 1581 de 2012, 1712 de 2014 y 1755 de 2015 y en las demás disposiciones que lo modifiquen, adicionen o sustituyan.

ARTÍCULO 29°. Precedente Administrativo. Al resolver los asuntos de su competencia, la Secretaría Distrital de Hacienda aplicará las disposiciones constitucionales, legales y reglamentarias de manera uniforme a situaciones que tengan los mismos supuestos fácticos y jurídicos. Así mismo, al adoptar sus decisiones deberá tener en cuenta las sentencias de unificación jurisprudencial del Consejo de Estado en las que se interpreten y apliquen dichas normas, debiéndose observar con preferencia los precedentes de la Corte Constitucional que interpreten las normas constitucionales aplicables a la resolución de los asuntos.

ARTÍCULO 30°. Vigencia. La presente Resolución regirá a partir de la fecha de su publicación en el Registro Distrital y deroga las disposiciones que le sean contrarias, en especial las Resoluciones Nos. SDH-0000083 del 11 de abril de 2014 y la SDH-000192 del 19 de agosto de 2014, expedidas por el Secretario Distrital de Hacienda.

PUBLÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los veintitrés (23) días del mes de diciembre de dos mil quince (2015).

JOSÉ ALEJANDRO HERRERA LOZANO
Secretario Distrital de Hacienda (E)

Resolucion Número SDH-000062
(Diciembre 31 de 2015)

Por la cual actualiza el Modelo Estándar de Control Interno de la Secretaría Distrital de Hacienda de conformidad con el Decreto 1083 de 2015.

EL SECRETARIO DISTRITAL DE HACIENDA (E)
En uso de sus facultades que le confiere el artículo 114 del Decreto Ley 1421 de 1993, artículos 3º, 4º, 6º y 8º de la Ley 87 de 1993 y el artículo 4° del Decreto Distrital 601 de 2014, modificado por el Decreto Distrital 364 de 2015 y,

CONSIDERANDO:

Que el artículo 209 de la Constitución Política de Colombia de 1991, establece: *"La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones y las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley".*

Que el artículo 269 de la Constitución Política, establece que: "En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas".

Que el literal b del artículo 3° de la Ley 87 del 29 de noviembre de 1993 *"por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones",* concordante con el artículo 114 del Decreto 1421 del 21 de julio 1993, establece que corresponde a la máxima autoridad del organismo o Entidad, la responsabilidad de establecer, mantener y perfeccionar el Sistema de Control Interno, el cual debe ser adecuado a la naturaleza, estructura y misión de la organización.

Que la Ley 87 del 29 de noviembre de 1993, en su artículo 4° prevé que toda entidad debe implantar aspectos que orientarán la aplicación del Control Interno.

Que el Artículo 6º de la Ley 87 de 1993, consagra que el establecimiento y desarrollo del Sistema de Control Interno de los organismos y las entidades públicas, será responsabilidad del representante legal o máximo directivo correspondiente. No obstante, la aplicación de los métodos y procedimientos al igual que la calidad, eficiencia y eficacia del control interno, también será de responsabilidad de los jefes de cada una de las distintas dependencias de las entidades y organismos.

Que el literal p) del artículo 4° del Decreto Distrital 601 de 2014, modificado por el Decreto Distrital 364 de 2015, establece entre las funciones del Despacho del Secretario Distrital de Hacienda, la de *"Responder por la implementación y desarrollo del Sistema de Control Interno en la Entidad".*

Que el artículo 1° del Decreto Nacional 943 del 21 de mayo de 2014, *"Por el cual se actualiza el Modelo Estándar de Control Interno (MECI)",* compilado por el Decreto Único Reglamentario del Sector de la Función Pública 1083 de 2015 en el numeral 2.2.21.6.1, adopta la actualización del Modelo Estándar de Control Interno para el Estado Colombiano MECI, en el cual se determinan las generalidades y estructura necesaria para establecer, implementar y fortalecer un Sistema de Control Interno en las entidades y organismos obligados a su implementación, de acuerdo con lo dispuesto en el artículo 5° de la Ley 87 de 1993. El Modelo se implementará a través del Manual Técnico del Modelo Estándar de Control Interno, el cual hace parte integral del Decreto, y es de obligatorio cumplimiento y aplicación para las entidades del Estado.

Que el Decreto Único Reglamentario del Sector de la Función Pública 1083 de 2015 en el numeral 2.2.21.6.2 señala que el establecimiento y desarrollo del Sistema de Control Interno en los organismos y las entidades públicas que hacen parte del campo de aplicación de dicho decreto, será responsabilidad de la máxima autoridad de la entidad u organismo correspondiente y de los jefes de cada dependencia de las entidades y los organismos, así como de los demás funcionarios de la respectiva entidad.

Que el Código Disciplinario Único, Ley 734 de 2002, en su Artículo 34, Numeral 31 establece entre los Deberes de todo Servidor Público: "Adoptar el Sistema de Control Interno y la función independiente de Auditoría Interna de que trata la Ley 87 de 1993 y demás normas que la modifiquen o complementen".

Que se hace necesario incorporar y establecer todos los elementos enunciados del Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI 2014 al Sistema de Control Interno de la Entidad, con el fin de ajustarlo a las nuevas normas y tendencias de control, para que este sea efectivo, eficiente y eficaz.

Que en mérito de lo expuesto;

RESUELVE:

TÍTULO I.
SISTEMA DE CONTROL INTERNO.

ARTÍCULO 1. ADOPCIÓN DEL MODELO ESTÁNDAR DE CONTROL INTERNO – MECI. Adoptar para la Secretaría Distrital de Hacienda, la actualización del Modelo Estándar de Control Interno –MECI- y su estructura establecida en el Decreto 943 del 21 de mayo de 2014.

ARTÍCULO 2. DEFINICIÓN DE CONTROL INTERNO. De conformidad con el artículo 1º de la Ley 87 de 1993, se entiende por Control Interno el Sistema integrado por el esquema de organización y el conjunto de planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una Entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.

ARTÍCULO 3. PRINCIPIOS DEL SISTEMA DE CONTROL INTERNO. Los siguientes principios del MECI se constituyen en el fundamento y pilar básico que garantizan la efectividad del Sistema de Control Interno y deben ser aplicados en cada uno de los aspectos que enmarcan el modelo. En consecuencia, las organizaciones en la implementación o revisión o fortalecimiento continuo del Sistema de Control Interno deben incluir estos principios de manera permanente en su actuar:

3.1 Autocontrol: Capacidad que deben desarrollar todos y cada uno de los servidores públicos de la organización, independientemente de su nivel jerárquico, para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos de manera oportuna para el adecuado cumplimiento de los resultados que se esperan en el ejercicio de su función, de tal manera que la ejecución de los procesos, actividades y/o tareas bajo su responsabilidad, se desarrollen con fundamento en los principios establecidos en la Constitución Política.

3.2 Autorregulación: Capacidad de cada una de las organizaciones para desarrollar y aplicar en su interior

métodos, normas y procedimientos que permitan el desarrollo, implementación y fortalecimiento continuo del Sistema de Control Interno, en concordancia con la normatividad vigente.

3.3 Autogestión: Capacidad de toda organización pública para interpretar, coordinar, aplicar y evaluar de manera efectiva, eficiente y eficaz la función administrativa que le ha sido asignada por la Constitución, la ley y sus reglamentos. La organización deberá establecer políticas, acciones, métodos, procedimientos y mecanismos de prevención, control, evaluación y mejoramiento continuo que permitan dar cumplimiento a cada uno de estos principios, con el propósito de estructurar su Sistema de Control Interno que permita tener una seguridad razonable en el cumplimiento de sus objetivos.

Por otro lado, es importante que se contemplen los principios establecidos en el COSO (Committee of Sponsoring Organizations of the Treadway Commission, modelos internacionales de control interno en Estados Unidos), en su versión 2013, teniendo en cuenta que es uno de los referentes internacionales para la estructuración del presente Modelo, estos son:

- Demostrar compromiso con la integridad y valores éticos.
- Ejercer la responsabilidad de supervisión.
- Establecer estructura, autoridad y responsabilidad.
- Demostrar compromiso con la competencia.
- Cumplir con la rendición de cuentas.
- Objetivos específicos adecuados.
- Identificar y analizar riesgos.
- Evaluar riesgos de fraude significativos.
- Seleccionar y desarrollar actividades de control.
- Seleccionar y desarrollar controles generales de TI.
- Desplegar a través de políticas y procedimientos.
- Usar información relevante.
- Comunicar internamente.
- Comunicar externamente.
- Realizar evaluación continua.
- Evaluar y comunicar las deficiencias.

ARTÍCULO 4. OBJETIVO GENERAL DEL MECI. Proporcionar una estructura que especifique los elementos necesarios para construir y fortalecer el Sistema de Control Interno en las organizaciones obligadas por la Ley 87 de 1993, a través de un modelo que determine los parámetros de control necesarios para que al interior de las entidades se establezcan acciones, políticas, métodos, procedimientos, mecanismos de prevención, verificación y evaluación en procura del mejoramiento continuo de la administración pública.

ARTÍCULO 5. OBJETIVOS ESPECÍFICOS DEL SISTEMA DE CONTROL INTERNO. Los objetivos específicos que busca el Sistema de Control Interno son los siguientes:

Objetivos de control de cumplimiento:

a) Identificar, el marco legal que le es aplicable a la organización, con base en el principio de autorregulación.

b) Establecer las acciones que permitan a la organización garantizar razonablemente el cumplimiento de las funciones a su cargo, con base en el marco legal que le es aplicable (principio de autogestión).

c) Diseñar los procedimientos de verificación y evaluación que garanticen razonablemente el cumplimiento del marco legal aplicable (principio de autogestión).

Objetivos de Control de Planeación y Gestión:

Velar porque la entidad disponga de:

a) Objetivos, metas y planes de acción de acuerdo con la normatividad vigente.

b) Procesos y procedimientos necesarios para el cumplimiento de los objetivos institucionales, de acuerdo con su naturaleza, características y propósitos, procurando su simplificación y actualización de manera permanente.

c) Políticas operacionales y delimitación precisa de la autoridad y niveles de responsabilidad.

d) Mecanismos que protejan los recursos de la organización, buscando su adecuada administración ante posibles riesgos que lo afecten.

e) Estrategias que busquen crear conciencia en todos los servidores públicos sobre la importancia del control, mediante la generación, mantenimiento y mejora continua

de un entorno favorable que permita la aplicación de los principios del Modelo Estándar de Control Interno.

Objetivos de Control de Evaluación y Seguimiento:

a) Garantizar que el Sistema de Control Interno disponga de sus propios mecanismos de verificación y evaluación, que faciliten en tiempo real, realizar seguimiento a la gestión de la organización por parte de los diferentes niveles de autoridad, permitiendo acciones oportunas de prevención, corrección y de mejoramiento.

b) Garantizar la existencia de la función de evaluación independiente de las Oficinas de Control Interno, como mecanismo de verificación de la efectividad del Control Interno.

c) Propiciar el mejoramiento continuo del control y de la gestión de la organización, así como de su capacidad para responder efectivamente a los diferentes grupos de interés.

d) Asegurar que la entidad cuente con los procedimientos que permitan integrar las observaciones de los órganos de control a los planes de mejoramiento establecidos por la Organización.

e) Garantizar razonablemente la correcta evaluación y seguimiento de la gestión organizacional.

Objetivos de Control de Información y Comunicación:

Velar porque la entidad cuente con procedimientos necesarios para la generación de información y comunicación veraz y oportuna con el fin de:

a) Establecer los procedimientos que permitan la generación de la información y comunicación que por mandato legal, le corresponde suministrar a la organización a los órganos de control.

b) Garantizar la publicidad de la información que se genere al interior de la organización, y que se cuente con los medios de comunicación para su adecuada difusión.

c) Garantizar el suministro de información veraz y oportuna para el proceso de rendición de cuentas públicas, y que ésta sea comunicada de manera efectiva a través de los canales correspondientes.

d) Establecer los procedimientos, que garanticen la generación y registro de información oportuna y confiable necesaria para la toma de decisiones, el cumplimiento de la misión y la rendición de cuentas a la comunidad; y los mecanismos apropiados para su adecuada comunicación.

e) Diseñar los procedimientos que permitan llevar a cabo una efectiva comunicación interna y externa, a fin de dar a conocer la información que genera la organización pública de manera transparente, oportuna y veraz, garantizando que su operación se ejecute adecuada y convenientemente.

ARTÍCULO 6. ESTRUCTURA DE CONTROL. El propósito del Modelo Estándar de Control Interno MECI es proporcionar una serie de pautas o directrices dirigidas a controlar la planeación, gestión, evaluación y seguimiento en las entidades de la administración pública, facilitando el desarrollo del Sistema de Control Interno. Estructura, que permite ser adaptada de acuerdo con la naturaleza de las mismas, organización, tamaño y particularidades, con el fin de identificar claramente los roles y responsabilidades de quienes liderarán y participarán activamente en el proceso, con base en lo previsto en los Artículos 3º y 4º de la Ley 87 de 1993. La estructura del modelo es la siguiente:

1. MÓDULO DE CONTROL DE PLANEACIÓN Y GESTIÓN

1.1 COMPONENTE TALENTO HUMANO

1.1.1 Acuerdos, Compromisos y Protocolos éticos.

1.1.2 Desarrollo del Talento Humano

1.2 COMPONENTE DIRECCIONAMIENTO ESTRATÉGICO

1.2.1 Planes, Programas y Proyectos.

1.2.2 Modelo de Operación por Procesos

1.2.3 Estructura Organizacional

1.2.4 Indicadores de Gestión

1.2.5 Políticas de Operación

1.3 COMPONENTE ADMINISTRACIÓN DEL RIESGO

1.3.1 Políticas de Administración del Riesgo

1.3.2 Identificación del Riesgo

1.3.3 Análisis y Valoración del Riesgo

2. MÓDULO DE EVALUACIÓN Y SEGUIMIENTO

2.1 COMPONENTE AUTOEVALUACIÓN INSTITUCIONAL

2.1.1 Autoevaluación del Control y Gestión

2.2 COMPONENTE AUDITORÍA INTERNA

2.2.1 Auditoría Interna

2.3 COMPONENTE PLANES DE MEJORAMIENTO

2.3.1 Plan de Mejoramiento

3. EJE TRANSVERSAL: INFORMACIÓN Y COMUNICACIÓN

3.3.1 Información y Comunicación Externa

3.3.2 Información y Comunicación Interna

3.3.3 Sistemas de información y Comunicación

TÍTULO II

CAPÍTULO I
MÓDULOS, COMPONENTES Y ELEMENTOS
MÓDULO DE CONTROL DE PLANEACIÓN Y GESTIÓN.

ARTÍCULO 7. MÓDULO DE CONTROL DE PLANEACIÓN Y GESTIÓN. Dentro de este Módulo de Control, se encuentran los componentes y elementos que permiten asegurar de una manera razonable, que la planeación y ejecución de la misma en la entidad tendrán los controles necesarios para su realización. El objetivo principal de este módulo es introducir en la cultura organizacional el control a la gestión en los procesos de direccionamiento estratégico, misionales, de apoyo y de evaluación.

Este Módulo se estructura en tres Componentes: Talento Humano, Direccionamiento Estratégico y Administración del Riesgo, orientados a generar los estándares que permiten el desarrollo y afianzamiento de una cultura del control al interior de la entidad.

ARTÍCULO 8. COMPONENTE TALENTO HUMANO. Tiene como propósito establecer los elementos que le permiten a la entidad crear una conciencia de control y un adecuado control a los lineamientos y actividades tendientes al desarrollo del talento humano, influyendo de manera profunda en su planificación, gestión de operaciones y en los procesos de mejoramiento institucional, con base en el marco legal que le es aplicable a la entidad.

ARTÍCULO 9. ELEMENTOS DEL COMPONENTE TALENTO HUMANO. Está integrado por los siguientes Elementos de Control:

9.1 Acuerdos, Compromisos y Protocolos Éticos. Elemento que busca establecer un estándar de conducta de los servidores al interior de la entidad pública. A través de él se plantean las declaraciones explícitas que, en relación con las conductas de los servidores públicos, son acordadas en forma participativa para la consecución de los propósitos de la entidad, manteniendo la coherencia de la gestión con los principios consagrados en la Constitución Política, la ley y la finalidad social del Estado.

9.2 Desarrollo del Talento Humano. Elemento que permite controlar el compromiso de la entidad pública con el desarrollo de las competencias, habilidades, aptitudes e idoneidad del servidor público, a través de las políticas y prácticas de gestión humana que debe aplicar, las cuales deben incorporar los principios de justicia, equidad y transparencia al realizar los procesos de selección, inducción, formación, capacitación y evaluación del desempeño de los servidores públicos del Estado.

ARTÍCULO 10. COMPONENTE DIRECCIONAMIENTO ESTRATÉGICO. Conjunto de Elementos de Control que al interrelacionarse establecen el marco de referencia que orienta la entidad pública hacia el cumplimiento de su misión y objetivos institucionales, en procura de alcanzar su visión.

El Direccionamiento Estratégico define la ruta organizacional que debe seguir una entidad para lograr sus objetivos institucionales; requiere de revisiones periódicas para ajustarla a los cambios del entorno y al desarrollo de las funciones de la entidad; encauza su operación bajo los parámetros de calidad, eficiencia y eficacia requeridos por la ciudadanía y las partes interesadas de la entidad, así como los parámetros de control y evaluación a regir, haciéndose necesario, por lo tanto, establecer su composición a través de cinco elementos: Planes, Programas y Proyectos; Modelo de Operación por Procesos; Estructura Organizacional, Indicadores de Gestión; y Políticas de Operación.

ARTÍCULO 11. ELEMENTOS DEL COMPONENTE DIRECCIONAMIENTO ESTRATÉGICO. El Componente Direccionamiento Estratégico está integrado por los siguientes Elementos de Control:

11.1 Planes, Programas y Proyectos. Este elemento considera la planeación como un proceso dinámico y sistemático que le permite a las entidades públicas proyectarse a largo, mediano y corto plazo, de modo tal que se planteen una serie de programas, proyectos y actividades con la respectiva asignación de responsabilidades para su ejecución, que le sirvan para cumplir con su misión, visión y objetivos institucionales.

11.2 Modelo de Operación por Procesos. Mediante el control ejercido a través de la puesta en marcha de este elemento, las entidades podrán contar con una estandarización de las actividades necesarias para dar cumplimiento a su misión y objetivos, lo cual permite, que su operación se realice de manera continua, garantizando la generación de productos o servicios.

De esta manera se conforma el soporte de la operación de la entidad pública, armonizando con un enfoque sistémico su misión y visión institucional, orientada hacia una organización por procesos, los cuales en su interacción, interdependencia y relación causa-efecto garantizan razonablemente una ejecución eficiente, y el cumplimiento de sus objetivos.

11.3 Estructura Organizacional. Se considera como aquel aspecto de control que configura integral y articuladamente los cargos, las funciones, las relaciones y los niveles de responsabilidad y autoridad en la entidad pública, para dirigir y ejecutar los procesos y actividades de conformidad con su misión y su función constitucional y legal.

Se compone por la estructura u organización interna de la entidad, por su planta de personal y por el manual específico de funciones y competencias laborales; se define a partir de los procesos y procedimientos que conforman el Modelo de Operación y que permiten cumplir los objetivos institucionales. La parte que la dinamiza es el recurso humano, por lo tanto, el diseño de los perfiles de los cargos o empleos debe estar acorde con dicho Modelo.

11.4 Indicadores de Gestión. Son el conjunto de mecanismos necesarios para la evaluación de la gestión de toda entidad pública. Se definen como un conjunto de variables cuantitativas y/o cualitativas sujetas a la medición, que permiten observar la situación y las tendencias de cambio generadas en la entidad, en relación con el logro de los objetivos y metas previstos.

Los Indicadores son mecanismos que permiten controlar el comportamiento de factores críticos en la ejecución de los planes, programas, proyectos y de los procesos de la entidad.

A partir del Direccionamiento Estratégico y de los objetivos y resultados (productos/servicios) de los procesos y con la ayuda de la caracterización de los mismos, se diseñan los Indicadores, cuya medición periódica permite establecer el grado de avance o logro de los objetivos trazados y de los resultados esperados del proceso, en relación con los productos y servicios que éste genera para la ciudadanía o para las partes interesadas de la entidad.

11.5 Políticas de Operación. Este elemento es fundamental para el direccionamiento dado que facilita la ejecución de las operaciones internas a través de guías de acción para la implementación de las estrategias de ejecución de la entidad pública; define los límites y parámetros necesarios para ejecutar los procesos y actividades en cumplimiento de la función, los planes, los programas, proyectos y políticas de administración del riesgo y de otros procesos previamente establecidos por la entidad.

Las Políticas de Operación constituyen los marcos de acción necesarios para hacer eficiente la operación de los componentes Direccionamiento Estratégico, Administración del Riesgo y lo relacionado con la información y comunicación.

A través de estas políticas se establecen las acciones y los mecanismos asociados a los procesos; definiendo parámetros de medición del desempeño de los procesos y de los servidores que tienen bajo su responsabilidad su ejecución. Así mismo, facilitan el control administrativo y reducen la cantidad de tiempo que los administradores ocupan en tomar decisiones sobre asuntos rutinarios. Estas guías de acción son de carácter operativo, de aplicación cotidiana y dan seguridad y confianza a quien debe responder por la ejecución de procedimientos y actividades muy específicas y se encuentran inmersas en los procedimientos previamente definidos.

ARTÍCULO 12. COMPONENTE ADMINISTRACIÓN DEL RIESGO. Conjunto de elementos que le permiten a la entidad identificar, evaluar y gestionar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales.

La Administración del Riesgo se sirve de la planeación (misión, visión, establecimiento de objetivos, metas, factores críticos de éxito), del campo de aplicación (procesos, proyectos, sistemas de información), del Componente Direccionamiento Estratégico y todos sus elementos. Su mirada sistémica contribuye a que la entidad no sólo garantice la gestión institucional y el logro de los objetivos sino que fortalece el ejercicio del Control Interno en las entidades de la Administración Pública.

ARTÍCULO 13. ELEMENTOS DEL COMPONENTE ADMINISTRACIÓN DEL RIESGO. Está integrado por los siguientes Elementos de Control:

13.1 POLÍTICAS DE ADMINISTRACIÓN DEL RIESGO. Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de los mismos, permiten tomar decisiones adecuadas y fijar los lineamientos, que van a transmitir la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad.

13.2 IDENTIFICACIÓN DEL RIESGO.

13.2.1 Contexto Estratégico. Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución. Las situaciones del entorno o externas pueden ser de carácter social, cultural, económico, tecnológico, político, ambiental y legal, bien sea internacional, nacional o regional según sea el caso de análisis. Las situaciones internas están relacionadas con la estructura, cultura organizacional, el modelo de operación, el cumplimiento de los Planes, Programas y Proyectos, los sistemas de información, los procesos y procedimientos y los recursos humanos y económicos con los que cuenta una entidad, entre otros.

13.2.2 Identificación de Riesgos. La identificación de los riesgos se realiza a nivel del Componente de Direccionamiento Estratégico, identificando las causas con base en los factores internos o externos a la entidad, que pueden ocasionar riesgos que afecten el logro de los objetivos.

13.3 ANÁLISIS Y VALORACIÓN DEL RIESGO.

13.3.1 Análisis del Riesgo. El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias; éste último aspecto puede orientar la clasificación del riesgo con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

El análisis del riesgo depende de la información obtenida en la fase de identificación de riesgos. Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados: Probabilidad e Impacto.

13.3.2 Valoración del Riesgo. La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas. Para adelantar esta etapa se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones.

CAPÍTULO II
MÓDULO CONTROL DE EVALUACIÓN Y SEGUIMIENTO

ARTÍCULO 14. MÓDULO CONTROL DE EVALUACIÓN Y SEGUIMIENTO. Dentro del proceso de mejoramiento continuo en la entidad, este módulo considera aquellos aspectos que permiten valorar en forma permanente la efectividad del Control Interno de la entidad pública; la eficiencia, eficacia y efectividad de los procesos; el nivel de ejecución de los Planes, Programas y Proyectos, los resultados de la gestión, con el propósito de detectar desviaciones, establecer tendencias y generar recomendaciones para orientar las acciones de mejoramiento de la Organización Pública.

Los instrumentos y herramientas de gestión y de control de la entidad requieren evaluación y seguimiento, es decir, un proceso que verifique el nivel de desarrollo del Sistema de Control Interno y de la gestión de la entidad. Esto se consigue mediante actividades de supervisión continua, evaluaciones periódicas o una combinación de ambas cosas.

Este Módulo se estructura bajo tres Componentes: Autoevaluación Institucional, Auditoría Interna y Planes de Mejoramiento.

ARTÍCULO 15. COMPONENTE DE AUTOEVALUACIÓN INSTITUCIONAL. Le permite a cada responsable del proceso, programas y/o proyectos y sus funcionarios medir la efectividad de sus controles y los resultados de la gestión en tiempo real, verificando su capacidad para cumplir las metas y los resultados a su cargo y tomar las medidas correctivas que sean necesarias para el cumplimiento de los objetivos previstos por la entidad.

La autoevaluación se convierte en un proceso periódico, en el cual participarán los servidores que dirigen y ejecutan los procesos, programas y/o proyectos, según el grado de responsabilidad y autoridad para su operación y toma como base los criterios de evaluación incluidos en la definición de cada uno de los elementos del control interno, así como la existencia de controles que se dan en forma espontánea en la ejecución de las operaciones y en la toma de decisiones.

15.1 Autoevaluación del Control y Gestión. La Autoevaluación, comprende el monitoreo que se le debe realizar a la operación de la entidad a través de la medición de los resultados generados en cada proceso, procedimiento, proyecto, plan y/o programa, teniendo en cuenta los indicadores de gestión, el manejo de los riesgos, los planes de mejoramiento, entre otros. De esta manera, se evalúa su diseño y operación en un período de tiempo determinado, por medio de la medición y el análisis de los indicadores, cuyo propósito fundamental será la de tomar las decisiones relacionadas con la corrección o el mejoramiento del desempeño.

En ese orden de ideas, lo que se busca es que cada líder de proceso con su equipo de trabajo verifique el desarrollo y cumplimiento de sus acciones, que contribuirán al cumplimiento de los objetivos institucionales.

ARTÍCULO 16. COMPONENTE DE AUDITORÍA INTERNA. Este componente busca verificar la existencia, nivel de desarrollo y el grado de efectividad del Control Interno en el cumplimiento de los objetivos de la entidad pública. La Oficina de Control Interno es la responsable de realizar la Evaluación del Sistema de Control Interno a través de su rol de evaluador independiente, observando siempre un criterio de independencia frente a la operación y la autonomía de los actos de la administración.

Igualmente, el (la) Jefe(a) de la Oficina de Control Interno, deberá presentar informes a la Dirección y al Comité de Coordinación de Control Interno en la entidad, haciendo énfasis en la existencia, funcionamiento y coherencia de los componentes y elementos que lo conforman, con el propósito de que allí se evalúen, decidan y adopten oportunamente las propuestas de mejoramiento del Sistema.

16.1 Auditoría Interna. Es la herramienta que debe usarse para el seguimiento del Sistema de Control Interno. La Oficina de Control Interno debe auditar los procesos, con el fin de verificar su gestión, es decir que se esté dando cumplimiento a lo programado. También analiza las debilidades y fortalezas del control, así como el desvío de los avances de las metas y objetivos trazados, influyentes en los resultados y operaciones propuestas en la entidad.

La auditoría por parte de la Oficina de Control Interno debe estar acorde con la planeación estratégica de la entidad, estableciendo prioridades frente a la programación de auditorías, y su alcance, en consideración de los planes de acción de cada vigencia y la disponibilidad de recursos para el ejercicio auditor.

El objetivo de la auditoría interna es hacer recomendaciones imparciales a partir de evidencias sobre el grado de cumplimiento de los objetivos, los planes, los programas, proyectos y procesos, así como sobre irregularidades y errores presentados en la operación de la entidad, apoyando a la Dirección en la toma de decisiones necesarias para corregir las desviaciones, sugiriendo la realización de las acciones de mejoramiento correspondientes.

Las Auditorías deben realizarse con base en un programa anual de auditoría interna aprobado por el Comité de Coordinación de Control Interno, y se entiende como el conjunto de auditorías a realizarse en un periodo determinado, documento de trabajo que se constituye en la guía para la ejecución del plan de las mismas en el que se detallan las actividades para su realización por parte de la Oficina de Control Interno.

No obstante lo anterior, la Oficina de Control Interno puede realizar Auditorías internas a procesos, actividades u operaciones no contempladas en el Programa Anual de Auditoría, cuando lo determine el representante legal o las condiciones así lo ameriten.

El ejercicio de auditoría se cierra en la validación de la implementación de las acciones propuestas por parte de los responsables en los planes de acción en las fechas establecidas y valorar su efectividad. Para ello, El Jefe de Control Interno debe establecer un proceso de seguimiento para vigilar y asegurar que las acciones de la dirección hayan sido implementadas eficazmente o que la alta dirección haya aceptado el riesgo de no tomar medidas.

ARTÍCULO 17. COMPONENTE PLANES DE MEJORAMIENTO. Acciones necesarias para corregir las desviaciones encontradas en el Sistema de Control Interno y en la gestión de los procesos, como resultado de la Autoevaluación realizada por cada líder de proceso, de la Auditoría Interna de la Oficina de Control Interno y de las observaciones formales provenientes de los Órganos de Control.

El Plan de Mejoramiento, es el instrumento que recoge y articula todas las acciones prioritarias que se emprenderán para mejorar aquellas características que tendrán mayor impacto con los resultados, con el logro de los objetivos de la entidad y con el plan de acción institucional, mediante el proceso de evaluación.

El objetivo primordial del Plan de Mejoramiento es promover que los procesos internos de las entidades se desarrollen en forma eficiente y transparente a través de la adopción y cumplimiento de las acciones correctivas o de la implementación de metodologías orientadas al mejoramiento continuo.

17.1 Plan de Mejoramiento. Este tipo de plan integra las acciones de mejoramiento que buscan fortalecer el desempeño, misión y objetivos institucionales, teniendo en cuenta, entre otros aspectos, los compromisos adquiridos con los organismos de control fiscal, de control político y con las partes interesadas, así como la evaluación de la Oficina de control Interno y las autoevaluaciones realizadas. El Plan de Mejoramiento Institucional recoge las recomendaciones y análisis generados en el desarrollo del Componente de Auditoría Interna y las observaciones del órgano de Control Fiscal.

En él se deben integrar las acciones de mejoramiento que tienden a fortalecer tanto a los procesos como a los servidores públicos y a la institución misma, abordando de esta manera planes de mejoramiento según sea el resultado de las evaluaciones o auditorías. Su contenido debe contemplar las observaciones y el resultado del análisis de las variaciones presentadas entre las metas esperadas y los resultados obtenidos

a nivel entidad, por proceso o individual; así como la definición de su objetivo, alcance, acciones a implementar, metas, la asignación de los responsables y de los recursos requeridos, el tiempo de ejecución y las acciones de seguimiento necesarias para verificar su cumplimiento.

CAPÍTULO III.
EJE TRANSVERSAL INFORMACIÓN Y COMUNICACIÓN

ARTÍCULO 18. EJE TRANSVERSAL INFORMACIÓN Y COMUNICACIÓN. Este eje es transversal a los Módulos de Control del Modelo, dado que en la práctica las organizaciones y entidades lo utilizan durante toda la ejecución del ciclo PHVA; de tal manera, que complementa y hace parte esencial de la implementación y fortalecimiento de los Módulos en su integridad.

La Información y Comunicación tiene una dimensión estratégica fundamental por cuanto vincula a la entidad con su entorno y facilita la ejecución de sus operaciones internas, dándole al usuario una participación directa en el logro de los objetivos. Es un factor determinante, siempre y cuando se involucre a todos los niveles y procesos de la organización.

Para su desarrollo se deben diseñar políticas, directrices y mecanismos de consecución, captura, procesamiento y generación de datos al interior y en el entorno de cada entidad, que satisfagan la necesidad de divulgar los resultados, de mostrar mejoras en la gestión administrativa y procurar que la información y la comunicación de la entidad y de cada proceso, sea adecuada a las necesidades específicas de la ciudadanía y de las partes interesadas.

A través de este eje se espera mejorar la transparencia frente a la ciudadanía por medio de la rendición de cuentas a la comunidad y el cumplimiento de las obligaciones frente a las necesidades de los usuarios. Para obtener los beneficios proporcionados por la Información y la Comunicación, es necesario conocer las necesidades de la ciudadanía, de las partes interesadas y las de la entidad, identificar sus fuentes y definir una estructura para su procesamiento y socialización.

ARTÍCULO 19. ELEMENTOS DEL EJE TRANSVERSAL INFORMACIÓN Y COMUNICACIÓN. Está integrado por los siguientes:

19.1 Información y Comunicación Externa. Hace referencia a todos los datos que provienen o son generados por el cliente y/o usuario externo. Es a través de la cual la organización está en contacto directo con la ciudadanía, los proveedores, los contratistas, las entidades reguladoras, las fuentes de financiación y otros organismos; o en contacto indirecto pero que afecta su desempeño, como el ambiente político, las tendencias sociales, las variables económicas, el avance tecnológico, entre otros.

Es a través de este mecanismo que se garantiza la difusión de información de la entidad pública sobre su funcionamiento, gestión y resultados en forma amplia y transparente hacia los diferentes grupos de interés.

Este elemento debe garantizar que efectivamente la interacción de la entidad con las partes interesadas y la ciudadanía estén enfocadas a la construcción de lo público y a la generación de confianza, mediante la definición de políticas de comunicación, participación ciudadana, de comunicación de gestión y resultados y la formulación de parámetros que orienten el manejo de la información.

La administración de las quejas y los reclamos constituye un medio de información directo de la entidad con la ciudadanía y las partes interesadas, permitiendo registrar, clasificar y realizar seguimiento al grado de cumplimiento de los intereses de los beneficiarios; estas son fuente de información sobre los incumplimientos institucionales y a través de éstos se puede conocer su origen, alcance, gravedad, impacto y frecuencia.

La Comunicación externa debe trabajarse como un eje estratégico transversal a la estructura organizacional con el fin de darle cumplimiento al principio constitucional de publicidad y transparencia. En este sentido, se hace necesario construir el concepto como algo inherente a la cultura organizacional y no solamente como una práctica focalizada de manera exclusiva en la difusión de mensajes informativos; entendiendo, que la comunicación es la forma concreta de cómo se expresa la cotidianidad de la cultura de la entidad.

19.2 Información y Comunicación Interna. Conjunto de datos que se originan del ejercicio de la función de la entidad y se difunden en su interior, para una clara identificación de los objetivos, las estrategias, los planes, los programas, los proyectos y la gestión de operaciones hacia los cuales se enfoca el accionar de la entidad.

Para el óptimo funcionamiento de este eje, debe garantizarse su registro y/o divulgación oportuna, exacta y confiable, en procura de la realización efectiva y eficiente de las operaciones, soportar la toma de decisiones y permitir a los funcionarios un conocimiento más preciso y exacto de la entidad.

Es importante fomentar en los servidores un sentido de pertenencia, una cultura organizacional en torno a una gestión ética, eficiente y eficaz que proyecte su compromiso con la rectitud y la transparencia, como gestores y ejecutores de lo público, contribuyendo al fortalecimiento continuo del clima laboral.

En la Entidad la información y la comunicación fluyen en varias direcciones lo que conduce a la necesidad de establecer estrategias comunicativas concretas, que incidan en los flujos de comunicación descendente, ascendente y transversal.

19.3 Sistemas de información y Comunicación. Conjunto de procedimientos, métodos, recursos (humanos y tecnológicos) e instrumentos utilizados por la entidad pública, para garantizar tanto la generación y recopilación de información; como la divulgación y circulación de la misma, hacia los diferentes grupos de interés, con el fin de hacer más eficiente la gestión de operaciones en la entidad pública.

A partir de las políticas fijadas en materia de Información y Comunicación, la entidad debe establecer mecanismos internos y externos para recopilar y/o socializar la información generada.

Para que la ejecución de estos Sistemas se desarrolle de manera eficaz, eficiente y efectiva, deben nutrirse de un componente físico (hardware), de programas, información y conocimiento (software), de recurso humano, y de datos a procesar o difundir.

El Componente Físico (hardware) es el medio utilizado para realizar la captura, procesamiento, almacenamiento, difusión y divulgación de la información, es deseable que se utilicen las tecnologías de punta para lograr una gestión oportuna y eficiente en almacenaje y procesamiento de datos y en la ampliación de la cobertura de información a difundir.

Los programas, información y conocimiento (software) son el conjunto ordenado de instrucciones, información y base de conocimientos dadas al computador y que son requeridas para el trabajo de estos sistemas.

El Recurso Humano administra, opera, alimenta y utiliza los Sistemas de Información.

Los Datos se constituyen como insumos primarios de los Sistemas de Información; para ello se deben identificar las fuentes para su obtención, los objetivos de difusión, los medios de captura y resulta de gran importancia su validación antes, durante y después de la captura y/o divulgación, para cumplir con los requisitos mínimos de calidad, cantidad, oportunidad y forma de presentación.

Es realmente importante que la Entidad cuente con un Plan de Comunicaciones, dicho plan define los medios de comunicación de carácter permanente para que la ciudadanía y partes interesadas conozcan lo que se planea y se ejecuta, y puedan realizar el seguimiento correspondiente.

Además, en este plan se establecen los responsables, tiempos, manejo de los sistemas y los medios que se utilizarán para comunicar tanto a los usuarios internos como a los externos, la información que la entidad desee publicar.

TÍTULO III.

CAPÍTULO I
ROLES Y RESPONSABILIDADES.

ARTÍCULO 20. ROLES Y RESPONSABILIDADES DEL COMITÉ DE COORDINACIÓN DE CONTROL INTERNO. Además de los señalados en el Decreto 1826 de 1994 o aquel que lo modifique o sustituya, el Comité de Coordinación de Control Interno cumplirá los siguientes roles y responsabilidades:

a) Recomendar pautas para la determinación, implantación, adaptación, complementación y mejoramiento permanente del Sistema de Control Interno, de conformidad con las normas vigentes y las características propias de cada organismo o entidad.

b) Estudiar y revisar la evaluación del Sistema de Control Interno.

c) Aprobar el plan de acción propuesto por el Equipo MECI para la implementación y fortalecimiento del Modelo.

d) Aprobar el Programa Anual de Auditoría presentado por la Oficina de Control Interno

e) Recomendar acciones de mejora para la eficiencia, eficacia y efectividad del Sistema.

f) Propender por una adecuada implementación de procedimientos de control interno para todos los riesgos significativos, independientemente de su naturaleza (operativa, de cumplimiento, financieros, fiscales).

ARTÍCULO 21. RESPONSABILIDAD DEL SECRETARIO DISTRITAL DE HACIENDA. El Secretario Distrital de Hacienda, es el responsable de orientar, establecer y desarrollar el Sistema de Control Interno en la Entidad.

El establecimiento y desarrollo del Sistema de Control Interno en los organismos y entidades públicas a que hace referencia el artículo 5 de la Ley 87 de 1993, será responsabilidad del Secretario Distrital de Hacienda, de los directores, jefes de oficina, subdirectores; así como de los demás funcionarios de la Secretaría de Hacienda.

ARTÍCULO 22. REPRESENTANTE DE LA DIRECCIÓN. Para efectos de garantizar la operacionaliza-

ción de las acciones necesarias para el desarrollo, implementación y mejoramiento continuo del Sistema de Control Interno basado en el Modelo Estándar de Control Interno, se designa al Jefe de la Oficina Asesora de Planeación quien actuará bajo las directrices establecidas por el Comité de Coordinación de Control Interno y el representante legal.

De acuerdo con el Decreto 943 del 21 de Mayo de 2014, o la norma que lo sustituya o modifique, el directivo designado para la implementación y fortalecimiento continuo del Modelo Estándar de Control Interno debe cumplir con los siguientes roles y responsabilidades:

a) Orientar, dirigir y coordinar el proyecto de implementación y/o fortalecimiento continuo del Modelo de acuerdo a lo dispuesto por el Comité de Coordinación de Control Interno y el Secretario Distrital de Hacienda.

b) Asegurar que se desarrollen a cabalidad cada una de las etapas previstas para el fortalecimiento continuo del Modelo en la entidad.

c) Informar a la alta dirección sobre la planificación y avances de la etapa implementación y fortalecimiento continuo del Modelo.

d) Dirigir y coordinar las actividades del Equipo MECI.

e) Coordinar con los directivos o responsables de cada área o proceso las actividades que requiere realizar el Equipo MECI, en armonía y colaboración con los servidores de dichas áreas.

f) Someter a consideración del Comité de Coordinación de Control, la aprobación y seguimiento de las actividades planeadas para el fortalecimiento continuo del MECI, sugiriendo correctivos donde se requiera.

ARTÍCULO 23. ROLES Y RESPONSABILIDADES DEL EQUIPO MECI. El equipo MECI cumplirá los siguientes roles y responsabilidades:

a) Apoyar el proceso de implementación y fortalecimiento continuo del Modelo bajo las orientaciones del representante de la dirección.

b) Capacitar a los servidores de la entidad en el Modelo e informar los avances en la implementación y fortalecimiento continuo del mismo.

c) Asesorar a las áreas de la entidad en la implementación y fortalecimiento continuo del Modelo.

d) Trabajar en coordinación con los servidores designados por las otras áreas en aquellas actividades requeridas para la implementación y fortalecimiento continuo del Modelo.

e) Revisar, analizar y consolidar la información para presentar propuestas para la implementación y fortalecimiento continuo del Modelo al representante de la dirección, para su aplicación.

f) Realizar seguimiento a las acciones de implementación y fortalecimiento continuo e informar los resultados al representante de la dirección, para la toma de decisiones.

ARTÍCULO 24. ROL DE LA OFICINA DE CONTROL INTERNO. La función de la Oficina de Control Interno debe ser considerada como un proceso retroalimentador a través de la actividad independiente y objetiva de evaluación y asesoría que contribuya de manera efectiva al mejoramiento continuo de los procesos de Administración del riesgo, Control y Gestión de la entidad.

En los diferentes roles de la gestión, la Oficina de Control Interno debe guardar la debida independencia para garantizar la objetividad de sus evaluaciones y seguimientos, por lo tanto no deben hacer parte en los procesos administrativos de la entidad, ni intervenir en el desarrollo de procesos internos.

De acuerdo con el artículo 3 del Decreto 1537 de 2001 o aquel que lo sustituya o modifique, los principales roles que deben desempeñar las Oficinas de Control Interno, dentro de las organizaciones públicas, se enmarca en los cinco tópicos a saber:

a) Evaluación y Seguimiento a la Gestión Institucional: Su propósito es emitir un juicio profesional acerca del grado de eficiencia y eficacia de la gestión de la entidad, para asegurar el adecuado cumplimiento de los fines institucionales.

b) Asesoría y acompañamiento: Promover el mejoramiento continuo de los procesos de la entidad asesorando a la Alta Dirección, en la búsqueda del cumplimiento de los objetivos y los propósitos institucionales.

c) Valoración del riesgo: Asesorar y capacitar a la alta dirección y a los líderes de los procesos en la metodología para su gestión, y

verificará que los controles existentes sean efectivos para minimizar la probabilidad e impacto de la ocurrencia de los mismos.

d) Relación con entes externos: Su propósito es facilitar el cumplimiento de las exigencias de Ley o las solicitudes formales realizadas por los entes externos.

e) Fomento de la Cultura del Control: Tiene como objetivo elaborar y construir herramientas e instrumentos orientados a sensibilizar e interiorizar el ejercicio del autocontrol y la autoevaluación, como un hábito de mejoramiento personal y organizacional.

ARTÍCULO 25. FUNCIONES DE LA OFICINA DE CONTROL INTERNO. De acuerdo con el artículo 230 del Decreto 019 de 2012, las funciones, competencias o responsabilidades de las Oficinas de Control Interno y de los Jefes de Control Interno son las definidas en la Ley 87 de 1993, o las leyes que las sustituyan o modifiquen. Además, de las contenidas en el manual de funciones de la Secretaría Distrital de Hacienda.

El Jefe de Control Interno solo estará obligado a presentar los informes y realizar los seguimientos previstos en la Ley, normas con fuerza de Ley y las que le asigne el Presidente de la República para los Jefes de Control Interno de la Rama Ejecutiva del Orden Nacional, y los solicitados por el Alcalde Mayor de Bogotá D. C., los organismos de control, la Contaduría General de la Nación y el Consejo Asesor del Gobierno Nacional en materia de Control Interno.

ARTÍCULO 26. ROL DE SERVIDORES PÚBLICOS Y/O PARTICULARES QUE EJERCEN FUNCIONES PÚBLICAS. Los servidores públicos y/o particulares que ejercen funciones públicas, son responsables por la operatividad eficiente de los procesos, actividades y tareas a su cargo, y por la supervisión continua a la eficacia de los controles integrados.

Así mismo, de desarrollar la autoevaluación permanente a los resultados de su labor, como parte del cumplimiento de las metas previstas por la dependencia o unidad administrativa a la cual pertenecen.

Igualmente, deben tomar acciones que permitan realizar el ejercicio del autocontrol en sus puestos de trabajo, con el fin de detectar las desviaciones que puedan entorpecer el desarrollo de sus funciones, como parte fundamental y eje principal de la correcta implementación y fortalecimiento continuo y permanente del Sistema de Control Interno.

ARTÍCULO 27. COMITÉ DE COORDINACIÓN DE CONTROL INTERNO. La Secretaría Distrital de Hacienda, tendrá un Comité de Coordinación del Sistema de Control Interno, de acuerdo con lo establecido en el artículo 13 de la Ley 87 de 1993. Deberá adoptar su reglamento interno y cumplir con las siguientes funciones:

27.1 Recomendar pautas para la determinación, implantación, adaptación, complementación y mejoramiento permanente del Sistema de Control Interno, de conformidad con las normas vigentes y las características propias de la Entidad.

27.2 Recomendar prioridades para adopción, adaptación, adecuado funcionamiento y optimización de los sistemas de información gerencial, estadística, financiera, de planeación y de evaluación de procesos, así como para la utilización de indicadores de gestión generales y por áreas.

27.3 Estudiar y revisar la evaluación al cumplimiento de los planes, sistemas de control y seguridad interna y los resultados obtenidos por las dependencias.

ARTÍCULO 28. CONFORMACIÓN El Comité de Coordinación del Sistema de Control Interno, estará conformado por:

a. Secretario Distrital de Hacienda, quien lo preside.

b. Subsecretario General, quien en ausencia del Secretario preside el Comité.

c. Un Director, designado por los Directores que participan en el Comité Directivo de la Entidad.

d. Jefe Oficina Asesora de Planeación

e. Jefe Oficina de Control Interno.

Las demás personas que en concepto del Comité deban participar en la sesión, con voz pero sin voto.

El Jefe de Oficina de Control Interno es el Secretario Técnico del Comité de Coordinación del Sistema de Control Interno.

ARTÍCULO 29. SESIONES. El Comité Coordinador del Sistema de Control Interno se reunirá, por lo menos una vez cada semestre o cuando las necesidades del servicio lo requieran, previa citación por parte del Secretario Distrital de Hacienda o por el Jefe de la Oficina de Control Interno.

La convocatoria a sesiones se hará mediante citación la cual contendrá la fecha, hora y lugar donde se llevará a cabo la sesión.

ARTÍCULO 30. ASISTENCIA. La asistencia al Comité de Coordinación de Control Interno es de carácter

obligatoria, salvo en el caso de quien lo preside.

ARTÍCULO 31. QUÓRUM. El Comité tendrá Quórum deliberatorio y decisorio con la mitad más uno de sus miembros.

ARTÍCULO 32. INFORMES. De las reuniones del Comité se levantarán actas sobre los temas tratados, decisiones, compromisos, recomendaciones y las responsabilidades asignadas con los plazos previstos para ellas.

PARÁGRAFO. Las decisiones, compromisos y recomendaciones adoptadas por el Comité de Coordinación de Control Interno, consignadas en las actas, serán de obligatorio cumplimiento.

TÍTULO IV
DISPOSICIONES VARIAS.

ARTÍCULO 33. NORMAS DE CONTROL INTERNO CONTABLE. La Secretaría Distrital de Hacienda, se acogerá a la reglamentación que sobre políticas, métodos y procedimientos de Control Interno Contable, expida la Contaduría General de la Nación a fin de garantizar la razonabilidad, confiabilidad y oportunidad de los estados e informes contables y la utilidad social de la información financiera, económica y social que debe generar la Entidad Pública para sí misma, los diferentes grupos de interés externos y para garantizar el cumplimiento de obligaciones de información.

ARTÍCULO 34. MÉTODOS Y PROCEDIMIENTOS DE CONTROL INTERNO. La Secretaría Distrital de Hacienda en cumplimiento de las normas vigentes y de la presente Resolución, expedirá a través de un acto administrativo, las políticas, directrices, métodos y procedimientos específicos mediante los cuales deberán implementarse los diferentes módulos, componentes y elementos de control del Sistema de Control Interno, así como los procedimientos, guías, formatos, y métodos para su evaluación, elaboración, ejecución de los planes de mejoramiento y cumplimiento de obligaciones de información y documentación. Para estos efectos adoptará los métodos y procedimientos conforme a las directrices emanadas del Departamento Administrativo de la Función Pública para las entidades del Estado, de conformidad con el artículo 3 del Decreto 943 del 21 de mayo de 2014, compilado por el Decreto Único Reglamentario del Sector de la Función Pública 1083 de 2015.

ARTÍCULO 35. ÁMBITO DE APLICACIÓN Y REGULACIÓN: La presente Resolución será aplicable a todas las áreas organizacionales de la Secretaría de Hacienda y su reglamentación de orden operativo se realizará por medio de actos administrativos por los cuales se adopten los conceptos, metodologías, guías e instrumentos de aplicación así como los manuales e instrumentos que le sean inherentes.

ARTÍCULO 36. VIGENCIA Y DEROGATORIAS. El presente Resolución rige a partir de la fecha de su publicación y deroga las normas que le sean contrarias, en especial las Resoluciones DSH-000209 de 2005 y SDH -000003 del 8 de enero de 2015

PUBLÍQUESE Y CÚMPLASE.

Dada en Bogotá, D. C., a los treinta y un (31) días del mes de diciembre de dos mil quince (2015).

JOSÉ ALEJANDRO HERRERA LOZANO
Secretario Distrital de Hacienda (E)

EMPRESA DE TRANSPORTE DEL TERCER MILENIO "TRANSMILENIO S.A."

Resolución Número 004
(Enero 4 de 2016)

"Por la cual se modifica la Resolución 078 del 31 de Julio de 2000, con el fin de actualizar el Manual de Procedimientos de la Empresa de Transporte del Tercer Milenio TRANSMILENIO S.A".

EL JEFE DE LA OFICINA ASESORA DE PLANEACIÓN DE LA EMPRESA DE TRANSPORTE DEL TERCER MILENIO "TRANSMILENIO S.A.", en ejercicio de sus facultades delegadas mediante la Resolución 278 de Julio de 2012, y

CONSIDERANDO:

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

Que cumpliendo con lo ordenado en el parágrafo único del artículo 1º de la Ley 87 de 1993, se adoptó el Manual de Procedimientos de TRANSMILENIO S.A., según Resolución 078 de 2000.

Que mediante Acuerdo 002 de 2011 de la Junta Directiva de la EMPRESA DE TRANSPORTE DEL TERCER MILENIO – TRANSMILENIO S.A." se determinaron las funciones de las dependencias.

Que siendo TRANSMILENIO S.A., el ente gestor del Sistema Integrado de Transporte Público, considera necesario actualizar el Manual de Procedimientos de la Entidad, con el objeto de ajustarlo a los nuevos parámetros, necesidades y desarrollo del Sistema TransMilenio y fijar las directrices y lineamientos del Personal de la Entidad y de los actores que intervienen en la Operación.

Que la Norma ISO-IEC 27001 establece los requisitos para la implementación de un Sistema de Gestión de seguridad de la información y la ISO-IEC 27002 establece el código de buenas prácticas para la gestión de la seguridad de la información.

Que mediante el Decreto 652 de 2011 se adopta la Norma Técnica Distrital del Sistema Integrado de Gestión NTD-SIG 001:2011, estableciendo que el Subsistema de Gestión de Seguridad de la información (SGSI) es un elemento constitutivo de él.

Que la Circular 007 de 2015 emitida por la Alta Consejería Distrital de TIC`s de la Alcaldía Mayor de Bogotá, solicitan el cumplimiento de los requisitos del Sistema de Gestión de la Seguridad de la información y de la Estrategia de Gobierno en Línea.

Que en mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: Modificar las Resolución 078 del 31 de Julio de 2000, con el fin de actualizar el Manual de Procedimientos de la Empresa de Transporte del Tercer Milenio TRANSMILENIO S.A en lo que corresponde a la incorporación del siguiente documento:

Código	Versión	Nombre
M-DT-001	0	Manual de Políticas de Seguridad de la Información

ARTÍCULO SEGUNDO: La presente Resolución rige a partir de su publicación en la Gaceta Distrital y deroga en su totalidad los documentos que le sean contrarios, los demás procedimientos no modificados con la presente resolución continúan vigentes.

PUBLÍQUESE Y CÚMPLASE.

Dada en Bogotá, a los cuatro (4) días del mes de enero de dos mil dieciséis (2016).

ANDRÉS ARBOLEDA SALAZAR
Jefe Oficina Asesora de Planeación

TRANSMILENIO	**TÍTULO:** **MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**			**ALCALDÍA MAYOR DE BOGOTA**
	Código **M-DT-001**	**Versión** **0**	**Fecha** **Diciembre 2015**	

TABLA DE CONTENIDO

1 OBJETIVO

2 ALCANCE

3 RESPONSABLES

4 DOCUMENTOS DE REFERENCIA

5 DEFINICIONES

6 CONDICIONES GENERALES

7 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

ELABORÓ:	APROBÓ:	
		Diciembre de 2015
		Página 1 de 64
PROFESIONAL ESPECIALIZADO 06 SEGURIDAD DE LA INFORMACION	**DIRECTOR TÉCNICO DE TIC´s**	

1 OBJETIVO

El propósito de este documento es comunicar los lineamientos establecidos por la Alta Dirección de TRANSMILENIO S.A. para la gestión de la seguridad de la Información, los cuales se constituyen como guía para la ejecución de las actividades de la Entidad, de forma que mitiguen los riesgos de pérdida de confidencialidad, disponibilidad e integridad de la información.

2 ALCANCE

Este Manual cubre las políticas de Seguridad de la Información de TRANSMILENIO S.A.

Este Manual de Políticas aplica para todos los funcionarios, terceros y contratistas que desarrollen labores de asesoría, consultoría, implementación, soporte o mantenimiento y demás personas que sin ser de planta de la entidad, tienen un nivel de vinculación, brindan algún tipo de servicio dentro de las instalaciones o tienen acceso a información de TRANSMILENIO S.A

3 RESPONSABLES

El responsable por la elaboración y mantenimiento de este documento es el Profesional Especializado (06) de Seguridad de la Información de la Dirección de Tecnología de la Información y por su estricto cumplimiento, implementación y mantenimiento el Director Técnico de Tecnología de la Información.

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

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

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.
- **Ley 23 de 1982:** Ley emitida por el Congreso de la República de Colombia, acerca de la Propiedad Intelectual y los Derechos de autor.
- **Ley 734 de 2002.** *"Por la cual se expide el Código Disciplinario Único".*
- **Ley 527 de 1999:** por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
- **Ley 603 del 2000:** Ley emitida por el Congreso de la República de Colombia, acerca del cumplimiento de las Normas de Propiedad Intelectual
- **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 1266 de 2008:** Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contendida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales, habeas data
- **Ley 1341 de 2009:** Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones acerca de la protección de los derechos de los usuarios.
- **Ley 1712 de 2014:** Ley de Transparencia Ley y del Derecho de Acceso a la Información Pública Nacional.
- **Reglamento Interno de trabajo de TRANSMILENIO S.A.** documento que se establece como norma reguladora de las relaciones internas de la Empresa con los trabajadores adscritos a ella.
- **Decreto 2573 de 2014:** Por el cual se reglamentan los lineamientos generales de la estrategia de Gobierno en Línea.
- **Decreto 1360 de 1989:** Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor. Decreto 460 de 1995: Por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal
- **Decreto 162 de 1995:** Por el cual se reglamenta en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos
- **Sentencia T-444 de 1992.** Recolección de información por parte de los Organismos de Seguridad del Estado.
- **ISO-IEC-27000:** *"Vocabulario Sistema de Gestión de la Seguridad de la Información"*.
- **ISO-IEC-27001:** *"Por la cual se establecen los requisitos para implementar el Sistema de Seguridad de la Información (SGSI)".*
- **ISO-IEC-27002:** *"Por el cual se establece el código de buenas prácticas para la gestión de la seguridad de la información".*
- **IS-IEC-27003:** *"Por la cual se determina el proceso de planificación e implementación de los procesos del SGSI".*
- **ISO-IEC-27004:** *"Por el cual se estipula el sistema de medición de la eficacia de los SGSI implementados".*
- **ISO-IEC- 27005:** *"Por el cual se estandarizan las guías sobre la gestión de riesgos".*
- **ISO-IEC-27006:** *"Por el cual se informa sobre cómo los organismos de certificación deben interpretar la ISO 17021-1 en el contexto de auditorías a SGSI, en cumplimiento con la norma ISO 27001".*
- **ISO-IEC- 27007:** *"Por el cual se estandarizan las auditorias según la norma ISO 27001, el alcance y la complejidad, la gestión de riesgos, la selección de controles y la competencia de los auditores de SGSI"*. ISO-IEC-27008: *"Por el cual se manejan los aspectos técnicos de los controles de seguridad definidos en el Anexo A de la ISO27001".*
- **NTC- 5411-1-2006:** Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la tecnología de la información y las comunicaciones. Parte 1: Conceptos y modelos para la gestión de la tecnología de la información y las comunicaciones.
- **NTC 5450-1-2006:** Tecnología de la información. Técnicas de seguridad. Criterios de evaluación para la seguridad de tecnologías de la información (TI) parte 1: Introducción y modelo general.
- **NTC GP 1000:2009:** Norma técnica que describe las generalidades y los requisitos mínimos para establecer, documentar, implementar y mantener un Sistema de Gestión de la Calidad en los organismos, entidades y agentes obligados, conforme al artículo 2 de la Ley 872 de 2003.
- **NTC ISO 9001:** 2008 Norma técnica que determina los requisitos para un Sistema de

Gestión de la Calidad (SGC), que pueden utilizarse para su aplicación interna por las organizaciones, sin importar si el producto o servicio lo brinda una organización pública o empresa privada, cualquiera que sea su tamaño, para su certificación o con fines contractuales.

- **NTD-SIG 001:2011:** Norma técnica distrital que determina los requisitos del Sistema Integrado de Gestión para las Entidades y Organismos distritales adoptada mediante el Decreto 652 de 2011 por la Alcaldía de Bogotá.

5 DEFINICIONES

Activo: Cualquier cosa que tiene valor para la organización.

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

Activo de Información: Todo aquel elemento lógico o físico en 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 y recursos humanos.

Administrador de Bases De Datos: Administrador de Bases de Datos - DBA Infraestructura.

Administración de Usuarios: La administración de usuarios corresponde a las labores de creación, modificación, consulta, bloqueo, desbloqueo y eliminación de la cuenta de un usuario.

Análisis de Riesgos: Uso sistemático de la información para identificar fuentes y estimar riesgos.

Auditoría al Sistema de Gestión de Seguridad de la Información: Examen sistemático e independiente para determinar si las actividades y los resultados relacionados con la seguridad de la información cumplen disposiciones preestablecidas, y si 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 entidades tales como usuarios, procesos, sistemas e información.

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

Comité de Seguridad: Comité de Seguridad de Tecnología de Información.

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

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

Dependencia: Oficina o área de la entidad.

Directorio Activo: Herramienta que permite a los administradores de red establecer políticas a nivel de empresa, desplegar programas en una cantidad determinada de computadores y almacenar información de usuarios en una base de datos centralizada.

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

Disponibilidad: Propiedad que determina que la información sea accesible y utilizable a solicitud de una entidad autorizada.

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, autentificación, etc., conforme a las políticas de seguridad de quien los 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: Cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

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 ó 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. // Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Integridad: 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 para uso exclusivo dentro de una empresa u hogar. 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.

LOGS : Registro de actividad del sistema, para que pueda facilitar 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 pueden ser contabilidad, gestión documental, administración y procesamiento de texto, bases de datos, etc. Otros paquetes ajustan a la computadora para acoplarse a necesidades y operaciones específicas, como bancarias, de seguros, hospitales, manufactura, etc.

Partes Interesadas: Son aquellos individuos 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 pueden considerarse como partes interesadas los usuarios internos, los clientes, los proveedores, la Dirección, etc.

Perfil: Conjunto de características que permiten establecer 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 perfil de usuario.

Personal: Funcionarios, empleados contratados, consultores y contratistas.

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.

Propietario de La Información: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

Proveedor: Entidad física o virtual que tiene el fin de ofrecer un servicio a otra u otras entidades. Aquellos que proveen o abastecen y entregan bienes o servicios a otros.

Registro: Un 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 Integrado de Gestion: Sistema integrado para la Gestión de los Organismos y Entidades públicas adoptado mediante el Decreto 652 de 2011 y el cual lo conforman el Subsistema de Gestión de la Calidad (SGC), Subsistema de Control Interno (SCI), Subsistema de Gestión Ambiental (SGA), Subsistema de Seguridad y Salud Ocupacional (S&SO), Subsistema de Gestión de Seguridad de la Información (SGSI), Subsistema Interno de Gestión Documental y Archivo (SIGA) y el Subsistema de Responsabilidad Social (SRS).

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

Sistema de Información: Conjunto de datos, aplicaciones, equipos, y recursos humanos que en forma interrelacionada, proveen a la empresa la información necesaria para la ejecución de las tareas y la toma de decisiones de los niveles estratégico, táctico y operativo.

Tercero o Subcontratista: Es el proveedor de un producto o servicio que afecta la calidad del servicio prestado por la empresa.

Tercero: Contratista que desarrollea labores de asesoría, consultoría, implementación, soporte o mante-

nimiento y demás personas que sin ser de planta de la entidad, tienen un nivel de vinculación o brindan algún tipo de servicio dentro de las instalaciones de TRANSMILENIO S.A.

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

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

6.1 INTRODUCCIÓN

Este documento describe la Política Institucional de Seguridad de la Información y las Políticas Generales y Específicas definidas por TRANSMILENIO S.A.

Para la elaboración del mismo, se toman como base los controles y requisitos identificados en el estándar ISO/IEC 27001:2013 (Information technology -- Security techniques -- Information security management systems -- Requirements), las referencias definidas en el estándar ISO/IEC 27002 (Information Technology - Code of Practice for Information Security Management).

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

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

Este documento es confidencial y de propiedad de TRANSMILENIO S.A. Las actualizaciones se publicarán internamente en la herramienta de Gestión documental y cuando existan cambios, oficializados y aprobados por la oficina de Planeación y el Profesional 06 de Seguridad de la Información, éste último realizará el cambio siguiendo el procedimiento establecido para tal fin. y se notificará a cada uno de los funcionarios y contratistas.

6.2 VIGENCIA Y ACTUALIZACIÓN DEL MANUAL DE POLÍTICAS

Este Manual de Políticas conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. Debe ser por lo tanto materia de estudio y conocimiento para todas aquellas personas que directamente o a través de empresas formalicen contractualmente relación con TRANSMILENIO S.A.

La definición, actualización y mantenimiento del Manual de Políticas de Seguridad de la Información de TRANSMILENIO S.A. es responsabilidad de la Dirección de TIC's de TRANSMILENIO S.A., con la debida aprobación del Comité de Seguridad de la Información y deberá seguir los lineamientos definidos en el Procedimiento de Control de Documentos. En las revisiones periódicas se deben tener en cuenta factores como: incidentes de seguridad, nuevas vulnerabilidades detectadas, cambios en la infraestructura tecnológica u organizacional, en los objetivos del sistema o de la Organización, entre otros.

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

Se efectuará una revisión anual al Manual o cada vez que se presenten cambios significativos en:

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

6.3 COMPROMISO DE LA DIRECCIÓN

La Junta Directiva de TRANSMILENIO S.A. aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

La Junta Directiva y la Alta Dirección de la entidad demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual 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.

6.4 SANCIONES PARA LAS VIOLACIONES DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores de TRANSMILENIO S.A. Por tal razón, se hace necesario que las violaciones a las Políticas de Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

6.5 POLITICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.5.1 POLITICAS DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

TRANSMILENIO S.A. establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

6.5.2 Normas que rigen para la estructura organizacional de seguridad de la información

Normas dirigidas a: LA ALTA DIRECCIÓN

- La Alta Dirección de TRANSMILENIO S.A., debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
- La Alta Dirección debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.
- La Alta Dirección debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.
- La Alta Dirección debe promover activamente una cultura de seguridad de la información en TRANSMILENIO S.A.
- La Alta Dirección debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la entidad y al personal provisto por terceras partes.
- La Alta Dirección de TRANSMILENIO S.A., debe asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la Entidad.

Normas dirigidas al: COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

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

Normas dirigidas a: CONTROL INTERNO

- La Oficina de Control Interno debe validar y monitorear de manera periódica el cumplimiento de los controles de seguridad establecidos.

- La Oficina de Control Interno debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información de TRANSMILENIO S.A. a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.
- La Oficina de Control Interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.

Normas dirigidas a: DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES

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

Normas dirigidas a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes que realicen labores en o para TRANSMILENIO S.A., tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

7 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

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

La Política General de Seguridad de la Información tiene como objetivo la consolidación de una cultura de Seguridad de la Información[1], al interior de la Entidad, que permita a su vez, brindar un apoyo directo al desarrollo e integración de los sistemas de transporte público masivo intermodal de pasajeros de la ciudad de Bogotá D.C., en cuanto al cuidado de su activo más valioso: la información.

7.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

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

De acuerdo a lo anterior, la aplicación de las políticas de seguridad de la información registradas en el presente manual se constituye en la plataforma doctrinal de TRANSMILENIO S.A., para proteger su información, por lo cual, el conocimiento y aplicación de las Políticas de Seguridad de la Información es de obligatorio cumplimiento y ejecución por parte de todos los funcionarios públicos que integran la TRANSMILENIO S.A.

Las herramientas tecnológicas con las que cuenta la 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 Dirección y Jefes de Oficina, se constituyen en un activo de propiedad exclusiva de TRANSMILENIO S.A., por ende a la naturaleza de los bienes públicos, por lo cual podrá ser objeto de verificación, control y monitoreo por parte del profesional especializado 06 de la Dirección de TIC's.

7.2 DIRECTRICES DE DIRECCIÓN EN SEGURIDAD DE LA INFORMACIÓN.

Frente al presente Manual de Seguridad de la información la Alta Dirección de TRANSMILENIO S.A. resalta lo enunciado a continuación a fin de dar estricto cumplimiento:

[1] Conjunto determinado de valores y normas que son compartidos por personas y grupos de la organización para el control de interacción con el entorno, manteniendo las medidas preventivas y reactivas que permitan resguardar y proteger la información y sus principios, toda vez que está encaminado al diseño, implementación y mantenimiento de los procesos para la gestión del acceso a la información, asegurando sus principios y minimizando los riesgos. (Sistema de Gestión de Seguridad de la Información).

1. Socializar el Manual de Seguridad de seguridad de la información de TRANSMILENIO S.A., en cada uno de los funcionarios, con el fin de generar y consolidar una cultura de seguridad de la información al interior de la entidad.

2. Cumplir con las políticas y lineamientos para el manejo y administración de la información de TRANSMILENIO S.A. registradas en el presente Manual.

3. Promover e impulsar el uso de la información de TRANSMILENIO S.A. de manera segura.

4. Socializar las acciones de control y supervisión frente al adecuado uso de la información de TRANSMILENIO S.A., realizadas por el profesional especializado 06 de la Dirección TIC's.

5. Aplicar el manual de políticas de seguridad de la información en el desarrollo de todas las actividades diarias y propias, en cada una de las dependencias de TRANSMILENIO S.A.

6. Evitar la difusión no autorizada de información clasificada como confidencial, perteneciente a TRANSMILENIO S.A.

7. Orientar a los funcionarios de TRANSMILENIO S.A., en el cumplimiento de las obligaciones y deberes establecidos para salvaguardar la seguridad de la información y la seguridad informática.

8. Fortalecer los niveles de seguridad de de TRANSMILENIO S.A. en relación con la administración y uso de la información, de tal forma que se disminuya el riesgo frente a la pérdida, alteración o difusión no autorizada de información.

7.2.1 Políticas para la seguridad de la información.

Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.

7.2.2 Revisión de las políticas para la seguridad de la información

Las políticas de seguridad de la información serán proyectadas por el Profesional Especializado (06) de Seguridad de la Información de la Dirección de TIC´s, revisadas por el Director de TIC's y evaluadas por el Comité de Seguridad de Información y el área Legal antes de su publicación.

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

1. Efectividad demostrada por la naturaleza, número y el impacto de los incidentes de seguridad registrados.

2. Vulnerabilidades y amenazas emergentes.

3. Prioridades del negocio, costos e impacto de los controles sobre la eficiencia del negocio.

4. Cambio de la infraestructura organizacional y/o técnica

5. Cambios en los requerimientos regulatorios y /o legales.

6. Transferencia de la responsabilidad o la propiedad tal como adquisiciones y/o escisiones.

7.3 CONTROL DE ACCESO

Los sistemas de información de TRANSMILENIO S.A. deben contar con mecanismos y procedimientos para el control de acceso a sus sistemas de información y a las instalaciones de procesamiento de información tales que:

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

7.3.1 Requisitos de negocio para el control de accesos

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

7.3.1.1 Política de control de accesos

Establecer, documentar y revisar la política de control de acceso con base en los requisitos de TRANSMILENIO S.A. y de seguridad de la información, teniendo en cuenta lo siguiente:

1. Requerimientos de seguridad para las aplicaciones en forma individual, que se encuentren en servicio en TRANSMILENIO S.A.

2. Identificación de toda la información relacionada con las aplicaciones de TRANSMILENIO S.A.

3. Consistencia entre el control de acceso y las políticas de clasificación de la información de los diferentes sistemas y redes.

4. Legislación relevante y cualquier obligación contractual relacionada con la protección de acceso a los datos o servicios.

5. Perfiles estándar de acceso para usuarios con roles de trabajo común donde sea posible.

6. Segregación de roles de control de acceso, por ejemplo requerimientos de acceso, autorización de acceso, administración de acceso.

7. Autorización formal en las solicitudes de acceso.

8. Revisiones periódicas de los derechos de acceso.

9. Remoción de derechos de acceso.

7.3.1.2 Control de acceso a las redes y servicios asociados

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

2. Todo acceso remoto debe ser configurado con la siguiente información: Responsable, Tiempo de acceso permitido, Número de sesiones autorizadas (si aplica) y expiración.

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

4. Para acceso a correo electrónico externo o páginas web restringidas, se debe realizar una solicitud justificada a través de correo electrónico a la Dirección de TIC´s, y al Profesional Especializado (06) de Seguridad, quien evaluará el requerimiento y determinará la viabilidad de la misma.

7.3.2 Gestión de acceso de usuario

Objetivo: De acuerdo a los perfiles, se debe asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios de TRANSMILENIO S.A.

7.3.2.1 Gestión de altas/bajas en el registro de usuarios

Se debe contar con un proceso formal del registro y cancelación del registro para posibilitar la asignación de los derechos de acceso que incluya:

Altas:

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

2. El uso de IDs de grupo solamente se permitirán donde sea necesario por razones operacionales o de negocio, y deben ser aprobados y documentados.

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

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

Bajas:

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

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

7.3.2.2 Gestión de los derechos de acceso asignados a usuarios

1. Los perfiles y derechos de acceso deben estar documentados y deben ser revisados periódicamente por los propietarios de la información. Adicionalmente, es responsabilidad del usuario, informar cualquier privilegio que no corresponda con su perfil para que sea ajustado.

2. Únicamente se asignarán a los usuarios los derechos y privilegios necesarios para el desarrollo de sus funciones.

3. El acceso a la información debe ser autorizado por el área responsable de la información acorde a las funciones a desempeñar, previo análisis de la justificación y manteniendo una adecuada segregación de funciones.

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

7.3.2.3 Gestión de los derechos de acceso con privilegios especiales

Las transacciones realizadas y los accesos a los aplicativos o programas, a la red o a los sistemas de TRANSMILENIO S.A., son registrados de manera que se pueden llevar a cabo auditorías.

1. Las transacciones realizadas y los accesos a los aplicativos o programas, a la red o a los sistemas de TRANSMILENIO S.A., son registrados de manera que se pueden llevar a cabo auditorías.
2. Los privilegios deben ser asignados a los usuarios de acuerdo con a los roles y responsabilidades. Los privilegios se deben extender sólo cuando sea necesario y deben contar con autorización del profesional especializado 06 de la Dirección de TIC's.
3. Se debe implementar un procedimiento que garantice conceder privilegios adecuados y efectivos a los usuarios.

7.3.2.4 Gestión de información confidencial de autenticación de usuarios

La asignación de autenticación secreta o confidencial se debe controlar por medio de un procedimiento de gestión formal, implementada por la Dirección de TIC´s de TRANSMILENIO S.A.

7.3.2.5 Revisión de los derechos de acceso de los usuarios

Para mantener un control efectivo sobre el acceso a datos y servicios de información, se deben revisar los derechos de acceso de los usuarios a intervalos regulares usando un proceso formal.

La revisión debe tener en cuenta:

1. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.
2. Los usuarios que han dejado TRANSMILENIO S.A. ya no tengan cuentas activas.
3. Los usuarios con cuentas privilegiadas solo tengan acceso a lo que necesiten con el fin de realizar sus responsabilidades de trabajo.
4. Los privilegios asociados con cada aplicación, sistema o servicio deben ser identificados por los propietarios o usuarios encargados responsables de la información o recursos. Se debe mantener un registro de los perfiles con los privilegios asignados.
5. Los cambios a cuentas privilegiadas deben ser registrados para revisión periódica.
6. La Dirección TIC's y el personal de Soporte, implementará los perfiles de los usuarios por solicitud, de acuerdo con lo establecido por el propietario o usuarios encargados responsables de la información.

7.3.2.6 Cancelación o ajuste de los derechos de acceso

Los derechos de acceso de todos los funcionarios y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios

7.3.3 Responsabilidades del usuario

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

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

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

7.3.3.1 Uso de información confidencial para la autenticación

Todos los usuarios deben tener un único identificador (ID de usuario) para su uso personal solamente, y una técnica de autenticación conveniente debe ser escogida para verificar la identidad del usuario.

1. El control debe ser aplicado para todo tipo de usuarios (incluyendo operadores, administradores de red, programadores, administradores de bases de datos).
2. Los usuarios de TRANSMILENIO S.A., deben cumplir con las prácticas de la organización para el uso de información y de autenticación secreta, implementadas por la Dirección TIC's y el personal de soporte.
3. El acceso a los recursos de la red debe ser estrictamente controlado para prevenir acceso no autorizado. Los Usuarios solamente deben tener acceso a los servicios de red y sistemas de información que son necesarios para realizar su trabajo. Por tanto, los recursos de cómputo y sistemas de información adicionales debe ser restringidos.

4. Todos los accesos remotos deben ser autorizados por el propietario de la información y la Dirección TIC's.

5. Todo acceso remoto a la red de TRANSMILENIO S.A., debe contar con mecanismos de autenticación, autorización, registros de auditoría y de cifrado, para reducir el riesgo de divulgación de información sensible y accesos no autorizados.

6. El acceso a la red interna por parte de los funcionarios autorizados se debe realizar a través de una conexión segura con un certificado de seguridad SSL (Secure Sockets Layer).

7. El acceso por parte de un proveedor a la red interna se debe realizar por medio de un mecanismo seguro y con previa autorización de la Dirección de TIC´s de TRANSMILENIO S.A.

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

7.3.4 Control de acceso a sistemas y aplicaciones

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

7.3.4.1 Restricción del acceso a la información

El acceso a la información y a las funciones de los sistemas de aplicación por usuarios y personal de la Dirección de TIC's se debe restringir de acuerdo con la política de control de acceso definida por TRANSMILENIO S.A.

Los siguientes controles se deben implementar con el fin de apoyar los requerimientos de restricción de acceso.

1. Proporcionar menús para controlar el acceso a las funciones de los sistemas de aplicación.

2. Controlar y verificar los derechos de acceso de los usuarios sobre las aplicaciones y datos, por ejemplo leer, escribir, eliminar y ejecutar.

3. Asegurar que las salidas de los sistemas de aplicación que manejan información sensible de TRANSMILENIO S.A, contengan solo la información relevante para su uso y que la misma se envíe solamente a terminales y localizaciones autorizadas. Se deben hacer revisiones periódicas de dichas salidas con el fin de garantizar la remoción de información redundante.

4. Asegurar que las aplicaciones están correctamente clasificadas de acuerdo con el estándar de clasificación de información de TRANSMILENIO S.A.

5. De acuerdo con las políticas de control de acceso la Dirección TIC's debe restringir el acceso a la información y a las funciones de los sistemas de las aplicaciones.

6. Se deben identificar los controles de acceso requeridos por las aplicaciones de acuerdo con la clasificación y criticidad de la información que la aplicación procesa o almacena. Dichos controles deben ser definidos por el responsable del proceso o de la información.

7.3.4.2 Procedimientos seguros de inicio de sesión

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

2. Los responsables de la administración de la red deben realizar una evaluación periódica de los riesgos de seguridad existentes, y definir los controles para minimizarlos. El intercambio de información hacia o desde redes externas debe ser controlado por sistemas de control de acceso, tales como Firewall. Dicha administración, deberá ser realizada por el proveedor externo contratado para tal fin.

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

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

5. Siempre que los usuarios dejen el puesto de trabajo, deben bloquear el equipo mediante la alternativa de teclado (Control, Alt, Suprimir y Enter) o la tecla Windows + L. 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.

6. Las terminales deben apagarse después de un periodo definido de inactividad para prevenir el acceso por personas no autorizadas.

7. La facilidad de control de tiempo inactivo debe limpiar la pantalla de sesión y también, posiblemente más tarde, cerrar las sesiones de aplicación y red luego de un periodo definido de inactividad. Esta última parte no siempre la pueden controlar los sistemas. 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.

8. Las restricciones sobre los tiempos de conexión deben ser usadas para suministrar seguridad adicional a las aplicaciones de alto riesgo.

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

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

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

7.3.4.3 Gestión de contraseñas de usuario

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

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

Todos los usuarios deben:

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

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

3. La política de creación de usuario y contraseña, de acuerdo al manual de políticas de TRANSMILENIO S.A., establecidas por la Dirección TIC's , está diseñada de forma segura donde:

    - La creación del usuario seguirá el modelo: nombre.apellido@dominioTRANSMILENIO S.A., ejemplo pablo.rodriguez@TRANSMILENIO.gov.co

    - La creación de la contraseña debe ser de (08) caracteres, alfanumérica, debe contener una letra mayúscula y un número, ejemplo [Ejemplo5]

    - No estén compuestas por caracteres idénticos consecutivos o caracteres seguidos (12345, abcdefg).

    - No estén basadas en información de la persona o personas cercanas: nombres, números de teléfono, fechas de nacimiento, nombres de mascotas, etc.

    - No sean palabras que aparezcan en diccionarios así sean de otro idioma.

    - No debe contener el nombre de usuario

4. Los usuarios deberán seguir las siguientes políticas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

5. Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.

6. Las contraseñas no deberán ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

7. Las contraseñas no se deberán escribir en ningún medio, excepto cuando son entregadas en custodia.

8. Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.

9. Las contraseñas se deberán cambiar según los requerimientos de la infraestructura de procesamiento de información.

10. Los usuarios deberán cambiar las contraseñas la primera vez que usen las cuentas asignadas

11. Cambiar las contraseñas a intervalos regulares o basados en el número de accesos.

12. Cambiar las contraseñas temporales al primer acceso.

13. Evitar el uso de contraseñas anteriormente usadas

14. Las aplicaciones y sistemas de información deben utilizar un sistema de control de acceso basado en contraseñas interactivas y de calidad.

15. La Dirección TIC's y el personal Soporte, deben verificar el cumplimiento de la política asociada a la periodicidad con la cual las contraseñas deben ser cambiadas y las cuentas deshabilitadas de TRANSMILENIO S.A. Este requerimiento aplica a, como mínimo, sistemas, bases de datos o aplicaciones

16. Las aplicaciones y sistemas de información deben utilizar un sistema de control de acceso basado en contraseñas interactivas y de calidad.

17. Requerir a los usuarios mantener la confidencialidad de las contraseñas personales (esto podría ser incluido en los términos y condiciones de empleo).

18. Las contraseñas temporales proporcionadas cuando los usuarios olviden su contraseña deben ser suministradas solamente cuando se haya hecho una validación positiva de la identidad del usuario.

19. Las contraseñas temporales deben ser entregadas a los usuarios de una manera segura, con expiración en el primer uso. Se debe evitar la entrega de la clave a una tercera persona.

20. Las contraseñas temporales deben ser únicas para un individuo y no deben ser previsibles.

21. Las contraseñas nunca deben ser almacenadas sin protección en los sistemas de computador.

22. Las contraseñas por omisión que vienen en los sistemas y software deben ser modificadas enseguida de su instalación.

23. Todas las contraseñas de los súper-usuarios (altos privilegios) deben ser protegidas y almacenadas de una manera coherente con los planes de continuidad del negocio y/o el de recuperación.

24. Asegurar que las contraseñas son auditadas en intervalos regulares para verificar el cumplimiento con los lineamientos de contraseñas o proporcionar un control para hacer cumplir la política de contraseña durante su creación por ejemplo cumplimiento de la política de contraseñas en sistemas Windows.

25. La asignación de autenticación secreta o confidencial se debe controlar por medio de un procedimiento de gestión formal, implementada por la Dirección de TIC's de TRANSMILENIO S.A.

26. Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.

Caducidad de la Contraseña

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

7.3.4.4 Uso de herramientas de administración de sistemas

1. La Dirección TIC's de TRANSMILENIO S.A., controlará el uso de programas utilitarios que podrían tener la capacidad de anular el sistema y los controles de las aplicaciones.

2. Los usuarios finales no deben tener acceso a la ejecución de comandos del sistema operativo; en caso que sea necesario, se debe restringir el acceso por medio de herramientas que sólo permitan las funciones que han sido autorizados a ejecutar.

3. La Dirección TIC's de TRANSMILENIO S.A. y el área responsable del cada sistema de información deben determinar las actividades mínimas realizadas por el usuario que deben ser registradas sobre el sistema operativo, con el fin de detectar fallas o prevenir violaciones a la política de seguridad.

7.3.4.5 Control de acceso al código fuente de los programas

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

- Se deben establecer protocolos, identificar dueños y custodios de dichas fuentes, contemplando controles de administración, logs de auditoria y controles físicos que garanticen la integridad, disponibilidad y confidencialidad de dichas fuentes.

7.4 SEGURIDAD EN LAS TELECOMUNICACIONES

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

7.4.1 Gestión de la Seguridad en las Redes

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

1. Se deben controlar los accesos a servicios internos y externos conectados en red.
2. El acceso de los usuarios a redes y servicios en red no debe comprometer la seguridad de los servicios en red si se garantizan:
    a) que existen interfaces adecuadas entre la red de la Entidad y las redes públicas o privadas de otras entidades;
    b) que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos;
    c) el cumplimiento del control de los accesos de los usuarios a los servicios de información.
3. La Dirección de TIC's debe mantener el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad).
4. Se debe Preparar e implantar estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.

7.4.2 Controles de red

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

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

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

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

Normas dirigidas a: **DIRECCION DE TECNOLOGIA**

a. Dirección de TIC's de TRANSMILENIO S.A., debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red del TRANSMILENIO S.A.

b. La Dirección de TIC's de TRANSMILENIO S.A., debe asegurar que las redes inalámbricas de la entidad cuenten con métodos de autenticación que evite accesos no autorizados.

c. La Dirección TIC's de TRANSMILENIO S.A., en conjunto con Soporte, debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de la entidad, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

Normas dirigidas a: **TODOS LOS USUARIOS**

a. 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 el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

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

7.4.3 Mecanismos de seguridad asociados a Servicios en Red

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

7.4.4 Segregación de Redes o Separación de Redes

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

2. TRANSMILENIO S.A., provee los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios inadecuados sobre los sistemas operacionales. Así mismo, TRANSMILENIO S.A. controlará el paso de software y aplicaciones de un ambiente a otro.

3. TRANSMILENIO S.A. se asegura mediante controles de acceso adecuados, que los usuarios utilicen diferentes perfiles para el ambiente de desarrollo y de producción; así mismo, se asegura que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

4. No deberán realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción.

5. Sistemas de Información o aplicaciones que se encuentran en estado de pruebas no podrán pasar al ambiente de producción sin antes haber sido aprobado el cambio sobre la infraestructura de procesamiento de la información mediante el Procedimiento de Control de Cambios.

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

7. Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.

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

7.5 INTERCAMBIO/TRASFERENCIA DE INFORMACIÓN CON PARTES EXTERNAS

Objetivo: Mantener la seguridad de la información trasferida dentro de una organización y con cualquier entidad externa.

7.5.1 Políticas y procedimientos de intercambio de información

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

7.5.2 Acuerdos de intercambio

TRANSMILENIO 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

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

- 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., área que además coordinará la verificación de los requerimientos para el proceso de transmisión. También se debe privilegiar este mecanismo o similares técnicamente, cuando el intercambio de información se produzca con otros Organismos Nacionales con los que exista intercambio regular de información. La información a intercambiar debe estar previamente definida y formalizada a través de una petición institucional.

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

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

7.5.3 Mensajería electrónica

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:

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

b) 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.

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 o entre una cuenta de correo corporativa y una externa.

ii) 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.

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

iv) No se podrá enviar información clasificada como Restringida sin la autorización previa de la Dirección de TIC's de TRANSMILENIO S.A.

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

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

vii) 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 TRANSMILENIO S.A. y deberá incluir un mensaje que le indique al destinatario cómo ser eliminado de la lista de distribución.

f) 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.

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

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.

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

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

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

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

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

INTERNET

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

a) No se permite:

i) Navegación o publicación en sitio de contenido pornográfico, basado en sentimientos de odio o segregación, de delincuencia computacional (hackers o crackers) o cualquier otro sitio que la Dirección de TIC's considere fuera de los límites permitidos.

ii) Dirección de Publicación o envío de información confidencial hacia fuera de la

Dirección de TIC's sin la autorización de los Dueños respectivos.

iii) Utilización de otros servicios disponibles a través de Internet, como por ejemplo FTP y Telnet.

iv) Publicación de anuncios comerciales o material publicitario.

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

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

vii) 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, puede inspeccionar, registrar e informar de 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 y contratistas no pueden asumir en nombre de TRANSMILENIO S.A., posiciones personales en encuestas de opinión, foros u otros medios similares.

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 TRANSMILENIO S.A.

RECURSOS TECNOLÓGICOS

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

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

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 TRANSMILENIO 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 TRANSMILENIO SA.

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

Los funcionarios no deben realizar cambios en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física y además, sólo podrán ser realizados por la Dirección de TIC's

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

7.5.4 Acuerdos de confidencialidad y secreto

1. Todos los funcionarios, contratistas y clientes deben firmar la cláusula y/o acuerdos de confi-

dencialidad definidos por TRANSMILENIO S.A. y este deberá ser parte integral de cada uno de los contratos. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de la Entidad a personas o entidades externas.

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

3. Todo funcionario de TRANSMILENIO S.A. es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

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

5. 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.

6. 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.

7. 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 TRANSMILENIO 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 TRANSMILENIO S.A. o del tercero.

   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 sí 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.

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

7.6 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

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

7.6.1 Antes de la contratación

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

Normas dirigidas a: GRUPO DE TALENTO HUMANO

1. 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.

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

Normas dirigidas a SUPERVISORES DE CONTRATO, VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

Cada Supervisor de Contrato, Vicepresidente, Director y Jefe de Oficina debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información de TRANSMILENIO S.A.

Normas dirigidas a: **Personal Provisto por TERCERAS PARTES**

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

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

7.6.1.1 Términos y condiciones del empleo

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

7.6.1.2 Términos y condiciones de contratación

Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.

7.6.2 Durante la contratación

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

TRANSMILENIO S.A. en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso de la Alta Dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información de la entidad.

Todos los funcionarios de TRANSMILENIO S.A. deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la entidad.

7.6.2.1 Responsabilidades de la Dirección

La Alta Dirección debe demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas, normas y demás lineamientos que desee establecer la Entidad.

- La Alta Dirección debe promover la importancia de la seguridad de la información entre los funcionarios de TRANSMILENIO S.A. y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.
- La Alta Dirección debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

7.6.2.2 Concienciación, educación y capacitación en seguridad de la información

La Dirección de TIC´s debe diseñar y ejecutar de manera permanente un programa de concienciación en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.

La Dirección de TIC´s debe capacitar y entrenar a los funcionarios de TRANSMILENIO S.A. en el programa de concienciación en seguridad de la información para evitar posibles riesgos de seguridad.

7.6.2.3 Proceso disciplinario

Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan

cometido una violación a la seguridad de la información de TRANSMILENIO S.A.

Normas dirigidas a: la **SUBGERENCIA GENERAL con funcionales de CONTROL INTERNO DISCIPLINARIO**

Control Interno debe aplicar el proceso disciplinario de la Entidad cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad de la información.

Normas dirigidas a: GRUPO DE TALENTO HUMANO

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

Normas dirigidas a: **TODOS LOS USUARIOS**

Los funcionarios y personal provisto por terceras partes que por sus funciones hagan uso de la información de TRANSMILENIO S.A., deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

7.6.3 Terminación o cambio de puesto de trabajo

Objetivo: Proteger los intereses de la Entidad como parte del proceso de cambio o terminación del empleo.

7.6.3.1 Terminación o cambio de responsabilidad de puesto de trabajo

TRANSMILENIO S.A. asegurará que sus funcionarios y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros

Normas dirigidas a: CONTROL INTERNO - GRUPO DE TALENTO HUMANO

El Grupo de Talento Humano debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios de la entidad llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

Normas dirigidas a: SUPERVISORES DE CONTRATO, VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

Cada Supervisor de Contrato, Vicepresidente, Director y Jefe de Oficina debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios o personal provistos por terceras partes a la Oficina de Control interno.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

La Oficina de Control interno debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios a la Dirección de TIC´s

7.7 GESTIÓN DE ACTIVOS

7.7.1 Responsabilidad sobre los activos

1. Todos los funcionarios, contratistas, o terceros que presten sus servicios a TRANSMILENIO S.A, son responsables del cumplimiento y seguimiento de esta política y demás políticas de seguridad de la información que se plasman en el presente manual adoptado por la Entidad.

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

    - Coordinar la implementación de todos los controles de seguridad necesarios para el tratamiento de los riesgos de seguridad de la información.

    - Generar y mantener un registro detallado de todos los eventos que sucedan sobre los diferentes activos de información a su cargo.

    - Coordinar sus esfuerzos para realizar el mejoramiento de los servicios informáticos de la Entidad, así como de controlar cualquier cambio que afecte los niveles acordados para la prestación de los servicios.

    - Coordinar la realización del inventario de activos de información.

3. Los administradores de los activos y servicios de información son responsables de implementar, preservar y garantizar la seguridad de la información referente a la configuración de los diversos componentes o servicios de información y tecnología de la Entidad que estén a su cargo.

4. Los administradores de equipos informáticos Entidad deben:

    - Mantener y aplicar los procedimientos de operación de los equipos o servicios informáticos definidos por TRANSMILENIO S.A.

- Mantener actualizado el registro de riesgos que afecte a los activos bajo su responsabilidad.
- Reportar lo cambios que sucedan sobre los activos a su cargo ante los responsables de áreas o procesos de TRANSMILENIO S.A.
- Aplicar los procedimientos definidos por TRANSMILENIO SA para el acceso de terceros a los activos a su cargo en situaciones como mantenimiento o garantía.
- Registrar el desempeño de los equipos o servicios a su cargo.
- Registrar las actividades realizadas por los administradores o los operadores de los equipos o servicios a su cargo.
- Registrar las fallas sobre los equipos o servicios a su cargo
- Mantener registros de los usuarios a los cuales se les ha otorgado acceso a cada activo, servicio o componente.
- Aplicar los procedimientos definidos por TRANSMILENIO S.A para la asignación de cuentas de usuario y contraseñas de acceso a servicios y componentes.
- En coordinación con los responsables de los procesos y áreas de TRANSMILENIO S.A. aplicar las medidas de mitigación para contrarrestar las vulnerabilidades que se identifiquen sobre los activos o servicios de tecnología.
- Mantener y aplicar los procedimientos de respaldo de la información.
- Mantener, Mejorar y probar periódicamente los procedimientos de contingencia, recuperación ante desastres y continuidad en la prestación de servicios de tecnología.
- Implementar, mantener y mejorar los controles de protección física lógica o procedimental para la protección de los activos de información, componentes o servicios a su cargo.

7.7.2 Inventario de activos

TRANSMILENIO S.A., debe mantener actualizado el inventario de los activos de información tecnológicos incluyendo redes, subredes, servidores, aplicaciones, dispositivos de red, estaciones de trabajo, portátiles y licencias de software.

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

- Misión Crítica.
- No-Crítica

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

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

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

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

7.7.3 Propiedad de los activos

Todos los activos deben ser justificados y tener asignado un propietario.

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

EL propietario de los activos debe implementar los controles necesarios para asegurar la protección de los activos que se encuentran bajo su responsabilidad.

Se debe elaborar y mantener el inventario de activos identificando los propietarios y custodios de los activos, directivos o gestores responsables de proteger los activos, ubicación, número de serie, número de versión, estado de desarrollo / pruebas / producción.

Se deben utilizar códigos de barras para facilitar las tareas de realización de inventario y para controlar los equipos de TI que entran y salen de las instalaciones con funcionarios.

7.7.4 Uso aceptable de los activos.

TRANSMILENIO S.A., debe documentar e implementar las reglas para el uso aceptable de la información y de los activos de información asociados.

Todos los funcionarios, contratistas y terceras partes deben seguir y cumplir las reglas definidas para el uso aceptable de los activos de información. Se deben definir:

- Reglas para el uso de correo electrónico e Internet.
- Guías para el uso de dispositivos móviles.

7.7.5 Devolución de activos

Todos los empleados, contratistas y usuarios de terceras partes deben retornar todos los activos que posean de TRANSMILENIO S.A. a la terminación de su empleo o contrato.

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

7.7.6 Clasificación de la información

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

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

7.7.6.1 Directrices de clasificación

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

- Información pública. Es toda información no sensible para la divulgación al público que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.
- Información pública clasificada. Es aquella información que es sensible o confidencial dentro de la entidad y destinada a uso de TRANSMILENIO. Solo la pueden acceder algunos funcionarios de acuerdo con sus funciones y responsabilidades.
- Información pública reservada. Es aquella información que es extremadamente sensible o privada del más alto valor para la entidad y destinada para un grupo de personas de confianza de la Organización; cualquier violación a este tipo de información puede ocasionar daño a intereses públicos.
- Publicar o divulgar. Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión.

7.7.6.2 Etiquetado y manipulado de la información

Toda la información generada por TRANSMILENIO S.A., debe ser etiquetada de acuerdo a los niveles de clasificación anteriormente descritos.

7.7.6.3 Manipulación de activos

Se deben desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la entidad.

7.7.7 Manejo de los soportes de almacenamiento

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

7.7.7.1 Gestión de soportes extraíbles

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

Los siguientes controles deben ser considerados:

- Si ya no se requieren los contenidos previos de cualquier medio reutilizable, que será removido de la organización, deben ser borrados (eliminados).
- Debe solicitarse autorización para los medios extraídos de la organización y un registro de tales movimientos debe guardarse para mantener una pista de auditoría.
- Todos los medios deben ser almacenados en un ambiente seguro de acuerdo con las especificaciones de los fabricantes.
- Todos los datos almacenados en medios removibles deben ser evaluados contra los estándares de clasificación de datos

y protegidos de la manera indicada en el presente Manual.

7.7.7.2 Eliminación de soportes.

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

7.7.7.3 Soportes físicos en tránsito

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

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

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

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

7.8 CIFRADO O CRIPTOGRAFIA

7.8.1 Controles Criptográficos

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

7.8.2 Política sobre el uso de controles Criptográficos

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

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

7.8.3 Gestión de Claves

Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.

Normas de Controles Criptográficos

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de TIC´s debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

La Dirección de TIC´s debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.

La Dirección de TIC´s, debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.

La Dirección de TIC´s, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.

Los desarrolladores deben asegurarse que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la Dirección de TIC´s.

7.9 SEGURIDAD FISICA Y AMBIENTAL

7.9.1 Áreas Seguras

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

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

7.9.1.1 Perímetro de seguridad física

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

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

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

- El perímetro de la construcción o sitio que contiene instalaciones de procesamiento de información debe ser físicamente sólido. Los muros externos del sitio deben ser de construcción sólida y todas las puertas externas deben estar protegidas contra el acceso no autorizado, ejemplo alarmas, cerraduras, etc.
- Debe definirse un área de recepción u otro medio para el control del acceso físico al sitio o edificio.

7.9.1.2 Controles físicos de entrada

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

- Los visitantes a las áreas seguras deben ser supervisados o aprobados, y se debe registrar la fecha y hora de entrada y salida, y la razón de ingreso.
- Los visitantes a las áreas seguras deben portar en forma visible la identificación.
- El acceso a información sensible y a las instalaciones de procesamiento de información requieren medios secundarios de control de acceso y estar restringido únicamente al personal autorizado. Se deben usar controles de autenticación para validar y autorizar todo acceso.
- Deben mantenerse pistas de auditoría de todos los accesos a las áreas restringidas.
- No se debe ingresar dispositivos de almacenamiento a las áreas de procesamiento de información, si existe la necesidad de ingresar dispositivos de almacenamiento es necesario realizar un proceso de sanitización[2] a los dispositivos de almacenamiento
- El personal debe portar su carné de identificación todo el tiempo y estar dispuesto a retar o confrontar a los extraños sin acompañante y cualquiera que no porte la identificación de forma visible.

[2] Procedimiento mediante el cual se valida la información ingresada en dispositivos de almacenamiento y se escanea el dispositivo asegurando que no ingrese aplicaciones no deseadas a la Red de TRANSMILENIO S.A.

- Los derechos de acceso a las áreas seguras deben ser regularmente revisados y actualizados por parte de la gerencia responsable.

- Se deben registrar todas los ingresos y salidas de equipos de cómputo a la Entidad.

7.9.1.3 Seguridad de oficinas, despachos y recursos

La selección y el diseño de las áreas seguras debe contemplar la posibilidad de daño por fuego, inundación, explosión, accidentes, ataques y otras formas de desastre natural o provocados por el hombre.

Los siguientes controles son consideraciones esenciales:

- Las instalaciones clave deben estar ubicadas donde se pueda evitar el acceso público.

- Las construcciones deben ser discretas y dar una indicación mínima de su propósito.

- Puertas y ventanas tendrán que estar cerradas cuando no estén vigiladas y efectuar la protección externa para ventanas, particularmente a nivel del suelo.

- Las instalaciones de procesamiento de la información administradas por TRANSMILENIO S.A., deben estar físicamente separadas de otras administradas por terceros.

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

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

- Las construcciones de áreas que contengan equipos de soporte de los centros de datos (back ups, generadores, torres de enfriamiento, UPS, etc), deben tener el mismo nivel de seguridad que el centro de datos: estructura segura, control de acceso y sistemas de vigilancia técnica para el monitoreo del acceso y las actividades alrededor del área.

- Debe ubicarse un área de recepción para el control del acceso físico al centro de proceso de datos. El acceso debe restringirse únicamente al personal autorizado.

- Los visitantes a las áreas seguras deben estar siempre acompañados, registrarse fecha y hora de entrada y salida. Ellos solo deben acceder a lugares específicos con propósitos autorizados. Se debe establecer un registro de control de visitantes. Los empleados responsables de los visitantes acompañados, deben mantener el control sobre ellos en todo momento.

- Se deben utilizar circuitos cerrados de televisión (CCTV) para monitorear las actividades dentro y alrededor de los sitios críticos.

- Las salidas de emergencia deben tener alarma.

7.9.1.4 Protección contra las amenazas externas y ambientales

- La Dirección de TIC's debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

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

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

- La Dirección de TIC's debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente

autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

7.9.1.5 Trabajo en áreas seguras

Se deben diseñar se deben diseñar y aplicar procedimientos, guías y lineamientos para la protección física para trabajo en áreas seguras. Las cuales deben incluir lo siguiente:

- Trabajo no supervisado en áreas seguras se debe evitar por razones de seguridad y para prevenir oportunidades de actividades maliciosas.
- Las áreas seguras que no estén ocupadas deben estar físicamente cerradas y se deben revisar periódicamente.
- Equipos de fotografía, vídeo o grabadoras de audio, dispositivos móviles no deben permitirse en áreas seguras a menos que haya una autorización específica, de ser necesario ingresarlos se debe realizar un proceso de sanitización a cada dispositivo.

7.9.1.6 Áreas de acceso público, carga y descarga

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

Deben aplicarse los siguientes controles:

- El acceso al área de carga desde fuera del edificio, debe ser restringido a personal autorizado e identificado.
- El área de carga debe estar diseñada de tal manera que los suministros puedan ser descargados sin que el personal de entrega acceda a áreas críticas del edificio de TRANSMILENIO S.A.
- Las puertas externas del área de carga deben estar aseguradas cuando las puertas internas estén abiertas.
- El material entrante debe ser revisado por peligros potenciales antes de ser movido del área de carga al punto de utilización.

7.9.2 SEGURIDAD DE LOS EQUIPOS

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

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

7.9.2.1 Instalación y protección de los equipos

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

Los computadores portátiles asignados a los funcionarios de TRANSMILENIO S.A. deben ser entregados con bloqueo físico, y es responsabilidad de los funcionarios de la entidad protegerlos contra robo en caso que el portátil sea dejado desatendido. Se deben implementar procesos de cifrado de disco.

7.9.2.2 Instalaciones de suministro

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

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

- Múltiples fuentes para evitar puntos de fallo en una fuente de poder.
- Fuentes de poder ininterrumpidas (UPS).
- Generadores de respaldo.

7.9.2.3 Seguridad del Cableado

El personal de la Dirección TIC's debe garantizar que el cableado de energía y telecomunicaciones que transporta los datos o soporta los servicios de información deben estar protegidos de daño o interceptación.

Deben aplicarse los siguientes controles:

1. Las líneas de energía y telecomunicaciones dentro de las instalaciones de procesamiento de la información deben estar ocultas donde sea posible o sujetas a protección alternativa.
2. El cableado de redes debe estar protegido de daño o interceptación no autorizada, por ejemplo usando conductos o rutas para evitar pasar a través de áreas públicas.
3. Los cables de potencia deben estar separados de los de comunicaciones para prevenir interferencias.

4. Los cables deben marcarse e identificarse claramente para evitar errores.

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

6. Para los sistemas sensibles o críticos además de los controles anteriores se debe tener en cuenta:

7. Instalación de conductos blindados y cuartos bloqueados o cajas para puntos de inspección y terminación.

8. Uso de enrutamiento alternativo y/o medios de transmisión.

9. Uso de cableado de fibra óptica.

10. Iniciación de barrido técnico e inspección física para dispositivos no autorizados que estén conectados a los cables.

7.9.2.4 Mantenimiento de Equipos

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

Deben mantenerse los registros de todas las fallas reales o sospechosas y todo el mantenimiento preventivo y correctivo.

Deben aplicarse controles cuando se envíe el equipo fuera de la entidad para su mantenimiento y prevenir el acceso no autorizado a la información sensible.

7.9.2.5 Salida de activos fuera de las dependencias de la empresa

Se deben implementar procedimientos y controles para asegurar los equipos fuera de las instalaciones de la organización.

Los siguientes controles deberán ser considerados:

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

7.9.2.6 Reutilización o retirada segura de dispositivos de almacenamiento

7.9.2.6.1 Eliminación de la Información

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

Los procedimientos de eliminación adecuados son:

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

7.9.2.6.2 Donación / Venta de Equipos

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

Antes de cualquier venta o donación, todos los medios de almacenamiento deben ser borrados de acuerdo con los mecanismos de eliminación de información mencionados anteriormente.

Cualquier marca que pudiera identificar el equipo como propiedad de TRANSMILENIO S.A. o asociado con él, debe ser eliminada.

Se debe asegurar que no exista garantía o responsabilidad de TRANSMILENIO S.A. para la función u operación del equipo.

7.9.2.7 Equipo informático de usuario desatendido

Los usuarios deben asegurar que el equipo desatendido tiene una adecuada protección.

Los usuarios deben:

- Terminar las sesiones activas cuando finalicen, a menos que puedan ser aseguradas por un mecanismo de bloqueo, por ejemplo el protector de pantalla protegido con contraseña.
- Usar el protector de pantalla con contraseña, el cual debe ser activado dentro del tiempo límite de inactividad. Este complementa el anterior mecanismo de bloqueo pero no actúa como un reemplazo.
- Cierre la sesión de usuario en computadores centrales y servidores cuando finalice la tarea (no es correcto apagar la pantalla o el equipo sin salir de la sesión de usuario).

7.9.2.8 Política de puesto de trabajo despejado y bloqueo de pantalla

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

Se debe aplicar:

- Información sensitiva o crítica del negocio en papel o en medios de almacenamiento electrónico debe estar protegida (idealmente en una caja o gabinete) cuando no se requiera, especialmente cuando no hay nadie en la oficina.
- Los computadores y terminales se deben dejar con las sesiones terminadas o protegidas con un mecanismo de bloqueo de pantalla y teclado controlado por una contraseña, cuando están desatendidos.
- Uso no autorizado de fotocopiadoras y otra tecnología de reproducción como scanners y cámaras digitales se debe prevenir.
- Documentos con información clasificada o sensitiva deben removerse de impresoras tan pronto como sea posible.

DECRETOS LOCALES

ALCALDÍA LOCAL DE LA CANDELARIA

Decreto Local Número 001
(Enero 4 de 2016)

"Por el cual se convoca a sesiones extraordinarias a la Junta Administradora Local"

EL ALCALDE LOCAL DE LA CANDELARIA (E) en uso de sus facultades legales y en especial las conferidas por el Artículo 71 del Decreto Ley 1421 de 1993 y

CONSIDERANDO:

Que el artículo 71 del Decreto Ley 1421 de 1993 REUNIONES.- Inciso final Reza.- *"También se reunirán extraordinariamente por convocatoria que les haga el respectivo Alcalde. En este evento sesionarán por el término que señale el Alcalde y únicamente se ocuparán de los asuntos que él mismo someta a su consideración".*

Que la Junta Administradora Local terminó sesiones ordinarias el día 31 de diciembre de 2015.

Que en el Instituto Distrital de Turismo mediante oficio N° 2015EE3408 de fecha 30-11 2015 el cual reza en el ASUNTO "Remisión de observaciones y solicitud de adopción de medidas urgentes. Concepto técnico sobre delegación Consejo Local de Turismo radicado IDT 2015ER1956. En el cual invitan a la Corporación para que genere los mecanismos de comunicación especiales y urgentes con que se pueda derogar el Acuerdo Local 12 de 2014 (El Despacho corrige el numero correcto es 008 de 2014), teniendo en cuenta, que este tema ya fue abordado por las autoridades Distritales Concejo de Bogotá mediante el acuerdo 305 de 2007 *"Por el cual se establecen los lineamientos de la Política Publica Distrital de Turismo para Bogotá".* Y por la Administración Distrital mediante Decreto 327 de 2008 *"Por el cual se adopta la Política Distrital de Turismo para Bogotá".*

Que el Acuerdo Distrital 284 de 2007 ordenaba la creación del Consejo Local de Sabios y Sabias, lo cual efectivamente se hizo mediante Acuerdo Local 07 de 2013, Al entrar en vigencia el Acuerdo Distrital 608 de 2015, derogando taxativamente el Acuerdo Distrital 284 de 2007, se hace necesario que esta instancia local se adecúe a la norma nueva y actualmente vigente en mención.

Que el Decreto 032 de 2007 ***"Por el cual se reglamenta el Acuerdo 12 de 1994, en lo referente al Consejo Territorial de Planeación Distrital"*** **Artículo 6. Designación de Ediles en el CTPD.** Durante la primera semana de la posesión del Alcalde Mayor, la Secretaría Distrital de Gobierno procederá a citar a sesiones extraordinarias a las Juntas Administradoras Locales (JAL), con el único objeto de designar el representante de dicha Corporación ante el CTPD.

En mérito de lo anterior,

DECRETA:

ARTÍCULO PRIMERO: Convocar a sesiones extraordinarias por el periodo comprendido entre el ocho (8) de enero al veintidós (22) de enero (2016) inclusive, con el fin de que la Junta Administradora Local se pronuncie sobre la invitación elevada ante la Alcaldía y la Corporación por el Instituto Distrital de Turismo, sobre la derogatoria del Acuerdo Local No. 008 de 2014.

ARTÍCULO SEGUNDO: Se deberá actualizar la instan-

cia de participación Consejo Local de Sabios y Sabias a fin de derogar el Acuerdo Local 07 de 2013 y proferir el nuevo en el marco del Acuerdo Distrital 608 de 2015 actualmente vigente.

ARTÍCULO TERCERO: Adelantar el tramite ordenado por el Decreto Distrital 032 de 2007 Art. 6 a fin de designar representante de la Corporación al Consejo Territorial de Planeación Distrital.

ARTÍCULO CUARTO: El presente Decreto Local rige a partir de la fecha de su publicación.

PUBLÍQUESE Y CÚMPLASE.

Dado en Bogotá, D. C, a los cuatro (4) días del mes de enero de dos mil dieciséis (2016)

CARLOS RODOLFO BORJA HERRERA
Alcalde Local de La Candelaria (E)

Decreto Local Número 002
(Enero 4 de 2016)

Por el cual se adoptan medidas de Policía transitorias para garantizar la Seguridad, Convivencia Ciudadana, Espacio Público, Consumo de bebidas embriagantes, Restricción de Horario y la Protección de los Derechos y Libertades Públicas en el desarrollo de las festividades de FIESTA DE REYES Y EPIFANIA en la Localidad de la Candelaria y la zona de influencia en la Localidad de Santa Fe en los días 9, 10 y 11 de enero de 2016

EL ALCALDE LOCAL DE LA CANDELARIA (E) Y DE LA LOCALIDAD DE SANTA FE (TITULAR) En uso de las facultades legales y en especial las conferidas en ejercicio de sus atribuciones legales y en especial las que le confiere el art. 287 de la Constitución Política, Decreto ley 1421 art 84 numerales 1, 3,4,5,7,8 y 13, Decreto Nacional 1355 de 1970, Acuerdo Distrital 79 de 2013 del Decreto Distrital 657 de 2011 y

CONSIDERANDO:

Que el Artículo 1º de la Constitución Política establece que *"Colombia es un Estado social de derecho, organizado en forma de República unitaria, descentralizada, con autonomía de sus entidades territoriales, democrática, participativa y pluralista, fundada en el respeto de la dignidad humana, en el trabajo y la solidaridad de las personas que la integran y en la prevalencia del interés general".*

Que el Artículo 2º de la Constitución Política consagra que *"Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; (…) asegurar la convivencia pacífica y la vigencia de un orden justo. Las Autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares."*

Que La Constitución Nacional en el art. 287. Las entidades territoriales gozan de autonomía para la gestión de sus intereses, y dentro de los límites de la Constitución y la ley. En tal virtud tendrán los siguientes derechos:

1. Gobernarse por autoridades propias. 2. Ejercer las competencias que les correspondan. 3. Administrar los recursos y establecer los tributos necesarios para el cumplimiento de sus funciones. 4. Participar en las rentas nacionales.

Que de conformidad con lo dispuesto en el Artículo 6 de la Ley 489 de 1998, en concordancia con el artículo 209 de la Constitución Política, las entidades públicas y las autoridades administrativas tienen la obligación de coordinar sus actividades para el logro de los fines estatales. Adicionalmente la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones.

Para el cumplimiento de lo anterior, el Alcalde Local deberá acatar las medidas de orden público que sean implementadas por el Alcalde Mayor y demás autoridades de orden Nacional o Departamental y las que considere indispensables cuando la necesidad lo exija o las conveniencias públicas lo aconsejen.

Que por mandato del Artículo 12 de la Ley 62 de 1993, el Gobernador y el Alcalde son las primeras autoridades de Policía en el Departamento y el Municipio, respectivamente. La Policía Nacional cumplirá con prontitud y diligencia las órdenes que éstas le impartan por conducto del respectivo Comandante o quien haga sus veces. Los Gobernadores y Alcaldes deberán diseñar y desarrollar planes y estrategias integrales de seguridad con la Policía Nacional, atendiendo las necesidades y circunstancias de las comunidades bajo su jurisdicción.

Que el Artículo 86 del Decreto Ley 1421 numerales1, 4, 5, 7,8 y 13, en concordancia con el numerales

1°,2,3,4,5,6 y 14 del artículo 193 del Código de Policía de Bogotá, determinan que el Alcalde Local como autoridad de Policía, debe velar por el mantenimiento del orden público y por la seguridad ciudadana en el territorio de su jurisdicción, bajo la dirección del Alcalde Mayor. dictará los reglamentos, impartirá las ordenes, adoptará las medidas y utilizará los medios de policía necesarios para garantizar la seguridad, salubridad y la tranquilidad ciudadanas, así como la convivencia y la protección de los derechos y libertades públicas.

Que el Decreto 657 de 2011 "Por el cual se adopta la Política Pública Distrital de Convivencia y Seguridad Ciudadana y se armonizan los procedimientos y mecanismos para la formulación, aprobación, ejecución, seguimiento, evaluación y control de los planes integrales de convivencia y seguridad ciudadana –PICS- del Distrito Capital y se dictan otras disposiciones." En su art. 10.- define: La Acción Policiva. Es la realización de todos los actos necesarios para proteger y garantizar la convivencia y seguridad ciudadana y prevenir su alteración a través de una labor preventiva y pedagógica, respetuosa de la integridad física y moral, la dignidad humana y los derechos humanos en la comunidad.

Conflictividades: Situación en que dos o más individuos con intereses contrapuestos entran en confrontación, oposición o emprenden acciones mutuamente antagonistas, con potencialidad de escalar a contravenciones o delitos en caso de no tomarse medidas preventivas para su resolución.

Convivencia ciudadana: Se entiende como la interacción de relaciones naturales y la interdependencia entre quienes comparten actividades, espacios y entornos, en el respeto a la ley, a los demás y a unas normas básicas de comportamiento y de convivencia social orientadas a garantizar la integridad de las personas, las pertenencias y el cuidado de los bienes de beneficio colectivo en la cultura de la no violencia, y al compromiso de los habitantes a tomar precauciones para evitar daños a los demás, prestarse apoyo entre sí y, sobre todo, ayudar a quienes se encuentren en situaciones de vulnerabilidad o peligro inminente.

Orden público: Son las condiciones necesarias para el ejercicio de los derechos y libertades públicas, para asegurar que los habitantes convivan en paz. El orden público resulta de la prevención y la eliminación de las perturbaciones de la seguridad, tranquilidad, salubridad, moralidad, el medio ambiente y el ornato públicos.

Que el Comandante de la Estación de Policía Candelaria mediante N° S2015-003 de fecha 31 de diciembre de 2015 radicado en la Alcaldía Local de la Candelaria mediante Orfeo No. 2016-1720000032 de fecha 4 de enero de 2016, da a conocer las recomendaciones de seguridad que se estiman convenientes para implementar durante las festividades de reyes magos y quema del diablo la cual se desarrollan del 09 al 11 de enero del 2016, por lo cual es de vital importancia realizar una restricción transitoria al horario de venta y consumo de bebidas embriagantes toda vez, que por tratarse de una fiesta popular se desborda hacia los barrios aledaños al evento propiciando entornos de inseguridad y problemas de convivencia ciudadana, de igual forma para proteger el espacio público reglamentar los vendedores informales especialmente desde la Av. Los comuneros hasta la Av. Presidencial sobre la carrera 3 este o Av. Circunvalar, y alrededor del evento para evitar la acumulación de vendedores facilitan el desorden público. Horario de restricción para la venta y consumo de bebidas embriagantes. A partir de las 20:00 horas se restrinja la venta y consumo de bebidas embriagantes en los establecimientos de comercio y vía pública teniendo en cuenta que la finalización del evento y eso de suma importancia evacuación de las personas y para evitar accidentes e inconvenientes. Cuadrantes a aplicar la medida de venta y consumo de bebidas embriagantes al igual que la protección al espacio público. Al occidente Desde la carrera 3 entre la Av. Los comuneros hasta la calle 11. Al oriente desde la carrera 5 este entre la Av. Los comuneros hasta la calle 11. Al norte desde la calle 11 entre la carrera 3 hasta la carrera 5 este. Al sur desde la Av. Los comuneros hasta entre la carrera 3 hasta la carrera 5 este

Cuadrante	CAI	Estación
4	Bolivia	Candelaria
20	Bolivia	Candelaria
16	Bolivia	Candelaria
8	Rosario	Candelaria
12	Rosario	Candelaria
17	Rosario	Candelaria
33	Gavio	Santafé

Que en mérito de lo expuesto,

DECRETA:

PARA LA LOCALIDAD DE LA CANDELARIA.

ARTÍCULO 1.- ORDÉNASE la restricción transitoria para los días 9, 10 Y 11 de Enero de 2016, al horario de venta y consumo de bebidas embriagantes, a partir de las 20 horas en los establecimientos de comercio que se ubican en: al occidente Desde la carrera 3 entre la av. Los comuneros hasta la calle 11. Al oriente desde la carrera 5 este entre la Av. Los comuneros hasta la calle 11. Al norte desde la calle 11 entre la carrera 3 hasta la carrera 5 este. Al sur desde la Av. Los comuneros hasta entre la carrera 3 hasta la carrera 5 este. CAI ESTACION Cuadrantes 4 Bolivia, 20 Bolivia, 16 Bolivia, 8 Rosario, 12 Rosario y 17 Rosario.

ARTÍCULO 2.- PROHÍBASE la venta y consumo de bebidas embriagantes y comestibles en vía pública por

fuera del sitio demarcado con vallas donde se realizará la fiesta de Reyes y Epifanía exactamente en: al occidente Desde la carrera 3 entre la Av. Los comuneros hasta la calle 11. Al oriente desde la carrera 5 este entre la Av. Los comuneros hasta la calle 11. Al norte desde la calle 11 entre la carrera 3 hasta la carrera 5 este. Al sur desde la Av. Los comuneros hasta entre la carrera 3 hasta la carrera 5 este. CAI ESTACION Cuadrantes 4 Bolivia, 20 Bolivia, 16 Bolivia, 8 Rosario, 12 Rosario y 17 Rosario.

ARTÍCULO 3 .- COMUNÍQUESE el presente acto administrativo al Comandante de Policía de la Estación de la Candelaria a fin de que ordene lo pertinente a los respectivos cuadrantes y operativise el cumplimiento de las medidas transitorias de Policía para el tranquilo y seguro desarrollo de las Festividades en el Barrio Egipto que da cuenta el presente.

PARA LA LOCALIDAD DE SANTA FE

ARTÍCULO 4.- ORDÉNASE la restricción transitoria para los días 9, 10 Y 11 de Enero de 2016, al horario de venta y consumo de bebidas embriagantes, a partir de las 20 horas en los establecimientos de comercio que se ubican en: Al sur desde la av. Los comuneros hasta entre la carrera 3 hasta la carrera 5 este. Cuadrante 33 El Guavio, Localidad de Santa Fe.

ARTÍCULO 5.- PROHÍBASE la venta y consumo de bebidas embriagantes y comestibles en vía pública por fuera del sitio demarcado con vallas donde se realizara la Fiesta de Reyes y Epifanía exactamente en: Al sur desde la Av. Los comuneros hasta entre la carrera 3 hasta la carrera 5 este. Cuadrante 33 El Guavio, Localidad de Santa Fe.

ARTÍCULO 6.- COMUNÍQUESE el presente acto administrativo al Comandante de Policía de la Estación de Santa Fe a fin de que ordene lo pertinente al respectivo cuadrante zona de influencia e impacto de las Festividades del Barrio Egipto de la Localidad la Candelaria y operativise el cumplimiento de las medidas transitorias de Policía para el tranquilo y seguro desarrollo de las mismas.

ARTÍCULO 7.- VIGENCIA. El presente Decreto rige a partir de su publicación.

PUBLÍQUESE Y CÚMPLASE.

CARLOS RODOLFO BORJA HERRERA
Alcalde Local de la Candelaria (E)
Alcalde Local de Santa Fe

ALCALDÍA LOCAL DE KENNEDY

Decreto Local Número 11
(Octubre 10 de 2015)

"Por medio del cual se amplía la convoca a sesiones extraordinarias a la JUNTA ADMINISTRADORA LOCAL DE KENNEDY para estudiar el proyecto de Acuerdo "POR MEDIO DEL CUAL SE CREA Y REGLAMENTA EL CONSEJO LOCAL DE BARRAS FUTBOLERAS DE LA LOCALIDAD OCTAVA DE KENNEDY Y SE ESTABLECEN OTRAS DISPOSICIONES",

EL ALCALDE LOCAL ENCARGADO DE KENNEDY,
en ejercicio de sus facultades legales y en especial por las conferidas en el Decreto No 1421/93 y atendiendo lo dispuesto en el Decreto 372 de 2010.

CONSIDERANDO:

Que el inciso segundo, del Artículo 71 del Decreto 1421 de 1993 prevé que los ediles se reunirán extraordinariamente por convocatoria que le haga el respectivo Alcalde Local, debiendo sesionar por el término que señale el Alcalde y únicamente se ocuparán de los asuntos que el mismo someta a consideración.

Que de conformidad con el Artículo 71 del Decreto 1421 de 1993 las **JUNTAS ADMINISTRADORAS LOCALES** se reúnen ordinariamente por derecho propio cuatro veces al año así: el primero de Marzo, el primero de Junio, el primero de septiembre, y el primero de Diciembre.

Que por medio del decreto local No. 10, del 09 octubre de 2015 se convocó a Sesiones extraordinarias para estudiar por parte de la Corporación el Proyecto de Acuerdo **"POR MEDIO DEL CUAL SE CREA Y REGLAMENTA EL CONSEJO LOCAL DE BARRAS FUTBOLERAS DE LA LOCALIDAD OCTAVA DE KENNEDY Y SE ESTABLECEN OTRAS DISPOSICIONES",** los días 27, 28 y 29 de octubre de 2015.

Que es necesario contar con un periodo de tiempo más amplio, para el desarrollo del estudio, análisis y aprobación del Proyecto de Acuerdo **"POR MEDIO DEL CUAL SE CREA Y REGLAMENTA EL CONSEJO LOCAL DE BARRAS FUTBOLERAS DE LA LOCALIDAD OCTAVA DE KENNEDY Y SE ESTABLECEN OTRAS DISPOSICIONES".**

Que en mérito de lo anteriormente expuesto

DECRETA:

ARTÍCULO PRIMERO: Derogar el Decreto No. 10 de octubre 09 de 2015, que convoca a sesiones extraordinarias a la **JUNTA ADMINISTRADORA LOCAL DE KENNEDY** Los Días 27, 28 Y 29 de Octubre de 2015

ARTÍCULO SEGUNDO: Convocar a Sesiones Extraordinarias a la Junta Administradora Local de Kennedy a Sesiones Extraordinarias por el periodo comprendido entre los días 03 y 18 de noviembre de 2015 inclusive, con el fin de estudiar el Proyecto de Acuerdo **"POR MEDIO DEL CUAL SE CREA Y REGLAMENTA EL CONSEJO LOCAL DE BARRAS FUTBOLERAS DE LA LOCALIDAD OCTAVA DE KENNEDY Y SE ESTABLECEN OTRAS DISPOSICIONES".**

Dado en Bogotá a los 10 (Diez) días del mes de octubre de dos mil quince (2015).

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE.

CÉSAR HENRY MORENO TORRES
Alcalde Local (E)

ALCALDÍA LOCAL DE USAQUÉN

Decreto Local Número 015
(Diciembre 29 de 2015)

Por el cual se aclara el artículo segundo del Decreto Local No. 014 de 2015 por el cual se liquida el Presupuesto Anual de Ingresos y Gastos del Fondo de Desarrollo Local de Usaquén, para la vigencia fiscal comprendida entre el 1º de enero y el 31 de diciembre de 2016.

LA ALCALDESA LOCAL DE USAQUEN
En uso de sus facultades legales y en especial la que le confiere el artículo 19 del Decreto 372 de 2010.

CONSIDERANDO:

Que la Junta Administradora Local aprobó el Presupuesto Anual de Ingresos y Gastos e Inversión para la vigencia fiscal de 2016 mediante Acuerdo No. 007 del 15 de diciembre, el cual fue debidamente sancionado por el Alcalde Local.

Que en virtud de lo establecido en el artículo 19 del Decreto 372 de 2010, el Alcalde debe liquidar el Presupuesto Anual de Ingresos y Gastos e Inversión a nivel de programas y proyectos.

Que mediante Decreto Local No. 014 del 18 de diciembre de 2015 se liquidó el Presupuesto Anual de Ingresos y Gastos del Fondo de Desarrollo Local de Usaquén, para la vigencia fiscal comprendida entre el 1º de enero y el 31 de diciembre de 2016

Que el Artículo 19 del Decreto No. 372 del 30 de agosto de 2010 en su parágrafo reza: *"Cuando en el Decreto de Liquidación del Presupuesto se presenten errores de transcripción, aritméticos, numéricos, de clasificación, y de ubicación, el Alcalde Local, de oficio podrá mediante Decreto enmendar tales errores"* .

Que se debe aclarar el artículo segundo del Decreto Local No. 014 de 18 Diciembre 2015 toda vez que debido a un error involuntario se presentaron dichas situaciones:

Que en el código 3.1.2.02 Adquisición de Servicios no se refleja la sumatoria del código 3.1.2.02.11, Promoción institucional.

Que de igual manera el código 3.1.8.02.02 Adquisición de Servicios no refleja la sumatoria del código 3.1.8.02.11, Promoción institucional.

Que la sumatoria totales de los códigos código 3.1 GASTOS DE FUNCIONAMIENTO y Código 3.1.8 OBLIGACIONES POR PAGAR no se alteran.

Que estas modificaciones no generan alteraciones en las sumatorias de los Grandes Agregados.

Que en mérito de lo expuesto,

DECRETA:

ARTÍCULO 1.: Aclárese el artículo segundo del Decreto Local No.014 de 2015 por el cual se liquidó el Presupuesto de Gastos del Fondo de Desarrollo Local de Usaquén para la vigencia fiscal comprendida entre el 1º de enero y el 31 de diciembre de 2016, por la suma de CUARENTA Y NUEVE MIL CUATROSCIENTOS VEINTIOCHO MILLONES DOSCIENTOS SESENTA Y TRES MIL PESOS M/CTE ($49.428.263.000) , conforme al siguiente detalle:

CÓDIGO	CONCEPTO	VALOR
3	GASTOS	49.428.263.000
3.1	GASTOS DE FUNCIONAMIENTO	1.936.291.000
3.1.2	GASTOS GENERALES	1.314.010.000
3.1.2.01	Adquisición de Bienes	107.000.000
3.1.2.01.02	Gastos de Computador	45.000.000
3.1.2.01.03	Combustibles Lubricantes y Llantas	40.000.000
3.1.2.01.04	Materiales y Suministros	20.000.000
3.1.2.01.05	Compra de Equipo	2.000.000
3.1.2.02	Adquisición de Servicios	1.207.010.000
3.1.2.02.01	Arrendamientos	40.000.000
3.1.2.02.03	Gastos de Transporte y Comunicación	52.000.000
3.1.2.02.04	Impresos y Publicaciones	35.900.000
3.1.2.02.05	Mantenimiento y Reparaciones	743.760.000
3.1.2.02.05.01	Mantenimiento Entidad	743.760.000
3.1.2.02.06	Seguros	184.950.000
3.1.2.02.06.01	Seguros Entidad	70.000.000
3.1.2.02.06.04	Seguros de Vida Ediles	20.900.000
3.1.2.02.06.05	Seguros de Salud Ediles	94.050.000
3.1.2.02.08	Servicios Públicos	125.400.000
3.1.2.02.08.01	Energía	41.800.000
3.1.2.02.08.02	Acueducto y Alcantarillado	26.125.000
3.1.2.02.08.03	Aseo	10.450.000
3.1.2.02.08.04	Teléfono	47.025.000
3.1.2.02.11	Promoción institucional	25.000.000
3.1.8	OBLIGACIONES POR PAGAR	622.281.000
3.1.8.02	GASTOS GENERALES	622.281.000
3.1.8.02.01	Adquisición de Bienes	65.705.205
3.1.8.02.01.02	Gastos de Computador	30.000.000
3.1.8.02.01.03	Combustibles Lubricantes y Llantas	20.705.205
3.1.8.02.01.04	Materiales y Suministros	15.000.000
3.1.8.02.02	Adquisición de Servicios	556.575.795
3.1.8.02.02.01	Arrendamientos	45.000.000
3.1.8.02.02.03	Gastos de Transporte y Comunicaciones	42.418.551
3.1.8.02.02.04	Impresos y Publicaciones	25.688.280
3.1.8.02.02.05	Mantenimiento y Reparaciones	358.077.447
3.1.8.02.02.05.0001	Mantenimiento Entidad	358.077.447
3.1.8.02.02.06	Seguros	9.328.849
3.1.8.02.02.06.0001	Seguros Entidad	2.505.449
3.1.8.02.02.06.0005	Seguros de Salud Ediles	6.823.400
3.1.8.02.02.08	Servicios Públicos	50.300.308
3.1.8.02.02.08.0001	Energía	7.064.900
3.1.8.02.02.08.0002	Acueducto y Alcantarillado	19.458.408
3.1.8.02.02.08.0003	Aseo	7.411.000

CÓDIGO	CONCEPTO	VALOR
3.1.8.02.02.08.0004	Teléfono	16.366.000
3.1.8.02.02.11	Promoción institucional	25.762.360
3.3	INVERSION	47.491.972.000
3.3.1	DIRECTA	28.537.590.000
3.3.1.14	Bogotá Humana	28.537.590.000
3.3.1.14.01	Una ciudad que supera la segregación y la discriminación: el ser humano en el centro de las preocupaciones del desarrollo	7.446.800.000
3.3.1.14.01.01	Garantía del desarrollo integral de la primera infancia	100.000.000
3.3.1.14.01.01.1253	Usaquén humana con la primera infancia	100.000.000
3.3.1.14.01.02	Territorios saludables y red de salud para la vida desde la diversidad	450.000.000
3.3.1.14.01.02.0827	Promoción de la salud desde la autonomía, la dignificación y la convivencia	450.000.000
3.3.1.14.01.03	Construcción de saberes. Educación incluyente, diversa y de calidad para disfrutar y aprender	280.000.000
3.3.1.14.01.03.0949	Fortaleciendo el saber en Usaquén	280.000.000
3.3.1.14.01.04	Bogotá Humana con Igualdad de Oportunidades y equidad de género para las mujeres	140.000.000
3.3.1.14.01.04.0957	Usaquén Humana y libre de violencias contra las mujeres	140.000.000
3.3.1.14.01.05	Lucha contra distintos tipos de discriminación y violencias por condición, situación, identidad, diferencia, diversidad o etapa del ciclo vital	1.676.800.000
3.3.1.14.01.05.0937	Usaquén Humana con la persona mayor	1.476.800.000
3.3.1.14.01.05.1252	Usaquén Joven e Incluyente	200.000.000
3.3.1.14.01.07	Bogotá un territorio que defiende, protege y promueve los derechos humanos	200.000.000
3.3.1.14.01.07.0886	Derechos humanos, convivencia, democracia, participación intercultural en Usaquén	200.000.000
3.3.1.14.01.08	Ejercicio de las libertades culturales y deportivas	4.600.000.000
3.3.1.14.01.08.1250	Sistema local de deportes de Usaquén	2.300.000.000
3.3.1.14.01.08.1251	Usaquén, localidad que fortalece la cultura	2.300.000.000
3.3.1.14.02	Un territorio que enfrenta el cambio climático y se ordena alrededor del agua	16.484.390.000
3.3.1.14.02.19	Movilidad Humana	11.746.000.000
3.3.1.14.02.19.0913	Usaquén al día con sus vías	11.746.000.000
3.3.1.14.02.20	Gestión integral de riesgos	4.458.390.000
3.3.1.14.02.20.0952	Usaquén previene riesgos	4.458.390.000
3.3.1.14.02.21	Basura cero	80.000.000
3.3.1.14.02.21.0858	Usaquén gestiona adecuadamente sus residuos sólidos	80.000.000
3.3.1.14.02.22	Bogotá Humana ambientalmente saludable	200.000.000
3.3.1.14.02.22.0872	Usaquén verde	200.000.000
3.3.1.14.03	Una Bogotá que defiende y fortalece lo público	4.606.400.000
3.3.1.14.03.24	Bogotá Humana: participa y decide	100.000.000
3.3.1.14.03.24.0912	Fortalecimiento de organizaciones y redes sociales en Usaquén	100.000.000
3.3.1.14.03.27	Territorios de vida y paz con prevención del delito	400.000.000
3.3.1.14.03.27.0908	Usaquén fortalece su sistema de seguridad	400.000.000
3.3.1.14.03.31	Fortalecimiento de la función administrativa y desarrollo institucional	4.106.400.000
3.3.1.14.03.31.0856	Fortalecimiento de la capacidad operativa en Usaquén	4.106.400.000
3.3.6	OBLIGACIONES POR PAGAR	18.954.382.000
3.3.6.14	Bogotá Humana	15.907.371.000

CÓDIGO	CONCEPTO	VALOR
3.3.6.14.01	Una ciudad que supera la segregación y la discriminación: el ser humano en el centro de las preocupaciones del desarrollo	3.935.319.731
3.3.6.14.01.01	Garantía del desarrollo integral de la primera infancia	195.581.506
3.3.6.14.01.01.1253	Usaquén humana con la primera infancia	195.581.506
3.3.6.14.01.02	Territorios saludables y red de salud para la vida desde la diversidad	122.030.000
3.3.6.14.01.02.0827	Promoción de la salud desde la autonomía, la dignificación y la convivencia	122.030.000
3.3.6.14.01.03	Construcción de saberes. Educación incluyente, diversa y de calidad para disfrutar y aprender	239.700.630
3.3.6.14.01.03.0949	Fortaleciendo el saber en Usaquén	239.700.630
3.3.6.14.01.04	Bogotá Humana con igualdad de Oportunidades y equidad de género para las mujeres	46.225.500
3.3.6.14.01.04.0957	Usaquén Humana y libre de violencias contra las mujeres	46.225.500
3.3.6.14.01.05	Lucha contra distintos tipos de discriminación y violencias por condición, situación, identidad, diferencia, diversidad o etapa del ciclo vital	232.568.095
3.3.6.14.01.05.0937	Usaquén Humana con la persona mayor	232.568.095
3.3.6.14.01.08	Ejercicio de las libertades culturales y deportivas	3.099.214.000
3.3.6.14.01.08.1250	Sistema local de deportes de Usaquén	1.159.214.000
3.3.6.14.01.08.1251	Usaquén, localidad que fortalece la cultura	1.940.000.000
3.3.6.14.02	Un territorio que enfrenta el cambio climático y se ordena alrededor del agua	9.369.392.000
3.3.6.14.02.17	Recuperación rehabilitación y restauración de la estructura ecológica principal y de los espacios del agua	700.000.000
3.3.6.14.02.17.0871	Usaquén fortalece su estructura ecológica principal	700.000.000
3.3.6.14.02.19	Movilidad Humana	6.984.392.000
3.3.6.14.02.19.0913	Usaquén al día con sus vías	6.984.392.000
3.3.6.14.02.20	Gestión integral de riesgos	1.570.000.000
3.3.6.14.02.20.0952	Usaquén previene riesgos	1.570.000.000
3.3.6.14.02.21	Basura cero	75.000.000
3.3.6.14.02.21.0858	Usaquén gestiona adecuadamente sus residuos sólidos	75.000.000
3.3.6.14.02.22	Bogotá Humana ambientalmente saludable	40.000.000
3.3.6.14.02.22.0872	Usaquén verde	40.000.000
3.3.6.14.03	Una Bogotá que defiende y fortalece lo público	2.602.659.269
3.3.6.14.03.27	Territorios de vida y paz con prevención del delito	420.185.269
3.3.6.14.03.27.0908	Usaquén fortalece su sistema de seguridad	420.185.269
3.3.6.14.03.31	Fortalecimiento de la función administrativa y desarrollo institucional	2.182.474.000
3.3.6.14.03.31.0856	Fortalecimiento de la capacidad operativa en Usaquén	2.182.474.000
3.3.6.90	OBLIGACIONES POR PAGAR VIGENCIAS ANTERIORES	3.047.011.000
	TOTAL GASTOS + DISPONIBILIDAD FINAL	49.428.263.000

ARTÍCULO 2. El presente Decreto rige a partir de la fecha de su publicación y surte efectos fiscales a partir del primero (1°) de enero de 2016.

PUBLÍQUESE Y CÚMPLASE.

Dado en Bogotá, a los veintinueve (29) días del mes diciembre de dos mil quince (2015).

JULIETA NARANJO LUJÁN
Alcaldesa Local de Usaquén