ESTRUCTURACIÓN DE UN PLAN CON PROCEDIMIENTOS PARA QUE EL MINISTERIO TIC IMPLEMENTE LA POLÍTICA DE SEGURIDAD DE TRATAMIENTO DE DATOS PERSONALES, APLICADA A LOS DATOS RECOLECTADOS EN CONTROL DE ACCESO DEL EDIFICIO

CHRISTIAN CAMILO HENAO URREGO
YESID FERNEL RODRÍGUEZ PEÑA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA PROGRAMA
INGENIERÍA DE SISTEMAS ESPECIALIZACIÓN EN
SEGURIDAD INFORMÁTICA BOGOTÁ D.C.
2016

ESTRUCTURACIÓN DE UN PLAN CON PROCEDIMIENTOS PARA QUE EL MINISTERIO TIC IMPLEMENTE LA POLÍTICA DE SEGURIDAD DE TRATAMIENTO DE DATOS PERSONALES, APLICADA A LOS DATOS RECOLECTADOS EN CONTROL DE ACCESO DEL EDIFICIO

CHRISTIAN CAMILO HENAO URREGO
YESID FERNEL RODRÍGUEZ PEÑA

Trabajo de grado para optar al título de
Especialista en Seguridad Informática

Tutor
JUAN CARLOS ALARCÓN SUESCÚN
Ingeniero de Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA PROGRAMA
INGENIERÍA DE SISTEMAS ESPECIALIZACIÓN EN
SEGURIDAD INFORMÁTICA BOGOTÁ D.C.
2016

Nota de aceptación:

_____

_____

_____

_____

Firma de Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C. Marzo de 2016

DEDICATORIA

Ante todo, gracias al que todo lo hace posible Dios, jefe de los Ingenieros e inspiración de este proyecto, a nuestras familias por su apoyo y motivación incondicional.

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

Juan Carlos Alarcón Suescún, tutor del proyecto por su aporte a nuestra formación profesional y personal.

A la Universidad Piloto de Colombia

A todas aquellas personas que de una u otra forma colaboraron en la elaboración de este proyecto

CONTENIDO

LISTA DE FIGURAS

pág.

LISTA DE DIAGRAMAS

pág.

GLOSARIO

CONTROL DE ACCESO FÍSICO: control implementado al ingreso de un edificio o zona donde sea necesario realizar identificación y registro de la persona o personas que ingresan. [1]

DATO PÚBLICO: es el dato que no es semiprivado, privado o sensible, por ejemplo, el estado civil de las personas, la profesión u oficio. Los datos públicos pueden estar contenidos en registros públicos, documentos públicos, sentencias judiciales y demás documentos o información de índole pública.[2]

DATO PERSONAL: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.[3]

DATO SENSIBLE: es aquel que afecta la intimidad del titular o cuyo uso indebido genere su discriminación, por ejemplo, el origen racial étnico, orientación política, la creencia religiosa, pertenencia a sindicatos, organizaciones sociales, los datos relativos a la salud, la vida sexual y los datos biométricos.[4]

ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento de datos.[5]

GRUPOS DE INTERÉS: conjunto de personas, entidades, empresas, comunidades etc. a los cuales se ofrece un servicio de acuerdo a las necesidades y expectativas de dicho grupo.[6]

---

[1] OBSERVATORIO TECNOLÓGICO. Sistemas físicos y biométricos de seguridad. [En línea], [Consultado el 1 de marzo de 2016]. Disponible en: http://recursostic.educacion.es/observatorio/web/eu/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad

[2]. ALCALDÍA DE BOGOTÁ (2013). Decreto 1377 del 2013, artículo 3, numeral 2: protección de datos. [En línea], [consultado el 23 de enero de 2016]. Disponible en: www.alcaldiabogota.gov.co/sisjur/ normas/ Norma1.jsp?i=53646

[3]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Ley 1581 del 2012, artículo 3, numeral b. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: www.mintic.gov.co/portal/604/**art**icles-4274_

[4]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Ley 1581 del 2012, articulo 5. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: www.mintic.gov.co/portal/604/**art**icles-4274_

[5]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Ley 1581 del 2012, artículo 3, numeral d. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: www.mintic.gov.co/portal/604/**art**icles-4274_

[6] WIKI EOI. Grupos de interés en Responsabilidad Social y Sostenibilidad Empresarial. [En línea], [Consultado el 1 de marzo de 2016]. Disponible en: http://www.eoi.es/wiki/index.php/Grupos_de_inter%C3%A9s_en_Responsabilidad_Social_y_Sostenibilidad_Empresarial

RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de datos.[7]

TITULAR DE LOS DATOS: es la persona natural a la que se refiere los datos que reposan en una base de una determinada entidad, organización, empresa etc. y que tienen derechos sobre dichos datos de acuerdo a la ley 1581 del 2012.[8]

TRATAMIENTO DE DATOS PERSONALES: es el uso o cualquier operación sobre los datos personales, como pueden ser almacenamiento, circulación, actualización o supresión. [9]

[7]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA Ley 1581 del 2012, artículo 3, numeral e. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: www.mintic.gov.co/portal/604/**art**icles-4274_

[8] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA Ley 1581 del 2012, artículo 3, numeral f. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: www.mintic.gov.co/portal/604/articles-4274_

[9]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA Ley 1581 del 2012, articulo 3, numeral g. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: www.mintic.gov.co/portal/604/**art**icles-4274_

RESUMEN

El presente trabajo de grado, documenta la propuesta de un plan para que el Ministerio TIC implemente la política de tratamiento de datos personales definida en la entidad, a los datos que son recolectados en el control de acceso físico del edificio. Como producto entregable no solo se genera las actividades y acciones del plan, sino que también se generan tres procedimientos básicos y fundamentales de acuerdo a la ley 1581 de 2012, para que el Ministerio TIC los pueda aplicar y dar a conocer a los titulares de los datos.

Para poder plantear las actividades y acciones del plan, en primera instancia se debió determinar, cuáles son los datos, dónde se encuentran alojados y el estado actual del tratamiento. Con el anterior insumo y con el apoyo de la normatividad y la política definida en el Ministerio, se procedió a plantear una serie de actividades, recomendaciones y acciones a tomar, documentando así la primera fase del trabajo.

Con las actividades y acciones definidas dentro de la propuesta del plan, se generan procedimientos acordes a dichas actividades y acciones. Los procedimientos propuestos son basados en la política definida por el Ministerio y marco legal que rige en el país, como la ley 1581 del 2012, principal fundamentación para la propuesta.

De esta forma se presentará al Ministerio la propuesta, con el fin de que sea evaluada y puesta a disposición, para su ejecución, en el control de acceso físico a la entidad.

Palabras calve: Plan, Procedimientos, Protección de datos personales, ley 1581 del 2012, Política de tratamiento.

INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), en su deber diario de atender a sus grupos de interés, personas del común y al sector TIC en general, mediante su punto de atención y sus distintas dependencias, donde acuden a solicitar información, realizar trámites, reuniones laborales etc., recolecta un volumen considerable de datos personales en la recepción de la entidad, los cuales no se sabe que tratamiento están recibiendo, tampoco se sabe dónde se guardan y si están disponibles para que los titulares de los datos soliciten su modificación o retiro de las respectivas bases de datos.

Este problema se hace complejo considerando que la forma en que se recolectan los datos es a través de la lectura biométrica, con el fin de recolectar rápidamente el número de identificación de la persona y el nombre completo, para así entregarle una escarapela de identificación. De esta forma no solo se recolecta el nombre y la identificación de la persona, sino que también se recolectan datos como el tipo de sangre, estatura, fecha de nacimiento y demás datos que suelen tener los documentos de identificación, los cuales permiten identificar e individualizar a una persona.

Es así como se hace evidente para la entidad que la política de tratamiento de datos personales, recientemente aprobada, no comenzara actuar por sí sola ya que para ello se debe hacer una investigación que determine cuáles son esos datos personales a tratar, dónde se están recolectando y guardando, qué estrategias se deben seguir para sensibilizar y apropiar la política mencionada por parte de los implicados en la recolección de los datos, definir los encargados del tratamiento, los responsables del tratamiento, el sitio o los sitios adecuados donde se guardaran los datos y por supuesto generar los procedimientos importantes y adecuados que le permitirán al MINTIC implementar y aplicar lo establecido en su política de tratamiento de datos, inicialmente los que son recolectados en el acceso a la entidad, teniendo en cuenta la ley 1581 de 2012 y su decreto reglamentario 1377 de 2013, que dicta disposiciones generales para la protección de datos personales.

El objetivo principal de esta propuesta es estructurar un plan con procedimientos para que el MINTIC proceda a implementarla política de tratamiento de datos personales definida de acuerdo a la ley 1581 del 2012, a los datos recolectados en la recepción del edificio. Con esto se espera entregar a la entidad un punto de partida y una hoja de ruta marcada y fundamentada que le permitirá la implementación de la política, para este caso, aplicar dicha política a los datos recolectados al ingreso del edificio.

1. FASE DE DEFINICIÓN Y PLANTEAMIENTO

1.1 PLANTEAMIENTO DEL PROBLEMA

El Ministerio de Tecnologías de la Información y las Comunicaciones, según la Ley 1341 del 2009 o Ley de TIC, es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

La entidad en el desarrollo de sus funciones diarias es un foco principal a donde acude personal de todo tipo, ciudadanos del común, representantes de las empresas del sector, representantes de proveedores del Ministerio, funcionarios de otras entidades públicas etc. La entidad recibe a diario un promedio de 350 visitantes. De esta manera el Ministerio realiza la captura de los datos personales de los aproximados 350visitantes diarios, en el control de acceso, con la finalidad de que los visitantes estén registrados e identificados durante su permanencia en la entidad.

Lo anterior indica que la entidad es responsable del buen tratamiento a una gran cantidad de datos personales, según lo establecido en la ley 1581 del 2012, por la cual se dictan disposiciones generales para la protección de datos personales y el decreto 1377 de 2013 por el cual se reglamenta parcialmente la ley 1581 del 2012. Teniendo en cuenta lo presente, el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) generó su Política de seguridad para el Tratamiento de Datos Personales, siguiendo como referencia la ley 1581 de 2012. La política definida le permite a la entidad cumplir con cada una de las disposiciones de dicha ley.

Considerando que una política de seguridad informática (PSI) es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de lo que se desee proteger y el por qué protegerlo.

Teniendo en cuenta lo anterior una política de seguridad de la información, no establece en detalle cómo implementarla. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías.

Es así que el MINTIC con su política de tratamiento de datos personales definida, ahora tiene que entrar a implementarla, surgiendo la necesidad de determinar cómo se debe implementar de una forma eficiente y efectiva, para este caso

específicamente aplicar dicha política a los datos personales que son recolectados al ingreso de la entidad.

Con base en el panorama anterior, surge la necesidad de estructurar un plan para que la entidad implemente la política de tratamiento de datos personales, recolectados al ingreso del edificio, donde el primer trabajo a realizar sea identificar puntualmente ¿cuáles son esos datos personales?, ¿cómo se está haciendo su recolección? (base de datos, planilla manual de datos etc.), ¿dónde están quedando?, determinar los roles encargados del tratamiento y responsables de dicho tratamiento. De esta forma dicho plan permitirá determinar y describir operativa y funcional cada uno de los procedimientos necesarios para realizar el correcto tratamiento de la información de acuerdo a la ley y a lo definido en la política de la entidad.

1.2 PREGUNTA DE INVESTIGACIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones tiene definida la política de tratamiento de datos personales de acuerdo a la ley 1581 del 2012. Quiere empezar aplicando dicha política a los datos personales recolectados en la recepción de la entidad, puesto que este punto es el único foco principal a donde llegan los visitantes y realizan su registro para ser identificados. Ahora surge la pregunta:

¿Cuáles son los procedimientos que el Ministerio de Tecnologías de la Información y las Comunicaciones debe tener, para aplicar la política de seguridad de la información a los datos personales que se recolecten al ingreso del edificio de la entidad?

1.3 JUSTIFICACIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones en el desarrollo normal de sus actividades para sus grupos de interés, recolecta un volumen considerable de datos personales, en la recepción del edificio, a los cuales debe dar un tratamiento adecuado, transparente, eficiente y eficaz de acuerdo a la ley 1581 del 2012. De esta forma el Ministerio tiene la necesidad de implementar la política de tratamiento de datos personales, que la entidad ya tiene definida, para este punto o zona particular del edificio, única sede, donde desarrolla sus actividades principales y centrales, a la cual concurren un número aproximado de 350 visitantes por día. Pero para poder implementar dicha política necesita saber y buscar cómo hacerlo, estableciendo los procedimientos necesarios para cumplir con la política definida para tal fin de acuerdo a la ley 1581 de 2012 y el decreto 1377 de 2013,

buscando siempre la transparencia, evitando practicas o conductas que puedan derivar en sanciones legales por el no cumplimiento de dicha ley.

La estructuración de un plan con procedimientos para que el MINTIC implemente su política de tratamiento de datos personales en el control de acceso del edificio, le permitirá a la entidad, empezar dando cumplimiento a la ley 1581 de 2012 de una forma eficiente y eficaz, manteniendo y mejorando sus índices de transparencia que una entidad pública siempre debe tener.

Con la estructuración de dicho plan se le brindara un oriente y una hoja de ruta al MINTIC para que pueda implementar y cumplir a cabalidad la política de tratamiento de datos personales al ingreso del edificio, con la información personal recolectada a sus visitantes. Esto también le servirá como guía para que se puedan estructurar otros planes o procedimientos a otras fuentes de recolección de datos que tenga la entidad.

1.4 OBJETIVOS

1.4.1 Objetivo General. Estructurar un plan con procedimientos para que el Ministerio de Tecnologías de la Información y las Comunicaciones proceda a implementarla la política de tratamiento de datos personales a la información personal recolectada en la recepción del edificio, mediante el respectivo control de acceso que tiene en esa zona.

1.4.2 Objetivos específicos. A continuación se presentan los objetivos específicos de la propuesta:

- Identificar los datos personales, recolectados en el acceso al edificio del Ministerio de Tecnologías de la Información y las Comunicaciones, a los cuales la entidad, debe dar un buen y adecuado tratamiento, de acuerdo a la ley 1581 de 2012, el decreto 1377 de 2013 y la política de tratamiento de datos personales de la entidad.

- Definir las actividades y acciones del plan, para que MINTIC implemente la política de tratamiento de datos personales, en el acceso físico del edificio de la entidad.

- Describir y detallar los procedimientos que le permitirá al MINTIC implementar y cumplir con la política de tratamiento de datos personales de la entidad, al ingreso físico de la entidad, donde el personal visitante realiza el registro de sus datos.

2. MARCO TEÓRICO

La normatividad contenida en el proyecto, hace referencia a la Ley 1581 de 2012 y a la aplicabilidad de la misma en el tratamiento de datos personales, para el MINTIC es de vital importancia que se apliquen los lineamientos contenidos en esta ley y regular los procedimientos de recolección de información establecidos, logrando que se tenga una claridad en cuanto al tratamiento de datos personales.

Definir que es el dato personal para MINTIC, quienes son los responsables del tratamiento, encargados del tratamiento, el titular del dato personal, y posteriormente el tratamiento que se le dará al dato personal. Por esto es necesario analizar la normatividad vigente y verificar la aplicabilidad de esta a los procedimientos de tratamiento de datos personales que realiza el MINTIC.

Es importante realizar una descripción de los aspectos teóricos relacionados con la terminología utilizada en el presente proyecto:

2.1 NORMATIVIDAD

Actualmente la protección de datos personales, es de gran relevancia en cuanto a su tratamiento, el estado colombiano ha determinado que se debe tener algún tipo de regulación legal, que permita aplicar la ley a quien infrinja la misma.

2.1.1 Ley estatutaria 1581 de 2012. La ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.[10] La ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

[10] ALCALDÍA DE BOGOTÁ. Ley estatutaria 1581 de 2012. [En línea], [Citado el 2 de noviembre de 2015] Disponible en la World Wide Web <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646>.

2.1.2 Decreto 1377 de 2013. "El Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales ".[11]

Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la ley.

2.1.3 Artículo 15 de la constitución política de Colombia. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución"

2.1.4 Sentencia C - 748/11. Ley estatutaria-Ley de especial jerarquía / ley estatutaria materias que regula.

2.1.5 Sentencia C - 981/05. Reserva de ley estatutaria-Criterios para su determinación respecto de derechos fundamentales.

2.1.6 Sentencia C-1011/08. Proyecto de ley estatutaria de habeas data y manejo de información contenida en bases de datos personales [12]

[11]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIADecreto 1377 de 2013. [En Línea], [citado el 2 de noviembre de 2015]. Disponible en: www.mintic.gov.co/portal/604/articles-4274_documento.**pd**

[12]CORTE CONSTITUCIONAL DE COLOMBIA. Artículo 15 de la Constitución Política de Colombia: Sentencias C- 748 de 2011, C-981 de 2005 y C-1011 de 2011. [En Línea], [consultado el 2 de noviembre de 2015]. Disponible en la World Wide Web http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15; http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm;<http://www.corteconstitucional.gov.co/relatoría /2008/C-1011-08.htm>; <http://www.corteconstitucional.gov.co/relatoria/2005/c-981-05.htm>

2.2 ESTADO DEL ARTE

En la actualidad tanto en el sector público como el sector privado, se están realizando una serie de revisiones acerca de la aplicación de la ley estatutaria 1581 de 2012, esta ley permite que el tratamiento de datos personales este regulado y se sujete a lo establecido en la misma y las disposiciones legales establecidas.

En el estado del arte se analizará cómo se maneja el tratamiento de datos personales en otras entidades, tratando de encontrar buenas prácticas en el tratamiento de datos personales, y poder aplicarlas al MINTIC, en el estado del arte se analizarán entidades públicas y empresas del sector privado, es necesario realizar un cotejamiento de los hallazgos en materia de tratamiento de datos personales en cada una de las entidades analizadas, este se realizará en entidades con diferentes niveles de seguridad en cuanto al tratamiento de datos personales.

2.2.1 Caso de estudio Dirección de Impuestos y Aduanas Nacionales. En la DIAN la política de calidad que se ha establecido para la entidad a través del Código del Buen Gobierno y que a continuación se describe, está orienta a dar cumplimiento a los siguientes elementos: procesos, clientes, partes interesadas, productos y servicios, recursos, y competencias técnicas.

La DIAN se gestionará a partir de un enfoque basado en procesos estandarizados, controlados, optimizados y debidamente documentados, que generen el impacto previsto, para la satisfacción de las necesidades de sus clientes, bajo los principios de la mejora continua.[13]

En el control de acceso al edificio no existe ningún tipo de control, la política de calidad, solo regula procesos técnicos que involucran a los contribuyentes (clientes), el control de acceso por su parte es asumido por la empresa de vigilancia, llevando un control manual de los registros en un libro minuta; este no está siendo auditado por ningún funcionario de la DIAN, se evidencia una falta de control y seguimiento a los bienes de propiedad de la DIAN

La recolección de los datos se realiza en la recepción del edificio donde se solicitan datos personales como: nombres, número de identificación, para lo cual se deben reglamentar las políticas y procedimientos que serán aplicables al manejo de información.

2.2.1.1 Responsable y encargado del tratamiento. La empresa de vigilancia es la encargada, aunque no existe ningún documento que formalice el proceso.

[13]DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES. Estandarización de la entrada y salida de información, atendiendo los principios constitucionales y legales. [En Línea], [citado el 2 de noviembre de 2015]. Disponible en la Intranet: http://insitu.dian.gov.co/pinterna/normatividad.nsf/e9327debba393.

2.2.1.2 Clasificación del tratamiento general de la información. Corresponde a cualquier operación o conjunto de operaciones sobre datos personales, como la recolección, almacenamiento, uso, circulación o supresión, en este caso es inexistente, solo se mantiene el registro (manual) libro minuto. Es por lo tanto nula la clasificación de proveedores, clientes, empleados.

2.2.1.3 Vigencia de la información recolectada. No se puede cuantificar al no tener definido cuál es la finalidad del tratamiento a los datos recolectados.

2.2.1.4 Derechos del titular. Es la persona natural cuyos datos personales sean objeto de Tratamiento, en la recolección se realiza un registro de ingreso, el cual no puede ser consultado sin autorización del responsable y encargado del tratamiento de la información.

2.2.1.5 Aviso de privacidad. En la recepción del edificio no existe ningún aviso de privacidad.

2.2.1.6 Procedimiento para consultas, actualización de datos y reclamos. No existe ningún procedimiento que lo contemple, sin embargo, bajo derecho de petición la información debe ser suministrada.

2.2.1.7 Requisito de procedibilidad. No está contemplado en la política de la entidad. En la DIAN no se tiene definida una política de procedimientos para el tratamiento de datos personales, aunque se encuentra estipulada la protección de datos personales en la CIRCULAR NÚMERO 0 0 0 0 0 - 1 1 ENE 2013, Circular sobre estandarización de la entrada y salida de información, atendiendo los principios constitucionales y legales. En el CAPÍTULO IV, se habla sobre DATOS PERSONALES - ADMINISTRACIÓN Y TRATAMIENTO “La Ley 1581 de 2012 define el tratamiento de la información que contenga datos como “Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión”.

También se encuentran:“DATOS PERSONALES – CARACTERÍSTICAS, PRINCIPIOS APLICABLES A LA RECOLECCIÓN, ALMACENAMIENTO, USO Y CIRCULACIÓN DE DATOS PERSONALES”

Estos no están gobernados por ninguna política de protección de datos personales. Por lo tanto, los datos recolectados en el control de acceso no están regulados, no obstante, la ley aplica con las disposiciones generales para la protección de datos personales.

2.2.1.8 Recomendaciones para el tratamiento de datos personales en la Dian. En la DIAN, es necesario definir una política para el tratamiento de datos personales, la cual debe estar fundamentada en la ley 1581 del 2012 y el decreto 1377 de 2013 y con esto generar los procedimientos que permitan aplicar e implementar dicha política para así cumplir con la normatividad vigente.

Algunos puntos relevantes después de que la política se defina, es que, en todos los procedimientos de recolección, tratamiento y clasificación de los datos personales, se tengan en cuenta aspectos que permitan cumplir con las disposiciones generales de dicha ley estatutaria:

- Definir los procesos de recolección, tratamiento, consulta de los datos recolectados en el control de acceso a la entidad.

- Dar a conocer la política de tratamiento de datos a la empresa de vigilancia, para que se responsabilice y cumpla la política como encargado del tratamiento.

- Definir el responsable del tratamiento de datos personales, que son recolectados en el control de acceso a la entidad.

- Definir las funciones del encargado del tratamiento de la información.

- Realizar la divulgación de la política de tratamiento de datos personales, mediante aviso de tratamiento de datos personales al ingreso de la entidad.[14]

2.2.2 Caso de estudio CONSALFA S.A.S. En la empresa CONSALFA S.A.S. existe una política de procedimientos de datos personales. “La Dirección Jurídica de CONSALFA S.A.S. actuará como ENCARGADO DEL TRATAMIENTO de Datos Personales.

Tratamiento al cual serán sometidos los datos y la finalidad del mismo:

“El tratamiento corresponde a cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

CONSALFA S.A.S. reconoce la importancia de la seguridad, privacidad y confidencialidad de los datos personales que suministran las personas, por lo cual está comprometida con su protección y el manejo adecuado, conforme al régimen legal de protección de datos”.*[15]*

---

[14]DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES. Op. Cit. p. 23.

[15] CONSALFA.COM. Manual interno de políticas y procedimientos de datos personales. [En Línea] [Consultado el 2 de noviembre de 2015]. Disponible en la World Wide

2.2.2.1 Tratamientos. Generales de la información. CONSALFA S.A.S. procesa información que contiene datos personales, productos y servicios e in formación de proveedores, la empresa CONSALFA S.A.S., procesa estos datos personales con las ordenes de cumplimiento, además de eso confirma la información suministrada. También se recolecta información personal en las transacciones y en la publicidad de los productos y servicios, la información recolectada es objeto de tratamiento de recolección, almacenamiento, grabación uso, circulación, procesamiento, supresión y transmisión.

2.2.2.2 Derechos del Titular. En CONSALFA S.A.S. se tienen en cuenta los derechos de los titulares de la información y definen el titular como una persona natural cuyos datos personales son recolectados, almacenados o utilizados por el Responsable del tratamiento. El Titular tendrá los derechos establecidos por la ley 1581 de 2012. Estos son: conocer y poder rectificar la información recolectada, rectificar información parcial o incompleta; además debe de ser informado por CONSALFA S.A.S. del tratamiento al que estará sujeta la información personal previa autorización.

2.2.2.3 Autorizaciones y consentimiento. En el caso se pudo identificar que en CONSALFA S.A.S., es requerido del consentimiento libre, previo, expreso e informado del titular de los datos personales, el tratamiento realizado se integra a la ley 1581 de 2012, solo exceptuando los casos definidos en la ley, al igual también se tiene un registro de la prueba de la autorización y CONSALFA S.A.S. utiliza los mecanismos con los que cuenta actualmente e implementará y adoptará las acciones tendientes y necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos de cuándo y cómo obtuvo autorización por parte de los titulares de datos personales para el tratamiento de los mismos[16].

2.2.2.4 Aviso de privacidad. El Aviso de Privacidad es informado al titular dando a conocer la existencia de la política de tratamiento de datos personales; con esto se pone en conocimiento al titular acerca el tratamiento que se le darán a los datos personales a través de un documento físico, electrónico o en cualquier tipo de formato que permita dar a verificar las características del tratamiento a los datos personales. (Ver figura 1)

Web<http://www.consalfa.com/Portals/0/Documentos/ManualPoliticasyProcedimientosDatosPersonalesCONSALFAS_AS_Rev1.pdf>.

[16] CONSALFA.COM. Op. Cit. p. 22.

Figura 1. Aviso de privacidad Consalfa S.A.S

AVISO DE PRIVACIDAD

CONSALFA S.A.S, con domicilio en la Ciudad de Bogotá, Colombia, actúa y es Responsable del Tratamiento de los datos personales.

Cómo contactarnos: Dirección de oficinas: Calle 110 N° 9-25, Oficina 801 Torre Empresarial Pacific (Bogotá), Dirección Jurídica de la Compañía, Correo electrónico: habeasdata.consalfa@gmail.com, Teléfono: 4926060.

Sus datos personales serán incluidos en una base de datos y serán utilizados de manera directa o a través de terceros designados, entre otras y de manera meramente enunciativa para las siguientes finalidades directas e indirectas relacionadas con el objeto y propósitos de CONSALFA S.A.S.:

- ✓ Dar cumplimiento a obligaciones contraídas con nuestros proveedores, contratantes, contratistas y empleados.
- ✓ Procesar.
- ✓ Confirmar.
- ✓ Cumplir.
- ✓ Efectuar reportes con las distintas autoridades administrativas, de control y vigilancia, nacionales, policivas o autoridades judiciales, entidades financieras y/o compañías de seguros.
- ✓ Registros contables.
- ✓ Correspondencia.
- ✓ Procesamiento.
- ✓ Almacenamiento.

Se le informa a los titulares de información que pueden consultar en nuestra página web: www.consalfa.com, el Manual Interno de Políticas y Procedimientos de Datos Personales de CONSALFA S.A.S que contiene las políticas para el tratamiento de la información recogida, así como los procedimientos de consulta y reclamación que le permitirán hacer efectivos sus derechos de acceso, consulta, rectificación, actualización y supresiones de los datos.

Fuente: elaborado por Consalfa S.A.S - manual interno de políticas y procedimientos de datos personales.

2.2.2.5 Autorización y refrendación de uso de datos personales. Se puede observar que tienen publicada la autorización de uso de datos personales: (Ver figura 2)

Figura 2. Autorización y refrendación de uso de datos personales Consalfa S.A.S

MANUAL INTERNO DE POLITICAS Y PROCEDIMIENTOS DE DATOS PERSONALES

ConSalfa

ANEXO No. 1 - AUTORIZACIÓN Y REFRENDACIÓN DE USO DE DATOS PERSONALES

Con la expedición de la Ley 1581 de 2012 y el Decreto 1377 de 2013, se desarrolla el principio constitucional que tienen todas las personas a conocer, actualizar y rectificar todo tipo de información recogida o, que haya sido objeto de tratamiento de datos personales en bancos o bases de datos y, en general en archivos de entidades públicas y/o privadas.

CONSALFA S.A.S. como Compañía privada que almacena y recolecta datos personales requiere obtener su autorización para que de manera libre, previa, expresa, voluntaria y debidamente informada, permita entre otros, recolectar, recaudar, almacenar, usar, circular, suprimir, procesar, compilar, intercambiar, dar tratamiento, actualizar, comunicar, relacionar, registrar, consolidar, acreditar, auditar y disponer de los datos que han sido suministrados y que se han incorporado en las distintas bases de datos con que cuenta CONSALFA S.A.S., de forma directa o a través de terceros, en los términos y condiciones plasmados en nuestro Manual Interno de Políticas y Procedimientos de Datos Personales.

CONSALFA S.A.S. con base en lo dispuesto en el artículo 10 del Decreto 1377 de 2013 queda autorizada de manera expresa e inequívoca para mantener y manejar toda su información, al no ser que Usted le manifieste lo contrario de manera directa, expresa, inequívoca y por escrito a la cuenta de correo electrónico dispuesta para tal efecto habeasdata.consalfa@gmail.com.

Si Usted no desea que sus datos personales sean utilizados por CONSALFA S.A.S., podrá revocar de manera parcial o total dicha autorización de manera expresa e inequívoca, directa, expresa y por escrito bien sea en medio físico o electrónico; o de manera oral, o por cualquier medio o conducta inequívoca que permita concluir de forma razonable que se revoca tal autorización o consentimiento.

Se le informa que puede consultar el Manual Interno de Políticas y Procedimientos de Datos Personales de CONSALFA S.A.S. en nuestra página web: www.consalfa.com.

Con esta aceptación, como titular de la información, autorizo de manera expresa e inequívoca que mis datos personales sean tratados para los fines anteriormente señalados y en el Manual Interno de Políticas y Procedimientos de Datos Personales de CONSALFA S.A.S. y reconozco que los datos que suministro son veraces. Conozco que si hay una falsedad y/u omisión, esto supondrá que no se me podrá prestar correcta y oportunamente los servicios prestados por CONSALFA S.A.S..

FIRMA
NOMBRE:
C.C.:
Fecha:

Fuente: elaborado por Consalfa S.A.S. - manual interno de políticas y procedimientos de datos personales.[17]

2.2.3 Caso de estudio Easy Colombia. Tiene la finalidad de regular los procedimientos de Tratamiento de datos de carácter personal que realiza EASY COLOMBIA a fin de garantizar y proteger el derecho fundamental de habeas data en el marco de lo establecido en la mencionada Ley 1581 de 2012, en el artículo 15 de la Constitución Política y las demás normas que las modifiquen, aclaren, reglamenten o adicionen.

[17] Ibíd., p. 27.

2.2.3.1 Objetivo general. En el caso se pudo identificar que pretenden garantizar la protección del derecho de Habeas Data que tienen toda persona natural, así como la reglamentación del uso de los datos por parte de CENCOSUD COLOMBIA S.A. en el ámbito de aplicación, la empresa CENCOSUD COLOMBIA S.A. define que teniendo en cuenta la condición de encargado y responsable del tratamiento de datos, que le asiste a CENCOSUD COLOMBIA S.A., según las definiciones que para este efecto incluye la citada ley, por lo tanto el tratamiento al cual serán sometidos los datos personales y finalidad. CENCOSUD COLOMBIA S.A. podrá usar los datos capturados de los Titulares para las siguientes actividades:

En EASY COLOMBIA S.A.S. el tratamiento de datos personales se desarrolló conforme a las disposiciones de la ley 1581 de 2012, se define que el encargado del tratamiento es CENCOSUD COLOMBIA S.A. y el tratamiento que se da es consecuencia de las finalidades descritas, conocer y actualizar datos de carácter personal, almacenarla, ordenar, clasificar, o separar la información suministrada por el titular.

2.2.3.2 Datos sensibles. Se pudo evidenciar que en CENCOSUD COLOMBIA S.A. se consideran datos sensibles aquellos relacionados con datos sobre origen racial o étnico, la pertenencia a sindicatos, organizaciones sociales o de derechos humanos, convicciones políticas, religiosas, de la vida sexual, biométricos o datos de la salud, además de esto se clarifica que esta información podrá no ser respondida por el Titular, si no desea hacerlo.

2.2.3.3 Divulgación del tratamiento de los datos. En EASY COLOMBIA S.A., tienen el aviso donde les indican a los visitantes, que los datos personales son tratados en cumplimiento a la regulación de protección de datos personales (Ley 1581 de 2012), indicando: (Ver figura 3)

Figura 3. Aviso de privacidad. Easy Colombia S.A.S

Fuente: foto tomada al aviso de privacidad. EASY COLOMBIA S.A.S.

Figura 4. Aviso de Privacidad. Easy Colombia S.A.S.

Fuente: foto tomada al aviso de privacidad. EASY COLOMBIA S.A.S.

2.2.3.4 Consultas y requerimientos. CENCOSUD COLOMBIA S.A. le ofrecen varios medios para hacer consultas o reclamaciones, a través de medio físico por

medio de una PQR (Petición, Queja o Reclamo), telefónicamente, por correo electrónico, por medio de la página web. Al igual que la definición del responsable del tratamiento para la organización es CENCOSUD COLOMBIA S.A., identificada con número de NIT. 900.155.107-1 con domicilio en la calle 175 n° 22-13 de la ciudad de Bogotá, dirección electrónica www.easy.com.co y teléfono (571) 7429800.

2.2.3.5 Derechos y obligaciones de los titulares de la información. El Titular de la información compartida con CENCOSUD COLOMBIA S.A. tiene los derechos establecidos por la ley 1581 de 2012; por lo tanto, se aplican al tratamiento con las disposiciones legales establecidas.[18]

2.2.3.6 Diagnóstico del tratamiento de datos personales en EASY COLOMBIA S.A.S. En la empresa EASY COLOMBIA S.A.S se encontró una política de protección de datos bien estructurada y también una buena aplicación de la ley 1581 de 2012, es necesario fortalecer los lineamientos de la compañía en cuanto a divulgación interna de la política ya mencionada, ya que se tienen algunas dudas acerca de que son los datos personales por algunos de sus funcionarios y es necesario que todos estén involucrados en la correcta divulgación de la política hacia un usuario externo, ya que confunden este tipo de solicitud con un reclamo acerca de los productos o servicios que ofrecen.

2.2.3.7 Conclusiones de los hallazgos. En los tres casos examinados se encontraron hallazgos relevantes para el proyecto los cuales son:

- En el primer caso se pudo revisar el estado actual de la protección de datos personales en la DIAN, donde se pudo determinar los pasos para realizar una correcta implementación y como se puede integrar la ley 1581 de 2012, a los procesos en este primer diagnóstico se encontraron muchas falencias y poca regulación para el tratamiento de datos personales, si bien con la circular emitida blinda el tratamiento de datos personales, es necesario la implementación de la política de seguridad de datos personales.

- El segundo de los casos es la empresa CONSALFA S.A.S., la definición de la política de seguridad y protección de datos personales está definida e integrada a los procesos, para el MINTIC es de gran relevancia los hallazgos de este caso ya que permite definir y estructurar los procesos de acuerdo a la experiencia en el tratamiento de información personal, son determinantes los hallazgos al momento

[18] EASY COLOMBIA S.A. Reglamento de uso, manejo protección datos personales. [En Línea] [Consultado el 2 de noviembre de 2015]. Disponible en la World Wide Web <https://store-totalcode.netdna-ssl.com/easy/web_content/assets/Reglamento_Habeas_Data.pdf>.

de definir una política que controle y regule los datos recolectados al acceso del edificio MINTIC.

- El tercer caso, fue un diagnóstico realizado a EASY COLOMBIA S.A., donde se encontró una integración de la ley 1581 de 2012, a los procesos y se pudo validar cuales son los requerimientos de la política y los avisos de privacidad y la correcta publicación de los mismos es un factor esencial al momento de divulgar la política.

- Con el estado del arte se pudo dar un enfoque más adecuado a la normatividad colombiana, en la actualidad es un tema que está tomando una relevancia y cada una de las entidades se preocupa cada vez más del correcto tratamiento de los datos personales. El ámbito de la ley y el sector de la seguridad de la información es un campo que poco a poco ha ganado más importancia en todas las entidades del país y los ciudadanos entienden que por lo regular se recolectan datos personales y que pueden ser objeto de cualquier tipo de solicitud por parte del titular del dato personal.

3. ESTADO ACTUAL DEL TRATAMIENTO DE LOS DATOS PERSONALES

El MINTIC actualmente tiene definida su política de tratamiento de datos personales, la cual debe aplicar a todos los datos personales que son recolectados en la entidad a través de sus diferentes áreas.

Para el caso específico del presente trabajo, se ha realizado un análisis del estado actual del tratamiento de los datos personales recolectados en el acceso físico al MINTIC, con el fin de estimar la brecha que actualmente tiene la entidad para implementar la política de tratamiento de datos personales en este punto o zona, la cual es el primer contacto que tienen los visitantes cuando ingresan al edificio.

3.1 POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES MINTIC

La política de tratamiento de datos personales en el Ministerio Tic, está definida bajo el marco jurídico de Ley 1581 de 2012 y el Decreto 1377 de 2013, orientada siempre a proteger la confidencialidad, privacidad y la intimidad de las personas en cuento al tratamiento de datos personales. De esta forma el Ministerio definió dentro de la política un esquema para su tratamiento, como se muestra en la figura 5.

Figura 5. Esquema para tratamiento de los datos personales MINTIC

Fuente: elaborado por el Ministerio basado en el decreto 1377 de 2013

3.1.1 Objetivo general. Establecer el derecho constitucional y legal que tienen todas las personas a conocer, actualizar y rectificar la información que se haya

recogido sobre ellas en bases de datos o archivos del Ministerio de Tecnologías de la Información y las Comunicaciones.[19]

3.1.2 Objetivos Específicos. La política de tratamiento de datos personales MINTIC, establece los siguientes objetivos específicos:

- Establecer el marco de referencia en temas de tratamiento de datos personales al interior del Ministerio TIC en cumplimiento de la normatividad vigente sobre la materia.

- Establecer el responsable y encargado del tratamiento de los datos personales.

- Asignar responsabilidades a las áreas involucradas en el tratamiento de datos personales.

- Determinar los mecanismos técnicos que soporten el tratamiento de los datos personales.

3.1.3 Ámbito de aplicación. De acuerdo a la política, el Ministerio ha destinado aplicarla a todos los datos personales que tenga la entidad bajo su poder y responsabilidad.

3.1.4 Alcance. La política de tratamiento de datos personales del Ministerio TIC cobijara a los datos personales de los funcionarios, contratistas, colaboradores, proveedores, visitantes, usuarios y todas las personas que puedan tener algún tipo de relación con la entidad.

3.2 ¿CUÁLES SON LOS DATOS?

Teniendo presente el numeral 4 “Clasificación de Los datos”, de la política de tratamiento de datos personales en el MINTIC y el artículo 3, numeral 2 del Decreto 1377 de 2013, el tipo de datos personales recolectados en el control de acceso del edificio del Ministerio TIC, son los siguientes:

[19] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Política para el tratamiento de datos personales política de privacidad. (20, marzo, 2015). Bogotá, D.C. El Ministerio. 2015. 28 p.

3.2.1 Datos públicos. Nombre, apellido, documento de identidad. Estos datos son considerados públicos, teniendo en cuenta el numeral 2, articulo 3 decreto 1377 del 2013, puesto que no son semiprivados, privados o sensibles, están contenidos en un documento público de los visitantes, como puede ser la cedula de ciudadanía.

3.2.2 Datos sensibles. Huella dactilar índice derecho, Fotografía del rostro. Los anteriores datos son considerados sensibles ya que el artículo 5 de la ley 1581, establece que los datos sensibles son los que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación y señala entre ellos datos referentes al origen racial, étnico, relativos a la salud, la vida sexual y los datos biométricos.

La huella y el registro fotográfico de los visitantes en el MINTIC, son datos biométricos puesto que describen rasgos físicos de las personas naturales que ingresan a la entidad.

3.3 ¿DÓNDE ESTÁN LOS DATOS?

Los anteriores datos identificados son almacenados en 3 computadores portátiles y en un libro de registro de elementos, el cual es diligenciado a mano. Las anteriores herramientas están ubicadas en la recepción del edificio y de ese lugar no se mueven.

Los datos recolectados en los computadores, son organizados en dos tipos de bases de datos, una propiamente de un software de registro de datos y otra en una plantilla en Excel. A estos datos no se les aplica ninguna política de backup, siempre permanecen en esos equipos. Dos de los equipos son propiedad de la empresa de vigilancia y otro equipo pertenece al grupo de mesa de servicio. Ningún equipo está dentro del dominio de red, tampoco están conectados a internet, por lo cual no se actualizan, corren el riesgo de infectasen por algún virus malicioso o simplemente pueden correr cualquier riesgo físico o lógico, comprometiendo la información de datos personales que allí reposa, hasta el punto de perderse.

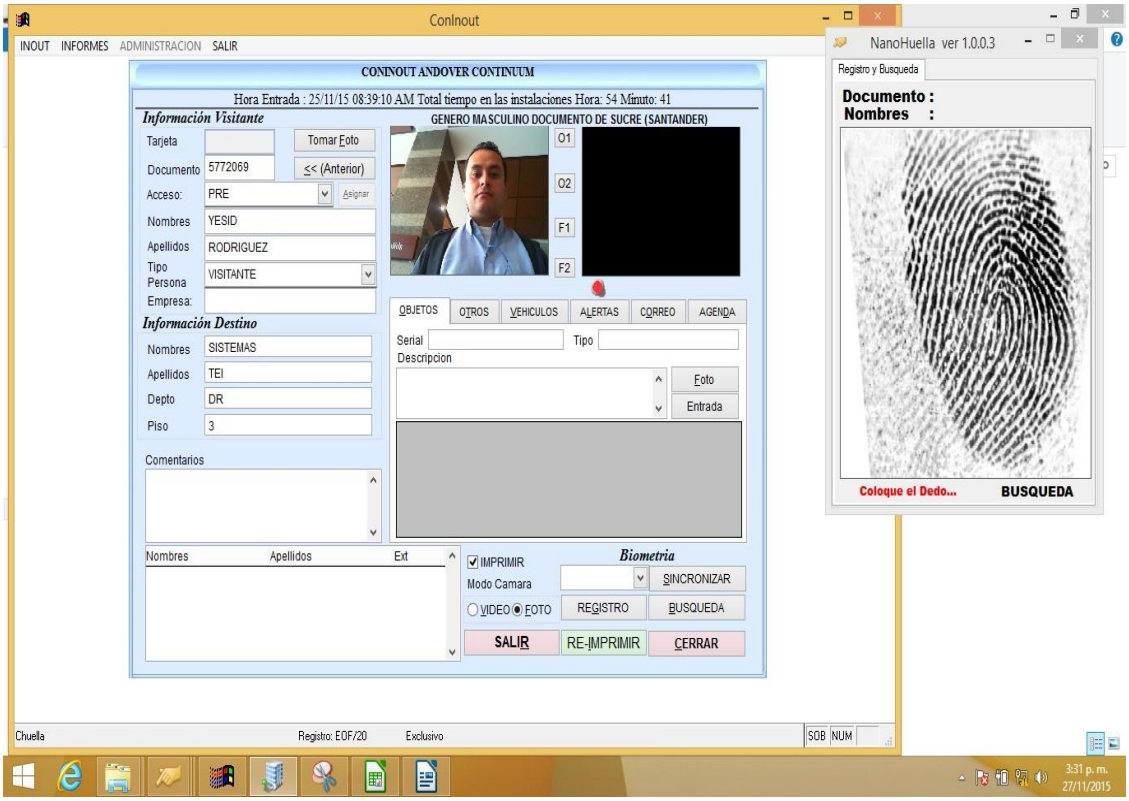
En el caso del libro de registro de elementos siempre permanece en las gavetas de la recepción, corriendo el riesgo de extraviarse o recibir algún daño físico, que pueda hacer ilegible la información de datos personales allí consignada.

3.4 ¿QUÉ HACEN CON LOS DATOS?

De acuerdo a la situación del registro solicitado al acceso del edificio del MINTIC, existen tres mecanismos bajo los cuales se pueden tomar los datos. De esta forma las personas pueden dejar sus datos personales en dos o los tres mecanismos de forma simultánea. A continuación, se aclaran esos tres mecanismos de registro.

3.4.1 Software de registro principal. Es el mecanismo de registro transcendental, puesto que es utilizado para registrar los datos personales de todos los visitantes que ingresan a la entidad. Los datos registrados en el software son los siguientes: Nombre, apellido, número de identificación, huella dactilar y fotografía de la persona. Con la recolección de esos datos el software genera una escarapela de identificación para el visitante, la cual se imprime y se le entrega a la persona para que la porte en un lugar visible mientras permanece en la entidad. (Ver figura 6)

Figura 6. Software de registro principal



Fuente: Snapshot tomado por los autores en pc utilizado para el registro.

3.4.2 Estampilla adhesiva de identificación personal. Esta estampilla o escarapela de identificación es generada después de que el visitante realiza el

registro en recepción y es entregada a éste, para que la porte en un lugar visible, mientras se encuentra en la entidad. Dicha estampilla contiene nombres, apellidos e identificación del visitante. (Ver figura 7)

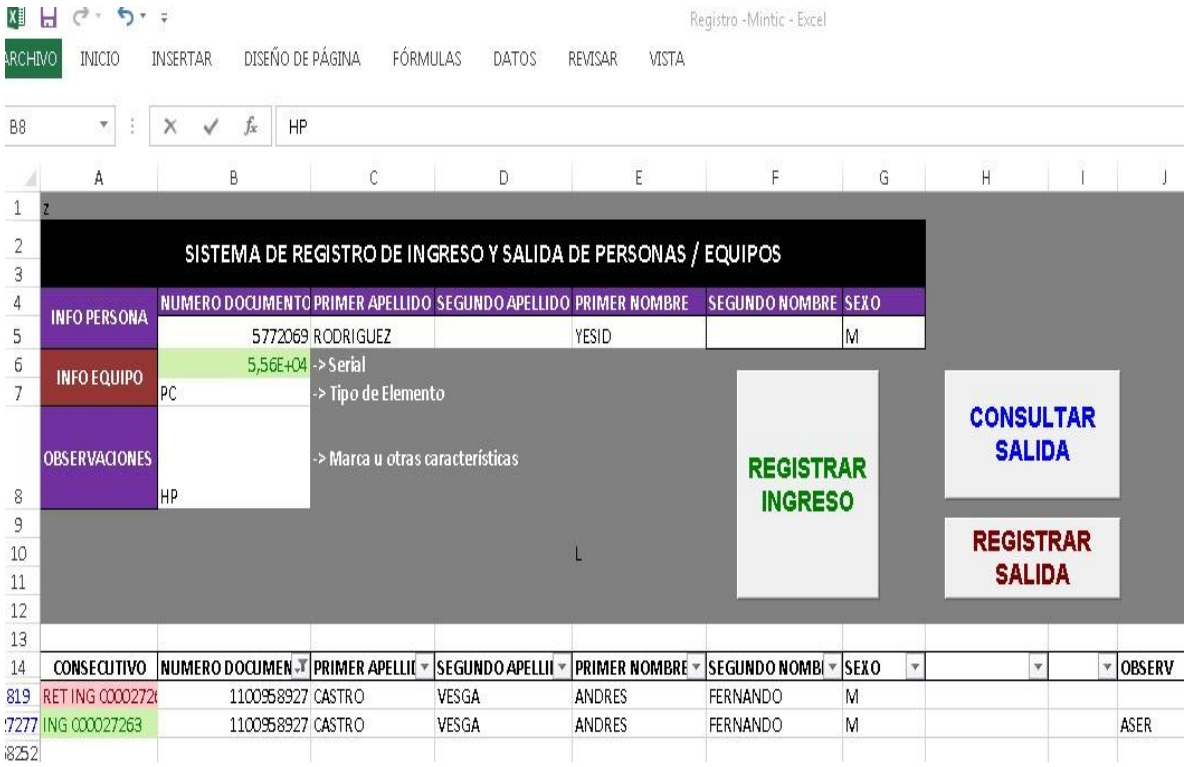
Figura 7. Estampilla adhesiva de identificación personal

Fuente: Fotografía tomado por los autores a una estampilla de identificación.

La estampilla de identificación es devuelta por el visitante en la recepción del edificio, recibida por el vigilante de turno, el cual apila junto con las otras estampillas, para que al final del día sean guardadas por la vigilancia en una caja. Las estampillas permanecen allí indefinidamente sin que de momento se destine un fin para las mismas.

3.4.3 Plantilla Excel para registro de computadores. Esta plantilla, está ubicada únicamente en un PC y la utilizan exclusivamente cuando la persona o visitante ingresa un computador. En esta plantilla son consignados el nombre y apellidos de las personas junto con el número de identificación; con el fin de asociarle los datos de serial y marca del computador que ingresa, para así poder retirar dicho equipo, cuando la persona sale de la entidad. De esta forma los datos personales anteriormente mencionados, pueden ser registrados en dos bases de datos distintos, siempre en cuando una persona ingrese a la entidad con un computador, realizando de esta forma un doble registro de sus datos. (Ver figura 8)

Figura 8. Plantilla Excel para registro de computadores

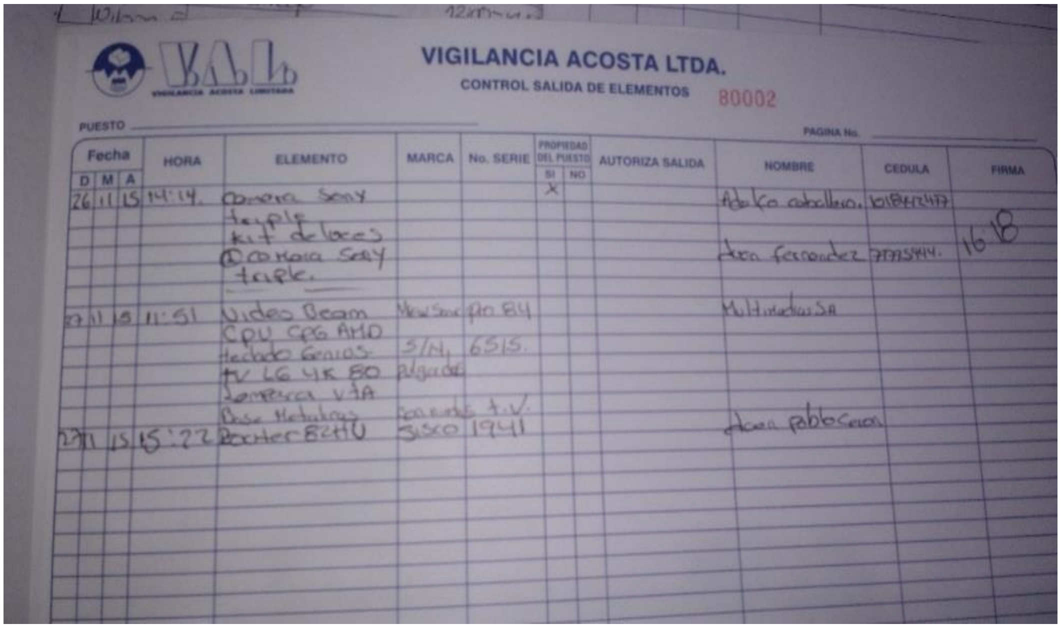


Fuente: Snapshot tomado por los autores en pc utilizado para el registro.

3.4.4 Libro de registro de elementos. Es un libro de registro auxiliar, el cual se diligencia a mano, y sirve para registrar elementos extra, que puede traer una persona, por ejemplo: una cámara fotográfica, herramientas de mano, equipos de comunicación, y en general cualquier elemento que sea significativo, el cual se debe registrar, por seguridad y para poder retirarlo cuando la persona salga de la entidad.

En dicho libro se registran los siguientes datos: Nombre, apellido y documento de identidad. (Ver figura 9)

Figura 9.Libro de registro de elementos



Fuente: fotografía tomado por los autores.

3.5 RESPONSABLE DEL TRATAMIENTO

A pesar de que existe una política de tratamiento de datos personales en la entidad, formalmente no se ha definido un responsable del tratamiento, para los datos personales recolectados en el control de acceso al ingreso de la entidad. Por lo cual es indispensable para la entidad definir un responsable idóneo, que pueda responder con claridad y oportunidad, ante cualquier requerimiento relacionado con el tratamiento.

3.6 ENCARGADO DEL TRATAMIENTO

Para este caso el encargado del tratamiento, es la empresa de vigilancia, que presta mediante contrato con el Ministerio, los servicios de seguridad física en la entidad. Dicha empresa actúa de manera libre, de la mejor manera e intensión posible, sin tener la plena conciencia y conocimiento que son los encargados del tratamiento de datos personales en el control de acceso a la entidad, puesto que no conoce la existencia de la política de tratamiento de datos personales del MINTIC, y tampoco la entidad a través del supervisor del contrato, la ha dado a conocer, es decir que

no existe una cláusula en el contrato donde la empresa se obligue a cumplir con dicha política.

La empresa de vigilancia, tiene el concepto que la recolección de datos la hacen, para registrar a los visitantes de la entidad, con el fin de cumplir con los requisitos de seguridad para el acceso de las personas. Por consiguiente, guardan los registros, para cuando una persona que regrese a la entidad, dicho registro sea más rápido.

El Ministerio cada año, cambia de empresa de vigilancia, y cada empresa ha implementado sus propios controles de registro para el acceso a la entidad, pero ninguna de ellas al final del contrato ha entregado las bases datos o libros de registros de datos personales, es decir el Ministerio ha tenido fuga de información de datos personales, recogidos al ingreso de la entidad y por consiguiente no tiene como responder ante cualquier requerimiento de datos personales, de años o meses anteriores, ya que la nueva empresa de vigilancia se encuentra prestando sus servicios desde noviembre del 2015.

De esta forma es necesario que el encargado del tratamiento de los datos personales, recolectados al ingreso del edificio de MINTIC, tenga pleno conocimiento de la política de tratamientos de datos personales de la entidad y se obligue a cumplirla mediante una cláusula estipulada en el contrato de servicios.

3.7 ANÁLISIS DE BRECHA PARA EL CUMPLIMIENTO DE LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES EN LA ENTIDAD

De acuerdo a la política de tratamiento de datos definida en el Ministerio de Tecnologías de la información y las comunicaciones, la cual está fundamentada en la ley 1581 del 2012 y el decreto 1377 de 2013, laentidad debe tener en cuenta los siguientes aspectos para cumplir con los objetivos general y específicos de dicha política.

- Definir el responsable del tratamiento de datos personales, que son recolectados en el control de acceso a la entidad.

- Dar a conocer la política de tratamiento de datos a la empresa de vigilancia, para que se responsabilice y cumpla la política como encargado del tratamiento.

- Actualmente en el contrato vigente que tiene el MINTIC con la empresa de vigilancia, no existen obligaciones o cláusula que exija el cumplimiento de la política de tratamiento de datos personales y otros aspectos relacionados, por lo cual el supervisor de dicho contrato debe solicitar una modificación al contrato vigente con

el fin de incluir todo lo pertinente al cumplimiento de la política, procedimientos y demás obligaciones relacionadas.

- Establecer una única herramienta de registro y base de datos, donde una persona mediante un único registro de sus datos personales, pueda registrar el computador o cualquier otro elemento, ya que de acuerdo a la situación actual una persona puede registra sus datos personales en tres herramientas de registro para un único ingreso, es decir, se puede registrar en la herramienta principal de registro, en la plantilla de Excel para registrar un computador y el libro de registro de elementos, por ejemplo, si trae consigo una cámara fotográfica.

- Realizar la divulgación de la política de tratamiento de datos personales, mediante aviso de tratamiento de datos personales al ingreso de la entidad y disponer de canales de comunicación entre los dueños de los datos y la entidad.

- Tener los procedimientos de autorización, consulta y reclamación de datos personales, que son recolectados en el control de acceso a la entidad, para que sean aplicados y cumplidos por los implicados.

- Recolección de dato biométrico. La herramienta tecnológica de registro mediante la cual se recolectan los datos personales es de propiedad de la empresa de vigilancia. Dicha herramienta tiene integrado un lector biométrico con el cual se recolecta la huella de los visitantes. No existe un requerimiento formal o necesidad explicita por parte del responsable de los datos donde se le indique a la empresa de vigilancia que se debe recolectar dicho registro biométrico, solamente se le indica de forma general que debe hacer control y registro de ingreso y salida de personal y elementos en el acceso al edificio, la entidad no le puntualiza cómo hacerlo y mucho menos qué datos recolectar. La única finalidad y uso por el cual la vigilancia recolecta la huella de los visitantes, es para cuando el titular del dato vuelva a ingresar a la entidad en una futura ocasión, se pueda encontrar rápidamente los datos registrados por la persona e imprimir la escarapela de identificación en el menor tiempo posible.

- Se recomienda al Ministerio no recolectar dicho dato hasta cuando tenga claro e identificada la necesidad de hacerlo, fundamentándose para ello en las excepciones que se mencionan en el artículo 6 de la ley 1581 del 2012, de lo contrario el control es excesivo y lesiona la intimidad del titular.

4. PROPUESTA DEL PLAN PARA LA IMPLEMENTACIÓN DE POLÍTICA

Se propone al Ministerio de Tecnologías de la Información y las Comunicaciones, el siguiente plan, para cumplir e implementar la política de tratamiento de datos personales, en los que son recolectados en el control de acceso de la entidad, el cual se compone de las siguientes actividades y acciones.

4.1 TRATAMIENTO DE LOS DATOS

4.1.1 Responsable del tratamiento de los datos personales. El Ministerio de Tecnologías de la Información y las Comunicaciones, en su política de tratamiento de datos personales, se define o se atribuye de forma general, como el responsable del tratamiento de datos personales que son recolectados en la entidad, encabezado por el Ministro. Éste a su vez puede delegar esas atribuciones en los funcionarios de la entidad que a bien convenga, como lo son: Jefes de área y/o dependencias, asesores, funcionarios de carrera administrativa etc.

Para el Ministro de Tecnologías de la Información y las Comunicaciones, hacerse cargo directamente como responsable del tratamiento de datos personales, se le puede volver un tanto dispendioso, debido a sus diversos compromisos y funciones primordiales. De esta forma para el Ministro TIC, le queda más eficiente delegar la responsabilidad, con el fin de tener un mejor control y eficiencia en el tratamiento de datos personales. De acuerdo a lo anterior el Ministro puede delegar la responsabilidad a diferentes dependencias en cabeza de sus coordinadores, siempre en cuando en las actividades diarias de dichas dependencias se recolecten datos personales.

Como la presente propuesta se centra en los datos personales que son recogidos en el control de acceso a la entidad, se estima conveniente que la responsabilidad del tratamiento de los datos personales en cuestión, sea delegada por el Ministro TIC a la Coordinación de Gestión de Servicios Administrativos, en cabeza de su respectivo Coordinador por las siguientes razones:

- Como se define en el numeral e) artículo 3 de la ley 1581 de 2012, el responsable del tratamiento es una “persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de datos”, es decir que para el caso de los datos personales recolectados en el control de acceso del MINTIC, el Ministro siendo una persona pública puede decidir sobre la base de datos y/o el tratamiento en asocio con la Coordinación de Gestión de Servicios Administrativos.

- Dicha coordinación es la encargada de gestionar y supervisar el contrato de prestación de servicios con la empresa de vigilancia, a través de la cual son recolectados los datos personales en el acceso físico a la entidad.

- Mediante la supervisión del contrato de la empresa de vigilancia, la Coordinación de Gestión de Servicios Administrativos puede controlar y manejar de una forma eficiente y efectiva el tratamiento de los datos personales recolectados en el control de acceso por dicha empresa exigiendo el cumplimiento de la política, la ley y los procedimientos planteados en la presente propuesta.

4.1.1.1 Funciones responsables del tratamiento. Las funciones para el responsable del tratamiento, se plantean de acuerdo a la política interna de tratamiento de datos personales del MINTIC, con el fin de que el responsable cumpla con lo establecido en el artículo 17 de la ley 1581 del 2012 (deberes de los responsables del tratamiento)

- Dar a conocer la política de tratamiento de datos personales a los titulares y encargado del tratamiento, mediante aviso impreso, comunicados internos, charlas o cualquier otro medio o forma que estime conveniente.

- Incluir el cumplimiento de la política de tratamiento de datos dentro del contrato de prestación de servicios que realice con la empresa de vigilancia de turno. Esto con el fin de que la empresa de vigilancia pueda ser designada como la encargada del tratamiento.

- Responder a los diferentes requerimientos, de acuerdo a la ley, que los titulares de los datos hagan o soliciten, por medio de los mecanismos de respuesta o comunicación que se establezcan

- Mantener los medios o canales, donde se le solicite la autorización al titular, se puedan recibir las consultas y solicitudes, donde se informe la finalidad del tratamiento y los derechos que tienen los titulares. Éstos medios o canales pueden ser un correo electrónico, aviso de tratamiento y solicitud de autorización, línea telefónica y punto de atención físico.

- Garantizar la disponibilidad, confidencialidad e integridad de los datos personales, gestionando los recursos que la entidad disponga para tal fin, como bases de datos, sistemas de almacenamiento, archivo etc.

- Solicitar de forma periódica, Backup de las bases datos utilizadas por el encargado del tratamiento, trasladando dicha información al sistema de almacenamiento de la entidad.

- Exigir al encargado del tratamiento la entrega de los libros de registro manual cuando éstos se hayan llenado completamente, con el fin de trasladarlos al archivo de la entidad. Dicha exigencia se puede establecer como una cláusula del contrato de prestación de servicios con la empresa de vigilancia.

4.1.2 Encargado del tratamiento. Para el caso de los datos personales que son recolectados al acceso de la entidad, el encargado del tratamiento debe ser la empresa de vigilancia, en cabeza del coordinador de vigilancia. Ya que son los encargados de recolectar los datos personales que las personas registran al ingreso, a través de las herramientas tecnológicas dispuestas para ello.

Es indispensable que la designación del encargado del tratamiento, para este caso la haga la Coordinación de Gestión de Servicios Administrativos, en cabeza de su respectivo Coordinador (responsables del tratamiento), dejando por escrito en el contrato de prestación de servicios, una cláusula donde se designe como encargado del tratamiento de los datos personales recolectados en el control de acceso a la entidad, puntualizando que deben cumplir con la política del MINTIC y lo establecido en la ley 1581 del 2012 y decreto 1377 del 2013. Designando para ello unas funciones específicas dentro del contrato, para lo cual, en el siguiente numeral se proponen las siguientes.

4.1.2.1 Funciones encargado del tratamiento. Las funciones para el encargado del tratamiento, se plantean de acuerdo a la política interna de tratamiento de datos personales del MINTIC, con el fin de que el encargado cumpla con lo establecido en el artículo 18 de la ley 1581 del 2012 (deberes de los encargados del tratamiento).

- Realizar el registro de los datos, una vez obtenida la autorización del titular, mediante el debido procedimiento establecido para tal fin.

- Conocer y aplicar los procedimientos establecidos, para cumplir y dar trámite a cualquier solicitud que hagan los titulares de los datos.

- Tener a disposición los registros de los datos, que son recolectados a través del software o base de datos de registro y de los que son recolectados en el libro de registro de elementos.

- No entregar los datos a terceros, a excepción de los casos reglamentados por ley y al responsable de dichos datos en la entidad.

- Permitir que se haga Backup de los datos, bajo el debido procedimiento aprobado por la entidad para tal fin.

- Entregar los libros de registro manuales de datos, al responsable del tratamiento, para que este pueda enviarlos al archivo de la entidad.

- Entregar la estampilla adhesiva de identificación que devuelve el visitante, al responsable del tratamiento.

- Entregar en su totalidad la base de datos y libro de registro manual de datos recolectados en el control de acceso de la entidad, al responsable del tratamiento una vez finalizado el contrato. Lo anterior con el fin de evitar fuga de datos personales y sobre los cuales el Ministerio está obligado a responder sobre el tratamiento a que se sometan.

4.1.3 Administración de los datos. Los datos recolectados en el control de acceso de la entidad, deben ser administrados por el responsable del tratamiento, es decir por la Coordinación de Gestión de Servicios Administrativos, en cabeza de su respectivo Coordinador. Dicha administración, teniendo en cuenta los deberes del encargado del tratamiento, enunciados en la ley 1581 del 2012, implica conservar los datos de forma segura, preservando la confidencialidad, la disponibilidad e integridad. De esta forma se sugiere, para los datos recolectados en el control de acceso los siguientes factores, con el fin de que el encargado del tratamiento, realice una buena administración.

4.1.3.1 Almacenamiento de los datos. Como los datos recogidos en la recepción del Ministerio, tienen dos formatos uno digital, los que son almacenados en los PC de registro y otro escrito, los que son colocados en el libro de registro de elementos. Se sugiere dos alternativas de almacenamiento para los mismos:

4.1.3.1.1 Datos recogidos en los PC de registro. En primera instancia, como los equipos son propiedad de la empresa de vigilancia, éstos se deben ingresar al dominio de red, con el fin de poder instalar la herramienta de data protector, que utiliza la entidad y de esta forma poder realizar de forma controlada backup a los datos recolectados en esos equipos. También se puede considerar instalar la base de datos, del programa de registro en un servidor remoto, el cual estaría en el centro de datos de la entidad, para que de esta forma los registros tomados con los equipos de la empresa de vigilancia, no quede almacenados en éstos, sino directamente en los equipos de la entidad, para de esta forma aplicar políticas de backup a los mismos.

Cualquiera de los dos mecanismos, mencionados anteriormente para el almacenamiento de los datos, debe estar bajo la responsabilidad de la Coordinación de Gestión de Servicios Administrativos, en cabeza de su respectivo Coordinador. Para lo anterior el responsable del tratamiento, debe solicitar las herramientas

tecnológicas de almacenamiento y backup a la Oficina de TI del Ministerio, quienes aprovisionaran dichas herramientas, bajo las respectivas prácticas de seguridad de la información, que dicha oficina aplique. Empezando con el ingreso al dominio de red de las maquitas, hasta la instalación de la herramienta de data protector en los equipos o configuración de la base de datos en un servidor remoto, junto con las respectivas credenciales de acceso.

4.1.3.1.2 Datos recogidos en el libro registros de elementos. Este tipo de datos como son recolectados de forma escrita, es preferible que cuando dicho libro se encuentre lleno o termine el contrato con la empresa de vigilancia, sea remitido por el responsable del tratamiento al archivo de la entidad, donde será foliado y almacenado, según como lo disponga la ley. Para ello el ministerio tiene contratado una empresa que administra dicho archivo, la cual aplica la normatividad vigente de la retención documental.

4.1.3.1.3 Estampilla adhesiva de identificación personal. Como se mencionó anteriormente, las estampillas de identificación de momento no tienen ningún fin, son almacenadas en una caja que custodia la empresa de vigilancia, corriendo el riesgo que dichas estampillas sean tomadas por terceros, para fines criminales que puedan comprometer la seguridad en general de la entidad.

Para evitar cualquier tipo de delito o incidente de seguridad, mediante el uso indebido de las estampillas, se sugiere destruirlas, con el fin de que no puedan ser reutilizadas con fines delictivos.

4.2 DIVULGACIÓN DEL TRATAMIENTO DE LOS DATOS

4.2.1 Aviso del tratamiento de datos personales de acuerdo a la ley y a la política. Es necesario que la entidad tenga visible un Aviso, donde se le indique a los visitantes, que los datos personales entregados en el registro, serán tratados de acuerdo a las disposiciones de la ley y la política interna de tratamiento de datos personales del Ministerio, para ello se propone que el aviso contenga los siguientes elementos:

- Identificación de la entidad
- Informar acerca de la política que será aplicada para el tratamiento
- La finalidad del tratamiento
- Los medios y mecanismos para acceder a la información, con el fin de corregirla, actualizarla, retirarla etc.

Teniendo en cuenta los anteriores elementos, se propone el siguiente Aviso:

El Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), dando cumplimiento a la ley 1581 del 2012, al decreto 1377 de 2013 el cual reglamenta la mencionada ley y la política de tratamiento de datos personales definida en la entidad, informa que los datos personales suministrados por los visitantes en el control de acceso de la entrada al edificio de la entidad, serán tratados mediante procedimientos técnicos y administrativos de seguridad, con el fin de impedir que los datos sean accedidos y utilizados por terceros no autorizados, lo anterior en virtud de lo definido en la ley.

El responsable del tratamiento de datos suministrados por los visitantes en el control de acceso de la entrada al edificio de la entidad, es el MINTIC a través de la Coordinación de Gestión de Servicios Administrativos, quien recogerá los datos personales mediante las herramientas de registro ubicadas en la entrada del edificio y serán usados para: actividades de registro e identificación dentro del Ministerio, atender o formalizar cualquier tipo de tramite o servicio que el visitante requiera o solicite y para el cumplimiento de una obligación legal o contractual

El titular de los datos podrá ejercer sus derechos amparados en la ley, mediante los procedimientos adoptados por la entidad para tales fines, los cuales pueden pedir en la recepción de la entidad o vía correo electrónico a la dirección datos_personales@mintic.gov.co.

Leído lo anterior, el titular de los datos, autoriza de forma previa, explicita e inequívocamente al Ministerio de Tecnologías de la Información y las comunicaciones para el tratamiento de los datos personales suministrados en el control de acceso de la entrada al edificio de la entidad, dentro de las finalidades legales establecidas en la ley. De esta forma el titular autoriza el tratamiento de sus datos personales, que ha suministrado voluntariamente, siendo completa, confiable, veraz, exacta y verídica, quedando como constancia de dicha autorización nombre, apellidos, identificación, foto registro del titular y firma.

4.3 DISPOSICIÓN DE CANALES DE COMUNICACIÓN PARA LOS TITULARES DE LOS DATOS

4.3.1 Correo institucional. De acuerdo a la política de tratamiento de datos personales de la entidad, el Ministerio TIC dispone de un correo institucional denominado *datos_personales@mintic.gov.co,* el cual lo deben poner a disposición para que los titulares de los datos, realicen sus respectivas solicitudes, relacionadas con el tratamiento de datos personales. De esta forma, el responsable del tratamiento, podrá dar respuesta oportuna y efectiva, a las solicitudes que al respecto se presenten.

4.3.2 Punto de atención. Es indispensable poner a disposición el punto de atención al ciudadano, para que, a través de este mecanismo, se reciban solicitudes referentes al tratamiento de los datos personales recolectados en el ingreso del edificio. Desde este punto también serán direccionadas las solicitudes al responsable del tratamiento, que lleguen al respecto.

4.3.3 Línea telefónica de atención. El Ministerio TIC, actualmente cuenta con dos líneas de atención, las cuales son el PBX 343460 y la línea gratuita 01-800-0914014. Con estos dos contactos telefónicos también se pueden canalizar las solicitudes de los titulares de los datos recolectados en el control de acceso de la entidad, para que sean enviadas al responsable del tratamiento.

4.3.4 Página Web. El Ministerio también pone a disposición de los ciudadanos, la página web de la entidad www.mintic.gov.co, mediante la cual a través del link atención al publicado - (PQRSD) como se muestra en la figura 10, el Ministerio podrá indicarles a los titulares de los datos recolectados en la recepción del edificio, que por dicho medio pueden realizar las solicitudes o consultas, que tengan sobre el tratamiento de sus datos personales.

Figura 10. Link MINTIC atención al público – PQRSD

Fuente: snapshot de la página MINTIC tomado por los autores.

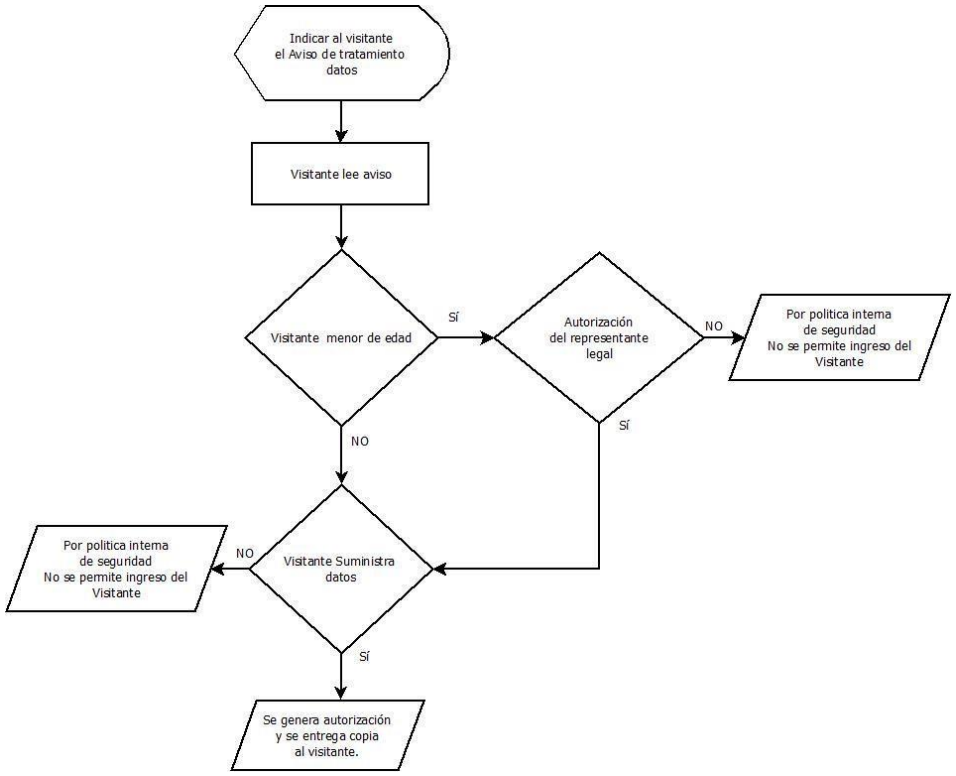
5. PROCEDIMIENTOS DE ACUERDO A LA POLÍTICA Y LA LEY

Se proponen tres procedimientos fundamentales y básicos, que le permitirá al Ministerio TIC poder implementar la política de tratamiento de datos personales al control de acceso en el ingreso de la entidad. Los procedimientos son planteados de acuerdo a la política, la ley 1581 del 2012 y el decreto 1377 del 2013, buscando en todo momento garantizar los derechos de los titulares y la seguridad en la información para los datos personales.

5.1 PROCEDIMIENTO PARA AUTORIZACIÓN

El procedimiento de autorización aplica una única vez, cuando la persona o visitante, ingresa por primera vez a la entidad y suministra sus datos personales. Posteriormente cada vez que el visitante quiera ingresar nuevamente al Ministerio, simplemente suministra el número de identificación, para imprimir una escarapela de identificación, con la previa autorización del funcionario o dependencia hacia donde se dirige.(Ver diagrama 1)

Diagrama 1. Procedimiento de autorización



Fuente: autores.

5.1.1 Ingreso del Visitante. Cuando la persona ingresa a la entidad, lo primero que debe hacer es registrarse en la recepción. En la recepción debe estar expuesto el Aviso de tratamiento de datos personales. Dicho aviso debe ser indicado al visitante por el personal de vigilancia, con el fin de que lo lea, para que decida si suministra o no los datos.

5.1.2 Generación de la autorización. Para realizar un óptimo tratamiento de los datos personales suministrados, en el acceso al edificio y en miras de poder garantizar la autenticidad de la persona, cuando realice una futura reclamación, el Ministerio debe pedir los siguientes datos:

- Nombres y apellidos
- Identificación, indicando el tipo de documento
- Teléfono o celular de contacto
- Correo electrónico
- Registro fotográfico.
- Fecha de la autorización
- Firma

Los anteriores datos, serán digitalizados por el personal de la recepción, con los cuales se genera la autorización, la cual será impresa y se le entregará al titular de los datos para que la firme. Con la autorización firmada, se le entregara una copia al visitante y se le permitirá el ingreso, entregándole la escarapela de identificación, previa autorización del funcionario o dependencia para donde se dirija.

5.1.3 Generación de autorización para menor de edad. Para menores de edad, la autorización para el tratamiento de los datos, la debe suministrar el tutor legal del menor, de forma verbal en la recepción o escrita con firma y copia del documento de identidad.

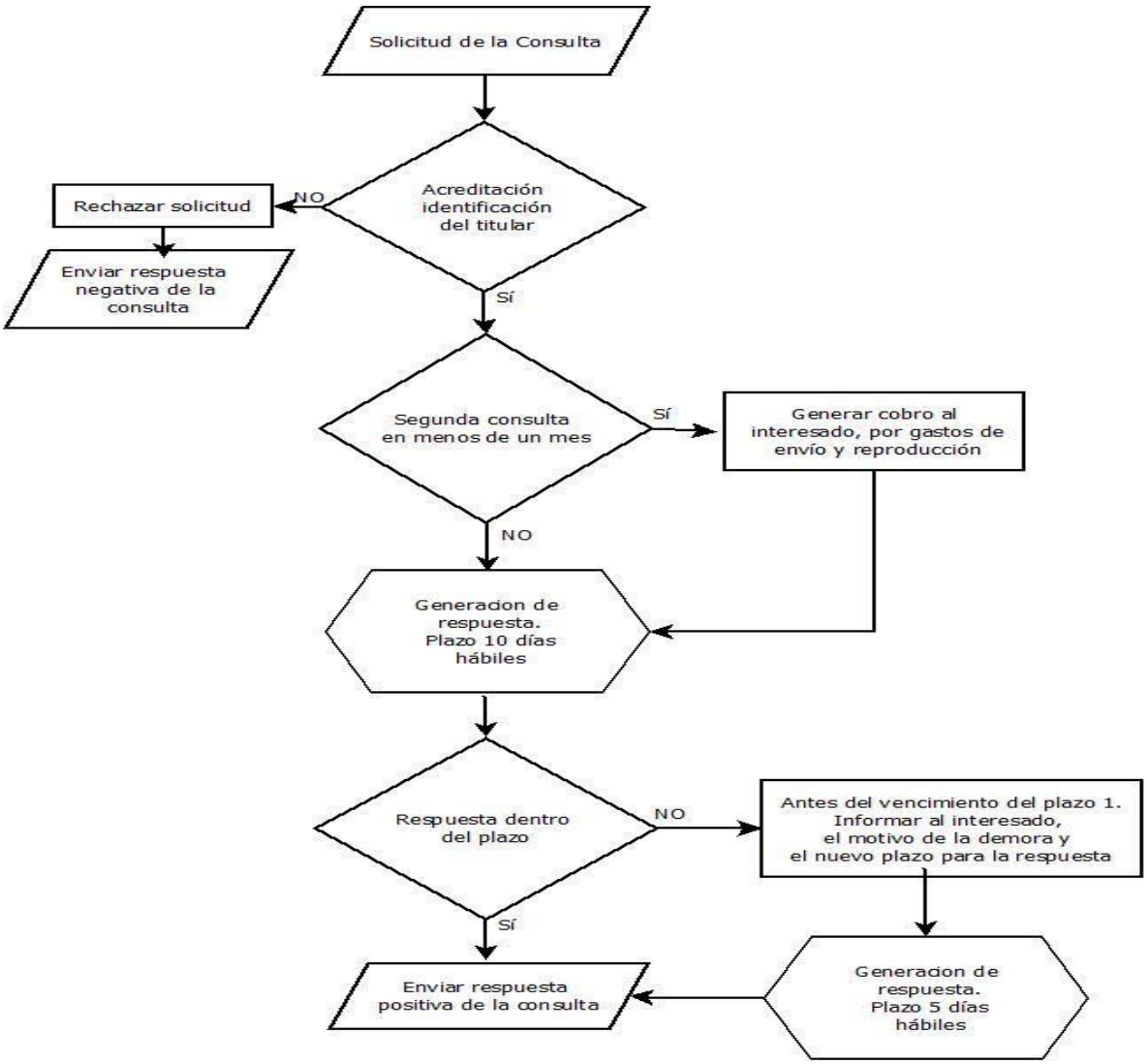
Cuando el tutor del menor concede de forma verbal la autorización, dicha autorización se imprime con los datos del menor y los datos de la persona que autoriza, para que sea firma por ésta, entregándole la respectiva copia de dicha autorización.

5.1.4 Negación para dar autorización. Cuando el visitante se niegue a suministrar los datos, el Ministerio puede negarle el ingreso a dicha persona, ya que por política de seguridad, toda persona que ingrese y transite por las instalaciones de la identidad, debe estar plenamente identificado. De esta forma el Ministerio debe dar a conocer al visitante dicha decisión a través del encargado del tratamiento, en primera instancia o una segunda instancia a través del responsable del tratamiento.

5.2 PROCEDIMIENTO PARA CONSULTA

El procedimiento de consulta busca garantizar al titular de los datos el derecho al acceso de la información, es decir el derecho saber o confirmar qué datos son los que tiene una determinada entidad pública o privada donde hayan registrado sus datos personales. (Ver diagrama 2)

Diagrama 2.Procedimiento de consulta



Fuente: autores.

5.2.1 Solicitud de Consulta. Para consulta de los datos personales, Ministerio TIC, tiene a disposición los siguientes canales de comunicación a donde los titulares de los datos pueden dirigir la consulta:

- Correo electrónico: *datos_personales@mintic.gov.co*
- Página web: www.mintic.gov.co en el link contáctenos (PQRSD).
- Punto de atención. En el edificio de la entidad

Por cualquiera de los anteriores canales, el titular de los datos puede realizar la solicitud de consulta de su información. De esta forma es obligación del responsable del tratamiento, una vez validados los datos del titular, dar una respuesta en los tiempos que exige la ley, 10 días hábiles a partir de la radicación de la solicitud.

5.2.2 Acreditación Identificación del Titular. Para que el usuario pueda presentar y recibir una respuesta a la solicitud de consulta, debe indicar los siguientes datos:

- Nombres y apellidos
- Identificación, indicando el tipo de documento
- Teléfono o celular de contacto
- Correo electrónico
- Fecha de la autorización
- Firma. Para los casos en donde el titular radique la solicitud en el punto de atención.

El titular debe tener en cuenta en relacionar los mismos datos que registro en el momento de la autorización, de lo contrario la solicitud de consulta será rechazada y la persona debe hacer una nueva solicitud con los datos correctos, o si es el caso, pedir una actualización o rectificación de los datos.

5.2.3 Consultas del titular en menos de un mes. Como se sustenta en la política de tratamiento de datos personales del MINTIC, cuando una persona realice solicitudes de consulta con una prioridad menor a un mes, la entidad a través del responsable del tratamiento le debe informar al titular que se generará un cobro por conceptos de envío, reproducción, y certificación según aplique. Es necesario dar a conocer el monto exacto junto con los medios de pago, donde la persona puede consignar dicho valor. De esta forma una vez realizado el pago por el titular de los datos, este le debe confirmar a la entidad, enviando un correo a *datos_personales@mintic.gov.co, o* llamando al PBX de la entidad, para que informe el número de transacción o consignación realizada.

Si el titular no ha confirmado el número de consignación o transacción, el responsable del tratamiento enviara un comunicado, antes de que se termine los 10 días hábiles para dar respuesta a dicho interesado solicitando el número en

cuestión, de lo contrario el Ministerio enviara una respuesta negativa explicando las razones.

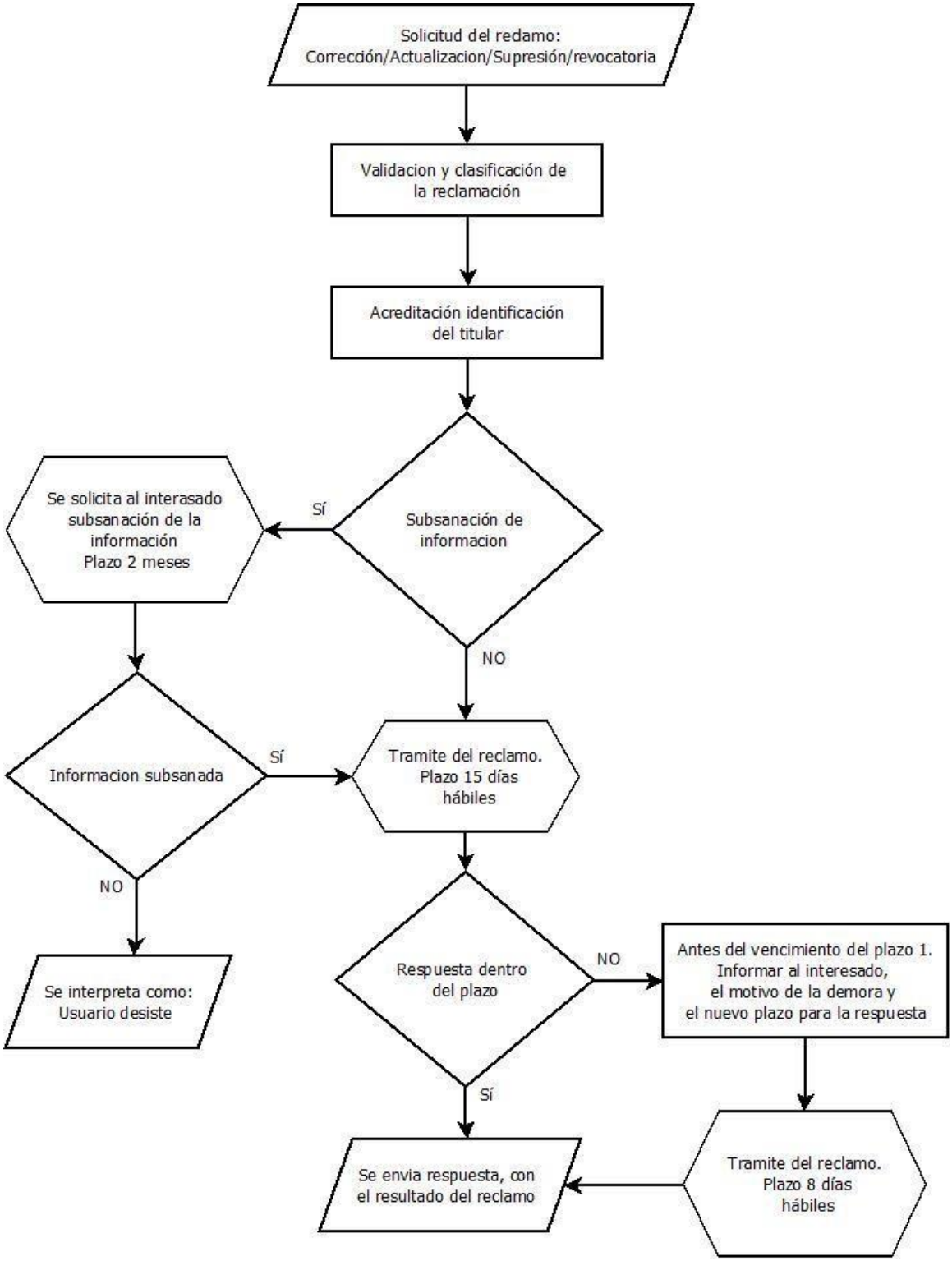
5.2.4 Plazo para dar respuesta. Como se señala en la ley 1581 del 2012 y como se adoptó en la política, el responsable del tratamiento tiene 10 días hábiles a partir del momento en que se radique la solicitud de consulta. El Ministerio debe confirmarle al titular un numero de radicado con fecha, para que así las dos partes empiecen a contar el tiempo. Dicha confirmación se debe hacer a través del correo o el número de contacto del interesado.

Cuando el responsable del tratamiento considere que no puede dar respuesta al titular dentro de los primeros 10 días hábiles, éste le debe informar al interesado, antes de que se acabe dicho plazo, los motivos de la demora e indicándole el nuevo plazo para la entrega de la respuesta. El nuevo plazo, como lo establece la ley, no podrá superar los 5 días hábiles una vez terminado el tiempo para el primer plazo.

5.3 PROCEDIMIENTO PARA RECLAMACIÓN

De acuerdo con la política de tratamiento de datos personales del MINTIC, el procedimiento de reclamación está encaminado para dar respuesta a solicitudes de corrección, actualización, supresión y revocatoria de la autorización de los datos personales, derechos que pueden exigir los titulares de los datos y que el responsable del tratamiento debe garantizar y cumplir, de acuerdo a la ley. (Ver diagrama 3)

Diagrama 3. Procedimiento de reclamación



Fuente: autores.

5.3.1 Solicitud de la reclamación. Para cualquier solicitud de reclamación (corrección, actualización, supresión) de los datos personales, Ministerio Tic, tiene a disposición los siguientes canales de comunicación a donde los titulares de los datos pueden dirigir la reclamación:

- Correo electrónico: *datos_personales@mintic.gov.co*
- Página web: www.mintic.gov.co en el link contáctenos (PQRSD).
- Punto de atención. En el edificio de la entidad

Por cualquiera de los anteriores canales, el titular de los datos puede realizar la solicitud de reclamación de su información. De esta forma es obligación del responsable del tratamiento, una vez validados los datos del titular, dar una respuesta en los tiempos que exige la ley, 15 días hábiles a partir de la radicación de la solicitud.

5.3.2 Validación y clasificación de la reclamación. El titular de los datos, debe ser específico y puntual en la solicitud de reclamación. De esta forma debe indicar cual o cuales datos personales se deben corregir/ actualizar / suprimir según el caso o indicar si la solicitud es de revocatoria de la autorización, justificando el motivo.

Para el caso de una solicitud de supresión de datos o revocatoria de la autorización para el tratamiento de datos personales, es deber del responsable del tratamiento evaluar bajo qué condiciones legales puede conceder o negar la supresión de los datos o la revocatoria de la autorización. Dando a conocer y justificando bajo un marco legal y normativo la decisión tomada.

Si la solicitud no es clara, el responsable del tratamiento debe pedir al titular de los datos la subsanación de la información indicándole que tiene como máximo 2 meses, pasado este plazo la reclamación será rechazada. El responsable del tratamiento también debe indicarle que una vez subsanada la información la solicitud quedará formalmente radicada.

5.3.3 Acreditación de la identificación del titular. Para que el usuario pueda presentar y recibir una respuesta a la solicitud de reclamación, debe indicar los siguientes datos:

- Nombres y apellidos
- Identificación, indicando el tipo de documento
- Teléfono o celular de contacto
- Correo electrónico
- Fecha de la autorización
- Firma. Para los casos en donde el titular radique la solicitud en el punto de atención.

El titular debe tener en cuenta en relacionar los mismos datos que registro en el momento de la autorización, con el fin de evitar contratiempos en la solicitud.

Si falta un dato o alguno está mal y este no ha sido advertido por el titular de la información dentro de la solicitud, el responsable del tratamiento debe pedir al titular de los datos la subsanación de la información indicándole que tiene como máximo 2 meses, pasado este plazo la reclamación será rechazada. El responsable del tratamiento también debe indicarle que una vez subsanada la información la solicitud quedará formalmente radicada.

5.3.4 Plazo para dar respuesta. Como se señala en la ley 1581 del 2012 y como se adoptó en la política, el responsable del tratamiento tiene 15 días hábiles a partir del momento en que se radique la solicitud de consulta. El ministerio debe confirmarle al titular un numero de radicado con fecha, para que así las dos partes empiecen a contar el tiempo. Dicha confirmación se debe hacer a través del correo o el número de contacto del interesado.

Cuando el responsable del tratamiento considere que no puede dar respuesta al titular dentro de los primeros 15 días hábiles, éste le debe informar al interesado, antes de que se acabe dicho plazo, los motivos de la demora e indicándole el nuevo plazo para la entrega de la respuesta. El nuevo plazo, como lo establece la ley, no podrá superar los 8 días hábiles una vez terminado el tiempo para el primer plazo.

6. CONCLUSIONES

- El presente trabajo permitió estructurar la propuesta de un plan y procedimientos, para que el Ministerio TIC implemente la política de tratamiento de datos personales, en una zona álgida de la entidad, como lo es el control de acceso físico en la recepción del edificio, donde diariamente ingresa un número considerable de visitantes, los cuales en cualquier momento pueden realizar cualquier solicitud respecto a sus datos personales registrados en dicha zona, amparados bajo la ley 1581 del 2012 y el decreto 1377 del 2013. De esta forma se le proporciona una herramienta al Ministerio Tic, para que pueda dar respuesta a dichas solicitudes basados en la ley y la política interna de la entidad.

- La identificación de los datos personales recolectados y el lugar actual donde reposan, permitió establecer el punto de partida para conocer el problema y establecer una brecha, con el fin de saber qué le hace falta al Ministerio para que pueda implementar su política de tratamiento de datos personales en el control de acceso a la entidad y así cumplir con la ley, para que de esta forma se eviten alguna demanda legal por el no cumplimiento.

- Mediante la identificación de la brecha para la implementación y cumplimiento de la política de tratamiento de datos personales definida en la entidad, se logró establecer actividades y acciones encaminadas a lograr el objetivo en cuestión. Dichas actividades y acciones también están encaminadas para dar el soporte a los procedimientos que se proponen fundamentados en la política y la ley. De esta forma se busca realizar una propuesta totalmente relacionada, con el fin de que la entidad pueda realizar un adecuado tratamiento de los datos personales en el control de acceso físico.

- Los procedimientos planteados están enfocados no solamente para que puedan ser comprendidos por el responsable y el encargado del tratamiento, sino también, para que puedan ser entendidos por los titulares de los datos, puesto que es un deber del Ministerio dar a conocer dichos procedimientos para que las personas que autoricen el tratamiento de sus datos personales en el control de acceso, tengan la garantía y tranquilidad de que sus datos van a estar seguros y solamente se utilizaran para el tratamiento que autorizaron, conociendo también como exigir los derechos a los que la ley 1581del 2012 hace referencia.

- La presente propuesta ayudará a los funcionarios y visitantes del Ministerio de Tecnologías de la Información y las Comunicaciones a dimensionar la magnitud de los datos personales y cuál es su importancia de garantizar un óptimo tratamiento y

de exigir que sea informado el uso que se le darán a dichos datos en las organizaciones, para este caso en el sector público.

- El proyecto permitió conocer y estudiar la normatividad vigente en el país, sobre la protección de los datos personales y el tratamiento que se le deben dar y exigir a dichos datos. Como profesionales de la seguridad en informática, permite establecer el alcance y la importancia de los datos personales que se suministran habitualmente en entidades, en internet, en la calle y en general en cualquier parte donde los soliciten, puesto que el titular debe entender y comprender muy bien para que se recolectan y el responsable debe tener claro el tratamiento y buen uso de los datos que se recolecten, de acuerdo a la ley y a las políticas internas de la organización o empresa donde se labore.

- El Ministerio TIC es un claro ejemplo, donde se evidencia y se muestra que todavía hay bastante trabajo por hacer en materia de protección de datos personales, puesto que definir una política de tratamiento para estos datos no es suficiente, se debe actuar, analizar y generar los procedimientos necesarios que permitan cumplir con la política. La presente propuesta es un inicio, para que el Ministerio Tic implemente su política de tratamiento de datos personales en el control de acceso físico a la entidad y desde allí realizar el monitoreo y evaluación de dicha implementación que le permitirá realizar los ajustes necesarios, no solo para tener una mejora continua al respecto, sino que también le permitirá generar conocimiento y experiencia para poder implementar dicha política en otras áreas o dependencias de la entidad, donde se recolecten datos personales.

7. RECOMENDACIONES

- Teniendo en cuenta que los procedimientos para la implementación de la política de tratamiento de datos personales en el acceso físico de la entidad, están fundamentados en la ley 1581 del 2012 y el decreto 1377 del 2013, el MINTIC puede adaptar dichos procedimientos a otras áreas o dependencias de la entidad realizando los ajustes necesarios que permitan su aplicabilidad.

- Se sugiere al MINTIC estar haciendo una evaluación constante de los procedimientos sugeridos, para lograr mejoras en el tratamiento y a la vez generar una base de conocimiento que sirva de apoyo y trazabilidad con el fin de no desmejorar en el cumplimiento continuo de la política.

- Es indispensable que el Ministerio haga una buena campaña de sensibilización para la divulgación de la política de tratamiento personales a nivel interno desde las dependencias hasta externamente con los grupos de interés, ya que solamente la política es publicada a nivel de la intranet y son muy pocos los funcionarios que la conocen y mucho menos las personas externas que tienen alguna relación con el MINTC.

- Es importante para el MINTIC en especial para el responsable del tratamiento garantizar que el encargado del tratamiento cumpla con la política y que dicho encargado que para el presente caso es la empresa de vigilancia, constantemente esté retroalimentando ese conocimiento al recurso humano que disponga para tal labor, puesto que el tema de rotación de personal puede convertirse en una vulnerabilidad que impida el cumplimiento de los procedimientos, la política y en general la normatividad vigente.

BIBLIOGRAFÍA

COLOMBIA - ALCALDÍA DE BOGOTÁ (2013). Decreto 1377 del 2013, artículo 3, numeral 2: protección de datos. [En línea], [consultado el 23 de enero de 2016]. Disponible en: www.alcaldiabogota.gov.co/sisjur/ normas/ Norma1.jsp?i=53646

_____. . Ley estatutaria 1581 de 2012. [En línea], [Citado el 2 de noviembre de 2015]. Disponible en la World Wide Web <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646>.

COLOMBIA DIGITAL. ABC para proteger los datos personales, Ley 1581 de 2012 Decreto 1377 de 2013. [En línea], [consultado el 23 de enero de 2016]. Disponible en:<http://www.colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html>.

COLOMBIA - MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Ley 1581 del 2012, articulo 3, numeral b. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: www.mintic.gov.co/portal/604/articles-4274_

_____. Acerca de Mintic - Misión y visión. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-540.html>.

_____. . Acerca de Mintic – Quienes somos. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: <http://www.mintic.gov.co/portal/604/w3-propertyvalue-540.html>

_____. Ley 1581 del 2012, articulo 5. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: www.mintic.gov.co/portal/604/articles-4274_

_____. Ley 1581 del 2012, articulo 3, numeral e. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: www.mintic.gov.co/portal/604/articles-4274_

_____. Ley 1581 del 2012, articulo 3, numeral g. [En línea], [consultado el 23 de febrero de 2016]. Disponible en: www.mintic.gov.co/portal/604/articles-4274_

_____. Decreto 1377 de 2013. [En Línea], [citado el 2 de noviembre de 2015]. Disponible en: www.mintic. gov.co/portal/604/articles-4274_documento.pd

_____. Política para el tratamiento de datos personales política de privacidad. (20, marzo, 2015). Bogotá, D.C. El Ministerio. 2015. 28 p.

CONSALFA.COM. Manual interno de políticas y procedimientos de datos personales. [En Línea] [Consultado el 2 de noviembre de 2015]. Disponible en/ www.consalfa.com/ Portals/0/ Documentos/ ManualPoliticasyProcedimientosDatos PersonalesCONSALFAS_AS_Rev1.pdf>.

CORTE CONSTITUCIONAL DE COLOMBIA. Artículo 15 de la Constitución Política de Colombia: Sentencias C- 748 de 2011, C-981 de 2005 y C-1011 de 2011. [En Línea], [consultado el 2 de noviembre de 2015]. Disponible en: http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15;http://www.corte constitucional.gov.co/relatoria/2011/c-748-11.htm;<http://www; Corte constitucional gov.co/relatoría/2008/C-1011-08.htm>;<http://www.corteconstitucional.gov.co/ relatoria/2005/c-981-05.htm>

DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES. Estandarización de la entrada y salida de información, atendiendo los principios constitucionales y legales. [En Línea], [citado el 2 de noviembre de 2015]. Disponible en la Intranet: <http://insitu.dian.gov.co/pinterna/normatividad.nsf/e9327debba393cf>

EASY COLOMBIA S.A. Reglamento de uso, manejo protección datos personales. [En Línea] [Consultado el 2 de noviembre de 2015]. Disponible en: <https://store-totalcode.netdna-ssl.com/easy/web_content/assets/Reglamento_Habeas_Data. pdf>.