



ALCALDÍA DE CANDELARIA VALLE

PLAN DE IMPLEMENTACION LEY 1581 - RNBD

Calle 9 No. 7 – 69
Código Postal: 763570
Teléfono: (57 2) 264 6209 / 2646344
www.candelaria-valle.gov.co
contacto@candelaria-valle.gov.co
Candelaria – Valle
Colombia - Noviembre de 2018 ©



TABLA DE CONTENIDO

Contenido

TABLA DE CONTENIDO	2
1. INTRODUCCION	3
2. EXPOSICIÓN DE MOTIVOS.....	4
3. ESTRATEGIAS DE COMPETITIVIDAD.	5
4. RECOMENDACIONES DE TIPO GENERAL.	6
4.1. Recomendación General 1: Adopción del Criterio Responsabilidad Demostrada.....	6
4.2. Recomendación General 2: Aprobación de la Política.....	7
4.3. Recomendación General 3: Definir la Persona Responsable de Aprobación del RNBD ante la SIC.....	7
4.4. Recomendación General 4: Autorizaciones para el Tratamiento de Protección de Datos Personales	7
4.5. Recomendación General 4: Inclusión Contractual.....	8
4.6. Recomendación General 6: Adoptar un Programa Integral de Protección de Datos Personales	9
4.7. Recomendación General 6: Autorización Digital.....	15
4.8. Recomendación General 7: Imágenes y vídeos	15
4.9. Recomendación General 9: Capacitación y Concientización en Protección de Datos personales	16
4.10. Recomendación General 10: Contratación de Menores de edad.....	16
4.11. Recomendación General 11 Información Personal privada y sensible sin las mínimas medidas de seguridad en documentos y computadores personales de funcionarios y contratistas	16
5. RECOMENDACIONES DE CARÁCTER CRITICO.....	17
5.1. Recomendación Crítica 1	17
5.2. Recomendación Crítica 2	18
5.3. Recomendación Crítica 3	19

1. INTRODUCCION

El cumplimiento de la Ley de Protección de datos personales y el Registro Nacional de Bases de Datos es un compromiso que asume el gobierno municipal frente a los ciudadanos, y que se encuentra enmarcado dentro de objetivo superior, y es que el Municipio de Candelaria sea reconocido en un futuro cercano como un "Territorio Inteligente", obteniendo para ellos los Sellos de Excelencia que dentro de ese propósito han establecido el Gobierno Nacional a través del Ministerio de las Tecnologías de la Información y las Comunicaciones.

En efecto, el plan de "implementación de la ley 1581 - RNBD" se enmarca dentro de los objetivos definidos por el Señor Alcalde Yonk Jairo Torres, de trabajar por el fortalecimiento del Municipio de Candelaria, como un territorio estratégico dentro de la región fomentado el empleo, la educación y la competitividad, y un aporte a la premisa fundamental de adelantar un "buen gobierno, con un gran tejido social que de soporte a los desafíos y las nuevas competencia de una Colombia en Paz".

El Municipio de Candelaria se encuentra alineado con las directrices dadas por el Ministerio TIC, como Entidad rectora de la política pública del sector TIC y quienes de acuerdo con la Ley 1341 de 2009, se encuentra estructurando el Modelo de Territorios y Ciudades Inteligentes para Colombia. En efecto la Dirección de Gobierno Digital dentro de su propósito de: "Liderar, articular e implementar con las entidades territoriales, las políticas y programas de ciudades inteligentes, que permitan la solución de problemáticas urbanas mediante la adopción de Tecnologías de la Información y las Comunicaciones". como un aporte a la consolidación de un rumbo "hacia el desarrollo económico, sociocultural, institucional y ambiental del Municipio y sus habitantes y alcanzar la tan anhelada mejor calidad de vida".

Es en este sentido que se presentan un plan de acción, con recomendaciones y alcances, que deriven en beneficios concretos para el Municipio, en aras de aportar a la estrategia "Candelaria en la Ruta del Desarrollo".

2. EXPOSICIÓN DE MOTIVOS

La ley 1581 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.

Esta implementación es de carácter obligatorio en las entidades jurídicas de naturaleza pública y como tal el Municipio de Candelaria ha asumido su cumplimiento como un compromiso entre la Administración y toda la ciudadanía; y aportando a consolidar el objetivo de generar a diversos niveles confianza entre sus ciudadanos; garantizando la pluralidad de adscripción identitarias y aportando a promover, promocionar y proteger los derechos fundamentales, previniendo la vulneración y restituyendo los derechos de la población en caso de haber sido quebrantados.

El Municipio tiene la firme convicción de que la economía digital es uno de los proyectos que aporta a su objetivo de materialización de proyectos de alto impacto. Lo anterior como eje diferenciador de una apuesta por la generación de empleo y de ingresos para los habitantes del municipio tomando como eje detonador el emprendimiento y la innovación en el marco de las ventajas competitivas y la vocación dada por el ordenamiento territorial y la necesaria diversificación productiva del municipio para el desarrollo rural integral sostenible.

3. ESTRATEGIAS DE COMPETITIVIDAD.

Modernización Institucional. La administración municipal orientará hacia el logro de altos niveles de gestión bajo principios de eficiencia, eficacia y transparencia, mejorar los procesos en la prestación de los productos y servicios que brinda a la comunidad.

La administración municipal entiende que los modelos tradicionales de gestión de los territorios deben evolucionar con el fin de contribuir a enfrentar los principales desafíos que propone el mundo económico, social y político contemporáneo.

Lo anterior acorde al nuevo plan de desarrollo nacional, en el que esta nueva economía (economía naranja), tiene como algunos de sus pilares esenciales que impulsan el desarrollo económico y social; la producción y transferencia del conocimiento, la capacidad de innovación y la gestión de tecnologías de información y las comunicaciones. En este sentido existe el interés de atraer empresas innovadoras y uno de los elementos que aportarían significativamente es que el Municipio pueda aplicar para poder obtener un sello de excelencia en territorios inteligentes.

El gobierno nacional otorgara el Sello de Excelencia en Territorios y Ciudades Inteligentes a Municipios que tengan "soluciones que se encuentren en ejecución y pretendan impactar positivamente la calidad de vida de todos sus habitantes a partir de un modelo sostenible que solventa problemáticas de carácter urbano, social, ambiental, económico y/o político, utilizando las tecnologías de la información y las comunicaciones de manera interconectada y apoyándose en una ciudadanía proactiva, innovadora y competitiva y contribuyendo al logro de los Objetivos de Desarrollo Sostenible".

El presente documento aporta a la evolución hacia un territorio inteligente en consideración a que este integra:

- a) Plan Estratégico de TI
- b) Plan de Seguridad y Privacidad de la Información del que forma parte esencial el tratamiento de datos personales
- c) El Plan Institucional de Capacitación
- d) Plan Anticorrupción y de Atención al Ciudadano

4. RECOMENDACIONES DE TIPO GENERAL.

4.1. Recomendación General 1: Adopción del Criterio Responsabilidad Demostrada

La responsabilidad demostrada es un concepto donde se enfatiza el rol del responsable del tratamiento (El Municipio de Candelaria en cabeza de su representante legal), como el llamado a implementar dentro de la organización las medidas que le permitan cumplir este objetivo. Y este concepto quedo formalizado en el artículo 26 del decreto 1377 de 2013.

En efecto, el artículo 26 del decreto 1377 se introduce en el sistema colombiano de protección de datos el criterio de responsabilidad demostrada como una obligación de los responsables del tratamiento, el cual está en la cabeza de los representante legales de cada entidad y dispone que los responsables deben ser capaces de demostrar que han implementado las medidas apropiadas y efectivas para cumplir con las obligaciones establecidas por la ley 1581 de 2012 y estas medidas son propios de cada entidad u organización de acuerdo a su tamaño y naturaleza jurídica, la naturaleza de los datos, tratamiento que se les darán y los riesgos que implique su recolección y circulación para los titulares.

El artículo 27 del Decreto 1377 igualmente dispuso que las políticas internas que se implementen deben garantizar:

- a. Que en la organización exista una estructura administrativa proporcional a la estructura de la entidad.
- b. Que se adopten mecanismos internos para poner en práctica las políticas, incluyendo herramientas de implementación, entrenamiento, y programas de educación.
- c. La adopción de procesos para la atención de reclamos y consultas de los titulares. La implementación de estándares en la protección de datos personales no solo se ve recompensada en una mayor proyección de datos personales, sino que será tenida en cuenta al momento de evaluar la imposición de sanciones por violación de deberes y obligaciones, establecidas en la ley

Por el tamaño, naturaleza jurídica, tipo de datos que maneja y tratamiento, se recomienda que el Municipio de Candelaria-Valle diseñe e implemente un programa integral de protección de datos personales.

4.2. Recomendación General 2: Aprobación de la Política

Remitir la Política de Información de datos personales a los responsables Despacho del alcalde, Jurídico y Calidad, para su pronta aprobación y habilitar su publicación en la página WEB.

4.3. Recomendación General 3: Definir la Persona Responsable de Aprobación del RNBD ante la SIC.

Si bien los consultores realizaran los 9 pasos de cargue y montaje en la plataforma de la SIC el RNBD, debe designarse un responsable que revisará y aprobará el inventario de bases de datos personales, y quien será el encargado, a través del usuario administrador, de hacer el click final, con el que finaliza el registro nacional de base de datos del Municipio, esto debe hacerse antes del 31 de enero de 2019.

4.4. Recomendación General 4: Autorizaciones para el Tratamiento de Protección de Datos Personales

Las entidades públicas no requieren autorización previa de los titulares, cuando la información es requerida por la entidad pública o administrativa en ejercicio de sus funciones legales. Pero no todas las labores cumplen esta condición. Por lo tanto y de acuerdo a la ley 1581 de 2012 se debe procurar obtener la autorizaciones, especialmente cuando se manejan datos que puedan afectar la intimidad del Titular o que puedan dar lugar a que sea discriminado, como aquellos que revelan su origen racial o étnico, su orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

En efecto este tipo de datos constituyen una categoría especial de datos personales y por ello, requieren una protección reforzada y algunas consideraciones especiales a la hora de solicitar autorización para su tratamiento.

Es en razón de esto que se debe retirar de todos los formatos en los cuales se recopila información confidencial el mensaje que aparece actualmente "Una vez impreso este documento se considera copia no controlada y no nos hacemos responsables por su actualización" e incluir el aviso de privacidad de Protección de Datos correspondiente al cada formato.

4.5. Recomendación General 4: Inclusión Contractual

Con el fin de complementar los controles actuales existentes, se hace necesario que cualquier tercero que desarrolle algún proceso de contratación, alianzas y acuerdos de cooperación con la Alcaldía de Candelaria , y que dentro de estos accedan, usen, traten y/o almacenen Datos Personales de funcionarios, ciudadanos y/o de terceros relacionados con dichos procesos contractuales, se encuentren obligados jurídicamente a adoptar en lo pertinente lo dispuesto en estas políticas, así como las medidas de seguridad que le indique la Alcaldía de Candelaria según el tipo de dato de carácter personal tratado.

Para tal efecto, se hace obligatorio el incluir una cláusula con esta obligación en los nuevos contratos, y generar un otrosí en los contratos existentes.

Se debe igualmente concertar con el Departamento Jurídico la obligación de incluir en los medios contractuales tanto de contratistas como de servidores, una cláusula integral de confidencialidad y manejo de información.

De igual manera se debe prever que la Alcaldía podrá adelantar la auditoria respectiva en el contrato o documento que legitima la entrega de los Datos Personales. La Alcaldía de Candelaria verificará que los datos solicitados sean necesarios, pertinentes y no excesivos respecto de la finalidad del Tratamiento.

En los contratos con los proveedores, donde el objeto contratado tenga relación con Datos Personales, se pactará una previsión en relación con los perjuicios que se pueden llegar a ocasionar a la Alcaldía de Candelaria como consecuencia de la imposición de multas y sanciones entre otras, por parte de las autoridades competentes y como consecuencia de incumplimiento de la ley de protección de datos personales por parte del proveedor.

4.6. Recomendación General 6: Adoptar un Programa Integral de Protección de Datos Personales

El programa se encuentra constituido por una serie de actividades orientadas al cumplimiento de objetivos que aportan a la construcción de un sistema de gestión efectivo en el tratamiento de datos personales. Generar esas actividades se sustenta en una serie de recomendaciones específicas así:

4.6.1. Recomendación Especifica 1. Generar evidencia del Compromiso de Alta Dirección.

Uno de los puntos críticos para contar poder evidenciar la adopción del criterio de la responsabilidad demostrada son aquellas relacionadas con el compromiso de la alta dirección (específicamente el señor Alcalde y los Secretarios), en las que se muestre que en el Municipio de Candelaria, se trabaja por buscar el generar una cultura en toda la organización de respeto por los datos personales.

Es en este sentido que recomendamos que, en uno de los consejos de gobierno, se genere un espacio donde se pueda adelantar una exposición motivada del plan integral de tratamiento de datos personales y su aporte al propósito de ser calificado como territorio inteligente.

4.6.2. Recomendación específica 2. Asignación de un oficial de seguridad.

El contar con políticas y procedimientos es un pre-requisito para tener el plan integral de protección de datos personales. En algunas ocasiones se comete el error de considerar que con contar con esos elementos es suficiente, sin embargo, esta apreciación es errada. Se debe evidenciar el que, para implementar este objetivo de manera exitosa, se ha adelantado un proceso de implementación y que en razón del cumplimiento de este objetivo se han destinado recursos y personal.

El artículo 23 del Decreto 1377 establece que: "Todo responsable o Encargado debe: designar a la persona o área que asuma la función de protección de datos personales y que dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la ley 1581 de 2012 y el presente decreto"

Es en razón de esto que recomendamos la designación de un rol de oficial de seguridad de la información y de protección de datos.

La función del oficial en cuanto hace a protección de datos sería el de velar por la implementación efectiva de las políticas y procedimientos adoptados por el Municipio de Candelaria para cumplir las normas, así como la implementación de buenas prácticas de gestión de datos personales dentro de la Alcaldía.

Sus funciones dentro del ámbito de la privacidad incluirían la labor de estructurar, diseñar y administrar el programa que permita a la organización cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente.

Funciones Propuestas para el Oficial de Protección de Datos

- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de los datos personales.
- Coordinar la definición e implementación de los controles del Programa integral de Gestión de Datos Personales.
- Servir de enlace y coordinador con las demás dependencias de la Alcaldía para asegurar una implementación transversal del Programa integral de Gestión de Datos Personales.
- Impulsar una cultura de protección de datos dentro del Municipio.
- Mantener un inventario de las bases de datos personales en poder de la Alcaldía y clasificarlas según su tipo.
- Actualizar el registro de las bases de datos de la Alcaldía en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC.
- Obtener las declaraciones de conformidad de la SIC cuando sea requerido.
- Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con los encargados residentes en Colombia.

- Analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos.
- Realizar un entrenamiento general en protección de datos para todos los colaboradores de la Alcaldía.
- Realizar el entrenamiento necesario a los nuevos funcionarios o contratistas, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la Alcaldía.
- Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call centers, gestión de proveedores, etc.). Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos.
- Requerir que, dentro de los análisis de desempeño de los colaboradores, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales.
- Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal. Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice a la Superintendencia de Industria y Comercio.
- Realizar seguimiento al Programa Integral de Gestión de Datos Personales.

4.6.3. Recomendación Específica 3. Definición de un responsable de datos personales por Secretaría

Se recomienda que desde la alta dirección se produzca la designación por Cada Secretaría del responsable de definir la información que se debe reportar al oficial de datos personales, con la finalidad de que este cuente con los insumos que le permitan actualizar ante la SIC, los requerimientos con respecto a las Bases de Datos registradas.

Lo anterior en consideración a que según con lo establecido en el Decreto 090 del 18 de enero de 2018 los responsables de Tratamiento están obligados a registrar sus bases de datos en el RNBD, deben actualizar la información registrada, como se indica a continuación:

- (i) Dentro de los primeros diez (10) días hábiles de cada mes, a partir de la inscripción de la base de datos, cuando se realicen cambios sustanciales en la información registrada.
- (ii) Anualmente, entre el 2 de enero y el 31 de marzo, a partir de 2020, los cambios considerados sustanciales. Estos son aquellos que se relacionen con:
 - La finalidad de la base de datos
 - El encargado del tratamiento
 - Los canales de atención al titular
 - La clasificación o tipos de datos personales almacenados en cada base de datos
 - Las medidas de seguridad de la información implementadas
 - La política de Tratamiento de la Información
 - La transferencia y transmisión internacional de datos personales
- (iii) Las bases de Datos que se creen con posterioridad al 31 de enero de 2019, las cuales deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.
- (iv) La información de los reclamos presentados por los Titulares, dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año, a partir de su inscripción. El primer reporte de reclamos presentados por los Titulares se deberá realizar en el segundo semestre de 2019 con la información que corresponda al primer semestre del 2019.
- (v) La información de los incidentes de seguridad sobre bases de datos, dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año, a partir de su inscripción. El primer reporte de incidentes de seguridad se deberá realizar en el segundo semestre de 2019 con la información que corresponda al primer semestre del 2019.

4.6.4. Recomendación específica 4. El Departamento de Calidad debe integrar las políticas protección de datos personales en el MIPG.

Con el fin de asegurar que las políticas adoptadas se implementen eficientemente al interior de la Alcaldía, el Departamento de Calidad debería:

- Adelantar la revisión de la pertinencia con respecto al MIPG de la política de tratamiento integral de los datos personales.
- La revisión y/o modificación de los procedimientos administrativos, para que estos sean coherentes con las políticas generales de protección de datos adoptadas por el Municipio.

4.6.5. Recomendación específica 5 - Definir un Plan de Divulgación

El departamento encargado de desarrollo humano debería desarrollar un plan de divulgación que permita dar conocer a los empleados y contratistas con respecto las Política de datos personales, las políticas internas para el cumplimiento de la ley en particular con respecto a:

- Recolección, almacenamiento, uso, circulación y supresión o disposición final de la información final.
- Requisitos y mecanismos para obtener la autorización de los titulares.
- Procedimientos para el acceso y corrección de datos personales
- La conservación y eliminación de información personal.
- Uso responsable de la información, incluyendo controles de seguridad administrativos, físicos y tecnológicos.
- Incluir en los medios contractuales, la cláusula de confiabilidad y manejo de información
- Procedimiento de la presentación de quejas, denuncias y reclamos relacionados con datos personales

4.6.6. Recomendación específica 6 - Cumplir la política de Gobierno Digital - Decreto 1078 de 2015

El Municipio se encuentra obligado a cumplir con los lineamientos generales establecidos en la política de Gobierno Digital establecida en el Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Recomendamos se inicie este cumplimiento de tal manera que se habilite el diseñar e implementar un sistema de administración de riesgos asociados al tratamiento de datos personales, que tenga en cuenta las siguientes etapas:

1. Identificación de los riesgos
2. Medición de la posibilidad de la ocurrencia del riesgo
3. Acciones de control para mitigar el riesgo
4. Monitoreo y seguimiento

4.6.7. Recomendación Especifica 7 - Protocolo de Incidentes

Entiéndase como incidente de seguridad de la información: como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información.

El Departamento de Informática debe implementar los protocolos de respuesta en el manejo de violaciones de incidentes, esto incluye la documentación de los pasos a seguir una vez se detecte la comisión del incidente, tanto a nivel correctivo como preventivo. Dentro de estos pasos se deben determinar tiempos, roles y responsabilidades

Una vez se han determinado las causas e impacto del incidente detectado relacionado con datos personales, es importante identificar oportunidades de mejora e implementar controles que redunden en la prevención de la ocurrencia de otros hechos relacionados con las vulnerabilidades detectadas.

4.6.8. *Recomendación Especifica 8 - Canal de Comunicación*

Se propone implementar un canal de comunicación con titular de la información para que sea él quien permanentemente este actualizando su información, (y que por ende la responsabilidad recaiga en el titular y no en la organización) de acuerdo a lo establecido en los Artículos 5, 6, 7, 8 del Decreto 1377 de 2013.

4.6.9. *Recomendación Especifica 9 - Política de Destrucción*

Se debe implementar una política clara y socializada a toda la Alcaldía sobre la destrucción de documentos, reportes y listas con datos personales. Toda destrucción de esta deberá estar acompañada de su correspondiente acta, la cual servirá como evidencia al momento que un Titular lo solicite y como soporte para verificar obsolescencia de cierto tipo de datos.

4.7. *Recomendación General 6: Autorización Digital*

Incorporar un Procedimiento que permita dar a conocer al ciudadano la política de protección de datos personales y recolectar la autorización por una única vez de manera digital. Lo anterior no solo traería ahorro en consumo de papel, también en aseguramiento de los datos Respecto a la veracidad y calidad de la información.

Cuando el Municipio se encuentre adelantando el proceso de implementación del esquema de Autorización Digital, se recomienda implementar la opción pertinente en la suite Lans Sentry, software licenciado por la Alcaldía y que cuenta con un módulo especial para ello.

4.8. *Recomendación General 7: Imágenes y vídeos*

Se debe tener especial precaución en las fotografías y videos que son tomados en eventos organizados por el Municipio de Candelaria –Valle, con miras a generar evidencia, publicación, etc. Se debe tener un mecanismo de autorización, que puede ser la misma grabación o cualquier medio alterno que genere evidencia. El cuidado debe ser mayor cuando se trate de imágenes de menores de edad, y en este caso tener autorización de sus padres o representante legal. Si no se tienen podrán tomarse fotografías, pero en ellas no se puede enfocar a alguien en especial.

En eventos masivos, se deben diseñar avisos que indiquen que los asistentes, ingresando al evento autorizan el almacenamiento y publicación de los registros visuales del evento.

4.9. Recomendación General 9: Capacitación y Concientización en Protección de Datos personales

Ejecutar el plan de capacitación y concientización acerca de las políticas, y procedimientos establecidos por la alcaldía para el cumplimiento de la ley de protección de Datos personales.

4.10.Recomendación General 10: Contratación de Menores de edad

En caso de que una práctica laboral sea desarrollada por parte de una persona menor de edad, se debe incluir en su carpeta una autorización de los padres para trabajar y para el tratamiento de los datos personales

4.11.Recomendación General 11 Información Personal privada y sensible sin las mínimas medidas de seguridad en documentos y computadores personales de funcionarios y contratistas

La Alcaldía debe enmarcar el hecho de que algunos colaboradores usen sus equipos de computo propios dentro de la política nacional de Teletrabajo. El Teletrabajo en Colombia se encuentra regulado por la Ley 1221 del 2008 y el decreto 884 del 2012 que la reglamenta.

Ley 1221 de 2008: Establece el reconocimiento del Teletrabajo en Colombia como modalidad laboral en sus formas de aplicación, las bases para la generación de una política pública de fomento al teletrabajo.

En razón de ello y dentro de este marco se autoriza la utilización de equipos personales a los colaboradores para la ejecución de sus obligaciones y/o funciones (cuando a ello haya lugar), siempre y cuando se implementen todas las medidas de seguridad definidas por la entidad.

Esto incluye concertar los procedimientos para realizar una copia de la información que se encuentra en los equipos del colaborador, con alguna frecuencia y en especial a la finalización de su relación y la subsecuente destrucción y/o borrado de la misma del equipo en referencia.

Se debe incluir en los acuerdos de confidencialidad o dentro del contrato; una clausula que indique las medidas de seguridad que deben aplicarse a la información personal privada y sensible que reposan en los computadores portátiles, memorias USB y en general medios físicos cuando se encuentran fue de las instalaciones de la Alcaldía, teniendo especial cuidado cuando se realizan intervenciones con enfoque diferencial.

5. RECOMENDACIONES DE CARÁCTER CRITICO

Entre las recomendaciones existen unas que afectan los macro procesos de la Alcaldía, y como tal recomendamos iniciar una intervención de tipo estructural.

5.1. Recomendación Critica 1

Se han detectado una brecha de seguridad muy sensible y que supone la necesidad de adelantar una remediación inmediata.

Hay una práctica muy arraigada dentro de la organización y que consiste en que los colaboradores dentro de sus funciones utilicen sus propias herramientas de trabajo, eso incluye el computador.

En efecto, muchos colaboradores utilizan un computador de su propiedad, y en el almacenan gran cantidad de datos, que recopilan dentro del desarrollo de su labor. Entre los datos almacenados hay un alto porcentaje de datos y además sensibles. Desafortunadamente estos equipos no cuentan con medidas de protección en caso de pérdida, daño y/o hurto.

Hay una falencia total con respecto a los procedimientos de entrega de información al momento de terminar un contrato, de tal manera que la Alcaldía tenga la certeza de que el colaborador entregue la totalidad de la información, que no se quede con copia de la

misma, que más adelante no pueda darle un tratamiento inadecuado y que finalmente si se produce un tratamiento inadecuado, el Municipio de Candelaria se encuentre blindado jurídicamente ante cualquier reclamación.

Dentro del cumplimiento de estos objetivos, se sugiere diseñar e implementar un procedimiento, que obligue al colaborador que termina su relación con el Municipio de Candelaria, el adelantar un trámite con el departamento de informática que se compondría de la ejecución de un backup de esta y la eliminación eficiente de esta información del equipo del colaborador.

5.2. Recomendación Crítica 2

Otra costumbre, consiste en toda información que pasa por manos de cada colaborador, se debe dejar copia. Es decir, cada vez que un funcionario recibe documentos que debe trasladar, procede a sacar una copia por "seguridad". Estas copias son guardadas o archivadas en diversos sitios, muchos de los cuales no tienen seguridad. Igualmente pueden reposar en computadores personales, o archivos, "por si pasa algo".

Este manejo descentralizado y des-regulado generan gran cantidad de puntos de riesgo de pérdida, fuga de información. Además, hacen imposible el reporte eficiente de incidentes, tal y como lo solicita la SIC, pues no se puede tener ni trazabilidad, ni determinación de responsables

Dentro de la política nacional de desarrollar al interior de las entidades públicas una cultura de cero papel, se debe tender a tener en un futuro cercano un sistema de integral de gestión documental. No obstante, en este momento se puede iniciar a tener una solución mediante el uso de Google Drive. Se deben definir políticas haciendo obligatoria esta opción para algunos documentos críticos, lo que facilitaría que todos los documentos que deben ser tramitados por múltiples colaboradores de la Alcaldía, se puedan almacenar en un mismo lugar, con acceso para los perfiles pertinentes, restringiendo ciertas funcionalidades, como la de compartir documentos con terceros.

5.3. Recomendación Crítica 3

Debido a que por limitaciones de tipo presupuestal no hay disponibilidad de cuentas de email corporativas para todos los colaboradores y solo se cuenta con una o dos por secretaría, los colaboradores han optado por utilizar su correo personal para trabajo, o abrir cuentas con nombre de usuario (parte izquierda de la arroba) referente a la sección de la secretaria y extensión gmail, hotmail, yahoo, etc. enviando y recibiendo correos que muchas veces contienen información personal y sensible. Una vez la información empieza a ser transmitida por este medio, la Alcaldía pierde control, no puede garantizar la integridad, confidencialidad y/o disponibilidad es decir no se podría aplicar reglas de seguridad de la información. Una vez finalizada la relación con el colaborador, este continuaría con privilegios de acceso, generando una brecha de seguridad crítica

Recomendamos buscar alternativas que permitan implementar bajo una adecuada relación beneficio/costo, una solución que le permita a la Alcaldía contar con cuentas suficientes para los colaboradores, o en caso contrario crear el procedimiento adecuado para que la entidad funcione eficientemente con la cantidad de cuentas actuales, e incorporar la política (o en caso de existir socializar y hacer obligatorio su cumplimiento), prohibiendo el uso de cuentas diferentes a las institucionales.