

**INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
GRUPO DE INVESTIGACIÓN FICB-PG**

**MODELO PARA IMPLEMENTAR LA PROTECCIÓN DE DATOS PERSONALES EN LA
ALCALDÍA LOCAL DE TUNJUELITO EN LA CIUDAD DE BOGOTÁ**

PRESENTA:

LUISA CRISTINA CABRALES DURAN

Código: 1712010283

HANS LWVER CARLOSAMA ALFEREZ

Código: 1622010131

ANDRES ORLANDO BRICEÑO DIAZ

Código: 1712010711

ASESOR TEMÁTICO:

ING. WILMAR JAIMES FERNANDEZ

Marzo de 2018



INSTITUCIÓN UNIVERSITARIA

POLITÉCNICO GRANCOLOMBIANO

ÍNDICE GENERAL

ÍNDICE DE TABLAS	5
ÍNDICE DE FIGURAS	5
RESUMEN	6
Palabras clave	6
INTRODUCCIÓN	7
Motivación	7
Antecedentes	7
Justificación	8
Alcance	9
Sistematización	9
Planteamiento del problema	10
Objetivos	11
General	11
Específicos	11
REVISIÓN DE LITERATURA / ANTECEDENTES	12
ESTRATEGIA METODOLÓGICA	13
Estado Actual	13
Gobierno de datos personales	13
Inventario de base de datos	13
Política de datos personales	14
Protección de datos en las operaciones	14
Programa de capacitación y concientización	14
Gestión de peticiones y quejas de los individuos	14
Programa de gestión de incidentes y vulneraciones de datos	14
Verificación de lineamientos en seguridad de información en alcaldía local	15
Metodología propuesta	16
1. Mantener un Gobierno	16
2. Crear y mantener actualizado un inventario de base de datos	16

3. Elaborar una política interna de datos.....	16
4. Integrar la protección de datos en las operaciones	17
5. Mantener un programa de capacitación y concientización	17
6. Gestionar las peticiones y quejas de los individuos	17
7. Mantener un programa de gestión de incidentes y vulneraciones de datos	17
DESARROLLO E IMPLEMENTACIÓN	19
Propuesta.....	19
Implementación.....	19
Desarrollo de metodología propuesta.....	21
Cronograma del plan de trabajo para implementación.....	25
Trabajo futuro.....	26
Aplicación de procedimientos en oficinas de alcaldía local	26
RESULTADOS	27
Entregables Y aplicación.....	28
Metodología en gestión del riesgo.....	28
Metodología de gestión del riesgo en tratamiento de datos.	28
Fase 1 Planear	29
Contexto de la organización.....	30
Misión	30
Visión.....	30
Contexto externo	30
Contexto interno	31
Definición del proceso.....	32
Fase 2 Hacer.....	33
Aspectos de gestión de riesgos en alcaldía local	33
Tratamiento del riesgo en alcaldía local	33
Aplicación de gestión de riesgos en alcaldía local.....	34
Controles a los riesgos en alcaldía local.....	37

Recursos a los controles en alcaldía local.....	38
Fase 3 Verificar.....	39
Implementación de procedimientos en alcaldía local	39
Fase 4 Actuar	40
PROCEDIMIENTOS PARA TRATAMIENTO	41
MODELOS DE FORMATOS	43
Aplicación de modelo para formatos en alcaldía local.....	44
MODELO DE CAMPAÑA DE CAPACITACIÓN Y SENSIBILIZACIÓN	45
Aplicación de modelo para capacitación en alcaldía local.....	46
Sensibilización.....	47
Actividades.....	47
Metodología	48
Listado de los lineamientos para seguridad en información.....	49
DISCUSIÓN Y CONCLUSIONES	51
Discusión	51
Conclusiones	52
REFERENCIAS	53

ÍNDICE DE TABLAS

Tabla 2. Definición del proceso	19
Tabla 3. Matriz de desarrollo de metodología propuesta.....	21
Tabla 4. Contexto externo de la alcaldía local.....	30
Tabla 5. Contexto interno de la alcaldía local.....	31
Tabla 6. Identificación de riesgos en proceso de recolección de datos personales de visitantes.....	34
Tabla 7. Criterios de valoración de probabilidad	35
Tabla 8. Criterios de evaluación del impacto.....	35
Tabla 9. Apreciación de riesgos en alcaldía local.....	36
Tabla 10. Matriz de apreciación a riesgos en alcaldía local.....	36
Tabla 11. Criterios sobre la zona de riesgo.....	37
Tabla 12. Matriz de controles.....	37
Tabla 13. Matriz de recursos para controles	38
Tabla 14. Formato de autorización de datos personales.....	43
Tabla 15. Programa 1: capacitación a la Alta Directiva	45
Tabla 16. Programa 2: capacitación para empleados	45

ÍNDICE DE FIGURAS

Ilustración 1. Matriz de verificación de lineamientos en alcaldía local	15
Ilustración 2. Diagrama de Gantt.....	25
Ilustración 3. Proceso de tratamiento de riesgos.....	28
Ilustración 4. Procesos identificados en alcaldía local.....	32
Ilustración 5. Diagrama metodología gestión del riesgo	40
<i>Ilustración 6. Procedimiento de recolección de datos personales</i>	<i>41</i>
Ilustración 7. Procedimiento para el almacenamiento de datos personales	41
Ilustración 8. Procedimiento de circulación de datos personales.....	42
Ilustración 9. Proceso de uso de datos personales	42
Ilustración 10. Proceso de supresión de datos personales.....	42
Ilustración 11. Formato implementado en Alcaldía Local	44
Ilustración 12. Eslogan de sensibilización	47
Ilustración 13. Personaje de sensibilización	47

RESUMEN

En la ciudad de Bogotá, la Alcaldía Mayor cuenta con la Secretaría de Gobierno que a su vez se compone de 20 dependencias, una para cada localidad de la ciudad, estas entidades públicas están sujetas a las leyes nacionales, en este documento se plantea un modelo para implementar la protección de datos en la Alcaldía Local de Tunjuelito de la secretaria de gobierno en base a lo estipulado en la ley 1581 de 2012[1], la Ley 1266 de 2008[2] y la Ley 1273 de 2009[3]. Por lo anterior para que la Alcaldía Local de Tunjuelito realice una adecuada implementación de protección de datos personales se deben minimizar los riesgos de llevar a cabo una recolección inadecuada, incorrecta e incompleta de datos personales públicos, privados y sensibles en formularios físicos o digitales, mediante una propuesta de gestión del riesgo y se definen procedimientos para las actividades de tratamiento de información, de igual manera se muestran bosquejos para el formato de autorización para el tratamiento de datos personales con todos los requerimientos de ley exigidos por la legislación colombiana en la materia, acompañados de un programa de capacitación.

Palabras clave

Datos personales

Regulación de seguridad de información

Tecnologías de la información

Tratamiento datos Alcaldía Local de Tunjuelito

INTRODUCCIÓN

En la actualidad Bogotá tiene un fortalecimiento en las tecnologías de la información en una Colombia Digital, el manejo de los datos personales ha cobrado gran importancia dado que es materia prima para entes de naturaleza pública como la Secretaria Distrital de Gobierno, como consecuencia de esta positiva evolución, este recurso se ha convertido en un tema de enfoque para alcaldías locales como la de Tunjuelito, quienes se han visto en la tarea de adecuar sus procedimientos a las directrices del ente regulador representado por la (SIC) a cumplir con lo estipulado en la Ley 1581 de 2012 y velar por que la protección en el uso de los datos de cada ciudadano sea cumplido, ya que su manejo está ligado a los derechos de carácter fundamental. Por lo anterior, dado que la Alcaldía Local de Tunjuelito no cuenta en la actualidad con un modelo puntual para su correcta implementación, este documento propone un modelo de implementación del tratamiento de los datos, con el fin de apropiarse esta legislación de la manera más adecuada en las entidades públicas.

Motivación

El Congreso de Colombia decretó la Ley 1581 del año 2012[1]; en general las alcaldías locales de Bogotá y de todo el país, incluida la de Tunjuelito están en la obligación de acoger y realizar su correcta implementación al interior de la institución y de cumplir el plazo para registrarse y registrar las bases de datos con información personal que tengan en la institución ante el Registro Nacional de Base Datos.

Antecedentes

La Secretaria de Gobierno está en la obligación de cumplir con las directrices que las leyes le imparten, sin embargo en la actualidad cuenta con un marco normativo interno que busca alinear los procesos y procedimientos de las alcaldías locales para cumplir a cabalidad con las leyes, pero se acogen únicamente a los lineamientos de la resolución 070 de 2017[4] de la alcaldía mayor y la regulación impartida por la SIC, pero no ha realizado un procedimiento a la fecha adecuado a cada una de las alcaldías locales y sus procedimientos para la adecuada implementación del tratamiento de datos.

Justificación

La tecnología busca mejorar el bienestar de personas alrededor del mundo. Por esto el congreso decretó la Ley 1581, de la normativa en el tema de datos personales y sin duda alguna como jurídico para la legislación colombiana; es válido aclarar que en la mencionada ley se contempló que las empresas públicas deben implementar la ley y que posteriormente se deben registrar y registrar las bases de datos, un ejemplo claro de empresas públicas son las alcaldías de todo el país incluida la alcaldía local de Tunjuelito.

No cabe duda que implementar la ley acarrea muchos cambios de paradigmas a nivel de tratamiento de datos y de seguridad de dichos datos, por tal motivo en este documento se plantea un modelo de implementación en la alcaldía local de Tunjuelito, de acuerdo con la normatividad establecida a nivel nacional y para que posteriormente a la implementación se cuente con un inventario de Databases con información lista para registro.

Ante el inminente cumplimiento de la legislación y la nueva realidad en temas de protección y privacidad de datos no solo en Colombia sino a nivel mundial, es muy importante que las empresas públicas entiendan y se acojan a la ley como un principio proactivo y necesario de responsabilizarse por el adecuado tratamiento de datos. De llegar a presentarse esta situación existe el riesgo de mala imagen y reputación ante los titulares de la información y la sociedad, así como el riesgo de investigación disciplinaria.

Dado lo anterior, estamos seguros que al acoger el modelo propuesto de implementación del tratamiento de datos para la alcaldía local de tunjuelito podemos minimizar el riesgo de incumplimiento de ley.

Precisamente noticias como las publicadas en México donde ya se establecen lineamientos específicos para el tratamiento de datos, referencian la importancia de estos modelos en una sociedad de la información. [Consultar artículo](#).

Otra referencia que da relevancia a la importancia es la inclusión en España del listado de cumplimiento normativo para facilitar la adaptación al Reglamento General de Protección de Datos. [Consultar artículo](#).

Otro país relevante en materia de metodología y regulación de tratamiento de datos personales es Costa Rica quien en sus leyes ya se contempla a profundidad el tema [8].

Lo anterior implica que como en la Unión Europea y en Norteamérica, Latinoamérica está en una época marcada por el avance de las tecnologías hacen necesaria la creación de una normativa acorde a los cambios suscitados en la era digital. Es una de las funciones del gobierno regular y ampliar la protección de los ciudadanos en vista de los peligros y las violaciones a la seguridad personal que se han perpetrado en los últimos tiempos; así mismo Colombia en la normativa concede un plazo de tiempo, para que las empresas examinen y adecúen sus protocolos de seguridad y procedimientos relativos al tratamiento de datos.

Alcance

El modelo de tratamiento presentada aplicará al proceso de Administración de Recursos Físicos y de Servicios Generales que contengan datos personales y que sean objeto de tratamiento por la Alcaldía Local de Tunjuelito en Bogotá.

Sistematización

La Alcaldía Local de Tunjuelito establecerá, implementará, mantendrá y realizará mejora en el marco de seguridad de información en base a los requisitos de las normas establecidas, toda vez que reconoce que los datos personales tienen un significado y valor para la Alcaldía Local en sus actividades cotidianas.

Planteamiento del problema

La protección de datos viene desarrollándose mediante Ley 1581 decretada para desarrollar el derecho de las personas sobre su información.

El encargado del tratamiento de datos de alcaldías locales de todo el país, incluida la alcaldía local de Tunjuelito de la ciudad de Bogotá, tienen obligación legal a desarrollar e implementar los principios en tratamiento de dato y lineamientos de seguridad, entre otras disposiciones, que aseguren el adecuado tratamiento de datos a dicha alcaldía local; pero se ha visto en general que las alcaldías locales de la Secretaria de Gobierno en Bogotá no tienen un modelo definido para la adecuada implementación de tratamiento de datos que se manejan en estas alcaldías. El modelo que se propone tiene como fin implementar una metodología que permita a la alcaldía local de Tunjuelito tener una directriz para el tratamiento de datos evitando incurrir en investigaciones por parte de SIC y sanciones.

OBJETIVOS

General

Realizar un modelo de implementación para tratamiento de datos personales en Alcaldía Local de Tunjuelito con fin de cumplir la Ley 1581 del 17 de 2012.

Específicos

1. Brindar directrices que busquen el adecuado tratamiento de datos en procesos de la alcaldía local de Tunjuelito.
2. Realizar una propuesta de metodología para gestión de riesgos en conveniente procedimiento de datos personales de la alcaldía local de Tunjuelito.
3. Proponer un programa de sensibilización al personal involucrado en el tratamiento de datos de alcaldía local de Tunjuelito.

REVISIÓN DE LITERATURA / ANTECEDENTES

Para este proyecto partimos de la Ley Estatutaria 1581-2012[1], y los demás derechos constitucionales que refiere el artículo 15 de Constitución; así como el derecho a la información consagrado en el artículo 20 de la misma.

Como antecedentes, Ley 1581 en Colombia se tenía la Ley 1266 de 2008[2] y Ley 1273. La Ley 1266, también como lo dice en el artículo 20 de constitución, en correspondencia con información bancaria o servicios, Ley 1273 de 2009[3].

Posteriormente la Ley 1581 de 2012 fue reglamentada en el Decreto 1377 de 2013[6], el cual salió el 27/06/2013 y, cuyo objeto sirve para reglamentar parcialmente la Ley 1581.

La SIC es la encargada de asegurar el cumplimiento de la legislación de protección de datos, solicitar los procedimientos para procesamiento de información, cursar investigaciones y asignar las sanciones o trasladar las investigaciones a otras entidades pertinentes.

Por este motivo la alcaldía local de Tunjuelito de Bogotá tenga presente que tiene plazo hasta el 31 de enero de 2019 para realizar la suscripción ante el Registro Nacional de Base de Datos y proceder a registrar las bases de datos personales que traten acorde a lo indicado por la SIC.

En base a la normativa citada anteriormente y a que la SIC es la encargada de vigilar cumplimiento de legislación, lo que buscamos con este documento es realizar un modelo de implementación para el tratamiento de datos en la alcaldía local de Tunjuelito de Bogotá que le permitirá garantizar ante los titulares de la información y la SIC que están tratando los datos como lo establece Ley 1581 y Decreto 1377.

Respecto a metodologías, lineamientos o guías en cuanto al tratamiento de datos, la SIC ha generado normatividad sobre protección de datos como por ejemplo; en servicios Cloud Computing nube[7], declaración de conformidad sobre transferencias de datos[8], implementación del principio de responsabilidad demostrada[9], aspectos prácticos en hábeasdata[10] o formatos datos[11].

ESTRATEGIA METODOLÓGICA

Se plantea una metodología para la implementación de la Ley 1581 en empresas públicas específicamente la alcaldía local de Tunjuelito de Bogotá sobre el proceso de Administración de Recursos Físicos y de Servicios Generales. Las empresas en razón al tratamiento de datos deben ser competentes de demostrar que han realizado medidas adecuadas con el fin de desempeñar los deberes de Ley 1581 y sus decretos, para ello la SIC puso a disposición una siguiente guía de responsabilidad demostrada[9]. Nuestra metodología planteada para el desarrollo de la Ley 1581 de 2012 en empresas públicas tiene un componente diferenciador que involucra y articula tres ejes fundamentales basados en personas, procesos en la operación y conocimiento sobre la ley.

Estado Actual

Gobierno de datos personales

En la actualidad no se encontró un gobierno definido en manejo de datos internamente de la alcaldía local de Tunjuelito, donde al menos se haya designado un funcionario o área que cumpliera las funciones de protección de datos personales, tampoco se contaba con apoyo o conocimiento de la alta dirección en la gestión de datos, no se contaba con un plan anual de trabajo, ni se tiene asignado roles o responsabilidades al interior de la alcaldía en cuestión de gestión de datos así como ausencia de gestión de riesgos sobre datos personales.

Inventario de base de datos

La no existencia de identificación de un inventario de base de datos, tampoco se conoce la clasificación de los datos tratados en la alcaldía local de Tunjuelito, tampoco se tiene cláusulas en los contratos para la transferencia o transmisión de datos personales.

Política de datos personales

No se ha implementado o desarrollado la política de protección de datos, avisos de privacidad o formatos de autorizaciones.

Protección de datos en las operaciones

No existen definidas políticas y procedimientos para el procesamiento de datos personales, procedimientos para velar por la calidad de los datos o políticas para obtener la autorización del titular, ni controles asociados a la seguridad de información en Databases.

Programa de capacitación y concientización

Ausencia de entrenamientos en protección de datos de manera general a toda la compañía, entrenamiento a los distintos puestos de trabajo que manejan datos de manera particular o campañas de sensibilización y actualización en materia de datos personales.

Gestión de peticiones y quejas de los individuos

Falta definir procedimientos para dar contestación a reclamos de titulares, procedimientos para responder solicitudes o para proveer mecanismos para que los individuos restablezcan o corrijan sus datos.

Programa de gestión de incidentes y vulneraciones de datos

Ausencia de plan de respuesta a incidentes, protocolo de notificación a los dueños afectados y de reportes a las autoridades referente a amparo de datos sobre incidentes.

En el siguiente cuadro se realiza la verificación en la alcaldía local de Tunjuelito del cumplimiento a los lineamientos indicados de acuerdo con lo indicado por el modelo planteado

Verificación de lineamientos en seguridad de información en alcaldía local

Verificación de estado actual de seguridad de información en Databases del subproceso identificado, se aplicó una matriz de acuerdo a la siguiente tabla.

Tabla 1. Tabla de verificación de cumplimiento

Tabla de verificación de cumplimiento de alcaldía Tunjuelito a lineamientos SIC		
Ítem	Lineamiento	Cumple o no cumple
1	Lineamiento 1	Revisar el cumplimiento
2	Lineamiento 2	Revisar el cumplimiento
3	Lineamiento 3	Revisar el cumplimiento

Con los siguientes resultados:

Tabla de verificación de cumplimiento de alcaldía Tunjuelito a lineamientos SIC					
Ítem	Lineamiento	Cumple o no cumple	Ítem	Lineamiento	Cumple o no cumple
1	Existe un documento de seguridad de la información personal o general que ya esté aprobado	NO	14	Tiene implementado un procedimiento que contemple la definición de especificaciones y requisitos de seguridad de los sistemas de información personal	NO
2	Anteriormente se ha realizado documentación de procesos entorno a la seguridad de la información personal	NO	15	Existen implementados controles de seguridad de la información durante el mantenimiento o Control de cambios de los sistemas de información personal	NO
3	Hay procedimientos de asignación de responsabilidades y autorizaciones en el tratamiento de la información personal	NO	16	Hay un procedimiento implementado de auditoría de los sistemas de información que contengan datos personales	NO
4	Anteriormente ya ha implementado algunos acuerdos de confidencialidad con las personas que tienen acceso a la información personal	NO	17	Las bases de datos con información personal poseen Monitoreo de consulta	NO
5	Se tienen controles de seguridad en la tercerización de servicios para el tratamiento de la información personal	NO	18	Cuenta con una política implementada para el correcto tratamiento de la información personal en las diferentes etapas del ciclo de vida del dato tanto en recolección, circulación y en disposición final	NO
6	Se asumen acciones implementadas con herramientas de gestión de riesgos en el tratamiento de datos personales	NO	19	Cuenta con un procedimiento implementado para la validación de datos de entrada y procesamiento de la información personal, para garantizar que los datos recolectados y procesados sean correctos y apropiados, como confirmación de tipos, formatos, longitudes, pertinencia, cantidad y uso	NO
7	Se tiene implementado un sistema de gestión de seguridad de la información o un programa integral de gestión de datos personales	NO	20	Cuenta con un control de seguridad de información para la validación de datos de salida	NO
8	Posee implementados controles de seguridad de la información personal para el Recurso Humano antes de la vinculación y una vez finalizado el contrato laboral	NO	21	Se tienen una política implementada para el Intercambio físico o electrónico de datos en casos como el comercio electrónico para la compra y venta de productos o servicios, o en transporte o almacenamiento de información personal	NO
9	Existe una política de control de acceso a la información personal, tanto en las instalaciones físicas como a nivel tecnológico	NO	22	Cuenta con un procedimiento o control implementado para la disposición final de la información personal en cuanto a la supresión, archivo, y destrucción.	NO
10	Cuenta con un procedimiento para la Gestión de usuarios con acceso a la información personal	NO	23	Cuenta con una política y procedimientos implementados de gestión de incidentes de seguridad de la información personal	NO
11	Se ha implementado una política específica para el acceso a la información personal de las bases de datos con información personal sensible	NO	24	Existe implementada una política para mejorar la seguridad de la información personal a partir de los incidentes o vulnerabilidades detectados	NO
12	Se usa una política implementada de copia de respaldo de la información personal	NO	25	Hay políticas de auditorías de seguridad de la información personal	NO
13	Se implementa una política de protección para el acceso remoto a la información personal	NO	26	Dentro de las auditorías de seguridad de información personal, tiene en cuenta el cumplimiento de requisitos, políticas y normas que específicamente le apliquen a la base de datos	NO

Ilustración 1. Matriz de verificación de lineamientos en alcaldía local

Como se concluye no hay cumplimiento de ningún lineamiento a la fecha a nivel de alcaldía local.

Metodología propuesta

A continuación, en este documento se plantea una novedosa y ágil metodología para cubrir la implementación de la ley en el marco de la alcaldía local de Tunjuelito y se entregarán algunos documentos que soportan el desarrollo del método propuesto con el fin de cumplir la metodología propuesta.

1. Mantener un Gobierno

- Nombrar un oficial de Protección de Datos.
- Involucrar a los directivos en la gestión de protección de datos
- Presentar un plan de trabajo anual.
- Crear roles y responsabilidades dentro de la organización en el manejo de datos.
- Generar informes a los directivos y partes interesadas externos sobre el estado del programa de protección de datos.
- Gestionar los riesgos sobre protección de datos.
- Gestionar los riesgos con terceros.

2. Crear y mantener actualizado un inventario de base de datos

- Mantener un inventario de base de datos.
- Clasificar los datos tratados en la organización.
- Registrar las bases de datos ante la SIC.
- Desarrollar e implementar contratos de transferencia o transmisión de datos.

3. Elaborar una política interna de datos

- Mantener una política de protección de datos personales.
- Desarrollar los avisos a la privacidad.
- Desarrollar formatos a las autorizaciones.

4. Integrar la protección de datos en las operaciones

- Mantener políticas con procedimientos que velen por la calidad de los datos.
- Mantener políticas con procedimientos que obtengan la autorización del titular.
- Realizar controles de seguridad de información en Databases.

5. Mantener un programa de capacitación y concientización

- Llevar a cabo entrenamientos en protección de datos personales de manera general a toda la compañía.
- Llevar a cabo entrenamiento a los distintos puestos de trabajo que manejan datos personales de manera particular.
- Desarrollar campañas de sensibilización y actualización en materia de datos.

6. Gestionar las peticiones y quejas de los individuos

- Mantener procedimientos para dar respuesta a las peticiones, quejas y reclamos.
- Mantener procedimientos para responder solicitudes o para proveer mecanismos para que los individuos actualicen o corrijan sus datos.

7. Mantener un programa de gestión de incidentes y vulneraciones de datos

- Mantener un plan de respuesta a incidentes de datos.
- Mantener un protocolo de notificación a los titulares afectados y de reportes a las autoridades de protección de datos sobre incidentes.
- Llevar a cabo pruebas periódicas del plan de respuesta a incidentes.

8. Análisis de resultados

- Auditorias de cumplimiento
- Resultados de implementación de metodología de riesgos
- Resultados al implementar procedimientos
- Análisis de resultados al implementar formatos de tratamientos

- Análisis de resultados de capacitación

9. Acciones de mejora continua

- Retroalimentación, balance y lineamientos de la alta dirección
- Atención a no conformidades
- Implementación de ajustes a la ejecución
- Optimización de procesos y seguimiento continuo

DESARROLLO E IMPLEMENTACIÓN

Propuesta


El tratamiento de los datos corresponde a las actividades de recolección y almacenamiento de información personal de titulares, cumpliendo así el ciclo de vida del dato. Esta labor es realizada por el administrador de datos. Siendo así, se entiende que la recolección de los datos es el primer momento en que comienza el ciclo del dato y da paso al tratamiento de los datos de titulares, razón por la cual se deben minimizar riesgos de llevar a cabo una recolección inadecuada e incompleta de datos públicos y privados al interior de alcaldía local de Tunjuelito en formularios físicos o digitales.

Implementación

En el siguiente proceso de la alcaldía se identificaron algunos subprocesos relacionados a la captura y posterior tratamiento de datos personales.

Se identificó la actividad propuesta en la metodología, diagnóstico inicial de la situación y los entregables para la alcaldía de local de Tunjuelito. Las actividades escogidas fueron acorde con los entregables que se definieron como resultados.

Tabla 2. Definición del proceso

ALCALDÍA LOCAL DE TUNJUELITO		
PROTECCIÓN DE DATOS PERSONALES		
		
TIPO DE PROCESO: Apoyo		
PROCESO: Administración de Recursos Físicos y de Servicios Generales		
SUBPROCESO 1: Recolección de datos personales de visitantes		
ACTIVIDAD	DIAGNÓSTICO	ENTREGABLES
Desarrollar formatos de autorizaciones.	Se identificó que no se cuenta con la debida autorización del titular para su recolección.	Autorización para el tratamiento de datos personales.
Gestionar los riesgos sobre protección de datos personales.	Se identificó que no se tiene analizados e identificados los riesgos de recolección de	Analizar, identificar y generar la metodología para la de riesgos para los diferentes

	datos personales y no existe la matriz de riesgos para el proceso que captura datos personales.	procesos que capturan datos personales.
Mantener políticas y procedimientos para la recolección, almacenamiento, uso, circulación y supresión de datos personales.	Se identificó que no existen procedimientos para todo el ciclo de vida del dato (recolección, almacenamiento, uso, circulación y supresión).	Procedimientos para el ciclo de vida del dato (recolección, almacenamiento, uso, circulación y supresión).
Implementar controles de seguridad de la información en Databases.	Se identificó que no existen controles asociados a la seguridad de información en Databases en mención.	Aplicar controles de seguridad de información

SUBPROCESO 2: Tratamiento de Datos para CCTV

ACTIVIDAD	DIAGNÓSTICO	ENTREGABLES
Desarrollar formatos de autorizaciones.	Se identificó que no se cuenta con formatos para la recolección de datos personales en CCTV.	Autorización para el tratamiento de datos personales.
Gestionar los riesgos sobre protección de datos personales.	Se identificó que no se tiene analizados e identificados los riesgos de recolección de datos personales en CCTV y no existe la matriz de riesgos para el proceso que captura datos personales.	Analizar, identificar y generar la metodología para la de riesgos para los diferentes procesos que capturan datos personales.
Mantener procedimientos para procesamiento de datos.	Se identificó que no existen procedimientos para todo el ciclo de vida del dato (recolección, almacenamiento, uso, circulación y supresión).	Procedimientos para el ciclo de vida del dato.
Implementar controles de seguridad de la información en las bases de datos.	Se identificó que no existen controles asociados a la seguridad de información de datos en mención.	Aplicar controles de seguridad de información en Databases.

SUBPROCESO 3: Elaboración de carnet para empleados		
ACTIVIDAD	DIAGNÓSTICO	ENTREGABLES
Desarrollar formatos de autorizaciones.	Se identificó que no se cuenta con formatos para la recolección de datos personales para la elaboración de carnet de personal.	Autorización para el tratamiento de datos personales.
Gestionar los riesgos sobre protección de datos personales.	Se identificó que no se tiene analizados e identificados los riesgos de recolección de datos personales en la elaboración de carnet del personal y no existe la matriz de riesgos para el proceso que captura datos personales.	Analizar, identificar y generar la metodología para la de riesgos para los diferentes procesos que capturan datos personales.
Mantener políticas y procedimientos para la recolección, almacenamiento, uso, circulación y supresión de datos personales.	Se identificó que no existen procedimientos para todo el ciclo de vida del dato (recolección, almacenamiento, uso, circulación y supresión).	Procedimientos para el ciclo de vida del dato (recolección, almacenamiento, uso, circulación y supresión).
Implementar controles de seguridad de la información en las bases de datos.	Se identificó que no existen controles asociados a la seguridad de la información en la base de datos en mención.	Aplicar controles de seguridad de la información para la base de datos.

Desarrollo de metodología propuesta

A continuación, se define el desarrollo que tendrá cada una de las actividades propuestas en la metodología para implementar la protección de datos en la alcaldía local de Tunjuelito.

Tabla 3. Matriz de desarrollo de metodología propuesta

LO QUE PROPONEMOS	COMO LO HAREMOS
Diagnóstico	
Antecedentes	Se plantea hacer una revisión de antecedentes ejecutados o no sobre datos.
Análisis de la situación actual	Se plantea hacer una revisión del estado actual sobre el desarrollo de datos.
Planificación	
Alcance, viabilidad y factibilidad	Se realiza un planteamiento del alcance de la implementación, así como un estudio de

	viabilidad y factibilidad de la metodología propuesta.
Documento con plan para acción	Se genera un plan para acción acorde al diagnóstico.
Definición de actividades de la ejecución	Se definen las actividades de ejecución requeridas en la alcaldía.
Mantener un Gobierno	
Nombrar un oficial de Protección de Datos Personales.	Incluir las funciones del oficial de datos en el cargo de analista de cumplimiento del área control de la alcaldía y sea oficialmente formalizado por el área de recursos humanos.
Involucrar a los directivos en la gestión de protección de datos	Realizar una presentación ejecutiva de inicio para dar a conocer la importancia de la implementación de la ley y el proceso de metodología que se seguirá al interior de la alcaldía.
Presentar un plan de trabajo anual.	Establecer el cronograma del plan de trabajo de todo el sistema de protección de datos.
Crear roles y responsabilidades dentro de la organización en el manejo de datos personales.	Crear un comité de datos interdisciplinario donde se vele el cumplimiento y desarrollo de la Ley al interior de la entidad.
Generar informes a los directivos y partes interesadas externos sobre el estado del programa de protección de datos personales.	Generar semestralmente informes a las partes interesadas de manera estructurada y clara.
Gestionar los riesgos sobre protección de datos personales.	Analizar, identificar y generar la metodología para la de riesgos para los diferentes procesos que capturan datos.
Gestionar los riesgos con terceros.	Analizar, identificar y generar la metodología para gestionar riesgo de procesos que comparten datos con terceros.
Crear y mantener actualizado un inventario de base de datos	
Mantener un inventario de base de datos.	Identificar y registrar las bases de datos detectadas en los procesos de la alcaldía.
Clasificar los datos tratados en la organización.	Clasificar los datos personales tratados en las bases de datos identificadas.
Registrar las bases de datos ante la SIC.	Proceder a registrarse en Databases de SIC.
Desarrollar e implementar contratos de transferencia o transmisión de datos personales.	A nivel contractual definir cláusulas para transferencia y transmisión de datos con encargados o responsables de las bases de datos de la alcaldía local de Tunjuelito.

Elaborar una política interna de datos personales	
Mantener una política de protección de datos.	Definir, crear y publicar la política de protección de datos.
Desarrollar los avisos de privacidad.	Definir, crear y publicar avisos de privacidad.
Desarrollar formatos de autorizaciones.	Definir, crear y publicar los formatos de autorización para la protección de datos.
Integrar la protección de datos en las operaciones	
Mantener políticas y procedimientos para la recolección, almacenamiento, uso, circulación y supresión de datos.	Definir las políticas y procedimientos para el adecuado ciclo de vida del dato.
Mantener políticas y procedimientos para velar por la calidad de los datos.	Definir las políticas y procedimientos para velar la calidad del dato.
Mantener políticas y procedimientos para obtener la autorización del titular.	Definir las políticas y procedimientos para obtener la autorización del titular.
Implementar controles de seguridad de información en Databases.	Realizar el desarrollo de los lineamientos de seguridad de información.
Mantener un programa de capacitación y concientización	
Llevar a cabo entrenamientos en protección de datos personales de manera general a toda la compañía.	Proponer y desarrollar el programa de capacitación y entrenamiento general para toda la entidad.
Llevar a cabo entrenamiento a los distintos puestos de trabajo que manejan datos de manera particular.	Proponer y desarrollar el programa de sensibilización para tratamiento de datos al interior de la alcaldía local de Tunjuelito.
Desarrollar campañas de sensibilización y actualización en materia de datos.	Proponer y desarrollar el de sensibilización y actualización periódica de datos personales al interior de la alcaldía.
Gestionar las peticiones y quejas de los individuos	
Mantener procedimientos para dar respuesta a las peticiones, quejas y reclamos.	Desarrollar el procedimiento que atienda quejas y reclamos y que de respuesta oportuna a los requerimientos de los titulares.
Mantener procedimientos para responder solicitudes o para proveer mecanismos para que los individuos actualicen o corrijan sus datos.	Desarrollar el procedimiento que atienda actualizaciones o correcciones de los datos.

Mantener un programa de gestión de incidentes y vulneraciones de datos	
Mantener un plan de respuesta a incidentes de datos.	Desarrollar el procedimiento que dé respuesta a los incidentes de datos.
Mantener un protocolo de notificación a los titulares afectados y de reportes a las autoridades de protección de datos sobre incidentes.	Implementar el protocolo de notificación a los titulares afectados y reporte a la autoridad.
Llevar a cabo pruebas periódicas del plan de respuesta a incidentes.	Ejecutar auditorías al plan de respuesta de incidentes de datos.
Análisis de resultados	
Auditorías de cumplimiento	Desarrollar el plan de auditorías internas a la metodología implementada
Resultados de implementación de metodología de riesgos	Detallar el análisis de implementación de la metodología de riesgos
Resultados al implementar procedimientos	Validar los resultados obtenidos en la implementación de procesos
Análisis de resultados al implementar formatos de tratamientos	Analizar los resultados obtenidos en cada una de los puntos de captura de datos personales
Análisis de resultados de capacitación	Analizar los resultados de capacitación propuestos en la metodología
Acciones de mejora continua	
Retroalimentación, balance y lineamientos de la alta dirección	Recibir las mejoras sugeridas por la alta dirección
Atención a no conformidades	Atención a no conformidades
Implementación de ajustes a la ejecución	Implementación de ajustes a la ejecución que mejoren la metodología propuesta
Optimización de procesos y seguimiento continuo	Optimización de procesos y seguimiento continuo a la metodología propuesta

Cronograma del plan de trabajo para implementación

A continuación, se presenta el cronograma presupuestado del plan de implementación de la metodología, por semestre y meses y sus respectivas semanas con el listado de las etapas y las correspondientes actividades a realizar.

CRONOGRAMA DE IMPLEMENTACION							
Etapas	Actividades	Tercer Trimestre 2018			Cuarto trimestre 2018		
		Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Diagnóstico	Antecedentes	■	■				
	Análisis de situación actual		■	■			
Planificación	alcance, viabilidad y factibilidad		■				
	Documento de plan de acción			■			
	Definición de actividades de la ejecución			■			
Ejecución	Recursos a utilizar para la ejecución			■			
	Mantener un Gobierno			■	■		
	Crear y mantener actualizado un inventario de base de datos			■	■		
	Elaborar una política interna de datos personales			■	■		
	Integrar la protección de datos en las operaciones			■	■		
Análisis de resultados	Mantener un programa de capacitación y concientización			■	■		
	Gestionar las peticiones y quejas de los individuos			■	■		
	Auditorías de cumplimiento				■		
	Análisis de resultados de implementación metodología riesgos				■	■	
Acciones de mejora continua	Análisis de resultados al implementar de procedimientos				■	■	
	Análisis de resultados al implementar de formatos de tratamiento					■	
	Análisis de resultados de capacitación					■	
	Retroalimentación, balance y lineamiento de la Alta Dirección						■
	Atención a No Conformidades						■
	Implementación de ajustes a ejecución						■
	Optimización de procesos y seguimiento continuo						■

Ilustración 2. Diagrama de Gantt

Trabajo futuro

Metódicamente el documento aborda la posibilidad de aplicar el modelo para implementar la defensa de datos en alcaldías locales, incluido el proceso de registro ante RNBD y el registro de las bases de datos identificadas en la alcaldía, sin embargo, puntualmente se tomó una como muestra para aplicar la metodología y ver los resultados obtenidos la alcaldía local de Tunjuelito.

Aplicación de procedimientos en oficinas de alcaldía local

Oficinas de la alcaldía local donde se aplicaron los procedimientos son:

- Correspondencia
- Almacén
- Atención al ciudadano
- Recepción
- Atención al consumidor
- secretaria de inspecciones
- Contratación
- Infraestructura
- Archivo
- Integración social
- Atención a adulto mayor
- Sistemas
- Comunicaciones
- Poblacionales
- Planeación
- Presupuesto
- Contabilidad
- Junta administradora local
- Riesgos locales
- Obras
- Asesoría jurídica
- Despacho
- Gestión para el desarrollo local
- Coordinación Jurídica
- Coordinación Normativa y policiva
- Inspecciones de policía
- Dirección de tecnología local

RESULTADOS

La metodología del manejo de datos tiene implícito los conjuntos de directrices de acción para referir y examinar el problema a través de instrucciones, es parte de la investigación realizada donde se refieren los mecanismos para efectuar los objetivos de esta investigación.

De manera general podemos relacionar que, con la implementación de la metodología propuesta, la Alcaldía Local de Tunjuelito logrará:

1. Estándares elevados de protección de datos personales.
2. Alineación a la legislación colombiana e internacional sobre la materia.
3. Mayor amparo de los datos de ciudadanos en la localidad.
4. Generar informes de transparencia a la ciudadanía con el uso adecuado de los datos personales recolectados.
5. Gestionar los riesgos del tratamiento de datos personales adecuadamente.
6. Permite conocer e inventariar los datos personales existentes en la entidad.
7. Conocer los tipos de datos tratados en la alcaldía.
8. Mantener una misión/visión de tratamiento de datos personales responsables en la entidad.
9. En caso de sanciones serán acorde al desarrollo demostrado de actividades enfocadas en proteger los datos personales de los ciudadanos.
10. Mantiene a los empleados y la alta dirección enterados y enfocados en el adecuado tratamiento de datos personales.
11. Mantener procedimientos para dar respuesta a las peticiones, quejas y reclamos de los ciudadanos acorde con la legislación.
12. Mantener un programa de gestión de incidentes y vulneraciones de datos.
13. Permite mantener procedimientos de mejora continua sobre la gestión de datos personales.

ENTREGABLES Y APLICACIÓN

Como entregables en el desarrollo del presente documento se encuentran las técnicas para gestionar riesgos en recolección de datos, procedimiento para la recolección de datos, modelos de formatos para la cogida de datos, propuesta de campaña de sensibilización a altos directivos y empleados, verificación de los lineamientos de seguridad de la información que se deben poseer para el procedimiento de los datos.

Metodología en gestión del riesgo

Metodología de gestión del riesgo en tratamiento de datos.

La evaluación de los riesgos de protección de datos es un requisito previo para el desarrollo adicional de un programa organizacional de protección de datos, en el cual el Oficial de Protección de Datos Personales crea y supervisa las autoevaluaciones individuales sobre protección de datos y seguridad. El proceso de evaluación de riesgos permite al Oficial de Protección de Datos identificar y dar prioridad a las vulnerabilidades o debilidades en el tratamiento de datos y en su seguridad para mitigar riesgos, favorecer el cumplimiento y mejorar la credibilidad del titular de los datos.

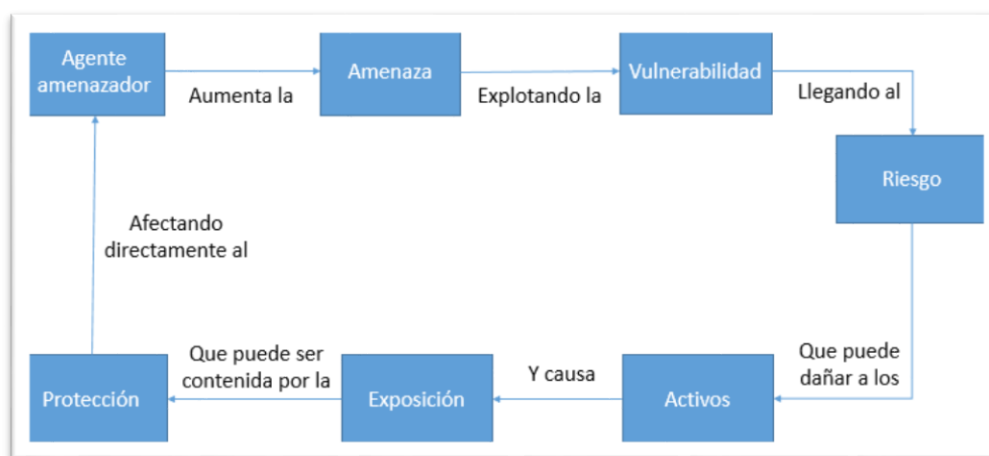


Ilustración 3. Proceso de tratamiento de riesgos

Con esta metodología planteada es basada en lineamientos definidos por la estructura de análisis de riesgos abordando las siguientes etapas o fases para la gestión del riesgo apoyados por el modelo Planear – Hacer – Verificar – Actuar (PHVA).

Fase 1 Planear

Establecimiento del Contexto, aquí debemos tener en cuenta que se debe revisar el marco estratégico de la alcaldía, se deben revisar los contextos a nivel interno y externo para lograr el entendimiento de los roles que se manejarán y también las responsabilidades que estarán inmersas durante el proyecto de la implementación.

Se debe tener en cuenta información de la alcaldía que sea de planeación estratégica y juega un papel muy importante también la participación del personal con encuestas, o también con entrevistas a los directivos, se pueden hacer visitas a instalaciones donde se puede recolectar más datos.

Básicamente se busca conocer los aspectos requieren protección teniendo en cuenta los recursos y los riesgos para saber los límites de adonde llegar con la implementación. Así entonces, poder determinar las actividades y los plazos que se van a usar durante todo el proceso.

Durante la definición del contexto externo se revisarán las variables que afecten a la administración de riesgos en la alcaldía, se debe definir también una relación de alcaldía con las normativas como estas puedan sobresaltar la operación de la alcaldía, así como al tratamiento de los datos.

Durante la definición del contexto interno hay que revisar los lineamientos de la alcaldía con su respectiva visión, la visión y sus objetivos y las metas.

El paso por seguir será entonces realizar una matriz de riesgos, donde se identifiquen las causas y actividades que pueden impactar directamente sobre la vulnerabilidad y se genere entonces el riesgo para la alcaldía local, en el marco del tratamiento de los datos.

Luego se asigna una numeración 1 - 5 de acuerdo a la afectación de los objetivos misionales de la alcaldía local.

De igual manera se dará un alcance en la gestión de riesgo donde se hará una retroalimentación teniendo en cuenta los procesos de la alcaldía local y los posibles factores donde es necesario la intervención de controles para garantizar la seguridad en el procesamiento de datos.

Para la implementación del modelo propuesto en esta fase se obtuvieron los siguientes datos en el caso de aplicación de la solución

Contexto de la organización

Misión

En la Entidad pública lideramos la articulación eficiente y efectiva de las autoridades para mejorar la calidad de vida de todos los ciudadanos. Garantizamos la convivencia pacífica y el cumplimiento de la ley en la ciudad, protegiendo los derechos y promoviendo los deberes de los ciudadanos. Servimos a todos los ciudadanos y promovemos una ciudadanía activa y responsable.

Visión

La Entidad pública, será en el 2025 la entidad líder en la articulación de un gobierno democrático, efectivo y confiable para la ciudadanía, reconocida por su modelo de buen gobierno, gestión por sus resultados, innovación institucional.

Contexto externo

Tabla 4. Contexto externo de la alcaldía local

ECONÓMICO:	POLÍTICO LEGAL
Disponibilidad de capital.	Cambios de administración (Efecto Político).
Bajos recursos para la adquisición de equipos de cómputo, principalmente servidores	Políticas públicas. Regulaciones.

MEDIOAMBIENTALES Energía. Catástrofes naturales.	SOCIALES Demografía. Terrorismo.
TECNOLÓGICOS Datos externos. Tecnología emergente.	LEGALES Legislación.

Contexto interno

Tabla 5. Contexto interno de la alcaldía local

INFRAESTRUCTURA: Disponibilidad de activos.	PROCESOS: Ejecución. Conocimiento.
PERSONAL: Carencias formativas. Salud. Seguridad. Compromiso y motivación de los funcionarios.	DATOS PERSONALES: La integridad y la disponibilidad de datos Software o infraestructura.

Dentro de los procesos que se analizan en la entidad existen procesos misionales, así como procesos estratégicos y de apoyo donde se generan macroprocesos liderados por la subsecretaría de gestión institucional. Realizando un diagnóstico inicial y de impacto sobre datos personales se tomó como muestra durante la implementación el proceso de “ADMINISTRACIÓN DE RECURSOS FÍSICOS Y DE SERVICIOS GENERALES”.

Definición del proceso.

TIPO DE PROCESO: Apoyo
PROCESO: Administración de Recursos Físicos y de Servicios Generales
SUBPROCESO 1: Recolección de datos personales de visitantes

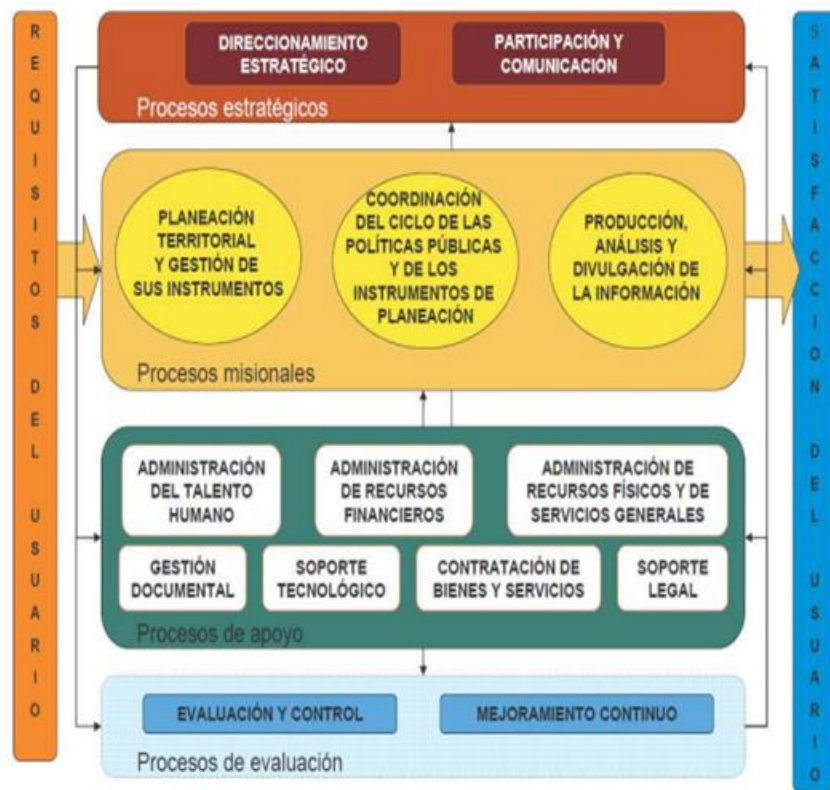


Ilustración 4. Procesos identificados en alcaldía local

Fase 2 Hacer

En esta fase es donde podremos identificar la gestión del peligro de afectación en procesos al interior.

Aspectos de gestión de riesgos en alcaldía local

Aspectos importantes a considerar en la gestión del riesgo son:

- Gestión de los riesgos para el tratamiento de datos
- Los recursos y funciones involucrados en el procesamiento de datos
- Asignar responsables respecto a la idoneidad para el procesamiento de datos.

La alcaldía local debe tener en cuenta la valoración que se haga a los riesgos y el personal que se encargara de aplicar los controles para garantizar que sea efectivo de eso depende la mejoras en acciones que se implantan a procesos de alcaldía, debe luego realizar una identificación y valoración de riesgos, para lo cual se debe tener en cuenta cómo hacer un correcto tratamiento.

Tratamiento del riesgo en alcaldía local

Para realizar el correcto tratamiento de los riesgos identificados analizamos los mejores métodos, para la toma de decisiones sobre cada uno de ella teniendo en cuenta los siguientes aspectos:

Aceptar: Mas allá de las medidas T.I con el desgaste es aceptada en caso de producirse y que a pesar de eso se ha aceptado por los directivos de la alcaldía local.

Transferir: Implica la disminución de la probabilidad del peligro.

Mitigar: cuando a pesar de aplicar los controles necesarios vemos que el impacto del peligro persiste y aun así es mínimo gracias al control.

Evitar: es cuando no se aplica ninguna acción puede ser debido a costos o decisiones administrativas.

El tratamiento de estos riesgos se puede realizar teniendo en cuenta el tipo de control:

- Control de eliminación: será cuando el riesgo que no se pueda controlar se convierte en un peligro en la alcaldía local. Lo aconsejables es gestionar al riesgo para eliminar y quitar el peligro.
- Control de sustitución: aquí tenemos en cuenta que el riesgo puede ser controlado y que se puede generar algún procedimiento que permita realizar el ajuste para minimizar el peligro.
- Control de ingeniería: en el caso que el peligro del riesgo no se puede controlar ni eliminar se buscan mecanismos que ayuden desde el área de ingeniería para poder manejar el peligro que se tiene con el riesgo.
- Control administrativo: en caso de que los anteriores controles no sean efectivos se puede acudir a la creación de políticas que se efectúen para controlar el peligro desde el área administrativa.

Aplicación de gestión de riesgos en alcaldía local

Para la implementación del modelo propuesto en esta fase se obtuvieron los siguientes datos en el caso de aplicación de la solución para un solo proceso escogido llamado “recolección de datos personales de visitantes”.

Tabla 6. Identificación de riesgos en proceso de recolección de datos personales de visitantes

ACTIVIDADES	CAUSA DEL RIESGO	RIESGO
Recolección de datos personales a visitantes.	Ausencia de autorizaciones en toma de datos otorgada del titular al momento de su captura.	Incapacidad de demostrar ante la autoridad o titular de los datos la autorización otorgada para el

		tratamiento de los datos.
Control de información recolectada	Los recepcionistas no tienen buena gestión sobre los datos recolectados.	Datos recolectados a la vista de visitantes y demás empleados de la alcaldía.
Políticas y/o procedimientos para la recolección, almacenamiento, uso, circulación y supresión de datos personales.	Inexistencia de procedimientos para todo el ciclo de vida del dato (recolección, almacenamiento, uso, circulación y supresión), lo cual no estandariza el proceso al interior de la entidad.	Manejo de datos personales sin lineamientos establecidos.
Capacitación de personal	Ausencia de conocimiento sobre protección de datos.	Incumplimiento de adecuado manejo de datos personales.

Crterios para la Gestión del riesgo

Tabla 7. Criterios de valoración de probabilidad

VALOR	DESCRIPCIÓN	OBSERVACIÓN	FRECUENCIA
1	Improbable	Sucede Ocasionalmente	No se ha presentado - 5 años
2	Menos Probable	Ciertos Casos	Presentada 1 vez - 5 años
3	Posible	Puede Suceder	Presentada 1 vez - 2 años
4	Probable	Cualquier Momento	Presentada 1 vez – 1 año
5	Casi Seguro	Cualquier Momento	Presentada más 1 vez - 6 meses

Tabla 8. Criterios de evaluación del impacto

NIVEL	CONCEPTO	DESCRIPCIÓN
1	INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	MODERADO	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	MAYOR	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad

5	CATASTRÓFICO	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.
---	--------------	--





Tabla 9. Apreciación de riesgos en alcaldía local

RIESGO	PROBABILIDAD	IMPACTO	VALORACIÓN
Incapacidad de demostrar ante la autoridad o titular de los datos la autorización otorgada para el tratamiento de los datos.	5	4	20
Datos recolectados a la vista de visitantes y demás empleados de la alcaldía.	5	4	20
Manejo de datos personales sin lineamientos establecidos.	4	3	12
Incumplimiento de adecuado manejo de datos personales.	3	4	12

Tabla 10. Matriz de apreciación a riesgos en alcaldía local

PROBABILIDAD	IMPACTO				
	INSIGNIFICANTE (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
IMPROBABLE (1)	B	B	M	A	A
MENOS PROBABLE (2)	B	B	M	A	E
POSIBLE (3)	B	M	A	E	E
PROBABLE (4)	M	A	A	E	E
CASI SEGURO (5)	A	A	E	E	E

Tabla 11. Criterios sobre la zona de riesgo

ZONA DE RIESGO	COLOR	DESCRIPCIÓN
Baja		La alcaldía local puede asumir el riesgo.
Moderada		La alcaldía local puede tratar de reducir riesgo.
Alta		La alcaldía local debe reducir - transferir riesgo.
Extrema		La alcaldía local requiere evitar - reducir - transferir el riesgo.

Controles a los riesgos en alcaldía local

Luego se deben aplicar los controles adecuados a los riesgos identificados

Tabla 12. Matriz de controles

RIESGO	CONTROLES
Incapacidad de demostrar ante la autoridad o titular de los datos la autorización otorgada para el tratamiento de los datos.	Desarrollar formatos de autorización de datos personales conforme a los requisitos mínimos exigidos por la legislación.
Datos recolectados a la vista de visitantes y demás empleados de la alcaldía.	Se deben definir y usar perímetros de seguridad para proteger áreas que contengan información restringida donde se manejen datos personales.
Manejo de datos personales sin lineamientos establecidos.	Definir e implementar modelos estándar al interior de la alcaldía donde se describan claramente los procedimientos a seguir en la captura, almacenamiento, uso, circulación y supresión de los datos recolectados.
Incumplimiento de adecuado manejo de datos personales.	Capacitar de manera específica al personal que se involucre en el tratamiento de datos personales

Recursos a los controles en alcaldía local

A los controles implementados se deben asignar unos recursos

Tabla 13. Matriz de recursos para controles

CONTROLES	RECURSOS
Desarrollar formatos de autorización de datos personales conforme a los requisitos mínimos exigidos por la legislación.	1 oficial de protección de datos personales (8 Horas) 1 abogado (8 Horas), 2 computadores de la entidad
Se deben definir y usar perímetros de seguridad para proteger áreas que contengan información restringida donde se manejen datos personales.	1 oficial de Seguridad de la Información (8 horas) 1 computador de la entidad
Definir e implementar modelos estándar al interior de la alcaldía donde se describan claramente los procedimientos a seguir en la captura, almacenamiento, uso, circulación y supresión de los datos recolectados.	1 oficial de protección de datos personales (8 Horas) 1 oficial de Seguridad de la Información (8 horas) 2 computadores de la entidad
Capacitar de manera específica al personal que se involucre en el tratamiento de datos personales	1 oficial de protección de datos personales (8 Horas) 1 oficial de Seguridad de la Información (8 horas) 2 computadores de la entidad

Fase 3 Verificar

En esta fase es donde la alcaldía local tendrá que validar la eficacia del tratamiento realizado y revisar si necesita realizar acciones que mejoren los controles implementados y así poder tratar los riesgos de la mejor forma mejorando en los procesos interiormente.

Se necesita entonces hacer un seguimiento minucioso con indicadores que permitan seguir la observación de cada control a los riesgos para poder concluir con los resultados óptimos en gestión de riesgos en implementación de seguridad de datos.

Auditorías, que son trabajos preventivos y perfeccionamiento: básicamente se deben diseñar desde el área de calidad mecanismos de auditorías o formatos de seguimiento que permitan dejar una reseña de los avances en la gestión de riesgos.

Implementación de procedimientos en alcaldía local

Por lo anterior se definen unos procedimientos para que sean implantados en las oficinas de la alcaldía local con los controles definidos para que se garantice los fundamentos de información y su tratamiento.

- Procedimiento para la recolección de datos personales
- Procedimiento de circulación de datos personales
- Procedimiento de recolección de datos personales
- Proceso de supresión de datos personales.
- Proceso de uso de datos personales

Estos procedimientos se explicarán en la sección siguiente denominado: Procedimiento para la recolección de datos personales donde se realizan unos procedimientos diagramados para la recolección y tratamiento de datos personales.

Fase 4 Actuar

Lo que se busca en esta fase es tener una óptima retroalimentación de los resultados que se han obtenido y los recursos que se han involucrado para así poder determinar si son necesarias modificaciones de mejora continua que le permitan a la alcaldía local mejorar en los procesos con la seguridad que se obtendrán avances en la gestión de riesgos minimizando así el peligro y aumentando la seguridad.

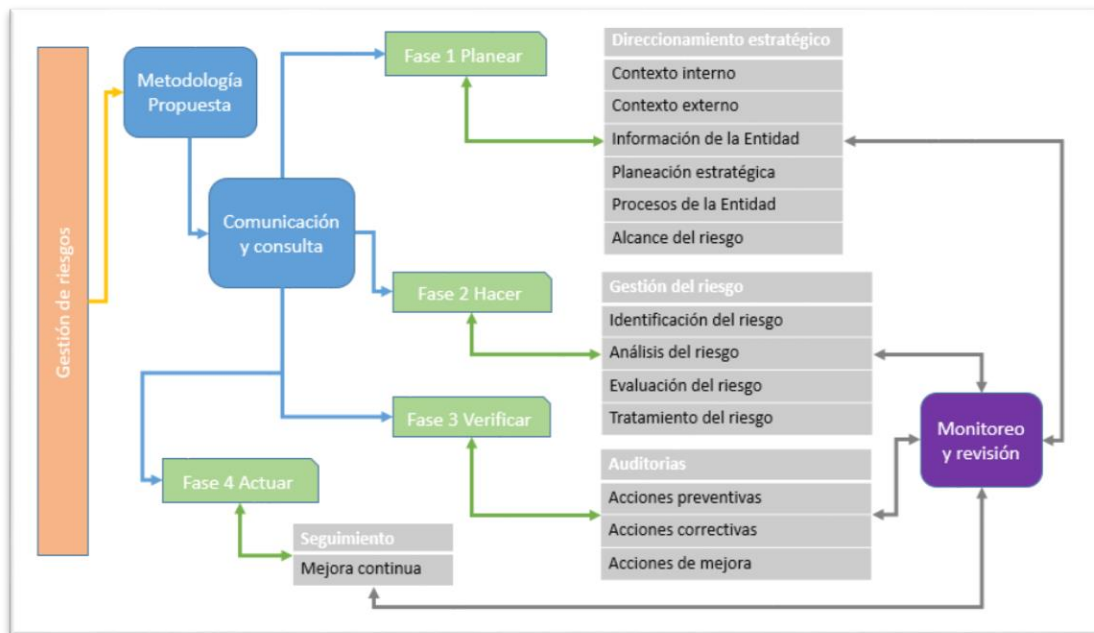


Ilustración 5. Diagrama metodología gestión del riesgo

PROCEDIMIENTOS PARA TRATAMIENTO

A continuación, se definen los siguientes procedimientos que comprenden todo el ciclo de vida del dato: recolección, almacenamiento, uso, circulación y supresión del dato.

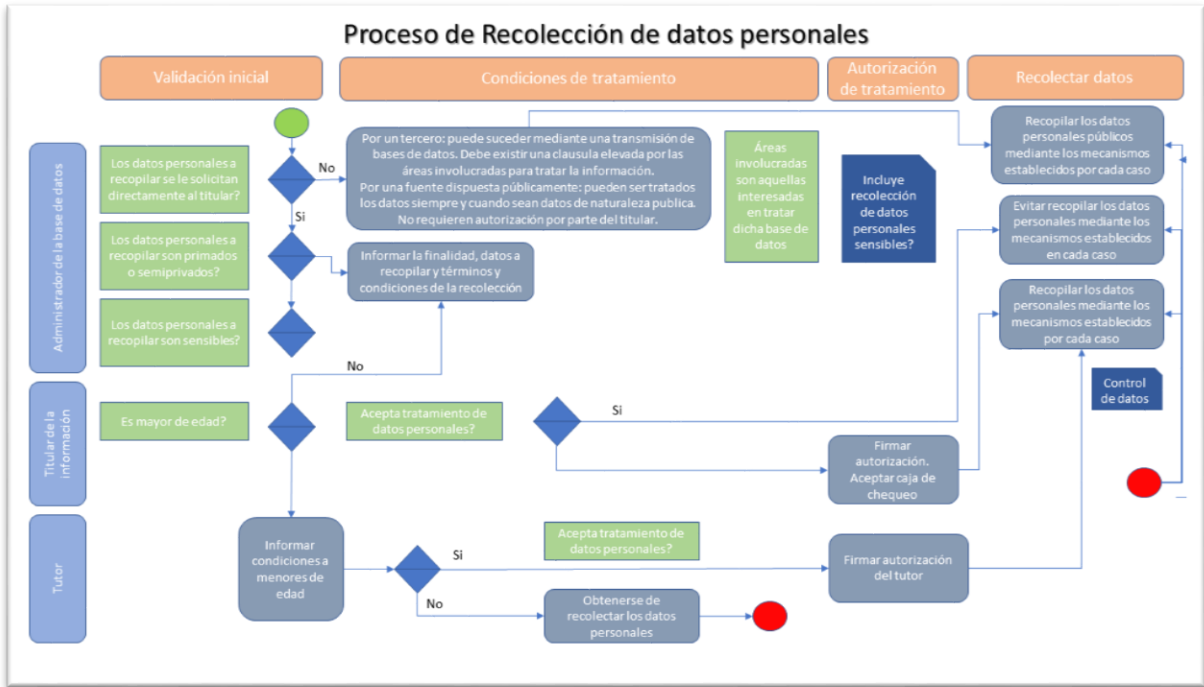


Ilustración 6. Procedimiento de recolección de datos personales

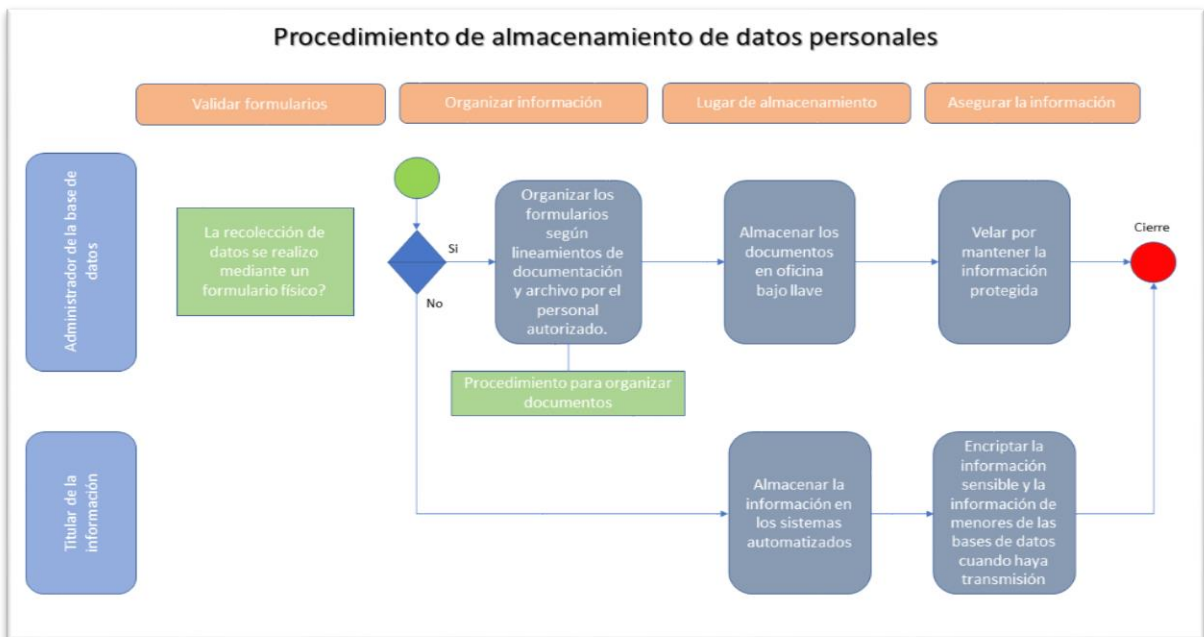


Ilustración 7. Procedimiento para el almacenamiento de datos personales

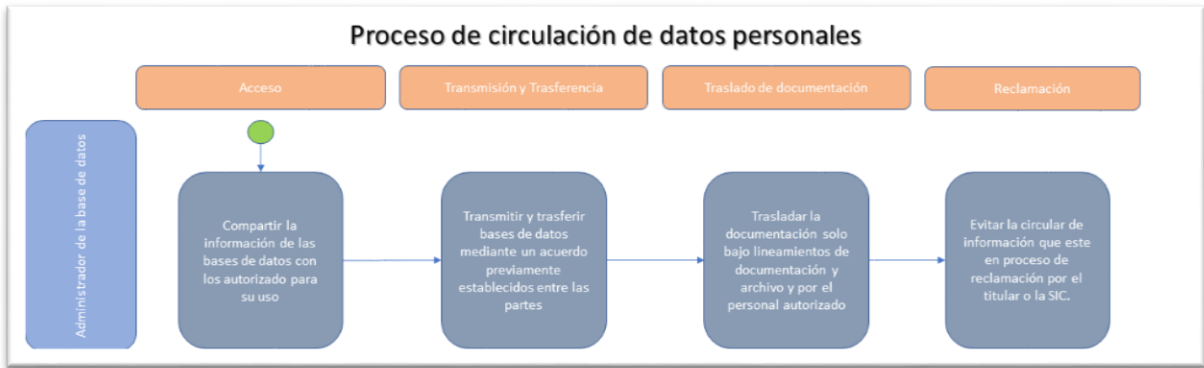


Ilustración 8. Procedimiento de circulación de datos personales

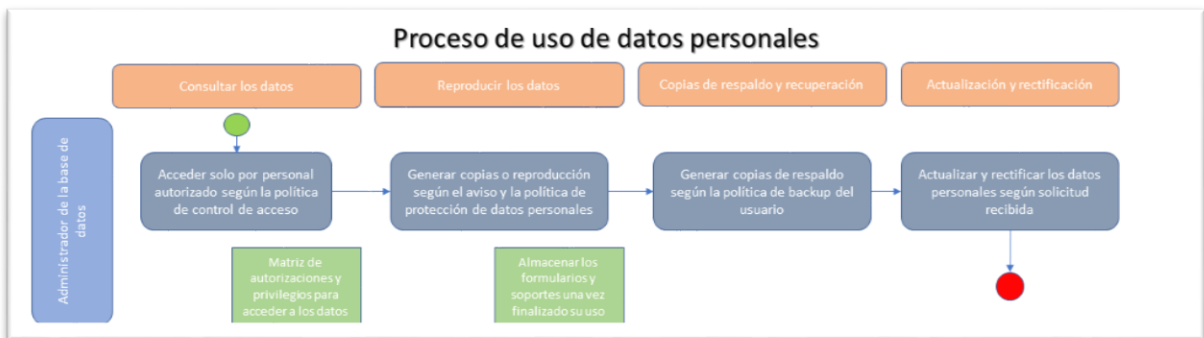


Ilustración 9. Proceso de uso de datos personales

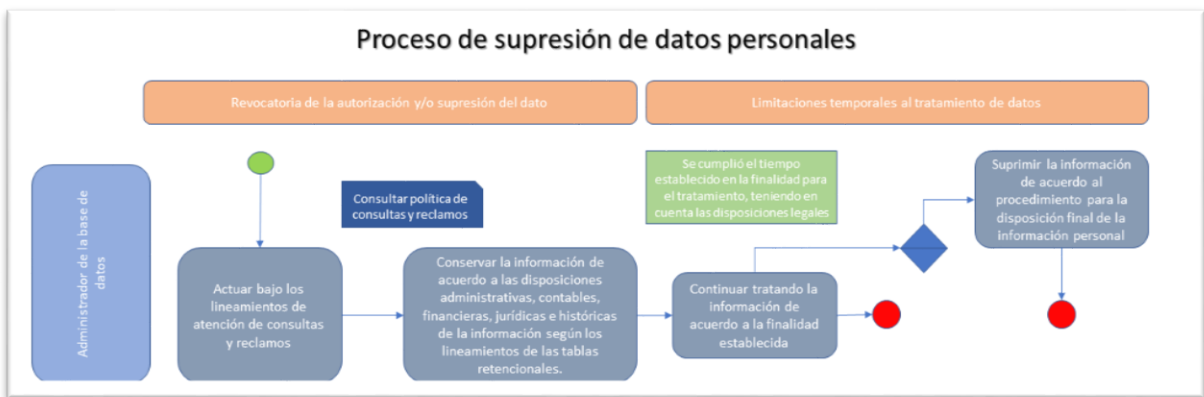


Ilustración 10. Proceso de supresión de datos personales.

MODELOS DE FORMATOS

Propuesta de formatos para la recolección de datos.

Tabla 14. Formato de autorización de datos personales

FORMATO DE AUTORIZACIÓN PARA TRATAMIENTO DE DATO PERSONAL	
Encabezado	Nombre y logo empresarial
Fecha	Fecha de expedición del documento
Contenido	<p>Como el dueño de Información acepto su procesamiento y autorizo de manera libre a NOMBRE DE LA EMPRESA para tratar mis datos personales con la finalidad de INCLUIR LA FINALIDAD QUE TENDRÁN LOS DATOS RECOPIRADOS. De igual manera, reconozco el derecho de validar, suprimir y modificar mis datos, y/o revocar esta autorización dirigiéndome por escrito al correo electrónico datospersonales@dominioempresa.com o al teléfono TELEFONO EMPRESARIAL.</p> <p>En lineamiento con lo previsto en la Ley 1581 y su(s) decreto(s) reglamentario(s), manifiesto que conozco el aviso de privacidad, de igual manera la directriz de seguridad de datos de NOMBRE DE LA EMPRESA publicado en la página web WWW.DOMINIOEMPRESA.COM</p> <p>Reafirmo que los datos dados son reales y que no se han alterado en ninguna información.</p> <p>Se firma en la ciudad de (día//mes//año)</p>
Firmas	Firmas Nombre Numero de documento de la persona
Pie de pagina	Datos de contacto y ubicación de la empresa

Aplicación de modelo para formatos en alcaldía local

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>GOBIERNO Alcaldía Local de Tunjuelito</small>	Radicado No. *RAD_S* Fecha: *F_RAD_S* **RAD_S**
FORMATO DE AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES	
<p>Bogotá, D.C.</p> <p>Como Titular de la Información acepto y autorizo de manera libre, voluntaria, previa, explícita, informada e inequívoca a ALCALDIA LOCAL DE TUNJUELITO para tratar mis datos personales con la finalidad de TRATAMIENTO DE INFORMACION PARA PROYECTOS DE INVERSION Y FUNCIONAMIENTO. Del mismo modo, reconozco el derecho de actualizar, rectificar y suprimir mis datos personales, y/o revocar esta autorización dirigiéndome por escrito al correo electrónico alcalde.tunjuelito@gobiernobogota.gov.co o al teléfono 7698460.</p> <p>De conformidad con lo previsto en la Ley 1581 de 2012 y su(s) decreto(s) reglamentario(s), manifiesto que he leído el Aviso de Privacidad y la Política de Protección de Datos Personales de ALCALDIA LOCAL DE TUNJUELITO publicado en la página web www.tunjuelito.gov.co Confirmando que los datos suministrados son verídicos y que no ha sido omitida o alterada ninguna información.</p> <p>Se firma en la ciudad de Bogotá, el día ____ del mes de _____ 2018.</p> <p>Firma: _____ Teléfono: _____ Email: _____</p>	
<small>Calle 51 Sur No. 7 - 35 vía Usme Código Postal: 111831 Tel. 7698460 Información Línea195 www.tunjuelito.gov.co</small>	

Ilustración 11. Formato implementado en Alcaldía Local

MODELO DE CAMPAÑA DE CAPACITACIÓN Y SENSIBILIZACIÓN

Dentro de la propuesta del modelo de campaña de sensibilización a altos directivos y empleados se proponen las siguientes opciones para el programa de capacitación y/o sensibilización.

Capacitación

Tabla 15. Programa 1: capacitación a la Alta Directiva

Programa de capacitación para altos ejecutivos formato 1	
Duración	2 horas x 1 vez a la semana.
Temario	Introducción: Breve introducción a normativas de seguridad de datos en Colombia: definiciones clave, principales obligaciones para los encargados de tratamiento. La responsabilidad demostrada en Colombia y el rol de los directivos en la creación de un programa integral de protección de datos
Discusión	Gestión efectiva de riesgos y oportunidades competitivas de alcaldía local derivadas de la implementación de seguridad de información.
Modalidad	Presencial.

Tabla 16. Programa 2: capacitación para empleados

Programa de capacitación de empleados formato 2	
Duración	6 horas (3 sesiones de 2 horas o 2 sesiones de 3 horas)
Temario	Introducción y conceptos básicos, ¿Qué es un dato personal? Tipos de datos y obligaciones especiales para su tratamiento Principales normas: contexto nacional e internacional Principios de protección de datos personales con énfasis en consentimiento y finalidad Sujetos obligados y principales obligaciones (Responsables y Encargados) Autoridad colombiana de protección de datos y régimen sancionatorio colombiano: responsabilidad corporativa e individual Políticas para proteger los datos en alcaldía local.

	Gestión interna de quejas e incidentes de seguridad
	Riesgos en la gestión de datos personales
	Usos inapropiados de la información personal en las organizaciones
	Construcción de un programa interno de seguridad de datos
Modalidad	Presencial.

Aplicación de modelo para capacitación en alcaldía local

Los resultados de este modelo se reflejan en los modelos aplicados a la alcaldía local de la siguiente manera:

Oficinas de la alcaldía local aptas para capacitación con formato 1 son:

- Despacho
- Oficina de gestión para el desarrollo local
- Coordinación Jurídica
- Coordinación Normativa y policiva
- Inspecciones de policía
- Dirección de tecnología local

Oficinas de la alcaldía local aptas para capacitación con formato 2 son:

- Radicación
- Correspondencia
- Almacén
- Atención al ciudadano
- Recepción
- Atención al consumidor
- Secretaria de inspecciones
- Contratación
- Infraestructura
- Archivo
- Integración social
- Atención a adulto mayor
- Sistemas
- Comunicaciones
- Poblacionales
- Planeación
- Presupuesto
- Contabilidad
- Junta administradora local
- Riesgos locales
- Obras
- Asesoría jurídica

Sensibilización

Actividades

- Creación de eslogan:

¡ Dato Seguro!

Ilustración 12. Eslogan de sensibilización

- Creación de personaje o mascota para la campaña.



Ilustración 13. Personaje de sensibilización

Escogimos la imagen de una lupa porque es de fácil asimilación o relación con los datos.
El nombre es tu dato seguro.

- Capacitaciones presenciales y virtuales.
- Semana de la protección de datos personales.
- Propagandas sobre protección de datos personales.

Metodología

- ✓ Capacitación presencial a las nuevas incorporaciones en la alcaldía. (Tarea en conjunto con recursos humanos, evaluación posterior para medir su comprensión en la capacitación).
- ✓ Capacitación presencial a todos los empleados de la alcaldía. (Evaluación posterior para medir su comprensión en la capacitación).
- ✓ Capacitación virtual a todos los empleados mediante una OVA (Objeto Virtual de Aprendizaje) que estará disponible a todos los empleados en la intranet de la alcaldía cuando no puedan asistir a las capacitaciones presenciales. (Evaluación posterior para medir su comprensión en la capacitación). Las evaluaciones para medir su comprensión en las capacitaciones nos permitirán identificar mejoras en el programa de sensibilización y nos permitirá medir su efectividad.
- ✓ Para llevar a cabo la semana del amparo de datos los otros días tendremos variedad actividades lúdicas en la empresa para captar la atención de los empleados y socializar y concienciar sobre la protección de datos personales.
 - El lunes se hará competencia de sopa de letras.
 - El martes se hará presentación de teatro (con apoyo de la casa de la cultura).

- El miércoles se hará presentación de show de humoristas (con apoyo de la casa de la cultura).
- El jueves se hará competencia de preguntas y respuestas por equipos.
- El viernes se hará presentación de grupo musical (con apoyo de la casa de la cultura).

Listado de los lineamientos para seguridad en información

Se propone dentro un modelo de seguridad en información sugeridos en SIC.

La alcaldía local debe reconocer que los siguientes lineamientos se cumplan de acuerdo con lo estipulado en el manual de usuario de la SIC[12]:

- a) La alcaldía debe validar si está vigente documentos de seguridad en información con aprobación.
- b) La alcaldía debe verificar si anteriormente ha realizado documentación en seguridad de información
- c) La alcaldía debe revisar si hay procedimientos de concesión de compromisos y permisiones en el tratamiento de información personal
- d) La alcaldía debe verificar si anteriormente ya ha realizado algunos pactos de reserva con personas que usan la información
- e) La alcaldía debe validar si ya tiene vigilancias de seguridad en la tercerización de productos para el procedimiento de información personal
- f) La alcaldía debe validar si se toman acciones realizadas con herramientas de gestión de riesgos en el método de datos
- g) La alcaldía debe revisar si tiene implementado un procedimiento de gestión de seguridad de información o una presentación integral de gestión a datos personales
- h) La alcaldía debe validar se posee efectuados controles de seguridad de la información para el personal antes y una vez finalizado contrato
- i) La alcaldía debe cotejar si existe una política de inspección de dirección a la información personal, tanto en las subestructuras físicas como tecnológico

- j) La alcaldía debe comprobar si cuenta con una manera para la gestión de usuarios con acceso a la información personal
- k) La alcaldía debe conocer si ha realizado una política para el acceso a la información personal de Databases con información sensible
- l) La alcaldía debe validar si ya se usa una política realizada de reproducción de respaldo a la información.
- m) La alcaldía debe revisar si se ya se implementa un procedimiento de protección para el acceso externo
- n) La alcaldía debe conocer si se tiene implementado un procedimiento que contemple la definición de especificaciones de seguridad
- o) La alcaldía debe validar si existen realizados controles de seguridad de la información durante el mantenimiento
- p) La alcaldía debe verificar si hay un procedimiento realizado de auditoría
- q) La alcaldía debe revisar si las bases de datos con información personal poseen referencia de consulta
- r) La alcaldía debe validar si cuenta con una política realizada para el correcto tratamiento de la información personal en los períodos del ciclo de vida del dato
- s) La alcaldía debe revisar si cuenta con un procedimiento realizado para la ratificación de datos de entrada y proceso de información
- t) La alcaldía debe aprobar si cuenta con un examen de seguridad de información para la ratificación de datos de salida
- u) La alcaldía debe verificar si ya se tienen una política realizada para el Intercambio físico o electrónico de datos en casos como el comercio electrónico
- v) La alcaldía debe aprobar si cuenta con un procedimiento o control realizado para la disposición final de la información
- w) La alcaldía debe cerciorarse de referir con una política y procedimientos implementados de gestión de incidentes
- x) La alcaldía debe examinar si existe implementada una política para mejorar la seguridad de la información personal a partir de los ocurrencias o debilidades detectados
- y) La alcaldía debe comprobar si hay políticas de auditorías de seguridad de la información
- z) La alcaldía debe revisar si dentro de las auditorías de seguridad de información personal, tiene en recuento la observancia de requisitos

DISCUSIÓN Y CONCLUSIONES

Discusión

Es importante que se tenga presente que la sociedad de la información está en constante desarrollo con las herramientas tecnológicas que se innovan a cada momento, pero se debe tener presente que el uso de la información tiene una regulación que está adaptándose a la misma y que busca velar por la salvaguarda de la ley.

También se debe referenciar el valor del desarrollo del Habeas Data en nuestro ordenamiento jurídico surge como mecanismo de protección a los derechos como la intimidad o la privacidad entre otros, que no tienen fin diferente al de proteger a los ciudadanos de la información contenida en las Databases de las entidades.

Así mismo, se puede decir que la información es de carácter personal cuyo titular es el único a quien concierne, esto a pesar de que se encuentren registradas en bases de datos, por lo que no debe ser usada de manera indebida o indiscriminada.

Es importante resaltar aquí respecto a la recaudación de la información en Colombia existe la debida reglamentación definida para obtener datos de las personas, así como los lineamientos en los procesos de tratamiento y divulgación de esta, los cuales al ser apoyados por las leyes colombianas son de estricto cumplimiento para los ciudadanos y acarrea las sanciones que las mismas determinen.

CONCLUSIONES

Es innegable que la protección de datos, es una obligación legal adquirida por los delegados del tratamiento de datos, con el fin de garantizar los derechos de los colombianos al adecuado tratamiento de datos, sin embargo aún se percibe el desconocimiento en la aplicabilidad de la ley y la falta de sensibilización e importancia sobre su adopción al interior de la alcaldía local de Tunjuelito y las actividades de procedimiento de datos, el desconocimiento sobre la existencia de la autoridad nacional de protección de datos personales y sus entes de vigilancia, traducen en inexistencia con un marco hacia el gobierno de gestión de datos personales al interior de la alcaldía local de Tunjuelito, que incluye entre otros la ausencia de apoyo y orientación de la alta dirección, y legal de la alcaldía local, el nombramiento de un cargo o área al interior de la alcaldía local de Tunjuelito que gestione los lineamientos y controles sobre seguridad de datos.

También se ven reflejadas las ausencias de capacitaciones en los empleados de la alcaldía local de Tunjuelito sobre la gestión de datos y los riesgos derivados del procedimiento de datos, la ausencia de formatos de autorizaciones para el procedimiento de datos, el desconocimiento del uso de información, de calidad en datos que debe estar presente en la recolección de datos, así como desconocer los diferentes tipos de datos sensibles, públicos y privados.

De manera relevante podemos concluir que las actividades de recolección de datos son actividades que no cuentan con actividades encaminadas a minimizar los riesgos en todo el ciclo del dato incluido las actividades de índole administrativa, legal y técnica, que aseguran el adecuado sistema de los datos suministrados por los titulares.

Es importante que los responsables y encargados continúen con el proceso de implementación, capacitación, sensibilización y amparo de las medidas responsablemente se cumplan los requerimientos de ley y sobre todo se respeten los derechos que tenemos los colombianos.

REFERENCIAS

- [1] B. Soediono, "Ley Estatutaria 1581 De 2012," *J. Chem. Inf. Model.*, vol. 53, no. Octubre 17, p. 160, 1989.
- [2] "Cartilla_Ley_1266_de_2008_Habeas_Data.pdf." .
- [3] Senado de la Republica, "Ley 1273," *D. Of. LEY*, vol. 2009, no. 36, 2009.
- [4] "Resolucion-070-de-2017 AM.pdf." .
- [5] Corte Constitucional de Colombia, "Constituci{ó}n pol{í}tica de Colombia actualizada con los actos legislativos a 2015," *Corte Const. Colombi*, p. 121, 1991.
- [6] M. D. E. Comercio and I. Y. Turismo, "Decreto 1377 de 2012," *Minist. comerico, Ind. y Tur.*, vol. decreto 13, pp. 1–11, 2013.
- [7] S. Eduardo, M. Benitez, and S. Redentoristas, "Datos personales," 1993.
- [8] "Guia_para_solicitar_la_declaracion_de_conformidad.pdf." .
- [9] "Guia-Accountability-SIC.pdf." .
- [10] "Aspectos_Derecho_de_Habeas_Data.pdf." .
- [11] F. Modelo, P. El, C. D. E. Obligaciones, and Y. S. U. S. D. Reglamentarios, "Formatos modelo para el cumplimiento de obligaciones establecidas en la ley 1581 de 2012 y sus decretos reglamentarios," 2012.
- [12] "Manual de Usuario del Registro Nacional de Bases de Datos – RNBD," 2016.