



31 ENE 2024

CONCEJO DE BELLO
Una decisión para todos

HORA: 13:56

FIRMA:

RESOLUCIÓN N°031
(Del 31 de enero de 2024)

"POR MEDIO DEL CUAL SE ADOPTA EL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL CONCEJO MUNICIPAL DE BELLO PARA LA VIGENCIA 2024"

EL PRESIDENTE DEL CONCEJO MUNICIPAL DE BELLO en uso de sus facultades y en especial las conferidas por la Ley 136 de 1994 modificada por la Ley 1551 de 2012, la Ley 1474 de 2011, el Decreto 1078 de 2015, el Decreto 1081 de 2015, el Decreto 1499 de 2017 y,

CONSIDERANDO

Que en virtud de lo previsto en la Ley 1581 de 2012, se protegerán los datos personales de todos los ciudadanos.

Que mediante el Decreto Ministerial 1078 de 2015, se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Que en el Decreto 1083 de 2015, se expidió el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran: "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital"

Que en el Decreto 612 de 2018, se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

Que en virtud de la Resolución 924 de 2020, se actualiza la política de tratamiento de datos personales del Ministerio/Fondo Único de TIC y se deroga la resolución 2007 de 2018.

Que a través de la Resolución 00500 de 2021 del Ministerio de las TIC, se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital.

Que por lo anterior se hace necesario crear el Plan de Seguridad y Privacidad de la Información el Concejo Municipal de Bello para la vigencia 2024.

En mérito a lo expuesto se,



RESUELVE

ARTÍCULO PRIMERO. Adoptar el Plan de Seguridad y Privacidad de la Información para la vigencia 2024 del Concejo Municipal de Bello, el cual hace parte integral del presente acto administrativo.

ARTÍCULO SEGUNDO. El presente Plan será de carácter obligatorio y deberá utilizarse de manera Permanente en todas las dependencias de la Corporación, con el objeto de mantener los estándares de calidad, seguridad y transparencia.

ARTÍCULO TERCERO. El seguimiento y control de las acciones contempladas en el Plan, le corresponde al Secretario General de la Corporación, de la entidad o quien haga sus veces.

ARTÍCULO CUARTO. La verificación de la elaboración, publicación en la página web de la entidad y evaluación de las acciones contempladas en este Plan, le corresponden al Jefe de la Oficina de Control Interno de Gestión o quien haga sus veces.

ARTÍCULO QUINTO. El Plan de Seguridad y Privacidad de la Información deberá ser publicado en la página web de la Corporación.

ARTÍCULO SEXTO: La presente resolución rige a partir de la fecha de expedición.

Dado en el Municipio de Bello a los treinta y uno (31) días del mes de enero de dos mil veinticuatro (2024).

PUBLÍQUESE Y CÚMPLASE

DANIEL RODRIGO VILLA MALDONADO
Presidente Concejo Municipal de Bello

Revisó: Jose Argemiro Restrepo Restrepo, Jefe de Oficina Asesora Jurídica

Proyectó: Paola Andrea Vélez Monsalve, Profesional Universitaria Planeación y Presupuesto Paola Vélez



CONCEJO DE BELLO
Una decisión para todos

Plan de Seguridad y Privacidad de la Información

Vigencia 2024



CONTENIDO

1. INTRODUCCIÓN	3
2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	6
3. NORMOGRAMA	4
4. DEFINICIONES	4
5. OBJETIVOS	6
6. ALCANCE	6
7. ANÁLISIS DE LA SITUACIÓN ACTUAL	7
8. ACTIVIDADES	8
9. SEGUIMIENTO	9
10. EVALUACIÓN	10



1. INTRODUCCIÓN

El presente documento describe el Plan de Seguridad y Privacidad de la Información en el Concejo Municipal de Bello, alineado con los objetivos, metas, procesos, procedimientos y la estructura organizacional.

En este Plan, se definen y detallan el uso adecuado de los sistemas de información, así como las herramientas de comunicaciones, internet y correo electrónico, principalmente con el fin de proteger al usuario y la Corporación de situaciones que pongan en peligro los sistemas de información contenida en ellos.

“La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente”.

La planificación e implementación del Plan de Seguridad y Privacidad de la Información – PSPI, en la Corporación está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos, y la estructura administrativa. El Plan de Seguridad y Privacidad de la Información – PSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Mediante el aprovechamiento de las TIC y el plan de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información en la Corporación, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación Colombiana.

El desarrollo de las actividades para lograr su consecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad



presupuestal oportuna y a las orientaciones de la alta dirección que se adopten para afrontar el desarrollo y cumplimiento de las actividades planificadas en este PSPI.

2. NORMOGRAMA

Decreto Ministerial 1078 de 2015: “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Resolución 924 de 2020. Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo Único de TIC.

3. DEFINICIONES

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).



Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).



4. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

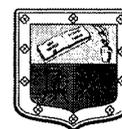
Para el Concejo Municipal de Bello en cuanto mayor sea el volumen y valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada. Por lo anterior, la Corporación adopta una metodología para la identificación y valoración de los activos de información, y una metodología para la evaluación y tratamiento de los riesgos; siendo éste el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto que éstos representan para la entidad y sus partes interesadas.

5. OBJETIVOS

1. Proteger los activos de información del Concejo Municipal de Bello, con base en los criterios de confidencialidad, integridad y disponibilidad.
2. Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
3. Sensibilizar a los servidores públicos y contratistas de la Corporación sobre el Plan de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de estos, en cuanto a la necesidad de salvaguardar los activos de información críticos de cada proceso.
4. Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante los controles respectivos.
5. Implementar acciones correctivas y de mejora para el del Plan de Seguridad y Privacidad de la Información establecido en la Corporación.

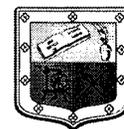
6. ALCANCE

Aplica a todos los procesos del Concejo Municipal de Bello, sus funcionarios, contratistas, proveedores y aquellas personas o terceros que debido al cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien o consulten cualquier tipo de información, ya sea interna o externamente independientemente de su ubicación.



7. ANÁLISIS DE LA SITUACIÓN ACTUAL

FACTORES INTERNOS	
FORTALEZAS (F)	
<ul style="list-style-type: none">• Compromiso de la Alta Dirección para la gestión de recursos para el desarrollo de proyectos de tecnológicos.• Suscripción de convenio interadministrativo con la Alcaldía Municipal de Bello para gestionar recursos y apoyo a los procesos de la Corporación	<ul style="list-style-type: none">• No se cuenta con un plan de contingencia para el respaldo de la información.• No se cuenta con ningún sistema de información que permita la consolidación de la información.• La Corporación no cuenta con los recursos suficientes para adquirir la infraestructura de TI que permita una gestión eficiente en sus procesos internos y externos.• Obsolescencia del software y el hardware de la Corporación.
FACTORES EXTERNOS	
OPORTUNIDADES	AMENAZAS
<ul style="list-style-type: none">• Disposición de donantes de orden municipal, departamental y nacional en materia de herramientas tecnológicas.• Acceso a nuevas tecnologías y herramientas web para la gestión y seguridad de la información.• Disposición de recursos en el Gobierno Nacional para invertir en programas de innovación en entidades públicas.	<ul style="list-style-type: none">• Riesgos de pérdida de información por agentes externos a la Corporación• No contar con instalaciones ni equipo tecnológico de propiedad de la Corporación.



8. ACTIVIDADES

ID	CONTROLES	ACTIVIDAD	ACTIVIDAD	ACTIVIDAD	RESPONSABLE
1	Política general de seguridad de la información	Establecer la política general de seguridad de la información	Revisar y/o ajustar la política de seguridad de la información al menos cada año	Hacer seguimiento a las evidencias de actualización y revisión del cumplimiento de la política de Seguridad	Presidente Secretaría General Profesional de Planeación y Presupuesto
2	Manual de seguridad de la información	Manual de seguridad de la información	Actualización del Manual de Seguridad de la Información	Realizar seguimiento del Manual de Seguridad de la Información	Presidente Secretaría General Profesional de Planeación y Presupuesto
3	Gestión de activos de Información	Levantamiento y/o actualización de los Activos de Información	Identificar nuevos activos de información en cada dependencia Validarla actualización de los activos de información	Verificación y aprobación de los activos de información para su publicación en Intranet Publicar los activos de información consolidada	Secretaría General Profesional de Planeación y Presupuesto
4	Gestión de riesgos (Identificación, Análisis y Evaluación de Riesgos)	Realizar seguimiento trimestral del Plan de Seguridad de la Información	Realizar valoración trimestral del riesgo residual	Realizar seguimiento a la documentación y evidencia de la ejecución del plan de seguridad de la información	Secretaría General Profesional de Planeación y Presupuesto



ID	CONTROLES	ACTIVIDAD	ACTIVIDAD	ACTIVIDAD	RESPONSABLE
5	Plan de comunicación, socialización y sensibilización	Elaborar y ejecutar el Plan de comunicación en temas relacionados con seguridad de la información Realizar mínimo 2 jornadas de sensibilización en seguridad de la información durante el año	Realizar evaluación de comprensión de seguridad posterior a las capacitaciones (Encuestas)	Hacer seguimiento a las evidencias de socialización del PSPI	Secretaría General Profesional de Planeación y Presupuesto
6	Auditoria Internas	Realizar auditorías internas al PSPI	Realizar seguimiento al cierre de las no conformidades producto de las auditorías internas del PSPI	Hacer seguimiento a las evidencias del cierre de las no conformidades por proceso	Jefe de Oficina de Control interno de Gestión
7	Gestión de incidentes y controles de seguridad	Gestionar los Incidentes de Seguridad de la Información identificados	Realizar controles a la gestión de incidentes de seguridad de la información	Realizar seguimiento de los reportes de eventos de seguridad de la información Seguimiento y aplicación de los controles y tomar acciones.	Secretaría General Profesional de Planeación y Presupuesto Jefe de Oficina de Control Interno

9. SEGUIMIENTO

El seguimiento y control de las acciones contempladas en el Plan, le corresponde al Secretario General de la Corporación, de la entidad o quien haga sus veces.



CONCEJO DE BELLO
Una decisión para todos

10. EVALUACIÓN

La verificación de la elaboración, publicación en la página web de la entidad y evaluación de las acciones contempladas en este Plan, le corresponden al Jefe de la Oficina de Control Interno de Gestión o quien haga sus veces.

DANIEL RODRIGO VILLA MALDONADO
Presidente Concejo Municipal

Revisó: Jose Argemiro Restrepo Restrepo, Jefe de Oficina Asesora Jurídica

Proyectó: Paola Andrea Vélez Monsalve, Profesional Universitaria Planeación y Presupuesto  Paola Vélez