Código:	D-GR-04
Versión:	02

POLITICA DE SEGURIDAD DIGITAL ALCALDIA DE BELLO

1. PRESENTACIÓN

El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, ha incrementado la participación digital de los ciudadanos, generando nuevas formas para atentar contra su seguridad y la del Estado, por ende, es necesario fortalecer las capacidades de las instituciones para identificar, gestionar el riesgo y atender las situaciones para brindar protección en el ciberespacio.

A través de la política de seguridad digital se han propuesto estrategias que permiten resolver problemas, generar diagnósticos más rápidamente, así como comparar diferentes escenarios posibles para prevenir riesgos cibernéticos en la plataforma dispuesta para Municipio de Bello.

Con la implementación de la Política de Seguridad de la Información, la Administración Central de Bello adopta un compromiso obligatorio de protección a la información frente a una amplia gama de amenazas. Contribuyendo a minimizar los riesgos asociados de daño y asegurar el eficiente cumplimiento de las funciones de la entidad apoyadas en un correcto uso de los Sistema de información.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar estrategias para mejorar las capacidades de la administración central de Bello en materia de seguridad digital generando confianza digital y adaptación para el

futuro digital.

2.2. OBJETIVOS ESPECÍFICOS

- Salvaguardar los activos tecnológicos y custodiar la información producida en la Alcaldía Municipal de Bello Antioquia.
- Definir lineamientos en materia de seguridad de la información.
- Promover la cultura de la seguridad de la información a los servidores públicos, contratistas, ciudadanos y público en general.
- Capacitar al personal de la Alcaldía en buenas prácticas digitales.
- Orientar a la ciudadanía en general sobre el uso responsable del medio digital.
- Fortalecer la capacidad de la administración en materia de prevención de riesgos digitales.

BASE NORMATIVA

- Acuerdo 08 de 2019
- Ley 1928 de 2018
- Acuerdo 02 de 2018
- Conpes 3854 de 2016
- Decreto 1078 de 2015
- Ley 1712 de 2014 - Transparencia y Acceso a la Información Pública
- Ley estatutaria 1581 de 2012
- Decreto 103 de 2015
- Ley 1273 de 2009

NORMATIVA	DESCRIPCION
Directiva Presidencial 04 de 2012	Eficiencia Administrativa y lineamientos de la política cero papeles en la Administración Pública.

NORMATIVA	DESCRIPCION
Acuerdo 03 de 2015 del AGN	Por el cual se establecen los lineamientos generales para las Entidades del Estado en cuanto a la gestión de documentos electrónicos generado como resultado del uso de medios tecnológicos de conformidad con lo establecido en el Capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el Decreto 2609 de 2012.
Ley 1150 de 2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos".
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
Ley 1273 de 2009	“Por medio de la cual se modifica el Código Penal, se crea un nuevo Bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 2693 de 2012	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones
Decreto 212 de 2014	Por medio del cual se crea el comité de Gobierno en línea, Anti-trámites y Eficiencia Administrativa

NORMATIVA	DESCRIPCION
Decreto 1078 de 2015	Art. 2.2.9.1.2.2 contemplo los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad un Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información
Decreto Nacional 2573 de 2014	por el cual se establecen los lineamientos generales de la estrategia de gobierno en línea, se reglamenta parcialmente la ley 1341 de 2009 y se dictan otras disposiciones
Decreto 612 de 2018	Por el cual se fijan las directrices para la integración de planes institucionales y estratégicos al Plan de acción por parte de las entidades del Estado

4. DEFINICIONES[1]

- **Activo de Información:** Es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Copias de respaldo:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Gestión de riesgos de seguridad digital:** es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar

[1] 1 definiciones tomadas del manual de Gobierno Digital Implementación de la Política de Gobierno Digital. Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1

el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **Resiliencia:** es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (Documento CONPES 3854).
- **Responsabilidad:** las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales.
- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **Riesgo de seguridad digital**: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

5. LINEAMIENTOS GENERALES DE LA POLÍTICA

La Alcaldía Municipal de Bello, asignará responsabilidades frente a la seguridad de la información que serán definidas, compartidas, publicadas y aceptadas por cada uno de los proveedores, socios de la Entidad o terceros.

- La Alcaldía Municipal de Bello, verificará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Alcaldía Municipal de Bello, protegerá la información creada, procesada, transmitida o resguardada por los procesos de la Entidad, con el fin de minimizar los impactos financieros, operativos o legales a causa de los usos de esta y las amenazas originadas por parte del personal.
- Toda información que provenga de un archivo externo de la Entidad o que deba ser descargado tiene que ser analizado con el antivirus institucional vigente.
- Todo usuario de los recursos TIC, NO debe visitar sitios restringidos de manera explícita o implícita, o sitios que afecten la productividad de la Institución; como el acceso desde la Entidad a sitios relacionados con la pornografía, juegos, redes sociales no autorizadas, etc.
- Minimizar el uso de dispositivos extraíbles para compartir archivos aprovechando los recursos compartidos del servidor de la entidad o haciendo uso del servicio de internet.
- Todo usuario de los recursos TIC debe advertir e informar a la Secretaria de Gobierno y/o oficina de Gobierno en Línea o quien haga sus veces, de las medidas específicas de protección para evitar el acceso a personal no autorizado, y/o establecer el sistema de respaldo para la misma.

6. POLÍTICA DE SEGURIDAD DIGITAL

La Alcaldía Municipal de Bello, con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales, adoptará en esta política que en su conjunto tendrá como fin contrarrestar el incremento de las amenazas informáticas que pueden afectar significativamente la institución y el correcto desarrollo normativo y legal de las mismas fortaleciendo la institucionalidad de la entidad.

6.1 ALCANCE

La Política de Seguridad Digital pretende identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades.

6.2 APLICABILIDAD

Esta política aplica para todos los procesos institucionales, pues la eficiencia de todos y cada uno de los procesos afecta directa o indirectamente los recursos institucionales, por lo tanto, será aplicable a todos los empleados, contratistas, proveedores, visitantes y ciudadanos de la Alcaldía y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

Es un compromiso y responsabilidad de todos conocer la Política y es su deber cumplirla y respetarla para el desarrollo de cualquier actividad o consulta.

6.3 NIVEL DE CUMPLIMEINTO

Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran en un 100% a la política. Las políticas de serán objeto de evaluación aplicando mecanismos de mejoramiento continuo que involucren participación, compromiso, cooperación, adaptación e inversión.

La Política de Seguridad Digital de la administración municipal será de obligatorio cumplimiento para todos los servidores públicos de planta, contratistas, practicantes, proveedores y terceros. La política abarca clientes internos que son las dependencias que componen la estructura de la administración.

6.4 IMPLEMENTACIÓN DE ESTRATEGIAS

A continuación, se describen las estrategias que se implementarán para alcanzar la política de seguridad digital.

- Implementar iniciativas apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias digitales para afrontar las amenazas y los riesgos que atentan contra la seguridad digital.
- Brindar capacitación especializada en seguridad de la información y seguridad digital
- Definir, implementar, operar y mejorar de forma continua el Plan de Seguridad y privacidad de la información, soportado en lineamientos claros alineados a las necesidades, a la normatividad y a los requerimientos regulatorios.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los usuarios, o terceros.
- Aplicar controles de acuerdo con la clasificación de la información salvaguardada y en custodia por cada uno de los funcionarios, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.
- Realizar ejercicios de auditoria y monitoreo de la operación de sus procesos que involucren la plataforma tecnológica para minimizar los riesgos asociados al manejo de los recursos tecnológicos y las redes de datos.
- Implementar controles de acceso a la información, sistemas y recursos de red.
- Adoptar una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información e implementar estrategias de mejoramiento continuo.
- Elaborar procedimientos de acuerdo con la normatividad que permitan minimizar los riesgos que puedan generar los eventos.

6.5 COMUNICACIÓN

La divulgación de la Política debe ser transmitida e implementada a través de las diferentes dependencias que conforman la estructura organizacional y jerarquía de la administración municipal.

6.6 EVALUACION Y SEGUIMIENTO

El seguimiento es un instrumento indispensable para la implementación adecuada de la política. Se trata de contar con la opción de supervisar el avance o, en su caso, los

problemas que registre el desarrollo de la misma para de manera oportuna tomar acciones o medidas correctivas.

ÍNDICES DE GESTIÓN Y DESEMPEÑO POLÍTICA SEGURIDAD DIGITAL

Índice de Desempeño Institucional

Gestión para Resultados con Valores

- Seguridad Digital

ESTRATEGIAS	UNIDAD DE MEDIDA	INDICADOR	RESPONSABLE	PERIODICIDAD
Implementar estrategias para afrontar las amenazas y los riesgos que atentan contra la seguridad digital.	Estrategias para minimizar riesgos	Seguridad Digital	Todas las dependencias	Final Vigencia
Brindar capacitación especializada en seguridad de la información	Capacitación en seguridad de la información	Seguridad Digital	Todas las dependencias	Final Vigencia
Definir, implementar, operar y mejorar de forma continua el plan de Seguridad y privacidad de la información,	Plan de Seguridad y privacidad de la Información	Seguridad Digital	Todas las dependencias	Final Vigencia
Definir responsabilidades frente a la seguridad de la información	Responsabilidades definidas	Seguridad Digital	Todas las dependencias	Final Vigencia
Aplicar controles de acuerdo con la clasificación de la información salvaguardada y en custodia por cada uno de los funcionarios	Controles aplicados	Seguridad Digital	Todas las dependencias	Final Vigencia

ESTRATEGIAS	UNIDAD DE MEDIDA	INDICADOR	RESPONSABLE	PERIODICIDAD
Realizar ejercicios de auditoria y monitoreo de la operación de sus procesos que involucren la plataforma tecnológica para minimizar los riesgos asociados al manejo de los recursos tecnológicos y las redes de datos.	Auditorías realizadas	Seguridad Digital	Todas las dependencias	Final Vigencia
Implementar controles de acceso a la información, sistemas y recursos de red.	Controles realizados	Seguridad Digital	Todas las dependencias	Final Vigencia
Adoptar una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información e implementar estrategias de mejoramiento continuo.	Estrategias de mejoramiento continuo	Seguridad Digital	Todas las dependencias	Final Vigencia
Elaborar procedimientos de acuerdo a la normatividad que permitan minimizar los riesgos que puedan generar los eventos.	Procedimientos	Seguridad Digital	Todas las dependencias	Final Vigencia

7. CONCLUSIONES

- La implementación de esta política permite establecer reglas, lineamientos y buenas prácticas que coadyuven a la confidencialidad, seguridad y disponibilidad de la información digital que permita minimizar el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, y duplicación e interrupción intencional de la información.

- El desarrollo de las estrategias de la Política de Seguridad Digital busca contrarrestar el incremento de las amenazas informáticas que pueden afectar significativamente la institución y el correcto desarrollo normativo y legal de las mismas fortaleciendo la institucionalidad de la entidad.

NOTAS DE CAMBIO

BREVE DESCRIPCIÓN DEL CAMBIO	VERSIÓN	FECHA aaaa-mm-dd
No aplica para la primera versión.	01	2020-12-21
Se actualiza la versión anterior de acuerdo a la base normativa y los indicadores de gestión de la función publica	02	2022-07-26

Elaboró:	León Darío Arbeláez Álvarez, Profesional Universitario	Fecha:	2022-07-26
Revisó:	Julián Montoya, Director de las TIC y Soporte Tecnológico	Fecha:	2022-07-26
Aprobó:	Julián Montoya, Director de las TIC y Soporte Tecnológico	Fecha:	2022-07-26

ANEXOS