Tabla de versiones

Versión	Fecha	Aprobado por
1.0	25 / 05 / 2012	Ing. Jhon Jairo Jiménez Álvarez Profesional Especializado en Sistemas
2.0	10 / 02 / 2019	Ing. Alberto Eloy Carrillo Vargas Secretario TIC
3.0	24 / 04 / 2020	Ing. Patricia Helena Fierro Vitola Secretaria de las TIC, Ciencia e Innovación
4.0	30 / 10 / 2020	Ing. Patricia Helena Fierro Vitola Secretaria de las TIC, Ciencia e Innovación

Contenido

1. INTRODUCCIÓN

La Alcaldía Distrital de Barrancabermeja, reconoce que la información que gestiona es uno de los activos más importantes para su funcionamiento y que ésta puede ser de naturaleza legal, estratégica, financiera, operativa y en algunos casos corresponder a datos personales de servidores públicos, contratistas y grupos de interés.

Igualmente, es consciente de las amenazas que enfrenta dichos activos y de las consecuencias a las que se expone la Entidad cuando ésta no cuenta con las medidas de seguridad adecuadas, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información (creación, procesamiento, almacenamiento, transmisión, utilización o destrucción).

En ese sentido, se hace necesario propender por la seguridad y privacidad de la información de la Alcaldía Distrital, teniendo en cuenta que la vulneración se encuentra en cualquier estado de su ciclo de vida y ésta puede llegar a tener impactos a nivel legal, de imagen, operacional, en el cumplimiento de la misión y los objetivos estratégicos de la Entidad.

El presente manual se establecen las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas por los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Alcaldía Distrital; Dichas políticas y estándares deberán ser tenidas en cuenta por los usuarios de los servicios de Tecnologías de la Información y las Comunicaciones, para proteger adecuadamente los activos tecnológicos y la información. Estas se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO/IEC 27001:2013 y al modelo de seguridad y privacidad de la información de la estrategia Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

2. BENEFICIOS

Las políticas y estándares de seguridad y privacidad de la información establecidas dentro de este documento son la base para la protección de los activos tecnológicos y de información de la Alcaldía Distrital de Barrancabermeja y a su vez define las responsabilidades de los usuarios asignados a la Secretaría de las TIC, Ciencia e Innovación

3. OBJETIVO GENERAL DEL MSPI

El presente documento define las políticas y estándares del Modelo de Privacidad y Seguridad de la Información (MSPI) de la Alcaldía Distrital de

Barrancabermeja que son de obligatorio cumplimiento para cualquier persona que tenga acceso a los activos de información de la Entidad, con el fin de proteger la información y los sistemas que la soportan frente a posibles amenazas y reducir los daños provocados por incidentes.

3.1. OBJETIVOS ESPECÍFICOS

Los objetivos del MSPI están enmarcados en el cumplimiento de las propiedades de la seguridad de la información con el propósito de preservar su Confidencialidad, Integridad y Disponibilidad a fin de fortalecer la continuidad de las actividades administrativas, operativas y logísticas de la Alcaldía Distrital de Barrancabermeja para fortalecer sus objetivos misionales y necesidades propias, reduciendo los riesgos y optimizando la inversión en tecnologías de información. Para tal efecto, se obrará en concordancia con las disposiciones legales vigentes.

Este enfoque es por procesos y debe extenderse a toda la Entidad.

- ✓ Establecer un modelo organizacional de Seguridad de la Información, definiendo claramente los roles y responsabilidades de los que intervienen en la implementación de la política.

- ✓ Proteger los recursos de información y tecnología frente a amenazas internas y externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, mediante la implementación de controles efectivos.

- ✓ Promover, mantener y realizar mejoramiento continuo del nivel de cultura en Seguridad de la Información, así como lograr la concienciación de todos los funcionarios y contratistas y demás personas que interactúen con la ALCALDÍA DISTRITAL DE BARRANCABERMEJA, para minimizar la ocurrencia de incidentes de Seguridad de la Información.

- ✓ Mantener la política de Seguridad de la Información actualizada, a efectos de asegurar su vigencia y eficacia.

4. CONTEXTO DE LA ORGANIZACIÓN

4.1. COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO

Los resultados medición y evaluación del estado de seguridad actual utilizando el instrumento de evaluación de MSPI - Modelo de Seguridad y Privacidad de la Información.
Fecha de Medición: Julio de 2020

No.	Evaluación de Efectividad de controles

	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	40	100	**REPETIBLE**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	4	100	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	0	100	**INEXISTENTE**
A.8	GESTIÓN DE ACTIVOS	14	100	**INICIAL**
A.9	CONTROL DE ACCESO	11	100	**INICIAL**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	16	100	**INICIAL**
A.12	SEGURIDAD DE LAS OPERACIONES	13	100	**INICIAL**
A.13	SEGURIDAD DE LAS COMUNICACIONES	9	100	**INICIAL**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	1	100	**INEXISTENTE**
A.15	RELACIONES CON LOS PROVEEDORES	0	100	**INEXISTENTE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	3	100	**INICIAL**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	**INEXISTENTE**
A.18	CUMPLIMIENTO	26	100	**REPETIBLE**
PROMEDIO EVALUACIÓN DE CONTROLES		**10**	**100**	**INICIAL**

BRECHAS DE SEGURIDAD A PARTIR DE LA MEDICIÓN REALIZADA

Brechas de seguridad de la información

Id Brecha	Brecha
SI-01	Inexistencia de una Política de Seguridad apropiada e implementada
SI-02	Inexistencia de un proceso de documentación de la Política
SI-03	Falta de Capacitación y Competencias del RR.HH.
SI-04	Vulnerabilidad de la Infraestructura Física del Data Center
SI-05	Falta de Gestión del Conocimiento lecciones aprendidas incidentes
SI-06	Falta de pruebas, simulaciones y acciones de continuidad operación
SI-07	Falta de la Cultura de Riesgo
SI-08	Falta de Indicadores de Medición

A partir del análisis de la matriz DOFA se definieron las acciones para minimizar las amenazas, potenciar las fortalezas, mejorar las debilidades y aprovechar las oportunidades; obteniendo el siguiente resultado:

DOMINIO	Estrategia/Acción
	Desarrollar y Fortalecer las capacidades estratégicas del área de TI para poder soportar los objetivos estratégicos y atender los requerimientos de las áreas operativas y de apoyo de la entidad.

Estrategia	Mejorar la capacidad de relacionamiento e interlocución con todos los actores del Ecosistema Digital a nivel local, regional y nacional.
	Desarrollar capacidades para hacer seguimiento al entorno, entender las tendencias, su impacto para poder anticiparse y generar proyectos que se adelanten a los problemas, necesidades del ciudadano en temas de TI
	Desarrollar el liderazgo del área de TI como agente de cambio e impacto por el uso adecuado y a tiempo de las TI para mejorar el bienestar de los ciudadanos del Distrito de Barrancabermeja
Gobierno TI	Desarrollar un Sistema de Gobierno y Gestión de TI para la Secretaría de las TIC-Cei del Distrito.
	Desarrollar e Implementar la Política de Gobierno Digital para fortalecer las capacidades de la Secretaría de las TIC-Cei.
	Desarrollar el Plan Estratégico de TI para dar cumplimiento al marco normativo del Gobierno nacional.
	Capacitar al Talento Humano de la Secretaría de las TIC-Cei en el marco normativo de la Política para mejorar la apropiación.
Información	Generar competencias en el equipo de TI para construir la arquitectura de información de la entidad.
	Definir estrategias y acciones que incentiven la participación de las áreas de la entidad en la gestión de la información para garantizar la cultura del dato.
	Desarrollar la cultura del dato como insumo para la toma de decisiones objetivas en la entidad.
	Asegurar y garantizar la integridad, confiabilidad y disponibilidad de la información de la entidad para generar valor a partir de su correcta gestión.
Sistemas Información	Desarrollar capacidades en el área de TI para fortalecer la gestión de los Sistemas de Información de acuerdo con el marco de arquitectura de TI.
	Desarrollar alianzas para mejorar las capacidades de respuesta de los sistemas de información para gestionar los trámites y servicios digitales.
	Mejorar la capacidad del área de TI para gestionar la Seguridad y Privacidad de la Información.
	Actualizar y aprobar la Política de Seguridad y Privacidad de la Información para garantizar la continuidad de la operación
Servicios Tecnológicos	Desarrollar un Plan de actualización de la Infraestructura de TI para cerrar la brecha de obsolescencia que presenta.
	Desarrollar una cartera estratégica de proyectos para actualizar la infraestructura de TI.
	Elaborar Mapa de Riesgos de Gestión y Operación de la Infraestructura de TI para identificar y mitigar los riesgos.
	Desarrollar planes, simulacros, pruebas de continuidad y recuperación de desastres para mejorar la capacidad de resiliencia ante eventos de alto riesgo.
Uso y Apropiación	Desarrollar un programa de formación del Talento humano del área de TI de acuerdo con el marco de arquitectura TI para cerrar la brecha en competencias del equipo.
	Desarrollar un Programa de Apropiación de las TI para sensibilizar a la entidad de su importancia.
	Realizar procesos de gestión del conocimiento para evitar su perdida en el área de TI.
	Gestionar recursos, alianzas, convenios para ampliar el cubrimiento de las TI en el Distrito de Barrancabermeja.
	Desarrollar un Programa de Apropiación de las TI para sensibilizar a los ciudadanos del Distrito.

A partir de la identificación de las anteriores acciones, donde se identificaron brechas por cada dominio y se definieron acciones para su tratamiento, se realizó

una clasificación de las brechas para generar el siguiente catálogo de alto nivel por dominios del marco de arquitectura TI.

BRECHAS	DESCRIPCIÓN	TEMA
1	Falta de una Visión estratégica para gestionar el área de TI, lo que no permite generar impacto con el despliegue de las TI.	GESTIÓN TI
2	Baja Capacidad en la estructura organizacional para soportar los roles estratégicos y de gestión que debe asumir el área para que se genere impacto con las tecnologías de la información.	GESTIÓN TI
3	La información no es considerada ni gestionada como un recurso estratégico al interior de la entidad.	ANALÍTICA DATOS
4	No existe la arquitectura de información para la gestión eficiente de los datos.	ANALÍTICA DATOS
5	No existen procesos y procedimientos para garantizar la seguridad y privacidad de la Información.	SEGURIDAD INFORMACIÓN
6	Baja capacidad del área de TI para garantizar la continuidad de la operación ante la falta de procesos claros de gestión de riesgos, seguridad de la información y continuidad de la operación.	SEGURIDAD INFORMACIÓN
7	Baja apropiación de la gestión de riesgos en el área de TI.	GESTION TI
8	Bajo relacionamiento con los actores del ecosistema para fortalecer capacidades de la seguridad de la información	SEGURIDAD INFORMACIÓN
9	Bajo Nivel de gestión TI en el Portafolio de Servicios al Ciudadano	SERVICIO AL CIUDADANO
10	Inexistencia de capacidades para optimizar la utilización e impacto de la Infraestructura de TI	INFRAESTRUCTURA
11	Falta de una cartera de proyectos que permita actualizar y disminuir el nivel de obsolescencia de los Servicios tecnológicos	INFRAESTRUCTURA
12	Falta de un Plan que permita planificar las inversiones para actualizar la infraestructura tecnológica de la entidad.	INFRAESTRUCTURA
13	Falta de un plan de formación para mejorar las capacidades y competencias del talento humano del área de TI	GESTION TI
14	Falta de una Política de Gestión del Conocimiento para la Secretaría de las TIC, Ciencia e Innovación	GESTION TI
15	Brecha en comunicaciones del área de TI hacia sus partes interesadas.	GESTION TI
16	Falta de un plan para apalancar oportunidades y dinámicas con los actores del ecosistema digital del distrito, la región y el país.	GESTION TI

4.2. PARTES INTERESADAS

Se mantienen contactos apropiados con grupos de interés especial

A. Partes Interesadas, Procesos internos de apoyo y empleados	
Proceso	**Expectativas**
ALTA DIRECCIÓN	* Protección a los activos de información de acuerdo a la clasificación y valoración de la misma. * Poder integrar y hacer parte activa del tratamiento de riesgos de seguridad de la información sobre sus activos. * Tener apoyo en la definición de procesos que garanticen la protección de los activos de información general de la Alcaldía desde el punto de vista de los empleados, teniendo en cuenta que el eslabón más débil de la cadena de seguridad es el usuario. * Generar conciencia dentro de la Alcaldía, de la importancia de la seguridad de la información en el desarrollo normal de las actividades diarias y el impacto generado cuando no se siguen lineamientos al respecto.
DIRECTORES Y LÍDERES DE TI	
SECRETARIOS DE DESPACHO	
EMPLEADOS	* Contar con los lineamientos y directrices que permitan no solo asegurar la seguridad de la información de la Alcaldía, sino también entender conceptos orientados a la seguridad de la información propia. * Entender y poner en práctica la importancia de la seguridad de la información en el desarrollo normal de las actividades diarias y el impacto generado cuando no se siguen lineamientos al respecto.
B. Partes Interesadas, externas	
CIUDADANIA Y COMUNIDAD EN GENERAL	Servicios ciudadanos en línea oportunos, fáciles de utilizar y con una respuesta positiva de sus solicitudes
CIUDADANOS USUARIOS ESPACIOS DIGITALES	Oferta oportuna de servicios de TI y capacitaciones relevantes para mejorar las competencias digitales de los ciudadanos.
GREMIOS EMPRESARIALES	Entrega de Información pública confiable que permita tomar decisiones objetivas para su gestión empresarial
PROVEEDORES DE TI	Procesos contractuales transparentes en igualdad de oportunidades para la oferta de soluciones de TI
MEDIO AMBIENTE	Cumplimiento de la Normatividad Ambiental con respecto al tratamiento y disposición final de los residuos electrónicos generados por el municipio
C. Partes Interesadas, Entidades regulatorias	
Entidad	**Expectativas**
Departamento Nacional de Planeación	Asociado a la ejecución de los recursos públicos en tiempos previstos (Rubros destinados para Seguridad de la Información).
MinTIC	Ente que promueve el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo

	social, económico y político de la Nación, en tal sentido podría requerir cumplimiento de lineamientos que tienen estipulados.
DIAN	Requiere el cumplimiento a nivel de legalidad de software.
Superintendencia de Industria y comercio	Vigila y requiere cumplimiento de Habeas Data y registro de Bases de datos RNBD.
Contraloría General de la República	es el máximo órgano de control fiscal del Estado. Como tal, tiene la misión de procurar el buen uso de los recursos y bienes públicos y contribuir a la modernización del Estado, mediante acciones de mejoramiento continuo en las distintas entidades públicas..
Departamento Administrativo de la Función Pública	Apoyo en el diseño y adopción de documentos en los que se establecen las directrices para la implementación de las políticas públicas en materia de Control Interno, Racionalización de Trámites, Calidad, Empleo Público y Desarrollo Organizacional.

D. Contacto Autoridades y Gremios			
Autoridad	**País /Ciudad**	**Describa la forma que interactúa con la autoridad**	**Contacto**
MINTIC	Colombia	Diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector tecnologías de la información y las comunicaciones en Colombia.	www.mintic.gov.co
Policía Nacional	Colombia	Es un apoyo general ya que tiene como función enfrentar grupos delictivos transnacionales organizados, grupos terroristas, que se dedican al tráfico de drogas ilícitas, blanqueo de dinero, tráfico ilícito de armas, trata de personas, entre otros.	112

4.3. DETERMINACIÓN DEL ALCANCE DEL MSPI

Todos los usuarios de los servicios de las tecnologías de la información y las comunicaciones, deberán atender de manera obligatoria los parámetros para el buen uso del equipo de los recursos tecnológicos y activos de información de la Entidad que se describen en el catálogo de servicios TI, así como a los designados para su uso y custodia.

4.4. REQUISITOS LEGALES Y OTROS REQUISITOS

ISO 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la Seguridad de la Información utilizable por cualquier tipo de organización. Entre las distintas normas que componen la serie ISO 27000 y que fueron tomadas como referente, se resalta ISO/IEC 27001 sobre los requisitos para el establecimiento del sistema de gestión de Seguridad de la Información.

Se definen las siguientes referencias normativas:

- ✓ Ley 1266 de 2008 "Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información".
- ✓ Ley 1273 de 2009 "Protección de la Información y de los Datos".
- ✓ Documento CONPES 3701 de julio del 2011 "Lineamientos de política para ciberseguridad y ciberdefensa".
- ✓ Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" y su decreto reglamentario 1377 del 27 de junio de 2013.
- ✓ Decreto 2573 de 2014 por medio del cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.
- ✓ Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la Republica de Colombia.
- ✓ Resolución No. 03049 del 24 de agosto de 2012, por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información.
- ✓ Norma Técnica Colombiana NTC – ISO/IEC 27000
- ✓ Decreto 1078 de 2015
- ✓ Política de Gobierno Digital.

5. LIDERAZGO

5.1. COMPROMISO DE LA ALTA DIRECCIÓN

El Alcalde Distrital aprueba la política general de seguridad de la información como muestra de su compromiso y apoyo a las actividades de diseño, implementación, mantenimiento y mejora continua de políticas y lineamientos consecuentemente orientados a la salvaguardar la Confidencialidad, Integridad y Disponibilidad de la información de la Entidad.

Su compromiso se demostrará a través de:

- ✓ Presidir el Comité de Seguridad y Privacidad de la información
- ✓ Revisar y aprobar de políticas y lineamientos de seguridad de la información.
- ✓ Promover de una cultura de seguridad y protección de la información.
- ✓ El apoyo para la divulgación de los propósitos y lineamientos de seguridad de la información a los servidores públicos y partes interesadas.
- ✓ Asignar recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información.
- ✓ Realizar actividades de verificación y evaluación del desempeño del sistema de gestión de seguridad de la información de manera periódica

5.2. ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.2.1. Secretario (a) de las Tecnologías de la Información y las Comunicaciones, Ciencia e Innovación

En su calidad de tal, responde ante el Alcalde Distrital por la existencia y cumplimiento legal y de las medidas que mantengan un nivel de seguridad de la información acorde con las necesidades de la Entidad y los recursos disponibles.

Responsabilidades

- ✓ Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de Seguridad de la Información.
- ✓ Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de Seguridad de la Información.
- ✓ Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de Seguridad de la Información.
- ✓ Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
- ✓ Definir e implementar la estrategia de concienciación y capacitación en Seguridad de la Información para los funcionarios, contratistas y demás terceros, cuando aplique.
- ✓ Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
- ✓ Gestionar la plataforma tecnológica que soporta los procesos de la entidad.
- ✓ Definir, mantener y controlar la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software base y de aplicaciones.
- ✓ Gestionar la adquisición de software y hardware.
- ✓ Asignar los equipos de cómputo a los funcionarios y/o contratistas.

5.2.2. Oficial de Seguridad de la Información

- ✓ Es el responsable de definir, gestionar y difundir al interior de Alcaldía Distrital de Barrancabermeja el Modelo de Seguridad y Privacidad de la Información.
- ✓ Es el responsable de velar por el cumplimiento y actualización de la política general de seguridad y privacidad de la información y sus políticas específicas.
- ✓ Debe velar por la implementación de controles de seguridad.

- ✓ Debe analizar periódicamente los niveles de riesgo existente y proponer soluciones que fortalezcan la seguridad y privacidad de la información en la Entidad.
- ✓ Debe gestionar los incidentes de seguridad y recomendar acciones preventivas y correctivas para evitar afectaciones al interior de la Entidad.
- ✓ Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.
- ✓ Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad
- ✓ Establecer, documentar y dar mantenimiento a los procedimientos de Seguridad de la Información que apliquen para la plataforma de tecnologías de información administrada por esta oficina.

5.2.3. Secretario (a) General

Incluir en los programas de inducción y de re-inducción el tema de seguridad de la información asegurando que los funcionarios conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información o de otros recursos informáticos, haciendo énfasis en las consecuencias jurídicas que puede acarrear al servidor público

5.2.4. Jefe de Oficina de Control Interno

Validar la aplicación y cumplimiento de las políticas de Seguridad de la Información definidas en esta Directiva, la aplicación de controles sobre los activos de información y los requerimientos del Sistema de Gestión de Seguridad de la Información.

5.2.5. Dueños de los procesos en cada sectorial

Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados con sus procesos, incluyendo aquellas actividades que sean consideradas como controles de Seguridad de la Información dentro de dichos procedimientos.

5.2.6. Propietarios de los Activos de Información

- ✓ Los funcionarios y contratistas son responsables de la calidad de la información ingresada en los diferentes sistemas de información usados en la Entidad, para lo cual deben alimentar los datos que son editables en forma íntegra y veraz.
- ✓ Comunicar sus requerimientos de seguridad de información oficial de Seguridad de la Información de la Secretaría de las TIC, Ciencia e Innovación
- ✓ Determinar y autorizar todos los privilegios de acceso a sus activos de información.
- ✓ Comunicar al Área de Seguridad de la Información sus requerimientos en capacitación sobre temas de seguridad.

- ✓ Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.

5.2.7. Funcionarios, contratistas y terceros

- ✓ Cumplir con las políticas de Seguridad y privacidad de la Información, contempladas en la presente Directiva.
- ✓ Velar por el cumplimiento de las políticas de Seguridad de la Información dentro de su entorno laboral inmediato.
- ✓ Reportar de manera inmediata y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de Seguridad de la Información.
- ✓ Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos que lo vinculan.
- ✓ Utilizar únicamente software y demás recursos tecnológicos autorizados.

5.2.8. Comité de seguridad y privacidad de la información

El Comité de Seguridad y privacidad de la Información, es creado mediante acto administrativo y el cual tiene dentro de sus funciones son: definir y aprobar las directrices, políticas y mecanismos de control y seguimiento de la Información de la Entidad de conformidad con el marco normativo vigente

El comité está integrado por:

1. Alcalde Distrital
2. Secretario (a) General
3. Secretario de las TIC, Ciencia e Innovación
4. Secretario de Planeación
5. Jefe de la Oficina Asesora Jurídica
6. Jefe Control Interno Administrativo
7. Jefe de Prensa

Funciones del Comité de Seguridad y privacidad de la Información

- ✓ Promover la mejora continua del Sistema de Gestión de Seguridad de la Información SGSI de la Alcaldía Distrital de Barrancabermeja
- ✓ Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información.
- ✓ Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información para la Alcaldía Distrital de Barrancabermeja
- ✓ Adoptar las medidas y acciones a que haya lugar, de conformidad con los resultados de los diagnósticos del estado de la seguridad de la

información para la Alcaldía Distrital de Barrancabermeja, con el fin de tomar y establecer las medidas necesarias.

- ✓ Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual que puedan generar pérdidas patrimoniales o afectar los recursos de información de la entidad.
- ✓ Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información
- ✓ Revisar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.
- ✓ Recomendar la investigación de los incidentes de seguridad de la información ante las instancias necesarias cuando haya lugar a ello.
- ✓ Evaluar los planes de acción para mitigar y/o eliminar riesgos en seguridad de la información.
- ✓ Alinear sus acciones y decisiones a la normatividad vigente en materia de tecnologías y seguridad de la información.
- ✓ Las demás funciones inherentes a la naturaleza del Comité.

Funciones del Secretario Técnico

- ✓ Convocar a los integrantes del Comité a las sesiones ordinarias y extraordinarias.
- ✓ Elaborar las actas de reunión del Comité oportunamente.
- ✓ Enviar la agenda a los miembros del Comité oportunamente.
- ✓ Llevar y custodiar el archivo de las actas y demás documentos soporte del Comité.
- ✓ Verificar el quórum al inicio de las sesiones.
- ✓ Recibir y preparar la respuesta a los documentos que sean de competencia del Comité.
- ✓ Firmar las actas que hayan sido aprobadas.
- ✓ Realizar seguimiento a los compromisos y tareas pendientes del Comité.
- ✓ Las demás que le sean asignadas por el Comité

6. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Alcaldía Distrital de Barrancabermeja, considera la información como un activo fundamental para la gestión administrativa y para la prestación de los servicios a los ciudadanos; por lo cual asigna un compromiso expreso a la protección y privacidad de los activos de información más significativos como parte de una estrategia orientada por la administración de riesgos y la consolidación de una cultura de seguridad y privacidad de la información en pro de generar y mantener la confianza de sus ciudadanos, usuarios, funcionarios, contratistas y terceros que se benefician directa e indirectamente con los servicios prestados por la Alcaldía.

Consciente de las necesidades actuales y apoyados en la innovación tecnológica como mecanismo para mejorar la seguridad y privacidad de la información, la Alcaldía Distrital de Barrancabermeja implementa un modelo de gestión de seguridad y privacidad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se exponen la información, ayudar a la reducción de costos operativos y financieros, establecer una cultura de seguridad y garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios, recursos de procesamiento de la información y cualquier otro activo de información de la Alcaldía Distrital de Barrancabermeja, deberán adoptar los lineamientos contenidos en el presente documento y en los demás relacionados, con el fin de mantener la confidencialidad, la integridad y disponibilidad de la información.

La política global de seguridad de la información de la Alcaldía Distrital de Barrancabermeja se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la Alcaldía. Adicionalmente, se establecerán políticas, directrices o lineamientos de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control de la norma internacional ISO/IEC 27001:2013, u otro marco de referencia que se adopte

Ante la evidencia del incumplimiento de la Política de seguridad y privacidad de la información, de las contenidas en los documentos de seguridad y privacidad de la información o cualquier otra violación de la seguridad por parte de algún funcionario, contratista o tercero, se iniciará en contra de estos las respectivas investigaciones disciplinarias y multas a que haya lugar, de acuerdo con los procedimientos internos de la institución y normatividad referente a la seguridad de la información, privacidad y confidencialidad.

Esta política deberá ser revisada de manera periódica (por lo menos una vez al año, cuando se adicione un nuevo servicio TIC o se identifiquen cambios en el contexto interno o externo en la institución) por el Comité de Gestión y Desempeño de la Alcaldía y cuando se requiera alguna información o aclaración sobre la política respectiva, será solicitada al Oficial de seguridad de la información.

6.2. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la Alcaldía Distrital de Barrancabermeja sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones y el DATA CENTER de la Administración DISTRITAL.

6.2.1. Controles de acceso físico

- Cualquier persona que tenga acceso a las instalaciones de la Alcaldía Distrital de Barrancabermeja, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la Alcaldía Distrital de Barrancabermeja, dichos equipos podrán ser retirados el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.
- Todo equipo de cómputo, módems y cualquier activo de tecnología de información y comunicaciones de propiedad de la Alcaldía Distrital de Barrancabermeja, podrán salir de las instalaciones únicamente con la autorización debidamente firmada por el Secretario de Despacho o jefe de la dependencia de donde saldrá dicho equipo.

6.2.2. Seguridad en áreas de trabajo protegidas y restringidas

- El Centro de Datos de la Alcaldía Distrital de Barrancabermeja es área restringida, por lo que sólo el personal autorizado por la Secretaría de las TIC, Ciencia e Innovación puede acceder a él.
- Las áreas protegidas y el Centro de Datos se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por la Secretaría de las TIC, Ciencia e Innovación, a fin de permitir el acceso solo a personal autorizado.
- Para la selección de las áreas protegidas y la ubicación del Centro de Datos se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad de las instalaciones.
- Las plataformas tecnológicas serán ubicadas y protegidas de tal manera que reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado. El cableado de datos que se incluya en cualquier proyecto en las instalaciones de la Entidad debe ser categoría 7A.
- El cableado de energía eléctrica y comunicaciones que transportan datos o brindan apoyo a los servicios de información estarán protegidos contra intercepción o daños. Se deberá garantizar la seguridad física del Centro de Datos, incluyendo entre otros los siguientes subsistemas:
    - Sistema Eléctrico suplementario
    - Sistema de Control de Acceso
    - Sistema de protección contra incendios
- En las áreas donde se encuentren activos informáticos de misión

crítica, se debe cumplir como mínimo con los siguientes lineamientos:

- No se deben consumir alimentos ni bebidas.
- No se deben ingresar elementos inflamables.
- No se debe permitir el acceso de personal ajeno sin que este acompañado por un funcionario durante el tiempo que dure su visita.
- No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
- No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
- No se permite el ingreso de equipos electrónicos, así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

- Las áreas protegidas deben contar con las condiciones ambientales que garanticen la correcta operación de los equipos y el estado de los medios que contienen información, así como un sistema de detección y control de incendios.
- La Secretaría de las TIC, Ciencia e Innovación podrá implementar servicios privados en la nube, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.

6.2.3. Protección y ubicación de los equipos dentro de las instalaciones

- Los usuarios no deben reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Secretaría de las TIC, Ciencia e Innovación, en caso de requerir este servicio deberá solicitarlo.
- El área de almacén será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen.
- El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones desempeñadas por los funcionarios en la Alcaldía Distrital de Barrancabermeja
- Los funcionarios velarán por el uso adecuado de los equipos de escritorio, portátiles y móviles que les hayan sido asignados, por lo tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU.

- Se debe mantener el equipo informático en un entorno limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos.
- Queda prohibido que el usuario manipule técnicamente los equipos de cómputo.
- Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes.
- Los equipos portátiles deberán estar asegurados con la guaya o el mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones de la Entidad.

6.2.4. Seguridad de los equipos fuera de las instalaciones

- Los usuarios que requieran usar los equipos fuera de las instalaciones de la Alcaldía Distrital de Barrancabermeja deben velar por la protección de los mismos sin dejarlos desatendidos en lugares públicos o privados en los que se puedan ver comprometidos la imagen o información del sector.
- En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información sensible relacionada con la Entidad, se deberá realizar inmediatamente el respectivo reporte de acuerdo con el procedimiento Gestión de Incidentes de Seguridad y se deberá poner la denuncia ante la autoridad competente, si aplica.
- Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones de la Alcaldía Distrital de Barrancabermeja deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieren o puedan poner en riesgo la información que contiene.

6.2.5. Uso de medios de almacenamiento

- Se encuentra restringida la conexión no autorizada a la infraestructura tecnológica de la Alcaldía Distrital de Barrancabermeja, de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales.
- Toda solicitud para utilizar un medio de almacenamiento de información compartido (File Share), deberá contar con la autorización de la Secretaría de las TIC, Ciencia e Innovación.
- Los medios de almacenamiento removibles como cintas, discos duros removibles, CDs, DVDs, medios impresos y dispositivos USB, entre

otros, que contengan información institucional, y hayan sido autorizados deben ser controlados y físicamente protegidos.

- Los usuarios deberán hacer una copia de seguridad diariamente de la información sensitiva y crítica que se encuentre en sus computadores personales o estaciones de trabajo.
- En caso de que por el volumen de información se requiera alguna copia en CD o DVD, este servicio deberá solicitarse por escrito al Secretaría de las TIC, Ciencia e Innovación.
- Los usuarios deberán almacenar toda la información en la segunda partición que tiene su equipo (si no tiene particionada el disco duro, Secretaría de las TIC, Ciencia e Innovación la partición del disco) a través de la plataforma de MESA DE AYUDA TIC
- Las actividades que realicen los usuarios en la infraestructura Informática y de Comunicaciones de la ALCALDÍA DISTRITAL DE BARRANCABERMEJA son registradas y susceptibles de auditoria.
- La Entidad definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas por Secretaría de las TIC, Ciencia e Innovación, en la plataforma tecnológica si es requerido para el cumplimiento de sus funciones.
- Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene. Para los procesos de baja, reutilización o garantías de los dispositivos que contengan medios de almacenamiento, se debe cumplir según sea el caso con la destrucción física del mismo o borrado seguro.
- El tránsito o préstamo de medios removibles deberá ser autorizado por el propietario del activo de información.

6.2.6. Mantenimiento de equipo

- Únicamente el personal autorizado por la Secretaría de las TIC, Ciencia e Innovación, podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.
- Los usuarios deberán asegurarse de realizar una copia de seguridad de la información en la Nube que consideren relevante cuando el equipo sea enviado a mantenimiento, si es mucha información se debe hacer la solicitud formal a través de la mesa de ayuda de TIC y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de mantenimiento.

6.2.7. Pérdida de equipo

- El usuario que tenga asignado algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo con la normatividad vigente, en los casos de robo, extravío o pérdida de este.
- La asignación de los computadores portátiles tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

- El usuario deberá dar aviso inmediato a la Secretaría de las TIC, Ciencia e Innovación, y Almacén de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su custodia.

6.2.8. Uso de dispositivos externos removibles

- El uso de las unidades grabadoras de discos compactos (unidades quemadoras de CD´s o DVD´s) es exclusivo para copias de seguridad de información institucional que por su volumen así lo justifiquen.
- La asignación de este tipo de equipos (unidades externas para Backup) será previa justificación por escrito y autorización del Secretario de Despacho y/o jefe del Área correspondiente.
- El usuario que tenga asignado este tipo de dispositivos será responsable del buen uso que se le dé.
- Queda prohibido el uso de módems externos en los computadores de escritorio.
- Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el Secretario de Despacho y/o Jefe del Área correspondiente.

6.2.9. Daño del equipo

- El equipo de cómputo o cualquier recurso de tecnología de información que sufra algún daño por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal la Secretaría de las TIC, Ciencia e Innovación. determinará la causa de dicho daño.

6.3. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN

- Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura tecnológica de la Alcaldía Distrital de Barrancabermeja
- De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de la Alcaldía Distrital de Barrancabermeja o hacia redes externas como Internet.
- Los usuarios de la Alcaldía Distrital de Barrancabermeja que hagan uso de equipos de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus informáticos: virus tipo gusano informático, virus tipo Caballo de Troya o “troyanos”, virus residentes en el sector de arranque y en las librerías del Sistema Operativo Windows y virus de sobreescritura que lo que hacen es sobrescribir en el interior de los archivos atacados haciendo que se pierda el contenido de las carpetas y archivos.

6.3.1. Clasificación de la Información

- Toda información al interior de la Alcaldía Distrital de Barrancabermeja deberá recibir el nivel de clasificación apropiado de acuerdo con las necesidades de protección de la mismo y a los riesgos potenciales asociados
- Toda Información clasificada deberá recibir el sistema de etiquetado con la identificación del nivel de clasificación asignado.

6.3.2. Resguardo y protección de la información

- El usuario deberá reportar de forma inmediata a la Secretaría de las TIC, Ciencia e Innovación, cuando detecte que existan eventos, incidentes o riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.
- El usuario tiene la obligación de proteger los discos, memorias, cintas magnéticas, CD-ROM y DVD que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.
- Es responsabilidad del usuario evitar en todo momento la fuga de la información de la Alcaldía Distrital de Barrancabermeja, que se encuentre almacenada en los equipos de cómputo asignados.
- En ningún caso se otorgará acceso a terceros a la información sensible, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.

6.3.3. Acuerdos de Confidencialidad

Todos los funcionarios, contratistas y demás terceros deben firmar la cláusula y/o acuerdo de confidencialidad y este deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada, de acuerdo al formato de confidencialidad. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o entidades externas.

6.3.4. Instalación de software

- Los usuarios que requieran la instalación de software que no sea propiedad de la Alcaldía Distrital de Barrancabermeja, deberán justificar su uso y solicitar su autorización al secretario de su área que lo haga a través de la plataforma de MESA DE AYUDA TIC indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación.
- Será considerado como un ataque a la seguridad informática el que los usuarios instalen cualquier tipo de programa (software) en sus computadores, estaciones de trabajo, servidores, o cualquier equipo

conectado a la red de la Alcaldía Distrital de Barrancabermeja, que no esté autorizado por el secretario de las TIC, Ciencia e Innovación

6.3.5. Gestión de Incidentes de Seguridad de la Información

- El usuario que sospeche o tenga conocimiento de la ocurrencia de un evento o incidente de seguridad informática deberá reportarlo al correo electrónico seguridaddigital@barrancabermeja.gov.co Secretaría de las TIC, Ciencia e Innovación lo antes posible, indicando claramente los datos por los cuales lo considera un evento o incidente de seguridad informática, adjuntando las evidencias con las que cuente y la mayor información posible acerca del mismo (fecha y hora de la ocurrencia, sistema, usuario, entre otros).
- Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de los Secretarios de Despacho y/o Jefes de área competentes, el usuario informático deberá notificar esta situación al Jefe del Área respectiva.
- Cualquier incidente generado durante la utilización u operación de los activos de Tecnología de la Información y las Comunicaciones de la Alcaldía Distrital de Barrancabermeja debe ser reportado a la Secretaría de las TIC, Ciencia e Innovación por los canales oficiales.
- Los funcionarios y contratistas de la Entidad deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la Confidencialidad, Integridad y Disponibilidad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.
- Para gestionar los incidentes de Seguridad y privacidad de la Información deberá existir como mínimo un funcionario con conocimientos en el manejo de incidentes en las áreas de Seguridad de la Información.
- Para los casos en que los incidentes reportados requieran judicialización se deberá coordinar con los organismos que cuentan con función de policía judicial.
- Se debe establecer y mantener actualizado un directorio de los funcionarios involucrados dentro del procedimiento de Gestión de Incidentes de Seguridad de la Información para la Entidad.
- Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.
- Las Áreas de Seguridad de la Información deben propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de Seguridad de la Información
- Los resultados de las investigaciones que involucren a los funcionarios de la Entidad deberán ser informados a las áreas de competencia.
- La Entidad deberá establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de Seguridad de la Información.

6.3.6. Administración de la configuración

- Los usuarios de las áreas de la Alcaldía Distrital de Barrancabermeja no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la Alcaldía Distrital de Barrancabermeja, sin la autorización de la Secretaría de las TIC, Ciencia e Innovación.
- Los equipos externos a la Alcaldía Distrital de Barrancabermeja que necesiten conectarse a la red deberán informar a la Secretaría de las TIC, Ciencia e Innovación para su debida autorización.

6.3.7. Seguridad para la red

- Será considerado como un ataque a la seguridad informática, cualquier actividad no autorizada por la Secretaría de las TIC, Ciencia e Innovación, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la Alcaldía Distrital de Barrancabermeja, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

6.3.8. Uso del correo institucional

- El único medio oficial de comunicación por correo es a través de Correos Institucionales en el dominio @barrancabermeja.gov.co por lo tanto está PROHIBIDO por parte de funcionarios públicos o contratistas gestores de correos de procesos de la Alcaldía Distrital de Barrancabermeja, utilicen o creen correos electrónicos que no sean INSTITUCIONALES en plataformas comerciales como gmail.com, hotmail.com, yahoo.com, entre otros para comunicación con la comunidad o para temas propios de su cargo.
- Alcaldía Distrital de Barrancabermeja asignará buzones de correo instituciona a sus servidores públicos y a procesos específicos que sean requeridos para comunicación con la comunidad, sin embargo, será prohibido asignar cuentas a terceros o contratistas.
- Los usuarios no deben usar cuentas de correo electrónico institucionales asignados a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la Alcaldía Distrital de Barrancabermeja, a menos que cuente con la autorización del Secretario de Despacho y/o jefe del área correspondiente.
- Los usuarios deben tratar los mensajes de correo electrónico institucional y archivos adjuntos como información de propiedad de la Alcaldía Distrital de Barrancabermeja. Los mensajes de correo electrónico institucional deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- Los usuarios podrán enviar información reservada y/o confidencial vía

correo electrónico siempre y cuando vayan de manera encriptada y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

- La Alcaldía Distrital de Barrancabermeja, se reserva el derecho a acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violado políticas de Seguridad Informática o realizado acciones no autorizadas.
- El usuario debe utilizar el correo electrónico de la Alcaldía Distrital de Barrancabermeja única y exclusivamente a los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso.
- La cuenta de correo institucional no debe ser inscrita en páginas o sitios publicitarios, de compras u otros
- El tamaño de los archivos adjuntos en el correo electrónico no debe superior a 10 Megas, de ser necesario el envío de un archivo de mayor tamaño, se debe utilizar el recurso de carpetas compartidas en la nube. En caso de requerirse una cuenta INSTITUCIONAL personalizada para algún proceso de soporte xxxxx@barrancabermeja.gov.co o la asignación de una cuenta de correo institucional a algún Contratista con orden de Prestación de Servicio que esté apoyando un proceso crítico, el proceso de solicitud es el siguiente:
  1. El SUPERVISOR DEL CONTRATO, el SECRETARIO O JEFE DE OFICINA deberá hacer la solicitud del dicho correo institucional a través del formulario creado para tal fin.
  2. Realizar la solicitud no garantiza la asignación inmediata del correo puesto que depende de las disponibilidades técnicas de LICENCIAS.
- Está PROHIBIDO por utilizar LISTAS MASIVAS DE DIFUSIÓN internas a la Administración Distrital y mucho menos Externas hacia la comunidad dado que este comportamiento podría incluirnos en listas negras de spammers. Lo únicos autorizados para difundir internamente comunicación oficial a través de listados masivos son los Secretarios De Despacho o Jefes De Oficinas Asesoras.
- En caso de requerirse utilizar una LISTA MASIVA DE DISTRIBUCIÓN a correos institucionales por parte del SECRETARIO DE DESPACHO o JEFE DE OFICINA ASESORA, el nombre de dicha lista DEBERÁ ir en el campo CCO o correo oculto para evitar respuestas masivas de los destinatarios y para cuidar la confidencialidad de dichas listas.
- No se deberán realizar el envío o distribución de información catalogada como confidencial, interna o privada dentro o fuera del Distrito de Barrancabermeja (sin la autorización correspondiente).
- No se podrá hacer uso de lenguaje ofensivo, inapropiado o con declaraciones de blasfemia, obscenidad, ilegales, incitadores a infringir la ley, hostigamiento basado en sexo, raza, nacionalidad, contenido despectivo o difamatorio en cualquier mensaje electrónico para con sus compañeros, clientes, proveedores u otros; su uso inadecuado, se

considerará fuera del alcance y responsabilidad la Alcaldía Distrital de Barrancabermeja y por lo tanto, los daños y perjuicios que pueda llegar a causar, serán de completa responsabilidad de la propietario de la cuenta de correo electrónico que la haya generado.

- Está prohibido utilizar el correo electrónico para el intercambio de información o de software que violen las leyes de derechos de autor.
- Es responsabilidad de los usuarios de correo electrónico hacer mantenimiento a su buzón de correo: eliminar mensajes de la bandeja de entrada, archivar mensajes, eliminar definitivamente los mensajes de la bandeja elementos eliminados.
- No se considera aceptado el uso del correo electrónico de la entidad para los siguientes fines:

    - Falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico institucional.
    - Interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas institucionales.
    - Enviar o retransmitir cadenas de correo, mensajes con contenido racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.
    - Enviar mensajes no autorizados con contenido religioso o político.
    - El envío de archivos adjuntos con extensiones como .mp3, .wav, .exe, .com, .dll, .bat, .msi o cualquier otro archivo que ponga en riesgo la Seguridad de la Información; en caso de que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por la Secretaría de las TIC, Ciencia e Innovación

- No debe concederse cuentas de correo electrónico a personas que no tengan vínculos laborales con la entidad a menos, de que estén debidamente autorizados por el Despacho Alcalde, en cuyo caso la cuenta no debe estar activa tiempo finito
- El envío masivo de mensajes corporativos deberá ser solicitado por el secretario o jefe del área que lo requiere y debe contar con la aprobación de la respectiva Secretaría de las TIC, Ciencia e Innovación
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido y deben conservar, en todos los casos, el mensaje legal institucional de confidencialidad. Por lo tanto No se permite la utilización de fondos de ninguna clase (color, motivo o dibujo), el formato de la firma es el definido por la Jefatura de Prensa, Protocolo y comunicaciones
- Todo correo electrónico deberá tener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos:
  El mensaje (incluyendo cualquier anexo) contiene información

confidencial y se encuentra protegido por la Ley. El mensaje sólo puede ser utilizado por la persona o empresa a la cual está dirigido. En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata. Se prohibe la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

6.3.9. Controles contra código malicioso

- La Alcaldía Distrital de Barrancabermeja otorga antivirus para todos sus equipos de cómputo con la finalidad de mantenerlos asegurados.
- Para prevenir infecciones por virus informático, los usuarios de la Alcaldía Distrital de Barrancabermeja no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Secretaría de las TIC, Ciencia e Innovación
- Los usuarios de la Alcaldía Distrital de Barrancabermeja deben verificar que la información y los medios de almacenamiento, considerando al menos discos, memorias, CD's, DVD's, cintas y cartuchos, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la Alcaldía Distrital de Barrancabermeja.
- Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y Seguridad de la Información deberán estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos dados por código malicioso.
- Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de la Secretaría de las TIC, Ciencia e Innovación, y deberán ser actualizados permanentemente.
- No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional todos los archivos de computador que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.
- Ningún usuario de la Alcaldía Distrital de Barrancabermeja debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computador diseñado para auto replicarse, dañar, o en otros casos impedir el funcionamiento de cualquier memoria de computador, archivos de sistema, o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas de la Alcaldía Distrital de Barrancabermeja. El incumplimiento de este estándar será considerado como una falta grave.
- Ningún usuario, empleado o personal externo, debe bajar o descargar

software de sistemas, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización por Secretaría de las TIC, Ciencia e Innovación

- Cualquier usuario que sospeche de alguna infección por virus de computador, deberá dejar de usar inmediatamente el equipo, desconectarlo de la red, apagarlo y reportarlo a la Secretaría de las TIC, Ciencia e Innovación de inmediato.
- Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la Alcaldía Distrital de Barrancabermeja en: Antivirus, Outlook, Office, Navegadores u otros programas.
- Debido a que algunos virus son extremadamente complejos, ningún usuario de la Alcaldía Distrital de Barrancabermeja debe intentar erradicarlos de los computadores.

6.3.10. Internet

- Internet es una herramienta de trabajo que permite navegar en sitios relacionados o no con las actividades diarias, por lo cual el uso adecuado de este recurso se controla, verifica y monitorea, considerando para todos los casos, las siguientes políticas:
- La navegación en Internet estará controlada de acuerdo con las restricciones de navegación definidas para los usuarios; sin embargo, en ningún caso se considerarán aceptables los siguientes usos:

    - Navegación en sitio de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.
    - Publicación, envío o adquisición de material sexualmente explícito, discriminatorio, que implique un delito informático o de cualquier otro contenido que se considere fuera de los límites permitidos.
    - Publicación o envío de información confidencial sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.
    - Utilización de otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados por la Secretaría de las TIC, Ciencia e Innovación.
    - Publicación de anuncios comerciales o material publicitario, salvo la oficina de prensa y Comunicaciones cuando lo requiera. Estas solicitudes, deben ser justificadas por el jefe de la oficina de Prensa y Comunicaciones y avaladas por el despacho del Alcalde.
    - Promover o mantener asuntos o negocios personales.
    - Descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.
    - Navegación en las cuentas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación por parte de la Entidad.

  - Uso de herramientas de mensajería instantánea no autorizadas por la Secretaría de las TIC, Ciencia e Innovación
  - Emplear cuentas de correo externas no corporativas para el envío o recepción de información institucional.
- El acceso a Internet provisto a los usuarios de la Alcaldía Distrital de Barrancabermeja es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.
- Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la Alcaldía Distrital de Barrancabermeja, en caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada por la Secretaría de las TIC, Ciencia e Innovación
- Los usuarios de Internet de la Alcaldía Distrital de Barrancabermeja, están en la obligación de reportar todos los incidentes de seguridad informática a la Secretaría de las TIC, Ciencia e Innovación inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática al correo electrónico seguridaddigital@barrancabermeja.gov.co.
- El acceso y uso de módems en la Alcaldía Distrital de Barrancabermeja tiene que ser previamente justificado por el secretario de despacho y autorizado por Secretaría de las TIC, Ciencia e Innovación
- Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

  - Serán sujetos de monitoreo de las actividades que realizan en internet.
  - Existe la prohibición al acceso de páginas no autorizadas.
  - Existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
  - Existe la prohibición de descargar software sin la autorización de la Secretaría de las TIC, Ciencia e Innovación
  - La utilización de Internet es para el desempeño de su función y puesto en la Alcaldía Distrital de Barrancabermeja y no para propósitos personales.

6.3.11. Aplicaciones de mensajería instantánea (MI)

- Está prohibido utilizar la aplicación móvil gratuita WhatsApp para gestión de las comunicaciones en las diferentes dependencias de la Alcaldía Distrital de Barrancabermeja que incluyan compartir activos de información de carácter reservado o confidencial.
- Con el fin de no perder las bondades de comunicación inmediata de las aplicaciones de MI al interior de la Alcaldía Distrital de Barrancabermeja, pero cuidar los aspectos de confidencialidad de la información compartida a través de las mismas, la Secretaría de las TIC, Ciencia e Innovación recomienda implementar la herramienta de

MI llamada SIGNAL https://signal.org/install

- Las comunicaciones que se sostienen por los GRUPOS INSTITUCIONALES a través de aplicaciones de MI **GRUPINAMI** y todos los grupos que tengan un carácter MISIONAL E INSTITUCIONAL dentro de la Alcaldía Distrital de Barrancabermeja están restringidos a asuntos netamente INSTITUCIONALES, no debe emplearse para asuntos personales como (envío de memes, oraciones, conversaciones privadas, desarrollo de actividades políticas, religiosas, comerciales o de entretenimiento o para el envío de mensajes irrelevantes, vulgares u obscenos)
- Todos los funcionarios, asesores o colaboradores externos que pertenezcan a GRUPINAMI de la Alcaldía Distrital de Barrancabermeja, deberán mantener un adecuado, ético y responsable uso de este recurso, cuidando no dañar la imagen y reputación de la Alcaldía Distrital.
- Los funcionarios, asesores o colaboradores externos que pertenezcan a GRUPINAMI de la Alcaldía Distrital de Barrancabermeja, no tienen derecho a violar la confidencialidad con relación a cualquier información o mensaje creado, recibido o enviado a través de este medio. Una práctica que a veces se usa es tomar una foto instantánea a la pantalla del grupo, si esta viola aspectos de confidencialidad, no deberá ser usada esta práctica.
- Igualmente, funcionarios, asesores o colaboradores externos que cambien de número de teléfono deberán asegurarse de BORRAR TODO EL HISTORIAL de los GRUPINAMI de la Alcaldía Distrital de Barrancabermeja a los que pertenezca y retirarse de los mismos, con el fin de salvaguardar la información ahí tratada. Igualmente deberá informar al Administrador del GRUPO.
- El horario sugerido para remisión de comunicaciones a GRUPINAMI de la Alcaldía Distrital de Barrancabermeja es de lunes a viernes de 7am a 7pm y sábados de 8:00am a 2:00pm. Estos horarios podrían contravenirse solamente si se requiere enviar una comunicación de carácter PRIORITARIO por parte del administrador del grupo, o algún funcionario que requiera una ayuda urgente con alguna situación especial relacionada con la misión de la Alcaldía Distrital de Barrancabermeja.
- Los GRUPINAMI de la Alcaldía Distrital de Barrancabermeja deberán ser administrados por el secretario, asesor o Jefe de oficina, quien a su vez podrá delegar funciones de administración al funcionario que este designe con las competencias requeridas.
- Hay varios comportamientos que no son aceptables dentro de la comunicación a través de GRUPINAMI de la Alcaldía Distrital de Barrancabermeja como los siguientes y están PROHIBIDOS:

  1. Utilizar GRUPINAMI de la Alcaldía Distrital de Barrancabermeja para enviar información que no sea propia de la Entidad y que esté enmarcada dentro de la ejecución de la labor institucional.
  2. Divulgar información de carácter privado o confidencial a cargo de la Institución a usuarios fuera de la jurisdicción de la Alcaldía

Distrital o usuarios a los cuales dicha información no sea de su interés y gestión directa.
3. Realizar cualquier otra actividad o envío de comunicaciones con la intención de difamar u ofender a otro funcionario, asesor o colaborador externo.
4. Remitir mensajes, comentarios, caricaturas o chistes de carácter sexual o racial que puedan ser considerados como hostigamiento o falta de respeto hacia otros funcionarios, asesores o colaboradores externos.
5. Remitir mensajes tipo cadenas, pornografía, chistes, venta de productos o servicios, promoción a actividades religiosas o de cualquier índole, que no sean patrocinadas por la Alcaldía Distrital de Barrancabermeja
6. Remitir mensajes con contenido texto o audiovisual de índole político o religioso discriminativo.
7. Enviar videos directamente a los grupos de chat, satura los equipos de quienes reciben el mensaje; si desea remitir un video de carácter INSTITUCIONAL deberá cargado oficialmente en la NUBE INSTITUCIONAL y posteriormente compartir la URL de dicho video al GRUPINAMI.
8. Evitar el envío de videos que no se encuentren previamente cargados en una nube corporativa.
9. Mantener la cortesía con los otros miembros del GRUPINAMI.
10. Mantener los mensajes personales a otros miembros del grupo en PRIVADO y enviar al GRUPINAMI sólo aquellos mensajes que sean de interés para todos los integrantes.
11. Diseñar comunicados de forma clara, corta y concisa. No enviar mensajes largos que monopolicen el grupo con un solo tema. El procedimiento correcto es colocar un mensaje resumido con los puntos principales que se deben resaltar.
12. Las letras MAYÚSCULAS se pueden usar para enfatizar, pero NO debe escribirse todo en mayúsculas pues esto se interpreta en la red como que ¡SE ESTA GRITANDO!
13. No es conveniente llevar asuntos negativos o llamados de atención al grupo pues se generará un clima de debate improductivo. Como norma “alabanzas y felicitaciones en público. Críticas y desacuerdos en privado”.
14. Evitar los saludos, despedidas, muestras de gratitud, comentarios de aceptación, negación a título personal, que no aporten nada al grupo INSTITUCIONAL.
15. Cuidar la ortografía y gramática en las comunicaciones a través de GRUPINAMI.
16. No se debe responder CONFIRMADO a todos los mensajes, solo si se solicita por el generador del mensaje la confirmación de recibido.
17. Si se remiten mensajes de FELICITACIÓN o CONDOLENCIA por cumpleaños o fallecimientos u otra situación especial en GRUPINAMI, se sugiere que el miembro del grupo por chat PRIVADO felicite o presente la condolencia a la persona motivo de la

comunicación y no se haga por el grupo general, para evitar que la información importante se pierda.

6.4. POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y contraseña necesarios para acceder a la información y a la infraestructura tecnológica de la Alcaldía Distrital de Barrancabermeja, por lo cual deberá mantenerlo de forma confidencial.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de la Alcaldía Distrital de Barrancabermeja, debe ser proporcionado por el dueño de la información, con base en el principio de la "necesidad de saber" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

6.4.1. Controles de acceso lógico

- El acceso a la infraestructura tecnológica de la Alcaldía Distrital de Barrancabermeja para personal externo debe ser autorizado por un Secretario de Despacho y/o Jefe de oficina asesora de la Alcaldía Distrital de Barrancabermeja, quien deberá notificarlo a la Secretaría de las TIC, Ciencia e Innovación quien lo habilitará.
- Está prohibido que los usuarios utilicen la infraestructura tecnológica de la Alcaldía Distrital de Barrancabermeja para obtener acceso no autorizado a la información u otros sistemas de información de la Alcaldía Distrital de Barrancabermeja.
- Todos los usuarios de servicios de Tecnologías de la Información y las Comunicaciones son responsables por el UserID y contraseña que recibe para el uso y acceso de los recursos.
- Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Secretaría de las TIC, Ciencia e Innovación, antes de poder usar la infraestructura tecnológica de la Alcaldía Distrital de Barrancabermeja.
- Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la Alcaldía Distrital de Barrancabermeja, a menos que se tenga la autorización del propietario de la información y la Secretaría de las TIC, Ciencia e Innovación .
- Cada usuario que acceda a la infraestructura tecnológica de la Alcaldía Distrital de Barrancabermeja debe contar con un identificador de usuario (UserID) único y personalizado. Por lo cual no está permitido el uso de un mismo UserID por varios usuarios.
- Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (UserID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tienen prohibido utilizar el UserID de otros usuarios.

6.4.2. Administración de privilegios

- Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de la ALCALDÍA DISTRITAL DE BARRANCABERMEJA, deberán ser notificados el Secretaría de las TIC, Ciencia e Innovación

6.4.3. Equipo desatendido

- Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados y autorizados por el secretario TIC, Grupo funcional Área de Infraestructura Tecnológica – Operaciones TI, cuando no se encuentren en su lugar de trabajo.
- Está prohibido consumir bebidas y alimentos en el puesto de trabajo, para evitar verter líquidos que puedan causar daños en los documentos y/o equipos electrónicos y esto será responsabilidad del funcionario, contratista y/o proveedor
- Siempre que se imprima información considerada como CONFIDENCIAL, se debe: (i) retirar de inmediato de la impresora usada, (ii) destruir cualquier duplicado que se pudo haber generado por error (iii) verificar que no queden documentos CONFIDENCIALES en cola de impresión, (v) verificar que no queden documentos CONFIDENCIALES en las bandejas de las impresoras.
- El escritorio del equipo de cómputo debe permanecer libre de documentos CONFIDENCIALES.

6.4.4. Administración y uso de contraseñas

- La asignación de la contraseña debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.
- Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo a través de la plataforma de mesa de ayuda TIC para que se le proporcione una nueva contraseña y una vez que lo reciba deberá cambiarlo en el momento en que acceda nuevamente a la infraestructura tecnológica.
- La obtención o cambio de una contraseña debe hacerse de forma segura, el usuario deberá autenticarse en la plataforma de Mesa de ayuda TIC Secretaría de las TIC, Ciencia e Innovación como empleado de la Alcaldía Distrital de Barrancabermeja.
- Está prohibido que los contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.
- Sin importar las circunstancias, los contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.
- Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

- Para el acceso al directorio activo la contraseña debe estar compuesta de mínimo ocho (8) caracteres, el primer carácter debe ser una letra en mayúscula y terminar con números y al final un carácter especial y contener máximo quince caracteres (15), estos caracteres deben ser alfanuméricos.
- Deben ser difíciles de adivinar, esto implica que los contraseñas no deben relacionarse con el trabajo o la vida personal del usuario, y no deben contener caracteres que expresen listas secuenciales y caracteres de control.
- No deben ser idénticos o similares a contraseñas que hayan usado previamente.

- Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, deberá cambiarlo inmediatamente.
- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.
- Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
- Las contraseñas no deberán ser reveladas.
- Las contraseñas no se deberán escribir en ningún medio, excepto para los casos de administradores, cuando son entregadas en custodia de acuerdo con el procedimiento establecido por la Secretaría de las TIC, Ciencia e Innovación.
- Los funcionarios y contratistas deben digitar siempre su usuario y contraseña para acceder a las diferentes aplicaciones de la entidad.
- La contraseña no se debe guardar de forma automática en los inicios de sesión de las aplicaciones.
- Igualmente, al terminar la jornada deben cerrar las sesiones abiertas antes de apagar el equipo.
- Es deber de cualquier funcionario y contratista reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad. Las contraseñas por seguridad deben cambiar periódicamente.

Acciones que deben evitarse en la gestión de contraseñas seguras:

- Utilizar la misma contraseña siempre en todas las aplicaciones.
- Utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf”, las típicas en numeración: “1234” ó “98765”)
- Repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
- Utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.
- Utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.
- Escribir la contraseña en un papel o documento donde quede constancia de esta. Tampoco se deben guardar en documentos de texto dentro del propio equipo de cómputo o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del

equipo de cómputo).
- Enviar la contraseña por correo electrónico o en un SMS, tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
- Utilización de sus credenciales de usuario de la entidad en equipos de
- carácter público, sitios de internet, cafés de internet, etc. donde desconozca su nivel de seguridad y control.
- Cambiar las contraseñas por defecto proporcionadas por desarrolladores o fabricantes.

6.4.5. Administración de Backup's, Recuperación y Restauración de la información

- Todas las copias de respaldo de la Entidad deben ser incrementales. El Backup incremental sólo copia los datos que han variado desde la última operación de Backup's de cualquier tipo. Se suele utilizar la hora y fecha de modificación en los archivos, comparándola con la hora y fecha del último Backup. La aplicación de Backup's identifica y registra la fecha y hora de realización de las operaciones de Backup's para identificar los archivos modificados desde esas operaciones. Como un Backup incremental sólo copia los datos a partir del último Backup de cualquier tipo, se puede ejecutar tantas veces como se desee, pues sólo guarda los cambios más recientes. La ventaja de un Backup incremental es que copia una menor cantidad de datos que un Backup completo. Por ello, esas operaciones se realizan más rápido y exigen menos espacio de almacenamiento.
- Los medios de las copias de respaldo se almacenarán localmente y en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.
- Se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia.
- Para garantizar que la información de los funcionarios y contratistas sea respaldada, es responsabilidad de cada uno mantener copia de la información que maneja.

6.4.6. Adquisición, de tecnología

- Los requerimientos de activos de tecnología de las diferentes áreas deben ser avalados por la Secretaría de las TIC, Ciencia e Innovación con el fin de tener estandarizada la infraestructura y garantizar que cumple con los estándares de seguridad exigidos.
- Todo programa, proyecto o iniciativa que requiera contratar alguna de las Secretarías, Jefaturas o dependencias de la Alcaldía Distrital de Barrancabermeja, y que involucre la adquisición de bienes o servicios que incluyan componentes de tecnología (hardware, software,

desarrollo de aplicaciones, digitalización de trámites, accesos a Internet, cableado, conectividad, apropiación tecnológica, entre otros) o Procesos de Ciencia o Innovación, para el Distrito deberá contar con la participación de funcionarios de la Secretaría de las TIC, Ciencia e Innovación desde su estructuración inicial, prefactibilidad, factibilidad, definición de requerimientos técnicos y recomendaciones de contratación.

- Se exigirá un VoBo técnico por parte de los funcionarios asignados a esta Secretaría y que son expertos en la materia, previo y para cualquier proceso de contratación con el fin de garantizar se cumpla con los estándares y requerimientos de seguridad y privacidad de la información.
- Los requerimientos de apoyo técnico para estructuración de estos procesos contractuales, deberán ser tramitados formalmente ante la Secretaria TIC, Ciencia e innovación a través de la aplicación e Mesa de Ayuda TIC con el fin de garantizar la trazabilidad de los mismos, respuesta oportuna y asignación del funcionario experto en cada tema requerido.

6.4.7. Desarrollo y mantenimiento de software

La Secretaría de las TIC, Ciencia e Innovación es la responsable de:

- controlar y verificar la utilización de software en los equipos de cómputo
- brindar asesoría y supervisión para la instalación de software especializado.
- Realizar el desarrollo de software a la medida teniendo en cuenta todos los requerimientos de seguridad y privacidad de la información

- Está PROHIBIDO que otras dependencias contraten con terceros desarrollo de aplicaciones software sin contar con el aval de la Secretaría de las TIC, Ciencia e Innovación
- En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de información, únicamente se permite la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual y bajo aprobación de la Secretaría de las TIC, Ciencia e Innovación
- Con el propósito de proteger la integridad de los sistemas de información y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que apliquen).
- Es responsabilidad de cada funcionario la utilización de uso del software que se encuentra instalado en el equipo de cómputo asignado para el desarrollo de sus funciones
- La Secretaría de las TIC, Ciencia e Innovación debe revisar con regularidad el software que se encuentra instalado en los equipos de cómputo de la entidad y tiene la protestad de desinstalar el software clasificado como inadecuado o que vulnere la seguridad de los recursos de red o que viole los derechos de autor.
- Los usuarios no deben introducir intencionalmente software diseñado

para causar daño o impedir el normal funcionamiento de los sistemas de información, por tanto, cada usuario es responsable de lo que pueda hacer o la información que pueda generar en los sistemas de información

6.4.8. Control de accesos remotos

- Está prohibido el acceso a redes externas vía dial-up, cualquier excepción deberá ser documentada y contar con el visto bueno de la Secretaría de las TIC, Ciencia e Innovación
- La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el propietario de la información y el Secretaría de las TIC, Ciencia e Innovación.

6.4.9. Control de versiones

- Antes de la puesta en producción de una aplicación nueva, o de la modificación de las plataformas existentes, se debe asignar un número de edición o versión a la misma. Así, el número de versión se irá incrementando en cada cambio que se genere sobre la misma aplicación.
- El método de enumeración de las versiones deberá distinguir entre versiones en producción, en etapa de desarrollo, en etapa de pruebas o versión archivada.
- Todas las versiones deben ser almacenadas en bibliotecas, repositorios o directorios y deben contar con controles de acceso lógicos donde sólo se permita el acceso al personal autorizado.
- Periódicamente, las versiones que se encuentran en los ambientes de producción deben ser verificadas contra los repositorios y la documentación de los controles de cambio con el fin de determinar si los dos son congruentes.
- Si llegase a presentarse incongruencia en la revisión realizada, esto será identificado como un incidente de seguridad y se atenderá de acuerdo con el procedimiento de Gestión de Incidentes de seguridad.

6.5. POLITICA DE SEGURIDAD DE RECURSOS HUMANOS

- La Secretaría de las TIC, Ciencia e Innovación de la Alcaldía Distrital de Barrancabermeja

1. Promulgará la aplicación de criterios de control de seguridad de los recursos humanos en los procesos de contratación de personal, que permitan asegurar la idoneidad de los candidatos basada en la responsabilidad y ética pertinentes de acuerdo con las necesidades de los roles a ocupar y la clasificación de la información a la cual accederá.
2. Divulgará con periodicidad definida, las directrices y lineamientos de seguridad de la información a todos los servidores públicos o terceros que tenga una relación contractual con la entidad o que tengan acceso

a la información de la Entidad, de manera que, se entiendan y comprendan sus responsabilidades y obligaciones asociadas, bien como usuarios o con la responsabilidad compartida desde los roles asignados.

3. Capacitará y sensibilizará a los servidores públicos y terceros con respecto a los propósitos de la protección de la información en la Entidad.
4. Se asegurará acerca de la aceptación de las responsabilidades del acceso y uso de información o activos de información en aseguramiento de la confidencialidad de la información y transparencia mediante la firma de formato definido por la Entidad.
5. Velará porque todos los servidores públicos o terceros realicen la devolución de cada uno de los activos de información asignados, ante la terminación del contrato acordado.

- Funcionarios, contratistas, terceros o cualquier persona que tenga una relación contractual o laboral con la entidad, o que tenga acceso a los activos de información, deberán mantener la confidencialidad de la información de su acceso y conocimiento dentro o fuera de las instalaciones de la Entidad.
- La Entidad debe mantener un programa anual de concienciación y capacitación para todos los funcionarios y contratistas que interactúen con la información institucional y desarrollen actividades en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta.
- Todos los funcionarios y contratistas al servicio de la entidad deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.
- Al momento de la desvinculación o cambio de roles en la entidad, todo funcionario o contratista debe hacer entrega de todos los activos de información que le hayan sido asignados.

6.5.1.Condiciones Técnicas Para Trabajo Desde Casa

- Los Secretarios de Despacho y/o Jefes de Oficinas Asesoras, establecerán con los Servidores Públicos a su cargo, la relación de actividades y labores que por su naturaleza puedan realizarse desde casa, usando herramientas y medios tecnológicos reglamentados por la Alcaldía Distrital de Barrancabermeja.
- Servidores Públicos que realicen sus actividades desde la casa, deberán disponer como medio de conexión remota la plataforma TEAMS de Microsoft 365, que es la herramienta colaborativa y de productividad implementada en la Alcaldía Distrital de Barrancabermeja, esta herramienta se utiliza bajo el siguiente lineamiento. PARAGRAFO PRIMERO. Para Empleados Públicos con correo electrónico en el dominio @barrancabermeja.gov.co la herramienta TEAMS de Microsoft 365 viene incluida en la licencia de correo electrónico asignada.
- Para minimizar las reuniones en grupo y optimizar el seguimiento de las

actividades realizadas por los Empleados Públicos en esquema de trabajo a distancia, los Secretarios y Jefes de despacho priorizarán el uso del paquete de herramientas que se encuentran en las licencias de MS Office 365 de las que dispone la Alcaldía Distrital como:

- TEAMS de MS - pizarra de trabajo y videoconferencias de grupo internas y/o externas,
- PLANNER - control y seguimiento de las actividades del equipo de trabajo,
- ONEDRIVE - compartir información y documentos en la nube,
- CALENDARIO - programar adecuadamente las reuniones y los compromisos,
- STREAM - cargar o compartir contenidos en video.

6.6. POLITICA DE GESTION DE PROVEEDORES

La Alcaldía Distrital de Barrancabermeja identificará pautas para establecer y mantener relaciones claras y fortalecidas con aquellos terceros con quien se establezca una relación contractual bien sea de servicios o de productos, que aseguren el adecuado cumplimiento de los acuerdos establecidos, donde se garantice la aplicación de medidas de seguridad de la información en cumplimiento de los objetivos de la Entidad.

6.7. POLÍTICA DE GESTIÓN DE SEGURIDAD EN LA CONTINUIDAD DEL NEGOCIO

- Para la Alcaldía Distrital de Barrancabermeja su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal establecer las estrategias para mantenerlo.
- La Entidad identificará las necesidades y requisitos de seguridad de la información para su vinculación en el plan de continuidad de negocio, de modo que se asegure que, ante situaciones de crisis o desastres, no se descuiden los niveles de seguridad y se incurra en impactos indeseados.
- La Entidad garantizará la existencia de pólizas o seguros para la reposición de los activos informáticos de misión crítica que respaldan los planes de contingencia y la continuidad de los servicios.
- La Entidad deberá contar con un Plan de Recuperación ante Desastres (DRP) que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.
- Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, estarán incorporados y definidos en el Plan de Recuperación ante Desastres.
- Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del Plan de Recuperación ante Desastres

6.8. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD DE LA INFORMACIÓN

La Secretaría de las TIC, Ciencia e Innovación tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de la información institucional y de los equipos e instalaciones de cómputo, así como de bases de datos de información automatizada en general.

6.8.1. Derechos de propiedad intelectual

- Está prohibido por las normas de derechos de autor y por la Alcaldía Distrital de Barrancabermeja, realizar copias no autorizadas de software, ya sea adquirido o desarrollado por la Alcaldía Distrital de Barrancabermeja.
- Los sistemas desarrollados por personal interno o externo que estén bajo responsabilidad de la Secretaría de las TIC, Ciencia e Innovación, son propiedad intelectual de la Alcaldía Distrital de Barrancabermeja.
- La Entidad cumplirá con la reglamentación de propiedad intelectual, para lo cual implementarán los controles necesarios que garanticen el cumplimiento de dicha reglamentación.
- No se permitirá el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.
- Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.
- Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor

6.8.2. Revisiones del cumplimiento

La Secretaría de las TIC, Ciencia e Innovación

- Realizará acciones de verificación del cumplimiento de las Políticas y Estándares de Seguridad e Informática para Usuarios, de acuerdo con lo establecido en su programa anual de trabajo.
- Podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado a la Secretaría General.
- Determinará los líderes de los procesos que deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

6.8.3. Violaciones de seguridad de la información

- Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática.
- Está prohibido realizar pruebas a los controles de los diferentes elementos de Tecnologías de la Información y las Comunicaciones. Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación de la Secretaría de las TIC, Ciencia e Innovación, con excepción de los Órganos Fiscalizadores.
- Ningún usuario de la ALCALDÍA DISTRITAL DE BARRANCABERMEJA debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Secretaría de las TIC, Ciencia e Innovación
- No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a los computadores, redes o información de la ALCALDÍA DISTRITAL DE BARRANCABERMEJA. El incumplimiento de lo anterior será considerado una falta grave.

6.8.4. Sanciones Previstas por Incumplimiento

- Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente política de seguridad, conforme a lo dispuesto por las normas estatutarias escalafonarias y convencionales que rigen a los servidores públicos y en caso de corresponder, se realizarán las acciones correspondientes ante el o los organismos pertinentes.
- Las sanciones solo pueden imponerse mediante un acto administrativo que así lo disponga, cumpliendo las formalidades impuestas por los preceptos constitucionales, la ley de procedimientos administrativos y demás normativas específicas aplicables.
- Además de las sanciones disciplinarias o administrativas, la persona que no da debido cumplimiento a sus obligaciones puede incurrir también en responsabilidad civil o patrimonial, cuando ocasiona un daño que debe ser indemnizado y/o en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el código penal y leyes especiales.

7. GLOSARIO

- Activos De Información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la institución y, en consecuencia, debe ser protegido.
- Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- Confiabilidad: Aseguramiento de que la información es accedida solo para quienes es tan autorizados.
- Información: conjunto de datos organizados y procesados que constituyen mensajes, instrucciones, operaciones, funciones y cualquier tipo de actividad que tenga lugar en relación con un ordenador.
- Perfiles de usuario: conjunto de usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
- Política: Son instrucciones mandatarias que indican la intención de la alta gerencia respecto a la operación de la organización.
- Responsable por el activo de información: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
- Riesgo: Es la probabilidad de que una amenaza se convierta en un desastre.
- Recursos tecnológicos: son componentes de hardware y software tales como: servidores, estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas y asistenciales necesarias para el buen funcionamiento y la optimización del trabajo al interior de la institución.
- Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la institución
- Usuarios del Sistema: persona que se conecta al sistema para hacer uso de los servicios que este disponga

8. REFERENCIAS BIBLIOGRÁFICAS

- Norma NTC-ISO-IEC 27001 tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos
    - GTC-ISO-IEC 27002
    - GTC-ISO-IEC 27035