ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HÁBITAT
Unidad Administrativa Especial de
Servicios Públicos

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Unidad Administrativa Especial de Servicios Públicos

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HÁBITAT
Unidad Administrativa Especial de
Servicios Públicos

CONTENIDO

1. INTRODUCCIÓN

La Unidad Administrativa Especial de Servicios Públicos – UAESP entiende la información como uno de los activos más importantes para el cumplimiento de su misionalidad y la toma de decisiones, por lo tanto, ha definido la Política General de Seguridad y Privacidad de la Información para mantener la confidencialidad, integridad y disponibilidad de la información, mitigando riesgos e implementando controles efectivos durante el ciclo de vida de la información y los datos, aplicando la normatividad vigente.

El presente documento expresa el compromiso de la alta dirección con la seguridad de la información, y contiene los principios y lineamientos generales para ser aplicados en el desarrollo de todas las actividades relacionadas con el tratamiento de la información de la Entidad, generando confianza en las partes interesadas. Así mismo define las obligaciones y responsabilidades de los sujetos aplicables de esta política.

Esta política y las contenidas en el Manual de Políticas de Seguridad y Privacidad de la información, que complementan este documento, serán revisadas con regularidad y podrán ser objeto de actualización cuando aporten valor como parte del proceso de mejora continua y se ajusten a los requerimientos y medidas definidas por la Entidad.

2. TÉRMINOS Y DEFINICIONES

Activos de información: Toda información o elemento relacionado con el tratamiento de esta (Documentos, hardware, software, servicios, edificios, personas, entre otros) que tenga valor para la organización y por lo tanto se debe proteger. Se puede considerar un activo de información los datos creados o utilizados por un proceso, pueden ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, equipos de cómputo relacionados al tratamiento o almacenamiento de información, software del sistema, servicios utilizados para la transmisión, recepción y control de la información, entre otros.

Amenaza: Causa potencial de un incidente no deseado que puede provocar daños o afectaciones aun activo de información.

Autoridad competente: Es la autoridad apta e idónea para tratar de un determinado procedimiento o proceso de acuerdo con la ley.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [ISO 27000]

DAFP: Departamento Administrativo de la Función Pública (DAFP), es la entidad técnica, estratégica y transversal del Gobierno Nacional que contribuye al bienestar de los

colombianos mediante el mejoramiento continuo de la gestión de los servidores públicos y las instituciones en todo el territorio nacional.

Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Disponibilidad: La propiedad de tener la información cuando es requerida. Se relaciona con la facilidad y oportunidad de acceso a la información.

Estándar informático: todo aquel patrón o parámetro que permite establecer uniformidad en características de equipos, sistemas de cómputo y procedimientos de operación, con el cual se pretende garantizar la integridad, compatibilidad y racionalidad para los procesos tecnológicos de la institución.

Evento de seguridad de la información: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la Política de Seguridad de la Información o falla en los controles.

Incidente de seguridad de la información: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones de la Entidad y de amenazar la seguridad y privacidad de la información

Integridad: Propiedad de la información relativa a su exactitud y completitud. [ISO 27000]

MSPI: Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones – MinTIC.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

Es pertinente señalar que "seguridad de la información" no solo corresponde a Seguridad Informática, sino que su alcance se complementa con ciberseguridad, seguridad física, ambiental y del recurso humano entre otras, buscando mantener la confidencialidad, la disponibilidad e integridad de la información. [Directiva 002 de 2021 – Alcaldía Mayor de Bogotá]

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Terceros: Para efectos de esta política, el termino hace referencia a proveedores, practicantes, partes interesadas o cualquier persona natural o jurídica que tenga un vínculo laboral con la Entidad y preste un servicio de forma directa o indirecta bien sea en las instalaciones de la Entidad o en sus propias instalaciones y que emplea algunos de los recursos informáticos y de comunicaciones de la Entidad.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3)

Usuario: Cualquier persona que tiene acceso a la plataforma y a los activos de información, sea en calidad de usuario final, tercero o administrador de la plataforma.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

3. OBJETIVOS

3.1 Objetivo General

Establecer los lineamientos orientados a proteger la información administrada por la Entidad y los sistemas que la soportan, garantizando la prestación, coordinación, supervisión y control de los servicios que presta, en concordancia con los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicación – MinTIC, el Modelo de Seguridad y Privacidad de la Información – MSPI, el estándar ISO 27001 y las disposiciones legales vigentes en la materia, preservando los niveles de confidencialidad, integridad, disponibilidad, privacidad, autenticidad y no repudio de los activos de información.

3.2 Objetivos específicos

- Minimizar los riesgos de seguridad y privacidad de la información de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información y la función administrativa.
- Mantener la confianza de los(as) servidores públicos, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.

- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los(as) servidores públicos, terceros, aprendices, practicantes y usuarios de la UAESP.
- Garantizar la continuidad del negocio frente a incidentes de seguridad y privacidad de la información.

4. ALCANCE

La Política General de Seguridad y Privacidad de la Información aplica a todos los(as) servidores públicos, contratistas y terceros que accedan a los activos de información de la Unidad Administrativa Especial de Servicios Públicos – UAESP.

De igual manera, la presente política está orientada a todos los procesos de la entidad, bajo el marco de gestión establecido en el Modelo Integrado de Planeación y Gestión - MIPG propuesto por el DAFP y el Modelo de Seguridad y Privacidad de la Información - MSPI.

5. MARCO NORMATIVO

Teniendo en cuenta las disposiciones legales sobre seguridad de la información, el marco normativo en la materia, sin ser restringido, corresponde a:

CONSTITUCIÓN POLITICA: Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (…).

Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva.

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012, derogado parcialmente por el Decreto 1081 de 2015.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Decreto 103 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Compilado en el Decreto Único Reglamentario 1081 de 2015 del Sector Presidencia de la República.

Decreto 1074 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo." Reglamenta parcialmente la Ley 1581 de 2012.

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

Decreto 1081 de 2015: Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República. Reglamenta parcialmente la ley 1581 de 2012 y compila el Decreto 103 de 2015.

CONPES 3854 de 2016: Política Nacional de Seguridad Digital.

Resolución 2710 del 2017: Por la cual se establecen lineamientos para la adopción del protocolo IPV6.

Directiva 002 de 2018 - Secretaría Jurídica Distrital: Tratamiento de Datos Personales.

Directiva 005 de 2018 - Secretaría Jurídica Distrital: Tratamiento de datos personales – Autorizaciones, datos sensibles, datos de niños, niñas y adolescentes, cámaras y videos de seguridad, sanciones y recomendaciones.

Ley 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Decreto 2106 DE 2019: Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.

Resolución 1519 de 2020: Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

Resolución 500 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

6. COMPROMISO DE LA DIRECCIÓN

La Dirección de la Unidad Administrativa Especial de Servicios Públicos, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación, seguimiento y medición del Modelo de Seguridad y Privacidad de la Información MSPI - SGSI, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión, visión, los objetivos y planes estratégicos de la Entidad.

7. PRINCIPIOS

Los principios están orientados a proteger los tres pilares de seguridad de la información, confidencialidad, integridad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados y se listan a continuación.

Principio de cumplimiento normativo:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, se ajustará a la normativa de aplicación legal vigente con relación a la seguridad digital y privacidad de la información, en especial aquellas relacionadas con la protección de datos de carácter personal, seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.

Principio de Gestión de Riesgos:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, gestionará los riesgos hasta niveles aceptables implementando controles de seguridad adecuados y pertinentes.

Principio de concienciación y formación:

La Unidad Administrativa Especial de Servicios Públicos – UAESP, articulará programas de formación, sensibilización y campañas de concienciación para todos los(as) servidores públicos, contratistas y terceros que tengan acceso a los activos de información de la entidad en materia de seguridad de la información.

Principios de continuidad del negocio:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, asegurará la continuidad del negocio mediante planes de contingencia para los servicios de la información críticos y

de procesos misionales, velando por la confidencialidad, integridad y disponibilidad de la información.

Principio de responsabilidad:

Todos los(as) servidores públicos, contratistas y terceros en relación con la Unidad Administrativa Especial de Servicios Públicos – UAESP, deben ser responsables de los activos de información y sus acciones relacionadas a la seguridad de la información, cumpliendo con las normas y controles establecidos.

Principio de gestión de incidentes:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, gestionará los incidentes de seguridad digital articulando las capacidades que permitan atender de forma oportuna y adecuada la materialización de riesgos.

Principio de mejora continua:

La Unidad Administrativa Especial De Servicios Públicos – UAESP, revisará de manera periódica el grado de eficacia de los controles de seguridad implementados en la Entidad y velará por la disponibilidad de sus procesos estratégicos, misionales, de apoyo y de evaluación y la continuidad de su operación basada en la prevención de incidentes de seguridad de la información.

Lo anterior, con el fin de aumentar la capacidad de adaptación a la constante evolución del riesgo y del entorno tecnológico.

8. POLÍTICA GENERAL

La Entidad brindará los recursos necesarios con el fin de asegurar la protección, la Confidencialidad, Integridad, Disponibilidad, Legalidad y No Repudio de sus activos de información en todo su ciclo de vida, mediante la gestión de riesgos, fomentando una cultura de seguridad y privacidad de la información en los(as) servidores públicos, contratistas y terceros que permita establecer un marco de confianza en sus deberes acorde con las necesidades de las diferentes partes de interés y el cumplimiento de los requisitos legales pertinentes.

9. OBLIGACIONES

Los(as) servidores públicos, contratistas y terceros son responsables por el manejo adecuado y aseguramiento de la información utilizada en el desarrollo de sus actividades y obligaciones contractuales.

Los sujetos de aplicabilidad de esta política deberán cumplir con los lineamientos, requisitos y buenas prácticas de seguridad y privacidad de la información que adopte la entidad y que se encuentran en el Manual de Políticas de Seguridad y Privacidad de la Información, en su última versión vigente, previniendo, detectando y reportando cualquier incidente relacionado con la seguridad y privacidad de la información.

La seguridad y privacidad de la información resulta prioritaria para la Unidad Administrativa Especial de Servicios Públicos, en esa medida, cualquier contravención u omisión de la política aquí descrita, se sancionará por parte de la autoridad competente y de conformidad con la normatividad vigente.

10. RESPONSABILIDADES

A continuación, se definen los roles y responsabilidades respecto a seguridad y privacidad de la información, los cuales se requieren para la implementación del Modelo de Seguridad y Privacidad de Información MSPI de la UAESP, tomando como referencia lo establecido en la norma NTC/ISO 27001:2013 y la Resolución 00500 10 de marzo del 2021 MinTIC, a través del cual se busca el logro de los objetivos de la seguridad de la información en la Entidad.

ROL	RESPONSABILIDAD
Comité Institucional de Gestión y Desempeño	• Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades: o Aprobación y seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna de las políticas de seguridad y privacidad de la información. o Promover la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad. o Aprobar acciones y mejores prácticas en la implementación del MSPI. o Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información. • Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.
Mesa Técnica Seguridad Digital	• Revisar los resultados de las herramientas de medición del estado de la seguridad y privacidad de la información en la Entidad. • Acompañar e impulsar el desarrollo de proyectos de seguridad y privacidad de la información. • Proponer al comité institucional de gestión y desempeño la gestión de roles y responsabilidades que se requieran para la implementación,

	mantenimiento y desarrollo del MSPI. • Proponer el uso de metodologías y procesos específicos para la seguridad y privacidad de la información. • Intervenir en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos de seguridad y privacidad de la información. • Apoyar en la adquisición y/o contratación de los recursos necesarios para el desarrollo y mantenimiento de la seguridad y privacidad de la información. • Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad. • Poner en conocimiento de la entidad, los documentos de seguridad que impacten de manera transversal a la misma, como normas, buenas prácticas, documentos del SIG, documentos del MSPI y normatividad vigente aplicable. • Debatir y aprobar las propuestas para la implementación de acciones de seguridad de la información, cuya aplicación sea de carácter transversal a la operación de la Entidad.
Jefe Oficina TIC	• Asesorar a la Dirección General y dependencias de la Unidad en materia de Seguridad y privacidad de la Información. • Planear y administrar los recursos informáticos y de telecomunicaciones para satisfacer las necesidades y requerimientos de los usuarios de la UAESP, de conformidad con las políticas, metodologías y normatividad vigente. • Adoptar e implementar buenas prácticas o estándares informáticos, de calidad y de seguridad y privacidad de la información. • Apoyar y aprobar estudios, investigación y análisis de tendencias tecnológicas para su posible aplicación en la Entidad. • Apoyar en la formulación del plan de capacitación en relación con seguridad y privacidad de la información.
Responsable de Seguridad de la Información	• Apoyar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información de conformidad con la regulación vigente. • Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad. • Realizar la planificación y cronograma de la implementación del MSPI. • Proponer, definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI. • Realizar el acompañamiento a los procesos y/o proyectos en materia de seguridad y privacidad de la información. • Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y

	metodologías en la materia. • Definir e implementar en coordinación con las dependencias de la Entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y Contratistas. • Apoyar a los procesos de la Entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información. • Liderar la implementación el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad. • Poner en conocimiento de las dependencias con competencia funcional, cuando se detecten irregularidades, incidentes o prácticas que atentes contra la seguridad y privacidad de la información de acuerdo con la normativa vigente. • Verificar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a la alta dirección. • Convocar la participación de los(as) servidores públicos y contratistas de las diferentes subdirecciones y Oficinas cuando el incidente lo amerite. • Verificar el cumplimiento de los procedimientos y buenas prácticas en gestión de incidentes y recomendar, si lo amerita, la aplicación de planes de contingencia y/o continuidad. • Indagar todos los incidentes de seguridad de la información y apoyar el análisis forense cuando se requiera.
Administrador de infraestructura tecnológica	• Estructurar y mantener los activos informáticos relacionados con la gestión de la seguridad y privacidad de la información, por ejemplo, equipo de firewall, sistemas de gestión y monitoreo, sistemas de prevención de intrusos (IPS), consola de despliegue de políticas de seguridad, routers de frontera, entre otros. • Participar y colaborar con la gestión y atención de incidentes de seguridad de la información con el fin de analizar, identificar, contener y erradicar los incidentes de seguridad y privacidad de la información. • Generar los reportes de eventos de seguridad que sean solicitados por parte del Responsable de Seguridad de la Información, por ejemplo, aquellos relacionados al uso de un canal de comunicaciones, registro de accesos a recursos, entre otros. • Elaborar los ajustes necesarios sobre los sistemas de seguridad que gestione y que sean indicados por el Responsable de Seguridad de la Información a manera de controlar, prevenir o detectar incidentes de seguridad y privacidad de la información.
Grupo de apoyo - MSPI	• Apoyar al responsable de seguridad de la información y a los líderes de procesos en la identificación de activos de información. • Apoyar al responsable de seguridad de la información y a los líderes

	de proceso en la aplicación de la metodología de valoración de riesgos de seguridad de la información. • Apoyar en la elaboración y seguimiento de indicadores del SGSI. • Apoyar al responsable de seguridad de la información en la actualización de la documentación del MSPI y en su mejora continua. • Apoyar en las campañas de sensibilización o divulgación del MSPI.
Responsable de protección de datos personales	• Consolidar y reportar la información de Base de datos personales que maneja o tiene la entidad en conformidad con la normatividad vigente. • Fomentar la cultura de la protección y privacidad de datos personales que tiene a cargo la entidad y el cumplimiento de la normatividad aplicable. • Apoyar en la definición, implementación y seguimiento de los controles para el tratamiento de datos personales y privacidad de la información de acuerdo con la normatividad vigente. • Apoyar en la elaboración, comunicación y aplicación de la política de datos personales, con los criterios de calidad y oportunidad.
Dueño del Riesgo de seguridad y privacidad de la información. (Custodio)	• Identificar e inventariar los nuevos activos de información y los riesgos de seguridad y privacidad de la información asociados. • Cumplir con las acciones correctivas y de mejora identificadas en las auditorias del MSPI. • Mantener actualizados y realizar la medición de la eficacia a los controles de seguridad de la información. • Suministrar las evidencias de la aplicación de los controles diseñados para mitigar los riesgos de seguridad y privacidad de la información de acuerdo a la periodicidad establecida. • Realizar el análisis de riesgos de seguridad y privacidad de la información de sus procesos y revisar el plan de tratamiento de riesgos con el responsable de seguridad de la información para implementar los controles y su ejecución periódica o continua
Administrador Mesa de Ayuda	• Recibir los reportes por parte de los usuarios sobre incidentes, registrarlos en la herramienta de Mesa de ayuda e informar al responsable de atención a incidentes de seguridad de la información. • Apoyar en la gestión o atención de incidentes de seguridad de la información. • Actualizar los indicadores de incidentes de seguridad de la información.
Usuarios	• Conocer y cumplir las políticas de seguridad y privacidad de la información y la normatividad vigente relacionada. • Reportar incidentes de seguridad que atenten contra la confidencialidad, integridad o disponibilidad de la información o evidencien un incumplimiento de las políticas de seguridad y privacidad de la información. • Participar constantemente de las campañas de sensibilización del MSPI.

	• Participar de las actividades para la identificación de activos de información y riesgos de seguridad y privacidad de la información. • Colaborar en el desarrollo de las auditorías internas y externas al MSPI.

CONTROL DE CAMBIOS:

Versión	Fecha	Descripción de la modificación
01	15/10/2019	Se adopta la Política de Seguridad de la Información mediante resolución interna 0589 de 2019
02	28/09/2021	Se actualiza la normativa legal vigente aplicable en relación con la seguridad de la información. Se ajustan los objetivos y se definen objetivos específicos de acuerdo con los requerimientos de la ISO 27001, el MSPI y la Política del Sistema integrado de Gestión. Se elimina las menciones al Modelo de Transformación Organizacional – MTO. Se ajustan los principios básicos y se define de forma explícita el compromiso por la dirección. Se definen y ajustan la matriz de roles y responsabilidades en materia de seguridad de la información de acuerdo con la implementación del MSPI.

AUTORIZACIONES:

	NOMBRE	CARGO	FIRMA
Elaboró	Osbaldo Cortes Lozano	Profesional Universitario – Oficina TIC	Acta o Grabación Teams del Comité Institucional de Gestión y Desempeño
	Juan Sebastian Perdomo Mendez	Profesional Universitario – Oficina TIC	
Revisó y Aprobó	Comité Institucional de Gestión y Desempeño		