INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA, RECREACIÓN Y DEPORTE
Instituto Distrital del Patrimonio Cultural

Manual

Seguridad de la Información

Proceso

Gestión de Sistemas de Información y Tecnología

Vigencia: 27 Septiembre 2019
Versión: 1

1. OBJETIVO

Proteger, asegurar y garantizar la confidencialidad, autenticidad, integridad, disponibilidad y confiabilidad de los activos de información del Instituto Distrital de Patrimonio Cultural, alineadas a los objetivos estratégicos de la entidad, a través de la formulación e implementación de políticas, medidas de seguridad y mecanismos de control

2. ALCANCE

Inicia desde la definición de la política de General de Seguridad de la Información y finaliza con los lineamientos de Tercerización u Outsourcing.

3. DEFINICIONES

TÉRMINO	DEFINICIÓN
Seguridad Informática	Entendemos por seguridad informática el conjunto de medidas adicionales a las usadas en el procesamiento computarizado normal, tales como: políticas, estándares, procedimientos, mecanismos, dispositivos y recursos, asignados expresamente para proteger la información contra su destrucción accidental o deliberada y su modificación o divulgación no autorizada.
Confidencialidad	Velar por la privacidad de la información, haciéndola accesible únicamente a usuarios autorizados.
Integridad	Proteger la información para que no sea alterada de manera aislada, ya sea interna o externamente a los sistemas.
Disponibilidad	Establecer los procedimientos necesarios para que los sistemas estén operativos y cuenten con los mecanismos de respaldo necesarios para permitir el acceso seguro a la información y la continuidad del negocio.
Auditabilidad	Permitir que todas las transacciones, incluidas las de seguridad informática, pueden ser revisadas y/o monitoreadas en línea o en forma posterior por los usuarios autorizados.
Legalidad	Velar por que toda la información y los medios o elementos que la contienen, procesen y/o transporten, cumplan con las reglamentaciones legales vigentes relacionadas con la privacidad y uso de la información.
Efectividad	La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
Confiabilidad	Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Internet	Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.
Intranet	Una intranet es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.
Tecnología de la Información	Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.
Recursos Tecnológicos	Elementos de tecnología que pueden ser hardware y/o software, tales como equipos de cómputo, servidores, impresoras, teléfonos, faxes, programas y/o aplicativos de software, dispositivos USB, entre otros.
Activos	Información importante que desea proteger frente a cualquier situación que suponga un riesgo o amenaza. Esta información que resulta fundamental para la organización es lo que se denomina activo.
Hardware	en informática se refiere a las partes físicas, tangibles, de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos
Software	Creación intelectual que comprende los programas, los procedimientos, las reglas y cualquier documentación asociada pertinente a la operación de un sistema de procesamiento de datos.
Carpeta de Red	Carpeta donde se almacena información de uso compartido.
Software Ilegal	El software ilegal es un programa que ha sido duplicado y distribuido sin autorización.
Riesgo Informático	Es una combinación de la posibilidad de que una amenaza contra un activo de información ocurra aprovechando una vulnerabilidad y/o falla en un control, y la severidad del impacto adverso resultante. Reduciendo la amenaza o la vulnerabilidad reduce el riesgo.
Contraseña	Código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.
WebMaster	Alude a la persona que tiene la responsabilidad del desarrollo, la coordinación y el mantenimiento de un sitio web.
Correo Electrónico	Servicio de red que permite a los usuarios enviar y recibir mensajes mediante redes de comunicación electrónica.
Respaldo de Información	Es la copia de los datos importantes de un dispositivo primario en uno ó varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una avería electromecánica ó un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria
Integridad de datos	La integridad de datos es un término usado para referirse a la exactitud y fiabilidad de los datos. Los datos deben estar completos, sin variaciones o compromisos del original, que se considera confiable y exacto.
VPN	(Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

4. NORMATIVIDAD

Ley 1273 de 2009 denominada "Protección de la información y los datos",

LEY 603 DE 2000 Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un

activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

CONPES 3854 de 2016 Política Nacional de Seguridad digital.

Resolución 305 de 2008, expide políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

Norma Técnica Colombiana NTC-ISO/IEC 27001:20013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

ISO 27005, Guía para la Gestión de los riesgos de la seguridad de la información.

ISO 27002 Guía de buenas prácticas de seguridad de la información,

Directiva 05 del 12 de 2005, Secretaría General- Alcaldía Mayor, Por medio de la cual se adoptan las políticas generales de tecnología de información y comunicaciones aplicables al Distrito Capital.

5. POLÍTICAS DE OPERACIÓN

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, Jefes de Oficina, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el Instituto Distrital de Patrimonio Cultural - IDPC, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual. Los usuarios tienen la obligación de dar cumplimiento a los presentes lineamientos.

Estas políticas contribuyen a la correcta Seguridad de la Información y tiene alcance en todos los procesos que hacen parte del Instituto Distrital de Patrimonio Cultural.

6. CONTENIDO

6.1 DECLARACION DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

El Instituto Distrital del Patrimonio Cultural - IDPC, se compromete a preservar la confidencialidad, disponibilidad e integridad, de sus activos de información, protegiéndolos contra amenazas internas y externas, mediante una identificación, valoración, implementación de controles, monitoreo y seguimiento de los niveles de riesgo de acuerdo a la metodología de gestión de riesgos en seguridad a niveles aceptables, manteniendo la mejora continua; apoyando el logro de sus objetivos y el cumplimiento de los compromisos institucionales con la lucha anticorrupción, lucha antipiratería, con la confidencialidad, la circulación y divulgación adecuada de la información, y con el gobierno en línea.

La Alta Dirección de la Entidad demostrará su compromiso a través de:

- La promoción activa de una cultura de seguridad.

- Facilitar la divulgación de este documento a todos los Subdirectores, funcionarios, contratistas de la Entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener la Política General de Seguridad de la Información

6.2 REGULACIÓN:

La Política General de Seguridad de la Información contenida en este documento deberá ser conocida, aceptada y cumplida por todos los Jefes de oficina, funcionarios, contratista del Instituto Distrital de Patrimonio Cultural. El incumplimiento de las mismas se considerará un incidente de seguridad, que de acuerdo con el caso podrá dar lugar a un proceso disciplinario para los funcionarios y se podrá convertir en un incumplimiento del contrato respecto de los contratistas, que pueda dar lugar a la imposición de sanciones e incluso su terminación, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

6.3 RESPONSABLES:

- La Alta Dirección, Jefes de Oficina, funcionarios, contratistas y todos los servidores públicos del Instituto Distrital de Patrimonio Cultural.
- Servidores Públicos de Órganos de Control y/o Entidades Gubernamentales que en cumplimiento de su función hagan uso de las tecnologías a las cuales aplica la presente Política.
- Terceros que utilicen equipos y herramientas informáticas propiedad de la entidad.

6.4 SOFTWARE Y LICENCIAMIENTO

El IDPC instalará los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización del IDPC (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para el Instituto, por lo que ésta práctica no está autorizada.

Todo el software usado en la plataforma tecnológica del IDPC debe tener su respectiva licencia y acorde con los derechos de autor.

Los programas instalados en los equipos, son de propiedad del IDPC, la copia no autorizada de programas o de su documentación, implica una violación a la política general del IDPC. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por el IDPC o las sanciones que especifique la ley.

El IDPC se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad del Instituto. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.

Los recursos tecnológicos y de software asignados a los funcionarios del IDPC son responsabilidad de cada funcionario y/o Contratista.

Los usuarios solo tendrán acceso a los datos y recursos autorizados por el IDPC, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.

Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.

6.5 USO DE RECURSOS TECNOLÓGICOS

El Instituto Distrital de Patrimonio Cultural asignará diferentes recursos tecnológicos como herramientas de trabajo para uso exclusivo de sus funcionarios y contratistas autorizados.

El uso adecuado de estos recursos se reglamenta bajo las siguientes directrices: La instalación de cualquier tipo de software en los equipos de cómputo del IDPC, debe ser realizada por el Grupo de Gestión de Sistemas de Información y por tanto son los únicos autorizados para realizar esta labor.

Los usuarios no deberán realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz, protector de pantalla corporativo o traslado de hardware. Estos cambios podrán ser realizados únicamente por las oficinas autorizadas.

El proceso de gestión de sistemas de información definirá 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, realizará el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

Sólo personal autorizado podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del IDPC; las conexiones establecidas para este fin, utilizarán los esquemas de seguridad definidos.

Los funcionarios de la entidad son responsables de hacer buen uso de los recursos tecnológicos del IDPC y en ningún momento podrán ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros funcionarios, terceros, la legislación vigente y las políticas y lineamientos de seguridad de la información del IDPC.

6.6 CARPETAS DE RED, DISCOS DE RED, CARPETAS VIRTUALES

Para que los usuarios tengan acceso a la información ubicada en los discos o carpetas de red, el Subdirector, jefe de oficina o Asesor deberá enviar un correo autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar al proceso de Gestión de Sistemas de Información y Tecnología del IDPC. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos o carpetas de red, dependiendo de sus funciones y su rol.

La información almacenada en cualquiera de los discos o carpetas de red debe ser de carácter institucional.

Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres del Instituto o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso.

Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos o carpetas de red sin expresa autorización del Subdirector o Jefe de Oficina de la dependencia correspondiente.

Se prohíbe el uso de la información de los discos o carpetas de red con fines publicitarios, de imagen negativa, lucrativa o comercial.

6.7 RESPALDO Y RESTAURACIÓN DE LA INFORMACIÓN

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

El administrador de los servidores, los sistemas de información o los equipos de comunicaciones, es el responsable de definir la frecuencia de respaldo y los requerimientos de seguridad de la información y el asignado por el subdirector de gestión corporativa es el responsable de realizar los respaldos periódicos.

Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.

Es obligación de los usuarios finales verificar la realización de las copias en las carpetas destinadas para este fin.

La Subdirección de Gestión Corporativa debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas del IDPC.

Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

Es responsabilidad de cada dependencia mantener depurada la información de las carpetas de red para la optimización del uso de los recursos de almacenamiento que entrega el IDPC a los usuarios.

6.8 CONTROL DE ACCESO

El IDPC suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

Ningún usuario deberá acceder a la red o a los servicios TIC del IDPC, utilizando una cuenta de usuario o clave de otro usuario.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose a la extensión del proceso de Gestión de Sistemas de información y Tecnología, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por el jefe inmediato por medio de una solicitud en la Mesa de Ayuda.

La conexión remota a la red de área local del IDPC debe ser hecha a través de una conexión VPN segura suministrada por el Instituto, la cual debe ser aprobada, registrada y auditada. El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.

6.9 MANEJO DE CONTRASEÑAS PARA ADMINISTRADORES DE TECNOLOGÍA

Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible, se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.

Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

El personal del proceso de Gestión de Sistemas de Información y Tecnología no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del líder del Área de Tecnologías y Sistemas de la Información.

Los usuarios y claves de los administradores de sistemas y del personal del proceso de Gestión de Sistemas de Información y Tecnología son de uso personal e intransferible.

El personal del proceso Gestión de Sistemas de Información y Tecnología debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo al rol asignado.

6.10TRANSFERENCIA DE INFORMACIÓN

Toda transferencia de información perteneciente al IDPC a la cual tengamos acceso por razones técnicas o comerciales debe ser susceptible de trazabilidad.

El IDPC en caso de tener un servicio de transferencia de archivos deberá realizarlo empleando protocolos seguros. Cuando el origen sea el IDPC hacia entidades externas, el IDPC establecerá los controles necesarios para preservar la seguridad de la información; cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de seguridad de la información con esa entidad; en todo caso se deben revisar y proponer controles en concordancia con las políticas de seguridad de la información del IDPC; los resultados de la revisión de requerimientos de seguridad se documentarán y preservarán para futuras referencias o para demostrar el cumplimiento con las políticas y con los controles de seguridad del IDPC.

Los usuarios de las Subdirecciones y Oficinas del IDPC 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 del Instituto, sin la autorización de la Subdirección de Gestión Corporativa.

La Oficina Asesora Jurídica del IDPC debe establecer en los contratos que se creen con los funcionarios y contratistas, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas por la divulgación no autorizada de información de beneficiarios del instituto que les ha sido entregada en razón del cumplimiento de los objetivos misionales del IDPC.

No está permitido el intercambio de información sensible del instituto por vía telefónica.

Los propietarios de los activos de información deben asegurar la validación y garantizar que el Intercambio de información solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de Seguridad.

Los propietarios de los activos de información deben velar porque la información del IDPC sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las clausulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

6.11SEGURIDAD PARA LAS RELACIONES CON PROVEEDORES

La Oficina Asesora Jurídica del IDPC debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre el instituto y proveedores incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos.

Los Supervisores de contratos deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.

6.12 USO DE INTERNET

La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.

No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas del IDPC o que representen peligro para el Instituto como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por el IDPC.

La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

6.13 USO DE CORREO ELECTRÓNICO

Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con el instituto.

Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC del IDPC se consideran bajo el control del Instituto.

Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en el IDPC y no debe utilizarse para ningún otro fin.

Cada Subdirector o Jefe de Oficina deberá solicitar la creación de las cuentas de correo electrónico por medio de la Mesa de Ayuda.

El área de Talento Humano para funcionarios de planta y temporales y el respectivo Subdirector para los contratistas del IDPC son los responsables de solicitar la modificación o cancelación de las cuentas electrónicas al proceso de Gestión de Sistemas de Información y Tecnología del IDPC.

El envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red, no está autorizado.

No está autorizado, el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre del Instituto.

Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire del IDPC, su cuenta de correo será desactivada y luego se elimina por parte del proceso de Gestión de Sistemas de Información y Tecnología.

Las cuentas de correo electrónico son propiedad del IDPC, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con el instituto, ya sea como personal de planta, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en el Instituto y no debe utilizarse para ningún otro fin.

Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo.

Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte del Instituto.

Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo a la cuenta sistemas@idpc.gov.co con la frase "correo sospechoso” en el asunto.

6.14 TERCERIZACIÓN U OUTSOURCING

Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información del IDPC, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

El proceso de Gestión de Sistemas de Información y Tecnología deberá mitigar los riesgos de Seguridad y privacidad de la información teniendo en cuenta lo definido en el Manual de Gestión de Riesgos del IDPC.

Se debe identificar y monitorear los riesgos relacionados con los contratistas o proveedores en relación a los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación.

Los funcionarios del IDPC que se asignen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

Se deben establecer mecanismos o condiciones con los contratistas o proveedores que permitan realizar la gestión de cambios en los servicios suministrados.

7. CONTROL DE CAMBIOS

Fecha	Versión	Naturaleza del cambio
27-09-2019	1	Creación del documento

8. CRÉDITOS

Elaboró	Revisó	Aprobó
Mary Elizabeth Rojas Muñoz Contratista Subdirección de Gestión Corporativa Cristian Velásquez - Profesional contratista Equipo SIG Oficina Asesora de Planeación	Juan Fernando Acosta Mirkow Subdirector de Gestión Corporativa	Juan Fernando Acosta Mirkow Subdirector de Gestión Corporativa
Aprobado	Memorando interno con N° radicado 20195400048943 de 25-09-2019	