 <p>PERSONERIA DE CARTAGENA DE INDIAS <i>Defender tus derechos es nuestro deber</i></p>	PERSONERIA DISTRITAL DE CARTAGENA	CODIGO: DE-P-007
	GESTIÓN DE DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 1
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	FECHA DE APROBACIÓN(d-m-a): 30/01/2020

PLAN TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PERSONERÍA AUXILIAR

**Personería Distrital de Cartagena de Indias
2023**



PERSONERIA DISTRITAL DE
CARTAGENA

CODIGO: DE-P-007

GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO

VERSIÓN: 1

PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION

FECHA DE
APROBACIÓN(d-m-a):
30/01/2020

INTRODUCCION

El presente Plan de Tratamiento de Riesgos se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno digital en el Eje Temático de la Estrategia en **seguridad y privacidad de la información**, el cual busca proteger los datos de los ciudadanos garantizando la seguridad de la información.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

1. INFORMACIÓN GENERAL DE LA ENTIDAD

La personería Distrital de Cartagena en cumplimiento de lo dispuesto en el artículo 118 de la Constitución política de Colombia que dispone. *“El Ministerio Público será ejercido por el Procurador General de la Nación, por el Defensor del Pueblo, por los procuradores delegados y los agentes del Ministerio Público, ante las autoridades jurisdiccionales, por los Personeros Municipales y por los demás funcionarios que determine la ley. Al Ministerio Público corresponde la guarda y promoción de los derechos humanos, la protección del interés público y la vigilancia de la conducta oficial de quienes desempeñan funciones públicas.”*

Considerando lo anterior le corresponde a la Personería de Distrital de Cartagena como órgano de control de orden constitucional, la guarda y promoción de los derechos humanos, propender por la vigencia de un orden social equitativo, la protección del interés público y la vigilancia de la conducta oficial de quienes desempeñan funciones públicas en la ciudad de Cartagena de Indias Distrito Capital y turístico. En ese orden de ideas las funciones esenciales de la Personería se pueden categorizar en cuatro dimensiones:

1. Función de defensa, protección y promoción de los derechos humanos
2. Función de Veeduría y vigilancia
3. Función de Ministerio público
4. Función de Vigilar la conducta oficial de los servidores públicos.

Es por ello, que se estableció el Plan Estratégico Institucional de la Personería Distrital del Cartagenade Indias 2020-2024 “Defender Tus Derechos es Nuestro Deber”, el cual se desarrolla a través de los siguientes objetivos estratégicos:



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

Atención oportuna y con calidad a la comunidad, Ampliación de cobertura y fortalecimiento Institucional, Modernización Institucional Gestión transparente y efectiva, Postconflicto y Alianzas Estratégicas Interinstitucionales, cuyo objetivo es la Protección, Promoción y Divulgación del ejercicio pleno de los derechos Humanos, la Vigilancia de la conducta oficial y la protección del interés Público de la comunidad Cartagenera, mediante espacios de Participación Ciudadana.

La personería Distrital de Cartagena actualmente tiene sede principal en el Centro Histórico, Calle del Candilejo No. 33-35 y en su proceso de descentralización, esta entidad hace presencia en Casas de Justicia, salas de Atención al Usuario —SAU- Unidades de Atención Inmediata —URI- Juzgados Penales Municipales, Fiscalías Seccionales y locales y Orientación a la población desplazadas — UAO-.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

2. MISIÓN

La Personería Distrital de Cartagena de Indias protege, promueve y divulga el ejercicio pleno de los Derechos Humanos, la Vigilancia de la conducta oficial y la protección del interés Público de la comunidad Cartagenera, para lograrlo promueve la creación de espacios de Participación Ciudadana impartiendo la instrucción y orientación en las comunidades con miras a la sensibilización y fortalecimiento de la cultura ciudadana y la defensa de los derechos fundamentales.

3. VISION

Ser en el año 2024 una entidad que impacte de forma efectiva en la defensa de los intereses de la comunidad, colaborando en la edificación de una sociedad democrática, participativa, incluyente y pluralista; que le permita tener reconocimiento local, en la guarda, vigilancia, promoción y divulgación de los derechos humanos.

4. POLITICA DE CALIDAD

La Personería Distrital de Cartagena es una entidad orientada al mejoramiento continuo, que se compromete día a día con la satisfacción de las necesidades de sus usuarios (comunidad) a través de la prestación de servicios de calidad, atendidos oportunamente y con respeto a la dignidad humana, enmarcados en los parámetros de ley; los cuales se soportan en procesos óptimos, un equipo de colaboradores competentes y en mecanismos de comunicación efectivos.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

5. PRINCIPIOS ETICOS

- La función primordial del servidor público es atender eficaz, eficiente y oportunamente la comunidad.
- El servicio público implica vivirlo y prestarlo cada día como si fuera el primero, con la misma disciplina, compromiso, emoción, iniciativa y mística.
- La fidelidad a la institución, jefes, compañeros y comunidad es imperativo del servicio público.
- Las decisiones y actividades del servidor público garantizan la prevalencia del interés general sobre el interés particular.
- El trato cortés, amable y considerado, acerca a las personas.
- Los servidores públicos están obligados a alcanzar con entusiasmo, convicción y trabajo en equipo, el mejoramiento de los procesos de atención ciudadano.
- El interés genuino por los demás, llena el corazón de seguridad, estímulo y paz.
- La imagen pública está reflejada en la consideración y el aprecio que cada uno de los servidores públicos muestra por la institución.
- Es imperativo del servidor público, obrar con equidad en todas sus formas y circunstancias.
- El servicio público comporta un alto nivel de paciencia, comprensión y transigencia con los seres humanos.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

6. VALORES ETICOS

- **Servicio.** Prestación y aplicación humana del trabajo que satisface necesidades a personas, comunidades y organizaciones.
- **Responsabilidad.** Cumplimiento a cabalidad de las obligaciones y deberes frente a la familia, la comunidad, la institución y el Estado con capacidad para asumir las consecuencias de sus propias acciones.
- **Lealtad.** Gratitud y amor con la entidad, los jefes, los compañeros, la familia y la sociedad.
- **Honestidad.** Consiste en actuar con rectitud, transparencia y coherencia con lo que se piensa, se expresa y se hace.
- **Respeto.** Consideración y estima, por la comunidad o sociedad civil, el entorno, su cuidado y la observancia de conductas para preservarlo y dignificarlo.
- **Productividad.** Capacidad para ejecutar acciones y lograr los mejores resultados, mediante la optimización del tiempo y los recursos.
- **Solidaridad.** Es la adhesión a la causa, que se manifiesta con relaciones de apoyo y cooperación con todas las personas.
- **Pertenencia.** Consiste en asumir el hecho de estar inmerso en la comunidad, en la personería y en sus valores aceptados.
- **Justicia.** Disposición para actuar con equidad y probidad en relación con las personas, los procesos y las decisiones.
- **Tolerancia.** Capacidad de escuchar, observar y respetar las acciones y diferencias de los demás para poder interrelacionarse en forma armónica.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

INTRODUCCION

La información es un activo de alto valor para la Personería Distrital de Cartagena de Indias. A medida que los procesos de la entidad se hacen más dependientes de la información y de la tecnología que la soporta, se hace necesario contar con reglas de alto nivel que permitan el control y administración efectiva de los datos.

Los sistemas computarizados y aplicaciones están en permanente evolución, por tal razón pueden surgir nuevos puntos vulnerables y crear interrupciones o degradación de los servicios apalancados por las TI, porque a pesar de los avances en los sistemas de seguridad, los usuarios autorizados o no al uso y apropiación de las TI, con herramientas muy sofisticadas tienen grandes posibilidades de acceder las redes, los sistemas o sitios que sin políticas claras y ampliamente difundidas pueden llegar a materializarse alguno riesgos.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

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

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

El presente modelo pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte de la entidad, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

Finalmente, a nivel metodológico es importante tener presente que se han incluido una serie de guías en cada una de las fases del modelo, para que los destinatarios del mismo tengan claridad de cuáles son los resultados a obtener y como desarrollarlos.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

JUSTIFICACION

El Ministerio TIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones, a través de las cuales contribuye a la construcción de un Estado más eficiente, más transparente y participativo, publica El Modelo de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea.

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



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

PRINCIPIOS

Las políticas contenidas en el presente manual se justifican y sustentan en los principios de la seguridad de la información, tales principios son:

- Propuesta de explicar el detalle de cada principio
- Promover comportamientos de seguridad.
- Responsables.
- Exhortar las actuaciones profesionales y técnicas.
- Promover una cultura positiva para la seguridad.
- Tener un enfoque basado en los riesgos.
- Buscar el cumplimiento de los requisitos legales y regulatorios pertinentes.
Promover la mejora continua.
- Proteger la información clasificada.
- Evaluar las amenazas actuales y futuras de la información.
- organización.
- Ofrecer calidad y valor a las partes interesadas.
- Ofrecer información puntual y precisa sobre la gestión de la seguridad.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

GLOSARIO

Activo de información: Todo aquello que tiene valor para la entidad y por lo tanto debe protegerse. De acuerdo con la norma ISO 27001 los activos de información se clasifican en: información, software, activos físicos, personas, servicios e intangibles como reputación, imagen de la entidad, etc.

Borrado seguro: procedimiento de eliminación de archivos que no permite la recuperación posterior de éstos.

Centro de Servicios Informáticos - CSI: equipo responsable de gestionar las solicitudes de servicio relacionadas con las plataformas de tecnologías de información de la Personería Distrital de Cartagena de Indias.

Comité de Dirección de Seguridad de la Información: Equipo interdisciplinario, conformado por servidores públicos de la Personería Distrital de Cartagena de Indias, que es presidido por el Director de Informática. Su función principal es la de gobernar y orientar gestión de la seguridad de la información en la Personería Distrital de Cartagena de Indias.

Confidencialidad: Que la información solo sea accedida por las personas autorizadas para ello
Contratista externo: trabajador que sin tener una vinculación laboral directa con la Personería Distrital de Cartagena de Indias, presta sus servicios para la entidad (por ejemplo, a través de un contrato de prestación de servicios o por medio de una organización que tenga un contrato con la entidad).

Correo masivo: expresión usada en el presente manual de políticas para referirse a mensajes de correo electrónico enviado a 100 o más destinatarios que no formen parte de los dominios de la Personería Distrital de Cartagena de Indias.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

Criterio de seguridad de la información de la Personería Distrital de Cartagena de Indias: conjunto de requisitos técnicos que deben considerarse para la planeación e implementación segura de infraestructura y aplicaciones de tecnología de información, así como para su posterior verificación.

Custodio de la información: es el usuario de la información que ejerza funciones de administración de sistemas de información. Sus responsabilidades incluyen: Garantizar que se cumplan los niveles de servicio definidos.

Proporcionar asistencia al dueño de la información en la selección de soluciones técnicas apropiadas. Proveer operativamente el aseguramiento de la confidencialidad, integridad y disponibilidad de la información.

Derechos / Privilegios de acceso: conjunto de permisos dados a un usuario o a un sistema para acceder a un determinado recurso (repositorio información, aplicativo, datos).

Disponibilidad: La información estará lista para acceder a ella o utilizarse cuando se necesite.

Dispositivos móviles: son aparatos con algunas capacidades de procesamiento y de conectividad. Su principal característica es su movilidad. Los dispositivos móviles abarcan una gran variedad de equipos como: teléfonos inteligentes, asistentes digitales personales (PDA), tabletas, y computadoras portátiles.

Dueño de activo de información: (o propietario). Servidor público de nivel directivo cuyo rol implica entender qué tipo de información es mantenida, creada, procesada o eliminada; cómo la información se desplaza en su área de responsabilidad y quien debe acceder a la información y por qué. Como resultado, son capaces de entender e identificar los riesgos a la información. Tiene la



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

responsabilidad de asegurar la Clasificación de los activos y tomar decisiones sobre estos (por ejemplo: ubicación, acceso y controles de seguridad).

Entidad: término que se usa en el presente documento para identificar a la Personería Distrital de Cartagena de Indias. Cuando sea conveniente. Equipos de trabajo de informática: equipos de trabajo de la Personería Distrital de Cartagena de Indias que son responsables de desarrollar, desplegar, mantener, proteger y administrar las plataformas de tecnología de información.

Equipo de seguridad de la información: grupo funcional adscrito a la Dirección de Informática, cuya función primordial es la de gestionar la seguridad de la información para el alcance previsto del Sistema de Gestión de Seguridad de la Información SGSI de la Personería Distrital de Cartagena de Indias, buscando que el nivel de riesgo de la información de la entidad permanezca en niveles aceptables.

Evento de seguridad de la información: Presencia identificada del estado de un sistema, servicio o red, que indica una posible violación de las políticas de seguridad de la información, una falla de los controles, o una situación desconocida previamente que puede ser relevante para la seguridad.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. Todo incidente es un evento, más no todo evento es un incidente.

Integridad: La información debe estar completa y correcta en todo momento.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

Manual de protección de la información: Documento donde se establecen los lineamientos de seguridad para el manejo de la información de la Personería Distrital de Cartagena de Indias, en función de la clasificación de dicha información.

Plataforma de tecnologías de información / Plataforma de T.I.C.: Para propósitos del presente documento, las expresiones “plataforma de T.I.” y “plataforma de tecnologías de Información” hace referencia a todo el conjunto de recursos de tecnología de la información usados para generar, procesar, almacenar y transmitir información de la Personería Distrital de Cartagena de Indias. Lo que incluye por ejemplo: sistemas de información, equipos de escritorio, portátiles, sistemas operativos e infraestructura de red.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Confidencialidad: Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. Integridad: Propiedad de mantener la exactitud y estado completo de la información, en otras palabras, proteger la información para que no sea adulterada o alterada de forma indebida. Disponibilidad: Propiedad de mantener la información disponible y utilizable cuando lo requiera un individuo, proceso o entidad autorizada.

Seguridad informática: Rama de la seguridad de la información que se enfoca en la protección de la plataforma de tecnología de Información y de los datos que circulan, se procesan o almacenan en dicha plataforma.

Servidores Públicos: Término que se usa en el presente documento para identificar a empleados públicos, trabajadores oficiales y practicantes de la Personería Distrital de Cartagena de Indias.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

Sistema de Gestión de Seguridad de la Información - SGSI: Sistema de gestión basado en un enfoque hacia los riesgos, cuyo fin es establecer, implementar, operar, hacer, seguimiento, revisar, mantener y mejorar la seguridad de la información. El SGSI se rige por los requisitos de la norma internacional de gestión ISO/IEC 27001.

Software malicioso: (También, código malicioso). Es un tipo de software que tiene como objetivo infiltrar o dañar un equipo de cómputo o sistema de información sin el consentimiento de su propietario. El software malicioso incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo y crimeware. El término “software malicioso” también hace referencia a software hostil o molesto.

Usuario: Persona, proceso o aplicación de la entidad autorizada para acceder a la información de entidad o a los sistemas que la manejan.

Zonas restringidas de procesamiento: Son áreas, recintos o edificaciones ubicadas dentro de las sedes de la Personería Distrital de Cartagena de Indias, destinadas a alojar Plataformas de tecnología de la información, recursos importantes o información de la entidad; razón por la que requieren controles especiales de seguridad física y control de acceso.



PERSONERIA DISTRITAL DE
CARTAGENA

CODIGO: DE-P-007

GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO

VERSIÓN: 1

PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION

FECHA DE
APROBACIÓN(d-m-a):
30/01/2020

MARCO NORMATIVO

Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales". Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

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". Reglamentada parcialmente por el Decreto Nacional 103 de 2015.

Decreto Nacional 2573 de 2014 "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

Decreto 1078 del 26 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

La Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

La información es un activo estratégico para las operaciones diarias de la Personería Distrital y a su vez un factor determinante para el éxito de su plan de desarrollo. Por ello, la entidad está comprometida con la adopción de buenas prácticas de seguridad de la información tendientes a implementar, mantener y mejorar su Sistema de Gestión de Seguridad de la Información SGSI. Las Políticas y lineamientos de Seguridad de la Información y de las TI son de carácter obligatorio y deben ser conocidas y cumplidas por los servidores públicos, proveedores, contratistas y usuarios externos que hagan uso de la información y de los recursos tecnológicos de la entidad.

POLÍTICAS PARA SERVIDORES PÚBLICOS Y CONTRATISTAS EXTERNOS

Estas políticas aplican tanto a los procesos realizados directamente por la Personería Distrital de Cartagena de Indias, como a los ejecutados a través de contratos o acuerdos con terceros. Deben ser conocidas y cumplidas por los servidores públicos, proveedores, contratistas y usuarios externos de la entidad y de las sedes externas de la entidad que hagan uso de la información institucional y de sus recursos tecnológicos.

Comprende desde la explicación de los riesgos a los que están expuestos los activos de información, hasta la ejecución y seguimiento al cumplimiento de las normas y/o políticas informáticas. Las políticas de seguridad de la información también aplican para los servidores públicos en modalidad de teletrabajo.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

POLÍTICAS DE IDENTIFICACIÓN Y PROTECCIÓN DE LA INFORMACIÓN

Los activos de información dentro del alcance del Sistema de Gestión de Seguridad de la Información SGSI de la Personería Distrital de Cartagena de Indias, deben ser identificados, clasificados y definidos los responsables de cada uno de ellos. Busca asegurar que la información recibe el nivel de protección apropiado de acuerdo a la clasificación establecida.

IDENTIFICACIÓN Y CLASIFICACIÓN DE LA INFORMACIÓN

- Los activos de información deben ser identificados y registrados en un inventario.
- Los activos de información deben tener propietario designado. 1.1.1.3 El Propietario de un activo de información es responsable de: Definir los usuarios autorizados que pueden tener acceso al activo y sus privilegios de acceso. Determinar las clasificaciones correspondientes a la sensibilidad del activo. Asegurar que se gestione el riesgo de seguridad del activo. Establecer las reglas de uso del activo, cuando sea necesario. Solicitar la aplicación de controles para la protección del activo de información.
- Cada activo de información debe tener un custodio designado, quien ha de protegerlo mediante la aplicación y el mantenimiento de los controles de seguridad autorizados por el propietario.
- La información de la Personería Distrital de Cartagena de Indias se clasifica en: **Información pública**. Es toda información que la Personería Distrital de Cartagena de Indias, genere, obtenga, adquiera, o controle en su calidad de obligado. **Información clasificada**. Es aquella información que estando en poder o custodia de la Personería Distrital de Cartagena de Indias, en su



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

calidad de obligado, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional). **Información reservada.** Es aquella información que estando en poder o custodia de la Personería Distrital de Cartagena de Indias, en su calidad de obligado, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).

- El manejo de la información de la Personería Distrital de Cartagena de Indias debe seguir los lineamientos del Manual de Protección de la Información.
- Sólo se permite la transferencia de información Clasificada o Reservada cuando exista un acuerdo de confidencialidad o compromiso contractual que lo regule.
- La Personería Distrital de Cartagena de Indias, tiene control total sobre la información que se almacene en la infraestructura de tecnología de la información de la entidad; por lo tanto se reserva el derecho de mover, borrar, monitorear o tomar custodia de dicha información.
- Los servidores públicos y contratistas son responsables de proteger la información de su trabajo y solicitar a la Dirección de Informática el almacenamiento seguro de la información cuya pérdida pueda causar incumplimientos legales y/o la interrupción de los procesos de la entidad.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

POLÍTICA DE GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

En la Personería Distrital de Cartagena de Indias, la gestión de los riesgos fundamenta la toma de decisiones de seguridad de la información. Busca establecer la gestión del riesgo como eje principal de las actuaciones institucionales relacionadas con la seguridad de la información.

- Servidores públicos y contratistas de la Personería Distrital de Cartagena de Indias, deben identificar y reportar condiciones que podrían indicar la existencia de riesgos de seguridad informática.

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

En la Personería Distrital de Cartagena de Indias, los eventos e incidentes de seguridad de la información son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad. Busca establecer las líneas de actuación de los servidores públicos frente a la ocurrencia de situaciones que afecten la seguridad de la información.

Reporte de Eventos, Incidentes y Debilidades de la Seguridad Informática.

- Los servidores públicos y contratistas deben reportar inmediatamente al Centro de Servicios de Informática CSI, todas las situaciones que puedan afectar la seguridad de la información.
- La información específica sobre Incidentes o vulnerabilidades de seguridad de la información, así como el detalle de las medidas para proteger las Plataforma de T.I.C., debe ser tratada como información Reservada.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

POLÍTICA DE USO ADECUADO DE LOS RECURSOS DE LA PLATAFORMA DE TI

Toda la información de la Personería Distrital de Cartagena de Indias, así como los recursos para su procesamiento, almacenamiento y transmisión deben ser empleados únicamente para propósitos laborales o de la entidad; evitando su abuso, derroche, uso ilegal o desaprovechamiento.

- Lineamientos generales de la gestión del riesgo de seguridad informática
- Requerimientos generales para el uso adecuado de la plataforma de TI.
- Se prohíbe el uso de los recursos de plataforma de T.I. de la Personería Distrital de Cartagena de Indias para la realización de cualquier actividad ilegal. 1.4.1.2.
- Para verificar el cumplimiento de las presentes políticas; la Personería Distrital de Cartagena de Indias podrá monitorear y auditar las Plataforma de T.I.C. de la entidad que son facilitadas a servidores públicos y contratistas para el cumplimiento de sus deberes y funciones laborales.
- Los servidores públicos y contratistas deben abstenerse de crear, acceder, almacenar o transmitir material ilegal, pornográfico, que promueva la violación de los derechos humanos o que atente contra la integridad moral de las personas o de las instituciones.
- Está prohibida la realización de pruebas a los controles de seguridad de la información.
- No está permitido aprovechar las vulnerabilidades de seguridad de la plataforma de TI.
- Solamente el grupo de Seguridad de la Información o un tercero autorizado por la Dirección de Informática puede utilizar herramientas de diagnóstico de



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

la seguridad de la información (herramientas de hacking) sobre los activos de información de la Entidad.

- Los programas informáticos desarrollados o adquiridos por Personería Distrital de Cartagena de Indias, son para el uso exclusivo de la entidad.

Uso Adecuado del Correo Electrónico

- No está permitido enviar correos masivos sin la autorización del personal directivo de la dependencia.
- La Dirección de Informática podrá establecer los límites en la cantidad de destinatarios y el tamaño de los mensajes de correo electrónico.
- No está autorizado el envío de correos electrónicos con contenido que atente contra la integridad y la dignidad de las personas, así como con el buen nombre de la entidad.
- Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico se retire de la Personería Distrital de Cartagena de Indias, su cuenta de correo será desactivada.
- Las cuentas de correo electrónico son propiedad de la Personería Distrital de Cartagena de Indias, son asignadas para la realización tareas propias de las funciones laborales y no deben utilizarse para ningún otro fin.
- Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Entidad.
- Cuando se detecte un correo fraudulento, con fines maliciosos o con contenido sospechoso se debe informar esta situación al Grupo de seguridad de la Información o a la mesa de ayuda del Centro de Servicios Informáticos.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

Uso Adecuado de Equipos de Cómputo Asignados

- No está permitida la instalación, ejecución y/o utilización de software diferente al preinstalado en los equipos de cómputo o al instalado por integrantes de los equipos de trabajo de informática.
- Los parámetros de configuración del sistema operativo solo deben ser modificados por integrantes de los equipos de trabajo de informática.
- Uso adecuado de los servicios de red.
- No deben almacenarse archivos personales en carpetas de la red y demás servicios de almacenamiento en internet suministrados por la Personería Distrital de Cartagena de Indias.
- No se permite el uso de servicios de descarga o intercambio de archivos que funcionan bajo el esquema P2P (person to person).
- La Personería Distrital de Cartagena de Indias, podrá controlar y limitar la navegación a ciertos sitios, recursos o servicios de internet con el fin de proteger la seguridad y la disponibilidad del servicio de internet.
- No está permitido deshabilitar o evadir los controles de navegación en internet.
- En horarios laborales, está prohibido el uso del servicio de internet de la entidad para acceder a páginas de transmisión de películas, programas de televisión y eventos deportivos
- El acceso remoto a los equipos y dispositivos de la plataforma de T.I. solo está permitido para labores de soporte técnico autorizado.
- El acceso remoto a equipos de cómputo debe contar con la aprobación del servidor público o contratista responsable de dicho equipo.
- Solo se permite el acceso remoto a estaciones de trabajo de la entidad si el servidor público o contratista responsable del equipo de cómputo lo aprueba.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

- Solo está permitido el uso de servicios de almacenamiento de información suministrados por la entidad.
- La red de visitantes está dispuesta únicamente para las personas que visitan temporalmente la Personería Distrital de Cartagena de Indias.

Uso de Material Protegido por Derechos de Autor

- Se prohíbe el almacenamiento de archivos multimedia (videos, música, imágenes o libros electrónicos) y cualquier otro tipo de contenido que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en las carpetas de red y demás servicios de almacenamiento en internet suministrados por la entidad.
- Se prohíbe el almacenamiento, uso, instalación y/o ejecución de software que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) y/o licenciamiento en la plataforma tecnológica de la entidad.

POLÍTICA DE SEGURIDAD INFORMÁTICA PARA CONTRATACIÓN

La información de la Personería Distrital de Cartagena de Indias, debe ser protegida en el proceso de contratación. Busca proteger los procesos de contratación frente a situaciones que comprometan la disponibilidad, la integridad y la confidencialidad de la información de dichos procesos; resguardando así su legalidad y transparencia.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

Disposiciones Generales

- Los servidores públicos y contratistas responsables por los servicios de contratistas o proveedores, son responsables de identificar y valorar los riesgos de la información asociados al acceso de éstos.
- Los contratos celebrados entre la Personería Distrital de Cartagena de Indias y contratistas o proveedores con acceso a la información de la entidad, deben incluir cláusulas para mitigar riesgos de seguridad de la información.
1.5.1.3. Con el fin de proteger la información de ambas partes, se debe formalizar un acuerdo de confidencialidad. El acuerdo deberá definir claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir.
- Siempre que haya un proceso de selección que implique la entrega de información Clasificada o Reservada de la entidad, los proponentes participantes deben firmar previamente un acuerdo de confidencialidad.

POLÍTICA DE SEGURIDAD FÍSICA DE LA INFORMACIÓN Y LOS EQUIPOS DE CÓMPUTO.

Se debe brindar seguridad física a la información de la entidad y a los recursos de la plataforma de T.I., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidos de situaciones como acceso no autorizado, robo, destrucción o desconexión.

Se pretende proteger la información, así como las tecnologías de información y la comunicación de la entidad frente a incidentes de seguridad causados por condiciones inadecuadas protección física, sean estas ambientales o que faciliten el acceso indebido a los activos de información.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

Seguridad en las Instalaciones

- Fuera del horario laboral normal o cuando se alejen de sus estaciones de trabajo, los Servidores públicos y contratistas deben despejar sus pantallas, escritorios y áreas de trabajo, de tal manera que los datos, bien sean físicos (como documentos impresos y carpetas) o electrónicos (como memorias USB, Discos Duros Externos, CDs y DVDs), estén resguardados adecuadamente.
- Cuando un servidor público se percate de la presencia de personas sospechosas en las instalaciones de entidad, debe reportar dicha situación a la Dirección de Seguridad Interna.
- No se deben prestar ni descuidar los elementos de identificación y acceso a las instalaciones de la Personería Distrital de Cartagena de Indias (tales como tarjetas de acceso, carnets, llaves y tokens).
- Cuando se imprima información clasificada o reservada, las impresiones deben ser retiradas inmediatamente.
- Siempre que sea posible, las impresiones deben ser protegidas por medio de una clave de seguridad.
- No está permitido fumar, ingerir alimentos o bebidas en las aulas con equipos de cómputo.

Seguridad de los Equipos

- Los servidores públicos y contratistas de la Personería Distrital de Cartagena de Indias, son responsables de garantizar la debida protección de los equipos asignados (computadores de escritorio y dispositivos móviles) dentro y fuera de la entidad, lo que contempla su vigilancia, el debido cuidado en su transporte y el uso de cualquier otra medida de seguridad física necesaria.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

- Los equipos suministrados por la Personería Distrital de Cartagena de Indias, como computadores de escritorio y dispositivos móviles (incluye computadores portátiles), no deben ser objeto de alteraciones en su hardware. Toda modificación a los equipos debe ser autorizada y realizada por personal de soporte técnico de los equipos de trabajo de informática.
- Se debe bloquear la sesión cuando el usuario se aleje del computador.
- La salida de los computadores (de escritorio o portátiles) de la entidad debe ser autorizada por el secretario general.
- Toda pérdida de equipos de cómputo o de alguno de sus componentes, debe ser informada inmediatamente al centro de servicios informáticos CSI.
- Los equipos de cómputo externos (no entregados por la Personería Distrital de Cartagena de Indias) no deben conectarse a la red de datos de la entidad, a menos que cumplan con los requisitos definidos por la Dirección de Informática. (Requisitos por definir).

POLÍTICA DE CONTROL DE ACCESO A PLATAFORMAS DE TECNOLOGÍA DE LA INFORMACIÓN.

La Personería Distrital de Cartagena de Indias, otorga el nivel de acceso necesario a la información y su plataforma de T.I. para el cabal cumplimiento de las funciones de los servidores públicos y contratistas. Se busca evitar y mitigar riesgos que comprometan la confidencialidad de la información y de las plataformas T.I.C. institucionales.

Gestión de Acceso a Usuarios

- Los dueños de los sistemas de información deben verificar que los privilegios de acceso de los usuarios en las Plataformas de tecnología de la información se han otorgado de acuerdo con la necesidad laboral legítima.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

- Los privilegios de acceso otorgados a los usuarios de las Plataformas de tecnología de la información deben ser autorizados por el superior inmediato.
- 1.7.1.3. Los privilegios de acceso otorgados a los usuarios de las Plataformas de Tecnología de Información deben ser revisados al menos anualmente por los jefes inmediatos de los usuarios.
- No están permitidas las cuentas de usuarios genéricas para el ingreso a la Plataforma de T.I.
- Todas las cuentas de usuario son personales e intransferibles.
- Servidores públicos y contratistas de la Personería Distrital de Cartagena de Indias, deben reportar a su jefe cuando tengan más derechos de acceso de los necesarios.
- A excepción de las carpetas de red, los usuarios deben abstenerse de ingresar a los servidores de la plataforma tecnológica de la Personería Distrital de Cartagena de Indias, a menos que lo requieran en virtud de sus funciones laborales (como los Administradores de plataforma de T.I. de la entidad).
- En la eventualidad de requerirse el ingreso a un equipo o a alguna de las cuentas de los sistemas de información de la entidad asignadas a un servidor público ausente, el jefe directo respectivo será el único autorizado para solicitar el acceso.
- Los servidores públicos y contratistas son los responsables de todas las transacciones o acciones efectuadas con su cuenta de usuario.
- Ningún servidor público, contratista deberá acceder a la red o a los servicios de T.I.C. de la Personería Distrital de Cartagena de Indias, utilizando una cuenta de usuario diferente a la que le fue asignada.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

Manejo de Contraseñas

- Los usuarios de las Plataformas de Tecnologías de la Información de la Personería Distrital de Cartagena de Indias, deben abstenerse de escribir las contraseñas en medios físicos o electrónicos.
- Las contraseñas de acceso a las Plataformas de Tecnologías de la Información son personales e intransferibles, cada usuario es responsable de su uso y de preservar su confidencialidad.
- El préstamo de contraseñas está prohibido bajo cualquier circunstancia, en caso de hacerlo el usuario de la información responsable de la cuenta asume las consecuencias generadas por dicha situación.

POLÍTICA DE OPERACIÓN DE PLATAFORMAS DE TECNOLOGÍA DE INFORMACIÓN

La Personería Distrital de Cartagena de Indias, aplica controles para el funcionamiento correcto y seguro de las Plataformas de tecnología de la información y la comunicación.

Requisitos para la Planeación y Operación de las Plataformas de TI.

- Los componentes y sistemas de la infraestructura de seguridad de la información, no deben ser inhabilitados, desviados, apagados o desconectados sin la previa autorización de la Dirección de Informática.

Protección Contra Software Malicioso

- No está permitido el ingreso intencionado de software malicioso a los equipos y redes de la Personería Distrital de Cartagena de Indias.
- La presencia identificada o sospechada de software malicioso debe ser reportada al Centro de servicios de Informática CSI.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

Intercambio de Información

- Todo intercambio de información con terceras partes debe ser realizado de conformidad a lo dispuesto en el Manual de Protección de la Información.
- Personal de la mesa de ayuda del Centro de servicios Informáticos no está obligado a realizar procedimientos de recuperación de información borrada, debido a que no puede garantizarse la eficacia (el éxito) de la realización de estas actividades de recuperación.

POLÍTICAS DE CIFRADO DE LA INFORMACIÓN

Deben aplicarse mecanismos de cifrado cuando exista un alto riesgo de comprometer la confidencialidad de la información clasificada o reservada de la entidad. Busca establecer lineamientos tendientes a la protección de la confidencialidad de la información a través de mecanismos de cifrado.

- Servidores públicos y contratistas que sean responsables de llaves (o claves) de cifrado deben reportar al Equipo de Seguridad de la información, novedades acerca del manejo de dichas llaves (por ejemplo: cambio de dueños, cambio de custodia, pérdidas, acceso no autorizado).
- Cada vez que se utilice el cifrado, los servidores públicos y contratistas no deben borrar la única versión legible de los datos, a menos que hayan probado que el proceso de des-cifrado puede restablecer una versión legible de los datos.
- Se deben utilizar mecanismos de cifrado cuando se requiera el almacenamiento de información reservada o clasificada en medios removibles (como memorias USB, discos duros externos, CD y DVD).
- Se deben utilizar mecanismos de cifrado cuando se requiera enviar información reservada o clasificada a través de redes externas (internet).



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

POLÍTICA DE DISPOSITIVOS MÓVILES

El acceso a los datos y sistemas de información de la Personería Distrital de Cartagena de Indias, a través de dispositivos móviles debe ser realizado de forma regulada y controlada con el fin de evitar incidentes de seguridad de la información.

Computadores Portátiles

- Los usuarios que tengan bajo su responsabilidad computadores portátiles de la Personería Distrital de Cartagena de Indias, son responsables de su protección dentro y fuera de las instalaciones de la entidad.
- Todo usuario al que se le asigne o facilite un computador portátil de la Personería Distrital de Cartagena de Indias, debe asegurarlo adecuadamente al puesto de trabajo con la guaya de seguridad.
- Los usuarios de computadores portátiles de la Personería Distrital de Cartagena de Indias, deben emplear medidas de seguridad para su adecuado manejo fuera de las instalaciones de la entidad.

Dispositivos Móviles Diferentes a Computadores Portátiles.

Esta sección hace referencia a dispositivos como teléfonos móviles inteligentes y tabletas.

- Los usuarios de dispositivos móviles entregados por la Personería Distrital de Cartagena de Indias, son responsables de su protección dentro y fuera de las instalaciones de la entidad.
- Los usuarios de dispositivos móviles entregados por la Personería Distrital de Cartagena de Indias, deben abstenerse de modificar las configuraciones de seguridad de dichos dispositivos.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

- Los usuarios de dispositivos móviles entregados por la Personería Distrital de Cartagena de Indias, deben reportar inmediatamente el robo o pérdida de dicho dispositivo al personal de los equipos de trabajo de informática.
- No está permitido el envío de información Clasificada o Reservada a través de servicios de mensajería instantánea no institucionales.
- La Personería Distrital de Cartagena de Indias, no está obligada a prestar soporte técnico a dispositivos móviles que sean de propiedad de los usuarios o cualquier otro que no sea propiedad de la entidad.
- Los usuarios que accedan a los servicios de la plataforma de T.I. (por ejemplo, al correo electrónico) a través de un dispositivo móvil propio, deben reportar inmediatamente el robo, cambio o pérdida de dicho dispositivo al centro de servicios informáticos CSI.

POLÍTICA DE CUMPLIMIENTO

La Personería Distrital de Cartagena de Indias, cumple la regulación y legislación vigente aplicable en materia de seguridad de la información. Busca identificar y asegurar el cumplimiento de los requisitos regulatorios y legales aplicables a la entidad en cuanto a la seguridad de la información.

Cumplimiento Legal y Normativo

- Será sancionado con las acciones disciplinarias y legales correspondientes, al que utilizare registros informáticos, software u otro medio para ocultar, alterar o distorsionar información requerida para una actividad de la entidad, para el cumplimiento de una obligación respecto al Estado o para ocultar los estados contables o la situación de un proceso, área o persona física o jurídica.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

- Toda la información de ciudadanos o servidores públicos y contratistas que incluya cédulas de identidad, datos de contacto o información financiera debe ser sólo accesible al personal de la entidad que necesite ese acceso en virtud de su trabajo.
- La realización de auditorías (verificaciones o pruebas de seguridad) no deben afectar la normal operación de los sistemas de información o plataformas.

POLÍTICAS PARA EL PERSONAL DE LOS EQUIPOS DE TRABAJO DE INFORMÁTICA

Estas Políticas aplican exclusivamente a personal de los equipos de Informática de la Personería Distrital de Cartagena de Indias ya sea interno o externo, en el ámbito del proceso de Planeación y Administración de las TI.

POLÍTICA DE GESTIÓN DEL RIESGO DE SEGURIDAD INFORMÁTICA

En la Personería Distrital de Cartagena de Indias, la gestión de los riesgos fundamenta la toma de decisiones de seguridad de la información. Busca establecer la gestión del riesgo como eje principal de las actuaciones institucionales relacionadas con la seguridad de la información.

Lineamientos Generales de la Gestión del Riesgo de Seguridad Informática

- Se deben identificar los riesgos a los que se encuentran expuestos los activos de información de la entidad.
- Los criterios de evaluación y aceptación de riesgos de seguridad de la información deben estar alineados con los criterios y políticas de gestión del riesgo de la entidad.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

- Los riesgos de seguridad de la información analizados deben ser objeto de tratamiento (mitigar, transferir, evitar, aceptar), dicho tratamiento debe ser coherente con los criterios de aceptación de riesgos.
- Los riesgos deben ser monitoreados después de su tratamiento para asegurar que siguen estando en niveles aceptables para la entidad.
- En los casos que se realice la estimación económica de los riesgos, se debe asegurar que el valor de la aplicación de medidas de mitigación sea inferior al costo de las consecuencias de la materialización de los riesgos.

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

En la Personería Distrital de Cartagena de Indias, los eventos e incidentes de seguridad de la información son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad. Busca establecer las líneas de actuación de los servidores públicos frente a la ocurrencia (confirmada o sospechada) de situaciones que afecten la seguridad de la información.

Gestión de Incidentes de Seguridad de la Información.

- Debe conformarse y mantenerse un equipo multidisciplinario para la respuesta y tratamiento a los incidentes de seguridad de la información.
- La atención de incidentes debe seguir el procedimiento descrito en el sistema de gestión de la calidad Gestión de Peticiones de Servicios e Incidentes.

POLÍTICA DE SEGURIDAD INFORMÁTICA ASOCIADA A CONTRATISTAS

La información de la Personería Distrital de Cartagena de Indias, debe ser protegida de los riesgos generados por el manejo o acceso de contratistas y proveedores. Busca mantener la seguridad de los activos de información accedidos por



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

contratistas, evitando situaciones como: Abuso de privilegios de acceso. Fuga de información. Negación de responsabilidades de incidentes de seguridad por parte del contratista.

- Requisitos de seguridad de la información asociados a contratistas y terceros Solamente cuando se demuestre la necesidad de su uso y esté expresamente autorizado por el propietario del activos de información o sistema de información respectivo.
- Únicamente debe concederse acceso remoto a plataformas de TI a contratistas y proveedores cuando estos tengan una necesidad legítima que lo justifique.
- El tercero que ejerza funciones de administración y soporte de sistemas de información, debe garantizar que se generan registros automáticos (los de auditoría) de dichas labores.

SEGURIDAD FÍSICA DE LA INFORMACIÓN Y LOS EQUIPOS DE CÓMPUTO

Se debe brindar seguridad física a la información de la entidad y a los recursos de la plataforma de T.I., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidos de situaciones como acceso no autorizado, robo, destrucción o desconexión. Se busca proteger la información, así como las tecnologías de información y la comunicación de la entidad frente a incidentes de seguridad causados por condiciones inadecuadas protección física, sean estas ambientales o que faciliten el acceso indebido a los activos de información.


Zonas Restringidas de Procesamiento

Se deben identificar y especificar las zonas restringidas de procesamiento de la Personería Distrital de Cartagena de Indias, destinadas a alojar equipos y dispositivos de la plataforma de T.I. de la entidad.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

	GESTIÓN DE DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 1
	PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	FECHA DE APROBACIÓN(d-m-a): 30/01/2020

- Cada zona restringida de procesamiento debe tener un responsable. 2.4.1.3. Las zonas restringidas de procesamiento deben contar al menos con mecanismos de control de acceso y vigilancia.
- Se deben definir las reglas para el trabajo al interior de las zonas restringidas de procesamiento, dichas reglas deben ser documentadas y publicadas en un lugar visible de cada una de estas zonas.
- Todo sistema, equipo, dispositivo, o medio crítico para la transmisión, procesamiento y almacenamiento de la información de la Personería Distrital de Cartagena de Indias, debe ser ubicado dentro de zonas restringidas de procesamiento. Si no se pudiera ubicar algún equipo dentro de estas zonas, dicho equipo debe ser objeto de controles complementarios de acceso físico.
- Sólo personal autorizado por el responsable de cada zona restringida de procesamiento puede ingresar a dicha zona.

Seguridad Física de los Equipos

- Siempre que se reutilice un servidor, computador portátil o un computador de estación de trabajo, se requiere la realización previa de un formateo de la información almacenada en dichos equipos antes que sean entregados a los nuevos usuarios.
- Debe realizarse Borrado Seguro de los equipos de forma previa al proceso de disposición final (por ejemplo: venta, donación o destrucción).
- Los servidores deben estar ubicados de modo que se reduzcan los riesgos generados por amenazas del entorno (es decir, evitando daños derivados de situaciones como manifestaciones sociales, inundaciones, humedad o incendio).



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

- Todos los equipos de procesamiento críticos deben tener controles para evitar caídas de la plataforma de TI causadas por fallas en el servicio eléctrico.

CONTROL DE ACCESO A PLATAFORMAS DE TECNOLOGÍA DE LA INFORMACIÓN

La Personería Distrital de Cartagena de Indias, otorga el nivel de acceso a la información necesario para el cabal cumplimiento de las funciones. Busca evitar y mitigar riesgos que comprometan la confidencialidad de la información y de las plataformas T.I.C. institucionales.

Proceso de Control de Acceso

- Todo proceso de control de acceso debe tener un responsable de su gestión.
- 2.5.1.2. La gestión del proceso de control de acceso debe comprender las actividades de solicitud, aprobación, asignación, modificación y revocación del acceso.
- Cuando aplique, las medidas de control de acceso a las plataformas de tecnología de la información deben cumplir el Criterio de seguridad de la información.

Gestión de Acceso a Usuarios

- Las cuentas de administración de las Plataformas de tecnología de la información sólo deben ser usadas cuando sea necesario dicho privilegio.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

Manejo de Contraseñas

- Los nombres de usuario y contraseñas se rigen por el Criterio de seguridad de la información de la Personería Distrital de Cartagena de Indias.
- No se permite el uso de contraseñas fijas. Todos los funcionarios sin excepción deben cambiar su password según lo establecido en el Criterio de seguridad de la Información.
- Las contraseñas de administración de las Plataforma de T.I.C. de tener un tiempo de caducidad, o en su defecto, deben ser cambiadas periódicamente. El periodo de vigencia de las contraseñas de administración de plataforma de T.I. se establece en el Criterio de Seguridad de la Información. (A desarrollar por la entidad).

OPERACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

La Personería Distrital de Cartagena de Indias, aplica controles para el funcionamiento correcto y seguro de las Plataformas de tecnología de la información y Telecomunicaciones. Busca proteger la operación de las plataformas de T.I.C. institucionales, garantizando la continuidad y la seguridad de los procesos institucionales.

Requisitos para la Planeación y Operación de las Plataformas de TI

Toda intervención a las Plataformas de Tecnologías de la Información que impliquen modificaciones o cambios debe ser ejecutada de conformidad a lo establecido en el procedimiento de control de cambios.

- La realización de auditorías, verificaciones o pruebas de seguridad de la información no deben afectar la normal operación de las Plataformas de tecnología de la información.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

- Protección contra software malicioso y móvil. 2.6.2.1. La plataforma de T.I de la Personería Distrital de Cartagena de Indias. Debe ser objeto de protección frente software malicioso.

Respaldo de la Información

- La información importante de la entidad alojada en los repositorios de red y los sistemas de información críticos deben ser respaldados a intervalos programados.
- Los respaldos de información deben ser probados regularmente, para verificar que la información si es recuperable ante un incidente.
- Los respaldos de información deben almacenarse además en un lugar externo a la Personería Distrital de Cartagena de Indias, evitando que ante la posibilidad de un desastre al interior de la misma, se pierda por completo la información.

Intercambio de Información

- Las direcciones IP internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la entidad, deberán ser considerados y tratados como información clasificada.
- La creación de una conexión directa entre las Plataformas de tecnología de la información de la Personería Distrital de Cartagena de Indias y las organizaciones externas a través de Internet o cualquier otra red pública, debe estar autorizada por el Grupo de Seguridad de la Información.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Los aplicativos y sistemas de información de la Personería Distrital de Cartagena de Indias, deben ser asegurados en sus fases de planeación, adquisición, desarrollo, implementación y operación. Se busca mitigar los riesgos de seguridad asociados a la existencia de seguridad en los aplicativos y sistemas de información de la entidad.

Requerimientos de Seguridad de los Sistemas de Información

- Durante la etapa de definición de requisitos para desarrollar, adquirir o modificar un aplicativo, se deben especificar claramente todos aquellos requisitos concernientes a la seguridad. Debe existir un registro que evidencie la documentación de tales requisitos.

DISPOSITIVOS MÓVILES

El acceso a los datos y sistemas de información de la Personería Distrital de Cartagena de Indias, a través de dispositivos móviles debe ser realizado de forma regulada y controlada con el fin de evitar incidentes de seguridad de la información. Busca evitar que las actividades de teletrabajo generen situaciones que amenacen la disponibilidad, la integridad y la confidencialidad de la información de la Personería Distrital de Cartagena de Indias.

Computadores portátiles

- Los computadores portátiles de la entidad deben tener instalada una herramienta de cifrado de datos que impida la fuga de información en caso de robo, pérdida o intentos de acceso no autorizado al equipo



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

ACTIVIDADES

El Plan de Tratamiento de riesgos de seguridad y privacidad de la información está compuesto por las siguientes actividades:

1. PROGRAMACIÓN Y AGENDAMIENTO DE ENTREVISTAS.

En esta fase se seleccionan los procesos incluidos en el alcance del SGSI de la Personería distrital Cartagena Indias y se procede a programar y a agendar a los líderes de proceso para la notificación de riesgos.

2. ENTREVISTA CON LOS LÍDERES DE PROCESO

La entrevista a cada líder de proceso, se explica la metodología y en conjunto se procede a realizar identificación de los riesgos, los cuales se consignan en la Matriz de Riesgos.

3. IDENTIFICACIÓN Y CALIFICACIÓN DE RIESGOS

Esta fase, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.

4. VALORACIÓN DEL RIESGO RESIDUAL

En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

5. MAPAS DE CALOR DONDE SE UBICAN LOS RIESGOS

Luego se procede a ubicar los riesgos en un mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

6. PLAN DE TRATAMIENTO DE RIESGOS

Cada líder de proceso debe implementar el plan de tratamiento de riesgos propuesto.

7. SEGUIMIENTO Y CONTROL

Seguimiento y control se realiza de acuerdo a la GUÍA PARA LA ADMINISTRACIÓN DE RIESGO -S-GC-06.



**PERSONERIA DISTRITAL DE
CARTAGENA**

CODIGO: DE-P-007

**GESTIÓN DE DIRECCIONAMIENTO
ESTRATEGICO**

VERSIÓN: 1

**PLAN DE TRATAMIENTO DE RIESGO
DE SEGURIDAD Y PRIVACIDAD DE
LA INFORMACION**

**FECHA DE
APROBACIÓN(d-m-a):
30/01/2020**

CRONOGRAMA

No	ACTIVIDAD	RESPONSABLE	FECHA IMPLEMENTACIÓN	VALORACIÓN
1	Agendamiento de entrevistas a líderes de proceso	Área de Sistemas	Febrero 2023	10%
2	Entrevistas con los líderes de procesos.	Área de Sistemas	Febrero 2023	10%
3	Identificación de los riesgos.	Área de Sistemas	Marzo 2023	10%
4	Valoración de los riesgos.	Área de Sistemas	Marzo 2023	10%
5	Mapa de calor para ubicar los riesgos encontrados	Área de Sistemas	Marzo 2023	20%
6	Socializar el plan de tratamiento de riesgos de seguridad y privacidad de la información	Área de Sistemas	Abril 2023	10%
7	Realizar seguimiento al plan de tratamiento de riesgos seguridad y privacidad de la información.	Área de Sistemas	Mayo – Agosto – noviembre 2023	30%