POLÍTICA DE SEGURIDAD DIGITAL

ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

Salvemos Juntos a Cartagena

Alcaldía Distrital De Cartagena de Indias - Bolívar

Dirección: Centro diagonal 30 # 30 - 78 Plaza de la Aduana.
(57) + (5) 6411370 - Línea Gratuita: 018000 415 393
alcalde@cartagena.gov.co / atencionalciudadano@cartagena.gov.co

CONTROL DE CAMBIOS

VERSIÓN	DESCRICPCION DE CAMBIOS
1.0	Elaboración de Documento.

Contenido

1 INTRODUCCION

La Política de Seguridad Digital es la declaración general que representa la posición de la administración de La **Alcaldía Distrital de Cartagena de Indias** con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Alcaldía Distrital de Cartagena de Indias y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

En cumplimiento a lo estipulado en el Modelo Integrado de planeación y gestión MIPG el cual es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos , con integridad y calidad en el servicio, incorpora la política de seguridad digital en el marco de la tercera dimensión: Gestión con valores para resultados, La implementación de la política, se hará a través de la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital.

El comité de Gestión y Desempeño Institucional, con el objeto de articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política de Gobierno Digital designó como responsable de la Seguridad Digital y de la Seguridad de la Información en la entidad, a la Oficina Asesora de Informática.

La implementación de la política por parte del Distrito de Cartagena se hará a través de la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital.

2 MARCO JURÍDICO

La Política de Seguridad Digital se enmarca en la normatividad que se relaciona a continuación:

Norma	Número	Fecha	Detalle
Ley	2080	2021	Establece los lineamientos de uso de medios electrónicos en los procedimientos administrativos de las entidades públicas
Resolución	1519	2020	Define los estándares y directrices para publicar la información señalada en la ley 1712 del 2014 (transparencia y acceso a información pública) y se define los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos.
Ley	2052	2020	Implementar los servicios ciudadanos digitales Crear, diseñar o adecuar los mecanismos de intercambio de información de los sistemas y soluciones tecnológicas que soportan sus trámites, dando cumplimiento al marco de interoperabilidad y los lineamientos de vinculación al servicio de interoperabilidad de los servicios ciudadanos digitales.
Decreto	620	2020	Reglamenta parcialmente los artículos 53, 54. 60, 61 y 64 de la Ley 1437 de 2011, los literales e, j y el parágrafo 2º del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019. y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución	2893	2020	La presente resolución tiene por objeto expedir: los lineamientos para estandarizar las ventanillas únicas, portales de programas transversales y unificación de sedes electrónicas del Estado colombiano; la guía técnica de integración de sedes electrónicas; la guía técnica de integración de ventanillas únicas; la guía técnica de integración de portales específicos de programas transversales del Estado , y la Guía Técnica de Integración de Trámites, Otros Procedimientos Administrativos (OPAs) y Consultas de Acceso a Información Pública.
Resolución	2160	2020	Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos
Ley	1955	2019	Plan Nacional de Desarrollo 2018-2020
Decreto	2106	2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública
Directiva Presidencial	02	2019	Simplificación de la interacción digital entre los ciudadanos y el Estado
Ley	1978	2019	Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones
Decreto	1008	2018	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones
Decreto	704	2018	Por el cual se crea la Comisión Intersectorial para el Desarrollo de la Economía Digital y se adiciona un artículo en el título 2 de la parte 1 del libro 1 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015
Resolución	1443	2018	Por la cual se sustituyen los artículos 15 y 19 y se modifica el artículo 17 de la Resolución No 2405 de 2016 (Sello de excelencia de Gobierno Digital)
Decreto	415	2016	La definición de estrategias, políticas, planes, objetivos, metas, estándares y lineamientos en materia de Tecnologías de la Información y las Comunicaciones que adopte cada sector, organismo o entidad, deberán estar articuladas con el Plan Nacional de Desarrollo, los planes de desarrollo sectorial y con la estrategias, políticas, planes, estándares, programas y lineamientos que para el efecto establezca el Ministerio de Tecnologías de la Información y las Comunicaciones.
Resolución	2405	2016	El modelo del Sello de Excelencia Gobierno en Línea en Colombia se rige por los principios de colaboración, participación, gratuidad, imparcialidad, buena fe, responsabilidad, apertura, publicidad, seguridad y privacidad de la información, calidad y transparencia, consagrados en los artículos 209 de la Constitución

			Política, 3° de la Ley 489 de 1998, 3 de la Ley 1437 de 2011 y 2.2.9.1.1.4 del Decreto número 1078 del 2015.
Decreto	1166	2016	El presente capítulo regula la presentación, radicación y constancia de todas aquellas peticiones presentadas verbalmente en forma presencial, por vía telefónica, por medios electrónicos o tecnológicos o a través de cualquier otro medio idóneo para la comunicación o transferencia de la voz.
Decreto Único Sectorial	1078	2015	Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones: http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf
Ley Estatutaria	1757	2015	Presente ley es promover, proteger y garantizar modalidades del derecho a participar en la vida política, administrativa, económica, social y cultural, y así mismo a controlar el poder político.
Decreto Reglamentario Único	1081	2015	Regula íntegramente las materias contempladas en él. Por consiguiente, de conformidad con el artículo 3 de la Ley 153 de 1887, quedan derogadas todas las disposiciones de naturaleza reglamentaria relativas al sector Presidencia de la República que versan sobre las mismas materias, con excepción, exclusivamente.
Decreto	103	2015	El Ministerio de Tecnologías de la Información y las Comunicaciones a través de la estrategia de Gobierno en Línea expedirá los lineamientos que deben atender los sujetos obligados para cumplir con la publicación y divulgación de la información señalada en la Ley 1712 de 2014, con el objeto de que sean dispuestos de manera estandarizada.
Resolución	3564	2015	Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública: http://estrategia.gobiernoenlinea.gov.co/623/articles-8240_esquema_ley1712.pdf
Acuerdo del Archivo General de la Nación	3	2015	El presente Acuerdo tiene como objeto reglamentar la gestión de documentos electrónicos en las entidades del Estado, generados y recibidos como resultado del uso de medios electrónicos en los procedimientos administrativos, de conformidad con lo establecido en el Título IV de la Ley 1437 de 2011.
Decreto	1074	2015	Este Decreto regula íntegramente las materias contempladas en él. Por consiguiente, de conformidad con el arto 3 de la Ley 153 de 1887, quedan derogadas todas las disposiciones de naturaleza reglamentaria relativas al sector Comercio, Industria y Turismo que versen sobre las mismas materias
Acuerdo	003	2015	Archivo General de la Nación
Decreto	1080	2015	Decreto Único Reglamentario del Sector Cultura
Ley	1753	2015	Plan nacional de desarrollo 2014-2018 "Todos por un nuevo país"
Decreto	2573	2014	Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad.
Ley	1712	2014	Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública: http://www.mintic.gov.co/portal/604/articles-7147_documento.pdf
Decreto	333	2014	Define el régimen de acreditación de las entidades de certificación, en desarrollo de lo previsto en el artículo 160 del Decreto-ley 19 de 2012
Ley estatutaria	1618	2013	Las entidades públicas del orden nacional, departamental, municipal, distrital y local, en el marco del Sistema Nacional de Discapacidad, son responsables de la inclusión real y efectiva de las personas con discapacidad, debiendo asegurar que todas las políticas, planes y programas, garanticen el ejercicio total y efectivo de sus derechos, de conformidad con el artículo 3° literal c), de Ley 1346 de 2009.
Decreto	2693	2012	Definir los lineamientos, plazos y términos para 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 eficiente, más transparente y participativo y que preste mejores servicios con la colaboración de toda la sociedad.
Decreto	019	2012	Los trámites, los procedimientos y las regulaciones administrativas tienen por finalidad proteger y garantizar la efectividad de los derechos de las personas naturales y jurídicas ante las autoridades y facilitar las relaciones de los particulares con estas como usuarias o destinatarias de sus servicios de conformidad con los principios y reglas previstos en la Constitución Política y en la ley.

NTC	5854	2012	Esta norma tiene por objeto establecer los requisitos de accesibilidad que se deben implementar en las páginas web en los niveles de conformidad A, AA y AAA.
Decreto	2364	2012	1.Acuerdo sobre el uso del mecanismo de firma electrónica 2. Datos de creación de la firma electrónica 3.Firma electrónica. Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, 4.Firmante.
Ley Estatutaria	1581	2012	La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
Decreto	235	2010	La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones" y que "las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado.
Ley	1341	2009	La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.
Circular de la Procuraduría General de la Nación	058	2009	Por la cual se expiden disposiciones para adelantar el programa de renovación de la administración pública y se otorgan unas facultades extraordinarias al Presidente de la Republica", en su artículo 14 dispone que el Gobierno Nacional promoverá el desarrollo de tecnologías y procedimientos denominados gobierno electrónico o en línea en las entidades de la rama ejecutiva del orden nacional y. en consecuencia. impulsara y realizara los cambios administrativos, tecnológicos e institucionales relacionados con el desarrollo de: la contratación pública con soporte electrónico, los portales de información y la prestación de servicios, así como de la participación ciudadana y sistemas intra gubernamentales de flujo de información.
Ley	1273	2009	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.
Decreto	1151	2008	El objetivo es contribuir con la construcción de un Estado más eficiente, más transparente y participativo, y que preste mejores servicios a los ciudadanos y a las empresas, a través del aprovechamiento de las Tecnologías de la Información y la Comunicación.
Ley	1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones
Ley	962	2005	Facilitar las relaciones de los particulares con la Administración Pública, de tal forma que las actuaciones que deban surtirse ante ella para el ejercicio de actividades, derechos o cumplimiento de obligaciones se desarrollen de conformidad con los principios establecidos en los artículos 83, 84, 209 y 333 de la Carta Política. En tal virtud, serán de obligatoria observancia los siguientes principios como rectores de la política de racionalización, estandarización y automatización de trámites, a fin de evitar exigencias injustificadas a los administrados: 1. Reserva legal de permisos, licencias o requisitos 2. Procedimiento para establecer los trámites autorizados por la ley 3. Información y publicidad 4. Fortalecimiento tecnológico

Ley	892	2004	Por la cual se establecen nuevos mecanismos de votación e inscripción para garantizar el libre ejercicio de este derecho, en desarrollo del artículo 258 de la Constitución Nacional.
Ley	906	2004	Por la cual se expide el Código de Procedimiento Penal. (Corregida de conformidad con el Decreto 2770 de 2004
Conpes	3292	2004	Proyecto de racionalización y automatización de trámites que tiene por objetivo establecer un marco de política para que las relaciones del gobierno con los ciudadanos y empresarios sean más transparentes, directas y eficientes, utilizando estrategias de simplificación, racionalización, normalización y automatización de los trámites ante la administración pública
Decreto	3107	2003	Suprímase en el Departamento Administrativo de la Presidencia de la República el Programa Presidencial para el Desarrollo de las Tecnologías de la Información y de las Comunicaciones
Ley	794	2003	Gratuidad de la justicia civil. El servicio de la justicia civil que presta el Estado es gratuito, con excepción de las expensas señaladas en el arancel judicial para determinados actos de secretaría. Las partes tendrán la carga de sufragar los gastos que se causen con ocasión de la actividad que realicen, sin perjuicio de lo que sobre costas se resuelva
Conpes	3248	2003	Renovación de la Administración Pública
Decreto	3816	2003	Créese la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública.
Acto legislativo	01	2003	Uso de medios electrónicos e informáticos para el ejercicio del derecho al sufragio
Ley	812	2003	Renovación de la Administración Pública
Ley	734	2002	Por el cual se expide el Código Disciplinario Único
Directiva Presidencial	No. 10	2002	Programa de renovación de la Administración Pública: hacía un Estado Comunitario
Ley	790	2002	Renovar y modernizar la estructura de la rama ejecutiva del orden nacional, con la finalidad de garantizar, dentro de un marco de sostenibilidad financiera de la Nación, un adecuado cumplimiento de los Fines del Estado con celeridad e inmediación en la atención de las necesidades de los ciudadanos, conforme a los principios establecidos en el artículo 209 de la C.N. y desarrollados en la Ley 489 de 1998
Decreto	127	2001	Por el cual se crean las Consejerías y Programas Presidenciales en el Departamento Administrativo de la Presidencias de la República
Conpes	3072	2000	Este documento presenta a consideración del CONPES la “Agenda de Conectividad”, que busca masificar el uso de las Tecnologías de la Información y con ello aumentar la competitividad del sector productivo, modernizar las instituciones públicas y de gobierno, y socializar el acceso a la información, siguiendo los lineamientos establecidos en el Plan Nacional de Desarrollo 1998 – 2002 "Cambio para Construir la Paz"
Directiva	2	2000	Plan de acción de la estrategia gobierno en línea
Ley	594	2000	La presente ley tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado.
Decreto	1747	2000	Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.
Ley	527	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
Conpes	2790	1995	Estrategia diseñada para el mejoramiento de la gestión pública en torno al cumplimiento de los objetivos del Plan Nacional de Desarrollo.
Decreto Ley	2150	1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la administración pública
Ley	57	1985	Publicidad de los actos y documentos oficiales

3 MARCO CONCEPTUAL

Aceptación del Riesgo: Decisión de aceptar un riesgo.

Activo: Según [ISO IEC13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales, estratégicos, operativos o de apoyo de la Alcaldía Distrital de Cartagena de Indias.

Alcance: Ámbito de la organización que queda sometido a la POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Según [ISO IEC13335-1:2004]: causa potencial de un incidente, el cual puede dar como resultado un daño a la entidad.

Análisis de riesgos: Según [ISO IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Aplicaciones: Es todo el software que se utiliza para la gestión de la información. Ejemplo: PREDIS, MATEO, COPSIS, CERTICO, SIGOB.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES de una organización.

Autenticación: Proceso que tiene por objetivo validar la identificación de una entidad o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, Propiedad que garantiza que la identidad de un sujeto o recurso es la que manifiesta.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los

estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas

Compromiso de la alta gerencia: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES.

Confiabilidad: la capacidad de un producto de realizar su función de la manera esperada.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO IEC13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

COPSIS: Sistema de Contratación de OPS

Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la Alcaldía Distrital de Cartagena de Indias. Ejemplo: archivo de Word “listado de personal.docx”

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Según [ISO IECTR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: es un activo, esencial para las actividades de una organización.

Instalaciones: Son todos los lugares en los que se almacenan o utilizan los sistemas de información. Ejemplo: Oficina Pagaduría.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance de la POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS

COMUNICACIONES, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IPS: Sistema de prevención de intrusos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de julio de 2007. No es certificable.

ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para una POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005.

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de julio de 2007.

ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

ISO IECTR 13335-3: "Information technology. Guidelines for the management of IT Security Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

ISO IECTR 18044: "Information technology. Security techniques. Information security incident management". Guía de utilidad para la gestión de incidentes de seguridad de la información.

ITIL IT Infrastructure Library: Un marco de gestión de los servicios de tecnologías de la información.

Keyloggers: Aplicaciones que registran el teclado efectuado por un usuario.

Legalidad: El principio de legalidad o Primacía de la ley, es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

Lista de chequeo: apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación de la POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES para facilitar su desarrollo.

Medida correctiva: Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación de la POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES con el fin de prevenir su repetición.

Medida preventiva: Medida de tipo pro-activo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación de la POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

MSPI: Modelo de seguridad y privacidad de la información

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

OAI: Oficina Asesora de Informática

Personal: Son todos los funcionarios de la Alcaldía Distrital de Cartagena de Indias, el personal subcontratado, aprendices, practicantes y peticionarios, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la Alcaldía Distrital de Cartagena de Indias.

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Política dé escritorio despejado: La política de la empresa que indica a los funcionarios, contratista y demás colaboradores de la Alcaldía Distrital de Cartagena de Indias, que deben dejar su escritorio libre de cualquier tipo de información que puede ser usada para perjudicar a la entidad.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO IEC27002:20005): intención y dirección general expresada formalmente por la Dirección.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican

Riesgo: Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual: Según [ISO IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

Salvaguarda: Véase: Control.

Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Según [ISO IEC27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SIGOB: Sistema de Gestión y Seguimiento a las Metas de Gobierno.

Terceros: Toda persona natural o jurídica que tenga una relación directa o indirecta con la Alcaldía Mayor de Cartagena de Indias

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de la Alcaldía Distrital de Cartagena de Indias, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la Alcaldía Distrital de Cartagena de Indias y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: Según [ISO IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Virus: tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

Vulnerabilidad: Según [ISO IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

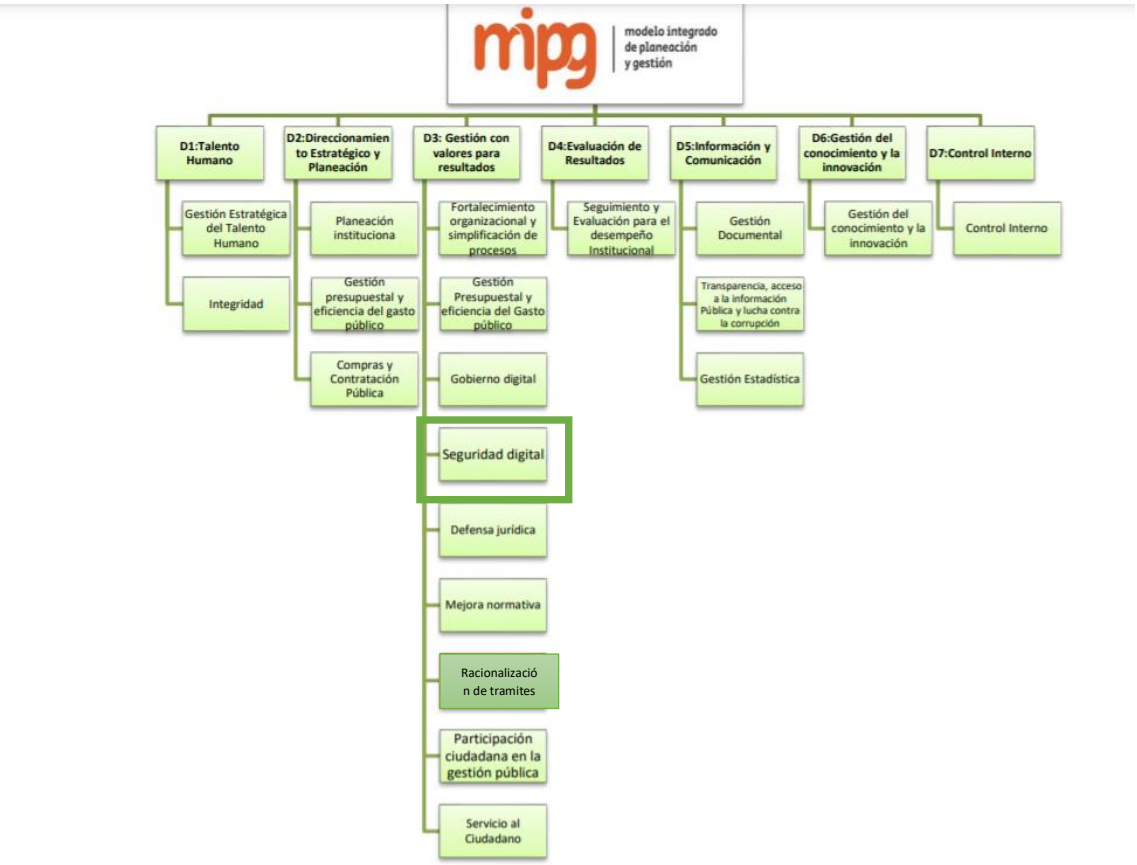
4 CONTEXTO ESTRATEGICO DE LA ENTIDAD

Con la expedición del Decreto 1499 de 2017 y el Manual Operativo de MIPG se debe elaborar e implementar la Política de seguridad digital en cada una de las entidades públicas, la cual hace parte integral de la Dimensión Gestión con Valores para Resultados, en este sentido, la Alcaldía de Cartagena, y bajo el liderazgo de la Oficina Asesora de Informática, establece la política estableciendo en ella los lineamientos para garantizar la seguridad y la privacidad de la información.

La Alcaldía de Cartagena, cuenta con un proceso de seguridad informática mediante el cual se realiza la verificación de las bases de datos y se establecen controles para el acceso a las mismas, sin embargo, las medidas establecidas requieren del liderazgo de todas las dependencias responsables de la emisión de la información.

5 ESTRUCTURA GENERAL DE LA POLITICA

5.1 DIMENSIÓN



5.2 DECLARACIÓN DE LA POLÍTICA

La Alcaldía Mayor de Cartagena de indias establece estrategias para el ***amparo de los activos de información, legitimar la confidencialidad, integridad y disponibilidad de los mismos***, emitiendo los lineamientos con respecto a la protección de los activos de información incluido el hardware y el software, que soportan los procesos y que apoyan la implementación del Sistema de Gestión de Seguridad

5.3 ÁMBITO DE APLICACIÓN DE LA POLÍTICA

La Política De Seguridad Digital establece las diferentes medidas de seguridad, privacidad y protección que ayudara a la Alcaldía Distrital de Cartagena a tener el control de la información que los Secretarios, Directores, jefes de oficina, funcionarios, contratistas y terceros externos que brinden sus servicios o tengan algún tipo de relación con la Alcaldía Distrital de Cartagena de Indias deben adoptar para persuadir, prevenir y/o corregir en el tratamiento de la información, con el ánimo de garantizar un adecuado nivel de seguridad y protección.

5.4 PROPÓSITO DE LA POLÍTICA DE GESTIÓN Y DESEMPEÑO

5.4.1 OBJETIVO GENERAL.

Establecer los componentes para blindar el sistema de información y los diferentes recursos tecnológicos de la Alcaldía Distrital de Cartagena de Indias, los cuales se deben conocer y cumplir por parte de todos los directivos, funcionarios, contratistas y terceros que presten su servicio o mantengan alguna relación en la Alcaldía Distrital de Cartagena de Indias.

5.4.2 OBJETIVOS ESPECIFICOS.

- ✓ Crear un adecuado análisis, diseño e implementación de seguridad y privacidad de tal manera que se logre el amparo de los activos de información para legitimar la confidencialidad, integridad y disponibilidad de los mismos.
- ✓ Adoptar una metodología y procedimiento en la gestión del riesgo para el tratamiento de la información que permita una adecuada seguridad y privacidad de la misma que logre fortalecer y sostener un adecuado nivel de riesgos.
- ✓ Implementar el plan de capacitación y sensibilización con la finalidad de crear una cultura de seguridad institucional por medio de la aplicación de la normatividad vigente y de la adopción de buenas prácticas.

5.5 |LINEAMIENTOS ESTRATÉGICOS PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

La Alcaldía Distrital de Cartagena de Indias, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un modelo de gestión de seguridad y privacidad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto

cumplimiento de las leyes y en concordancia con la misión y visión de la Alcaldía Distrital de Cartagena de Indias.

Para la Alcaldía Distrital de Cartagena de Indias, la seguridad y la protección de la información busca la disminución del impacto generado sobre los activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

Esta política aplica a La Alcaldía Distrital de Cartagena de Indias, consta de los siguientes ***elementos direccionadores,*** que determinan su implementación:

POLÍTICA DE SEGURIDAD DIGITAL

ELEMENTO DIRECCIONADOR		ESRATEGIA	PRODUCTO
Modelo de Seguridad y Privacidad de la Información - SPI	El Modelo de Seguridad y Privacidad de la Información, busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.	Consta de 5 fases: Diagnostico Planeación Implementación Evaluación de desempeño Mejora continua	Modelo de Seguridad y Privacidad de la Información Plan estratégico de Seguridad y Privacidad de la Información Etapa de Diagnóstico: Plan de Cierre de Brechas
Plan de Mitigación de Riesgos y Privacidad de la Información	En cumplimiento al decreto 612 del 2018 por el cual se fijan las directrices de integración de los planes institucionales y estratégicos al plan d acción por parte de las entidades del estado, se establece, el cual contiene la definición de una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, asi como la declaración de aplicabilidad.	Se soporta en la matriz de riesgos de seguridad y privacidad de la información	Plan de Manejo de Riesgos de Seguridad y Privacidad de la Información
Políticas de Seguridad y Privacidad de la Información	EL manual de Política de Seguridad y Privacidad de la información está contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.	Manual de políticas, se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la	Manual de Políticas de Seguridad y Privacidad de la Información

		seguridad de la información	
Política de Seguridad Digital	Lineamientos generales para la implementación de la Política de acuerdo a los lineamientos del MinTIC		Documento Técnico de implementación de la política y Plan de acción de ejecución

6 NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política que soportan el SGSI de La **Alcaldía Distrital de Cartagena de Indias**:

1. La **Alcaldía Distrital de Cartagena de Indias** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
3. La **Alcaldía Distrital de Cartagena de Indias** protegerá la información generada, procesada, transmitida o resguardada por medio de las secretarías, los despachos y activos de información que hacen parte de los mismos.
4. La **Alcaldía Distrital de Cartagena de Indias** protegerá la información creada, procesada, transmitida o resguardada por medio de las secretarías y los despachos, con el fin de minimizar impactos financieros, operativos, reputacionales y/o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. La **Alcaldía Distrital de Cartagena de Indias** resguardará su información de las amenazas originadas por parte del personal.
6. La **Alcaldía Distrital de Cartagena de Indias** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. La **Alcaldía Distrital de Cartagena de Indias** controlará la operación a nivel de procesos establecidos por medio de las secretarías, los despachos garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. La **Alcaldía Distrital de Cartagena de Indias** implementará control de acceso a la información, sistemas y recursos de red.
9. La **Alcaldía Distrital de Cartagena de Indias** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. La **Alcaldía Distrital de Cartagena de Indias** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
11. La **Alcaldía Distrital de Cartagena de Indias** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
12. La **Alcaldía Distrital de Cartagena de Indias** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la Política de seguridad Digital (Información e informática), traerá consigo, las consecuencias legales que apliquen a la normativa de la Alcaldía Distrital de Cartagena de Indias, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

7 ROLES Y RESPONSABILIDADES

Los funcionarios y contratistas de la Alcaldía Distrital de Cartagena de Indias deberán asumir siguientes roles y responsabilidades, donde se garantice la implementación, revisión y mejora continua del Modelo de Seguridad y Privacidad de la Información al interior de la Alcaldía Distrital de Cartagena de Indias.

ROL	RESPONSABILIDADES	RESPONSABLE
Líder de la Política Seguridad digital Digital MINTIC	Emitir las normas, manuales, guías y la metodología de seguimiento y evaluación para la implementación de la política de Gobierno Digital, en las entidades públicas del orden nacional y territorial. De igual manera, a través de la Dirección de Gobierno Digital se desarrollan diferentes iniciativas y proyectos que buscan apalancar la implementación de la política en las entidades públicas.	Ministerio de Tecnologías de la Información y Comunicación a través de la Dirección de Gobierno Digital
Responsable Institucional de la Política de Seguridad Digital: REPRESENTANTE LEGAL	Responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política de Seguridad Digital. Debe garantizar el desarrollo integral de la política al interior de sus entidades, entendiendo que esta es un eje transversal y apalancador de su gestión interna, que apoya el desarrollo de las políticas de gestión y desempeño institucional.	Representante Legal -Alcalde Mayor
Responsable de orientar la implementación de la Política de Gobierno Digital ROL DE ORIENTAR LA IMPLEMENTACIÓN	Orientar la implementación y operación de todas las políticas del Modelo Integrado de Planeación y Gestión -MIPG (entre las que se encuentra seguridad Digital); debe articular todos los esfuerzos institucionales, recursos, metodologías y estrategias para el desarrollo de las políticas del MIPG y en esta medida, lograr que Gobierno Digital se desarrolle articuladamente con las demás políticas en el marco del sistema de gestión de la entidad. Aprobar y verificar del cumplimiento de las políticas y procedimientos de seguridad y privacidad de la información. Hacer que los miembros del Gabinete sean conscientes de la criticidad de los activos de información para el desarrollo de los procesos de la Alcaldía Distrital de Cartagena de Indias. Divulgar las responsabilidades de seguridad y privacidad de la información de la Alcaldía Distrital de Cartagena de Indias con base en los lineamientos del MSPI.	Comité Institucional de Gestión y Desempeño

Responsable de liderar la implementación la Política de Seguridad Digital  	Hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad. Las demás áreas serán corresponsables de la implementación de la Política de Seguridad Digital en los temas de su competencia. Además de: Liderar y apoyar la mejora continua para la aplicación del MSPI al interior de la Alcaldía, Asignar dentro de su equipo de trabajo quien servirá como oficial de seguridad y privacidad de la información, Apoyar las actividades relacionadas con el MSPI. En este sentido, áreas o dependencias afines a los siguientes temas también son responsables en la implementación de la política de Seguridad Digital, dada su transversalidad en la gestión de la entidad: planeación, secretaría general, servicio al ciudadano, participación ciudadana, comunicaciones o prensa, desarrollo organizacional, talento humano, archivo y gestión documental. .	Jefe de Oficina Asesora de Informática en articulación con las dependencias del Distrito
Otros roles e instancias importantes  	Estas instancias deben actuar en coordinación con el comité institucional de gestión y desempeño para la toma de decisiones. Liderar y apoyar de mejora continua para la aplicación del MSPI al interior de la dependencia a cargo. Alineación de los objetivos de la dependencia para que su cumplimiento este apoyado por el MSPI. Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguridad y privacidad de la información para los roles definidos en la dependencia a cargo. Proveer los recursos necesarios para la implementación del MSPI al interior de la dependencia a cargo. Apoyar la capacitación y entrenamiento requerido para que los funcionarios y contratistas de la dependencia a cargo que cumplan con el MSPI. Aplicar el proceso disciplinario ante los incidentes de seguridad y privacidad de la información originada por un funcionario o contratista de la dependencia a cargo.	<nivel directivo secretarios, asesores, directores y jefes de oficina.
Verificación, seguimiento y control de las políticas de seguridad digital	Apoyar en definir y actualizar el inventario de los activos de información. Realizar análisis de riesgos de seguridad y privacidad de la información con base en lo establecido en el MSPI. Definir y generar el modelo de seguridad y privacidad de la información - MSPI. Identificar los requerimientos normativos, de servicios o software necesarios para implementar, mejorar y garantizar la eficacia del protocolo de seguridad informática, garantizando la integridad, la confidencialidad y la protección de todos los activos de la empresa a nivel tecnológico.	Oficial de seguridad y privacidad de la información

	Definir la arquitectura de la seguridad de la red y sus políticas de acceso y control Potenciar la cultura de seguridad informática a nivel global en la Alcaldía Analizar los sistemas de información con el ánimo de encontrar eventos o incidentes que puedan afectar el procedimiento y ocasionar fugas de información, suplantación o corrupción de los datos, apoyando en definición del plan de tratamiento de los riesgos de seguridad y privacidad de la información. Participar en el seguimiento y evaluación de las políticas, programas e instrumentos relacionados con la información pública, confidencial y sensible que esté bajo la responsabilidad de la alcaldía de Cartagena de Indias Impartir lineamientos tecnológicos para el cumplimiento de estándares de seguridad, privacidad, calidad y oportunidad de la información de la Entidad y la interoperabilidad de los sistemas que la soportan, así como el intercambio permanente de información. Hacer seguimiento de los esquemas de seguridad operativa. Auditar procesos, aplicativos, gestión de usuarios y servicios. Investigar las posibles amenazas y vulnerabilidades a nivel de toda la Alcaldía. Controlar la implementación de sistemas de información, Sistemas informáticos y/o servicios a nivel trasversal de la Alcaldía Atender y responder inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.	

8 DEBERES DE FUNCIONARIOS, CONTRATISTAS Y TERCEROS VINCULADOS CON LA ALCALDÍA DISTRITAL

Todos los funcionarios, contratistas y terceros vinculados a la Alcaldía tendrán la responsabilidad de velar por la confidencialidad, integridad, disponibilidad y privacidad de la información que maneje, así mismo debe reportar los incidentes de seguridad, eventos sospechosos o un mal uso de los recursos que identifique.

El incumplimiento a la política general de seguridad y privacidad de la información traerá consigo, las consecuencias legales que apliquen a la normativa de la Alcaldía Distrital de Cartagena de Indias, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

9 POLITICAS ESPECÍFICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se prosigue con la descripción de las políticas de seguridad de la información para el cumplimiento del Modelo de Seguridad y privacidad de la Alcaldía Distrital de Cartagena. Este conjunto de recomendaciones se encuentra compilados en el manual de políticas de seguridad y privacidad de la información. A continuación, se agrupan las políticas con el objetivo de hacer una implementación transversal en la Alcaldía Distrital de Cartagena de Indias

POLITICA	DEFINICION
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Se deben especificar los objetivos del comité como por ejemplo el mejoramiento continuo de los programas o las distintas actividades que se realizarán en dichos comités, verificación de avance de los distintos proyectos, la revisión del documento de la política de seguridad etc.
GESTION DE ACTIVOS	En ellas se encuentran los lineamientos para: Identificación de Activos Clasificación de Activos de información Etiquetado de la Información Disposición de los activos de la información Creación de Activos Devolución de los Activos Devolución de muebles e inmuebles Devolución de equipos tecnológicos Devolución de credenciales Gestión de medios removibles Dispositivos móviles
POLÍTICA DE CONTROL DE ACCESO	Control de acceso con usuario y contraseña Suministro del control de acceso Gestión de Contraseñas
PERÍMETROS DE SEGURIDAD	Política orientada a los lugares de alta confidencialidad y que contengan información confidencial o privada, semiprivada y/o sensible ya sean en físico o digital
CONTROL DE ACCESO A REDES E INTERNET	Se orienta a la asignación de contraseñas de acceso a los servicios de red, servicios y sistemas de información que necesite para el buen desarrollo de sus funciones contractuales.
GESTIÓN DE ACCESO A USUARIOS	Establece los métodos de asignación de contraseñas y los lineamientos de seguridad para su custodia.

REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS	Se establecen los derechos de acceso de los usuarios a la información y a las plataforma o servidores tecnológicos y de procesamiento de información de la Alcaldía Distrital de Cartagena de Indias
POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO	Se establecen los lineamentos sobre: Perímetro de Seguridad Física Controles de Acceso Físico Ubicación y Protección de los equipos Seguridad de los equipos fuera de las instalaciones Seguridad en la reutilización o eliminación de los equipos Retiro de Equipos de Activos Retiro de Equipos de Activos Áreas De Carga
POLÍTICA DE ESCRITORIO DESPEJADO Y PANTALLA DESPEJADA	Definir los aspectos generales para mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida, modificación y daño de la información de la Alcaldía Distrital de Cartagena de Indias
PROTECCIÓN Y PRIVACIDAD DE DATOS PERSONALES	Emite lineamientos para el cumplimiento de la política del tratamiento de datos personales que se encuentra alineada y conforme a lo establecido en la normatividad vigente
INTEGRIDAD DE LA INFORMACION	Se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los mismos.
DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN	Se establece con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Alcaldía Distrital de Cartagena de Indias
GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Lineamientos para documentar todos los eventos, incidentes y vulnerabilidades de seguridad de la información.
COPIAS DE SEGURIDAD	Lineamientos para alojar las copias de seguridad, información catalogada confidenciales, backups de equipos de escritorio, backups de correo electrónico y demás que sea relevante en el cumplimiento de los objetivos de la Alcaldía.
PROTECCIÓN CONTRA CÓDIGO MALICIOSO	Lineamientos para aplicar un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

POLÍTICA DE GESTIÓN DE SEGURIDAD DE LAS REDES	Política para establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.
DESARROLLO SEGURO	Políticas para la seguridad durante la implementación y el ciclo de vida del desarrollo del software y para todos los desarrollos nuevos y de las actualizaciones de cualquier aplicación
POLÍTICA DE CUMPLIMIENTO LEY DE TRANSPARENCIA	Lineamientos para garantizar el derecho de acceso a la información pública por medio de los canales establecidos por la Alcaldía excluyendo las excepciones constitucionales, legales, Sensibles.
SERVICIOS DE COMPUTACIÓN EN LA NUBE	Lineamientos para garantizar la disponibilidad, privacidad, confidencialidad, integridad y cumplimiento de los requisitos legales en materia de protección de información personal, que sean autorizados a ser tratados en los servicios de computación en la nube
SENSIBILIZACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN	Lineamientos para garantizar la formación del personal en temas relacionados con la seguridad Y privacidad de la información.
USO DE TOKENS DE SEGURIDAD	Políticas para el manejo de los tokens de seguridad para las dependencias y oficinas que lo requieran utilizar y asignar a los funcionarios que serán responsables, acción que será intransferible.
TELETRABAJO	Garantizar la seguridad de la información, de tal manera que la confidencialidad, disponibilidad y autenticidad durante el teletrabajo.

10 Documentos estratégicos

- ✓ Plan de acción de implementación Política de Seguridad Digital
- ✓ Manual de políticas de Seguridad Digital
- ✓ Modelo de Seguridad y privacidad de la información
- ✓ Plan de seguridad y privacidad de la información
- ✓ Plan de tratamiento de riesgos de seguridad y privacidad de la información

11 FIRMA DE LOS INTEGRANTES DEL COMITÉ INSTITUCIONAL DE GESTION Y DESEMPEÑO DE LA ALCALDIA DISTRITAL DE CARTAGENA DE INDIAS

_____

William Dau Chamat

Alcalde Mayor de Cartagena

Aprobado mediante acta número XX del xxx del mes xxxxxx del xxxx del Comité Institucional de Gestión y Desempeño