MANUAL DE 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.
2.0	Modificación de la redacción del documento bajo la estructura del lenguaje claro Organización del documento de acuerdo con los dominios del MSPI Inclusión de políticas de seguridad de acuerdo al MSPI Aprobado mediante acta 004 del 01 de septiembre del 2023 por el comité de gestión y desempeño institucional.

TABLA DE CONTENIDO

1. INTRODUCCION 7
2. PROPOSITO 7
3. ALCANCE 7
4. MARCO CONCEPTUAL 8
   4.2 SIGLAS 13
   4.3 NOMENCLATURA 13
5. RESPONSABILIDAD Y AUTORIDAD 14
6. POLÍTICAS DE OPERACIÓN 14
   6.1 DOMINIO 5: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 14
      6.1.1 Los objetivos 15
      6.1.2 Alineación con la estrategia y objetivos de la entidad 15
      6.1.3 Aprobación y socialización al interior de la entidad por la alta dirección 15
      6.1.4 Concepto de la seguridad de la información. 15
   6.2 DOMINIO 6: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 15
      6.2.1 Organización Interna 16
      6.2.2 Dispositivos Móviles 17
      6.2.3 Teletrabajo 17
   6.3 DOMINIO 7: SEGURIDAD DE LOS RECURSOS HUMANOS 19
   6.4 DOMINIO 8: GESTIÓN DE ACTIVOS 21
      6.4.1 Inventario de Activos 21
      6.4.2 Propiedad de los activos 22
      6.4.3 Devolución de activos 23
      6.4.4 Clasificación de la información 23
      6.4.5 Etiquetado de la Información 24
      6.4.6 Manejo de los activos 25
      6.4.7 Gestión de medios removibles 25
      6.4.8 Disposición de los medios 25
      6.4.9 Transferencia de medios físicos 25
      6.4.10 Creación de Activos 26
   6.5 DOMINIO 9: CONTROL DE ACCESO 26
      6.5.1 Control de acceso con usuario y contraseña 27

6.5.2 Suministro del control de acceso 27
6.5.3 Gestión de Contraseñas 27
6.5.4 Acceso a redes y a servicios en red 28
6.5.5 Gestión de información de autenticación secreta de usuarios 28
6.5.6 Gestión de acceso a usuarios 29
6.5.7 Ingreso seguro a los sistemas de información 30
6.5.8 Políticas sobre perímetros de seguridad 30
6.5.9 Políticas para la revisión de los derechos de acceso de los usuarios 31
6.5.10 Política para el manejo de copias de seguridad 31
6.6 DOMINIO 10: CRIPTOGRAFIA 32
6.7 DOMINIO 11: SEGURIDAD FISICA Y DEL ENTORNO 33
6.7.1 Perímetro de Seguridad Física 33
6.7.2 Seguridad de oficinas, recintos e instalaciones 34
6.7.3 Controles de Acceso Físico 34
6.7.4 Ubicación y Protección de los equipos 34
6.7.5 Mantenimiento de equipos 35
6.7.6 Retiro de Equipos de Activos 35
6.7.7 Seguridad de los equipos fuera de las instalaciones 36
6.7.8 Seguridad en la reutilización o eliminación de los equipos 36
6.7.9 Política de escritorio y pantalla despejados 36
6.8 DOMINIO 12: SEGURIDAD DE LAS OPERACIONES 37
6.8.1 Procedimientos de operación documentados 37
6.8.2 Gestión de cambios 38
6.8.3 Separación de los ambientes de desarrollo, pruebas y operación 38
6.8.4 Control contra códigos maliciosos 38
6.8.5 Respaldo de información 40
6.8.6 Registro de eventos 41
6.8.7 Protección de la información de registro 41
6.8.8 Registros del administrador y del operador 41
6.8.9 Sincronización de relojes 42
6.8.10 Instalación de software en sistemas operativos 42
6.8.11 Gestión de la vulnerabilidad técnica 42

6.8.12 Restricciones sobre la instalación de software 43
6.9 DOMINIO 13: SEGURIDAD DE LAS COMUNICACIONES 43
6.9.1 Controles de redes 43
6.9.2 Seguridad de los servicios de red 44
6.9.3 Separación en las redes 44
6.9.4 Políticas y procedimientos de transferencia de información 44
6.9.5 Acuerdos sobre transferencia de información 44
6.9.6 Mensajería electrónica 45
6.9.7 Acuerdos de confidencialidad o de no divulgación 45
6.9.8 Políticas para el servicio de computación en la nube 46
6.9.9 Política de disponibilidad del servicio e información 47
6.9.10 Política de gestión de seguridad de las redes 47
6.9.11 Políticas para la sensibilización y capacitación en seguridad de la información 48
6.10 DOMINIO 14: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 48
6.10.1 Análisis y especificación de requisitos de seguridad de la información 48
6.10.2 Seguridad de servicios de las aplicaciones en redes publicas 50
6.10.3 Protección de transacciones de los servicios de las aplicaciones 50
6.10.4 Política de desarrollo seguro y principios de construcción de sistemas seguros 51
6.10.5 Procedimientos de control de cambios en sistemas y restricciones en los cambios a los paquetes de software y ambiente de desarrollo seguro 53
6.10.6 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación 54
6.10.7 Desarrollo contratado externamente 54
6.10.8 Pruebas de seguridad de sistemas 55
6.10.9 Prueba de aceptación de sistemas 55
6.10.10 Protección de datos de prueba 56
6.11 DOMINIO 15: RELACIÓN CON LOS PROVEEDORES 57
6.11.1 Seguridad de la información en las relaciones con los proveedores 57
6.12 DOMINIO 16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 57
6.12.1 Responsabilidad y procedimientos 58
6.12.2 Reporte de eventos de seguridad de la información 59

6.12.3 Reporte de debilidades de seguridad de la información 59
6.12.4 Respuesta a incidentes de seguridad de la información 60
6.12.5 Aprendizaje obtenido de los incidentes de seguridad de la información 60
6.13 DOMINIO 17: ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO 60
6.13.1 Planificación de la continuidad de la seguridad de la información 60
6.13.2 Implementación de la continuidad de la seguridad de la información 61
6.14 DOMINIO 18: CUMPLIMIENTO 61
6.14.1 Identificación de la legislación aplicable y de los requisitos contractuales 61
6.14.2 Derechos de propiedad intelectual 61
6.14.3 Protección de registros 62
6.14.4 Protección de los datos y privacidad de la información relacionada con los datos personales. 63
6.14.5 Cumplimiento con las políticas y normas de seguridad digital 63
6.14.6 Revisión del cumplimiento técnico 64
6.14.7 Política de cumplimiento ley de transparencia 64
6.14.8 Sanciones y seguimiento de las medidas de seguridad 65
7. BIBLIOGRAFÍA 66
8. FIRMA DE LOS INTEGRANTES DEL COMITÉ INSTITUCIONAL DE GESTION Y DESEMPEÑO DE LA ALCALDIA DISTRITAL DE CARTAGENA DE INDIAS. 68

1. INTRODUCCION

La Alcaldía Distrital de Cartagena de Indias identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por el plan estratégico de TI PETI de la Entidad, por esta razón establece un modelo que asegura que la información es protegida de una manera adecuada para su recolección, manejo, procesamiento, transporte y almacenamiento.

Este documento describe las políticas y normas de seguridad digital definidas por el distrito. Para la elaboración de este, se toman como base las leyes y demás regulaciones aplicables, las políticas incluidas en este manual son parte integral del sistema de gestión de seguridad digital y son la base para la implantación de los controles, procedimientos y estándares.

La seguridad digital es una prioridad para la Alcaldía y por tanto el cumplimiento de estas políticas es responsabilidad de todos sus colaboradores. A lo largo del documento al emplear el término seguridad digital se agrupan los conceptos de seguridad de la información, seguridad informática, ciberseguridad y la protección de los datos personales.

Este documento es complementario a la política de seguridad y privacidad de la información, dado que en ella se encuentran los objetivos, la alineación estratégica y la declaración del compromiso de cumplimiento por parte de funcionarios, contratistas y terceros que realizan actividades en el distrito de Cartagena.

2. PROPOSITO

El propósito del siguiente manual es brindar al Distrito de Cartagena los lineamientos correspondientes a la implementación de las políticas de seguridad y privacidad de la información, con el fin actúe como elemento de consulta y soporte para la implementación de los controles y procedimientos estándares que se deben adoptar para mitigar los riesgos de seguridad y privacidad de la información.

3. ALCANCE

El alcance del presente manual de Seguridad de la Información contiene los lineamientos generales para la implementación de un modelo de gestión de seguridad y privacidad de la información, a través de la identificación de responsabilidades y disposiciones generales en torno a la gestión de activos, el control de accesos, la privacidad y confidencialidad, la integridad, la disponibilidad del servicio y la información, la gestión de incidentes y las acciones de capacitación y sensibilización.

4. MARCO CONCEPTUAL

- **Aceptación del Riesgo:** Decisión generada por la entidad de aceptar las consecuencias y probabilidad de un riesgo en particular, sin adelantar acciones de reducción y control.(ICONTEC Internacional, 2013)

- **Activo:** Según cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de esta. (MINTIC, 2016)

- **Alcance:** Ámbito de la organización que queda sometido a la política de seguridad y privacidad de la información y las comunicaciones. (NORMA INTERNACIONAL, 2015)

- **Alerta:** notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre. (ICONTEC Internacional, 2007)

- **Amenaza:** Según causa potencial de un incidente, el cual puede dar como resultado un daño a la entidad. (MINTIC, 2016)

- **Análisis de riesgos:** Uso sistemático de la información para identificar fuentes y estimar el riesgo. (MINTIC, 2016)

- **Aplicaciones:** 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. (ICONTEC Internacional, 2018)

- **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. (MINTIC, 2016)

- **Autenticación:** Proceso que tiene por objetivo validar la identificación de una entidad o sistema. (ICONTEC Internacional, 2013)

- **Autenticidad:** Los activos de información solo pueden estar disponibles al verificar la identidad deun sujeto o recurso. También hacer referencia a la propiedad que garantiza que la identidad de un sujeto o recurso es la que manifiesta. (ICONTEC Internacional, 2013)

- **Estándar**: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. También hace referencia a orientaciones obligatorias que buscan hacer cumplir las

políticas. Estos son diseñados para promover la implementación de las políticas de alto nivel de laentidad antes de crear nuevas políticas. (MINTIC, 2016)

- **Compromiso de la alta gerencia:** Alineamiento firme de la Dirección de la organización con elestablecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejoradel Política de Seguridad y Privacidad de la Información y las Comunicaciones. (ICONTEC Internacional, 2013)

- **Confiabilidad:** Es un término colectivo utilizado para describir la disponibilidad de un producto y los factores que la condicionan. (MINTIC, 2016)

- **Confidencialidad:** Acceso a la información por parte únicamente de quienes estén autorizados, característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados. (MINTIC, 2016)

- **Control:** políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (MINTIC, 2016)

- **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. (ICONTEC Internacional, 2013)

- **Datos:** 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. (MINTIC, 2016)

- **Incidente:** 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. (ICONTEC Internacional, 2018)

- **Información:** Es el conjunto de datos que configuran un mensaje que emite un emisor y que se pretende llegue al receptor para que quede informado. (MINTIC, 2016)

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

- **Integridad:** Principio que garantiza que la información sea exacta, coherente y completa desde su creación hasta su destrucción. (MINTIC, 2016)

- **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 deban, por tanto, ser protegidos de potenciales riesgos. (MINTIC, 2016)

- **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. (ICONTEC Internacional, 2018)

- **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. (ICONTEC Internacional, 2013)

- **Medida preventiva:** Medida de tipo proactivo orientado a prevenir potenciales no conformidades asociadas a la implementación y operación de la Política de Seguridad y Privacidad de la Información y las Comunicaciones. (NORMA INTERNACIONAL, 2015)

- **Mejor Práctica**: Regla de seguridad específica o plataforma que es aceptada mediante, 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 (MINTIC, 2016).

- **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. (NORMA INTERNACIONAL, 2015)

- **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. (ICONTEC Internacional, 2013)

- **No repudio:** Es un servicio de seguridad que permite probar la participación de las partes en una comunicación. (MINTIC, 2016)

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

- **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). Esta es una buena definición. (Federación colombiana de municipios, 2018)

- **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 quelas ponga en peligro. (ICONTEC Internacional, 2018).

- **Plan de tratamiento de riesgos (Risk treatment plan**): Documento de gestión que define lasacciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ICONTEC Internacional, 2018)

- **Política**: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico. (MINTIC, 2016)

- **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 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 enfoquede la organización en la gestión de la seguridad de la información. Intención y dirección general expresada formalmente por la Dirección. (ICONTEC Internacional, 2013)

- **Procedimiento**: Descripción detallada de la manera en la que se implementa una política. (MINTIC, 2016)

- **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias. (ICONTEC Internacional, 2018)

- **Riesgo Residual:** Es el riesgo que permanece después de se han hecho todos los esfuerzos para identificar y eliminar el riesgo, es decir, sus controles de mitigación. (Departamento nacional de planeación, 2016)

- **Salvaguarda:** Consisten en medidas para tratar las posibles amenazas del sistema y reducir el riesgo total del mismo.

- **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:** 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. (MINTIC, 2016)

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

- **Terceros:** Persona natural o jurídica que tenga una relación directa o indirecta con la Alcaldía Mayor de Cartagena de Indias.

- **Usuario:** Se refiere 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:** Proceso completo de análisis y evaluación de riesgos. (MINTIC, 2016)

- **Virus:** Agente que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario. (Departamento nacional de planeación, 2016)

- **Vulnerabilidad:** Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza. (MINTIC, 2016)

4.2 SIGLAS

- **IPS:** Sistema de prevención de intrusiones, identifica el tráfico malicioso y bloquea de manera proactiva el ingreso de dicho tráfico a su red.
- **ISO:** Organización Internacional de Normalización, Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.
- **COPSIS:** Sistema de Contratación de OPS (contratos de prestación de servicios).
- **MSPI:** Modelo de seguridad y privacidad de la información, define los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad.
- **OAI:** Oficina Asesora de Informática.
- **SIGOB:** Sistema de Gestión y Seguimiento a las Metas de Gobierno.

4.3 NOMENCLATURA

- **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. (NORMA INTERNACIONAL, 2005).
- **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. (NORMA INTERNACIONAL, 2018)
- **ISO 27001:** Estándar para sistemas de gestión de la seguridad de la información adoptado porISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005. (ICONTEC Internacional, 2013).
- **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. (ICONTEC Internacional, 2007)
- **ISO 9000:** Normas de gestión y garantía de calidad definidas por la ISO. (NORMA INTERNACIONAL)

- **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.

5. RESPONSABILIDAD Y AUTORIDAD

Oficina Asesora de Informática – Seguridad y privacidad de la información. La responsabilidad y autoridades del manual de políticas se describe en el instructivo para la definición de roles y responsabilidades del modelo de seguridad y privacidad de la información con código GTIGPS01-I002

6. POLÍTICAS DE OPERACIÓN

Las políticas de operación están organizadas de acuerdo con los dominios establecidos en la NTC ISO 27001 Técnicas De Seguridad Sistemas de gestión de la seguridad de la Información (SGSI). Documento base para la definición del modelo de seguridad y privacidad de la información, la numeración se realiza de acuerdo con los dominios que contiene el modelo:

6.1 DOMINIO 5: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Fuente

El Distrito de Cartagena definió un conjunto de políticas para la seguridad de la información, las cuales fueron aprobadas por el comité de Gestión y Desempeño Institucional, y comunicadas a los empleados y a las partes externas pertinentes, a través de la sede electrónico de la alcaldía de Cartagena https://mipg.cartagena.gov.co/gestion-valores-resultados/seguridaddigital.

Estas políticas son revisadas a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continua.

Este documento contiene:

a) Los objetivos de la política

b) Alineación con la estrategia y objetivos de la entidad
c) Aprobación y socialización al interior de la entidad por la alta dirección
d) Concepto de la seguridad de la información.

6.1.1 Los objetivos

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.

- ✓ 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 estos.
- ✓ Adoptar una metodología y procedimiento en la gestión del riesgo para el tratamiento de la información que permita una adecuada seguridad y privacidad de esta 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.

6.1.2 Alineación con la estrategia y objetivos 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 que contiene 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.

6.1.3 Aprobación y socialización al interior de la entidad por la alta dirección

El comité de gestión y desempeño institucional es la autoridad competente para la aprobación de los documentos que hacen parte del modelo de seguridad y privacidad de la información, el presente manual fue aprobado mediante acta 004 del 01 de septiembre del 2023.

6.1.4 Concepto de la seguridad de la información.

El marco conceptual que hace parte integral del presente manual se encuentra especificado en el documento denominado política de seguridad, allí se encuentran todos los conceptos asociados a la seguridad y la privacidad de la información. (capitulo 3 política de seguridad)

6.2 DOMINIO 6: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Fuente

6.2.1 Organización Interna

Para esta política el Distrito de Cartagena ha definido un documento denominado “instructivo para la definición de roles y responsabilidades del modelo de seguridad y privacidad de la información código GTIGPS01-I002" en el cual se reglamenta los roles y responsabilidades para la seguridad y privacidad de la información, el cual contiene lo siguiente:

Los roles y responsabilidades frente a la ciberseguridad

a) Los roles y responsabilidades de seguridad de la información alineados con los roles internos y las terceras partes externas se encuentran definidos y son de estricto cumplimiento código GTIGPS01-I002 instructivo para la definición de roles y responsabilidades del modelo de seguridad y privacidad de la información.
b) Los proveedores, clientes, funcionarios, contratistas, secretarios de despacho, jefes de oficina, directores, gerentes, alcaldes locales, personal de seguridad física, personal de seguridad de la información, pueden consultar la información sobre la política de seguridad digital y los roles, responsabilidades en la sede electrónico micrositio seguridad digital https://mipg.cartagena.gov.co/gestion-valores-resultados/seguridaddigital.
c) Todas las dependencias del Distrito de Cartagena deben tener la claridad sobre los deberes y áreas de responsabilidad que generen conflicto, estas se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
d) Para el contacto con las autoridades el Distrito de Cartagena se estableció un documento denominado procedimiento de gestión de incidentes de seguridad de la información código GTGPS02-P003. En el cual se ha establecido el procedimiento que especifica cuándo y a través de que autoridades se debe contactar y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados.
e) El Distrito cuenta con el instructivo para la gestión de riesgos de seguridad y privacidad de la información TI código GTIGPS01-I005, el cual contiene los requisitos para establecer los riesgos de seguridad de la información que se identifiquen y traten como parte de un proyecto.

Para esto se debe tener en cuenta lo siguiente:

a) Todos los proyectos TI deben incluir objetivos de la seguridad de la información

b) Todos los proyectos TI deben valorar riesgos de seguridad de la información en una etapa temprana del proyecto para identificar los controles necesarios
c) Para todas las fases de la metodología del proyecto aplicada se debe tener en cuenta la seguridad de la información.

6.2.2 Dispositivos Móviles

Los jefes de las Dependencias informarán a la Oficina Asesora de Informática, los funcionarios, contratistas o terceros que pueden tener acceso a las redes inalámbricas, quiénes pueden realizar instalación de chats corporativos y/o correos electrónicos de la Alcaldía Distrital de Cartagena de Indias mediante el uso de este tipo de dispositivos, adicionalmente deben comunicar las responsabilidades de estos en el uso de la información almacenada en los dispositivos móviles así como como los controles de seguridad establecidos por la Alcaldía Distrital de Cartagena de Indias.

Cuando aplique, el Distrito de Cartagena adoptará la política de dispositivos móviles y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles, de acuerdo con las mejores prácticas considerando lo siguiente:

a) Todo dispositivo móvil institucional debe ser registrado
b) Se restringe la instalación de software en los dispositivos móviles sin autorización
c) Los dispositivos móviles deben estar protegidos contra software malicioso

Cuando los funcionarios utilizan dispositivos móviles de propiedad personal autorizados por el Distrito de Cartagena para el normal funcionamiento de sus actividades, también se deben tener en cuenta las consideraciones de esta política y las siguientes:

a) La separación entre el uso privado y de la Entidad de los dispositivos
b) Brindar acceso a la información de la Entidad solo cuando los usuarios hayan firmado un acuerdo de usuario final, en el que se reconocen sus deberes (protección física, actualización del software, etc.), desistir de la propiedad de los datos de la Entidad, permitir el borrado remoto de datos por parte de la organización en caso de robo o pérdida del dispositivo, o cuando ya no se posee autorización para usar el servicio.

6.2.3 Teletrabajo

Para la modalidad de teletrabajo o trabajo en casa la Oficina Asesora de Informática deberá tener en cuenta para un correcto uso de los equipos y herramientas tecnológicas para los funcionarios del Distrito de Cartagena los siguientes lineamientos:

a) Uso de herramientas tecnológicas: Los medios tecnológicos y de ambiente (herramientas tecnológicas) requeridos, así como la descripción de equipos y programas informáticos, junto con las restricciones y las responsabilidades desde el punto de vista técnico de acuerdo con la autorización recibida por Dirección Administrativa de Talento Humano se le asignara al funcionario un equipo de cómputo que cumpla con las siguientes características:
    - Sistema operativo licenciado

- Antivirus actualizado
- Software de VPN previamente autorizado.
- Herramienta de Monitoreo de los activos de información.
- Herramienta de soporte y mantenimiento remoto.

b) El Distrito de Cartagena deberá proveer y garantizar las conexiones necesarias para desempeñar sus funciones. En caso de que la vivienda del funcionario se encuentre ubicada en sectores donde no exista recursos para la conectividad, la Oficina Asesora de Informática enviara un informe a Dirección Administrativa de Talento Humano con el fin de tomar las acciones y evaluar la posibilidad de asignar los recursos (Auxilio monetario compensatorio por gastos de internet, energía y telefonía) que propicien la conectividad, durante el tiempo aprobado para el teletrabajo.

c) La Oficina Asesora de Informática deberá realizar una visita (solicitada por Talento Humano a la mesa de ayuda al correo soportegti@cartagena.gov.co) de inspección a la vivienda, con el fin de determinar el acceso a las redes de internet, del cual generará un informe detallando de la situación.

d) En caso de que el Distrito autorice el recurso para la conectividad del funcionario, debe acogerse a los procesos contractuales vigentes y/o que sean aplicables.

e) Las medidas de seguridad digital que debe conocer y cumplir el teletrabajador y el trabajador habilitado para trabajar en casa, con el fin de minimizar la ocurrencia de riesgos digitales, el funcionario debe seguir con las siguientes recomendaciones:

- Los elementos y medios suministrados no podrán ser usados por persona distinta al teletrabajador, quien tampoco podrá darles usos distintos a sus funciones laborales.
- Al finalizar el teletrabajo o el vínculo laboral con la Entidad, el teletrabajador deberá restituir los objetos entregados para la ejecución del mismo, en buen estado, salvo el deterioro natural.
- Los elementos y medios suministrados no deben salir del sitio asignado sin la autorización previa y escrita del funcionario competente.
- Realizar la salvaguarda de información laboral crítica en las cuentas institucionales dispuestas en la nube.
- Cerrar las sesiones de programas y bloquear el computador, cuando se retire de su puesto de trabajo.
- Cambiar las contraseñas, de acuerdo con el instructivo para la gestión de usuario y contraseña con código GTIGPS02-I001 y las políticas para la gestión de contraseñas.
- No compartir las contraseñas de sus equipos de cómputos y/o redes WIFI del hogar.
- Se deberán enviar información solo por medios autorizados: herramientas institucionales, compartir archivos por enlace de acceso, con los permisos autorizados.
- Se prohíbe el uso de memorias USB y discos duros externos con información laboral crítica.

- Durante la jornada de Teletrabajo se debe cerrar las páginas de navegación no requeridas.
- No descargar programas sin la autorización de la Oficina Asesora de Informática. Cualquier tipo de solicitud de soporte técnico se debe hacer a través de la mesa de servicios al correo soportegti@cartagena.gov.co
- No utilizar redes WIFI públicas para intercambio de información laboral.
- Cualquier sospecha o anomalía, en cuanto a la información, repórtela a la mesa de servicio al correo soportegti@cartagena.gov.co y al líder del proceso de Seguridad y Privacidad de la Información al correo seguridad.oai@cartagena.gov.co del Distrito de Cartagena.
- No se deberá consumir bebidas ni alimentos en su puesto de trabajo.
- Al terminar la jornada laboral apagar su computador.
- Conocer y poner en práctica las políticas de seguridad y privacidad de la información, manuales de seguridad digital, el Decreto 0619 del 26 de mayo del 2020 políticas de tratamiento de datos personales del Distrito de Cartagena; las cuales se encuentran alojadas en el micrositio Política de seguridad digital

f) Para el manejo de los sistemas de información, aplicaciones y software institucionales el funcionario deberá seguir los siguientes lineamientos:
   - El funcionario deberá seguir los lineamientos del procedimiento para la solicitud de acceso con código GTIGPS02-P001 y el diligenciando del formato de solicitud de acceso a recursos digitales con código GTIGPS02-F001.
   - El funcionario solo tendrá acceso a los sistemas de información y bases de datos autorizados.
   - El funcionario deberá garantizar la confidencialidad de la información propia de la Alcaldía de Cartagena.

g) La Oficina Asesora de Informática deberá recibir por la Dirección Administrativa de Talento Humano la relación de las personas que estarán en la modalidad de teletrabajo suplementario, especificando las características o condiciones especiales que tenga el funcionario.

h) La Oficina Asesora de Informática brindara soporte técnico remoto cuando sea necesario en los horarios laborales de la Alcaldía Mayor de Cartagena, en los casos que no se pueda dar solución de manera remota se realizara el soporte en sitio en el lugar de residencia del funcionario.

6.3 DOMINIO 7: SEGURIDAD DE LOS RECURSOS HUMANOS

Fuente

El Distrito de Cartagena establece la siguiente política de seguridad de la información asociada a la incorporación de talento humano, la cual se debe hacer cumplir por parte de la Dirección de talento humano para el personal de contratistas que desarrollan labores al interior de la Alcaldía en la modalidad de contratación por prestación de servicios:

a) Verificación de referencias satisfactorias
b) Verificación de la de la hoja de vida del solicitante incluyendo certificaciones académicas y laborales;
c) Confirmación de las certificaciones académicas y profesionales declaradas;
d) Verificación de la información de antecedentes penales.
e) Cuando un individuo es contratado para un rol de seguridad de la información específico, la Dirección de talento humano deberá asegurar que el candidato tenga la competencia necesaria para desempeñar el rol de seguridad;
f) Verificar que sea confiable para desempeñar el rol, especialmente si es crítico para la organización.
g) Cuando el contratista requiera acceso a las instalaciones de procesamiento de información, y en particular, si ahí se maneja información confidencial, el Distrito de Cartagena debe hacer las verificaciones correspondientes para garantizar que el tercero pueda realizar esta actividad.
h) La información sobre todos los candidatos que se consideran para cargos dentro de la organización se debería recolectar y manejar apropiadamente de acuerdo con la ley de protección de datos personales.
i) Los acuerdos contractuales con funcionarios y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
j) Todo funcionarios y contratista deben aplicar las políticas de la seguridad de la información de acuerdo con el presente manual y los procedimientos establecidos por la organización.
k) Todo funcionarios y contratista deben estar debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales.
l) Todo funcionarios y contratista deben conocer las directrices que establecen la seguridad de la información de sus roles dentro de la Entidad.
m) Todas las dependencias del Distrito de Cartagena deberán generar acciones o estrategias que logren un nivel de toma de conciencia sobre seguridad de la información pertinente a los roles y responsabilidades dentro de la organización y que contratistas y funcionarios estén motivados para cumplir con las políticas.
n) Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deben definir, comunicar al funcionario o contratista y se deben hacer cumplir.
o) Los secretarios de despacho, jefes de oficina, directores, gerentes alcaldes locales deben revisar los acuerdos de confidencialidad suscritos con funcionarios o contratistas verificando que deben acordar que después de terminada la relación laboral o contrato seguirán vigentes por un periodo de tiempo.

6.4 DOMINIO 8: GESTIÓN DE ACTIVOS

Fuente

Esta política describe las directrices mediante las cuales se indica a los secretarios de despacho, jefes de oficina, directores, gerentes alcaldes locales, funcionarios, contratistas y terceros que presten su servicio o mantengan alguna relación en la Alcaldía Distrital de Cartagena de Indias, los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información, las políticas relacionadas con gestión de activos deben contemplar como mínimo:

6.4.1 Inventario de Activos

a) El Distrito de Cartagena cuenta con un instructivo para la identificación y clasificación de los activos código GTIGPS01-I006, el cual comprende la Información, Software, Hardware, servicios, intangibles, componentes de red, personas e instalaciones.
b) El inventario de activos de información debe ser diligenciado por todas las Dependencias del distrito a través del formato de inventario y clasificación de activos de información GTIGPS01-F007.
c) Cada Dependencia es responsable por la actualización del inventario de activos de información, la cual se deberá hacer una vez al año, informando a la Oficina Asesora de Informática, proceso de seguridad estratégica, las modificaciones a que haga lugar.
d) El inventario de activos de información debe ser revisado y aprobado por el jefe de la Oficina Asesora de Informática y se debe ajustar a lo requerido en el instructivo para la identificación y clasificación de los activos de información código GTIGPS01-I006.
e) Para llevar a cabo una correcta identificación de los activos de información se debe:
    - Establecer que, todo activo de información debe tener un **ID o código** de identificación secuencial que permita identificar la unidad a la cual pertenece.
    - La dirección de talento humano identifica, registra y controla la actualización del inventario en cuanto al conocimiento de las personas claves en el proceso, aplica para aquellas que tienen cualquier vínculo con la Alcaldía.
    - Toda la documentación física debe ser rotulada bajo el lineamiento de la Gestión Documental dirigida por la Dirección de Archivo y correspondencia, quien sigue las especificaciones dadas desde el Archivo General de la Nación y será almacenada bajo las mismas directrices establecidas de acuerdo con la norma

vigente y siguiendo la estructura de las tablas de retención documental TRD y Tablas de Valoración Documental -TVD definidas.

- Todo dispositivo tecnológico, debe ser rotulado con una identificación única, sellado para evitar su apertura, registrado por Almacén y desde el área de infraestructura tecnológica se debe llevar la respectiva hoja de vida por cada equipo, para garantizar el historial de cada actividad generada en el equipo.
- Los activos como infraestructura física, muebles e inmuebles serán inventariados por el almacén y entregados bajo custodia a la dependencia asignada.
- El inventario de los activos de información deberá ser actualizado cada vez que se presente una novedad por cada área que le corresponde el activo; no obstante, anualmente se debe realizar un inventario para hacer la verificación.
- Los responsables de los activos teniendo como base el decreto 0304 del 19 de mayo de 2003 de la Alcaldía Distrital de Cartagena, por el cual establece la estructura general de la Alcaldía mayor de Cartagena de Indias los objetivos y funciones de cada una de las dependencias:
  - **Talento Humano**: debe llevar el control de todo el personal que trabaja en la alcaldía.
  - **Dirección de Archivo General**: se encarga de la Gestión documental de la Alcaldía Distrital de Cartagena de Indias.
  - **Almacén**: Se encarga de llevar el control del inventario de los Activos, propiedad de la Alcaldía de Cartagena, incluyendo equipos tecnológicos, así como de los insumos necesarios para que los mismos puedan tener un desempeño óptimo, con la claridad que una vez entregado a custodios estos reporten las novedades que sean necesarias.

6.4.2 Propiedad de los activos

a) Los activos mantenidos en el inventario deben ser asignados a un funcionario responsable en cada dependencia.
b) Todo secretario de despacho, jefes de oficina, directores, gerentes alcaldes locales debe asegurar la asignación oportuna de la propiedad de los activos, asegurarse de que los activos están inventariados, asegurarse de que los activos están clasificados y protegidos apropiadamente, definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables, y asegurarse del manejo apropiado del activo cuando es eliminado o destruido.
c) Los funcionarios a quienes se les asigna el activo deberán responden por su custodia, protección y preservación tanto del hardware como del software.
d) En caso de daño en los activos asignados a los funcionarios, estos deben elevar un informe detallado del incidente con las respectivas fotografías y enviarlo vía SIGOB a la Oficina Asesora de Informática quien adelantara el respectivo proceso.
e) En ninguna circunstancia los activos deberán salir de las instalaciones del distrito de Cartagena, para casos excepcionales solo el jefe de la dependencia deberá firmar el acta de salida, bajo su responsabilidad.

f) Los equipos tecnológicos solo serán asignados a funcionarios, quienes deberán firmar el acta de entrega de equipos de cómputo y periféricos código GTIGI04-F003 y responder por estos.
g) Cuando el contratista en estricto cumplimiento de sus obligaciones contractuales se vea en la utilidad de tratar con un activo de información el responsable sería el jefe de la Oficina.

6.4.3 Devolución de activos

a) Devolución de equipos informáticos

Todos los funcionarios, que realicen actividades en el Distrito de Cartagena deberán devolver todos los activos de la organización que se encuentren a su cargo una vez finalizada la relación contractual del contratista de acuerdo con lo establecido en el procedimiento para devolución de equipos informáticos código GTIGI04-P002.

b) Devolución de documentación física y digital

Para la devolución de la documentación física y digital los funcionarios deberán realizar la devolución de acuerdo con el procedimiento establecido por el Archivo General. Para los contratistas esta entrega se realizará a la persona que el secretario o jefe de Dependencia asigne, diligenciando y plasmado por escrito. Se aclara que la información digital que se encuentra en los equipos de mesa, portátiles debe hacerse por medio de una copia de seguridad a la Oficina Asesora de Informática mediante la mesa de servicios o en el aplicativo SAUS.

c) Devolución de muebles e inmuebles

Este tipo de enseres se deberá entregar bajo los lineamientos y el procedimiento establecidos por Almacén, guardando la respectiva evidencia de ello.

d) Devolución de credenciales

Solo se puede entregar las credenciales de acceso a los aplicativos a funcionarios responsables de usuarios genéricos; por medio de la notificación a la jefe de la Oficina Asesora de Informática, mediante el diligenciamiento del formato de control de accesos a servicios digitales con código GTIGPS02-F001, para llevar control de la persona que se encuentra garante del acceso a través de dicho usuario genérico. Para los usuarios no genéricos se debe notificar la desvinculación en caso de que se realice antes de la terminación del contrato dado que los mismo se bloquearán una vez finalice la relación contractual. Cuando se termina la obligación contractual el funcionario está obligado a entregar al jefe inmediato o en caso de ser contratista a su supervisor las devoluciones de las credenciales que se les fueron asignadas.

6.4.4 Clasificación de la información

Cada Dependencia de la Alcaldía clasifican de acuerdo a la criticidad, sensibilidad y reserva de la misma, los activos de información, conforme a las leyes y normatividades actuales de la Alcaldía Distrital de Cartagena de Indias, los mismo se deben llevar a verificación mediante una

mesa de trabajo a las área de seguridad y privacidad de la información y Archivo General para garantizar que se encuentran bajo los parámetros establecidos por la normatividad Colombiana que rige para este ítem en particular.

La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizado, estableciendo la clasificación de activos de información y teniendo en cuenta que las convenciones y criterios de clasificación sean claros y estén documentados, que se defina cada cuanto debe revisarse la clasificación de un activo y que la clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad.

La clasificación de los activos se debe hacer de acuerdo con los siguientes parámetros:

a) Información Pública: En el Decreto 1377 de 2013 se define como*: "Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva"*

b) Información Privada o Reservada: Tomando la definición del MinTic es: *"aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional."*

c) Información Semiprivada: "*Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercia*l" según la ley 1581 del 2012.

d) Información Sensible: De acuerdo a la ley 1582 de 2012 es "*aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos*"

6.4.5 Etiquetado de la Información

El mecanismo, el responsable y la obligatoriedad de establecer pautas para el etiquetado o rotulación de Activos, es dirigido desde la Dirección de Archivo General, quien sigue las especificaciones dadas desde el Archivo General de la Nación y será almacenada bajo las mismas directrices establecidas de acuerdo con la norma vigente y siguiendo la estructura de las tablas de retención documental TRD y Tablas de Valoración Documental -TVD definidas. Para el etiquetado de la información se debe tener en cuenta las siguientes consideraciones:

a) Todos activos en formatos físicos y electrónicos requieren ser etiquetados (etiquetas físicas, metadatos)

b) El etiquetado debe reflejar el esquema de clasificación establecido
c) Los funcionarios y contratistas deben conocer el procedimiento de etiquetado

6.4.6 Manejo de los activos

El manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación se debe hacer teniendo en cuenta las siguientes consideraciones:

a) Las restricciones de acceso a los activos de información se realizarán de acuerdo con los requisitos de protección para cada nivel de clasificación
b) Todas las Dependencias del Distrito deben realizar el registro formal de los receptores autorizados de los activos; a través de los canales de SIGOB y de la plataforma SAUS, dispuestos por la Oficina asesora de informática.
c) La Oficina Asesora de Informática deben mantener la protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original, en cumplimiento al procedimiento de las copias de respaldo y restauración código GTIGI03-P001
d) Todas las Dependencias deben garantizar el almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes.

6.4.7 Gestión de medios removibles

Para todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores, se determina que los puertos USB, quemadores deben estar bloqueados salvo la necesidad especial la cual debe ser solicitada por medio del formato de solicitud de acceso a recursos digitales, con código GTIGPS02-F001, el cual debe estar debidamente diligenciado y debe ser tramitado a través de la mesa de servicios. El uso de medios removibles en la Alcaldía Distrital de Cartagena de Indias debe ir alineados a las clasificaciones de activos dispuestas en la política de “Clasificación de Activos”.

6.4.8 Disposición de los medios

Todos los activos que se encuentran bajo la responsabilidad de los funcionarios, contratistas o terceros es de obligatoriedad cumplir con el procedimiento entrega de equipos de cómputo y periféricos con código GTIGI04-P003 y el procedimiento para devolución de equipos informáticos con código GTIGI04-P002 mediante el cual se realiza de forma segura y correcta la creación, asignación, eliminación, retiro, y disposición final de los mismos.

6.4.9 Transferencia de medios físicos

Los secretarios de despacho, jefes de oficina, directores, gerentes, alcaldes locales deben garantizar la protección de los medios que contienen información durante el transporte, verificando los siguientes aspectos:

a) El uso de un transporte o servicios de mensajería confiables.
b) Se debe verificar el embalaje el cual debe proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito, y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protección contra cualquier factor ambiental que pueda

reducir la eficacia de la restauración del medio, tal como exposición al calor, humedad o campos electromagnéticos;

c) Se debe dejar registros del transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.

6.4.10 Creación de Activos

La asignación dependiendo de la clase de los activos se realiza, como se establece continuación:

a) Activos documentales físicos o digitales: Todos los manuales, procedimientos, procesos, instructivos, lista de chequeos, directorio de contactos, oficios, planes, políticas, proyectos, documentación generada por desarrollos in house, de acuerdo con los parámetros establecidos por la Secretaría General y etiquetados como lo dispone la Dependencia del Archivo General.

b) Activos software: Todas las aplicaciones informáticas, motores de base de datos, programas de desarrollo, aplicaciones de administración de proyectos; en si todo software, debe estar bajo la dirección de la Oficina Asesora de Informática traslado o re uso cuando ya no se requieran los activos. Se debe seguir los lineamientos del procedimiento para copias de seguridad de los activos evitando así el acceso o borrado no autorizado de la información.

6.5 DOMINIO 9: CONTROL DE ACCESO

Fuente

Este grupo de políticas hace referencia a todas aquellas directrices mediante las cuales la Alcaldía Distrital de Cartagena de Indias determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos; las políticas relacionadas con el control de acceso deben contemplar como mínimo:

6.5.1 Control de acceso con usuario y contraseña

a) El control de acceso a redes, aplicaciones, y/o sistemas de información de la Alcaldía Distrital de Cartagena de Indias, se deberá realizar mediante la solicitud en la mesa de servicios de acuerdo con lo establecido en el procedimiento para la solicitud de acceso GTIGPS02-P001 y una vez se haya diligenciado el formato de control de Acceso a Recursos Digitales GTIGPS02-F001 mediante el cual se determinen los responsables formalmente.
b) La creación, modificación, suspensión o eliminación de usuarios (ID) y asignación de contraseñas se debe centralizar en la Oficina Asesora de Informática.
c) La responsabilidad que los funcionarios, contratistas o terceros tengan un usuario y contraseña de acceso a los servicios que son pertinentes para su desempeño está a cargo de cada dependencia, que son quienes deben tramitar la solicitud ante la Oficina Asesora de Informática.
d) En la Alcaldía Distrital de Cartagena por medio de Talento Humano y la unidad o dependencia a la que pertenece el funcionario, contratista o tercero son responsables de informar a la Oficina Asesora de Informática por medio del formato de control de Acceso a Recursos Digitales GTIGPS02-F001 para que se asigne las personas el usuario y contraseña a los servicios que necesita para cumplir con la relación contractual establecida.

6.5.2 Suministro del control de acceso

a) La Oficina Asesora de Informática es la responsable de gestionar las solicitudes de asignación, modificación, desactivación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados, se debe también tenerse en cuenta los casos especiales con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la Alcaldía Distrital de Cartagena de Indias los cuales deben venir con la firma del jefe de la Oficina Asesora de informática en el formato de control de Acceso a Recursos Digitales GTIGPS02-F001.
b) Los usuarios genéricos o no, son de uso unitario; es decir, una cuenta NO debe ser utilizada por más de una persona.
c) Los desarrolladores, administradores de los recursos tecnológicos y servicios de red no tendrán acceso a sistemas de información en producción. Se restringe las conexiones remotas a los recursos de la plataforma tecnológica solo a personal debidamente autorizado y solo para las labores asignadas.

6.5.3 Gestión de Contraseñas

Para la administración de las contraseñas se deben tener en cuenta los siguientes lineamientos:

a) Las contraseñas son personales e intransferibles, y se prohíbe el uso de terceros.
b) Es responsabilidad de los funcionarios y contratistas el correcto uso de las contraseñas asignadas para el manejo de los aplicativos de la Alcaldía Distrital de Cartagena.
c) El acceso a los aplicativos se realiza mediante el procedimiento para la solicitud de acceso GTIGPS02-P001. No se realizarán accesos por fuera de este procedimiento.

d) El jefe inmediato dependiendo el rol del funcionario o contratista aprueba la solicitud de acceso a los sistemas de información.
e) La solicitud de acceso a sistemas tiene un tiempo determinado, dependiendo la duración del contrato o la relación del tercero con la entidad.
f) Los lineamientos a tener en cuenta para evaluar y en la asignación de las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la Alcaldía Distrital de Cartagena de Indias deben cumplir con los parámetros mínimos establecidos en el instructivo para la gestión de usuario y contraseña GTIGPS02-I002 el cual indica, que una contraseña sea considera como fuerte, gestión de cambio de contraseña, debe ser mínimo de 8 caracteres, alfanumérica, una letra en mayúsculas, con un carácter especial, la contraseña debe caducar cada tres meses y cambiar por una nueva la cual debe ser diferente de las cuatro últimas que han sido registradas con anterioridad.
g) El acceso de cuentas con a la red, las aplicaciones y sistemas de información deben requerir un usuario (ID) y una contraseña fuerte para que realice la correspondiente autenticación y acceso a la información de forma segura.

6.5.4 Acceso a redes y a servicios en red

El Distrito de Cartagena cuenta con el procedimiento de aseguramiento de servicios de red, el cual contiene los lineamientos para el aseguramiento de servicios red, lo cual incluye:

a) La Alcaldía Distrital de Cartagena de Indias entrega a todos los usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que necesite para el buen desarrollo de sus funciones contractuales.
b) Las contraseñas son estrictamente de uso personal e intransferible y es responsabilidad de cada usuario el uso de las credenciales asignadas.
c) Toda actividad que requiera acceder a los servidores, equipos o a las redes de la Alcaldía Distrital de Cartagena de Indias, se debe realizar presencialmente en las instalaciones. No se debe realizar ninguna actividad y/o ejercicio de tipo remoto sin la debida autorización de la Oficina Asesora de Informática.
d) La conexión remota a la red de área local de la Alcaldía Distrital de Cartagena de Indias debe ser establecida a través de una conexión VPN segura entregada por el Distrito, la cual debe ser autorizada por el jefe de la unidad o Dependencia, el Oficial de seguridad y privacidad de la información que se encuentra adscrito(a) a la Oficina Asesora de Informática, a través del formato de control de Acceso a Recursos Digitales GTIGPS02-F001.

6.5.5 Gestión de información de autenticación secreta de usuarios

El Distrito de Cartagena genera políticas para la asignación de información de autenticación secreta que se debe controlar por medio de un proceso de gestión formal. Para esto, se establece que:

a) Los secretarios de despacho, jefes de oficina, directores, gerentes, alcaldes locales, funcionarios, contratistas y terceros que realicen actividades al interior del Distrito de Cartagena deberán firmar una declaración para mantener la confidencial de la

información de autenticación secreta personal, y mantener la información de autenticación secreta del grupo (cuando es compartida).

b) Todo funcionario, contratista y tercero que realicen actividades al interior del Distrito deben mantener su propia información de autenticación secreta, la Oficina Asesora de Informática les suministra una autentificación secreta temporal segura, la cual deben a cambiar al usarla por primera vez.

6.5.6 Gestión de acceso a usuarios

Para la gestión de acceso a usuarios se deben tener en cuenta los siguientes lineamientos:

a) Los usuarios deben cambiar sus claves de acceso periódicamente, incluso pueden hacerlo antes de que la cuenta expire.
b) Los lineamientos a tener en cuenta para la asignación de las contraseñas se deben cumplir con los parámetros mínimos establecidos en el instructivo para la gestión de usuario y contraseña GTIGPS02-I001 el cual indica, que una contraseña debe contener mayúsculas, minúsculas, números y por lo menos un carácter especial y de una longitud mayor a 8 caracteres.
c) Los sistemas de información deben obligar al usuario a cambiar la contraseña por lo mínimo 1 vez cada 90 días.
d) Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por el administrador.
e) Se mantiene un registro de las 4 últimas contraseñas utilizadas por el usuario con el fin de evitar la reutilización de estas.
f) Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.
g) Cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware.
h) No se debe prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, jefes u otras personas que lo soliciten.
i) Todos los usuarios deben dar cumplimiento a las políticas de seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.
j) Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.
k) Reportar a la Oficina Asesora de Informática al correo seguridad.oai@cartagena.gov.co sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.
l) Está rotundamente prohibido utilizar las credenciales asignadas a un funcionario en otros equipos y para otros usuarios. Cada funcionario debe tener su cuenta.
m) El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de las plataformas y sistemas de información debe estar autorizado por la Oficina Asesora de Informática.

n) Todo equipo de cómputo que requiera acceso a la red interna de la Alcaldía Distrital de Cartagena de Indias deberá tener como mínimo las siguientes medidas de seguridad: solución de antimalware instalada, actualizada y parches de seguridad al día.

6.5.7 Ingreso seguro a los sistemas de información

El Distrito de Cartagena cuenta con el Instructivo para ingreso a los sistemas de información GTIGPS01-I004, el cual contiene los lineamientos para el ingreso seguro a los sistemas de información, lo cual incluye:

a) No visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso se haya completado exitosamente;
b) Visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador;
c) Evitar los mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado;
d) Validar la información de ingreso solamente al completar todos los datos de entrada ante una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta;
e) Proteger contra intentos de ingreso mediante fuerza bruta.
f) Llevar un registro con los intentos exitosos y fallidos.
g) Declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso.

Visualizar la siguiente información al terminar un ingreso seguro:

a) Registrar la fecha y la hora del ingreso previo exitoso.
b) Registrar los detalles de cualquier intento de ingreso no exitoso desde el último ingreso exitoso.
c) No visualizar una contraseña que se esté ingresando.
d) No transmitir contraseñas en un texto claro en una red.
e) Terminar sesiones inactivas después de un período de inactividad definido, especialmente en lugares de alto riesgo tales como áreas públicas o externas por fuera de la gestión de seguridad de la organización o en dispositivos móviles.
f) Restringir los tiempos de conexión para brindar seguridad adicional para aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.

6.5.8 Políticas sobre perímetros de seguridad

Para los perímetros de seguridad se deben tener en cuenta los siguientes lineamientos:

a) Los lugares de alta confidencialidad y que los mismos contengan información confidencial o privada, semiprivada y/o sensible ya sean en físico o digital deben contar con la autorización para su acceso pues las mismas áreas son delimitadas como de acceso restringido.
b) El acceso a los centros de cómputo siempre debe estar acompañado de un funcionario adscrito a la Oficina Asesora de Informática y con previa autorización.

6.5.9 Políticas para la revisión de los derechos de acceso de los usuarios

El Distrito de Cartagena debe aplicar políticas para la revisión de los derechos de acceso de los usuarios, lo cual incluye:

a) 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, debe ser revisada periódicamente y cada vez que se realicen cambios de personal.
b) Para el retiro de los derechos de acceso, cada dependencia de la Alcaldía Distrital de Cartagena de Indias y la Dirección de Talento humano son los responsables de comunicar a la Oficina Asesora de Informática, las novedades relacionadas como el cambio de cargo, funciones o actividades o la terminación contractual de los colaboradores pertenecientes a cada Dependencia.

6.5.10 Política para el manejo de copias de seguridad

Para el manejo de las copias de seguridad en el Distrito de Cartagena se deben tener en cuenta los siguientes lineamientos:

- Por ningún motivo se permite alojar en las copias de seguridad, información catalogada como personal, música, videos, documentos transitorios, documentos confidenciales, backups de equipos de escritorio, backups de correo electrónico y demás que no sea relevante en el cumplimiento de los objetivos de la Alcaldía.
- Los líderes de proceso y jefes de Dependencias son los únicos autorizados para solicitar al jefe de la Oficina Asesora de Informática, el respaldo y/o recuperación de información mediante el formato dispuesto para tal fin, indicando los datos del solicitante, datos de la aplicación, datos de los archivos (tipo y ubicación), datos del BD (ubicación, motor y versión), accesos, periodicidad de respaldo y tipo de respaldo. Siempre que exista alguna modificación o adición en la fuente de la información, se debe generar el formato descrito y entregarlo al administrador de copias o quien haga sus veces.
- Identificar claramente la información crítica que se debe respaldar, indicando los niveles de seguridad e incluir las condiciones necesarias para futuras restauraciones.
- Se debe garantizar la custodia y almacenamiento de los medios magnéticos
- El software de respaldo y restauración de información debe estar instalado en los servidores para los cuales se haya hecho solicitud de backups. Se debe contar con las licencias necesarias que garanticen el cumplimiento de dicha solicitud.
- El administrador de copias diariamente revisará los logs, anotará los eventos o novedades sucedidos durante la copia del día anterior en el formato registro diario de novedades de backups, el cual contendrá nombre de la tarea, fecha, hora, novedades y acción a tomar.
- El usuario final es responsable de la información que maneja, y cumplir con las políticas de seguridad y privacidad de la información mientras este bajo su custodia.
- Los líderes de proceso y jefes de dependencias son los únicos autorizados para solicitar a la Oficina Asesora de Informática, el respaldo y/o recuperación de información mediante el formato dispuesto para tal fin, indicando los datos del solicitante, datos de la aplicación, datos de los archivos (tipo y ubicación), datos del BD (ubicación, motor y

versión), accesos, periodicidad de respaldo y tipo de respaldo. Siempre que exista alguna modificación o adición en la fuente de la información, se debe generar el formato descrito y entregarlo al administrador de copias o quien haga sus veces.

- Identificar claramente la información crítica que se debe respaldar, indicando los niveles de seguridad e incluir las condiciones necesarias para futuras restauraciones.
- Se debe garantizar la custodia y almacenamiento de los medios magnéticos o almacenamiento de nube, bajo la protección de la OAI en donde se disponga.
- El líder designado por la Oficina Asesora de Informática vigilará diariamente el perfecto cumplimiento de la copia de seguridad, revisando el registro diario de novedades de Backups diligenciado por el Administrador de copias.

6.6 DOMINIO 10: CRIPTOGRAFIA

Fuente

Para el manejo de las criptografías en el Distrito de Cartagena se deben tener en cuenta los siguientes lineamientos:

a) El Distrito de Cartagena utiliza encriptaciones en comunicaciones de acceso externo a través de VPN (Red privada virtual), esta es una tecnología que permite crear una conexión segura y cifrada entre dos dispositivos a través de Internet. En otras palabras, una VPN permite que los usuarios de la Entidad naveguen por Internet de forma segura y privada, ocultando su dirección IP y cifrando sus datos para evitar que sean interceptados por terceros.
b) El Distrito de Cartagena utiliza el certificado SSL (Capa de sockets seguros) para el uso de páginas web de la Entidad para garantizar que los datos transferidos entre usuarios y sitios web, o entre dos sistemas, sean imposibles de leer. Utiliza algoritmos de cifrado para cifrar los datos en tránsito, lo que evita que los hackers lean la información que se envía a través de la conexión. Este certificado digital autentica la identidad de un sitio web y habilita una conexión cifrada.
c) El Distrito de Cartagena, utiliza tecnología SD-WAN y SD-LAN segura como servicio, que garantiza que el intercambio de datos entre oficinas y sedes que están interconectadas accedan de forma segura a las aplicaciones y sistemas de información, esto es porque la tecnología utiliza túneles de encriptación que permite que la información viaje encriptada desde la LAN hasta las aplicaciones y viceversa.

6.7 DOMINIO 11: SEGURIDAD FISICA Y DEL ENTORNO

Fuente

En esta política se busca evitar accesos físicos no autorizados a las instalaciones de la Alcaldía Distrital de Cartagena de Indias, y proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información que pueda ser vulnerada, eliminada o alterada, o que pueda estar expuesta y generar incumplimiento frente a la confidencialidad, integridad o disponibilidad.

6.7.1 Perímetro de Seguridad Física

Para el manejo los perímetros de seguridad física en el Distrito de Cartagena se deben tener en cuenta los siguientes lineamientos:

a) Todas las entradas que utilizan un sistema de control de acceso deben permanecer cerradas y es responsabilidad de todos los funcionarios, contratistas y terceros autorizados evitar que las puertas se dejen abiertas.
b) Todos los funcionarios y contratistas, sin excepción deben portar su carné o escarapela en un lugar visible mientras permanezcan dentro de las instalaciones de la Alcaldía Distrital de Cartagena de Indias.
c) Los visitantes deben permanecer acompañados de un funcionario y/o contratista de la Alcaldía Distrital de Cartagena de Indias, cuando se encuentren en las oficinas o áreas donde se maneje información.
d) Es responsabilidad de todos los funcionarios, contratistas y terceros de la Alcaldía Distrital de Cartagena de Indias borrar toda información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. De igual manera, no se debe dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.
e) Los visitantes que requieran ingresar a las oficinas de la Alcaldía Distrital de Cartagena de Indias deben permanecer acompañado de un funcionario o contratistas, salvo las oficinas de atención al ciudadano.
f) Los visitantes que requieran permanecer en las oficinas de la Alcaldía Distrital de Cartagena de Indias por periodos superiores a un (1) días deben ser presentados al personal de la oficina donde permanecerán.
g) El horario autorizado para recibir visitantes en las instalaciones de la Alcaldía Distrital de Cartagena de Indias es de lunes a viernes de 8:00 a.m. a 12:00 p.m. Y de 2:00 p.m. a 5:00 p.m. En horarios distintos se requerirá de la autorización del director jefe de Oficina de la dependencia correspondiente.

h) Los dispositivos de almacenamiento removibles, así como toda información CONFIDENCIAL de la Alcaldía Distrital de Cartagena de Indias, independientemente del medio en que se encuentre, deben permanecer bajo seguridad durante horario no hábil o en horarios en los cuales los funcionarios o contratistas responsables no se encuentre en su sitio de trabajo.
i) Las instalaciones de la Alcaldía Distrital de Cartagena de Indias deben estar equipadas de un circuito cerrado de TV y control de acceso con el fin de monitorear y prevenir algún incidente de seguridad frente a los activos de información o tecnológicos.

6.7.2 Seguridad de oficinas, recintos e instalaciones

El Distrito de Cartagena debe aplicar políticas para seguridad física a oficinas, recintos e instalaciones, tales como:

a) En las edificaciones del Distrito donde se realizan actividades de procesamiento de información se deben tener controles para el acceso, con el fin de evitar que personal ajeno a la Dependencia tenga acceso a ello.
b) En las instalaciones donde se procese información de carácter confidencial se debe mantener el máximo de reservas y restringir el acceso.
c) Cada Dependencia debe definir directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial que no deben ser accesibles a ninguna persona no autorizado.

6.7.3 Controles de Acceso Físico

El Distrito de Cartagena debe aplicar políticas para los controles de accesos físicos, para la protección física y ambiental, tales como:

a) Las áreas seguras dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.
b) En las áreas seguras, en ninguna circunstancia se puede fumar, comer o beber.
c) Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un o colaboradores del proceso. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.
d) Se debe contar con al menos dispositivos de control de acceso físico a los Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, el cual garantice el acceso a solo el personal autorizado.

6.7.4 Ubicación y Protección de los equipos

Para la ubicación y protección de los equipos, se deben tener en cuenta las siguientes consideraciones:

a) La plataforma tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

b) Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.
c) Autorizar y gestionar el acompañamiento permanente de los visitantes a las áreas de procesamiento de información y centros de comunicación.
d) Registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia.
e) Proveer las condiciones físicas y medioambientales necesarias y óptimas para garantizar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo, los cuales deben ser monitoreados de manera permanente.
f) Las áreas de carga y descarga deben estar aisladas de equipos de cómputo, del centro de cómputo y otras áreas de procesamiento de información.
g) Velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados
h) Autorizar los ingresos temporales a sus áreas, evaluando la pertinencia del ingreso; y definir los responsables del registro y supervisión de los ingresos autorizados a sus áreas.

6.7.5 Mantenimiento de equipos

Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad de acuerdo con el Instructivo para la elaboración de mantenimiento preventivo código GTIGI04-I001, mediante el cual se establece lo siguiente:

a) Se debe programar los mantenimientos de los equipos de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor;
b) Establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos.
c) Todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo; se debe reportar a través de la plataforma SAUS.
d) Implementar los controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debe borrar del equipo, o el personal de mantenimiento debería retirarse (cleared) lo suficientemente de la información;
e) Establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.

6.7.6 Retiro de Equipos de Activos

El Distrito de Cartagena cuenta con el procedimiento para la baja de activos informáticos código GTIGI04-P004 y el formato acta de baja de equipos y periféricos código GTIGI04-F002, el cual contiene los lineamientos para el retiro de los equipos, lo cual incluye:

a) Ningún equipo de cómputo, información o software debe ser retirado de la Alcaldía Distrital de Cartagena de Indias sin una autorización formal por parte de la Oficina Asesora de Informática.
b) La Oficina Asesora de Informática realiza periódicamente comprobaciones puntuales para detectar el retiro no autorizado de activos de la Alcaldía Distrital de Cartagena de Indias.

6.7.7 Seguridad de los equipos fuera de las instalaciones

Para la seguridad de los equipos que se encuentran fuera de las instalaciones, se deben tener en cuenta las siguientes consideraciones:

a) De acuerdo con la política de protección de datos, los equipos portátiles y de mesa que contengan información clasificada como CONFIDENCIAL o RESERVADA, deben contar con controles de seguridad que garanticen la confidencialidad de la información, y la misma debe estar encriptada.
b) Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En casos de viaje siempre se debe llevar como equipaje de mano y resguardado.
c) En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente a la Oficina Asesora de Informática. Así mismo, se debe poner la denuncia ante las autoridades competentes y se debe hacer llegar copia de esta.
d) Para el caso de los equipos que cuentan con puertos de transmisión y recepción de infrarrojo y Bluetooth estos deben estar deshabilitados.
e) La salida de equipos tecnológicos del Distrito de Cartagena se encuentra restringida. En caso de requerir el traslado de estos equipos se debe solicitar autorización a los jefes de áreas diligenciando el acta de entrega de equipos de cómputo y periféricos GTIGI04-F003
f) Todos los equipos de cómputo deben ser registrados al ingreso y al retirarse de las instalaciones de la Alcaldía Distrital de Cartagena de Indias.

6.7.8 Seguridad en la reutilización o eliminación de los equipos

Cuando un equipo de cómputo sea reasignado, devuelto o dado de baja, se debe realizar de acuerdo con el procedimiento baja de activos informáticos código GTIGI04-P004 y el acta de baja de equipos y periféricos código GTIGI04-F002, de igual forma realizar una copia de respaldo de la información que se encuentre almacenada de acuerdo al procedimiento de copias de respaldo y restauración código GTIGI03-P001, para ello se debe solicitar a la mesa de servicios de la Oficina Asesora de Informática, por medio de la herramienta SAUS. Posteriormente debe ser sometido al procedimiento de borrado seguro de la información y de los softwares instalados, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

6.7.9 Política de escritorio y pantalla despejados

Para mantener los escritorios y pantallas despejadas, se deben tener en cuenta las siguientes consideraciones:

a) Todo el personal de funcionarios y contratistas de la Alcaldía Distrital de Cartagena de Indias debe conservar su escritorio libre de información propia de la Entidad que contenga información sensible, privada e importante, que pueda ser copiada, movida,

utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

b) Todo el personal de funcionarios y contratistas de la Alcaldía Distrital de Cartagena de Indias debe bloquear la pantalla de su equipo cuando no estén haciendo uso de él o que por cualquier motivo deban dejar su puesto de trabajo.
c) Todo el personal de funcionarios y contratistas al finalizar sus ejercicios diariamente deben salir de todas las aplicaciones y apagar las estaciones de trabajo.
d) En horario no hábil o cuando los puestos de trabajo se encuentren libres, los funcionarios y contratistas deben dejar la información CONFIDENCIAL protegida bajo llave o en un lugar seguro para evitar fuga, replica o eliminación de los datos.

6.8 DOMINIO 12: SEGURIDAD DE LAS OPERACIONES

Fuente

6.8.1 Procedimientos de operación documentados

La Oficina Asesora de Informática tiene a disposición del Distrito de Cartagena los procedimientos de operación en el siguiente enlace Gestión Tecnología e Informática | MIPG - Alcaldía distrital de Cartagena de indias en el cual se encuentra lo siguiente:

a) Manuales e instructivos para la instalación y configuración de sistemas;
b) Procedimientos e instructivos para establecer la gestión de las copias de respaldo;
c) Formato para definir los requisitos de programación (Desarrollo de Software), incluidas las interdependencias con otros sistemas, los tiempos de finalización del primer y último trabajos.
d) Formato planeación y gerencia de proyectos.
e) Instructivo desarrollo de software.
f) Procedimientos e instructivos para definir la gestión de la información de rastros de auditoría y de información del log del sistema.

6.8.2 Gestión de cambios

La Oficina Asesora de Informática tiene un procedimiento mediante el cual se controla los cambios en la organización en materia de infraestructura tecnológica de acuerdo con los procesos de negocios, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información, el cual contiene:

a) Identificación y registro de los cambios significativos;
b) Planificación y aprobación de los cambios;
c) Valoración de los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información;
d) Aprobación formal para los cambios propuestos;
e) Verificación de que se han cumplido los requisitos de seguridad de la información;
f) Comunicación de los cambios a todas las personas pertinentes;
g) Tener un procedimiento de apoyo, incluidos procedimientos y responsabilidades para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos;
h) Contar con un suministro de un proceso de cambio de emergencia que posibilite la implementación rápida y controlada de los cambios necesarios para resolver un incidente.

6.8.3 Separación de los ambientes de desarrollo, pruebas y operación

El Distrito de Cartagena cuenta con el procedimiento para la separación de ambientes de desarrollo pruebas y operación, el cual contiene los lineamientos para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación, lo cual incluye:

a) Definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de operaciones.
b) Establecer que el software de desarrollo y de operaciones debe funcionar en diferentes sistemas o procesadores de computador y en diferentes dominios o directorios;
c) Definir que los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales;
d) Definir que solo en circunstancias excepcionales, las pruebas no se deben llevar a cabo en los sistemas operacionales;
e) Establecer que los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no debe ser accesibles desde sistemas operacionales cuando no se requiere;
f) Establecer que los usuarios deben usar diferentes perfiles de usuario para sistemas operacionales y de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error;
g) Definir que los datos sensibles no se deben copiar en el ambiente del sistema de pruebas, a menos que se suministren controles equivalentes para el sistema de pruebas.

6.8.4 Control contra códigos maliciosos

El Distrito de Cartagena cuenta con el procedimiento de protección contra códigos maliciosos código GTIGPS02-P002, el cual contiene los lineamientos para la prevención, detección y

corrección frente a las amenazas causadas por códigos maliciosos en la Entidad, lo cual incluye:

a) Se prohíbe la conexión de cualquier equipo en la red de la Alcaldía que no cuente con antivirus instalado y actualizado.
b) La Oficina Asesora de Informática a través de la mesa de servicios, deben garantizar que los funcionarios y/o contratistas no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
c) Los funcionarios y/o contratistas no deberán hacer uso de software que no sea instalado por Infraestructura y mesa de servicios, toda vez que esto puede llevar a infecciones por virus u otro tipo de código malicioso.
d) Los funcionarios y/o contratistas deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos o instalación de software malicioso.
e) Para evitar problemas de códigos maliciosos a través de medios extraíbles o correo electrónico, los funcionarios y/o contratistas, deben realizar la verificación respectiva de los archivos a través del software de antivirus, instalado en sus equipos cada vez que instale o conecte un dispositivo o se reciban archivos sospechosos por correo electrónico.
f) La Oficina Asesora de Informática difundirá mediante los medios de comunicación los posibles riegos y los cuidados para tener en cuenta frente a una amenaza.
g) Se prohíbe el uso de software no autorizado.
h) Todas las Dependencias de la Alcaldía deben procurar que se lleven a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; solicitando que investiguen formalmente la presencia de archivos no aprobados o de enmiendas no autorizadas;
i) Todo el personal de funcionario o contratistas que desarrollen actividades dentro de las instalaciones del Distrito deben realizar análisis de cualquier archivo recibido por la red o por cualquier forma de medio de almacenamiento, para detectar el software malicioso, antes de uso.
j) El Distrito de Cartagena debe preparar planes de continuidad del negocio apropiados, para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para la recuperación.

La Alcaldía de Cartagena cuenta con lineamientos para el control contra códigos maliciosos, lo cual incluye:

a) Se tiene que proveer controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.
b) Contamos con una protección de manipulación de políticas utilizando endpoints en donde los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.

c) La Oficina Asesora de Informática se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.
d) Todos los colaboradores y terceros que hacen uso de los servicios de tecnología de la información y comunicaciones de la Alcaldía son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.
e) La Alcaldía cuenta con el software necesario como antivirus para protección a nivel de red y de estaciones de trabajo, contra virus y código malicioso, el servicio es administrado por la Oficina Asesora de Informática.
f) La herramienta de antivirus sólo debe ser instalados por los responsables de la Oficina Asesora de Informática.
g) Los colaboradores y terceros de la Alcaldía pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los colaboradores y terceros cuando sea necesario siempre podrán consultar a la Oficina Asesora de Informática sobre el tratamiento que debe darse en caso de sospecha de malware.
h) Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por la Alcaldía, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta establecida para ello.

6.8.5 Respaldo de información

El Distrito de Cartagena cuenta con el instructivo para copias de respaldo para equipos de cómputo código GTIGI04-I002, el procedimiento copias de respaldo y restauración código GTIGI03-P001 y el formato solicitud respaldo de información código GTIGI03-F001, el cual contiene los lineamientos para asegurar el respaldo de la información, lo cual incluye:

a) Los registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados.
b) La cobertura (copias de respaldo completas o diferenciales) y la frecuencia con que se hacen las copias de respaldo las cuales reflejan los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada, y la criticidad de la información para la operación continua de la organización;
c) Las copias de respaldo se deben almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal;
d) La información de respaldo y un nivel apropiado de protección física y del entorno, de coherencia con las normas aplicadas en el sitio principal;
e) Los medios de respaldo se deben poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; esto se debería combinar con una prueba de los procedimientos de restauración, y se debe verificar contra el tiempo de restauración requerido.

f) Las situaciones en las que la confidencialidad tiene importancia, las copias de respaldo deben estar protegidas por medio de encriptación.

6.8.6 Registro de eventos

Se debe contar con una herramienta que permita elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información, la cual debe tener lo siguiente

a) Identificación de los usuarios;
b) Establecer las actividades del sistema;
c) Definir las fechas, horas y detalles de los eventos clave, (entrada y salida);
d) Identificar el dispositivo o ubicación, si es posible, e identificador del sistema;
e) Tener registros de intentos de acceso al sistema exitosos y rechazados;
f) Definir registros de datos exitosos y rechazados y otros intentos de acceso a recursos;
g) Establecer los cambios a la configuración del sistema;
h) Definir el uso de privilegios;
i) establecer el uso de utilitarios y aplicaciones del sistema;
j) definir los archivos a los que se tuvo acceso, y el tipo de acceso;
k) establecer las direcciones y protocolos de red;
l) definir las alarmas accionadas por el sistema de control de acceso;
m) activar y desactivar los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión;
n) registrar las transacciones ejecutadas por los usuarios en las aplicaciones.

6.8.7 Protección de la información de registro

Se debe contar con herramientas que permitan configurar el control para que todas las instalaciones y la información de registro sean protegidas contra alteración y acceso no autorizado.

Revisar los procedimientos y controles dirigidos a proteger contra cambios no autorizados de la información del registro y contra problemas con la instalación de registro, que incluya:

a) verificar todas las alteraciones a los tipos de mensaje que se registran;
b) establecer los archivos log que son editados o eliminados;
c) verificar cuando se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobre escritura de eventos pasados registrados.

6.8.8 Registros del administrador y del operador

El tercero (nube) deben reportar al gestor del área de infraestructura de la Oficina Asesora de Informática las actividades del administrador y del operador del sistema que deben ser registradas, y revisar con regularidad.

6.8.9 Sincronización de relojes

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro del Distrito se deben sincronizar con una única fuente de referencia de tiempo, como puede ser el Directorio activos o servicios NTP (protocolo de tiempo de red).

6.8.10 Instalación de software en sistemas operativos

Para mantener las instalaciones de software en los sistemas operativos, se deben tener en cuenta los siguientes controles:

a) La Oficina Asesora de Informática, debe utilizar usuarios de dominio mediante políticas de grupo GPO del directorio activo. Esta directiva (GPO: Group Policy Object) debe establecer una configuración para la totalidad de los equipos unidos al dominio de la Alcaldía, y deben ser configuradas de tal forma que solo la parte técnica, dueño del usuario administrador, es el único con la potestad de realizar instalaciones de software y aplicaciones.
b) Los sistemas operacionales sólo deben contener códigos ejecutables aprobados, no el código de desarrollo o compiladores.
c) El área de desarrollo deberá asegurar que las aplicaciones y el software del sistema operativo solo se debe implementar después de pruebas extensas y exitosas; los ensayos deben abarcar la usabilidad, la seguridad, los efectos sobre otros sistemas y la facilidad de uso, y se debe llevar a cabo en sistemas separados; se debe asegurar que todas las bibliotecas de fuentes de programas correspondientes hayan sido actualizadas.
d) Todo el software implementado debe ser registrados en el acta de entrega de equipos de cómputo y periféricos con código GTIGI04-F003 al igual que la documentación del sistema.
e) Se deben realizar validaciones de efectividad del software instalado y en caso de requerirlo se hará un (rollback) antes de implementar los cambios.
f) Todas las versiones de software anteriores se deben llevar al archivo permanente, diligenciando el formato control de cambios de software con código GTIGS01-F007, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores.

6.8.11 Gestión de la vulnerabilidad técnica

La Oficina Asesora de Informática debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la Entidad a estas vulnerabilidades y tomar las medidas apropiadas para tratar el riesgo asociado.

a) La Oficina Asesora de Informática debe seguir el instructivo para la definición de roles y responsabilidades del modelo de seguridad y privacidad de la información código GTIGPS01-I002 para establecer los roles y responsabilidades asociados con la gestión y seguimiento de la vulnerabilidad técnica, el seguimiento de activos y toda responsabilidad de los gestores del área.
b) La Oficina Asesora de Informática una vez haya identificado una vulnerabilidad técnica, deberá identificar los riesgos asociados y las acciones correctivas, así como registrando estos en la herramienta de SAUS.

c) Cuando se materializa un riesgo se debe gestionar de acuerdo con lo descrito en el procedimiento de gestión de incidentes de seguridad de la información con código GTIGPS02-P005.
d) El líder de seguridad informática debe realizar un seguimiento y evaluación regulares del proceso de gestión de vulnerabilidad, con el fin de asegurar su eficacia y eficiencia.

6.8.12 Restricciones sobre la instalación de software

El Distrito de Cartagena, deberá establecer e implementar las reglas para la instalación de software por parte de los usuarios.

6.9 DOMINIO 13: SEGURIDAD DE LAS COMUNICACIONES

Fuente

6.9.1 Controles de redes

Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones, y se debe tener en cuenta los siguientes lineamientos:

a) La Oficina Asesora de Informática deben definir las responsabilidades y procedimientos para el área de infraestructura relacionada a la gestión de equipos de redes.
b) El área de infraestructura de la Oficina Asesora de Informática debe ser el responsable de segmentar las redes por sedes y servicios.
c) El área de infraestructura y de seguridad deben instalar equipos de redes controlados con claves seguras y establecer canales de datos que conserven y salvaguarden la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas, para proteger los sistemas y aplicaciones conectados.
d) Aplicar logging y seguimientos adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información.
e) Se deben definir las actividades de los gestores de las diferentes áreas de la Oficina Asesora de Informática para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.
f) Todos los equipos que sean conectados a la red institucional deben estar dentro del dominio y con una IP autorizada.

6.9.2 Seguridad de los servicios de red

Para la seguridad de los servicios de la red, se deben tener en cuenta las siguientes consideraciones:

a) Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
b) Establecer la tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red;
c) Definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red;
d) Establecer los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.

6.9.3 Separación en las redes

La Alcaldía Distrital de Cartagena de Indias determina que dentro de la política de separación en las redes y acorde a las pautas del NIST (Instituto Nacional de Estándares y Tecnología de los Estados Unidos) es fundamental proteger la integridad de los sistemas y datos en la Entidad, y se deben tener en cuenta las siguientes consideraciones:

a) Utilizar controles técnicos para implementar la separación de redes, como firewalls, routers, VLAN (Virtual LAN), ACL (Listas de Control de Acceso) y sistemas de detección de intrusiones (IDS/IPS).
b) Una vez determine qué comunicaciones son necesarias entre los segmentos de red y establezca reglas claras para permitirlas, esto podría incluir comunicaciones esenciales para la operación de la organización.

6.9.4 Políticas y procedimientos de transferencia de información

La Oficina Asesora de Informática tiene un procedimiento el cual debe seguirse de manera sistemática y organizada para lograr una transferencia de información de manera segura y se debe tener en cuenta las siguientes consideraciones para la mensajería electrónica:

- Asegurar el direccionamiento y transporte correcto del mensaje
- La confiabilidad y disponibilidad del servicio.
- Niveles más fuertes de autenticación para control del acceso desde redes públicas.

En todos los contratos o acuerdos del Distrito con terceras partes, que implique un intercambio uso o procesamiento de información, se deben realizar acuerdos de confidencialidad y/o acuerdos de protección de datos, los cuales deben hacer parte integral de los contratos o documentos que legalicen la relación contractual.

6.9.5 Acuerdos sobre transferencia de información

En los acuerdos se deben tener en cuenta la transferencia segura de información entre el Distrito y las partes externas. Para ello la Entidad cuenta con herramientas tecnológicas que

ayudan a medir la trazabilidad de la información a partir del aplicativo SIGOB. Por lo cual se debe tener en cuenta las siguientes consideraciones:

a) Establecer las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo.
b) Aplicar lo descrito en el procedimiento del manual de SIGOB para asegurar la trazabilidad.
c) Todos los contratos o acuerdos de la Alcaldía con terceros, que impliquen un intercambio, uso o proceso de información del Distrito, se deben realizar acuerdos de confidencialidad y protección de datos sobre el manejo de la información.
d) A través de los codificadores y tipo de correspondencia interna o externa se deben identificara la mensajería.
e) El Distrito ha establecido que todos los usuarios del sistema de correspondencia SIGOB deben ser responsables de la seguridad y protección de la información gestionada.
f) Establecer el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente
g) Se deben implementar las normas técnicas para registro y lectura de información descritas en el manual del sistema de correspondencia SIGOB.
h) Deben existir niveles de controles de accesos aceptables configurados.

6.9.6 Mensajería electrónica

La Entidad debe contar con contraseñas para la mensajería electrónica, con cambios periódicos y deben ser sincronizadas y controladas con el Directorio Activo.

Revisar las siguientes directrices para mensajería electrónica:

a) La protección de mensajes contra acceso no autorizado, modificación o denegación del servicio debe estar ajustado al esquema de clasificación adoptado por la Entidad.
b) El servicio de mensajería debe ser confiable y disponible
c) Se debe cumplir con una aprobación y una cuenta institucional antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información.
d) Se debe realizar doble autenticación de los correos institucionales que son los únicos autorizados para el acceso a redes accesibles públicamente.

6.9.7 Acuerdos de confidencialidad o de no divulgación

Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la Entidad para la protección de la información, lo cual incluye:

a) Se debe clasificar la información que se va a proteger, de acuerdo con el instructivo para la identificación y clasificación de los activos de información con código GTIGPS01-I006
b) Se deben incluir las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información en los acuerdos de confidencialidad de acuerdo con lo establecido.

c) definir el uso permitido de información confidencial y los derechos del firmante para usar la información;
d) Se deben controlar el derecho a actividades de auditoría y de seguimiento que involucran información confidencial, mediante la firma del formato establecido como acuerdo de confidencialidad y protección de datos.
e) Control disciplinario debe tomar las acciones que se espera tomar en caso de violación del acuerdo.

6.9.8 Políticas para el servicio de computación en la nube

Para la política de los servicios de computación en la nube, se deben tener en cuenta las siguientes consideraciones:

a) Los activos de información de la Alcaldía Distrital de Cartagena de Indias que sean autorizados a ser tratados en los servicios de computación en la nube deben lograr garantizar la disponibilidad, privacidad, confidencialidad, integridad y cumplimiento de los requisitos legales en materia de protección de información personal.
b) La utilización de servicios de computación en la nube de carácter gratuito o abierto debe ser aprobada por la OAI, quienes contemplarán desde las diferentes esferas y teniendo en cuenta la estrategia de Gobierno Digital frente a la seguridad y privacidad.
c) En cualquier contrato celebrado con proveedores de servicios de computación en la nube se debe incluir la necesidad de cumplir las políticas de seguridad digital, el cumplimiento de los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual sobre la información, leyes y regulaciones sobre la protección de la información de la Entidad e información de carácter personal.
d) El uso de plataformas internacionales de almacenamiento o procesamiento en la nube para datos de carácter personal deben contar con la autorización del titular de los datos. No se debe almacenar datos personales en servicios de computación en la nube sin la autorización del titular para la transmisión internacional de datos.
e) Se deben realizar y evaluar controles para mitigar los riesgos de seguridad digital a través de los monitoreos periódicos reportados por el proveedor.
f) Proveer servicios de copia de respaldo para la información que está autorizada para almacenamiento en computación en la nube.
g) Mantener inventario de los servicios de computación en la nube autorizados para uso dentro de las redes institucionales, incluyendo el inventario de servidores, sistemas de información y las licencias de Microsoft office 365
h) Mantener inventario de los usuarios a los que se les autoriza el uso de servicios de computación en la nube, el cual deben ser controlados por el profesional de control de accesos
i) Asegurar la existencia de acuerdos y/o cláusulas de confidencialidad con proveedores de servicios de computación en la nube.
j) Especificar responsabilidades sobre el uso de servicios de computación en la nube (almacenamiento y/o procesamiento) en el formato acta de entrega de equipos de

cómputo y periféricos con código GTIGI04-F003, el cual es administrado por el proceso de infraestructura.

k) Garantizar que en los contratos con los proveedores tienen la capacidad para demostrar que los servicios ofrecidos cuentan con certificación en ciberseguridad emitida por ente independiente al prestador de servicios; así como, el derecho de auditoría independiente al cumplimiento de seguridad y requisitos legales aplicables a la Alcaldía.

l) No almacenar información sujeta a derechos de autor (videos, imágenes, audio, libros, entre otros).

6.9.9 Política de disponibilidad del servicio e información

La Alcaldía Distrital de Cartagena de Indias deberá contar con un plan de continuidad del negocio 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, ante el evento de un incidente de seguridad de la información.

La política de disponibilidad debe cumplir con los siguientes aspectos:

- Niveles de disponibilidad: La Oficina Asesora de Informática debe velar por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con clientes, proveedores y/o terceros en función de las necesidades de la Alcaldía Distrital de Cartagena de Indias, los acuerdos de nivel de servicios ofrecidos y evaluaciones de riesgos.
- Planes de recuperación: Es responsabilidad de todas las Dependencias y oficinas establecer los planes de recuperación en los que se incluyan las necesidades de disponibilidad de la Alcaldía Distrital de Cartagena de Indias.
- Interrupciones: Toda acción que se realice en las Dependencias de la Alcaldía y que conlleve a interrupciones en los servicios ya sea por mantenimiento programados o por alguna eventualidad y que afecten la disponibilidad del mismo deben ser supervisados y monitoreados con el acompañamiento de la Oficina Asesora de Informática.
- Acuerdos de Nivel de servicio: Se deben definir los acuerdos de niveles de servicios (ANS) para las interrupciones de los servicios.
- Segregación de ambientes: Se deben configurar ambientes de desarrollo, pruebas y producción para minimizar los riesgos inherentes de los cambios y nuevos desarrollos.
- Gestión de Cambios: Todos los cambios deben ser gestionados bajo condiciones controladas. Esta deberá estar apoyada con herramientas tecnológicas que ayuden a mantener un control de versionamiento, gestionado dentro de un entorno controlado y planificado.

6.9.10 Política de gestión de seguridad de las redes

La Entidad debe 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.

La segmentación de red es un enfoque de arquitectura que divide una red en varios segmentos o subredes, que actúan como redes pequeñas. Esto les permite a los administradores de red controlar el flujo de tráfico entre subredes según políticas detalladas. El Distrito debe usar la segmentación para mejorar la supervisión, aumentar el rendimiento, identificar problemas técnicos y, lo más importante, mejorar la seguridad.

El acceso a los recursos de red inalámbrica debe ser restringido y se solicitará a los usuarios la identificación por MAC, a través del formato de solicitud de acceso a recursos digitales con código GTIGPS02-F001, esto nos ayudará a tener un mayor control y separar las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.

6.9.11 Políticas para la sensibilización y capacitación en seguridad de la información

La Oficina Asesora de Informática cuenta con un manual plan de capacitación, sensibilización y comunicación de seguridad de la información con código GTIGPS01-M004, lo cual se debe actualizar cada año con el fin de garantizar la formación del personal en temas relacionados con la seguridad y privacidad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano, siguiendo como parámetros lo siguiente:

- Todo el personal de la alcaldía debe ser capacitados.
- Todos los funcionarios y contratistas tienen la obligación de asistir a los eventos o cursos de capacitación.

6.10 DOMINIO 14: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Fuente

6.10.1 Análisis y especificación de requisitos de seguridad de la información

Dentro de los requisitos para los nuevos sistemas de información se deben incluir en lo definido por seguridad de la información en el instructivo control de seguridad y privacidad de la información con código GTIGPS01-I003.

a) Todas las Dependencias del Distrito deben realizar la identificación y actualización de los activos de información con lo establecido en el instructivo para la identificación y clasificación con código GTIGPS01-I006 y en el formato de inventario y clasificación de activos de información con código GTIGPS01-F007 y deben ser reportadas al correo de seguridad.oai@cartagena.gov.co

b) Todas las Dependencias del Distrito deben identificar las amenazas potenciales de acuerdo con lo establecido en el instructivo para ingreso a los sistemas de información con código GTIGPS01-I004.
c) Todas las Dependencias del Distrito deben identificar y evaluar los riesgos del área, utilizando la matriz de identificación de riesgos OAI con código GTIGPS01-F001, y se debe reportar cada vez que exista una actualización al correo de seguridad.oai@cartagena.gov.co.
d) La Oficina Asesora de Informática ha definido los siguientes controles para los componentes de seguridad, que se deben cumplir por todas las Dependencias del Distrito, así:
    - Controles de acceso: De acuerdo con el procedimiento para la solicitud control de acceso con código GTIPS02-P001, se han implementado controles a los aplicativos y sistemas desarrollados. Todo contratistas, funcionarios y terceros que realicen actividades dentro del Distrito y requieren solicitar acceso a aplicativos deberán diligenciar el formato de control de accesos a recursos digitales con código GTIGPS02-F001 y para acceso de servidores deben usar el formato de solicitud de acceso a terceros servidores con código GTIGPS02-F005.
    - Protección de datos: Todos los sistemas de información y aplicativos deben implementar protocolos y técnicas en cifrado de datos; y cuando exista captura de información de usuarios, se debe solicitar la aceptación de tratamiento de datos personales, y almacenar esta autorización en el repositorio de SharePoint predefinido de acuerdo con la Ley 1581 de 2012. Todas las dependencias del Distrito deben reporta al correo electrónico protecciondedatos@cartagena.gov.co los 5 primeros días del mes la información correspondiente en el formato para el cumplimiento de la ley de protección de datos con código GTIGPS01-F008.
    - Seguridad en procesos: El proceso de seguridad realiza evaluaciones de vulnerabilidades periódicas en los sistemas de información para identificar y corregir controles faltantes, generando un informe que debe ser compartido al área de desarrollo con el fin de implementar mejoras.
    - Concientización en seguridad: la Oficina Asesora de Informática debe definir y actualizar el manual para el plan de capacitación, sensibilización y comunicación de seguridad de la información con código GTIGPS01-M004, con el fin de, promover una cultura de seguridad donde todos los funcionarios y contratistas del Distrito generen conciencia de la importancia de salvaguardar la información.
e) La Oficina Asesora de Informática cuenta con una política de seguridad de la información aprobaba por el comité de gestión y desempeño institucional la cual es de estricto cumplimiento por todos los funcionarios, contratistas y terceros que realizan actividades en el Distrito de Cartagena, Esta debe estar disponible en el link https://mipg.cartagena.gov.co/gestion-valores-resultados/seguridaddigital ; a su vez cuenta con el Instructivo para la definición de roles y responsabilidades del modelo de seguridad y privacidad de la información con código GTIGPS01-I002 donde están establecidas las responsabilidades y autoridades de quienes realizan supervisión y hacen cumplir las políticas.

f) Todas las Dependencias del Distrito que soliciten desarrollo de aplicativos deben diligenciar en compañía del proceso de desarrollo de aplicaciones y el de seguridad el formato levantamiento de requerimiento detallado del software con código GTIGS01-F002, en el cual se debe establecer el nivel de confianza requerido para obtener los requisitos de autenticación de usuario.
g) Todas las Dependencias del Distrito deben cumplir con los controles de seguridad establecidos de acuerdo con el instructivo control de seguridad y privacidad de la información con código GTIGPS01-I003.

Todas las Dependencias que realicen desarrollo de software y/o adquisición, deberán velar por las interfaces de ingreso o seguimiento se registren, auditen y supervisen por parte del proceso de seguridad quien aprobará el cumplimiento del control.

6.10.2 Seguridad de servicios de las aplicaciones en redes publicas

La Oficina Asesora de Informática ha establecido controles para que la información involucrada en los servicios de aplicaciones que pasen sobre redes públicas sea protegida de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizada, dentro de las cuales se encuentran:

a) Implementación del firewalls y seguridad perimetral, para la revisión del tráfico entrante y saliente, con el objetivo de prevenir ataques y eventuales fallos en los servidores que alojan las aplicaciones, mediante monitoreos automáticos.
b) Implementación de VPN para acceso de aplicativos de la entidad desde redes públicas, esto aplica solo para los funcionarios y contratistas autorizados a través del formato de solicitud de acceso a recursos digitales con código GTIGPS02-F001.
c) Todos los aplicativos y sistemas deben contar con mecanismos de multi factor y verificación de acceso mediante el acceso anti-robot, mediante el uso de captchas, esto se debe incluir como requerimientos en el formato levantamiento del requerimiento detallado del software con código GTIGS01-F002.
d) La Oficina Asesora de Control Interno establece y aplica auditorias al proceso de seguridad, que permitan identificar y atender debilidades en los sistemas e infraestructura, generando un informe de auditoría.
e) Implementación del cifrado de datos, como requerimiento en todos los procesos de desarrollo, especificando el tipo a utilizar.
f) Contemplar las políticas de backups y bases de datos definidos en el procedimiento para la elaboración y comprobación de las copias de seguridad de servidores, e informar a la Oficina Asesora de Informática, para que el sistema o aplicativo se incluya en los planes definidos.
g) Definir la responsabilidad civil asociada con cualquier transacción fraudulenta.

6.10.3 Protección de transacciones de los servicios de las aplicaciones

La Oficina Asesora de Informática contiene los lineamientos para la protección de las transacciones de los servicios que se realizan a través de las aplicaciones con el fin de proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada. Para lo cual establece las siguientes políticas:

a) Todos los aplicativos deben usar el protocolo HTTPS, mediante el uso de un certificado SSL bajo el dominio de la Entidad, siempre y cuando sea una aplicación web. Se debe solicitar apoyo a la Oficina Asesora de Informática para la adecuada configuración y ajuste. El área de infraestructura asigna los dominios y realiza la configuración de publicación en DNS de la red interna y externa. El uso de este protocolo garantiza que las comunicaciones entre el navegador web y servidor sea cifrada.
b) La autenticación de los usuarios en todas las aplicaciones, se deben implementar desde el desarrollo del sistema, técnicas y métodos de autenticación mediante usuario y contraseña, y si las transacciones son de alto riesgo incluir autenticación de doble factor.
c) Todos los aplicativos y sistemas de información deben contar con un registro de auditoría, este proceso permite almacenar datos de las transacciones como fechas, usuarios y acciones realizadas. Debe quedar definido como requerimiento en los documentos definidos para el desarrollo o actualización del software.
d) Todos los sistemas de información y demás aplicativos deben estar bajo infraestructura de la Entidad, lo cual permite llevar un control detallado. Y se deben realizar monitoreos en tiempo real permiten detectar patrones anómalos o intentos de fraudes o ataques.
e) La información almacenada en las bases de datos se debe encriptar teniendo en cuenta los métodos TDE (Transparent Data Encryption), encriptando todo el contenido, garantizando eficiencia e integridad de la información.

6.10.4 Política de desarrollo seguro y principios de construcción de sistemas seguros

Todas las Dependencias del Distrito deben cumplir con la política de desarrollo seguro y de integrar la seguridad en todas las etapas del ciclo de vida del desarrollo de software. Definido en el procedimiento desarrollo de software con código GTIGS01-P001. El equipo de seguridad supervisa el cumplimiento de esta política y brinda orientación y apoyo en cuestiones de seguridad, teniendo en cuenta los siguientes lineamientos:

a) Evaluación de Riesgos: Antes de iniciar cualquier proyecto de desarrollo, se debe realizar una evaluación de riesgos de seguridad para identificar posibles amenazas y vulnerabilidades. El cual esta soportado en el procedimiento Plan de aseguramiento de la calidad proceso desarrollo de software con código GTIGS01-F003.
b) Capacitación y Concienciación: Todos los miembros del equipo de desarrollo deben recibir capacitación en seguridad de aplicaciones y estar al tanto de las mejores prácticas de seguridad. El cual esta soportado en el manual para la capacitación, sensibilización y comunicación de seguridad de la información con código GTIGPS01-M004.
c) Estándares de codificación segura: Se deben seguir estándares de codificación segura establecidos, que incluyen la validación adecuada de datos de entrada, la prevención de inyecciones SQL y autorización adecuadas.
    - Inyecciones de SQL
    - Autenticación y sesiones
    - Exposición de datos sensibles
    - Controles de acceso
    - Componentes y bibliotecas seguras.
    - Redirección y reenvíos de información.

d) Pruebas de Seguridad: Antes del lanzamiento, todas las aplicaciones deben someterse a pruebas de seguridad, incluyendo análisis de vulnerabilidades.
e) Gestión de Dependencias: El área de seguridad realiza seguimiento de todas las bibliotecas y Dependencias utilizadas y se asegura de que estén actualizadas y no contengan vulnerabilidades conocidas, mediante el uso de herramientas web como: Zap y Nessus
f) Control de Acceso: La Oficina Asesora de Informática cuenta con el Instructivo para ingreso a los sistemas de información con código GTIGPS01-I004 para restringir el ingreso a los sistemas y datos sensibles solo a personas autorizadas. Esto debe identificarse en el levantamiento de requerimientos y debe quedar especificado el mecanismo a utilizar con el formato levantamiento de requerimiento detallado del software con código GTIGS01-F002.
g) Revisiones de Código: Todas las actualizaciones de código deben revisarse con dos componentes uno de seguridad y otro de desarrollo, para identificar y corregir problemas antes de su implementación.
h) Seguridad en el Ciclo de Vida del Desarrollo: La seguridad debe ser parte integral de todas las etapas del ciclo de vida del desarrollo de software, desde la definición de los requerimientos hasta el mantenimiento continuo.
i) Cumplimiento normativa protección de datos: Incluir en todos los desarrollos y actualizaciones el cumplimiento de la normativa de protección de datos personales y todo lo que estas requieren para garantizar transparencia. Consultar en Lineamientos de protección de datos personales
j) Cumplimiento y Auditoría: Se llevarán a cabo auditorías regulares para evaluar el cumplimiento de esta política y la seguridad de las aplicaciones y sistemas.
k) Mejora continua en todos los procesos: este enfoque es fundamental para lograr una óptima seguridad, ajustando y actualizando constantemente las medidas en respuesta de las amenazas.
l) Ningún desarrollo nuevo o actualización sale a producción sin haber pasado por las pruebas exhaustivas en un ambiente de pruebas las cuales deben estar documentadas y sin el visto bueno del área de seguridad y privacidad de la información.
m) La aplicación que se encuentre en desarrollo debe apuntar al nombre y no a la dirección IP.
n) Todos los ingenieros que se encarguen de realizar desarrollos deben seguir los lineamientos del líder del área de desarrollo.
o) Todo proyecto que implique desarrollo debe ser llevado al comité de proyectos de la Oficina Asesora de Informática bajo el procedimiento de desarrollo. Cada solicitud debe ser evaluada desde la pertinencia, accesibilidad, alcance, disponibilidad de recursos informáticos, tratamiento de la seguridad y privacidad; así como también la priorización y se asigne el responsable de ser aprobada; por lo tanto, ningún desarrollo puede ser realizado de manera autónoma desde una Dependencia u oficina.

6.10.5 Procedimientos de control de cambios en sistemas y restricciones en los cambios a los paquetes de software y ambiente de desarrollo seguro

Los procedimientos de control de cambios en sistemas se refieren a un conjunto de prácticas y políticas diseñadas para gestionar y supervisar de manera efectiva cualquier cambio planificado o no planificado en un sistema de información de la Entidad. Estos procedimientos se implementan para garantizar la integridad, disponibilidad y seguridad de los sistemas de información.

Los cambios a los sistemas de información deberán realizarse bajo los lineamientos establecidos en el instructivo para ambientes independientes en el ciclo de vida de los sistemas de información con código GTIGS01-I002, los cuales deberán controlarse mediante el uso del formato de control de cambios con código GTIGS01-F007. Todas las Dependencias del Distrito que requieran realizar cambios o modificaciones deberán seguir los siguientes lineamientos:

a) Solicitudes de cambios o actualizaciones: En las Dependencias del Distrito que requieran o identifiquen cambios sobre un software, deben solicitar apoyo a la Oficina Asesora de Informática, y se debe aplicar lo dispuesto en instructivo para ambientes independientes en el ciclo de vida de los sistemas de información con código GTIGS01-I002. Se inicia con la nueva identificación de requerimientos y afinación de estos, mediante sesiones (reuniones) entre los interesados, y se da continuidad el proceso de desarrollo.
b) Evaluación preliminar: El equipo de desarrollo de la Oficina Asesora de informática debe realizar una revisión de lo identificado y definir si hay viabilidad técnica y de recursos para proceder con el desarrollo. Este concepto debe emitirse de manera formal y ser remitido mediante un oficio a la Dependencia o personal solicitante.
c) Aprobación de cambios: Las solicitudes de cambios o actualizaciones se deben presentar a un comité de proyectos compuesto por los gestores de la Oficina Asesora de informática y demás expertos en temas TIC. Este comité debe definir si aprueba o rechaza, emitiendo un concepto final, el cual debe ser remitido mediante un oficio a la Dependencia o personas solicitantes.
d) Planificación de cambios: Después de que se realiza la aprobación, se inicia la fase de planificación que abarca el proceso de desarrollo, generando la documentación necesaria como cronograma de actividades, entre otros. Especificados en procedimiento de desarrollo de software con código GTIGS01-P001.
e) Desarrollo y pruebas: El proceso se debe llevar a cabo teniendo en cuenta lo dispuesto por el ciclo de vida del desarrollo de software y la metodología definida. Luego, se debe estructurar un plan de pruebas y ejecutarlas: Se contemplan pruebas unitarias, pruebas funcionales y de seguridad.
f) Documentación del proceso: Todo el proceso debe estar acompañado del levantamiento y actualización documental, los desarrolladores deben realizar el procedimiento definido para actualización.
g) Implementación y cierre: Se debe realizar el proceso de implementación en un ambiente de producción, en momentos de inactividad y con monitoreo de las áreas involucradas. Finalmente se confirma a la Dependencia o solicitante del cierre de la solicitud, utilizando el formato despliegue de software con código GTIGS01- F011.
h) Identificar las políticas y procedimientos de seguridad aplicables en el desarrollo: Es importante conocer los procedimientos definidos en el área de desarrollo, es decir el proceso de vida del software y la metodología. La Entidad cuenta con la política de

seguridad y debe ser consultada en el micrositio Política de seguridad digital y lo dispuesto por la política de seguridad del MINTIC.

i) Los procesos de desarrollo y adquisición deben cumplir con las mejores prácticas de seguridad, como la validación de entradas y la protección contra ataques comunes como inyecciones de SQL Y XSS (Cross-site scripting).

6.10.6 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.

a) Se debe identificar los cambios aplicados en la plataforma, mediante una revisión detallada, generando una lista de chequeo que incluya los siguientes ítems:
   - Estado de actualizaciones en el sistema operativo
   - Estado del servidor (se realizó migración o actualización).
   - Cambios de infraestructura de red.
   - Confirmar si el sistema fue actualizado teniendo en cuentas las librerías y Dependencias.

b) Se debe seleccionar las aplicaciones o sistemas de información a revisar, siempre identificar las aplicaciones críticas que pueden verse afectadas por los cambios aplicados a las plataformas, este proceso de revisión está directamente relacionado con el servidor. Como base de este proceso se tienen el documento de catálogos de sistemas de información y el formato para la identificación y clasificación de los activos de información con código GTIGPS01-F007.

c) En caso esenciales y que proyecte una afectación de sistemas de información es importante solicitar un entorno de pruebas, donde se pueda validar si hay compatibilidad y una adecuada respuesta sobre las actualizaciones de librerías. El proceso de solicitud de este ambiente se hace a través del formato de solicitud de acceso a recursos digitales con código GTIGPS02-F001.

d) Realizar pruebas funcionales y de seguridad en las aplicaciones que se identifiquen como potenciales afectados por la actualización de la plataforma.

e) La notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación, el cual se debe realizar mediante publicaciones en la sede y correos electrónicos.

6.10.7 Desarrollo contratado externamente

La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente, y se debe revisar las siguientes directrices:

a) Definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente.

b) Establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas, con lo establecido en el procedimiento de desarrollo de la Oficina Asesora de Informática con código GTIGS01-P001

c) Elaborar y entregar toda la documentación del desarrollo, de acuerdo con los formatos establecidos por el área de desarrollo de la Oficina Asesora de Informática, tales como:
   - Levantamiento de requerimiento detallado del software con código GTIGS01-F002
   - Formato diseño de la arquitectura de solución con código GTIGS01-F003
   - Pruebas unitarias con código GTIS01- F009.
   - Cumplimiento usabilidad de la web con código GTIGS01-F005.
   - Formato cumplimiento accesibilidad de la web con código GTIGS01-F008.
   - Formato control de cambios de software con código GTIGS01-F007.
   - Proceso de actualización del software (Sharepoint)
   - Documentación del código fuente (Repositorio AzureDevOps),
   - Diseños web
   - Catálogo de sistemas de información (MAE).
   - Formato despliegue con código GTIGS01- F011.
   - Cronograma de actividades con código GTIS01- F010.

d) Realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables, desde el área de seguridad de la Oficina Asesora de Informática, se debe hacer seguimiento al plan de pruebas que deberá ser completado por la Entidad que realice el desarrollo.
e) Dependiendo de lo definido por la empresa y su título de propiedad sobre el código fuente, si este pasa a propiedad de la Entidad debe aplicar lo definido en el instructivo de gestión de código fuente.
f) Desde la Oficina Asesora de Informática, se pueden generar procesos de auditoria frente al proceso de desarrollo.
g) Cumplir lo definido en la política de gobierno digital, resoluciones 1519 y 2893 de 2020 y demás que designe el supervisor del contrato.

6.10.8 Pruebas de seguridad de sistemas

Para las pruebas de seguridad de sistemas, se deben tener en cuenta las siguientes consideraciones:

a) Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.
b) Se debe verificar en una muestra la producción de los desarrollos y se deben realizar pruebas de seguridad. También verificar que los procesos de detección de incidentes sean probados periódicamente.
c) Se debe remitir una solicitud al área de seguridad de la Oficina Asesora de Informática, donde se relacione el requerimiento de realización de pruebas de seguridad, y el equipo define el mecanismo y herramientas a utilizar. (Esto depende del tipo de aplicativo y lenguajes usados en el desarrollo).

6.10.9 Prueba de aceptación de sistemas

Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados. Para realizar adecuadamente esta tarea se deberán seguir los siguientes lineamientos:

a) Preparación: Se deben definir quienes son los usuarios finales del sistema o aplicativo. Esta información se puede tomar del levantamiento de actores potenciales, de este listado se definen quienes participaran en las pruebas.
b) Organizar los casos de pruebas basados en los requerimientos identificados del sistema y en los flujos de trabajo del usuario. Esta información será custodiada por el área de desarrollo y seguridad de la Oficina Asesora de Informática.
c) Preparar y organizar el entorno de pruebas: Teniendo en cuenta el instructivo de separación de ambientes con código GTIGS01-I002, se debe instalar el sistema bajo el ambiente de pruebas y permitir el acceso de usuarios a este, proporcionando medios y credenciales de autenticación.
d) Se debe proveer a los usuarios un formato para plasmar las respuestas del sistema y las distintas interacciones y resultados, esto permite identificar errores.
e) Al identificar problemas o errores se debe establecer un plan de atención inmediata, generando una nueva planificación en el cronograma de actividades e iniciar una nueva iteración en el ciclo de desarrollo del software. Esto implica asignar desarrolladores para la atención de los inconvenientes detectados. Este proceso de ajustes debe quedar registrado en la documentación del software.
f) Después de resolver cada fallo identificado, se debe realizar un proceso de validación final con los usuarios, ellos deben proporcionar su aceptación. Este proceso debe quedar registrado en el acta de entrega.
g) Toda la documentación del proceso debe remitirse a la Oficina Asesora de Informática, a los lideres de área de desarrollo y seguridad.

6.10.10 Protección de datos de prueba

Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente. Para ello se debe tener en cuenta las siguientes consideraciones:

a) Amonificación de datos: Al realizar pruebas sobre aplicativos, utiliza datos de clientes o usuarios ficticios o que se genere de manera automática. No se debe comprometer datos personales.
b) En el enmascaramiento de los datos, se debe priorizar para datos sensibles, correos electrónicos, contraseñas de acceso y datos de transacciones.
c) Al realizar pruebas con datos de usuarios solo se deben permitir el acceso a desarrolladores que requieran y no a todo el equipo.
d) La información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas.
e) Establecer que el copiado y uso de la información operacional se debe registrar en Log para suministrar un rastro de auditoría.

6.11 DOMINIO 15: RELACIÓN CON LOS PROVEEDORES

Fuente

6.11.1 Seguridad de la información en las relaciones con los proveedores

a) La Oficina Asesora de Informática debe establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en la gestión de cambios.
b) La Oficina Asesora de informática debe verificar mensualmente el cumplimiento de Acuerdos de Nivel de Servicio establecidos con sus proveedores de tecnología.
c) El área de seguridad debe establecer lineamientos para el cumplimiento de las obligaciones contractuales de la dimensión de Seguridad y Privacidad de la Información con terceros o proveedores, cumpliendo las políticas de seguridad establecidas por la Oficina Asesora de Informática.
d) La Oficina Asesora de informática debe establecer en el momento de suscribirse contratos de cualquier tipo los riesgos asociados a la seguridad y privacidad de la información, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información del Distrito.

6.12 DOMINIO 16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Fuente

Conforme a lo establecido en la Circular Única, todo incidente relacionado con la seguridad de datos personales debe ser notificado a la Superintendencia de Industria y Comercio. Cuando se produce un incidente de seguridad que involucra información personal, el proceso encargado de la seguridad y privacidad de los datos debe llevar a cabo esta notificación en un plazo máximo de 15 días a partir del momento en que se tenga conocimiento del incidente. Este procedimiento se ajusta a la normativa vigente en cuanto a la protección de datos personales.

La Oficina Asesora de Informática deberá documentar todos los incidentes de seguridad de la información de acuerdo con el procedimiento de gestión de incidentes de seguridad de la información con código GTIGPS02-P005. Aquellos relacionados con la infraestructura tecnológica y servicios administrados por esta área deben ser reportados en el formato reporte de incidentes de seguridad.

El procedimiento de incidentes de seguridad debe describir los lineamientos mediante los cuales se les indica a los funcionarios, contratistas o terceros, como minimizar, controlar, reportar y responder de manera oportuna y apropiada ante un impacto de un incidente de seguridad en la Alcaldía Distrital de Cartagena de Indias, incluyendo:

a) Las personas que deben ser notificadas cuando ocurra un incidente de seguridad teniendo en cuenta el nivel de impacto, son las siguientes:
    - El equipo de respuesta a incidentes de seguridad de la información, quienes seguirán lo descrito del procedimiento de gestión de incidentes de seguridad de la información con código GTIGPS02-P005.
    - Líder del equipo de seguridad: seguridad.oai@cartagena.gov.co
    - Jefe de la oficina asesora de informática: informatica@cartagena.gov.co
    - Equipo de atención de incidentes del Ministerio de defensa: colcer.gov.co
b) Se reportan los Incidentes cibernético, por el área de seguridad del Distrito, y se envía un mensaje de correo electrónico informando el incidente al buzón csirtgob@mintic.gov.co, adjuntando el formato de reporte de incidentes de seguridad debidamente diligenciado.
c) Posterior a que un incidente se haya analizado y priorizado se debe notificar al personal encargado de la gestión y atención de incidentes y a las Entidades que determine el líder de la Oficina Asesora de Informática.

6.12.1 Responsabilidad y procedimientos

La Oficina Asesora de Informática debe establecer las responsabilidades para cada rol del equipo de respuesta a incidentes de seguridad de la información y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

e) Los procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento de gestión de incidentes de seguridad de la información con código GTIGPS02-P005.

f) Los procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas.
g) Formatos de reporte de eventos de seguridad de la información para apoyar la acción de reporte y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento de seguridad de la información;
h) El área de seguridad debe reportar los eventos de seguridad de la información a la mesa de ayuda mediante la herramienta SAUS.
i) El área de seguridad debe retroalimentar a las personas que reportan eventos de seguridad de la información, notificando los resultados después que haya sido gestionado y solucionado.

6.12.2 Reporte de eventos de seguridad de la información

Los eventos de seguridad de la información se deben informar a través de los canales de gestión definidos por la Oficina Asesora de Informática, tan pronto como sea posible.

a) Todos los funcionarios, contratistas y/o terceros deben reportar todo evento y/o incidente de seguridad de la información, a través de los siguientes canales:
   - Correo institucional de la mesa de servicios soportegti@cartagena.gov.co
   - Línea de Atención telefónica: 3023798584.
   - Todos los incidentes y/o eventos deben quedar registrados en la herramienta de SAUS.
   - Todos los casos de seguridad o incidentes de seguridad, los cuales deban ser gestionados por la mesa de servicios, o por el área de Desarrollo o Infraestructura, que han sido registrados por el área de seguridad Oficina Asesora de Informática, solo podrán ser cerrados o establecer como solucionados con el visto bueno del emisor o dueño del registro del incidente.
b) El registro, trazabilidad, solución del incidente y/o evento de seguridad de información y lecciones aprendidas deberán ser gestionadas de acuerdo con el procedimiento de gestión de incidentes de seguridad de la información con código GTIGPS02-P005.

6.12.3 Reporte de debilidades de seguridad de la información

Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la Entidad, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios al correo electrónico seguridad.oai@cartagena.gov.co y soporteseguridad@cartagena.gov.co

Todos los eventos deben ser reportados de forma clara y con evidencias que soporten la vulnerabilidad para iniciar la gestión y solución del mismo.

6.12.4 Respuesta a incidentes de seguridad de la información

Para dar respuesta a un incidente de seguridad se debe seguir los lineamientos descritos en el procedimiento de gestión de incidentes de seguridad de la información con código GTIGPS02-P005.

Todos los casos de seguridad o incidentes de seguridad, los cuales deban ser gestionados por la mesa de servicios, o por el área de Desarrollo o Infraestructura, que han sido registrados por el área de seguridad Oficina Asesora de Informática, solo podrán ser cerrados o establecer como solucionados con el visto bueno del emisor o dueño del registro del incidente.

6.12.5 Aprendizaje obtenido de los incidentes de seguridad de la información

La Oficina Asesora de Informática debe registrar las lecciones aprendidas y el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información que se presenten, para reducir la posibilidad o el impacto de incidentes futuros.

6.13 DOMINIO 17: ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

Fuente

6.13.1 Planificación de la continuidad de la seguridad de la información

a) La Oficina Asesora de informática debe continuar con la negociación con un tercero para realizar el proceso de continuidad del negocio con el siguiente alcance en el proyecto:
   - Análisis de riesgos
   - Análisis de impacto al negocio (BIA) para 10 macroprocesos.
   - Estrategia de continuidad.
   - Plan de continuidad del negocio (BCP)
   - Plan de recuperación de desastre (DRP) (Para 15 aplicaciones más críticas)
   - Pruebas y ejercicios.

b) El área de seguridad y privacidad de la información y el área de infraestructura deben identificar los impactos potenciales que amenazan la continuidad de las actividades de

las Dependencias, y se realiza un análisis con la capacidad de una respuesta efectiva, y generar estrategias para definir el plan de recuperación de desastres.

6.13.2 Implementación de la continuidad de la seguridad de la información

El Distrito de Cartagena debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa, teniendo en cuenta los siguientes lineamientos:

a) La Oficina Asesora de informática debe definir una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias.
b) La Oficina Asesora de Informática debe contar con personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información, de acuerdo con lo descrito en el procedimiento de gestión de incidentes de seguridad de la información con código GTIGPS02-P005.
c) La Oficina Asesora de informática debe tener aprobado los procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información.

6.14 DOMINIO 18: CUMPLIMIENTO

Fuente

6.14.1 Identificación de la legislación aplicable y de los requisitos contractuales

Se debe identificar la relación de requisitos legales, reglamentarios, estatutarios, que le aplican a la Entidad, contenidos de acuerdo con el documento Marco Normativo con código GADCA01-F003.

6.14.2 Derechos de propiedad intelectual

Estas directrices aplican a todos los colaboradores, empleados, contratistas y terceros que tengan acceso o interactúen con los activos de información de la Alcaldía Distrital de Cartagena de Indias.

- **Derechos de Propiedad Intelectual:**

  a) Derechos de Autor: Todos los activos de información, incluyendo, pero no limitándose a software, aplicaciones, documentos, imágenes, videos y otros contenidos relacionados de la Alcaldía Distrital de Cartagena de Indias, están protegidos por derechos de autor. Los derechos de autor de estos activos pertenecen a la misma a menos que se especifique lo contrario.
  b) Licencia de Uso: Los colaboradores y terceros que tengan acceso a los activos de información de la Alcaldía Distrital de Cartagena de Indias solo pueden utilizarlos de acuerdo con las licencias y acuerdos específicos que rigen dichos activos. Cualquier uso no autorizado está prohibido y sujeto a medidas disciplinarias y legales.
  c) Marcas Registradas y Derechos de Marca: Las marcas comerciales y logotipos relacionados con la Alcaldía Distrital de Cartagena de Indias son propiedad exclusiva de la empresa. Cualquier uso no autorizado de estas marcas está prohibido y será procesado legalmente.
  d) Derechos de Terceros: Cuando se utilicen activos de información de terceros en el contexto de la seguridad digital de la Alcaldía Distrital de Cartagena de Indias, se deben respetar y cumplir los derechos de propiedad intelectual de dichos terceros. Esto incluye el cumplimiento de las licencias de software de código abierto y cualquier otro acuerdo de licencia, las cuales se deben definir en el proceso de levantamiento de requerimientos y formalización de contratos.

- **Responsabilidades:**

  a) Equipo de Seguridad Digital: El equipo de seguridad digital de la Alcaldía Distrital de Cartagena de Indias, liderado por la Oficina Asesora de Informática es responsable de supervisar y hacer cumplir las políticas de propiedad intelectual en el entorno de seguridad digital. Deben garantizar que se respeten los derechos de propiedad intelectual de la entidad y de terceros.
  b) Colaboradores, funcionarios y contratitas: Deben cumplir con las políticas de propiedad intelectual al utilizar los activos de información. Esto incluye el respeto de los derechos de autor, licencias y marcas registradas.

6.14.3 Protección de registros

El Distrito debe utilizar el formato tablas de retención documental con código GDOPD02-F003 en el cual se especifican los registros de retención, además el almacenamiento, el manejo y destrucción. Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales. Los posibles tipos de registros pueden ser registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos etc.

6.14.4 Protección de los datos y privacidad de la información relacionada con los datos personales.

Los servicios tecnológicos previstos y gestionados por la Oficina Asesora de Informática deben cumplir con la protección y privacidad de la información personal tal como se requiere en el Decreto 0619 del 26 de mayo del 2020 que pueden ser consultado en el micrositio de Seguridad Digital y basado en la ley estatutaria 1581 de 2012 y Decreto 1377 que reglamenta la ley de 2013.

La Alcaldía Distrital de Cartagena debe seguir los lineamientos establecido por la Oficina Asesora de Informática de acuerdo con el instructivo para el tratamiento de los datos personales con código GTIGPS01-I008. Las políticas definidas por el Distrito deben estar publicadas en el micrositio Política de seguridad digital de la Alcaldía, en la cual se define lo derechos de los titulares de los datos.

Todos los procesos del Distrito de Cartagena que requieran utilizar instrumentos para el levantamiento de información de terceros deben tener en cuenta los siguientes lineamientos:

a) Toda información se deberá solicitar desde correos institucionales y no personales.
b) Los formularios y/o encuestas deberán ser diseñados por la herramienta de Microsoft 365 o aplicativos autorizados para este fin (Lista de asistencias a capacitaciones, reuniones u otro tipo de formulario).
c) Se deberá solicitar la autorización para el tratamiento de los datos personales.
d) No se deberá utilizar nubes asociadas a correos personales para compartir y/o almacenar información propia de los procesos del Distrito de Cartagena.
e) Todas las Dependencias del Distrito deberán reportar a la Oficina Asesora de Informática todos los aplicativos y formularios a través de los cuales solicitaron información a terceros y se debe diligenciar en el formato para el cumplimiento de la ley de protección de datos con código GTIGPS01-F008 y de ser requerido el formato de autorización para el tratamiento y protección de datos personales Código GTIGPS02-F003
f) Todas las Dependencias de Distrito deberán contar con la aprobación del área de la Oficina Asesora de Informática del proceso de seguridad y privacidad de la información previo a la utilización de los formatos definidos para la recolección de datos personales la cual será solicitada al correo protecciondedatos@cartagena.gov.co
g) Este reporte debe realizarse y ser enviado los 5 primeros días del mes al correo protecciondedatos@cartagena.gov.co incluyendo la descripción de la ruta o destino de las bases de datos recopiladas. Las cuáles serán reportadas ante la Superintendencia de industria y comercios.

Todos los servidores públicos, terceros, funcionario y/o contratistas deberán cumplir con esta política y firmar de ser requerido los acuerdos de confidencialidad.

6.14.5 Cumplimiento con las políticas y normas de seguridad digital

Es responsabilidad de los secretarios, directores, asesores, supervisores, interventores, jefes de oficina, gerentes y alcaldes locales, realizar el seguimiento a los controles establecidos en

la presente política con el fin de garantizar que funcionarios, contratistas y/o terceros que realicen actividades al interior de la Alcaldía Distrital de Cartagena cumplan los lineamientos establecidos.

El incumplimiento a las medidas de seguridad digital podrá acarrear responsabilidad disciplinaria, de acuerdo con lo establecido en la ley 1952 del 2019 (código general disciplinario), modificada por la ley 2094 del 2021, en el artículo 38 numerales 5, 6, 22, 23, 26 y 29. Son deberes de los servidores públicos los siguientes:

5. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.

6. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

22. Vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a que han sido destinados.

23. Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.

29. Controlar el cumplimiento de las finalidades, objetivos, políticas y programas que deban ser observados por los particulares cuando se les atribuyan funciones públicas.

6.14.6 Revisión del cumplimiento técnico

Los sistemas de información deben cumplir con los estándares técnicos definidos para los desarrollos de software y la implementación de infraestructura, con el formato cumplimiento usabilidad de la Web con código GTIGS01-F005, y el formato cumplimiento accesibilidad de la Web con código GTIGS01-F008.

6.14.7 Política de cumplimiento ley de transparencia

De acuerdo con la Ley 1712 de 2014, se regula los derechos de acceso a la información pública, dicha información debe ser publicada en la sede electrónica del Distrito de Cartagena de Indias, en el sitio de transparencia, y la Ley 1755 del 2015, que regula los derechos fundamentales de petición y se sustituye un título del código de procedimiento administrativo y de lo contencioso administrativo, se deberá tener en cuenta las siguientes directrices:

a) Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con el Art. 2 de la Ley 1712 de 2014.

b) Toda información en poder de los sujetos obligados se presume pública y conforme al principio de transparencia, se debe proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca el Artículo 3 de la Ley 1712 de 2014. El acceso a la misma debe cumplir con los criterios de razonabilidad y proporcionalidad, así como aplicar los principios de buena fe, con motivación honesta, leal y desprovista de cualquier intención dolosa o culposa y el principio de responsabilidad en el uso de la información.
c) De acuerdo con el Articulo 24 de la Ley 1755 del 2015 son documentos de carácter reservado los siguientes:
    - Los que involucren derechos a la privacidad e intimidad de las personas, incluidas en las hojas de vida, la historia laboral y los expedientes pensionales y demás registros de personal que obren en los archivos de las instituciones públicas o privadas, así como la historia clínica.
    - Los amparados por el secreto profesional.
    - Los datos genéticos humanos.
d) El acceso a la información podrá ser rechazada o denegada, si se considera que la divulgación puede afectar alguno de los siguientes derechos, definidos en el artículo 18 de la ley 1712 de 2014:
    - El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado por el artículo 24 de la Ley 1437 de 2011.
    - El derecho de toda persona a la vida, la salud o la seguridad.
    - Los secretos comerciales, industriales y profesionales.
e) A la hora de solicitar o suministrar información, que involucren derechos a la privacidad e intimidad u otro tipo de reserva, que recae sobre algún servidor público o proceso relacionado, se tenga en cuenta los criterios anteriormente enunciados, y lo dispuesto en el Decreto No. 1081 de 2015 y demás disposiciones legales vigentes.

La Alcaldía Distrital de Cartagena de Indias debe garantizar el derecho de acceso a la información pública por medio de los canales establecidos por la Alcaldía, excluyendo las excepciones constitucionales, legales, sensibles; para el cumplimiento con la Ley de transparencia vigente es menester generar los instrumentos, procedimientos y demás documentación requerida para la gestión y trámite de su publicación.

La responsabilidad de actualizar periódicamente la información pública se encuentra bajo la responsabilidad de los jefes de Dependencias y Oficinas del Distrito.

6.14.8 Sanciones y seguimiento de las medidas de seguridad

El incumplimiento de los deberes podría ser tenida, dentro de la responsabilidad disciplinaria del servidor público, como faltas gravísimas, las cuales se describen en los numerales 1 y 5 del artículo 62 del Código General Disciplinario, en el cual reza:

Artículo 62, Faltas relacionadas con la moralidad publica

1. Dar lugar a que por culpa gravísima se extravíen pierdan o dañen bienes del Estado o a cargo del mismo, o de empresas o instituciones en que este tenga parte o bienes de particulares cuya administración o custodia se le haya confiado por razón de sus funciones, en cuantía igual o superior a quinientos (500) salarios mínimos legales mensuales.

5. Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas.

De acuerdo con lo expuesto, su incumplimiento puede acarrear investigaciones y sanciones disciplinarias en los términos de la ley 1952 del 2019 y sus modificaciones.

Es deber de los jefes inmediatos reportar los incidentes de seguridad digital, los daños físicos, perdidas de los activos de información y a toda la infraestructura TI, ante la oficina Asesora de informática, quien a su vez realizará el respectivo reporte ante la Oficina Asesora de Control Disciplinario de la Alcaldía Distrital de Cartagena, en cumplimiento a la ley 1952 del 2019 (código general disciplinario), modificada por la ley 2094 del 2021, en el artículo 38 numerales 25 y 26

25. Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.

26. Poner en conocimiento del superior los hechos que puedan perjudicar el funcionamiento de la administración y proponer las iniciativas que estime útiles para el mejoramiento del servicio.

7. BIBLIOGRAFÍA

Departamento nacional de planeación. (2016). *Guia para la administración de riesgo de seguridad de la información.* Obtenido de https://colaboracion.dnp.gov.co/CDT/DNP/SE-G02%20Gu%C3%ADa%20metodol%C3%B3gica%20para%20la%20admon%20de%20riesgos%20del%20SGSI.Pu.pdf?

Federación colombiana de municipios. (2018). *Dirección de tecnologias de información y las comunicaciones.* Obtenido de https://www.fcm.org.co/wp-content/uploads/2021/07/PoliticaGeneral-ManualSeguridadPrivacidadInformacion2019.pdf

ICONTEC Internacional. (16 de 11 de 2007). *NORMA TECNICA COLOMBIANA NTC-ISO/IEC 27002*. Obtenido de Tecnologia de la Información. Tecnicas de seguridad. Codigo de practicas para la gestion de seguridad de la informacion.

ICONTEC Internacional. (2013). *NORMA TECNICA COLOMBIANA NTC-ISO IEC 27001.* Obtenido de Tecnología de la información.Técnica de seguridad, sistema de gestión de la seguridad de la información.

ICONTEC Internacional. (2018). *NORMA TECNICA COLOMBIANA NTC ISO 27000.* Obtenido de Tecnología de la información- Seguridad tecnica- seguridad de la informacion sistemas de gestion -vision general y vocabulario: https://akela.mendelu.cz/~lidak/IPI/ISO_IEC_27000_2018.pdf

MINTIC. (11 de 05 de 2016). *Elaboración de la politica general de seguridad y privacidad de la información.* Obtenido de Guia 2: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINTIC. (06 de 05 de 2016). *Guía de auditoria.* Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-5482_G15_Auditoria.pdf

MINTIC. (01 de 04 de 2016). *Guía de gestión de riesgo.* Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-5482_G7_Gestion_Riesgos.pdf

MINTIC. (15 de 03 de 2016). *Guía para la gestión y clasificación de activos de información.* Obtenido de https://mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MINTIC. (29 de 07 de 2016). *Modelo de seguridad y privacidad de la información.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINTIC. (25 de 04 de 2016). *Roles y responsabilidades.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

MinTIC, M. d. (11/05/2016). *Guía 2 - Política General MSPI v1.* Bogota. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

NORMA INTERNACIONAL. (15 de 06 de 2005). *Tecnología dela información - tecnicas de seguridad-Código para la practica de la gestión de la seguridad de la informacion.* Obtenido de https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

NORMA INTERNACIONAL. (15 de 09 de 2015). *ISO 9001.* Obtenido de Sistema de gestión de la calidad - Requisito.

NORMA INTERNACIONAL. (2018). *Directrices para la auditoria de los sistemas de gestión.*

NORMA INTERNACIONAL. (s.f.). *Sistema de gestión de la calidad - fundamentos y vocabularios.* Obtenido de https://itp.itpachuca.edu.mx/SGC/documentos%20de%20referencia/ISO%209000-2015.pdf

8. 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 04 del 01 del mes septiembre del 2023 del comité Institucional de Gestión y Desempeño.