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.

Contenido

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 la estrategia 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 del mismo, 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.

2. MARCO CONCEPTUAL

Aceptación del Riesgo: Decisión de aceptar un riesgo.

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

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

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

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

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

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

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

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

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

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

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

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas

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

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

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

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

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

COPSIS: Sistema de Contratación de OPS

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

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

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

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

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

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

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance de la POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IPS: Sistema de prevención de intrusos.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MSPI: Modelo de seguridad y privacidad de la información

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

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

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

OAI: Oficina Asesora de Informática

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

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

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

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

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

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

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

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

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

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

Salvaguarda: Véase: Control.

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

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

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

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

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

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

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

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

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

3. POLITICAS ESPECÍFICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se prosigue con la descripción de las políticas de seguridad de la información para el cumplimiento del Modelo de Seguridad y privacidad de la Alcaldía Distrital de Cartagena. Este conjunto de recomendaciones no es exhaustivo. A continuación, se agrupan las políticas con el objetivo de hacer una implementación transversal de Seguridad y privacidad de la Información en la Alcaldía Distrital de Cartagena de Indias

3.1. POLIICA PARA LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Esta política tiene como finalidad establecer el comité directivo de la seguridad de la información. Debe tener los siguientes elementos:

- ¿Quiénes conforman el comité directivo de seguridad de la información?
- **Objetivos**: Se deben especificar los objetivos del comité como por ejemplo el mejoramiento continuo de los programas o las distintas actividades que se realizarán

en dichos comités, verificación de avance de los distintos proyectos, la revisión del documento de la política de seguridad etc.

Cumplimiento: Debe establecerse que dicho comité verifique el cumplimiento de las políticas.

3.2. POLITICA PARA LA GESTION DE ACTIVOS

Esta política describe las directrices mediante las cuales se indica a los directivos, 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:

3.2.1. Identificación de Activos: Para llevar a cabo una correcta identificación de los activos de información se debe:

- La Alcaldía de Cartagena establece 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 el personal que tiene 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 General, quien sigue las especificaciones dadas desde el Archivo General de la Nación y será almacenada bajo las mismas directrices establecidas de acuerdo a la norma vigente y siguiendo la estructura de las tablas de retención documental TRD y Tablas de Valoración Documental -TVD definidas.
- La información digital, debe seguir el mismo lineamiento y su almacenamiento y valoración documental será acorde a lo establecido físicamente y bajo la estructura de las tablas de retención documental TRD y Tablas de Valoración Documental -TVD definidas y lideradas acorde a la Gestión documental establecida por la Dirección de Archivo General.
- 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 será 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 de 2013 de la Alcaldía son:

  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.

3.2.2. Clasificación de Activos de 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 que 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 item en particular.

- 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"*
- 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."*
- 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.

- 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*"

3.2.3. Etiquetado de la Información: El mecanismo, responsable y obligatoriedad 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 a la norma vigente y siguiendo la estructura de las tablas de retención documental TRD y Tablas de Valoración Documental -TVD definidas.

3.2.4. Disposición de los activos de la información: Todos los activos que se encuentran bajo la responsabilidad de los funcionarios, contratistas o terceros es de obligatoriedad cumplir con el procedimiento mediante el cual se realiza de forma segura y correcta la creación, asignación, eliminación, retiro, y disposición final de los mismos.

3.2.5. Creación de Activos: La asignación dependiendo de la clase de los activos se realiza, como se establece continuación:

- **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, grabaciones de audios y/o videos deben ser codificados de acuerdo a los parámetros establecidos por la Secretaría General y etiquetados como lo dispone la Dependencia del Archivo General
- **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 Informática traslado o re uso cuando ya no se requieran los activos. Esta política debe determinar la toma de backup de los activos evitando así el acceso o borrado no autorizado de la información, la política debe indicar quien es el responsable de emitir las correspondientes autorizaciones y debe aplicar tanto para medios removibles como activos de procesamiento y/o almacenamiento de información.

3.2.6. Devolución de los Activos: El instrumento y responsable del cumplimiento, mediante el cual se genera obligatoriedad para que los funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizada la relación, el empleo, acuerdo o contrato que se tenga con la Alcaldía Distrital de Cartagena de Indias.

- Devolución de documentación física y digital: Los funcionarios realizarán la devolución de toda la documentación física y digital de acuerdo al 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

3.2.7. Devolución de muebles e inmuebles: Este tipo de enseres se entregarán bajo los lineamientos y el procedimiento establecidos por Almacén, guardando la respectiva evidencia de ello.

3.2.8. Devolución de equipos tecnológicos: Una vez finalizada la relación contractual, Todos los elementos tecnológicos serán entregados bajo el procedimiento para devolución de equipos informáticos No GTIGI04-POO2

3.2.9. Devolución de credenciales: Solo se puede entregar las credenciales de acceso a una nueva persona responsable de usuarios genéricos; por medio de la notificación a la Oficina asesora informática, mediante el diligenciamiento del formato de control de accesos a servicios digitales, 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 que se realice antes de la terminación del contrato dado que los mismo se bloquearán una vez finalice la relación contractual.

3.2.10. **Gestión de medios removibles**: Para todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores. Esta política 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 GTIGI03-F001, el cual debe estar debidamente diligenciado. 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".

3.2.11. Dispositivos móviles: Esta política debe determinar 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 debe describir las responsabilidades que deben tener los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles así

como como los controles de seguridad que la Alcaldía Distrital de Cartagena de Indias utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.

3.3. POLÍTICA PARA EL CONTROL DE ACCESO A APLICACIONES

Objetivo: Definir las directrices generales para un acceso controlado y seguro a la información de la Alcaldía Distrital de Cartagena de Indias

Este grupo de políticas deben hacer 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:

3.4.1. Control de acceso con usuario y contraseña

- El control de acceso a redes, aplicaciones, y/o sistemas de información de la Alcaldía Distrital de Cartagena de Indias, se realiza mediante la solicitud en la mesa de servicios una vez se haya diligenciado el formato de control de Acceso a Recursos Digitales GTIGI03-F001 mediante el cual se determinen los responsables formalmente
- La creación, modificación, suspensión o eliminación de usuarios (ID) y asignación de contraseñas se debe centralizar en la Oficina Asesora de Informática.
- 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.
- 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 GTIGI03-F001 para que se asigne las personas el usuario y contraseña a los servicios que necesita para cumplir con la relación contractual establecida.

3.4.2. Suministro del control de acceso:

- 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 GTIGI03-F001.
- Los usuarios genéricos o no, son de uso unitario; es decir, una cuenta NO debe ser utilizada por más de una persona.
- Se debe verificar y asegurar que los *desarrolladores, administradores de los recursos tecnológicos y servicios de red* no tengan acceso a sistemas de información en producción. Restringir las conexiones remotas a los recursos de la plataforma tecnológica solo a personal debidamente autorizado y solo para las labores asignadas.

3.4.3. Gestión de Contraseñas

- 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 siguientes parámetros mínimos para que una contraseña sea considera como fuerte, gestión de cambio de contraseña: 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.

- 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.

3.4. POLITICAS SOBRE PERÍMETROS DE SEGURIDAD

- 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 autorizar para su acceso pues las mismas áreas son delimitadas como de acceso restringido.
- 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.

3.5. POLITICAS PARA EL CONTROL DE ACCESO A REDES E INTERNET

- 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.
- Las contraseñas son estrictamente de uso personal e intransferible y es responsabilidad de cada usuario el uso de las credenciales asignadas.
- 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.
- 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 GTIGI03-F001.

3.6. POLITICAS PARA LA GESTIÓN DE ACCESO A USUARIOS

- Los usuarios deben cambiar sus claves de acceso periódicamente, incluso pueden hacerlo antes de que la cuenta expire.
- Las contraseñas deben contener Mayúsculas, Minúsculas, números y por lo menos un carácter especial y de una longitud mayor a 8 caracteres.
- Los Sistemas de información debe obligar al usuario a cambiar la contraseña por lo mínimo 1 vez cada 90 días.
- Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por el administrador.
- Se mantiene un registro de las 4 últimas contraseñas utilizadas por el usuario con el fin de evitar la reutilización de estas.
- Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.
- Cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware.
- No se debe prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, jefes u otras personas que lo soliciten.
- 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.

- Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.
- Reportar a la Oficina Asesora de Informática al correo seguridadoai@cartagena.gov.co sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.
- Está rotundamente prohibido utilizar las credenciales asignadas a un funcionario en otros equipos y para otros usuarios. Cada funcionario debe tener su cuenta.
- Reportar a la Oficina Asesora de Informática al correo seguridadoai@cartagena.gov.co sobre cualquier sospecha o evidencia de que una persona esté utilizando una contraseña y usuario que no le pertenece.
- 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.
- 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 y actualizada y parches de seguridad al día.

3.7. POLITICAS PARA LA REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS

- 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.

- Retiro de los derechos de acceso: Cada dependencia de la Alcaldía Distrital de Cartagena de Indias y la Dirección de Talento humano son responsable 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.

3.8. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo: Evitar accesos físicos no autorizados a las instalaciones de la Alcaldía Distrital de Cartagena de Indias, donde se procese o trate información que pueda ser vulnerada,

eliminada o alterada, o que pueda estar expuesta y generar incumplimiento frente a la confidencialidad, integridad o disponibilidad.

3.8.1. Perímetro de Seguridad Física

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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 o Coordinador de la dependencia correspondiente.
- Los dispositivos 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.
- 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.

3.8.2. Controles de Acceso Físico

- 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.

- En las áreas seguras, en ninguna circunstancia se puede fumar, comer o beber.
- 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.
- 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.

3.8.3. Ubicación y Protección de los equipos

- 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.
- 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.
- Autorizar y gestionar el acompañamiento permanente de los visitantes a las áreas de procesamiento de información y centros de comunicación.
- Registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una
- 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.
- L las áreas de carga y descarga deben estar aisladas de equipos de cómputo, del centro de cómputo y otras áreas de procesamiento de información.
- Velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados
- 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.
- Velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las áreas solo sean utilizados por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios.

3.8.4. Seguridad de los equipos fuera de las instalaciones

- 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, la misma debe estar encriptada.
- 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.
- En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente a la Oficina Asesora de Informática, se debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de esta.
- Para el caso de los equipos que cuentan con puertos de transmisión y recepción de infrarrojo y Bluetooth estos deben estar deshabilitados.
- Todos los equipos de cómputo deben ser registrados al ingreso y al retirarse de las instalaciones de la Alcaldía Distrital de Cartagena de Indias.

3.8.5. Seguridad en la reutilización o eliminación de los equipos

- Cuando un equipo de cómputo sea reasignado, devuelto o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada, 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.

3.8.6. Retiro de Equipos de Activos

- 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.
- Se debe realizar periódicamente comprobaciones puntuales para detectar el retiro no autorizado de activos de la Alcaldía Distrital de Cartagena de Indias.

3.8.7. Áreas De Carga

- Las áreas físicas en las cuales se va a realizar despacho y carga de paquetes físicos para bodegas o espacios definidos de carga, esto con el fin de evitar el acceso no autorizado a otras áreas de la Alcaldía Distrital de Cartagena de Indias, queda bajo la responsabilidad de la Secretaría General.

3.9. POLÍTICA DE ESCRITORIO DESPEJADO Y PANTALLA DESPEJADA

Objetivo: Definir los aspectos generales para mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida, modificación y daño de la información de la Alcaldía Distrital de Cartagena de Indias.

- Todo el personal 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.
- Todo el personal 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.
- Todos los usuarios al finalizar sus ejercicios diariamente deben salir de todas las aplicaciones y apagar las estaciones de trabajo.
- En horario no hábil o cuando los puestos de trabajo se encuentren libres, los usuarios deben dejar la información CONFIDENCIAL protegida bajo llave o en un lugar seguro para evitar fuga, replica o eliminación de los datos.

3.10. POLITICA PARA LA PROTECCIÓN Y PRIVACIDAD DE DATOS PERSONALES

Se debe llevar en estricto cumplimiento de la política del tratamiento de datos personales que se encuentra alineada y conforme a lo establecido en la normatividad vigente. La política de privacidad debe resguardar los siguientes principios establecidos en la ley de protección de datos personales:

- *"Principio de la Legalidad*: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
- *Principio de finalidad*: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
- *Principio de libertad*: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
- *Principio de veracidad o calidad:* La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- *Principio de transparencia:* Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.

- *Principio de acceso y circulación restringida:* El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
- *Principio de seguridad:* La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento
- *Principio de confidencialidad*: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información."

Esta política está encaminada al garantizar los **Derechos de los titulares La política debe indicar los derechos de los titulares de los datos.**

La confidencialidad de la información, debe establecerse por medio de un compromiso o acuerdo de confidencialidad, en el cual todo funcionario, contratista y/o tercero vinculado a la Alcaldía Distrital de Cartagena de Indias, deberá firmar un compromiso de no divulgar la información interna y externa que conozca de la Alcaldía Distrital de Cartagena de Indias, así como la relacionada con las funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

3.11. POLITICA DE INTEGRIDAD

La política de integridad debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros que hagan parte de la Alcaldía Distrital de Cartagena de Indias, la cual se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los mismos.

De esta manera, toda información verbal, física o digital, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información. En el caso de vinculación contractual, el Compromiso de administración y manejo integro e integral

de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información.

La política de integridad, deberá establecer asimismo la vigencia del mismo acorde al tipo de vinculación del personal al cual aplica el cumplimiento

3.12. POLITICA 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 OAI 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 OAI
- **Acuerdos de Nivel de servicio:** Tener en cuenta los acuerdos de niveles de servicios (ANS) en las interrupciones del servicio.
- **Segregación de ambientes**: Minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos con el fin de minimizar el impacto de la indisponibilidad del servicio durante las fases de desarrollo, pruebas y producción.
- **Gestión de Cambios:** Los cambios para que los pasos a producción afecten mínimamente la disponibilidad y se realicen bajo condiciones controladas.

3.13. POLITICA PARA LA GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Alcaldía Distrital de Cartagena de Indias deberá documentar todos los eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

Ante un incidente de Seguridad en el que se encuentren implicados datos personales, el oficial de seguridad y privacidad debe reportar a la Superintendencia de Industria y Comercio de manera inmediata en el Registro Nacional de Base de Datos tal como se encuentra establecido en la normatividad vigente de la protección de los datos personales.

3.14. POLITICA PARA EL MANEJO DE COPIAS DE SEGURIDAD

- 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 OAI, 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 backup. 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
- Backup, el cual contendrá Nombre de la Tarea, Fecha, Hora, Novedad, Acción a tomar.

- El líder designado por la Oficina Asesora de Informática (OAI), vigilará diariamente el perfecto cumplimiento de la Copia de Seguridad, revisando el Registro diario de novedades de Backup diligenciado por el Administrador de Copias.
- 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.
- 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 OAI, 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 software de respaldo y restauración de información debe estar instalado en los servidores para los cuales se haya hecho solicitud de backup. Se debe contar con las licencias necesarias que garanticen el cumplimiento de dicha solicitud.
- El líder designado por la Oficina Asesora de Informática (OAI), vigilará diariamente el perfecto cumplimiento de la Copia de Seguridad, revisando el Registro diario de novedades de Backup diligenciado por el Administrador de Copias.
- 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 Backup, el cual contendrá Nombre de la Tarea, Fecha, Hora, Novedad, Acción a tomar.

3.15. POLITICAS PARA LA PROTECCIÓN CONTRA CÓDIGO MALICIOSO

La entidad cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Actualmente poseen capacidades de inspección de contenido más profundas. Estas capacidades ofrecen la habilidad de identificar ataques, malware y otras amenazas, y permiten a los NGFW bloquear estas amenazas.

Actualmente se cuenta con herramientas para la protección como:

- Web Filter
- DNS Filter
- Control de Aplicaciones
- Prevención de Intrusos
- Antiransomware
- Detección y respuesta para endpoints
- Bloqueo de periféricos (USD, Disco extraíbles, etc)
- Bloqueos de IP maliciosas

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.

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.

La Oficina Asesora 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.

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.

La Alcaida 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 de Tecnologías de la Información y las Comunicaciones.

El antivirus adquirido por MEN, sólo debe ser instalados por los responsables de la Oficina de Tecnologías de la Información y las Comunicaciones

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 de Tecnología y Sistemas de Información sobre el tratamiento que debe darse en caso de sospecha de malware.

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.

3.16. POLÍTICA DE GESTIÓN DE SEGURIDAD DE LAS REDES

La Entidad establece 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. La Alcaldía usan la segmentación para mejorar la supervisión, aumentar el rendimiento, identificar problemas técnicos y, lo más importante, mejorar la seguridad.

Con la segmentación de la red, el personal de la seguridad de red cuenta con una herramienta potente para evitar que usuarios no autorizados, ya sean infiltrados o atacantes malintencionados, obtengan acceso a recursos valiosos, como la información personal de clientes, los registros financieros

Para comprender el uso que la seguridad hace de la segmentación de red, primero hay que analizar el concepto de confianza en la seguridad de red.

El acceso a los recursos de red inalámbrica está restringido y se solicitara a los usuarios la identificación por MAC, a través del formato de control de acceso GTIGI03-F001, esto nos ayudara a tener un mayor control y separar las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.

La segmentación lógica crea subredes mediante uno de dos métodos primarios: las redes de área local virtuales (VLANs) o los esquemas de direcciones de red. Los enfoques basados en las VLANs son bastante sencillos de implementar porque las etiquetas VLAN en rutan el tráfico de forma automática a la subred adecuada. Los enfoques de direcciones de red son igual de eficaces, pero requieren un conocimiento más detallado de la teoría de la red. La segmentación lógica es más flexible que la física porque no requiere cableado ni el movimiento de componentes físicos. El aprovisionamiento automático puede simplificar en gran medida la configuración de las subredes.

El traslado a una arquitectura de segmentación brinda la oportunidad de simplificar la administración de las políticas de firewall. Una práctica recomendada emergente es usar una sola política consolidada para el control de acceso a las subredes, al igual que para la detección y la mitigación de las amenazas, en lugar de realizar esas funciones en diferentes partes de la red. Con este método, se reduce la superficie de ataque y se fortalece el enfoque de seguridad de la Alcaldía.

3.17. POLITICA PARA EL DESARROLLO SEGURO

La seguridad digital debe implementarse durante el ciclo de vida del desarrollo del software para todos los desarrollos nuevos y de las actualizaciones de cualquier aplicación, teniendo en cuenta:

- Cada desarrollo debe estar debidamente documentado, en estricto seguimiento y cumplimiento de los lineamientos establecidos frente para su arquitectura, utilización de las aplicaciones de desarrollo, pruebas funcionales, esquema y niveles de seguridad.
- Todo proyecto que implique desarrollo debe ser llevado al comité de proyectos de la OAI 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.

- 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.
- La aplicación que se encuentre en desarrollo debe apuntar al nombre y no a la dirección IP.
- Todos los ingenieros que se encarguen de realizar desarrollos deben seguir los lineamientos del Gestor de desarrollo.

3.18. POLÍTICA DE CUMPLIMIENTO LEY DE TRANSPARENCIA

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 su responsabilidad a través de los procedimientos establecidos.

3.19. POLITICAS PARA EL SERVICIOS DE COMPUTACIÓN EN LA NUBE

- 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.
- 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.
- 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.
- 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.

- Hacer la identificación, valoración y evaluación de los riesgos asociados al uso de servicios de computación en la nube.
- Realizar y evaluar controles para mitigar los riesgos de seguridad digital
- Proveer servicios de copia de respaldo para la información que está autorizada para almacenamiento en computación en la nube.
- Implementar controles de seguridad digital los servicios en la nube.
- La Alcaldía Distrital de Cartagena debe Definir e implementar plan de contingencia para preservar la información almacenada en servicios de computación en la nube.
- Mantener inventario de los servicios de computación en la nube autorizados para uso dentro de las redes corporativas.
- Mantener inventario de los usuarios a los que se les autoriza el uso de servicios de computación en la nube.
- Realizar monitoreo de seguridad digital utilizando las tecnologías de correlación aprovisionadas por la Alcaldía o por un servicio contratado para este fin
- Asegurar que todo servicio de computación en la nube se diseñe, implemente y opere conforme a las políticas de seguridad digital y gestión de riesgo institucional.
- Asegurar la existencia de Acuerdos y/o Cláusulas de Confidencialidad con proveedores de servicios de computación en la nube.
- Especificar responsabilidades sobre el uso de servicios de computación en la nube (almacenamiento y/o procesamiento) del personal a su cargo.
- 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.
- Cuando se use almacenamiento en la nube, toda información calificada como Sensible, confidencial y toda información de carácter personal esta debe permanecer cifrada para evitar su divulgación o acceso no autorizadas.
- No hacer uso de servicios de computación en la nube desde equipos de cómputo de uso compartido inseguros como café internet o centros de alquiler de equipos públicos.
- No almacenar información sujeta a derechos de autor (videos, imágenes, audio, libros, entre otros).

3.20. POLITICAS PARA LA SENSIBILIZACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Se debe 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 parámetros como:

- El compromiso para destinar los recursos suficientes para desarrollar los programas.
- 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.
- Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.

3.21. POLITICA PARA EL USO DE TOKENS DE SEGURIDAD

- La Alcaldía Distrital proveerá el manejo de los tokens de seguridad para las dependencias y oficinas que lo requieran utilizar y asignar a los funcionarios que serán responsables, acción que será intransferible.
- Recibir los tokens y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar las operaciones con ellos.
- Avisar a las Entidades emisoras en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.
- El almacenamiento de los tokens debe efectuarse bajo estrictas medidas de seguridad, previendo su acceso o utilización no autorizada (almacenamiento en la tula, sobre caja fuerte, escritorio con llave, gaveta u otros).
- Prevenir su daño por contacto con líquidos, sustancias químicas, fuego o agentes que los puedan dañar (polvo, fuentes de calor extremo, campos magnéticos fuertes, etc.
- Mantener en secreto las claves de uso del token

3.22. POLITICA PARA EL TELETRABAJO

El objetivo Garantizar la seguridad de la información, de tal manera que la confidencialidad, disponibilidad y autenticidad

Para poder realizar el teletrabajo y serializarlo de manera segura se debe:

- Instalar y mantenga actualizado el software antivirus, de un fabricante reconocido, para evitar infecciones con virus o software malicioso.
- Instalar permanentemente las actualizaciones del sistema operativo
- No se debe conectar de rede abiertas o públicas
- Solicitar a la mesa de servicios o realizar copias de seguridad periódicamente.
- Asegurar un espacio adecuado y óptimo sin riesgo a perder información por causa de daño del equipo por la mala manipulación de alimentos.
- No instalar aplicaciones de fuentes desconocidas ya que estas suelen traer malware, el cual puede afectar sus dispositivos y extraer la información sensible.

3.23. 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 No. XX del XX de XXXXX del XXXX del Comité Institucional de Gestión y Desempeño