POLÍTICA DE SEGURIDAD DIGITAL

EQUIPO MIPG 2021

Fondo de Vivienda de Interés Social y Reforma Urbana Distrital
CORVIVIENDA
Cartagena 2021

FONDO DE VIVIENDA DE INTERES SOCIAL Y REFORMA URBANA DISTRITAL - CORVIVIENDA
Dir: Manga 3ª Avenida, Calle 28 #21-62
Email: atencionalusuario@corvivienda.gov.co
www.corvivienda.gov.co
Tel: 301 479 3336 – 301 479 3290

TABLA DE CONTENIDO

1.INTRODUCCIÓN

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

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

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

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

2. MARCO JURÍDICO

Constitución Política de Colombia 1991 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 23 1982 Derechos de Autor.

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

Ley 594 2000 Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

Ley 603 2000 Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

Ley 962 2005 Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.

Ley 1150 2007 Seguridad de la información electrónica en contratación en línea.

Ley 1266 2008 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

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

Ley 1341 2009 Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley 1474 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la

gestión pública. Decreto 4632 de 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

Ley 1581 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 1755 2015 Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Título II Capítulo I.

Conpes 3854 2016 Política Nacional de Seguridad Digital

Decreto 2364 2012 Firma electrónica

Decreto 2609 2012 Expediente electrónico Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

Decreto 2693 2012 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones

Decreto 1377 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 103 2015 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

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

3.OBJETIVO GENERAL

Fortalecer las capacidades institucionales para la identificación, gestión, tratamiento y mitigación de los riesgos de seguridad digital en las actividades institucionales en el entorno digital, en un marco de cooperación, colaboración y asistencia con los grupos de valor y grupos de interés.

3.1 OBJETIVOS ESPECIFICOS.

- Definir las acciones a implementar en materia de seguridad y privacidad de la información basándose en los resultados del diagnóstico de la gestión de seguridad y privacidad de la información al interior de la institución y en el marco de la metodología de gestión del riesgo.
- Crear las condiciones para la gestión del riesgo de seguridad digital en los procesos y actividades institucionales generando confianza en el uso del entorno digital por parte de los grupos de valor y grupos de interés.
- Evaluar la efectividad, la eficiencia y la eficacia de las acciones implementadas en materia de seguridad y privacidad de la información para la mejora continua de las mismas

4.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.

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.

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 de un proceso.

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 de las políticas institucionales.

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.

Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la Entidad. 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 Digital, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

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.

ISO 19011: Guía de utilidad para el desarrollo de las funciones de auditor interno.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO.

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información

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

ISO IECTR 13335-3: Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

ISO IECTR 18044: Guía de utilidad para la gestión de incidentes de seguridad de la información.

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

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 aspectos a revisar, 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.

Medida correctiva: Medida de tipo reactivo orientada a eliminar, minimizar o mitigar la causa y consecuencias de una no conformidad.

Medida preventiva: Medida de tipo pro-activo orientada a prevenir potenciales no conformidades.

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.

Personal: Son todos los funcionarios de la Entidad, 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 Entidad.

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 Entidad, 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.

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.

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

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de la Entidad, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la Entidad 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.

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

5. CONTEXTO ESTRATEGICO DE LA ENTIDAD

MISION

El Fondo de Vivienda de Interés Social y Reforma Urbana Distrital – Corvivienda, es una Entidad que construye comunidad desde el derecho fundamental a la vivienda digna, a la prosperidad y a un hábitat sostenible, en articulación con el Sistema Nacional de Vivienda, apoyados en la planificación estratégica del crecimiento territorial organizado.

VISION

En el 2025 seremos la Entidad líder en la gestión y ejecución de soluciones de vivienda de interés social y de interés prioritario en el ámbito local, reconocidos a Nivel Regional y Nacional como grandes promotores del desarrollo territorial sostenible y del bienestar social en Cartagena.

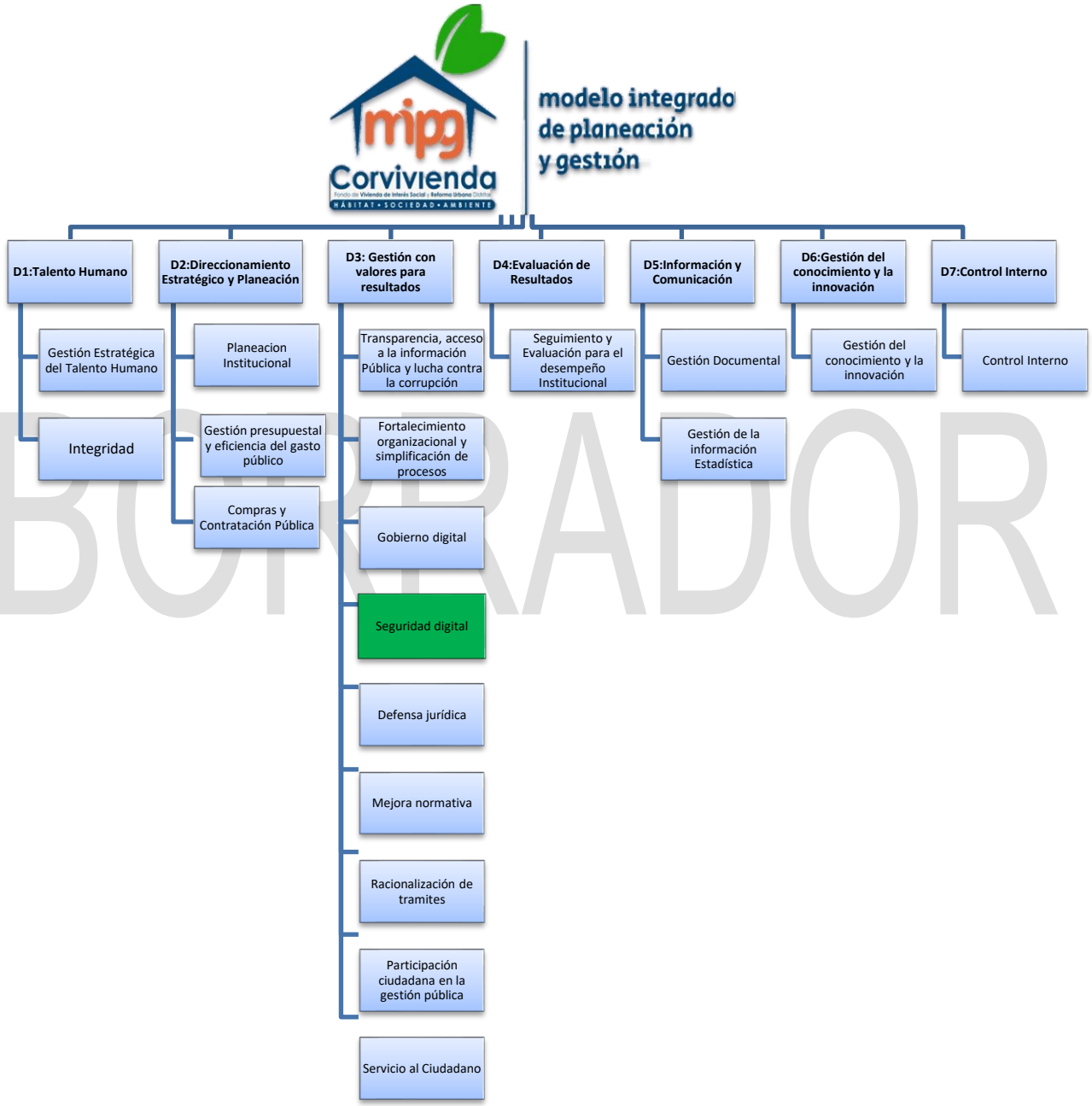
DIMENSIÓN

La Política de Seguridad Digital, pertenece a la 3ª. Dimensión: Gestión con valores para resultados El propósito de esta dimensión es permitirle a la entidad realizar las actividades que la conduzcan a lograr los resultados propuestos y a materializar las decisiones plasmadas en su planeación institucional, en el marco de los valores del servicio público.

Para concretar las decisiones tomadas en el proceso de planeación institucional, y teniendo en cuenta el talento humano del que se dispone, en esta Dimensión se abordan los aspectos más importantes que debe atender una organización para cumplir con las funciones y competencias que le han sido asignadas. Para ello, esta dimensión se entenderá desde dos perspectivas: la primera, asociada a los aspectos relevantes para una adecuada operación de la organización “de la ventanilla hacia adentro”; y la segunda, referente a la relación Estado Ciudadano “de la ventanilla hacia afuera”.

6. ESTRUCTURA GENERAL DE LA POLÍTICA

6.1 DIMENSIÓN



6.2 ÀMBITO DE APLICACIÓN DE LA POLÍTICA

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

6.3 PROPÓSITO DE LA POLÍTICA

La **política de seguridad digital** busca fortalecer las capacidades de la institución para identificar, gestionar y mitigar los riesgos de seguridad digital en las actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia que permita gestionar la confidencialidad, integridad.

6.4 LINEAMIENTOS ESTRATÉGICOS PARA LA IMPLEMENTACIÓN DE LA POLÍTICA

La dirección de la Entidad, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un modelo de gestión de seguridad y privacidad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

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

Esta política aplica a la Entidad teniendo en cuenta los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Disminuir el riesgo de las funciones más importantes de La Entidad.

- Desempeñar de manera activa la protección de los activos de información bajo la confidencialidad, integridad y disponibilidad que son los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Generar y mantener la confianza entre todas las personas involucradas en el tratamiento de la información.
- Fortalecer la innovación tecnológica.
- Preservar los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, terceros, aprendices, practicantes y contribuyentes de Entidad
- Coadyuvar a la continuidad del distrito frente a incidentes.
- La Entidad ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de la Entidad:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- La Entidad protegerá la información generada, procesada o resguardada por los procesos, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- La Entidad protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales

debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La Entidad protegerá su información de las amenazas originadas por parte del personal.
- La Entidad protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La Entidad controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Entidad implementará control de acceso a la información, sistemas y recursos de red.
- La Entidad garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Entidad garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Entidad garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Entidad garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

La Entidad, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la Entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Entidad
- Garantizar la continuidad del negocio frente a incidentes.

6.4.1 NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política. A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de La Entidad:

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

- La Entidad implementará control de acceso a la información, sistemas y recursos de red.
- La Entidad garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Entidad garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Entidad garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- La Entidad garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- El incumplimiento a la Política Digital (Información e informática), traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

6.4.2 ROLES Y RESPONSABILIDADES

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

6.4.2.1 Comité De Gestión Y Desempeño Institucional

- Aprobar y verificar del cumplimiento de las políticas y procedimientos de seguridad y privacidad de la información.
- Hacer que los miembros del Gabinete sean conscientes de la criticidad de los activos de información para el desarrollo de los procesos de la Entidad.
- Divulgar las responsabilidades de seguridad y privacidad de la información de la Entidad con base en los lineamientos del MSPI.

6.4.2.2 Nivel Directivo: Asesores, directores y jefe de oficinas

- Liderar y apoyar de mejora continua para la aplicación del MSPI al interior de la dependencia a cargo.
- Alineación de los objetivos de la dependencia para que su cumplimiento este apoyado por el MSPI.
- Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguridad y privacidad de la información para los roles definidos en la dependencia a cargo.
- Proveer los recursos necesarios para la implementación del MSPI al interior de la dependencia a cargo.
- Apoyar la capacitación y entrenamiento requerido para que los funcionarios y contratistas de la dependencia a cargo que cumplan con el MSPI.
- Aplicar el proceso disciplinario ante los incidentes de seguridad y privacidad de la información originada por un funcionario o contratista de la dependencia a cargo.

6.4.2.3 Líder de Gestión TIC

- Liderar y apoyar la mejora continua para la aplicación del MSPI al interior de la Entidad.
- Asignar dentro de su equipo de trabajo quien servirá como oficial de seguridad y privacidad de la información.
- Apoyar las actividades relacionadas con el MSPI.

6.4.2.4 Oficial de seguridad y privacidad de la información

- Apoyar en definir y actualizar el inventario de los activos de información.
- Realizar análisis de riesgos de seguridad y privacidad de la información con base en lo establecido en el MSPI.

- Velar por la ejecución del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
- Definir y generar el modelo de seguridad y privacidad de la información - MSPI.
- Identificar los requerimientos normativos, de servicios o software necesarios para implementar, mejorar y garantizar la eficacia del protocolo de seguridad informática, garantizando la integridad, la confidencialidad y la protección de todos los activos de la empresa a nivel tecnológico.
- Definir la arquitectura de la seguridad de la red y sus políticas de acceso y control
- Potenciar la cultura de seguridad informática a nivel global en la Entidad
- Responder y dar solución a posibles problemas e incidencias que se presenten.
- Analizar los sistemas de información con el ánimo de encontrar eventos o incidentes que puedan afectar el procedimiento y ocasionar fugas de información, suplantación o corrupción de los datos, apoyando en definición del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
- Participar en el seguimiento y evaluación de las políticas, programas e instrumentos relacionados con la información pública, confidencial y sensible que esté bajo la responsabilidad de la Entidad de Cartagena de Indias
- Impartir lineamientos tecnológicos para el cumplimiento de estándares de seguridad, privacidad, calidad y oportunidad de la información de la Entidad y la interoperabilidad de los sistemas que la soportan, así como el intercambio permanente de información.
- Evaluación de iniciativas a nivel del riesgo, interrupción de operación, medidas de seguridad de los sistemas de información y de los sistemas informáticos que lo soporta.
- Analizar la relación de usuarios, roles, funciones y responsabilidad asignada en los diferentes accesos a las Redes, Aplicaciones, Base de Datos, Infraestructura, Almacenamiento de información Física y Digital.
- Aprobar la gestión de accesos a los servicios informáticos.
- Hacer seguimiento de los esquemas de seguridad operativa.
- Asesorar en la creación de desarrollos nuevos o en la adquisición de servicios y aplicaciones.
- Representar a la Entidad ante los entes de control y vigilancia.

- Realizar matriz de riesgo de los activos de información.
- Auditar procesos, aplicativos, gestión de usuarios y servicios.
- Investigar las posibles amenazas y vulnerabilidades a nivel de toda la Entidad.
- Supervisar todos los cambios que se produzcan en materia de seguridad informática y estar al día de las nuevas amenazas que aparecen en el mundo de la seguridad informática para prepararse ante ellas de manera preventiva.
- Controlar la implementación de sistemas de información, Sistemas informáticos y/o servicios a nivel trasversal de la Entidad
- Guiar al cuerpo directivo y a la administración de la organización ante incidentes de seguridad mediante un Plan de Respuesta a Incidentes, con el fin de atender rápidamente este tipo de eventualidades
- Ser el nexo entre la entidad y la compañía contratada para la realización de auditorías externos de ser necesario
- Trabajar en el cumplimiento de la política de seguridad, política de tratamiento de datos de la Entidad
- Atender y responder inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.
- Lo anterior es responsabilidad del oficial de seguridad y privacidad de la información, pero debe contar con la participación de todos los funcionarios y contratistas de la Entidad.

6.4.3 GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Validar la documentación propia del MSPI dentro de la dependencia que representa.
- Fomentar dentro de su dependencia la práctica de directrices de seguridad y privacidad de información.
- Apoyar la identificación y actualización del inventario de activos de información y riesgos de estos.
- Disminuir las brecas de seguridad de la información a nivel de seguridad táctica como operativa

- Apoyar la identificación e implementación de controles para la mitigación de riesgos de seguridad y privacidad de información.
- Realizar o gestionar la auditoría, análisis de vulnerabilidad, hacking ético o cualquier actividad que permita disminuir los riesgos en seguridad y privacidad de información.
- Participar en las jornadas de implementación, mantenimiento y mejora del MSPI.
- Sensibilizar del cumplimiento de la seguridad digital.

6.4.4 DEBERES DE FUNCIONARIOS, CONTRATISTAS Y TERCEROS VINCULADOS CON LA ENTIDAD

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

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

6.4.5 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 Entidad 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 Entidad

6.4.6 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 Entidad, 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:

6.4.6.1 Identificación de Activos

Para llevar a cabo una correcta identificación de los activos de información se debe:

- La Entidad 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 Oficina Asesora Administrativa y Financiera, identifica, registra y controla el personal que tiene cualquier vínculo con la Entidad.
- 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.
- 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.

6.4.6.2 Clasificación de Activos de información

Cada dependencia de la Entidad clasifica de acuerdo a la criticidad, sensibilidad y reserva de la misma, los activos de información, conforme a las leyes y normatividades actuales que la Entidad, los mismo se deben llevar a verificación mediante una mesa de trabajo a las áreas 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.

- 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 comercial” 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”

6.4.6.3 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.

6.4.6.4 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.

6.4.6.5 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, 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.

6.4.6.6 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 Entidad.

6.4.6.7 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 Planeación.

6.4.6.8 Devolución de equipos tecnológicos

Una vez finalizada la relación contractual, todos los elementos tecnológicos serán entregados a al supervisor del contrato con el visto bueno de la Oficina Asesora Administrativa y Financiera quien a su vez informara al equipo de Gestión TIC para determinar el estado del equipo devuelto.

6.4.6.9 Devolución de credenciales

Solo se puede entregar las credenciales de acceso a una nueva persona responsable de usuarios genéricos; por medio de la notificación al equipo de Gestión TIC, 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.

6.4.6.10 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 Entidad 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 Entidad utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.

6.4.7 POLÍTICA DE CONTROL DE ACCESO

Objetivo: Definir las directrices generales para un acceso controlado y seguro a la información de la Entidad.

Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales la Entidad 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:

6.4.7.1 Control de acceso con usuario y contraseña

- El control de acceso a redes, aplicaciones, y/o sistemas de información de la Entidad, 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 Planeación – Equipo Gestión TIC.
- 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 Planeación – Equipo Gestión TIC.

- En la Entidad 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 Planeación – Equipo Gestión TIC 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.

6.4.7.2 Suministro del control de acceso

- La Oficina Asesora de Planeación – Equipo Gestión TIC 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 Entidad los cuales deben venir con la firma del jefe de La Oficina Asesora de Planeación, la firma del líder del Equipo Gestión TIC 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.

6.4.7.3 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 Entidad 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.

6.4.8 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 Planeación – Equipo Gestión TIC y con previa autorización.

6.4.9 CONTROL DE ACCESO A REDES E INTERNET

- La Entidad 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 Entidad, 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 Planeación – Equipo Gestión TIC.

- La conexión remota a la red de área local de la Entidad 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 Planeación – Equipo Gestión TIC, a través del formato de control de Acceso a Recursos Digitales GTIGI03-F001.

6.4.10 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 Planeación – Equipo Gestión TIC al correo sistemas@corvivienda.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 Planeación – Equipo Gestión TIC al correo sistemas@corvivienda.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 Planeación – Equipo Gestión TIC.
- Todo equipo de cómputo que requiera acceso a la red interna de la Entidad deberá tener como mínimo las siguientes medidas de seguridad: solución de antimalware instalada y actualizada y parches de seguridad al día.

6.4.11 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 Entidad, debe ser revisada periódicamente y cada vez que se realicen cambios de personal.

- Retiro de los derechos de acceso: Cada dependencia de la Entidad y la Oficina Asesora Administrativa y Financiera son responsable de comunicar a La Oficina Asesora de Planeación – Equipo Gestión TIC, las novedades relacionadas como el cambio de cargo, funciones o actividades o la terminación contractual de los colaboradores pertenecientes a cada dependencia.

6.4.12 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo: Evitar accesos físicos no autorizados a las instalaciones de la Entidad, 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.

6.4.12.1 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 Entidad.
- Los visitantes deben permanecer acompañados de un funcionario y/o contratista de la Entidad, cuando se encuentren en las oficinas o áreas donde se maneje información.
- Es responsabilidad de todos los funcionarios, contratistas y terceros de la Entidad 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 Entidad, 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 Entidad 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 Entidad 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 Entidad, 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 Entidad 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.

6.4.12.2 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.

6.4.12.3 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.

6.4.12.4 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 Planeación – Equipo Gestión TIC, 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 Entidad.

6.4.12.5 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 Planeación – Equipo Gestión TIC, 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.

6.4.12.6 Retiro de Equipos de Activos

- Ningún equipo de cómputo, información o software debe ser retirado de la Entidad sin una autorización formal por parte de La Oficina Asesora de Planeación – Equipo Gestión TIC.
- Se debe realizar periódicamente comprobaciones puntuales para detectar el retiro no autorizado de activos de la Entidad.

6.4.13 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 Entidad.

- Todo el personal de la Entidad 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 Entidad 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.

6.4.14 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 Entidad, deberá firmar un compromiso de no divulgar la información interna y externa que conozca de la Entidad, 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.

6.4.15 INTEGRIDAD

La política de integridad debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros que hagan parte de la Entidad, 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

6.4.16 DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

La Entidad 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 Entidad, 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 Planeación – Equipo Gestión TIC, 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 Entidad, 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 Entidad.
- Interrupciones: Toda acción que se realice en las dependencias de la Entidad 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 Planeación – Equipo Gestión TIC.
- 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.

6.4.17 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Entidad 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.

6.4.18 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 Entidad.
- Los líderes de proceso y jefes de dependencias son los únicos autorizados para solicitar, 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 de la 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 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 Entidad.
- 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 Oficina Asesora de Planeación – Equipo Gestión TIC en donde se disponga.

6.4.19 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 se cuenta con herramientas para la protección como:

- Web Filter
- DNS Filter
- Control de Aplicaciones
- Prevención de Intrusos
- Antiransomware
- Detección y respuesta para endpoints
- Bloqueos de IP maliciosas

La Oficina Asesora de Planeación – Equipo de Gestión TIC 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.

Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por la Entidad, 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.

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

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 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.

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 Entidad.

6.4.21 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.

6.4.22 POLÍTICA DE CUMPLIMIENTO LEY DE TRANSPARENCIA

La Entidad debe garantizar el derecho de acceso a la información pública por medio de los canales establecidos por la Entidad 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.

6.4.23 SERVICIOS DE COMPUTACIÓN EN LA NUBE

- Los activos de información de la Entidad 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 Oficina Asesora de Planeación – Equipo Gestión TIC, 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 Entidad 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 Entidad 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 Entidad.
- 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).

6.4.24 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 Entidad 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.

6.5 DECLARACIÓN DE LA POLÍTICA

La Política de Seguridad digital (información e informática) es la declaración general que representa la posición de la administración de La Entidad con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos y que apoyan la implementación del Sistema de Gestión de Seguridad de la Información, a través de un adecuado análisis, que logre el amparo de los activos de información para legitimar la confidencialidad, integridad y disponibilidad de los mismos.

La política se enmarca en establecer los componentes para blindar el sistema de información y los diferentes recursos de la Entidad, 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 Entidad, adoptando una metodología y procedimiento en la gestión del riesgo para el tratamiento de la información que permita una adecuada seguridad y privacidad de la misma que logre fortalecer y sostener un adecuado nivel de riesgos.

7. MECANISMOS PARA LA DIVULGACIÓN DE LA POLÍTICA

La política contenida en el presente documento será divulgada en los siguientes medios:

- Página web.
- Plan anual de capacitación.
- Impresos.
- Otros mecanismos que resulten aplicables.

8. DOCUMENTOS ESTRATEGICOS

- Plan de Acción: Se establece como criterio documental para la implementación de la política esta herramienta, ya que enmarca la hoja de ruta a seguir en la ejecución de esta.
- Manual operativo MIPG versión 4.0.

9. ROLES Y RESPONSABILIDADES

La oficina asesora de planeación institucional, a través de los funcionarios responsables de TI es la responsable de asumir los roles y responsabilidades, donde se garantice la implementación, revisión y mejora continua de la política de Seguridad Digital al interior de la Entidad.

CONTROL DE CAMBIOS

VERSIÓN	DESCRICPCION DE CAMBIOS
1.0	Elaboración de documento.

REFERENCIAS