INSTITUTO MUNICIPAL DE CULTURA DE YUMBO "IMCY"

POLITICA DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL AÑO 2.025

ELABORADO POR:
HÉCTOR FABIO GÓMEZ
ASESOR CONTROL INTERNO

YUMBO, ENERO 2.025

Contenido

1. INTRODUCCIÓN

Con la Generación Zillennials, también conocida como la generación “Z”; en donde el entorno global se define por el acceso al internet y posibilidad de contar con gran cantidad de información y la Revolución 5G se caracteriza por una fusión de tecnologías actualmente en prueba o en desarrollo, es decir, el mundo de los sistemas ciberfísicos cada vez más al alcance a la sociedad; los ciudadanos, las empresas, la entidades, están expuestos en el entorno digital a altos riesgos, por ende la necesidad protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos.

Una estrategia para contrarrestar estos riesgos, es educar y fomentar una cultura para crear consciencia del manejo de los riesgo y responsabilidad en uso de las plataformas digitales, de acuerdo a esto el IMCY inicia la creación e implementación de una Política de Seguridad Digital que nos acercará a los ciudadanos con estrategias de Ciberseguridad, en el desarrollo de capacidades institucionales para anticiparnos a las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones.

Para la creación de la Política de Seguridad de la Información y Digital nos basamos en los principios de la Política de Gobierno Digital, consagrados en el numeral 3 del artículo 4 de la ley 1341 de 2009, determina que el estado requiere la promoción y desarrollo de contenidos, así como la prestación de servicios que usen Tecnologías de la información y la Comunicaciones y la masificación del gobierno digital; orientados en brindar las garantías del derecho de acceso a la transparencia de la información pública, LEY 1712 DE 2014; punto de partida de Seguridad y Privacidad de la Información. Todas las referencias a las políticas, definiciones relacionadas publicadas en el resumen de las normas técnicas colombianas NTC ISO/IEC 27001 vigentes, así como a los anexos con derechos reservados por parte de ISO/ICONTEC; Ley 1955 de 2019: Plan Nacional de Desarrollo 2023– 2027 “Colombia potencia mundial de la vida”, Capitulo 2. Seguridad Humana y Justicia Social.

Al definir las políticas de seguridad digital (información e informática) que se deben seguir por parte de los colaboradores y terceros de la entidad, estas se deben guiar con el fin de preservar la disponibilidad, integridad y confidencialidad de la información, las cuales, deben enmarcarse en un proceso de mejora continua.

2. ALCANCE DE LA POLÍTICA.

La Política de Seguridad Digital y de la Información establece los lineamientos de seguridad desde cada uno de los procesos definidos en la entidad, y debe ser estipulada a todos los funcionarios, contratistas, proveedores, terceros y demás ciudadanos de forma interna o externa, logrando así el uso, cumplimiento y mejora continua de cada uno de los lineamientos en toda la Entidad.

3. DEFINICIONES.

- Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la Entidad.

- Acuerdos de Niveles de servicio: El modelo de Acuerdo de Nivel de Servicios (ANS) consiste en un contrato en el que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes, así, refleja contractualmente el nivel operativo de funcionamiento, penalizaciones por caída de servicio, limitación de responsabilidad por no servicio, etc. En esta parte del contrato se describe y obliga a un nivel específico de calidad en el suministro. Los puntos que debe cubrir un acuerdo de niveles de servicio son: servicio, soporte y asistencia, provisiones para seguridad y datos, Garantías del sistema y tiempos de respuesta, disponibilidad entre otros.

- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema de información o la Entidad.

- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- Análisis de vulnerabilidad: Es la medida o grado de debilidad de ser afectado por amenazas o riesgo según la frecuencia y severidad de estos. La vulnerabilidad depende de varios factores, entre otros: La posibilidad de ocurrencia del evento, la frecuencia de ocurrencia de este, los planes y programas preventivos existentes, la posibilidad de programación anual entre otros.

- ARL: Administradora de Riesgos Laborales.

- Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- CCTV: Circuito Cerrado de Televisión.

- Ciberamenaza o amenaza cibernética: Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

- Ciberataque o ataque cibernético: Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

- Ciberespacio: Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

- Ciber-riesgo o riesgo cibernético: Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos

- Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad.

- Cifrado: Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

- Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados.

- Contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

- Control de acceso: El proceso que limita y controla el acceso a los recursos de un sistema computarizado; un control físico o lógico diseñado para proteger contra usos o entradas no autorizadas. El control de acceso puede ser definido por el sistema (mandatory access control – MAC), o definido por el usuario propietario del objeto (discretionary access control – DAC)

- DBA: Esta palabra define el administrador de base de datos.

- Disponibilidad: Propiedad de ser accesible y utilizable sobre demanda por una Entidad autorizada.

- DRP: Disaster Recovery Plan - Plan de Recuperación de Desastres.

- Encriptación (Cifrado, codificación): La encriptación es el proceso para volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser Accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

- Estimación de riesgos: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

- Evaluación de Riesgos: Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad.

- Evidencia Digital: También conocida como evidencia computacional, única y conocida como: registros o archivos generados por computador u otro medio equivalente, registros o archivos no generados sino simplemente almacenados por o en computadores o medios equivalentes y registros o archivos híbridos que incluyen tanto registros generados por computador o medio equivalente como almacenados en los mismos.

- Firewall (Muro de Fuego - Cortafuego): Herramienta de seguridad que controla el tráfico de entrada/salida de una red.

- Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una Entidad con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

- Hacking - Hackear: Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar.

- Hardware: Es un término genérico para todos los componentes de Tecnología físicos (Redes, servidores, computadores, Portátiles, etc.)

- HIDS: Sistema de detección de intrusos en un Host. Busca detectar anomalías que indican un riesgo potencial, revisando las actividades en la máquina. Puede tomar medidas protectoras.

- IMAC: Instalación, Movimiento, Actualización y Cambio.

- Impacto: El costo para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros Eje: pérdida de reputación, implicaciones legales, etc.

- Incidente de Seguridad: Evento único o serie de eventos de seguridad de la información inesperados o no deseado que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

- Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

- Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal (Ley 1712 de 2014).

- Información: Datos relacionados que tienen significado para la Entidad. Además, es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la Entidad y, en consecuencia, necesita una protección adecuada.

- Infraestructura de TI: Todo el hardware, software, redes, instalaciones etc. requeridas para desarrollar, probar, proveer, monitorizar, controlar o soportar aplicaciones y servicios de TI.

- Integridad: Propiedad de la información que hace referencia a su exactitud y completitud.

- Internet: Es un sistema mundial de redes de computadores, integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computador puede, en caso de contar con los permisos apropiados, obtener información, efectuar transacciones, comunicarse y participar en toda gama de procesos públicos y privados puesto en dicha red.

- IP: Es un número que identifica de manera lógica y jerárquica a un dispositivo (habitualmente un computador) dentro de una red que utilice el protocolo IP (parte de la capa de Internet).

- Keylogger (registrador de teclas): Es una herramienta que se encarga de registrar las pulsaciones que se hacen sobre el teclado, para guardarlas en un archivo o enviarlas a través de Internet.

- Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el sistema de información.

- Mitigación: Acciones desarrolladas antes, durante y después de un siniestro, tendientes a contrarrestar sus efectos críticos y asegurar la supervivencia del sistema, hasta tanto se efectúe la recuperación.

- MSPI: Modelo de Seguridad y Privacidad de la Información.

- Navegador: Es un programa que, a través de la Web, permite visualizar hipertextos de datos o imágenes que estén en algún computador o en dispositivos conectados a la misma. La función primordial es la de poder acceder a páginas que se encuentran como hipervínculo en algún archivo. A esta acción de traslado de ubicación entre portales o sitios Web se le denomina Navegación. Los navegadores más utilizados son Internet Explorer y Mozilla Firefox.

- OTI: Oficina de Tecnología e Información.

- Password: Significa contraseña, clave, key o llave.

- Planes de contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

- VPN: En informática, acrónimo del Ingles Virtual Prívate Networks, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, por ejemplo, Internet manteniendo y garantizando la protección de la información.

- Política: Una política de seguridad es una regla de definición general, independiente de los ambientes tecnológicos, que representa los objetivos sobre los que se sustenta el Modelo de Seguridad de los Activos de Información. Debe cumplir con una directriz de la Entidad en general, debe revisarse y estar sujeta a modificaciones ante cambios estructurales.

- Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la Entidad en el marco de las funciones que a ella le compete realizar

- Propietario de Información: Unidad organizacional o proceso donde se crean los activos de información.

- Redundancia: Cuando la opción de las copias de respaldo no satisfaga el RPO (Recovery Point Objective, se refiere al volumen de datos en riesgo de pérdida que una Entidad considera tolerable) y RTO (Recovery Time Objective, expresa el tiempo durante el cual una Entidad puede tolerar la falta de funcionamiento de sus aplicaciones y / o nivel de servicio, sin afectar a la continuidad del negocio) se debe contar con un esquema de redundancia para los componentes de hardware y/o software involucrados.

- Requerimiento: Es una característica que el sistema debe tener o es una restricción que el sistema debe cumplir para satisfacer las necesidades del solicitante.

- Responsable de Seguridad de la Información: Es la persona con la función de supervisar el cumplimiento de la presente Política.

- Responsable por el activo de Información: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

- Riesgo de Seguridad de la Información: Es el potencial de que una amenaza pueda explotar una vulnerabilidad de un activo de información afectando la operación o imagen de la Entidad

- Riesgo: Es el potencial de exposición a pérdidas. Los riesgos, ya sean naturales o provocados por el hombre, son constantes a lo largo de nuestra vida diaria. El potencial es medido normalmente por su probabilidad de ocurrencia en un periodo determinado.

4. OBJETIVO DE LA POLÍTICA.

Establecer las políticas de seguridad digital y seguridad de la información, mediante el uso y la apropiación de los lineamientos de seguridad que permitan salvaguardar la confidencialidad, integridad y disponibilidad de la información en cumplimiento a la normatividad vigente y la protección de la información como el activo más relevante para la entidad, considerando los lineamientos de MINTIC.

5. PRINCIPIOS.

De acuerdo al MinTic la Política de Seguridad Digital se basa en unos principios fundamentales, que contemplan:

- Salvaguardar los derechos humanos y los valores fundamentales de los individuos.

- Adoptar un enfoque incluyente y colaborativo que involucre activamente a todos los interesados.

- Asegurar una responsabilidad compartida entre todos los actores involucrados.

- Adoptar un enfoque basado en riesgos, que permita a los individuos el libre, confiable y seguro desarrollo de sus actividades en el entorno digital.

6. EJES DE LA POLÍTICA DE SEGURIDAD DIGITAL.

Para lograrlo, se implementarán acciones en torno a cinco ejes de trabajo:

1. Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.

2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.

3. Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.

4. Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

7. MARCO NORMATIVO.

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 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 23 1982 y la Ley 603 2000 Derechos de Autor. 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 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.

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

Conpes 3854 2016 Política Nacional de Seguridad Digital.

2016 Guía para la Apertura de Datos en Colombia - Ministerio de Tecnologías de la Información y las Comunicaciones - Programa de Gobierno en línea.

Junio de 2016 Guía de Datos Abiertos en Colombia - Dirigida a las entidades sujeto de aplicación de la Ley 1712 de 2014 de Transparencia y Acceso a la Información Pública, para la aplicación de orientaciones y buenas prácticas en el desarrollo de estrategias de apertura y reúso de Datos Abiertos.

Septiembre de 2019 Guía para el Uso y Aprovechamiento de Datos Abiertos en Colombia.

2020 Resolución MinTIC 1519 del 2020 Directrices de accesibilidad web.

3975 del 2019 Conpes. Política Nacional para la Transformación Digital e Inteligencia Artificial.

Ley 1955 del 2019. Las entidades estatales del orden nacional deben incorporar en sus planes de acción el componente de transformación digital de acuerdo con los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones.

8. SEGURIDAD DIGITAL.

Con la política de Seguridad Digital se pretende fortalecer las capacidades de las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

Entre tanto, “el CONPES de Seguridad Digital es una herramienta para que todos los colombianos cuenten con un ambiente digital seguro, para ello las entidades del Estado y las empresas privadas deben implementar acciones para que los ciudadanos realicen, sin temor alguno, compras a través de internet, transacciones en línea, trámites con el Estado y todo tipo de actividades soportadas en medios digitales”

Por lo anterior el IMCY se compromete a implementar y garantizar los tres (3) pilares fundamentales de la seguridad de la información - confidencialidad, integridad y disponibilidad, gestionando y reduciendo los riesgos a un nivel aceptable, definición de roles y responsabilidades en seguridad digital, de acuerdo Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información (MSPI), así como garantizar la implementación del Sistema de Gestión de Seguridad de la Información – SGSI, y a contribuir con acciones continua del SGSI a través de un conjunto de reglas, y directrices orientadas proteger los activos de información, de una manera contundente, eficiente y efectiva.

9. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL.

El IMCY designó como responsable de la Seguridad Digital y de la Seguridad de la Información en la entidad, al líder del tema de sistemas de la entidad. De igual forma la entidad velará por el cumplimiento a las actividades relacionadas en el plan de acción de acuerdo al Plan Nacional del CONPES 3854 de 2016.

10. DIRECTRICES DEL MANUAL DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN.

El manual de políticas de seguridad de la información debe ser revisado al menos una vez al año o cuando surjan cambios relevantes de mejora y de cumplimiento al Sistema de Gestión de Seguridad de la Información.

La documentación a la que hace llamado cada una de las políticas relacionadas en este manual, hacen parte de la caracterización del proceso de Administración y Mantenimiento de Bienes y de su operación, tales como:

- IMCY - Seguimiento PTRSPI.
- IMCY - Seguimiento MAPA DE RIESGOS.

- IMCY - Seguimiento PETI.

11. ADMINISTRACIÓN DE TECNOLOGÍAS E INFORMACIÓN MANUAL POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

- IMCY - Licencias de Software
- IMCY - Seguimiento controles MSPI-MGRSD
- IMCY - Catalogo Sistemas de Información
- IMCY - Catalogo Servicios TI
- IMCY - Activos de Información
- Procedimiento Derechos Propiedad Intelectual.

12. RESPONSABLES.

La implementación de la Política de la Seguridad Digital repercute en todo el personal del IMCY (funcionarios, contratistas, proveedores, colaboradores, terceros, entre otros) que tenga acceso a la información de la entidad y cumplir las políticas establecidas en este manual.

12.1. Roles y responsables.

El Líder de Sistemas de Información, debe asumir la responsabilidad en el desarrollo e implementación del SGSI, debe velar por el cumplimiento de las políticas de Seguridad Digital y de la Información, debe orientar a todo el personal que tenga acceso a la información de la Entidad, debe coordinar actividades de gestión de riesgos de seguridad y ciberseguridad, debe apoyar la identificación de controles y debe poner en contexto al Comité Institucional de Gestión y Desempeño, de toda la Gestión del Sistema de Seguridad de la Información.

El Comité Institucional de Gestión y Desempeño.

Este comité asumiera el rol recomendado por la norma ISO 27001:2022, denominado Comité de Seguridad de la información.

Es responsable de revisar y aprobar las políticas de Seguridad de la Información y Ciberseguridad, revisar los lineamientos definidos por Seguridad de la Información; revisar la implementación del SGSI en Entidad; realizar el seguimiento a la gestión de Seguridad de la Información y Ciberseguridad; apoyar la implementación de los lineamientos en la Entidad en temas de Seguridad de la Información y Ciberseguridad; promover la sensibilización y comunicación al interior de la Entidad del Sistema de Gestión de Seguridad de Información.

La Alta Dirección, es el ente máximo jerárquico y se encuentra representado, es responsable de revisar y aprobar la política de Seguridad de la Información y Ciberseguridad; revisar la eficacia de la implementación de la política de Seguridad; proporcionar y avalar los recursos necesarios para el desarrollo e implementación de iniciativas de Seguridad; comunicar la importancia de una gestión eficaz de la Seguridad de la Información y Ciberseguridad; promover el cumplimiento de las políticas y normas definidas en el SGSI, todo esto lo puede hacer a través del comité de gestión y desempeño.

La Oficina de Tecnologías de Información.

Lidera y apoya la implementación y gestión de los controles de ciberseguridad que afecten sistemas de información, aplicaciones, plataformas de apoyo o infraestructura de comunicaciones y seguridad que se encuentre bajo administración la oficina, es responsable de definir políticas, procedimientos de gestión de accesos lógicos y esquema, metodología de construcción de roles y perfiles para los accesos a plataformas e

infraestructura de la Entidad; definir procedimientos de gestión; definir líneas base, guías de aseguramiento, etc. para aseguramiento de los sistemas; definir la estrategia de respaldo de información; definir políticas y procedimientos de gestión de cambios; definir el diseño de red y plataformas tecnológicas teniendo en cuenta las necesidades de la Entidad Implementación de planes de remediación de vulnerabilidades; adquirir e implementar tecnologías de seguridad; adquirir, implementar y configurar la red y las plataformas tecnológicas de acuerdo con el diseño propuesto y realizar los ajustes/mejoras necesarias en el proceso de desarrollo de software.

13. POLÍTICA DE ORGANIZACIÓN INTERNA.

Establecer un marco de referencia de gestión para iniciar y controlar la implementación de la seguridad digital al interior de la entidad por medio de la definición de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con las autoridades y grupos de interés y la incorporación de la seguridad digital en la gestión de los proyectos, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información definido desde el Alto Gobierno, buscando preservar la confidencialidad, integridad y disponibilidad de la información.

Con el objetivo: Definir y asignar las responsabilidades a los colaboradores en el IMCY para todo el ciclo de vida de las políticas de seguridad de la información, con la finalidad de proteger los activos y poder llevar a cabo los procesos y procedimientos específicos de seguridad.

13.1. Organización De La Seguridad Digital Información Lineamientos plan de toma de conciencia del SGSI.

Crear e implementar dentro del plan de Seguridad Digital acciones para la toma de conciencia que el Sistema de Gestión de Seguridad de la Información va dirigido a todo el personal del IMCY. El cual debe incluir actividades de sensibilización, capacitación, y comunicación de la seguridad de la información, con el fin de promover el cumplimiento de las políticas, roles y responsabilidades de seguridad de la información.

Los siguientes lineamientos de la Política de Seguridad Digital del IMCY tiene como referente lo propuesto por el Gobierno Nacional a través de las diferentes normas y guias y permite brindar de forma detallada actividades para alcanzar los objetivos de esta.

Lineamientos para la Oficina de Tecnologías e Información.

a. Fortalecer las capacidades de monitoreo para la operación remota, con el fin de detectar accesos indebidos o situaciones anormales.
b. Contar con las capacidades y disponibilidad de los servicios de VPN4 (Red Privada Virtual), seguridad en los servicios de correo electrónico y el acceso a la información de la Entidad, realizando un análisis de riesgos.
c. Fortalecer el monitoreo en el uso de los datos personales e información confidencial.

d. Realizar oportunamente copias de seguridad de los datos a través del medio que se tenga a disposición.

e. Contemplar herramientas para la gestión remota en la Entidad.

f. Verificar el uso de software licenciado, de tal forma que la entidad quede eximida de responsabilidades por el no licenciamiento de software en las estaciones de trabajo de los funcionarios.

g. Determinar requisitos de seguridad sobre el firewall y de protección contra software malicioso.

h. El correo electrónico personal no debe utilizarse para ningún proceso de la entidad.

13.2. Contacto con las autoridades.

El IMCY debe mantener contacto actualizado con las autoridades competentes para el cumplimiento de la Ley; como los organismos de control (Procuraduría General de la Nación, Contraloría General de la República, Fiscalía General de la Nación), Fuerzas Militares (Policía Nacional, Comando Conjunto Cibernético). La Oficina de Control Interno del IMCY, actualizar y publicar el listado de autoridades a contactar en caso de que se sospeche de la violación de la Ley (Normograma), para mantener contacto con organismos de control y autoridades; los funcionarios y contratistas pueden consultar el marco legal aplicable en el Normograma del ente territorial.

13.3. Contactos con grupos de interés.

El IMCY, a través de la Oficina de Tecnología e Información debe mantener contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior con el fin de estar al día con la información relacionada con la seguridad de la información, retroalimentando comunicados de actualizaciones de software, notificaciones de ataques de vulnerabilidad día cero, avisos de ciberataques o ataques cibernéticos, reporte de vulnerabilidades y nuevas amenazas.

13.4. POLÍTICA DE ACTIVOS DE INFORMACIÓN

El líder de proceso es quien tiene la responsabilidad de establecer la valoración de los activos, clasificación y respectivo etiquetado teniendo en cuenta el modelo de clasificación de la información ene l IMCY, igualmente definir el nivel de protección requerido ante accesos no autorizados, pérdida de la confidencialidad, integridad o disponibilidad; realizar el respectivo etiquetado de la información teniendo en cuenta la clasificación definida; mantener actualizada la matriz de activos de información definida por el lider de la administración y mantenimiento de bienes de la institución, validando los controles de acceso asignado a los activos; Identificar riesgos asociados con la Seguridad de la Información en los procesos de los cuales son responsables o tienen participación; reportar oportunamente eventos o incidentes de Seguridad de la Información. Identificar los activos de información del IMCY, para definir las responsabilidades de protección apropiadas y clasificarlas para asegurar que la información de la entidad recibe un nivel apropiado de protección, de acuerdo con su importancia, y se efectúe un manejo adecuado de los medios para evitar la divulgación, modificación, el retiro o la destrucción no autorizada de la información de la entidad contenida en ellos.

Además del Procedimiento relacionado en la Política Seguridad De Activos De Información se debe realizar la gestión de los mismos, garantizando su identificación, inventario, clasificación, uso y manejo, preservación, etiquetado e implementación de las medidas de protección y seguridad tenientes para cada tipo de información de conformidad con sus condiciones y características.

13.4.1. Gestión De Activos.

Los sistemas de información y la misma información digital están sujetos a amenazas graves desde el ciberespacio pueden llegar a comprometer la Confidencialidad, Integridad y Disponibilidad de la información procesada, almacenada y transmitida. Es así como, se deben proporcionar niveles de protección a todos los activos de información de la Entidad.

13.4.2. Inventario de activos.

El líder de sistemas debe ser responsable de mantener actualizado el inventario de activos de seguridad de la información con el acompañamiento del líder de la gestión de mantenimiento y administración de bienes del IMCY, de acuerdo con la política contable en su ítem para el manejo de activos. Se deben identificar y registrar la información en el Formato previsto para tal fin incluye: archivos físicos, sistemas, servicios, y los equipos (ej. estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfono, entre otros) propiedad del IMCY,

todos los funcionarios y contratistas deben identificar la información, y darle un manejo adecuado según su clasificación, siguiendo las directrices.

Los funcionarios, contratistas, proveedores o terceros y, todo aquel que cuente con acceso a la información de la entidad debe reportar los eventos de seguridad de la información identificados, de acuerdo con el Procedimiento de Gestión de Incidentes.

14. DISPOSITIVOS MÓVILES.

Los dispositivos móviles corporativos (teléfonos inteligentes, tablet, portátiles), son herramientas de trabajo que se deben utilizar únicamente para el desarrollo de actividades relacionadas con los procesos de la Entidad.

14.1. Política de Dispositivos Móviles Corporativos.

a. Conexión a redes de la entidad: Con el fin de minimizar los riesgos de seguridad de la información que implica el uso de dispositivos móviles la Oficina de Tecnología e Información debe controlar la conexión de dispositivos móviles tales como Smartphone, tablets y computadores personales de los contratistas a la red corporativa, a excepción de los dispositivos que sean propiedad del IMCY.

b. Software y protección: Las estaciones de trabajo y equipos portátiles que son propiedad del IMCY cuentan con software licenciado y protección contra código malicioso. Solo el personal de soporte de la OTI está autorizado a instalar software específico en los dispositivos móviles propiedad de la entidad.

Auditoría: El IMCY se reserva el derecho de revisar cuando se requiera el software instalado y utilizado en equipos de cómputo y servidores, además para los portátiles de los contratistas que se conecten a la red corporativa, se deben validar algunos aspectos de seguridad, entre éstos: antimalware activo y actualizado, sistema operativo actualizado, no permitir que se conecte a internet desde la red de los funcionarios, etc.

c. Registro de equipos: El grupo encargado de inventarios debe mantener un registro de los dispositivos móviles asignados (qué dispositivo y a quién se le asigna).

d. Mantenimiento de dispositivos: El mantenimiento de dispositivos que son propiedad de el IMCY queda restringido al área responsable de su mantenimiento. Por tanto, debe controlar que el usuario no haga cambios en el hardware, instale software o modifique la configuración del equipo sin autorización de la OTI.

e. Almacenamiento de la información: La información de la entidad que no sea estrictamente necesaria para el desarrollo de las tareas del usuario no debe almacenarse en el dispositivo. Si se accede a la información desde varios dispositivos, esta tiene que estar sincronizada para evitar duplicidades y errores en las versiones. Los funcionarios autorizados por su respectivo jefe deben solicitar a la OTI o Coordinación TIC la creación de los almacenamientos de datos para el intercambio de información al interior de la Entidad.

f. Conexión a redes: Todas las conexiones de redes ajenas a la Entidad, deben seguir los lineamientos establecidos en la sección en este manual denominado Acceso a Redes y a Servicios en Red.

g. Notificación en caso de infección: Si un funcionario o contratista sospecha la infección por virus u otro software malicioso, se debe notificar a la mayor brevedad posible al personal de soporte de la OTI.

Transporte y custodia: El computador de la entidad, no debe quedar expuesto a altas temperaturas que puedan dañar sus componentes. El usuario debe impedir que se pueda acceder a la información almacenada en el mismo. En ningún caso se debe descuidar el portátil, celular o tablet si viaja en transporte público. También debe estar protegidos físicamente contra robo, especialmente cuando se dejan en automóviles y otras formas de transporte, habitaciones de hotel, centros de conferencias y lugares de reuniones. En caso de robo o pérdida del equipo se debe notificar de manera inmediata al personal pertinente.

Los dispositivos que contienen información sensible o crítica para entidad, no se deben dejar sin supervisión, y donde sea posible, deben estar protegidos bajo llave para asegurarlos, adicionalmente, los computadores portátiles que salgan de la entidad y, de surgir un robo a éste, se debe comunicar inmediatamente a la líder del proceso de mantenimiento y administración de bienes, para seguir los pasos de reporte del incidente y comunicarlo a los entes tales como Policía Nacional, la Fiscalía, etc. La información sensible o crítica para el IMCY no se debe reposar o ser almacenada en los equipos personales de los contratistas.

h. Uso del puesto de trabajo: El usuario debe aplicar las buenas prácticas de uso del puesto de trabajo que sean relativas al uso de un equipo móvil (obligación de notificar incidentes de seguridad, uso correcto de las contraseñas, bloqueo del equipo, entre otras).

i. Responsabilidades: El usuario es el responsable del equipo portátil o móvil que se le ha facilitado para el desempeño de sus tareas fuera de las instalaciones de la entidad. Por tanto, es el funcionario el que debe garantizar la seguridad tanto del equipo como de la información que contiene. Esta normativa es de obligatorio cumplimiento y debe ser objeto a los acuerdos que se firmen al aceptar el uso de estos dispositivos.

j. Viajes de trabajo: Los funcionarios que viajan por asuntos de la Entidad son responsables de la seguridad de la información propiedad de la Entidad.

a. Acceso a contratistas: El contratista que utilice equipos de cómputo de su propiedad para el desarrollo del objeto del contrato debe:

- Tener y usar solo software legal instalado en su equipo.
- Contar con software antivirus licenciado.
- Adjuntar a los técnicos de soporte de la Mesa de Ayuda, el listado del software que va a utilizar y evidencia de las licencias correspondientes (tanto para el sistema operativo como para las aplicaciones), se debe entregar al supervisor del contrato con copia a la OTI.

b. Información en dispositivos propios: Los contratistas que tienen información corporativa en sus dispositivos móviles personales son responsables de la seguridad de la información en su poder.

c. Almacenamiento de información: En lo posible se debe evitar almacenar información de la entidad en los dispositivos móviles personales.

15. POLÍTICA PARA TELETRABAJO Y TRABAJO REMOTO.

El IMCY no tiene modalidad de teletrabajo, pero cuenta con trabajo remoto. Sin embargo, en adelante tendrá en cuenta los lineamientos en estas modalidades:

a. Garantizar que los equipos de trabajo en caso de ser suministrados a los teletrabajadores tengan los medios de protección adecuados para la tarea a realizar.

b. Informar y dar una copia al Teletrabajador de la política de la empresa en materia de seguridad digital, y así asegurar la confidencialidad, la integridad y la disponibilidad de la información de la entidad contenida en estos.

c. Evitar acceder a redes Wifi-públicas, es importante que como funcionario trabaje en redes de conexiones a internet seguras y protegidas con contraseña.

d. Asegurar la comunicación a través de herramientas seguras de mensajes de texto, de modo que, si los sistemas de información no funcionan y el correo electrónico no se encuentra disponible no se pierda la comunicación.

e. Cumplir con las políticas definidas por la entidad respecto al uso de equipos, aplicaciones y programas informáticos, protección de datos personales, propiedad intelectual y seguridad de la información, que se encuentren señaladas en la Ley.

f. Utilizar los datos de carácter personal, privado o sensible a los que tenga acceso, única y exclusivamente, para cumplir con las funciones propias, así como, garantizar que ningún tercero tenga acceso por cualquier medio a los datos de carácter personal, privado o sensible de la Entidad.

g. Informar a la Oficina de Tecnologías de la Información o coordinación TIC, según la ruta establecida, sobre conflictos de red o problemas tecnológicos o del equipo que requieran ser solucionados para el cumplimiento de las funciones.

h. El Teletrabajador se compromete a guardar la máxima reserva y confidencialidad sobre las actividades laborales que desarrolle. Se considera información confidencial la información de propiedad de la entidad y la información que genere el Teletrabajador en virtud de su vinculación laboral.

i. En general, cumplir con todas las obligaciones establecidas en el artículo 22 del Decreto 1295 de 1994.

16. INICIO DE EJECUCIÓN DEL CONTRATO.

El cumplimiento de las Políticas de Seguridad de la Información por parte de todos los funcionarios, contratistas, proveedor o terceros o cualquier persona que tenga una relación contractual o situacional con la Entidad, o que tengan acceso a los activos de información del IMCY debe ser informado en el momento que inicie sus actividades contractuales, desde Talento Humano para los funcionarios de planta y para los demás colaboradores de la Entidad, desde el supervisor del contrato, con apoyo del Oficial de Seguridad de la Información, además:

a. Todo funcionario, contratista, proveedor o tercero que desde su gestión o alcance del contrato requiera del acceso a un sistema de información ejemplo, (Trámites en Línea, etc.) o a la red corporativa de el IMCY, debe hacer la solicitud a través del formato y, éste debe estar autorizado por el líder del grupo o supervisor del contrato.

b. La solicitud debe especificar claramente los permisos que el funcionario, contratista, proveedor o tercero, requiere para sus actividades y acceso a los sistemas de información u otro componente tecnológico, especificando los privilegios a ser asignados en el sistema de información.

c. Desde la Oficina de Tecnología e Información se debe notificar el alcance dado desde la firma del contrato, con el fin de que el funcionario, contratista, proveedor o tercero, sea notificado y de inicio a sus labores o actividades contractuales.

16.1. Durante la Ejecución del empleo de funcionario o contratista.

Todos los funcionarios o contratistas al firmar el contrato deben ponerse de acuerdo para el tema de confidencialidad y no divulgación de información, antes de tener acceso a las instalaciones de procesamiento de información. Para los contratistas se maneja el contrato de prestación de servicios de apoyo a la gestión, además:
Los dueños de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades y derechos legales con relación a leyes sobre derecho de autor o legislación sobre protección de datos personales.

a. Los líderes de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades para la clasificación de la información y la gestión de activos institucionales asociados con información, instalaciones de procesamiento de información y servicios de información que deben ser manejados por el funcionario o contratista.

b. Los líderes de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades del funcionario o contratista para el manejo de la información recibida de otras Entidades o partes externas.

c. Gestión de Talento Humano y el equipo de Contratación deben asegurar que los funcionarios y contratistas respectivamente conozcan y acepten la política de seguridad digital – información.

c. Para los contratistas dentro del contrato se establecen responsabilidades de seguridad de la información y existe cláusula de confidencialidad.

e. El Grupo de Gestión de Talento Humano debe establecer los mecanismos para asegurar que los funcionarios asistan a las charlas de sensibilización en seguridad de la información brindadas por la oficina de tecnologías. Se debe tener en cuenta el manejo de datos personales, clasificación de la información, solicitud de recursos tecnológicos, incidentes de seguridad de la información y puntos de información para asesoría sobre seguridad de la información.

f. Gestión de Talento Humano o el Supervisor del Contrato para los contratistas y/o terceros, deben comunicar a la Oficina de Tecnología e Información (OTI) los cambios de cargo de personal, indicando los cambios en los recursos tecnológicos asignados. Especialmente actualizaciones sobre los accesos a carpetas compartidas y sistemas de información.

16.2. Terminación o cambio de responsabilidades de empleo.

Se debe informar al personal los deberes y responsabilidades después de la terminación del empleo. Previa emisión de paz y salvo para funcionario o contratista se debe considerar:

a. Tener formato de paz y salvo firmado por la OTI, el cual asegura que se retiraron los accesos lógicos y físicos de acuerdo con el procedimiento de control de acceso.

b. Tener formato de paz y salvo igualmente firmado por jefe inmediato o coordinador de grupo donde se aseguró de la transferencia apropiada de información al sucesor del cargo e informe de gestión que indica el estado de las actividades realizadas (en desarrollo, finalizadas o pendientes) y la aceptación del jefe inmediato o coordinador del grupo.

16.3. Intercambio de información.

Procesos Disciplinarios en atención a los requisitos de la norma NTC-ISO/IEC 27001:2022, la Ley 734 de 2002 (Código Único Disciplinario), y demás legislación aplicable con relación a los procesos disciplinarios, el IMCY de debe firmar acuerdos de confidencialidad o compromisos de confidencialidad con los servidores públicos, intercambio de información entre Entidades Públicas u otros Entes Externos, y debe incluir una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información restringida o confidencial. Cada una de las partes debe firmar antes de permitir el acceso o uso de dicha información, teniendo presente los siguientes lineamientos:

a. El intercambio de información con organismos de control y autoridades de supervisión debe seguir el Procedimiento Intercambio Seguro de Información con los que se intercambie todo tipo de información.

b. Cuando se realicen acuerdos entre organizaciones para el intercambio de información física o digital, se debe especificar el grado de sensibilidad de la información de la entidad según procedimiento de Gestión de Activos y las consideraciones de seguridad sobre la misma, así como, los controles a implementar.

c. Es importante gestionar la firma de un acuerdo de intercambio de información por parte de los representantes legales de las partes involucradas.

d. Mantener la seguridad de la información transferida dentro de la entidad y cualquier entidad externa mediante el uso del correo electrónico, con un procedimiento seguro.

17. USO DE EQUIPOS DE CÓMPUTO DE PROPIEDAD DEL INSTITUTO MUNICIPAL DE CULTURA DE YUMBO.

a. Está prohibido que personal ajeno a la Oficina de Tecnología e Información destape o retire partes de los equipos de cómputo.

b. La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad del proceso de Tecnología e Información y, por tanto, se debe solicitar soporte a la Oficina de Tecnología e Información para la realización de estas labores.

c. Los equipos de cómputo no deben ser trasladados del sitio asignado inicialmente, ni cambiar el funcionario al que le fue asignado, sin previo aviso a la Oficina de Tecnología e Información.

d. Debe respetarse y no modificarse la configuración de hardware y software establecido por la Oficina de Tecnología e Información.

e. No se autoriza el uso de medios extraíbles para almacenamiento de información institucional (USB, Celulares, Memory Card etc.) en las estaciones de trabajo de la Entidad, con excepción para aquellos funcionarios que, por sus funciones y actividades propias institucionales, sean autorizados por el Gerente, mediante formato o comunicación debidamente diligenciado.

f. Toda actividad informática (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) no autorizada que afecte tanto las redes corporativas como los sistemas de información de la entidad, están prohibidas dando lugar a los procesos disciplinarios y/o legales correspondientes.

g. Durante la permanencia en las instalaciones de la entidad, los equipos de cómputo externos deben estar conectados únicamente a la red de datos corporativos configurada por el proceso de Administración de Tecnología e Información.

h. Todas las estaciones de trabajo deben apagarse o hibernarse al finalizar la jornada laboral.

Los equipos de cómputo (CPU y monitor), servidores, teléfonos IP y equipos de comunicaciones, debe conectarse a los puntos de corriente eléctrica identificados como regulados, con el fin de evitar picos alto que puedan dañar el componente tecnológico. Estos puntos de corriente regulada se usan para regular la energía y algunos soportados igualmente por las UPS en dado caso que se vaya la luz y no se apaguen abruptamente.

La entidad no se responsabiliza por daños que puedan sufrir los dispositivos de cualquier tipo y de carácter personal que se conecten dentro de la institución.

i. La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones de la entidad y que no son propiedad de la Entidad, es responsabilidad única y exclusiva de sus propietarios.

18. USO DE INTERNET

a. No se autoriza conectar módems, celulares u otros dispositivos que permitan acceso a Internet dentro de las redes WAN, LAN, WLAN, PAN o mediante conexiones Ad-Hoc, Hotspots o VPN no autorizadas dentro de la Entidad.

b. No se autoriza a los funcionarios y contratistas acceder a cualquier página o dirección que contenga material pornográfico en cualquiera de sus variantes, o bien páginas que promuevan cualquier tipo de ideas que puedan ser consideradas ofensivas para las normas de la Entidad como violencia, terrorismo, grupos al margen de la Ley, discriminación, entre otras.

c. No se autoriza el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal o institucional.

d. Con el propósito de minimizar la probabilidad de saturación, interrupción, alteraciones no autorizadas y errores en la red del IMCY, no se permite el envío o descarga de información masiva como música, videos y software no autorizado.

e. Todo usuario es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta de acceso.

f. Todas las actividades realizadas en los sistemas de información de la entidad deben ser monitoreadas con el fin de preservar la seguridad informática de la Entidad.

g. Ningún usuario está autorizado para asignar claves de administrador sobre los computadores de la Entidad. Esto es competencia de la Oficina de Tecnología e Información o quien haga sus veces.

h. Los usuarios no deben intentar burlar los sistemas de seguridad y de control de acceso; acciones de esta naturaleza se consideran violatorias de las políticas de la Entidad.

19. USO DEL CORREO INSTITUCIONAL

Se prohíbe enviar o reenviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y/o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

a. La Entidad debe proveer a los usuarios un correo electrónico institucional con el dominio @imcy.gov.co.

b. La cuenta de correo electrónico institucional es personal e intransferible, los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y el buzón asociado a la Entidad.

c. El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de la Entidad; esto es para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo desempeñadas.

d. El correo electrónico institucional es una herramienta para el intercambio de información necesaria que permita el cumplimiento de las funciones propias de cada cargo, no es una herramienta de difusión masiva de información y no debe ser utilizada como servicio personal de mensajes o cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, programas piratas, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso.

e. Cuando se reciban correos desde una cuenta de divulgación masiva, evite dar una respuesta utilizando la opción responder a todos.

f. El servidor de correo debe bloquear archivos adjuntos o información nociva como archivos EXE o de ejecución de comandos.

g. Bajo ningún motivo se debe abrir o ejecutar un correo de origen desconocido, debido a que podría tener código malicioso (virus, troyanos, keyloggers, gusanos, etc.), lo cual podría atentar contra los sistemas, programas y datos de la Entidad.

h. No está permitido abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario como si fuera propia, sin embargo, es responsabilidad de cada usuario mantener sus sesiones atendidas, entiéndase no dejar los equipos sin cerrar sesión al alcance de cualquier intruso.

i. El usuario debe notificar cualquier recibo de correo sospechoso, el correo sospechoso no debe ser abierto ni reenviado a ningún usuario.

20. CLASIFICACIÓN DE LA INFORMACIÓN.

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2022, la Ley 1712 de 2014 y sus decretos reglamentarios y la Ley 1581 de 2012 de protección de datos personales la

entidad clasifica, etiqueta y maneja la información y sus activos asociados de acuerdo con el Procedimiento de Gestión de Activos, además:

a. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse de que el activo está inventariado lo mismo que los programas y demás software.

b. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse de que los activos están clasificados y protegidos apropiadamente.

c. El funcionario, contratista, proveedor y/o tercero responsable del activo de información, debe definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables.

d. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse del manejo apropiado del activo cuando es eliminado o destruido.

20.1. Gestión de Medios Removibles.

Los medios removibles (cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB) en los que se almacene información clasificada como información pública clasificada e información pública reservada deben estar cifrados, de acuerdo con las directrices del procedimiento de gestión de activos (tabla controles según clasificación de información). La Oficina de Tecnología e Información debe establecer herramientas tecnológicas para el cifrado de la información, además:

a. La OTI debe proveer el uso de carpetas compartidas en lugar de medios removibles para el intercambio de información al interior de la Entidad.

d. Se debe hacer seguimiento a la transferencia de información de los medios removibles mediante herramientas tecnológicas que permita realizar la trazabilidad de la información transmitida a estos medios.

e. a través del formato de salidas de equipos de la Gestión de Administración y mantenimiento de Bienes de debe controlar el ingreso y salida de los equipos de cómputo y otros.

f. Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la Entidad se debe remover y formatear el dispositivo.

g. Los medios removibles no deben ser utilizados en sitios públicos como un café internet, así mismo, debe tratarse bajo cuidado alejado de daños externos como agua, polvo o fuego.

20.1. Disposición de los Medios.

a. Los medios que contienen información confidencial se deben disponer en forma segura, mediante incineración, destrucción o el borrado de datos antes de ser reutilizados o dados de baja.

b. La información en las cintas de backups que contienen información pública clasificada o información pública reservada se debe cifrar, además deben estar protegidas en un lugar seguro y bajo llave, el lugar que disponga la OTI.

c. La información almacenada en medios removibles debe ser transferida a medios nuevos antes de que se vuelvan ilegibles, de acuerdo con el tiempo de vida útil de los mismos.

d. Se debe guardar varias copias de datos valiosos para el IMCY en medios separados, con el fin de evitar la pérdida de información por daño, pérdida o robo de los medios removibles.

21. CONTROL DE ACCESO

21.1. Acceso a Redes y Servicios en Red.

a. El acceso a redes Wi-Fi se controla con autenticación por contraseña utilizando el protocolo WPA2-PSK.

La Oficina de Tecnología e Información provee un servicio de conectividad a todos los funcionarios y contratistas de la Entidad para la navegación en internet, dicho acceso es controlado por usuario mediante la autorización.

b. Para los usuarios que requieran contar con servicios de páginas de encuentro o descargas, deben ser autorizados por el jefe inmediato, mediante formato IMAC dirigido a la Oficina de Tecnología de la Información, justificando la necesidad del acceso.

c. La conexión a servicios en red se controla mediante el directorio activo, a excepción del control de acceso físico y el servicio de impresión.

d. La conexión a redes públicas abiertas está prohibida, así como la conexión a redes Wi-Fi públicas.

d. Todo acceso o privilegio a sistemas, redes, aplicaciones o información de la entidad debe estar aprobado por los líderes de las áreas y los propietarios de información según aplique.

h. El acceso a la red Wi-Fi para los visitantes, estudiantes y comunidad en general, el IMCY tiene dispuesto una red, de no conocer este acceso de esta se debe solicitar al administrador del punto de para su debida activación.

i. Es responsabilidad del Coordinador del proceso definir los lineamientos a seguir para garantizar accesos seguros y confiables a los sistemas y plataformas de la entidad.

21.2. Solicitud o Inicio de Acceso.

Los procedimientos definidos por la entidad para administrar los privilegios de acceso de los usuarios a la información de la entidad deben comprender la asignación, la modificación y la revocación de los permisos. Todos los sistemas, recursos y aplicaciones, que procesen cualquier información propietaria deben requerir autenticación y debe tener en cuenta por lo menos, que:

a. Ningún colaborador autorizado puede realizar solicitudes de acceso para sí mismo, excepto la alta dirección.

c. El gerente o líder de proceso debe realizar las solicitudes de acceso a los sistemas de información requeridos por los funcionarios o colaboradores a su cargo en las herramientas establecidas por la entidad para tal fin, para lo que debe tener en cuenta la importancia de su acceso.

d. La confirmación de la gestión del requerimiento y el envío de los datos de autenticación deben ser enviados usando un canal seguro. Esta entrega debe estar controlada por un proceso de administración formal que permita, informar a los usuarios sobre el compromiso de cumplir con los lineamientos de seguridad establecidos para el buen uso de los datos de acceso (usuarios / contraseña) otorgados.

e. El re-uso de nombres de cuentas no está permitido, aun cuando la cuenta de usuario ya se encuentre eliminada/inactiva. Para lo cual la OTI debe aplicar el procedimiento definido para la creación de cuentas de usuario y correo electrónico.

f. Asignar identificaciones únicas a todos los funcionarios y colaboradores, es decir, que no deben existir cuentas genéricas para el acceso o gestión sobre los sistemas tecnológicos de la Entidad (equipos, aplicaciones, bases de datos, sistemas operativos, entre otros). Cuando por razones del negocio u operación deben ser creadas únicamente como cuentas de servicio y no deben ser utilizadas por ningún funcionario o contratista. En el Directorio Activo se debe detallar el responsable de cada cuenta.

g. La asignación y utilización de los derechos de accesos privilegiados se debe restringir y controlar, es decir el uso de las claves de usuarios administradoras, tales como: “root”, “adm”, “Administrator”, “system”, y otras cuentas privilegiadas, entre otros, debe ser controlado por la OTI quienes son los responsables de dichos accesos, de esta gestión existirá un registro que permita identificar la trazabilidad es decir conocer el funcionario o colaborador que está haciendo uso de estos accesos.

h. Todo usuario del sistema debe tener un mecanismo de autenticación privado.

k. En caso de ser necesario se debe utilizar métodos de autenticación fuerte como sensores biométricos, huellas dactilares o “tokens” de hardware.

l. El acceso de un usuario debe ser limitado sólo a la información requerida para el desarrollo de sus funciones.

m. Para los equipos de cómputo se debe establecer bloqueos o terminación de sesiones automáticas en caso de que queden desatendidos, con el propósito de proteger la información.

La utilización de información compartida por ejemplo unidades de red debe estar restringida mediante controles ejecutados por la OTI. El responsable y/o dueño de la información debe definir los accesos a la información únicamente al personal autorizado.

n. Todos los usuarios creados en ambiente de producción de los sistemas de información o servicio de la entidad deben ser solicitados según el procedimiento establecido en el formato, con el fin de mantener un registro formal o la trazabilidad de los privilegios otorgados a los colaboradores autorizados para cumplir con las labores asignadas, utilizando algún servicio tecnológico.

o. Los accesos a la información o sistemas de información no deben otorgarse por los administradores de Base de Datos y de Aplicaciones del servicio hasta que se hayan completado los procedimientos de autorización.

p. Se debe considerar la inclusión en los contratos del personal y contratos de servicio con terceros, cláusulas que especifiquen las sanciones si los colaboradores o terceros intentan un acceso no autorizado.

21.3. Suspensión o Terminación de Acceso.

El acceso a los sistemas debe ser suspendido para todo funcionario o colaborador del IMCY que se encuentre en licencia, permisos, vacaciones, entre otras novedades; si por necesidad se requiere mantener habilitado, únicamente para cargos a nivel de Gerencia o Líderes de procesos, Coordinación o Secretaria, para los demás cargos si existen funciones que se deban reasignar para dar continuidad durante dichas novedades, el Gerente o Lideres deben realizar las solicitudes de acceso necesarias a los colaboradores que ejecutaran las actividades, una vez cumplido el plazo se debe solicitar retiro de los permisos, además:

a. La OTI debe mantener actualizado el Directorio Activo con la información de los usuarios de funcionarios y colaboradores, de acuerdo a formato solicitado para la gestión de los usuarios de la entidad; en la cual debe registrarse las novedades de estos para que se realice la suspensión o eliminación según corresponda.

d. La OTI debe disponer de mecanismos documentados para desactivar el acceso a los usuarios, en las siguientes, situaciones:

- Desvinculación por parte de los funcionarios al IMCY.

- Ausencias temporales de los colaboradores por motivo de vacaciones, viajes o licencias.

- Los funcionarios de la Entidad que no han accedido a los recursos tecnológicos por un período de tiempo determinado (entre 3 meses y 6 meses).

- Número de intentos fallidos durante el ingreso de la contraseña a un recurso tecnológico o aplicativo o cuando se presente algún tipo de incidente de seguridad de la información sobre el código de usuario.

- Cuando el responsable de la información lo solicite.

21.3. Revisión o Validación de Accesos.

El líder de Tecnologías de la Información debe revisar o monitorear en intervalos de tiempo regulares los privilegios asignados a los usuarios, para asegurar que no tengan accesos no autorizados; teniendo en cuenta los siguientes aspectos:

a. Validar solicitudes de accesos especiales como USB y VPN, administrador de máquina y acceso remoto.

21.4. Identificación de los Usuarios.

Todos los usuarios deben tener un identificador único (ID de usuario) para uso personal y se debe seleccionar una técnica de autenticación adecuada para garantizar la identidad del usuario. Este control se aplica a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de redes, proveedores, programadores de sistemas y administradores de bases de datos etc.).

21.5. Normas para la Creación de Contraseñas seguras.

Los usuarios y contraseñas son de uso personal e intransferible, cualquier utilización indebida y/o irregularidad debe ser responsabilidad del colaborador. Como medida de seguridad los usuarios deben crear y administrar sus contraseñas siguiendo las siguientes normas para la creación y el uso:

a. Las contraseñas se consideran como información confidencial y deben ser protegidas como tal.

b. La contraseña debe tener al menos ocho (8) caracteres, donde se tengan letras en mayúscula, minúscula y números o caracteres especiales.

c. Las contraseñas deben cambiarse mínimo cada 60 días y no se pueden repetir las últimas 10 contraseñas.

d. No utilizar contraseñas por defecto, éstas se deben cambiar una vez se adquieran componentes tecnológicos nuevos o sistemas de información que perfectamente las puedan incluir.

g. No es permitido compartir usuarios, contraseñas y cualquier mecanismo de autenticación asignado (ej. Tokens- fichas seguras de seguridad de datos).

h. Dispositivos como los Tokens que permitan el acceso a un sistema de información en la Entidad o Entidades externas deben ser almacenados y salvaguardados en lugares seguros, donde solamente el dueño del Token tenga acceso.

i. En los casos que se sospeche del compromiso de una contraseña en un posible incidente de seguridad, ésta debe ser cambiada inmediatamente por el administrador de la aplicación y debe reportarse al Oficial de Seguridad de la Información.

j. Los usuarios deben tener presente no incluir las claves en ningún proceso de registro automatizado; por ejemplo, almacenado en una macro o sistema de información.

21.6. Segregación de Funciones

La segregación de funciones en el IMCY, representa una actividad de control clave para separar las responsabilidades de las diversas actividades que intervienen en la ejecución de los procesos, una adecuada segregación de funciones permite mantener la confidencialidad, integridad y disponibilidad de la información:

a. La segregación de funciones permite reducir el riesgo de un mal uso accidental o deliberado del sistema, razón por la cual se debe definir lineamientos para evitar accesos no autorizados que permitan, modificar o utilizar los activos sin autorización o detección.

b. La segregación de funciones en cada uno de los procesos de la Entidad, debe garantizar como mínimo la independencia de las siguientes actividades:

- Operación de equipos de cómputo
- Administración de red
- Administración de sistemas Operativos
- Administración de Bases de datos
- Administración de aplicaciones (Administradores Funcionales)
- Administración de seguridad informática Teniendo en cuenta lo anterior los líderes de cada proceso, tienen la responsabilidad de generar las respectivas matrices de Segregación de Funciones las cuales deben ser validadas periódicamente.

22. ACCESO A DATOS DE PRODUCCIÓN.

El jefe de la OTI debe tener en cuenta las siguientes consideraciones respecto al acceso a datos de producción:

a. Se debe definir un procedimiento para el control de acceso el cual incluya la aprobación, supervisión etc. a los datos de producción.

b. Para todo usuario autorizado, la disponibilidad de la información debe ser limitada.

c. Los procedimientos deben ser definidos para conceder el acceso de emergencia de usuarios a datos de producción.

d. El acceso a datos de producción debe ser auditable. El acceso a los datos de producción debe generar archivos de trazabilidad (logs) que pueden ser auditados, por entes de control.

23. CONEXIONES REMOTAS.

Se define como acceso remoto cualquier conexión establecida desde fuera de la Entidad que requiere acceso a la red o aplicaciones internas del IMCY por parte de funcionarios, proveedores entre otros. Para dichos accesos se debe tener en cuenta las siguientes consideraciones:

a. Iniciar la conexión remota de red desde computadores y sitios seguros, evitar conexiones remotas desde computadores públicos o desconocidos como, cafés internet, aeropuertos, hoteles o redes inalámbricas públicas.

b. Las conexiones remotas a los recursos de la plataforma tecnológica; deben estar restringidas, únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

c. La autenticación para los accesos remotos debe complementarse con doble factor de autenticación y/o a través de la plataforma de seguridad.

d. Si es el caso se debe aprobar o aceptar del lado de la Entidad para que el proveedor tome el control remoto. No debe permitirse el acceso y control total de manera automática, sino cuando la entidad lo autorice y monitorear las actividades realizadas por estos proveedores.

e. El trabajo remoto por VPN lo debe solicitar el líder del proceso, conforme al procedimiento definido. la OTI valida la pertinencia de dicha solicitud y otorga el privilegio, evaluando y aplicando las medidas de protección adecuadas que garanticen una conexión segura.

f. El acceso remoto a los servidores debe estar controlado, es decir quién puede o no ingresar por este servicio, teniendo presente que este servicio debe ser autorizado únicamente para los administradores de los servidores, los usuarios o proveedores fuera de la oficina no deben tener estos accesos o llamado a este servicio.

g. Las aplicaciones críticas de la entidad deben forzar la autenticación mediante el protocolo del personal experto.

23. EL USO DE FIRMA DIGITAL.

Es seguro por el hecho de usar mecanismos y algoritmos de cifrado bastantes robustos. Sin embargo, la seguridad puede ser comprometida si el funcionario que hace uso de la firma digital no toma las medidas necesarias para proteger la clave.

a. El único funcionario autorizado para hacer uso de la Firma Digital es el gerente.

b. La firma digital se utilizará para cumplir con las normativas legales, para identificar al firmante de manera inequívoca, para certificar la integridad del documento o cuando se requiera proteger un documento o la información (autenticidad e integridad) con un riesgo asociado resultado de una evaluación de riesgos.

e. La firma digital, debe ser verificada a través de una llave pública incluida en un certificado válido emitido por una Entidad certificadora, a la cual, se le debe exigir acuerdos de niveles de servicio para el servicio de certificación o verificación.

f. Se debe realizar mantenimiento anual a todas las firmas digitales, así como las API correspondientes.

g. Una vez firmados los documentos con la firma digital, debe conservarse en su estado electrónico para garantizar su validez.

h. Una vez firmados digitalmente los documentos, se deben convertir en formato PDF y debe visualizarse a través del sistema de Gestión Documental.

i. Los artículos 20 y 21 de la Ley 527 de 1999 únicamente rigen los efectos relacionados con el acuse de recibo. Las consecuencias jurídicas del mensaje de datos se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.

j. Los certificados digitales, firmas digitales, llaves de cifrado de la información, son de uso personal e intransferible.

k. Los funcionarios autorizados para el uso de firma digital en el IMCY, antes de firmar un documento que tiene otras firmas digitales, debe asegurarse de que estas firmas previas no han sido alteradas.

l. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

- Es única a la persona que la usa.
- Es susceptible de ser verificada.
- Está bajo el control exclusivo de la persona que la usa.
- Está ligada a la información o mensaje de datos, de tal manera que, si éstos son cambiados, la firma digital es invalidada.

a. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional. El uso de firma digital y según la Ley 527 de 1999 establece a su favor tres atributos fundamentales en el aseguramiento jurídico, por lo que es necesario que los funcionarios autorizados para

el uso de la firma digital velen por que estos tres atributos se cumplan en su implementación y uso.

b. La autenticidad: En la medida que se puede verificar en un mensaje de datos firmado digitalmente quién es su autor, es quién se compromete jurídicamente.

c. La integridad: El destinario de ese mensaje de datos podrá verificar si la información ha sido o no alterada en el proceso de comunicación electrónica, lo que es muy útil para determinar la originalidad electrónica del mensaje de datos, especialmente a la luz de los artículos 8 y 9 de la Ley 527 de 1999.

d. El no repudio: Quien firma digitalmente se compromete con la suscripción respectiva y posteriormente no le es dado retractarse o refutar dicho acto.

24. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO.

Ante una falla en el suministro de energía, un enlace de red redundante y un sistema de monitoreo de las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) la Entidad debe cumplir con la normatividad de cableado estructurado y estár debidamente certificado. A sí mismo el IMCY debe exigir a los proveedores de servicios informáticos, cumplir con las políticas de seguridad de la entidad. Mantenimiento de Equipos. La Oficina de Tecnología e Información debe establecer y ejecutar planes anuales de mantenimiento de la infraestructura.

• En caso de pérdida o robo de un equipo tecnológico o dispositivos de almacenamiento de información de la entidad, se debe poner la denuncia ante la autoridad competente e informar inmediatamente al líder del proceso de Gestión de Administración y Mantenimiento de Bienes, para que se inicie el trámite interno correspondiente. Disposición Segura o Reutilización de Equipos Cuando una estación de trabajo o equipo portátil vaya a ser reasignado o dado de baja, se debe realizar una copia de respaldo de la información de la entidad que allí se encuentre almacenada (en caso de ser necesario). Posteriormente, el equipo debe ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobre escritura de los medios que contienen información) con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma. Ver indicaciones adicionales en el procedimiento de borrado seguro.

25. POLÍTICA DE EQUIPO DESATENDIDO, ESCRITORIO LIMPIO Y PANTALLA LIMPIA.

Todos los colaboradores del IMCY deben conservar su escritorio libre de información propiedad de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento, cada vez que se vayan a retirar de sus puestos de trabajo se deben contemplar los siguientes lineamientos:

a. Al imprimir documentos de carácter confidencial (información pública clasificada e información pública reservada), estos deben ser enviados con confidencialidad, indicando el grado previsión y retirados de la impresora inmediatamente.

b. Los computadores deben cargar por defecto el fondo de pantalla de la entidad, éste no debe ser modificado y debe permanecer activo.

c. Los funcionarios y contratistas de la entidad deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo (aplique el comando de bloqueo oprimiendo simultáneamente las teclas Windows+L), a su vez, la Oficina de Tecnología e Información debe implementar mecanismos para cierres de sesión automáticos no superior a cinco minutos.

d. Los usuarios son responsables y asumen las consecuencias por la pérdida de información que este bajo su custodia. Se prohíbe el almacenamiento de información personal en lo computadores del IMCY. El escritorio lógico (del computador) debe estar libre de información pública clasificada e información pública reservada.

e. La información de gestión del área deber ser almacenada por los usuarios en carpetas compartidas del área y la información de gestión del usuario en el almacenamiento virtual de One Drive corporativo de Office

26. SEGURIDAD DE LAS OPERACIONES.

Los cambios en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información se deben realizar de acuerdo con los lineamientos del Procedimiento de Gestión de Cambios Tecnológicos. a. Gestión de Capacidad entidad debe gestionar la capacidad de su plataforma tecnológica (hardware y software) de acuerdo con las indicaciones del Procedimiento de Gestión de Capacidad. b. Separación de los Ambientes la entidad debe contar con ambientes de desarrollo, pruebas y producción separados por máquinas físicas y máquinas virtuales. C. El IMCY debe controlar el acceso al ambiente de pruebas de la misma forma que controla el acceso al ambiente de producción.

27. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS.

a. Se deben proteger las estaciones de trabajo, equipos portátiles y servidores del IMCY contra códigos maliciosos.

b. Los contratistas que hagan uso de sus equipos portátiles personales deben contar con un software antivirus licenciado.

c. El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos conectados a la red deben tener el antivirus instalado y activo.

d. El único servicio de antivirus autorizado en la entidad es el asignado directamente por la Oficina de Tecnología e Información (OTI), el cual cumple con todos los requisitos técnicos y de seguridad. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura.

e. El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados por virus o códigos maliciosos o sean sospechosos de estar infectados.

f. El usuario no debe instalar o emplear programas no autorizados para manejo de antivirus.

g. Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa de antivirus y que han sido establecidos por la Oficina de Tecnología e Información.

h. El programa de antivirus debe ser instalado única y exclusivamente por la Oficina de Tecnología e Información en los servidores y estaciones de trabajo.

28. COPIAS DE RESPALDO.

El IMCY debe realizar copias de respaldo de la información y pruebas periódicas a las mismas. Para ello la Oficina de Tecnología e Información, define el Procedimiento de Copias de Respaldo e Instructivo, que definen las actividades para la estrategia de backup requeridas; además:

a. La Oficina de Tecnología e Información debe establecer las políticas de copias de seguridad desde la herramienta de backups, para los sistemas de información y bases de datos.

Todos los administradores de base de datos, aplicaciones y servicios deben cumplir con las políticas de backup establecidas por la Oficina de Tecnología e Información.

b. La Oficina de Tecnología e información debe realizar copias de respaldo a las carpetas compartidas definidas en el servidor de archivos de la entidad.

c. La Oficina de Tecnología e Información debe realizar copias de respaldo a las carpetas con información de la entidad de los equipos portátiles y/o computadores de escritorio críticos de cada uno de los grupos (funcionarios VIP).

d. Todas las copias de respaldo deben ser almacenadas en un área adecuada y con control de acceso, y aplicar los controles para la protección de los medios de respaldo.

e. Todas las copias de respaldo deben contemplar un plan de continuidad del negocio, orientado a evitar la pérdida de la información al contemplar un sitio secundario para su preservación.

f. Las copias de respaldo deben ser guardadas únicamente con el objetivo de restaurar el sistema cuando por situaciones como: borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o computadores o por requerimientos legales sea necesario recuperarla.

g. Toda la información institucional que se almacena en los equipos asignados a los funcionarios o contratistas es de propiedad de la Entidad, motivo por el cual no debe ser divulgada a terceros, salvo autorización expresa de la entidad.

29. CONTROL DE SOFTWARE OPERACIONAL.

Instalación de Software en Sistemas Operativos. El proceso de instalación y desinstalación de software está autorizado exclusivamente al personal de la OTI, Por lo tanto, a los funcionarios o contratistas no le es permitido realizar esta labor, en excepción los funcionarios autorizados expresamente. Para la instalación de software se debe seguir las siguientes directrices:

- El software licenciado debe contar con su respectiva documentación (Licencia) y en el caso del software libre debe estar permitido el uso comercial.

- El instalador debe ser descargado de la página oficial del fabricante.

- Debe dejarse evidencia documentada de que las directrices anteriores fueron seguidas a cabalidad. Se debe proporcionar capacitación adecuada a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de las nuevas adquisiciones de software o mejoras al software existente, antes de su puesta en producción. Todo el software nuevo y mejorado debe estar completamente soportados por una documentación suficientemente amplia y actualizada, y no debe ser puesto en el ambiente de producción sin contar con la debida documentación.

- Documento de Licencia del Software (representa el permiso que le da el fabricante para la instalación y uso de su producto)

- Manual de Instalación del Software (Para determinar que el software ha sido instalado apropiadamente)

Manual del Usuario para uso del Software (Para guiar al usuario en su uso y apropiación). La OTI debe realizar revisiones periódicas del uso del software instalado en las estaciones de trabajo y servidores de la Entidad, con el fin de validar el cumplimiento de la Ley 603 de 2000 de Derechos de Autor, conjuntamente debe identificar los activos de información que se encuentran afectados por derechos de propiedad intelectual. Todo software que viole los acuerdos de licenciamiento debe ser desinstalado inmediatamente y debe ser reportado el hecho como incidente de seguridad por incumplimiento de la política y de los términos y condiciones de uso, poniendo en riesgo la seguridad de la información y quizás sanciones económicas por incumplimiento a la Ley 603 de 2000 de derechos de autor para la cual se implementa MANUAL POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Para contar con una trazabilidad del software instalado en los componentes tecnológicos de la entidad, (sistemas operativos, programas ofimáticos, sistemas de información), entre otros, se debe contar con un sistema de control de la configuración, en donde se observen los cambios ejecutados en dicho software, como (instalación de parches, cambios de versiona miento, actualizaciones, etc.), con el fin de mantener el historial y el control del software operacional en el IMCY. Toda reproducción del software, transporte, almacenamiento, adquisición para la venta o distribución sin la debida autorización del titular, se constituye como un delito a los Derechos Patrimoniales del Autor.

Todo software que la entidad adquiera debe ser del conocimiento de Arquitectura Empresarial quien a su vez debe emitir criterios adicionales con el fin de que el software a adquirir cuente con la interoperabilidad en su instalación y uso con los demás sistemas de información de la Entidad. La OTI debe comunicar a los funcionarios y contratistas sobre

las consecuencias por utilizar software ilegal; conjuntamente con la Oficina Jurídica debe definir y establecer las cláusulas de los contratos para cumplir con la legislación vigente relacionada con los derechos de autor y datos personales.

Es importante que la Oficina Jurídica haga parte de esta adquisición en cuanto a la lectura que se haga a la licencia, derechos de autor y propiedad intelectual del software adquirido y que será propiedad de la entidad. Para llevar el Control del Software Operacional instalado en la entidad, se han establecido los siguientes procedimientos:

- Procedimiento de Derechos de Propiedad Intelectual
- Formato Dar de Baja un Software

30. GESTIÓN DE LA VULNERABILIDAD TÉCNICA.

La Oficina de Tecnología e Información, es responsable de verificar de manera periódica la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la Entidad. Adicionalmente, debe contar con el mapa de riesgos que permita la identificación y mitigación de las vulnerabilidades identificadas en toda la plataforma tecnológica de la entidad.

30.1. Gestión de las Vulnerabilidades Técnicas.

a. Se debe generar y ejecutar por lo menos una vez al año el plan de análisis de vulnerabilidades y/o Hacking Ético para las plataformas críticas que maneja la Entidad, cuya viabilidad técnica y de administración lo permita.

b. Una vez se lleve a cabo la ejecución de escaneos de vulnerabilidad en la plataforma tecnológica de la Entidad, la identificación de estas vulnerabilidades o hallazgos se deben remediar de acuerdo con los lineamientos establecidos desde el mapa de riesgos.

c. Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad de La Oficina de Tecnología e Información.

31. POLÍTICA AUDITORÍAS DE SISTEMAS DE INFORMACIÓN.

Controles sobre auditorio de sistemas de información para la ejecución de auditorías a los sistemas de información se debe tener en cuenta las siguientes consideraciones:

a. Los requisitos de auditoría para acceso a sistemas y a datos se deberían acordar con los líderes de proceso de la(s) Dependencia(s) involucradas.

b. El alcance de las pruebas técnicas de auditoría se debería acordar y controlar.

c. Las pruebas de auditoría (incluidas las pruebas de análisis de vulnerabilidades y/o hacking ético) que puedan afectar la disponibilidad del sistema se debe realizar en horario laboral en un ambiente controlado.

d. Se debe hacer seguimiento de todos los accesos y logs para producir un rastro de referencia. Las pruebas de auditoría se deben limitar a acceso a software y datos únicamente para lectura.

32. POLITICA SEGURIDAD EN LAS COMUNICACIONES.

La Oficina de Tecnología e Información debe definir e implementar los mecanismos de control que considere apropiados para proteger la Confidencialidad, Integridad y Disponibilidad de la información en las redes definidas en la Entidad, la disponibilidad de los servicios en red y la seguridad en sí de la información que viajan a través de estos canales de redes de comunicaciones.

a. Proteger la información transferida al interior y exterior del IMCY.

b. La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, realiza el control del uso de sistemas de transferencia de archivos vía FTP (Protocolo de Transferencia de Archivos) a internos.

c. Los documentos generados o cargados al Sistema de Gestión Documental deben incorporar condiciones de seguridad mediante la utilización del formato PDF.

Establecer estrategias de preservación digital para garantizar que la información almacenada pueda permanecer en el futuro, pese a los cambios tecnológicos u otras causas que puedan interferir en la entidad.

32.1. Gestión de la Seguridad en las Redes.

La Oficina de Tecnología e Información debe definir e implementar mecanismos de separación de las redes de la entidad con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de computador de escritorio, dominio de servidor), por dependencias (por ejemplo, oficina de talento humano, oficina de gestión financiera, oficina de tecnología e información) o alguna combinación (por ejemplo, un dominio de servidor que se conecta a múltiples dependencias), además:

a. La Oficina de Tecnología e Información debe mantener separadas la red de datos y la red de voz, con el fin de minimizar el impacto de interceptación de alguna de las dos redes.

b. El acceso remoto a las redes de la entidad se controla mediante conexiones VPN, las cuales deben estar monitoreadas para que se evidencie la desactivación de ésta en el tiempo que se ha definido. La transferencia de Información debe firmar acuerdos o compromisos de confidencialidad con los servidores públicos y debe incluir una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información restringida o confidencial. En este acuerdo deben quedar especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se debe firmar antes de permitir el acceso o uso de dicha información. Todos los lineamientos para la transferencia de información deben aplicarse en toda la Entidad, proveedores y terceros que dentro de sus funciones se establezca la necesidad de intercambio de información física como digital. Cuando haya la necesidad de contar con el formato de intercambio de información entre Entidades, el cual deber ser firmado por los representantes de las partes cuando se lleve a cabo esta transferencia de información, además tener en cuenta:

a. Cuando se realicen acuerdos entre organizaciones para el intercambio de información física o digital, se debe especificar la clasificación de la información y las consideraciones de seguridad sobre la misma, así como, los lineamientos que se establecen en el Procedimiento de Intercambio Seguro de Información.

b. Todos los responsables de la información deben asegurar que el intercambio de información con el tercero (Contratos, convenios, pólizas, etc.), esté debidamente autorizada y protegida conforme a los lineamientos del procedimiento Intercambio Seguro de Información.

c. Todos los responsables de la información son quienes autoricen la transferencia de la información que esté bajo su responsabilidad, teniendo en cuenta la legislación (Ley 1581 de 2014 y Ley de Habeas Data de 2008).

d. Todos los responsables de la información deben seguir las indicaciones del Procedimiento de Gestión de Activos de Información, para la transferencia y transporte de la información, teniendo presente que esté totalmente etiquetada como se indica en este procedimiento.

e. La transferencia de información digital debe contemplar una trazabilidad de toda la actividad de envío de los datos, a través de blogs, en donde se registre la siguiente información:

32.1.1. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

La Oficina de Tecnología e Información debe definir los requisitos de seguridad de la información para sistemas de información nuevos o mejoras a los sistemas de información existentes, contratados externamente o desarrollados en el IMCY. Las dependencias que contraten el desarrollo de software o adquieran software de terceros, deben apoyarse en la Oficina de Tecnología e Información para definir los requisitos de seguridad de la información. Para ello, debe tener en cuenta los lineamientos establecidos en el Manual de Adquisición, Desarrollo y Mantenimiento de Sistemas de información, además los siguientes:

32.1.1.1. Requisitos de Seguridad de los Sistemas de Información.

a. El nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario. Por ejemplo, la implementación de segundos factores de autenticación y un sistema de gestión de contraseñas que exija el uso de contraseñas fuertes, el cambio periódico de contraseñas y que guarde un historial de contraseñas para evitar su reutilización.

b. Los procesos de suministro de acceso y de autorización para usuarios, al igual que para usuarios privilegiados o técnicos. Por ejemplo, el suministro de datos de acceso por correo electrónico.

c. Las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad e integridad. Por ejemplo, cifrado de información almacenada, el envío de información por canales cifrados.

d. Los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso, seguimiento, y no repudio, formularios de autenticación mediante HTTPS, cifrado de contraseñas almacenadas.

e. Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.

f. La necesidad de exigir la implementación de metodologías de desarrollo seguro.

g. Los desarrolladores propios del IMCY liberan de derechos de autor cualquier desarrollo hecho para el cumplimiento de sus funciones u obligaciones contractuales. Seguridad en los Procesos de Desarrollo y Soporte La Oficina de Tecnología e Información debe definir e implementar principios de desarrollo seguro en actividades de construcción de sistemas de información internos. Los principios de desarrollo establecidos se deben revisar con regularidad (al menos anualmente) para asegurar que están contribuyendo a mejorar los estándares de seguridad dentro del proceso de construcción. También se debe revisar regularmente para que permanezcan actualizados en términos de combatir nuevas amenazas potenciales y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican. Los lineamientos para el desarrollo seguro deben aplicarse también para los sistemas de información existentes en la ANM y, a los de uso externo con los proveedores (Fábrica de desarrollo) además:

a. La entidad (OTI y supervisor del contrato); deben velar por el desarrollo tanto interno como externo de los sistemas de información, que estos cumplan con los requisitos de seguridad esperados, así como con pruebas de aceptación y seguridad al software desarrollado. Además, el IMCY debe asegurar que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la Entidad.

b. Los cambios en sistemas deben realizarse de acuerdo con el procedimiento determinado para tal fin.

En todo desarrollo interno, externo, se debe hacer uso de metodologías de desarrollo seguro, que contemplen lineamientos de seguridad en todas las etapas del desarrollo.

a. La Oficina de tecnología e Información debe aplicar los mismos controles en al ambiente de producción y ambiente de desarrollo, tales como, control de acceso, copias de respaldo, registro de eventos y separación de ambientes (desarrollo y producción).

b. La Oficina de Tecnología e Información debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y producción han sido aprobadas.

c. La Oficina de Tecnología e Información debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la entidad.

32.1.1.2. Desarrollo Contratado Externamente.

Cuando se contrata desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por el IMCY. Adicionalmente, se debe acordar la entrega de manuales técnicos, que describan la estructura interna del sistema, así como el diccionario de datos, librerías ejecutables, entidad relación de la base de datos, manuales funcionales, manual del usuario y manual de instalación, además:

a. Las dependencias deben asegurarse que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.

b. Las dependencias deben exigir el suministro de evidencia de que se realizaron pruebas de seguridad al software desarrollado por terceros.

c. Los principios de desarrollo seguro se deben aplicar, en donde sea pertinente, a desarrollos contratados externamente.

d. Las dependencias que contraten desarrollos externos deben asegurar que se realicen pruebas de aceptación del software, con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.

e. Las dependencias deben tener en cuenta e incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes aplicables.

f. Las dependencias deben incluir en acuerdos contractuales, en donde sea posible, el derecho de la entidad a realizar auditorías durante el desarrollo del contrato.

g. Pruebas de Seguridad de Sistemas Se debe exigir tanto para desarrollos internos como externos. La ejecución de pruebas funcionales que incluyan la evaluación de los requisitos de seguridad de la información y la protección contra vulnerabilidades conocidas.

Pruebas de Aceptación de Sistemas Independientemente de que sea un desarrollo interno o un desarrollo contratado externamente, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de desarrollo de sistemas seguros (en donde sea aplicable). En estas pruebas se puede hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y se debe verificar que se han corregido las brechas de seguridad, además:

a. Se debe realizar pruebas de aceptación del software que sea una persona diferente de quien han desarrollado el software, además estas pruebas evidenciadas a través de un documento deben estar firmadas por quienes realizaron las pruebas, en donde se acepte que el software desarrollado cumple con los lineamientos y funcionalidades para su uso.

b. De ser posible, las pruebas se deben llevar a cabo en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades al ambiente productivo de la entidad, y que las pruebas son confiables.

c. En donde la funcionalidad de la seguridad no satisface el requisito especificado, antes de comprar el software se debe reconsiderar el riesgo introducido y los controles asociados. Datos de Prueba La Oficina de Tecnología e Información debe certificar que la información entregada a los desarrolladores (tanto internos como externos) para sus pruebas debe ser enmascarada y los datos sensibles deben ser eliminados con el fin de no

revelar información confidencial de los ambientes de producción, dando cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública).

33. POLÍTICA RELACIÓN CON LOS PROVEEDORES.

33.1. Seguridad de la Información en las Relaciones con los Proveedores.

Debe establecer mecanismos de verificación de lineamientos de seguridad en sus relaciones con todos los proveedores, especialmente aquellos proveedores críticos para la entidad por el manejo de información crítica o confidencial, con el objetivo de asegurar la información a la que tengan acceso o servicios que sean provistos por los mismos, y que cumplan con las políticas de seguridad de la información, es fundamental que se llevan a cabo visitas a los proveedores con el fin de identificar situaciones que puedan comprometer la información de la entidad en el no cumplimiento de los lineamientos establecidos en esta política.

33.2. Tratamiento de la Seguridad dentro de los Acuerdos con Proveedores.

a. Los supervisores de contratos deben asegurar que se comuniquen las políticas y procedimientos de seguridad de la información a los proveedores y/o contratistas.

b. El Grupo de contratación debe incluir en los acuerdos con proveedores y/o contratistas, como mínimo, los siguientes requisitos de seguridad de la información:

- Cláusula de confidencialidad.
- Cláusula que defina las responsabilidades que continúan después de terminado el contrato (por ejemplo, confidencialidad durante 5 años después de terminado el contrato).
- Cumplimiento de las políticas de seguridad de la información del IMCY.
- Reporte de eventos de seguridad de la información a través de los canales definidos en el procedimiento de gestión de incidentes de seguridad de la información.
- Etiquetado y manejo de la información de acuerdo con las directrices del proceso.
- Cláusula de seguimiento y revisión de los servicios de los proveedores o terceros para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, en los acuerdos contractuales correspondientes.

c. Los supervisores de contratos deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad de la información establecidos con ellos y monitoreando la aparición de nuevos riesgos.

d. Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal a la Oficina de Administración de Tecnología e Información utilizando el formato respectivo.

34. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

La gestión de incidentes de seguridad debe estar basados de acuerdo con los lineamientos del proceso, donde se debe establecer como mínimo: quiénes deben reportar, los canales de comunicación, tipo de situaciones que se deben reportar, decisiones sobre las situaciones reportadas, respuesta a incidentes, aprendizaje de estos y recolección de evidencias digitales. Es deber de todo funcionario, contratista o colaborador informar el incumplimiento de los lineamientos descritos en este manual. Cualquier incumplimiento identificado debe remitirse al Oficial de Seguridad de la información, quien debe determinar si el evento se considera como incidente de seguridad de la información, teniendo en cuenta las categorías y criterios de clasificación. Categorías de incidentes de seguridad de la información: Si el incumplimiento es sujeto de clasificación teniendo en cuenta las siguientes categorías, se debe considerar como incidente de seguridad de la información:

a. Fuga de información: Se evidencia divulgación no autorizada de información de la entidad.

b. Acceso no autorizado:

- Se evidencia que una persona ingresa a un sistema de información sin credenciales de acceso.
- Se evidencia que una persona (interna o externa) tiene credenciales de acceso asignadas a otro usuario.
- Personal no autorizado ingresa a la información clasificada y reservada.

c. Ataque:

- Se evidencia intención de afectar un recurso específico.
- Se modifica la imagen institucional en aplicaciones de la entidad.
- No se cuenta con la disponibilidad de un sistema de información por ataques de denegación de servicio.
- Se evidencia caso de suplantación ya sea en correo electrónico o en páginas web.

d. Código dañino:

- El daño (modificación o indisponibilidad de la información) se manifiesta en memorias USB que alteran la información.
- El daño (modificación o indisponibilidad de la información) se manifiesta en un equipo y el vector de propagación fue por medio de USB contaminada o correo malicioso.

e. Denegación de servicio:

- El sistema de información no responde por alta cantidad de peticiones.
- El sistema de información se encuentra con latencia o degradación del servicio.

f. Robo o pérdida:

Se presenta robo o pérdida de equipos portátiles, cargadores, periféricos de entrada y salida.

- Se presenta robo o pérdida de elementos personales en las instalaciones del IMCY.

g. Alarmas de sistemas de monitoreo: Estos incidentes son reportados por dispositivos de seguridad según las reglas implementadas.

h. Usos inadecuados:

- Si se ingresa texto copiado de internet en documentación oficial de la entidad, sin registrar la fuente.
- Si se publica comunicados en nombre de la Entidad sin revisión y aprobación del proceso de comunicación estratégica.

35. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

a. El acceso a redes Wi-Fi se controla con autenticación por contraseña utilizando el protocolo WPA2-PSK.

La Oficina de Tecnología e Información provee un servicio de conectividad a todos los funcionarios y contratistas de la Entidad para la navegación en internet, dicho acceso es controlado por usuario mediante la autorización.

Al incurrir en el incumplimiento de estas políticas se debe notificar inmediatamente a la Oficina de Tecnología e Información a través de los siguientes canales.

- E-mail: comunicaciones@imcy.gov.co

- Mesa de Ayuda; está dirigida por el líder oficial a través de la herramienta de gestión que labora reportando el incidente de seguridad, dentro de lo posible con copia al líder de Sistemas de Información. Así mismo, se debe notificar situaciones tales como: personas ajenas al IMCY, correos maliciosos o sospechosos, reinicio de los equipos de cómputo o enrutadores, mala utilización de recursos, uso de software ilegal, divulgación, alteración y robo de información.

36. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DEL RIESGO.

La gestión del riesgo de Seguridad de la información y Ciberseguridad se encuentra alineada a la Metodología del Sistema Integral para la Administración y Gestión de Riesgos del IMCY de y a los lineamientos que desde la Norma ISO 31000:2018 - Sistema de Gestión de Riesgos se describen: La matriz de riesgos definida en la metodología de riesgos de seguridad incluye el análisis de los atributos generales de Seguridad de la Información y Ciberseguridad; (Confidencialidad, Integridad y Disponibilidad), es decir, se identifican y analizan para cada uno de los riesgos, estos pilares.

La Gestión del Riesgos para la Confidencialidad se define como riesgos que afectan este pilar, aquellos que describen que la Información puede ser conocida o utilizada sin autorización por cualquier colaborador, persona o ente dentro o fuera del IMCY.

37. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN.

Revisión de la Seguridad de la Información El proceso de Evaluación, Control y Mejora debe realizar auditorías internas de revisión mínimo una vez al año. Esta revisión independiente es necesaria para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque de la Entidad para gestionar la seguridad de la información. Esta revisión que es responsabilidad de Control Interno del IMCY Municipal debe incluir la valoración de las oportunidades de mejora y la necesidad de efectuar cambios en el enfoque hacia la seguridad, incluyendo la política y los objetivos de control.

38. CONTROL, SEGUIMIENTO Y MEJORA.

Se realizará el control y seguimiento con una periodicidad semestral, dejando los soportes correspondientes de acuerdo a lo establecido en la política de seguridad Digital, relacionando las acciones correctivas, preventivas o de mejora según los hallazgos identificados.

Elaboró:	Asesor de Control Interno	Héctor Fabio Gómez
Revisó:	Gestión Mejoramiento Institucional	Francia Elena Chanchi Hoyos
Aprobó:	Comité Institucional de Control Interno	Líder Gestión de Dirección y Planeación Líder Gestión Económica y Financiera Líder Gestión Administración y Mantenimiento de Bienes.