ALCALDIA MUNICIPAL DE PALMIRA
VALLE DEL CAUCA

POLITICAS DE SEGURIDAD DE LA INFORMACION

PALMIRA VALLE

2018

Proyecto: Ing. José Dennys Toro

TABLA DE CONTENIDO

Pág.

MANUAL DE POLITICAS Y ESTANDARES DE SEGURIDAD INFORMATICA

INTRODUCCIÓN

La información es un activo de gran valor para la Alcaldía Municipal de Palmira, por consiguiente debe ser debidamente protegido; garantizado, confiable al cual se deben de minimizar los riesgos de daño o perdida; Por lo tanto, lograr que los principios de Seguridad Informática sean efectivos en la entidad, hace necesario la implementación de Políticas de Seguridad de la Información que formen parte de la cultura organizacional y cumplan a cabalidad los estándares aplicables y requeridos para la administración integral de la misma.

La Oficina de Tecnologías Innovación y Ciencia, como agente de gestión y apoyo en materia tecnológica, formula un conjunto de reglas que definen lo que está permitido y lo que está prohibido, igualmente propone prácticas que implican el manifiesto compromiso de todas las personas vinculadas de una manera u otra a la entidad, es por ello, que la Administración Municipal se ha puesto a la tarea de implementar sus propias políticas de seguridad informática, basándose en las características establecidas en el Modelo de Política de Seguridad y privacidad de la Información propuesto por MinTIC.

Así pues, con la promulgación de la presente Política de Seguridad de la Información la Alcaldía Municipal de Palmira, formaliza su compromiso con el proceso de gestión responsable de la información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo come eje el cumplimiento de los objetivos misionales.

"Porque la seguridad informática depende más de las personas que de las maquinas"

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer y Cumplir todos los directivos, funcionarios contratistas y terceros que presten sus servicios o tengan algún tipo de Relación con el Departamento Administrativo de la Alcaldía de Palmira.

1.2. OBJETIVOS ESPECÍFICOS

La Seguridad de la Información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

- CONFIDENCIALIDAD: Los activos de la información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- INTEGRIDAD: El contenido de los activos de la información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- DISPONIBILIDAD: Contar con la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, es importante en sistemas informáticos cuyos compromiso con el usuario, es prestar servicio permanente.

2. ALCANCES Y LIMITACIONES

2.1 ALCANCES

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que Deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún

Tipo de relación con el Departamento Administrativo de la Presidencia de la República - DIRECCIÓN DE TECNOLOGÍA, INNOVACIÓN Y CIENCIA (TIYC), para el adecuado Cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y Seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad del presente manual. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por la Dirección General.

2.2 LIMITACIONES

Tener escritas las políticas de seguridad, no aplicar ni socializar se convertiría en una limitación; como también la falta de actualización acorde a las normas y necesidades o avances de las tecnologías de información.

3. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Las Políticas de Seguridad de la Información, surgen como una herramienta institucional para sensibilizar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el de la Dirección de Tecnología, Innovación y Ciencia (TIYC) sobre la importancia y sensibilidad de la información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.

Es relevante asegurar que los funcionarios, contratistas y demás colaboradores de la Dirección de Tecnología, Innovación y Ciencia (TIYC), entiendan sus responsabilidades y las funciones de sus roles y usuarios, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

3.1 IMPORTANCIA DE LA APLICABILIDAD DE POLITICAS DE SEGURIDAD.

Los usuarios responsables deben identificar los riesgos a los que está expuesta la Información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

Un activo de información es un elemento definible e identificable de gran relevancia que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como “Valiosa” para la Dirección de Tecnología, Innovación y Ciencia (TIYC); Independiente del tipo de activo, se deben considerar la importancia.

3.2 POLÍTICAS ESPECÍFICAS PARA USUARIOS INFORMÁTICA.

- El personal de Tecnología, Innovación y Ciencia no debe dar a conocer su clave de usuario a terceros sin previa autorización del Jefe del Área de Tecnología, Innovación y Ciencia.
- Los usuarios y claves de los administradores de sistemas y del personal del Área de Tecnología, Innovación y Ciencia son de uso personal e intransferible.
- El personal del Área de Tecnología, Innovación y Ciencia debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo al rol asignado.
- Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
- Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la entidad.
- Ej: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
- Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.
- Los funcionarios del Área de Tecnología, Innovación y Ciencia no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Jefe del Área de Tecnología y Sistemas.
- Los funcionarios del Área de Tecnología, Innovación y Ciencia se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones, en consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.
- Los funcionarios del Área de Tecnología, Innovación y Ciencia no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.
- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
- Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.
- La copia de programas o documentación, requiere tener la aprobación escrita Informática y del proveedor si éste lo exige.
- El personal del Área de Tecnología, Innovación y Ciencia debe velar por que se cumpla con el registro en la bitácora de acceso al datacenter, de las personas que ingresen y que hayan sido autorizadas previamente por la jefatura del área o por quien esta delegue.

- Por defecto deben ser bloqueados, todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por la entidad a través del Comité de Seguridad Informática.
- Aquellos servicios y actividades que no son esenciales para el normal funcionamiento de los sistemas de información, deben ser aprobados oficialmente por la entidad.
- Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.
- Las pruebas de software o piloto deben ser autorizadas por el Comité de Seguridad Informática y de Sistemas, estas deben ser realizadas sin conexión a la red LAN de la entidad y con una conexión separada de internet o en su defecto con una dirección IP diferente a las direcciones públicas de producción y en servidores de prueba.
- Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
- Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la entidad.
- Ej: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
- Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.
- Los funcionarios del Área de Tecnología, Innovación y Ciencia no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Jefe del Área de Tecnología y Sistemas.
- No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.
- El Área de Tecnología, Innovación y Ciencia será la única dependencia autorizada para realizar copia de seguridad del software original.
- Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.
- Los funcionarios del Área de Tecnología, Innovación y Ciencia se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones, en consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.
- Los funcionarios del Área de Tecnología, Innovación y Ciencia no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.

- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
- Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.
- La copia de programas o documentación, requiere tener la aprobación escrita Informática y del proveedor si éste lo exige.
- El personal del Área de Tecnología, Innovación y Ciencia debe velar por que se cumpla con el registro en la bitácora de acceso al datacenter, de las personas que ingresen y que hayan sido autorizadas previamente por la jefatura del área o por quien esta delegue.
- Por defecto deben ser bloqueados, todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por la entidad a través del Comité de Seguridad Informática.
- Aquellos servicios y actividades que no son esenciales para el normal funcionamiento de los sistemas de información, deben ser aprobados oficialmente por la entidad.
- Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.
- Las pruebas de software o piloto deben ser autorizadas por el Comité de Seguridad Informática y de Sistemas, estas deben ser realizadas sin conexión a la red LAN de la entidad y con una conexión separada de internet o en su defecto con una dirección IP diferente a las direcciones públicas de producción y en servidores de prueba. Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.
- Las pruebas de software o piloto deben ser autorizadas por el Comité de Seguridad Informática y de Sistemas, estas deben ser realizadas sin conexión a la red LAN de la entidad y con una conexión separada de internet o en su defecto con una dirección IP diferente a las direcciones públicas de producción y en servidores de prueba. Se deberá seguir la Política Editorial y Actualización de Contenidos Web, que permita auditar la publicación o modificación de información oficial en las páginas web.
- Las claves de acceso de los responsables de los contenidos de las páginas Web (web masters), son estrictamente confidenciales, personales e intransferibles
- La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como cinta, cartucho, CD, DVD, cloud, unidad de red.
- Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso adecuado.

- El Área de Tecnología, Innovación y Ciencia debe mantener un inventario actualizado de las copias de respaldo Bases de Datos e información y los aplicativos o sistemas Informáticos (siif web).
- Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro1 y posteriormente serán eliminados o destruidos de forma adecuada.
- Periódicamente, el Área de Tecnología, Innovación y Ciencia, efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considera como una violación a las Políticas de Seguridad de la Información Informática

3.3 VISION GENERAL LAS POLITICAS DE SEGURIDAD INFORMATICA

Estas políticas aplican en todas las dependencias de la Administración Municipal de Palmira y aplican a Directores, Secretarios, Jefes de Oficina, Jefes de Área, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la Dirección de Tecnología, Innovación y Ciencia (tiyc).

3.4 PROCEDIMIENTOS QUE APOYAN LA POLÍTICA DE SEGURIDAD

Los procedimientos son uno de los elementos dentro de la documentación del Manual de la Política de Seguridad para las Tecnologías de la Información y las comunicaciones. Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso, en él se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso.

También es recomendable el uso de instructivos para detallar aún más las tareas y acciones puntuales que se deben desarrollar dentro de un procedimiento, como son los instructivos de trabajo y de operación; los primeros para la ejecución de la tarea por la persona y los segundos para la manipulación o la operación de un equipo.

Los usuarios de Informática pueden consultar las descripciones detalladas de cada procedimiento a través del sistema integrado de gestión o en el Área de Tecnología, Innovación y Ciencia Informática.

3.5 PROCEDIMIENTO DE REVISIÓN DEL MANUAL DE LA POLÍTICA DE SEGURIDAD

El objetivo de este procedimiento es el de revisar, por parte de la dirección o su representante, el Manual de la Política para la Tecnología de Información y Comunicaciones - Tics del Departamento Administrativo de la Presidencia de la República en intervalos planificados, para asegurar su conveniencia, eficiencia y eficacia continúa.

4. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de que se tomen oportunamente las acciones correctivas.

4.1 PROCESO DISCIPLINARIO

Dentro de la estrategia de seguridad de la información Informática, está establecido un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y otros colaboradores Informática violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al Proceso de Talento Humano.

4.2 ACTUACIONES QUE CONLLEVAN A LA VIOLACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ESTABLECIDA POR LA DIRECCIÓN DE TECNOLOGÍA, INNOVACIÓN Y CIENCIA (TIYC)

- ✓ No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- ✓ No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- ✓ No actualizar la información de los activos de información a su cargo.
- ✓ Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para
- ✓ este fin. No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la
- ✓ jornada laboral, de documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada).
- ✓ No guardar la información digital, producto del procesamiento de la información perteneciente a la Dirección de Tecnología, Innovación y Ciencia (TIYC)
- ✓ Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos,
- ✓ obviando las medidas de seguridad.
- ✓ Dejar las gavetas abiertas o con las llaves puestas en los escritorios,
- ✓ Dejar los computadores encendidos en horas no laborables.

- ✓ Permitir que personas ajenas a la Dirección de Tecnología, Innovación y Ciencia (TIYC), deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
- ✓ Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad.
- ✓ Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- ✓ Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (exceptuando el penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
- ✓ Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- ✓ Recepcionar o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
- ✓ Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- ✓ Utilizar equipos electrónicos o tecnológicos desatendidos o que a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recepcionar y almacenar datos.
- ✓ Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el Área de Tecnología, Innovación y Ciencia Informática.
- ✓ Permitir el acceso de funcionarios a la red corporativa, sin la autorización del Área de Tecnología, Innovación y Ciencia Informática.
- ✓ Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos por Informática o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
- ✓ Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias Informática.
- ✓ No cumplir con las actividades designadas para la protección de los activos de información Informática.
- ✓ Destruir o desechar de forma incorrecta la documentación institucional.
- ✓ Descuidar documentación con información pública reservada o clasificada de la institución, sin las medidas apropiadas de seguridad que garanticen su protección.
- ✓ Registrar información pública reservada o clasificada, en pos-it, apuntes, agendas, libretas, etc. Sin el debido cuidado.
- ✓ Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca en la Dirección de Tecnología, Innovación y Ciencia (TIYC) o conectar computadores portátiles u otros sistemas eléctricos o electrónicos

personales a la red de datos de la Dirección de Tecnología, Innovación y Ciencia (TIYC), sin la debida autorización.

- ✓ Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
- ✓ Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos Informática para beneficio personal.
- ✓ El que sin autorización acceda en todo o parte del sistema informático o se mantenga dentro del mismo en contra de la voluntad Informática.
- ✓ El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos
- ✓ informáticos o las redes de telecomunicaciones Informática, sin estar autorizado.
- ✓ El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de
- ✓ información Informática.
- ✓ El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica Informática.
- ✓ El que viole datos personales de las bases de datos Informática.
- ✓ El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de
- ✓ autenticación y autorización establecidos por Informática.
- ✓ No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos
- ✓ los sistemas de información Informática o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- ✓ Permitir el acceso u otorgar privilegios de acceso a las redes de datos Informática a personas no Autorizadas.
- ✓ Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador Informática o de terceros.
- ✓ Ejecutar acciones tendientes a eludir o variar los controles establecidos por Informática.
- ✓ Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan
- ✓ Información institucional sin la autorización pertinente.
- ✓ Sustraer de las instalaciones Informática, documentos con información institucional calificada como
- ✓ Información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
- ✓ Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y Clasificada a personas o entidades no autorizadas.

- ✓ No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento Informática, Para traslado, reasignación o para disposición final.
- ✓ Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala Imagen Informática o de alguno de sus funcionarios.
- ✓ Realizar cambios no autorizados en la plataforma tecnológica la Dirección de Tecnología, Innovación y Ciencia (TIYC).
- ✓ Acceder, almacenar o distribuir pornografía infantil.
- ✓ Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles Institucionales, cuyo uso no esté autorizado por el Área de Tecnología, Innovación y Ciencia de la Dirección de Tecnología, Innovación y Ciencia (TIYC).
- ✓ Copiar sin autorización los programas Informática, o violar los derechos de autor o acuerdos de licenciamiento.

5. CUMPLIMIENTO

Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los funcionarios, contratistas y otros colaboradores Informática. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, Informática tomará las acciones disciplinarias y legales correspondientes.

El Manual de la Política de Seguridad para las Tecnologías de la Información y las Comunicaciones - TICs debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

5.1 CONTROLES

El Manual de la Política de Seguridad para las Tecnologías de la Información y las Comunicaciones Informática esta soportado en un conjunto de procedimientos que se encuentran documentados en archivos complementarios a este manual. Los usuarios de los servicios y recursos de tecnología Informática pueden consultar los procedimientos a través del Área de Tecnología, Innovación y Ciencia y del aplicativo del SIGEPRE.

6. DECLARACIÓN DE APLICABILIDAD.

La Declaración de Aplicabilidad (Statement of Applicability - SOA) referenciado en la cláusula 4.2.1j del estándar ISO 27001 es un documento que lista los objetivos y controles que se van a implementar en la Entidad, así como las justificaciones de aquellos controles que no van a ser implementados.

Para cada uno de los controles establecidos en los 11 dominios o temas relacionados con la gestión de la seguridad de la información que este estándar específico, y una vez se complete este análisis ya se puede realizar la declaración de aplicabilidad.

7. MARCO LEGAL

• Constitución Política de Colombia 1991.

• Código Penal Colombiano - Decreto 599 de 2000

• Ley 527 de 1999, por 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.

• Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.

• Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.

• Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.

• Ley 1581 de 2012, "Protección de Datos personales".

• Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011

• Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012

• Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”

8. RESPONSABLE DEL DOCUMENTO

Director de Tecnología, Innovación y Ciencia TIyC

9. PLAN DE CAPACITACIÓN PARA LAS POLITICAS DE SEGURIDAD INFORMATICA

- Contar con un plan de capacitación para el personal encargado de la implementación de de las políticas de seguridad
- Evaluar los resultados de evaluaciones y monitoreo a las políticas.
- Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.
- Evaluar los resultados de cada actividad.

BIOGRAFIA

https://www2.sgc.gov.co/AtencionAlCiudadano/Paginas/politica-seguridad-informatica.aspx

http://lospatios-nortedesantander.gov.co/Conectividad/InformesGEL/GT-D-05%20POLITICAS%20DE%20SEGURIDAD%20DE%20LA%20INFORMACION.pdf

https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

http://seguridadinformatica-ezequielgarcia.blogspot.com/2012/08/para-que-sirve-la-seguridad-informatica.html

Elaboro: Ing. Auditor de sistemas José Dennys Toro Pineda.

Directora TIyC: Ing. Maria Rosario Tasama Jiménez.