ESE CENTRO DE SALUD DE GALAPA
Progreso en Salud para Todos
Nit 802.007.798-1

POLITICA DE GOBIERNO DIGITAL

E.S.E.

CENTRO DE SALUD DE GALAPA

IVAN ESTRADA HERNANDEZ

GERENTE

2022

POLITICA DE SEGURIDAD DIGITAL

DR. IVAN ESTRADA HERNANDEZ
GERENTE

BELINDA BAENA ORTIZ
JEFE DE CONTROL INTERNO

CONTENIDO

INTRODUCCIÓN

En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, con la finalidad de orientar y dar los lineamientos respectivos a las entidades y se realicen en el país una gestión sistemática de riesgos de seguridad digital, promoviendo un entorno digital confiable y seguro, que maximice los beneficios económicos y sociales de todos los actores públicos y privados, impulsando la competitividad y productividad en todos los sectores de la economía.

Con la expedición del Decreto 1499 de 2017, se actualiza el Modelo Integrado de Planeación y Gestión – MIPG, con el propósito de consolidar, en un solo lugar, todos los elementos que se requieren para que una organización pública funcione de manera eficiente y transparente, y que esto se refleje en la gestión del día a día.

La Política de seguridad Digital es el resultado de un proceso de participación entre representantes del sector privado, del gobierno, la sociedad civil, la industria TI y la academia, además de las recomendaciones efectuadas por instancias internacionales como la Organización para la Cooperación y el Desarrollo Económicos - OCDE y de la Organización de Estados Americanos - OEA, las mesas de trabajo concertadas entre el Departamento Nacional de Planeación, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional y otras entidades relacionadas con la seguridad digital en Colombia.

En este contexto, la E.S.E. Centro de Salud de Galapa a través de su Política de Seguridad Digital busca promover un entorno digital seguro para el libre desarrollo de las actividades que todos desarrollamos, conscientes de los riesgos a los que estamos expuestos en el entorno digital y en consecuencia, adoptar buenas prácticas de comportamiento en este entorno, tales como las que se señalan en los programas de prevención para velar por su seguridad y proteger la información en el mundo digital.

1. OBJETIVO

1.1. OBJETIVO GENERAL

Adoptar la política de Seguridad Digital e identificar los riesgos a los que la E.S.E. Centro de Salud de Galapa se encuentra expuestos en el entorno digital y prepararse en el cómo protegerse, como prevenir y cómo reaccionar ante los delitos y ataques cibernéticos, fomentando una cultura en pro de crear consciencia de que el manejo del riesgo basa en principios fundamentales, con un fuerte enfoque hacia el ciudadano, buscando crear condiciones para que entre todos gestionemos el autocontrol del riesgo de seguridad digital en nuestras actividades digitales, fomentando la confianza en el entorno digital como medio para alcanzar nuestros objetivos.

1.2. OBJETIVOS ESPECÍFICOS

- Garantizar un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos de la E.S.E. Centro de Salud de Galapa.
- Sensibilizar los usuarios para que gestionen condiciones del riesgo de seguridad digital en sus actividades y se genere confianza en el uso del entorno digital.
- Fortalecer la seguridad de los usuarios en el entorno digital, con un enfoque de gestión de riesgos.
- Establecer normas de cuidado de equipos, periféricos y demás dispositivos físicos.
- Reglamentar y controlar la instalación de todo tipo de software, entre todos los funcionarios y contratistas de la E.S.E. Centro de Salud de Galapa.

2. ALCANCE Y CAMPO DE APLICACIÓN

Este documento aplica para la institucionalización, divulgación y apropiación de la Política de Seguridad Digital, la cual deben ser atendidas por todos los funcionarios y contratistas de las distintas dependencias, procesos institucionales y misionales en el Centro de Salud de Galapa ESE.

3. GLOSARIO

Para la implementación de la política es importante contemplar los siguientes términos que permitirá determinar tanto el vocabulario como las expresiones, con lo que, entre otras cosas, se conseguirá que los textos sean más coherentes y homogéneos y así evitará la posibilidad de encontrar terminología distinta en esta política:

- **Administración Remota:** Forma de administrar (manejar o controlar) equipos informáticos o servicios físicamente separados.
- **Accesibilidad:** facilidad con que la información estadística puede ser ubicada y obtenida por los usuarios. Contempla la forma en que ésta se provee, los medios de difusión, así como la disponibilidad de los metadatos y los servicios de apoyo para su consulta.
- **Amenaza:** Evento que puede desencadenar un incidente en la institución, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Análisis predictivo:** acción que implica proponer escenarios futuros a partir de la aplicación de diferentes métodos estadísticos de proyección, por ejemplo, de: tendencia, incremental, mínimos cuadrados, entre otros.
- **Análisis sistémico:** comprender el comportamiento de un sistema a través de la interacción de los elementos que lo componen.
- **Analítica de datos:** se refiere al manejo de datos con la intención de identificar patrones y/o tendencias que generen proyecciones para la toma de decisiones basada en evidencia.
- **Arquitectura empresarial:** es una práctica estratégica que consiste en analizar integralmente la entidad desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad. Una arquitectura se descompone en varias estructuras o dimensiones para facilitar su estudio. En el caso colombiano, se plantea la realización de la arquitectura misional o de negocio y la definición de la arquitectura de TI, cuya descomposición se hizo en seis dominios: Estrategia de TI, Gobierno de TI, Información, Sistemas de Información, Servicios Tecnológicos y Uso y Apropiación.
- **Ataque:** Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- **Autocontrol:** capacidad que deben desarrollar todos y cada uno de los servidores públicos de la organización, independientemente de su nivel jerárquico, para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos de manera oportuna para el adecuado cumplimiento de los resultados que se esperan en el ejercicio de su función, de tal manera que la ejecución de los procesos, actividades y/o tareas bajo su responsabilidad, se desarrollen con fundamento en los principios establecidos en la Constitución Política.
- **Autogestión:** capacidad de toda organización pública para interpretar, coordinar, aplicar y evaluar de manera efectiva, eficiente y eficaz la función administrativa que le ha sido asignada por la Constitución, la ley y sus reglamentos.
- **Barreras para la innovación:** factores internos o externos a la entidad que detienen o retrasan esfuerzos enfocados a la innovación
- **Bases de Datos:** conjunto de resultados y la documentación que los soportan, que se obtienen de las operaciones estadísticas y que describen o expresan características sobre un elemento, fenómeno u objeto de estudio

- **Calidad:** entendida como el impulso hacia la mejora permanente de la gestión, para satisfacer cabalmente las necesidades y expectativas de la ciudadanía con justicia, equidad, objetividad y eficiencia en el uso de los recursos públicos
- **Canal itinerante:** espacios adicionales que cada entidad puede crear por un período determinado de tiempo para poner a disposición de la ciudadanía, su oferta de trámites y servicios, como, por ejemplo, las ferias de servicios.
- **CD (Disco compacto):** Soporte digital óptico utilizado para almacenar cualquier tipo de información (audio, imágenes, vídeo, documentos y otros datos).
- **Código de Integridad:** herramienta diseñada por Función Pública en la cual se establecieron unos mínimos de integridad homogéneos como base para todos los servidores públicos del país, y para que las entidades promuevan sus propios procesos de socialización y apropiación en su cotidianidad, a través de la inclusión de principios de acción particulares sobre los 5 valores del Código General.
- **Comando:** Instrucción u orden que el usuario proporciona a un sistema informático, a través de una línea de texto basada en palabras clave.
- **Comité Institucional de Coordinación de Control Interno:** es el órgano asesor e instancia decisoria en los asuntos de control interno de una entidad pública (Decreto 1083 de 2017, artículo 2.2.21.1.5).
- **Comité Institucional de Gestión y Desempeño:** Encargado de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión – MIPG, el cual sustituye los demás comités que tengan relación con el Modelo y que no sean obligatorios por mandato legal (Decreto 1499 de 2017, art 2.2.22.3.8.)
- **Confidencialidad:** Proteger la información de su revelación no autorizada. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.
- **Control de Acceso:** Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria. Característica o técnica en un sistema de comunicaciones que permite o niega el uso de algunos componentes o algunas de sus funciones.
- **Direccionamiento Estratégico:** ejercicio emprendido por el equipo directivo de una entidad, en el que, a partir del propósito fundamental de la misma, las necesidades de sus grupos de valor, las prioridades de los planes de desarrollo (nacionales y territoriales) y su marco normativo, define los grandes desafíos y metas institucionales a lograr en el corto, mediano y largo plazo, así como las rutas de trabajo a emprender para hacer viable la consecución de dichos desafíos.
- **Dirección IP:** Es una etiqueta numérica que identifica, de manera lógica y jerárquica, una interface de conexión de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol).
- **DVD (Disco Versátil Digital):** Dispositivo de almacenamiento óptico en forma de disco, similar al CD, pero de mayor capacidad de almacenamiento (4.7 GB).
- **Equipo de Cómputo:** Dispositivo con la capacidad de aceptar y procesar información, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

- **Equipo de Telecomunicaciones:** Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.
- **Estabilizador:** Dispositivo para la toma de la tensión de la red eléctrica que alimenta al computador y a la red.
- **Filtro de contenidos web:** Herramienta informática que bloquea o permite el acceso a determinados sitios de internet.
- **FTP (File Transfer Protocol):** Protocolo y software que permite la transferencia de archivos entre máquinas conectadas a una red.
- **Hacking:** Acción de infiltrarse ilegalmente a sistemas informáticos y redes de telecomunicación con fines delictivos.
- **Hardware:** Partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.
- **HOAX:** (Engaño, mentira, patraña). Mensaje de e-mail con contenido falso o engañoso generalmente proveniente en forma de cadena.
- **Integridad:** Proteger la información de alteraciones no autorizadas por la institución. Internet: Red de redes de computadoras conectadas a nivel mundial, se emplea para el intercambio de información, el acceso a bases de datos, entre otros fines.
- **Intranet:** Red de computadoras privadas que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información, datos y sistemas operativos.
- **Keygen:** Programa informático, generalmente ilegal, que al ejecutarse genera un código para que un determinado programa software de pago en su versión de prueba pueda ofrecer los contenidos completos del mismo.
- **Mantenimiento:** Acciones que tienen como objetivo mantener un artículo o restaurarlo a un estado original.
- **Memoria USB:** Dispositivo de almacenamiento masivo que utiliza memoria flash para guardar la información que se puede requerir**.**
- **Módulo:** Parte de un programa de computador.
- **Periférico:** Dispositivos externos que se conectan al computador.
- **Red:** Conjunto de computadoras y elementos interconectados que permiten una comunicación entre sí y forman parte de un mismo ambiente.
- **Servicio:** Conjunto de aplicativos, programas informáticos o sitios web que apoyan la labor administrativa de la institución, sobre los procesos diarios que demanden información o comunicación en la misma.
- **Software:** Conjunto de componentes lógicos necesarios que hacen posible la realización de tareas específicas.
- **Software espía:** Controla el uso de la computadora sin el conocimiento o consentimiento del usuario, los software espía pueden grabar la secuencia de pulsación de teclas, el historial de navegación, contraseñas y cualquier otra información confidencial y privada, y enviar estos datos a un tercero vía Internet.

- **Soporte Técnico:** Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores o equipo de oficina dentro de la institución.
- **SPAM:** Mensajes no solicitados, no deseados o de remitente no conocido.
- **UPS (Uninterrupted Power System):** Sistema de Potencia Ininterrumpida, es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.
- **Usuario:** Cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional y tenga algún tipo de vinculación con la ESE Centro de Salud de Galapa.
- **Virus Informático:** Programa software que altera el normal funcionamiento del computador, sin el permiso o el conocimiento del usuario.
- **Vulnerabilidad:** Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

4. CONTENIDO

4.1. MARCO NORMATIVO

❖ *Ley 1928 de 2018*	*"Por medio de la cual se aprueba el «convenio sobre la Ciberdelincuencia». adoptado el 23 de noviembre de 2001, en Budapest."*
❖ *Ley 1712 de 2014*	*Por la cual se dictan disposiciones generales para la protección de datos personales..*
❖ Ley 1273 de 2009	*Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.*
❖ *Conpes 3854 de 2016*	Política Nacional de Confianza y Seguridad Digital
❖ *Decreto 1078 de 2015*	*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*
❖ *Decreto 103 de 2015*	***Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.***
❖ *Acuerdo 08 de 2019*	
❖ *Acuerdo 02 de 2018*	

4.2. ARTICULACIÓN DE LA POLÍTICA DE INTEGRIDAD CON LAS DIMENSIONES DEL MIPG,

De conformidad con el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades y el Decreto Nacional 1499 de 2017 (art. 2.2.22.3.2), el Modelo Integrado de Planeación y Gestión –MIPG- es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio. Este Modelo, constituye una apuesta del Estado colombiano por articular los anteriores sistemas de Gestión de Calidad y de Desarrollo Administrativo, con el Sistema de Control Interno, para consolidar en un solo lugar, todos los elementos que se requieren para que una organización pública funcione de manera eficiente y transparente.

El marco de referencia establecido por la Política de Seguridad Digital de MIPG, busca se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia.

De otro lado, en el Comité Institucional de Gestión y Desempeño se debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política.

5. POLITICA

Teniendo en cuenta los principios que orientan la gestión pública y los lineamientos del Sistema de Gestión Institucional:

La ESE Centro de Salud de Galapa está comprometida en establecer lineamientos de referencia de gestión para controlar la implementación de la seguridad digital a través de la asignación de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con las autoridades y los grupos de interés con la incorporación de la seguridad digital, lo anterior alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información, buscando preservar la confidencialidad, integridad y disponibilidad de la información..

La Política de Seguridad Digital se desarrollara con base en la aplicación de las siguientes politicas que son fundamentales para su implementacion y que le apuntan de manera transversal al desarrollo de la temática.

5.1. Política de Seguridad de Equipos.

La ley 734 de 2002 en su artículo 48, considera una falta gravísima lo siguiente: **“Artículo 48. Faltas gravísimas. Son faltas gravísimas las siguientes: Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera**

de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas."

Los equipos son la parte fundamental para el almacenamiento y gestión de la información. La función de la Oficina de Sistemas de Información o soporte Tecnológico es velar que los equipos funcionen adecuadamente y establecer medidas preventivas y correctivas en caso de robo, incendio, desastres naturales, fallas eléctricas y cualquier otro factor que atente contra la infraestructura informática. Comprende las siguientes políticas:

1. Todo equipo de cómputo, periférico o accesorio que esté o sea conectado a la Red de la ESE Centro de Salud de Galapa, sea propiedad o no de la institución debe de sujetarse a las normas y procedimientos de instalación establecidos por la oficina de Sistemas de Información o Soporte Tecnológico, de lo contrario no le será permitido conectar su equipo o dispositivo. Para los equipos que no sean propios de la ESE Centro de Salud de Galapa, se debe diligenciar un formato donde su propietario asuma la total responsabilidad sobre su equipo mientras esté conectado a la red eléctrica y de datos de la institución, ya que esta no se hace responsable de daños físicos o lógicos que puedan sufrir los equipos o periféricos de terceros.

2. La oficina de Sistemas de Información tendrá registro de todos los equipos que son propiedad de la ESE Centro de Salud de Galapa, Si se requiere hacer un traslado de computador, periférico o accesorio, debe contar con el consentimiento de la oficina de Sistemas de Información. Si el equipo necesita trasladarse en calidad de préstamo (periodos de horas o días), debe notificarse a la oficina de Sistemas de Información y diligenciar el formato correspondiente.

3. Cualquier equipo, periférico o accesorio de propiedad de la ESE Centro de Salud de Galapa que necesite ser retirado de la Institución tendrá que autorizarlo la Oficina de Sistemas de Información o Soporte Tecnológico.

4. Todo equipo de la Institución, debe estar ubicado en un área que cumpla con los requerimientos de: seguridad física, condiciones ambientales adecuadas, seguridad y estabilidad en la parte eléctrica, garantías que deben proporcionarse en conjunto con el área de mantenimiento de la E.S.E Centro de Salud de Galapa. En general, todos los equipos, periféricos y accesorios computacionales de la red de la E.S.E Centro de Salud de Galapa deben estar lejos de dos factores principales: La luz directa del Sol y de humedades, filtraciones y demás medios que puedan hacer que el equipo tenga contacto con el agua.

5. Todo equipo o periférico perteneciente a la red de la E.S.E Centro de Salud de Galapa, deberá contar con un dispositivo de protección eléctrica, ya sea estabilizador de corriente o UPS, que proteja al equipo ante un cambio brusco en la corriente eléctrica de la entidad o del sector donde se ubica. Por lo anterior:

   - Todo equipo propiedad de la institución, y que no cuente con alguno de estos dispositivos de protección, no puede ponerse en funcionamiento. Si el funcionario conectara el equipo, será el directo responsable de los daños que puedan ocurrirle a este, y se le aplicará ley 734. Régimen Único Disciplinario

- En caso que se necesite poner en funcionamiento un equipo que no tenga UPS o estabilizador, podrá hacerse de manera temporal y con el acompañamiento de un funcionario de la oficina de Sistemas de Información.

6. Los usuarios responsables de los equipos en cada dependencia deberán dar cumplimiento con las normas y estándares de instalación con las que fue entregado el equipo, y deberán pedir aprobación de actualización o instalación de cualquier software, reubicación del equipo, reasignación, y todo aquello que implique cambios respecto a su instalación, asignación, función y misión original. Los equipos de cómputo no deben moverse o reubicarse sin la aprobación previa de la oficina de Sistemas de Información, que evaluará la viabilidad de dicho cambio.

7. La protección física y la limpieza externa de los equipos corresponde al funcionario de sistema al que se le asigne la tarea, y la custodia y cuidado en el sitio de trabajo le corresponde al funcionario que lo manipula y quien debe notificar las eventualidades, tales como daños, pérdidas y demás en el menor tiempo posible a la oficina de Sistemas de Información o Soporte Tecnológico de la E.S.E Centro de Salud de Galapa.

   Está totalmente prohibido el consumo o ubicación de alimentos cerca de los equipos e impresoras, así como pegar distintivos, calcomanías y demás. En caso que ocurra un incidente producido por el derrame de algún tipo de alimentos sobre un equipo, periférico o accesorio, este debe apagarse y desconectarse de inmediato e informar oportunamente a la oficina de Sistemas de Información quien hará el mantenimiento necesario he informara a quien corresponda para que se tomen las medidas correctivas necesarias.

8. No se permite el uso de dispositivos de almacenamiento extraíble tales como memorias USB, CD o DVD, nuevas tecnologías en los equipos de la E.S.E Centro de Salud de Galapa, salvo en aquellos casos en donde por fuerza mayor se requiera y previamente evaluado y aprobado por la oficina de Sistemas de Información.

   Para garantizar lo anterior, la oficina de Sistemas de Información bloquea los puertos USB (solamente para el uso de memorias), y las unidades de CD/DVD, si algún usuario necesita que ese bloqueo sea levantado, deberá solicitarlo a la oficina de Sistemas de Información, que a su vez hará llegar la solicitud a la Gerencia para su evaluación y decisión. Esta medida aplica para funcionarios y contratista que laboren en la Institución y que de una u otra manera tengan acceso a los equipos del Hospital.

9. Toda instalación de equipo, mantenimiento o proceso de soporte técnico a nivel de hardware, sin importar su nivel de complejidad, debe ser única y exclusivamente realizado por personal de la oficina de Sistemas de Información de la E.S.E Centro de Salud de Galapa. Bajo ningún concepto se autoriza que personal ajeno a la oficina de Sistemas de Información manipule los equipos de la E.S.E Centro de Salud de Galapa.

10. Para solicitar servicio de mantenimiento a un equipo, periférico o accesorio, se debe hacer por escrito al correo institucional de la Oficina de Sistemas.

11. Los equipos de cómputo de la E.S.E Centro de Salud de Galapa no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) bajo ninguna causa. (Ley 734). Está

totalmente prohibido a los usuarios destapar o desarmar los equipos o impresoras bajo cualquier motivo, sin exclusión. El único personal autorizado para esta labor, es el de la oficina de Sistemas de Información. De detectarse que se está presentando esta conducta se informara y se tomaran las medidas correctivas necesarias.

12. No se puede dar mantenimiento o soporte técnico a nivel de hardware a un equipo de cómputo que no es propiedad de la E.S.E Centro de Salud de Galapa.

13. Los funcionarios de La oficina de Sistemas de Información de la E.S.E Centro de Salud de Galapa son los únicos autorizados para manejar, mantener y velar por la integridad y seguridad de los servidores centrales de la institución, a su vez de mantener las claves de estos.

14. El servidor central de la red de la E.S.E Centro de Salud de Galapa debe estar ubicado en un lugar exclusivo, sin acceso de personas ajenas a la oficina de Sistemas de Información, y con las condiciones adecuadas de espacio, temperatura, iluminación, entre otras.

15. Los equipos propiedad del Hospital deben usarse solamente para las actividades propias de la E.S.E Centro de Salud de Galapa, por lo tanto, los usuarios no deben usarlos para asuntos personales. (Delito contra los bienes de la administración pública).

16. La adquisición de nueva infraestructura de procesamiento de la información (hardware, software, aplicaciones e instalaciones físicas) o la actualización de la existente, deberá ser autorizada por la Oficina de Sistemas de Información y el jefe de la oficina afectada.

17. Todo equipo que sea asignado a un funcionario o contratista, deberá ser entregado al responsable de este, en las mismas condiciones en que lo recibió, como parte de las actividades definidas en la terminación del contrato o cambio de cargo.

18. Todo equipo de cómputo que este asignado a áreas asistenciales y requiera ser retirado del servicio para mantenimiento, reparación, reubicación o reemplazo, debe previamente pasar por un proceso de desinfección en sitio, con el fin de prevenir posible contaminación.

5.2. Política de Seguridad de Usuarios.

Los usuarios son las personas que utilizan la estructura tecnológica de la Institución, ya sean equipos, recursos de red o gestión de la información. La oficina de Sistemas de Información establece normas que buscan reducir los riesgos a la información o infraestructura informática. Estas normas incluyen, restricciones, autorizaciones, denegaciones, perfiles de usuario, protocolos y todo lo necesario que permita un buen nivel de seguridad informática.

Todos los funcionarios y contratistas de la E.S.E Centro de Salud de Galapa, deberán cumplir con estos requerimientos de seguridad de la Información. Igualmente, durante el proceso de vinculación deberán recibir inducción sobre lo establecido en este Documento y sobre la responsabilidad del cumplimiento de las políticas, procedimientos y estándares definidos por el Hospital.

La información almacenada en los equipos de cómputo es propiedad de la E.S.E Centro de Salud de Galapa y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad. No es permitido divulgar, alterar, borrar, eliminar información sin la debida autorización.

Toda información en formato electrónico o impreso del Hospital debe estar debidamente identificada mediante rótulos o etiquetas, lo que permitirá su identificación y clasificación. Con esto se alimenta el inventario y clasificación de los archivos de información.

Las claves o los permisos de acceso que les sean asignados a los funcionarios y/o contratista, son responsabilidad exclusiva de cada uno de ellos y no deben utilizar la identificación o contraseña de otro usuario, excepto cuando los funcionarios de Sistemas la soliciten para la reparación o el mantenimiento de algún servicio o equipo.

1. Los permisos a usuarios son personales e intransferibles y serán acordes a las funciones que desempeñen y no deberán tener permisos adicionales a estos. Estos permisos se conceden a solicitud escrita del jefe de la Oficina quien debe velar por su adecuado manejo.

2. Los usuarios deben renovar periódicamente su clave de acceso al sistema, esto deben solicitarlo a la oficina de Sistemas de Información quienes le facilitarán el acceso y lo acompañarán en el proceso.

   Está totalmente prohibido: El intento o violación de los controles de seguridad establecidos; El uso sin autorización de los activos informáticos; El uso no autorizado o impropio de la conexión al Sistema; el uso indebido de las contraseñas, firmas, o dispositivos de autenticación e identificación; acceder a servicios informáticos utilizando cuentas, claves, contraseñas de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma

3. El usuario será el directo responsable de cualquier daño producido por medidas o decisiones mal tomadas, mantenimientos, reparaciones o instalaciones realizados por él que no fueran informadas o consultadas a la oficina de Sistemas de Información de la E.S.E Centro de Salud de Galapa.

4. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario. Si detectan actividades irregulares con su código, tienen solicitar una auditoría a la oficina de Sistemas de Información que se encargará de dar soporte e informar al usuario la actividad completa en el período y módulos solicitados y de igual manera informara qué medidas se deben tomar al respecto. (Investigación preliminar, cambio de usuario, proceso disciplinario).

5. Informar inmediatamente a la oficina de Sistemas de Información cualquier anomalía, aparición de virus o programas sospechosos e intentos de intromisión y no intente distribuir este tipo de información interna o externamente. A cualquier infracción a la política de seguridad informática cometida por un funcionario y/o contratista de la E.S.E Centro de Salud de Galapa, se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 24:“Son deberes de todo servidor público:

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

6. En caso de presentarse un problema crítico a nivel informático en horario no laboral afectando el normal funcionamiento de la E.S.E Centro de Salud de Galapa, la oficina de Sistemas de Información dispone de un funcionario para atender y solucionar estos inconvenientes que está debidamente reportado en la oficina de Regionalización medica quien es el encargado de localizarlo.

7. Está prohibido intentar sobrepasar los controles de los sistemas, o tratar de saltar los bloqueos de acceso a internet (cambio de dirección IP, cambio de nombre de equipo, etc.) o introducir intencionalmente software malintencionado que impida el normal funcionamiento de los sistemas. En este caso se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 24:"Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley."

8. Todo funcionario que utilice los recursos informáticos, tiene la responsabilidad de velar por su integridad, confidencialidad y disponibilidad de la información que maneje, especialmente si dicha información es crítica. Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 22: "Son deberes de todo servidor público: Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización."

9. La oficina de Sistemas de Información es la única encargada y responsable de capacitar a los usuarios en el manejo de las herramientas informáticas que son exclusivas de la misión y función de la institución.

10. . Los usuarios de la red de la E.S.E Centro de Salud de Galapa recibirán capacitación para el manejo de las herramientas desarrolladas en la institución. La asistencia a la capacitación es obligatoria y requisito indispensable para acceder al sistema de información de lo contrario no se le asigna claves y contraseñas. Está totalmente prohibido el uso de contraseñas o claves de otro usuario.

11. No se permitirá el almacenamiento y/o procesamiento de información propiedad del Hospital, en equipos o dispositivos de propiedad de los funcionarios o contratistas. Todos los contratistas y funcionarios deben firmar una cláusula de confidencialidad, que permita al Hospital proteger la información.

5.3. Política de Seguridad de Software.

1. La oficina de Sistemas de Información es la única responsable de la instalación de software informático y de telecomunicaciones.

2. En los equipos de cómputo de la E.S.E Centro de Salud de Galapa, no se permite la instalación de software que no cuente con el licenciamiento apropiado. Está prohibido el uso de aplicaciones ilegales y el uso de “Cracks”, “Keygens” y demás aplicativos.

3. Está totalmente prohibido la instalación de juegos, programas de mensajería o aplicativos que no estén relacionados con las labores institucionales que se realizan en la E.S.E Centro de Salud de Galapa.

4. Con el propósito de proteger la integridad de los equipos y sistemas informáticos y de telecomunicaciones, es obligatorio que todos y cada uno de estos dispongan de software de seguridad (antivirus, filtros de contenido web, controles de acceso, entre otros). Equipo que no cuente con estos aplicativos de seguridad, no puede conectarse a la red de la institución.

5. las medidas de protección lógica (a nivel de software) son responsabilidad del personal de sistemas de información y el correcto uso de los sistemas corresponde a quienes se les asigna y les compete notificar cualquier eventualidad a la oficina de Sistemas de Información.

6. La adquisición y actualización de software para los equipos de cómputo y de telecomunicaciones se llevará a cabo de acuerdo al calendario y requerimientos que sean propuestos por la oficina de Sistemas de Información y a la disponibilidad presupuestal con el que se cuente.

7. Es obligación de todos los usuarios que manejen información masiva y/o crítica, solicitar respaldo correspondiente a la Oficina de sistemas sobre la generación copias de seguridad ya que se considera como un activo de la institución que debe preservarse. Las copias de respaldo a la información generada por el personal y los recursos informáticos de la institución deben estar resguardados en sitios debidamente adecuados para tal fin.

8. La oficina de Sistemas de Información administrará los diferentes tipos de licencias de software con la que cuenta la E.S.E Centro de Salud de Galapa y vigilará su vigencia de acuerdo a sus fechas de caducidad.

5.4. Política de Seguridad de la Red e Internet.

1. Toda cuenta de acceso al sistema, a la red y direcciones IP, será asignada por la oficina de Sistemas de Información de la E.S.E. Centro de Salud de Galapa previa solicitud por escrito.

2. Se prohíbe utilizar la red y los equipos para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular. En este caso se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 24: “Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.”

3. En lo relacionado con el uso de correo electrónico, no está permitido el uso del correo personal. Los correos institucionales deben ser para uso exclusivo de las actividades de la E.S.E. Centro de Salud de Galapa.

4. Para garantizar la seguridad de la información y el equipo informático, la oficina de Sistemas de Información establece filtros y medidas para regular el acceso a contenidos en el cumplimiento de esta normatividad:

Se prohíbe:

- Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar o insultar a otras personas, o interferir con el trabajo de los demás.
- Utilizar los recursos de la E.S.E. Centro de Salud de Galapa para el acceso no autorizado a redes y sistemas remotos.
- Acceder remotamente a los equipos de la E.S.E. Centro de Salud de Galapa, los únicos funcionarios autorizados para realizar estas prácticas son los de la oficina de Sistemas de Información, al momento de dar soporte a los usuarios en horario extra laboral.
- Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas, mediante técnicas, comandos o programas a través de la red.
- Monopolizar los recursos en perjuicio de otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones en masa, uso de recursos de impresión no autorizado.
- Poner información en la red que infrinja el derecho a la intimidad de los demás funcionarios y/o contratistas.
- Utilizar los servicios de la red para la descarga, uso, intercambio y/o instalación de juegos, música, películas, imágenes protectoras o fondos de pantalla, software de libre distribución, información y/o productos que de alguna manera atenten contra la propiedad intelectual de sus actores o que contenga archivos ejecutables.
- El intercambio no autorizado de información de propiedad del Hospital, de sus usuarios y/o sus funcionarios, con terceros.
- El acceso a cuentas de correos personales de ningún tipo desde la red del Hospital y solo se podrán utilizar las cuentas de correo electrónico suministradas por la Institución. Algunos ejemplos de los sistemas de correos electrónicos personales no autorizados son yahoo, Hotmail, gmail.
- Utilizar los servicios para acceder a páginas de radio o TV en línea, descargar archivos de música o video, visitar sitios de pornografía, ocio, entre otros que estén fuera de las funciones del usuario. Código Único Disciplinario (Ley 734 de 2002) Art. 35 Num. 9: “A todo servidor público le está prohibido: Ejecutar en el lugar de trabajo actos que atenten contra la moral o las buenas costumbres.”

5. La oficina de Sistemas de Información tiene habilitado un equipo con acceso total a internet, en el cual, los usuarios puedan realizar consultas o actividades personales, de corta duración. La oficina de

Sistemas de Información no se responsabiliza por pérdidas de información en ese equipo, ya que es de uso público y periódicamente se está eliminando información ajena a la institución. La oficina de sistemas realizará monitoreo permanente de tiempos de navegación y actividades realizadas a páginas vistas por parte de los funcionarios y/o contratistas

6. Los servicios bancarios vía web a nombre de la E.S.E. Centro de Salud de Galapa, solamente podrán ser utilizados por el Tesorero y únicamente en el equipo que este tenga asignado. La oficina de Sistemas de Información, tendrá habilitado otro equipo para esta tarea a fin de dar apoyo y soporte cuando se solicite.

7. El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido únicamente por la oficina de Sistemas de Información.

8. El uso de carpetas compartidas está prohibido para todos los funcionarios y/o contratistas, ya que en caso de infiltrase un virus o programa malicioso, usa este medio para propagarse. Las únicas carpetas compartidas que pueden existir en la red de la E.S.E. Centro de Salud de Galapa, son las copias de seguridad programadas, tanto de base de datos como de información de los usuarios. Está prohibido el uso abusivo de estos recursos por parte de los usuarios en forma tal que afecte negativamente el rendimiento de la red.

9. Para posibilitar el uso compartido de archivos, la oficina de Sistemas de Información tiene habilitado un servidor FTP en el cual se pueden almacenar y compartir la información Pública y Privada de cada dependencia. La información Pública puede ser accedida por cualquier funcionario de cualquier dependencia. La información Privada solo está disponible para los funcionarios de la misma dependencia.

10. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoría de seguridad y un reporte de los hallazgos a la oficina de Control Interno y Control Interno para que dé tramite y se tomen las medidas pertinentes.

11. Los mensajes y la información contenida en los buzones de correo son de propiedad del Hospital. Los buzones no deberán contener mensajes con más de un año de antigüedad. Pero se debe dejar un histórico del registro de los mensajes. Todos los mensajes enviados deben respetar los formatos de imagen corporativa definidos por el Sistema de Gestión Documental y conservar todas las normas de legalidad de los documentos.

5.5. Política Seguridad de Datos e Información

La información es en uno de los elementos más importantes dentro de una organización. La seguridad informática debe evitar que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para

obtener ventajas de ella o que sea manipulada, ocasionando datos errados o incompletos. El objetivo de esta política es la de asegurar el acceso a la información en el momento oportuno.

1. Toda información de relevancia debe contar con copia de seguridad y un tiempo de retención determinado, por lo cual, la información no se debe guardar indefinidamente en un archivo activo ocupando espacio innecesario de almacenamiento, el usuario debe establecer cuándo su información pasará a ser inactiva. Aplicación de la Ley 594 de 2000 Ley de Archivos. Tablas de Retención Documental.

2. La copia de seguridad de la base de datos central de la E.S.E. Centro de Salud de Galapa se genera así: Tres copias diarias en tres equipos diferentes al servidor; Una copia semanal en disco, que será almacenada de acuerdo a los requerimientos necesarios para dicho fin ubicado en un sitio distante del área de trabajo. Estas copias deben ser monitoreadas a diario con el objetivo de garantizar la correcta realización y funcionamiento de las mismas. La ubicación de los medios de almacenamiento, deberá estar alejada del polvo, humedad o cualquier contacto con material que produzca corrosión.

3. El propietario de la información, con la participación de un funcionario de la oficina de Sistemas de Información son los encargados de la creación y seguimiento de las copias de seguridad realizadas a la información previamente seleccionada por el usuario.

4. Cualquier aplicación, archivo desconocido o sospechoso que aparezca en la información del usuario (ya sea en el equipo local, correo electrónico), no debe ser abierto o ejecutado sin antes contar con la asesoría de la oficina de Sistemas de Información, que se encargará de examinar y determinar si la aplicación o archivo es potencialmente peligrosa para el equipo o la red de la entidad.

5. No está permitido extraer información por ningún medio y bajo ningún motivo de la institución.

6. Atender todas las disposiciones de la Ley 527 de 1999. Que 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.

7. La Ley 594/00 Ley General de Archivos, en sus Artículos 19 y 21 establece: Art. 19 “. Las entidades del Estado podrán incorporar tecnologías de avanzada en la administración y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumplan con los siguientes requisitos: a) Organización archivística de los documentos; b) Realización de estudios técnicos para la adecuada decisión, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema.

PARAGRAFO 1o. Los documentos reproducidos por los citados medios gozarán de la validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por las leyes procesales y se garantice la autenticidad, integridad e inalterabilidad de la información.

PARAGRAFO 2o. Los documentos originales que posean valores históricos no podrán ser destruidos, aun cuando hayan sido reproducidos y/o almacenados mediante cualquier medio.

ARTICULO 21. PROGRAMAS DE GESTION DOCUMENTAL. Las entidades públicas deberán elaborar programas de gestión de documentos, pudiendo contemplar el uso de nuevas tecnologías y soportes, en cuya aplicación deberán observarse los principios y procesos archivísticos.

PARAGRAFO. Los documentos emitidos por los citados medios gozarán de la validez y eficacia de un documento original, siempre que quede garantizada su autenticidad, su integridad y el cumplimiento de los requisitos exigidos por las leyes procesales Acuerdo 060/2001 del Archivo General de la Nación. POR EL CUAL SE ESTABLECEN PAUTAS PARA LA ADMINISTRACIÓN DE LAS COMUNICACIONES OFICIALES EN LAS ENTIDADES PÚBLICAS Y LAS PRIVADAS QUE CUMPLEN FUNCIONES PÚBLICAS. “Comunicaciones por Email ARTICULO DÉCIMO TERCERO: Comunicaciones oficiales por correo electrónico: Las entidades que dispongan de Internet y servicios de correo electrónico, reglamentarán su utilización y asignarán responsabilidades de acuerdo con la cantidad de cuentas habilitadas. En todo caso, las unidades de correspondencia tendrán el control de los mismos, garantizando el seguimiento de las comunicaciones oficiales recibidas y enviadas. Para los efectos de acceso y uso de los mensajes de datos del comercio electrónico y de las firmas digitales se deben atender las disposiciones de la Ley 527 de 1999 y demás normas relacionadas.

CODIGO PENAL Artículo 257. Del acceso ilegal o prestación ilegal de los servicios de telecomunicaciones. El que acceda o use el servicio de telefonía móvil celular u otro servicio de comunicaciones mediante la copia o reproducción no autorizada por la autoridad competente de señales de identificación de equipos terminales de éstos servicios, derivaciones, o uso de líneas de telefonía pública básica conmutada local, local extendida o de larga distancia no autorizadas, o preste servicios o actividades de telecomunicaciones con ánimo de lucro no autorizados, incurrirá en prisión de dos (2) a ocho (8) años y multa de quinientos (500) a mil (1.000) salarios mínimos legales mensuales vigentes. Texto resaltado declarado EXEQUIBLE por la Corte Constitucional mediante Sentencia de la Corte Constitucional 311 de 2002.

La pena anterior se aumentará de una tercera parte a la mitad, para quien hubiese explotado comercialmente por sí o por interpuesta persona, dicho acceso, uso o prestación de servicios de telecomunicaciones no autorizados.

Igual aumento de pena sufrirá quien facilite a terceras personas el acceso, uso ilegítimo o prestación no autorizada del servicio de qué trata este artículo.

Texto subrayado declarado INEXEQUIBLE por la Corte Constitucional mediante Sentencia de la Corte Constitucional 311 de 2002

Artículo 258. Utilización indebida de información privilegiada. El que como empleado o directivo o miembro de una junta u órgano de administración de cualquier entidad privada, con el fin de obtener provecho para sí o para un tercero, haga uso indebido de información que haya conocido por razón o con ocasión de su cargo o función y que no sea objeto de conocimiento público, incurrirá en multa.

Artículo 294. Documento. Para los efectos de la ley penal es documento toda expresión de persona conocida o conocible recogida por escrito o por cualquier medio mecánico o técnicamente impreso, soporte material que exprese o incorpore datos o hechos, que tengan capacidad probatoria.

Artículo 398. Peculado por uso. El servidor público que indebidamente use o permita que otro use bienes del Estado o de empresas o instituciones en que éste tenga parte, o bienes de particulares cuya administración, tenencia o custodia se le haya confiado por razón o con ocasión de sus funciones, incurrirá en prisión de uno (1) a cuatro (4) años e inhabilitación para el ejercicio de derechos y funciones públicas por el mismo término.

5.6. Política en Administración de Seguridad Informática.

1. El nivel de prioridad de cada servicio en cuanto a seguridad y estabilidad informática, deberán estar bajo monitoreo permanente.

2. Las auditorías de uso de los recursos informáticos a cada dependencia de la E.S.E. Centro de Salud de Galapa deberán realizarse periódicamente de acuerdo al calendario que establezca la Oficina de sistemas de información. Los hallazgos encontrados serán reportados a la oficina de Control Interno, Control Interno y Gerencia para que se establezcan los correctivos necesarios.

3. Toda la información almacenada en los equipos de la E.S.E. Centro de Salud de Galapa, puede ser auditada por funcionarios de la oficina de Sistemas de Información en la verificación del cumplimiento de las políticas de seguridad establecidas. Los hallazgos encontrados serán reportados a la oficina de Control Interno, Control Interno Disciplinario y Gerencia para que se establezcan los correctivos necesarios.

4. Los jefes de oficina son los responsables en la implementación y garantía inicial del cumplimiento de políticas que hayan sido publicadas, modificadas o adicionadas recientemente. Cualquier violación a las políticas y normas de seguridad establecidas en este documento y aprobadas mediante acto administrativo será sancionada disciplinaria o penalmente. Para las infracciones más graves, se acatará lo estipulado en la ley 1273 de 2009 de delitos informáticos, y Ley 734 de 2002 Código Único Disciplinario.

6. DESARROLLO DE LA POLITICA

La Política de Gobierno Digital se desarrollará a través de la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital, que será desarrollado y socializado por MinTic, por parte de las entidades y departamentos administrativos de la rama ejecutiva inicialmente, para los entes territoriales y demás partes interesadas, se adelantarán jornadas de sensibilización en temas de Seguridad Digital. Adicionalmente, Las entidades designadas, deberán dar cumplimiento a todas las actividades relacionadas en el plan de acción de seguimiento PAS del Conpes 3854 de 2016.

1. Componentes de la Política de Gobierno Digital: Son las líneas de acción que orientan el desarrollo y la implementación de la Política de Gobierno Digital, a fin de lograr sus propósitos. Los componentes son:

   1.1. **TIC para el Estado:** Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones.

   1.2. **TIC para la Sociedad:** Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común.

2. **Habilitadores Transversales de la Política de Gobierno Digital:** Son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

3. **Lineamientos y estándares de la Política de Gobierno Digital:** Son los requerimientos mínimos que todos los sujetos obligados deberán cumplir para el desarrollo de los componentes y habilitadores que permitirán lograr los propósitos de la Política de Gobierno Digital.

4. **Propósitos de la Política de Gobierno Digital:** Son los fines de la Política de Gobierno Digital, que se obtendrán a partir del desarrollo de los componentes y los habilitadores transversales, estos son:

   4.1. Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.

   4.2. Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.

   4.3. Tomar decisiones basadas en datos a partir del aumento el uso y aprovechamiento de la información.

   4.4. Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto

   4.5. Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC.

7. REFERENCIAS

HUERTAS LEONARDO. Políticas de seguridad [en línea]. http://www.slideshare.net/SamuraiBlanco/politicas-seguridad-leonardo-huertas LEY 734 de 2002

Código Único Disciplinario.

UNIVERSIDAD NACIONAL DE COLOMBIA. Guía para elaboración de políticas de seguridad [en línea] www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf >

LEY 1273 de 2009.Delitos Informáticos Manual de seguridad en redes [en línea].

COORDINACIÓN DE EMERGENCIA EN REDES TELEINFORMÁTICAS DE LA ADMINISTRACIÓN PÚBLICA. ARGENTINA NORMA ISO 12001

Aprobado mediante acta No. 03-2022 del 20 de diciembre del 2022 del Comité Institucional de Gestión y Desempeño