**RESOLUCION No** 1017
**( 25 MAR 2021 )**

***"Por la cual se actualizan las políticas de seguridad y privacidad de la información del Instituto Departamental de Salud de Norte de Santander"***

**EL REPRESENTANTE LEGAL DE LA INSTITUTO DEPARTAMENTAL DE SALUD DE NORTE DE SANTANDER,** y,

**CONSIDERANDO:**

Que, el Instituto Departamental de Salud de Norte de Santander debe incentivar y estimular el uso y apropiación de tecnologías de información y comunicaciones como apoyo a las tareas misionales y de gestión de la entidad.

Que, la Ley 734 de 2002 en el Artículo 48, establece como falta gravísima en su numeral 43: "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".

Que, la ley 1437 de 2011, en el Capítulo 4, Artículo 60, señala que "La autoridad respectiva garantizará condiciones de calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad de la información de acuerdo con los estándares que defina el Gobierno Nacional.

Que, mediante el Decreto Nº 1078 de 2015, Título 9 Políticas y Lineamientos de tecnologías de Información, Capítulo 1 Estrategia de Gobierno en Línea, Sección 2, Artículo 2.2.9.1.2.1 Componentes; se definieron cuatro componentes, entre los que se encuentra el Componente Tic para la Seguridad y Privacidad de la información que comprende las acciones tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Que, mediante el Decreto Nº 1008 de 2018, Artículo 2.2.9.1.1.3. Principios, se define la seguridad de la información como uno de los principios de la Política de Gobierno Digital, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Que, según el numeral 2, Sección 2, Artículo 2.2.9.1.2.1 Estructura, del Decreto anteriormente citado; los 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 componentes TIC para el Estado y TIC para la Sociedad, y el logro de los propósitos de dicha Política.

Que, mediante Resolución 2189 del 01 de junio de 2017 se aprueban las Políticas de Seguridad Informática, que sirven de guía para que los usuarios que accedan y utilicen los servicios tecnológicos que presta la Entidad y puedan hacer un adecuado uso de los

RESOLUCION No 1017
( 25 MAR 2021 )

mismos, teniendo en cuenta que la utilización de tecnología en el procesamiento, almacenamiento, recuperación y transmisión de la información, implica importantes riesgos para su disponibilidad, confidencialidad e integridad.

Que, mediante Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, que establece los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital, en el artículo 3º establece que las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI.

Que, según Acta Nº 001 de Marzo 19 de 2021 del Comité Institucional de Gestión y Desempeño revisó y aprobó la propuesta de actualización de las Políticas de Seguridad Informática de la Entidad.

Que teniendo en cuenta lo anteriormente expuesto, se hace necesario actualizar la Resolución 2189 del 01 de junio de 2017 y establecer las políticas de seguridad y privacidad de la información del Instituto Departamental de Salud de Norte de Santander que propenderá en garantizar el óptimo funcionamiento de las tecnologías de información y comunicaciones.

**RESUELVE:**

**Artículo Primero.** Actualizar y Aprobar las Políticas de Seguridad y Privacidad de la Información, contenidas en el Anexo Técnico que forma parte integral de la presente Resolución; que sirvan de guía para que los usuarios que accedan y utilicen los servicios tecnológicos que presta la Entidad y puedan hacer un adecuado uso de los mismos, teniendo en cuenta que la utilización de tecnología en el procesamiento, almacenamiento, recuperación y transmisión de la información, implica importantes riesgos para su disponibilidad, confidencialidad e integridad.

**Parágrafo 1**. Las Políticas de Seguridad y Privacidad de la Información se publicarán en el Link de Políticas de la página web institucional.

**Artículo Segundo.** Responsabilidades de todos los funcionarios. Será de obligatorio cumplimiento aplicar lo estipulado en el anexo técnico de la resolución, tanto para los funcionarios y contratistas del Instituto Departamental de Salud de Norte de Santander.

**Parágrafo 1.** Las coordinaciones de las Dependencias, Grupos y Subgrupos serán responsables de ponerlas en conocimiento del personal a cargo.

**Artículo Tercero.** Monitoreo y cumplimiento de la Política. Constituirá responsabilidad de los funcionarios con función de coordinar Dependencias, Grupos y Subgrupos funcionales, al igual que la Oficina de Sistemas de Información realizar el monitoreo y seguimiento al cumplimiento de las Políticas.

RESOLUCION No 1017

( 25 MAR 2021 )

**Artículo Cuarto.** Violaciones y Sanciones El incumplimiento de las políticas establecida en el Anexo Técnico de la presente resolución, podrá incurrir en una falta disciplinaria. Según la gravedad que se cometa se estandariza tres niveles: leves, graves y gravísimas y se procederá de acuerdo a lo estipulado en el anexo técnico de la resolución.

**Artículo Quinto.** Vigencia y derogatorias. La presente resolución rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias.

**PUBLÍQUESE Y CÚMPLASE**

Se expide en San José de Cúcuta, a los 25 MAR 2021

**CARLOS ARTURO MARTINEZ GARCIA**
**Director**

**Proyectó y elaboró:** Armando Rojas C.
**Revisó:** Laury L. Páez.

# ANEXO TÉCNICO RESOLUCIÓN 1017 DE 25 DE MARZO DE 2021

# POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

# INSTITUTO DEPARTAMENTAL DE SALUD DE NORTE DE SANTANDER

## HISTORIAL

| Versión No. | Descripción | Fecha |
|---|---|---|
| 01 | Aprobada por el Comité Antitrámites y de Gobierno en Línea | 1-Jun-17 |
| 02 | Aprobada por el Comité de Gestión y Desempeño Institucional | 19-Mar-2021 |

# CONTENIDO

## MOTIVACIÓN

Las tecnologías y sistemas de información permanecen en continua evolución, lo que conlleva a una mayor responsabilidad en su manejo, teniendo en cuenta que las amenazas también se encuentra en proceso continuo de expansión, presentándose cada día mayores riesgos, vulnerando la estabilidad de los activos de información y la infraestructura tecnológica.

Con el transcurrir de los años, en el Instituto Departamental de Salud de Norte de Santander las operaciones institucionales se han incrementado, lo que ha trascendido en la adquisición de tecnologías y sistemas de información que facilite el quehacer diario. En la actualidad, nuestro Instituto cuenta con una gran talento humano, distribuidos en dependencias, grupos y subgrupos, quienes tienen asignados equipos informáticos y sistemas de información, que se utilizan diariamente de manera ardua, por tal razón, surge la necesidad de establecer políticas de seguridad y privacidad de la información, las cuales, deberán ser aplicadas por cada uno de los funcionarios de la entidad; con el fin de concientizar el buen uso, manejo, y compartimiento de recursos informáticos que ayuden a que los activos de información, bienes y servicios de la Entidad se preserven y sean de gran utilidad para las actividades diarias que se llevan a cabo.

## INTRODUCCION

En Colombia existe normatividad que reglamenta y propende por la implementación de medidas de seguridad y privacidad de la información, como el decreto 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital. Siendo la Seguridad de la Información, uno de los habilitadores transversales de esta Política.

La actualización de las políticas de seguridad y privacidad de la información del Instituto Departamental de Salud de Norte de Santander, tiene como base la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Las políticas de seguridad y privacidad de la información, que se establecen en el presente documento, se encuentran alineadas con la estrategia y objetivos de la entidad. Y son herramientas que ayudan al funcionamiento y ejecución de las actividades que se llevan a cabo con los dispositivos informáticos y activos de información de la Entidad y busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, en procura de preservar la confidencialidad, integridad y disponibilidad de la información de la entidad, y de los servicios que presta al ciudadano.

Al implementar estas políticas se requiere que tanto los directivos como funcionarios, contratistas y terceros tengan un gran compromiso en su cumplimiento.

# 1. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

## 1.1. OBJETIVO GENERAL DEL MSPI

Determinar los lineamientos, las normas, políticas y recomendaciones inherentes a la seguridad y privacidad de la información y adopción de buenas prácticas en el uso de los recursos tecnológicos del Instituto Departamental de Salud de Norte de Santander, con el ánimo de preservar los activos de información en óptimos niveles de integridad, privacidad y confidencialidad.

.

## 1.2. DETERMINACIÓN DEL ALCANCE DEL MSPI

Este manual debe aplicarse para servir a la alta dirección en la protección de los activos, la protección de la infraestructura tecnológica que soporta la operación de la Entidad y gestión de los riesgos de seguridad y privacidad de información. Las políticas aquí enmarcadas deben ser cumplidas por todo el personal de la Entidad sus funcionarios, contratistas, terceros y la ciudadanía en general que accede a la información del Instituto Departamental de Salud de Norte de Santander.

## 1.3. DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

Según el Decreto Nº 1008 de 2018 del Ministerio de las Tecnologías de la Información y las Comunicaciones - MINTIC, se define la seguridad de la información como uno de los principios de la Política de Gobierno Digital, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

## 2. APLICACIÓN DE LAS POLÍTICAS Y LIDERAZGO

Las políticas de Privacidad y Seguridad de la Información deberán ser publicadas en la página web de la Entidad.

Todo el personal de la Institución tiene la responsabilidad de cumplir con lo formalizado en este documento y aplicarlo en su entorno laboral. Además, tiene la obligación de alertar de manera oportuna y adecuada, cualquier incidente que atente contra la seguridad de la información.

### ROLES Y RESPONSABILIDADES SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La definición de roles permite tener establecidas las tareas que realizará cada uno de los miembros del equipo del MSPI, disminuyendo el campo a las imprecisiones se presenten en referencia a las responsabilidades que cada personaje tiene.

Es importante resaltar la necesidad del compromiso de la Alta dirección de la entidad, para que el apoyo se vaya garantizando desde la fase de planeación del proyecto e ir marcando un punto de partida de éxito con la implementación del modelo de gestión de seguridad de la información planteado para la entidad.

**Responsable de Seguridad de la Información**: Designado por el Comité Institucional de Gestión y Desempeño. El funcionario a cargo es el Líder de la oficina de Sistemas de Información. Tiene como responsabilidad diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad de la información, y someterlos a decisión del Comité Institucional de Gestión y Desempeño, realizando la implementación y seguimiento de estos.

**Líder o responsable de protección de datos personales**: El funcionario a cargo es el Líder de la oficina de Sistemas de Información. Es responsable de establecer lineamientos para la protección de los datos personales tratados en la Entidad.

**Comité Institucional de Gestión y Desempeño**: Debe asegurar la implementación de la política de seguridad y privacidad de la información en la entidad. Debe apoyar al líder de proyecto al interior de la entidad. Debe comunicar a los funcionarios, contratistas y particulares que participan en actividades de forma directa o indirecta con la Entidad, la importancia de satisfacer los requisitos de seguridad digital.

**Responsable de TI**. El funcionario a cargo es el Líder de Sistemas de Información, quien es el principal responsable en la definición de los criterios de seguridad digital de la información en el IDS, para lo cual deberá analizar periódicamente el nivel de riesgo existente, proponiendo soluciones. Es responsable de participar en la elaboración del cronograma de capacitación de seguridad digital en la Entidad. Implementar las mejorar identificadas en la plataforma de seguridad relacionadas con hardware, software, canales de comunicaciones de datos o infraestructura TI.

**Líderes de proceso:** Son responsables de identificar e inventariar los nuevos activos digitales de información y los riesgos cibernéticos asociados.

Las coordinaciones de los distintos Grupos, Subgrupos y dependencias serán responsables de poner las políticas de seguridad y privacidad de la información en conocimiento de su personal subordinado y demás personas

Para el caso del personal que se vincule o contrate con posterioridad a la fecha de publicación, se le deberá indicar el link de publicación para su conocimiento.

**Oficina de Control Interno:** Desempeña un rol específico en materia de control y gestión del riesgo, con el fin de apoyar el desarrollo de un adecuado ambiente de control, una efectiva gestión del riesgo, la implementación de controles efectivos y un monitoreo y supervisión continua a la gestión de la entidad. En tal sentido, se debe articular con la oficina de control interno el desarrollo de acciones, métodos y procedimientos de control y de gestión del riesgo en la implementación de la política de seguridad y privacidad de la información en la entidad

## 3. VULNERABILIDADES

Son aquellas que afecta la disponibilidad, confidencialidad e integralidad.

**Vulnerabilidades físicas**:

- Instalaciones inadecuadas
- Ausencia de equipos de seguridad
- Cableados desordenados y expuestos
- Falta de identificación
- Instalaciones eléctricas inadecuadas

**Vulnerabilidades naturales:**

- Humedad
- Polvo
- Desastres naturales
- Incendios

**Vulnerabilidades de hardware:**

- Ausencia de actualizaciones
- Conservación inadecuada

**Vulnerabilidades de software**

- Configuración e instalación indebida de los programas
- Ausencia de actualizaciones
- Sistemas operativos mal configurados y mal organizados
- Correos maliciosos
- Ejecución de macro virus
- Navegadores de internet

**Vulnerabilidades de medios de almacenaje**

- Defecto de fabricación
- Uso incorrecto
- Áreas o lugares de depósito inadecuado

**Vulnerabilidades de comunicación**

- Información disponible a usuarios incorrectos afectando la confidencialidad
- Altera el estado original de la información afectando la integridad

**Vulnerabilidades humanas**

- Falta de capacitación específica y adecuada
- Falta de conciencia de seguridad de los usuarios
- Vandalismos

## 4. VIOLACIONES Y SANCIONES

De acuerdo al Código Disciplinario Único – Ley 734, Artículo 34, como servidor público se tiene deberes entre los cuáles se encuentran:

- Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.
- Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.
- Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.

Además, en el Artículo 48, señala como falta gravísima "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".

Teniendo en cuenta lo anteriormente expuesto, el incumplimiento de las políticas de seguridad y privacidad de la información, podrá incurrir en una falta disciplinaria. Según la gravedad que se cometa se estandariza tres niveles: leves, graves y gravísimas.

En cualquier caso de amonestación verbal o escrita y en el caso que lo amerite, el funcionario deberá resarcir el daño o devolver, restituir o reparar el bien afectado.

Cuando se determine una falta a los deberes establecidos en la Ley 734 de 2002 y a las políticas de seguridad y privacidad de la información se dará a conocer a la Oficina de Jurídica y Control Disciplinario de la Institución para que en Comité determine las faltas cometidas y las sanciones a imponer de acuerdo a la norma.

## 5. POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Teniendo en cuenta el objetivo general del Modelo de Seguridad y Privacidad de la Información - MSPI, se hace necesario establecer las políticas de seguridad y privacidad de la información, que serán de gran ayuda para proteger a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la institución.

### 5.1 POLÍTICA PARA EL USO ADECUADO DE ESTACIONES DE TRABAJO

El instituto departamental de Salud asigna a los funcionarios en apoyo al cumplimiento de sus labores, cuando así se requiere una estación de trabajo. Estos equipos son parte del patrimonio institucional y por lo tanto debemos buscar la mejor forma de utilizarlos, tomando en cuenta aspectos de seguridad físicos y lógicos para su protección. Las normas asociadas a esta política incluyen entre otras, las mejores prácticas de uso de las estaciones para proteger el equipo y la información contenida en él.

**Instalación de Equipos**

a) Los equipos de cómputo (computadores, sitios de trabajo, servidores y demás equipos) deben tener una instalación adecuada concorde con cada una de las diferentes partes así como las partes eléctricas, por ejemplo, los estabilizadores no deben estar cerca de la pantalla y los dispositivos de computo siempre deben estar sobre las superficies de trabajo, para que el manejo y control del equipo sea el mejor.
b) Los equipos deben estar ubicados en sitios adecuados, evitando la exposición al sol, al polvo o zonas que generen electricidad estática.
c) No se puede instalar ni conectar dispositivos o partes diferentes a las entregadas en los equipos. Es competencia de la oficina de sistemas de información el retiro o cambio de partes y/o componentes.
d) Los equipos, escáner, impresoras, lectoras y demás dispositivos, no podrán ser trasladados del sitio que se les asignó inicialmente, en el caso de ser necesario, debe ser notificado tanto a Almacén como a la oficina de Sistemas de Información para su respectivo control.
e) Se debe garantizar la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos estén conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra.
f) La oficina de Sistemas de Información debe realizar la hoja de vida de los equipos de cómputo para llevar un control de los equipos propiedad del Instituto, en donde se manifieste el usuario que tenga asignado el equipo bajo su responsabilidad.
g) La oficina de Sistemas de Información deberá especificar las características necesarias para la adquisición de equipos de acuerdo a su operación y

funcionamiento.

h) Al responsable del equipo se le asigna un usuario con la respectiva contraseña, independiente del usuario administrador que ejerce control sobre las configuraciones específicas del equipo.

**Manipulación de Equipos**

a) La infraestructura tecnológica (servidores, computadores, impresoras, UPS, escáner, lectoras y equipos en general) no puede ser utilizada en funciones diferentes a las institucionales.
b) Ningún funcionario a excepción de la oficina de Sistemas de Información se encuentra autorizado para manipular los componentes de los equipos de cómputo.
c) El equipo que ha sido asignado al usuario es de su responsabilidad la manipulación y acceso al equipo para conservar el activo físico como se le ha sido asignado.
d) La manipulación, daños y partes faltantes son de responsabilidad del usuario a quien se le asignó el equipo, quien deberá controlar el acceso a las demás personas no autorizadas debido a que el equipo está a su cargo.
e) Los equipos deben ser manipulados de tal manera que cumplan y satisfagan las tareas a las cuales fueron designados debido a cada una de las funciones y programas instalados, con el fin de realizar el cumplimiento de las actividades designadas por su dependencia.
f) Los equipos deben ser manipulados de la forma en la que se encuentra situadas sus partes con el fin de que no existan fallas tanto eléctricas como funcionales debido a los movimientos bruscos o por la ubicación incorrecta de sus partes.
g) La manipulación de los equipos también incluye la revisión de los equipos con fallas causadas por la mala conexión o falta de conexión eléctrica que puede ser realizadas por los mismos usuarios sin hacer solicitud a la oficina de sistemas de información.
h) La utilización de los equipos es con fin de trabajo; no se pueden realizar descargas de otra serie de software ajeno a las actividades informáticas de la oficina.
i) No es permitido destapar o retirar la tapa de los equipos, ni podrá retirar o instalar partes sin la autorización de la Oficina de sistemas de información.
j) Ningún funcionario podrá formatear los discos duros de los computadores, sin previa autorización de la oficina de sistemas de información.
k) Antes de desconectar cualquier dispositivo del computador se debe desconectar previamente del equipo, en caso contrario, se puede perder datos, o incluso dañar el dispositivo, haciendo inaccesible todo el contenido.
l) No es recomendable guardar ningún dispositivo de almacenamiento magnético de información cerca de ninguna fuente electromagnética, como altavoces, transformadores, etc.

**Buenas prácticas frente a un computador**

a) Mantener limpio de polvo el computador y libre de otros objetos, de modo que no se obstruya ningún punto de ventilación, pues a través de las ranuras de la CPU capta el aire del exterior para la refrigeración de los distintos componentes. Igualmente, se debe tener la prevención con los periféricos.
b) Por seguridad en el lugar de trabajo, la espalda debe estar recta y los pies apoyados en el suelo, con el fin de prevenir problemas en la columna.
c) Mantener los codos con un ángulo de 90 grados del teclado y mouse para que las muñecas no estén flexionadas y apoyadas para evitar dolores en las articulaciones de la mano y futuras complicaciones.
d) No comer, fumar ni ingerir líquidos frente el computador para evitar incidentes y accidentes, además, por su salud se evita adquirir bacterias y en algunos casos prevenir la obesidad.
e) Mantener una distancia mínima de 55 cm de la pantalla y los ojos deben estar a la misma altura que el borde superior de la pantalla con el fin de prevenir cansancio en los ojos, posible problemas con la visión, dolores de cabeza, espalda o cuello.
f) No golpear ni mover bruscamente los equipos ni sus periféricos.
g) Se aconseja utilizar colores claros y mate en la pantalla para evitar cansancio en la vista.
h) La posición del monitor debe evitar que la luz incida directamente sobre la pantalla para prevenir daños a causa del reflejo de la misma y, al mismo tiempo, evitar una visualización incómoda.
i) Evitar limpiar la pantalla con productos que puedan dañarla como alcohol o jabones, se aconseja usar un trapo de tela suave ligeramente humedecido y no hacer fuerza excesiva durante la limpieza.
j) En el caso de personas zurdas han de cambiar la posición del ratón al lado izquierdo del teclado y configurarlo así en las propiedades del ratón desde el Panel de Control.
k) Mantener los equipos apagados mientras no se estén utilizando.

**Mantenimiento de Equipos**

a) La conservación de los equipos, su funcionamiento, la seguridad física de cada equipo hacen parte de las responsabilidades de los usuarios.
b) La instalación de cada uno de los equipos conforme al sitio y espacio de trabajo, el mantenimiento preventivo y correctivo es responsabilidad de la Oficina Sistemas de Información.
c) Está prohibido que los equipos informáticos sean atendidos por personal ajeno a la Oficina de Sistemas de Información para el manteamiento preventivo y correctivo. El funcionario responsable del equipo responderá por daños adversos a estos mantenimientos o arreglos realizados por

terceros.

d) Los usuarios también hacen parte del mantenimiento de los equipos de cómputo haciendo un buen uso y utilidad de los equipos para que su funcionamiento sea el mejor y los manteamientos preventivos y correctivos se prolonguen con la ayuda de la buena manipulación.
e) Los responsables de cada una de las dependencias, grupos y subgrupos pueden hacer una solicitud a Sistemas de Información en el formato respectivo de mantenimiento correctivo desde el momento que el equipo este fallando y las precauciones realizadas por el usuario no hayan sido satisfactorias para que el equipo funcionara.
f) Las solicitudes de mantenimientos externos a equipos del Instituto son determinadas por la Oficina de Sistemas de Información con un previo análisis de funcionamiento, con el fin de dar a conocer que el mantenimiento o arreglo se debe realizar externamente.
g) Es estrictamente obligatorio, informar oportunamente a la Oficina de sistemas la ocurrencia de novedades por problemas técnicos, eléctricos, de planta física, líneas telefónicas, o cualquiera otra, que altere la correcta funcionalidad.
h) Queda rotundamente prohibido realizar mantenimiento preventivo y correctivo a equipos ajenos al Instituto.

**Actualización de Equipos**

Los equipos de cómputo (computadores, sitios de trabajo, servidores y demás equipos), y equipos de red que sean propiedad del Instituto Departamental de Salud se debe actualizar de manera periódica manteniendo las funcionalidades necesarias por el usuario, con el fin de aumentar la calidad de servicio, actividades y atención por cada uno de los usuarios y responsables de los equipos, aumentando su desempeño.

## 5.2 POLÍTICA PARA DISPOSITIVOS MÓVILES

**Políticas para el uso de equipos portátiles.**

La institución asigna equipos tipo portátil a sus funcionarios, para facilitarles el cumplimiento de sus labores. Los funcionarios que tengan asignado cualquier equipo tipo portátil, deben hacer correcto uso de los mismos y de la información que contienen, porque dadas las características de ese tipo de tecnología, se presentan más vulnerabilidades de seguridad, por las facilidades de conectarse diferentes ambientes informáticos, en los cuales la institución no tiene control, y adicionalmente son más susceptibles a robo o pérdida.

a) Establecer contraseñas de acceso robustas, mantener el equipo con el sistema operativo siempre actualizado y con un antivirus activo Asegurar el equipo portátil cada vez que deje de utilizarlo, en lo posible guárdelo en un lugar que cuente con unas medidas mínimas de seguridad.
b) Cada vez que descargue algún archivo a su equipo portátil, utilice siempre

la aplicación de antivirus para revisar su contenido. Normalmente el antivirus automáticamente revisa cualquier tipo de archivo. Si desea realizar un escaneo de archivos manual, podrá contactarse con la Oficina de Sistemas de Información.

c) Para reportar cualquier incidente de seguridad (ya sea virus, SPAM, otros) deberá comunicarse con la Oficina de Sistemas de Información para minimizar los daños. No reenvíe archivos desde su computador si sospecha que este pueda estar infectado, en estos casos DESCONECTE el equipo de la red de datos hasta que se le indique lo contrario.
d) Los equipos portátiles asignados a las oficinas son de uso exclusivo para los funcionarios que laboran en el IDS ya sea de planta o contratista, no es aceptable el uso de los mismos por familiares y/o amigos.
e) Evite dejar el equipo portátil con la sesión abierta. Siempre apague, bloquee (teclas Windows + L) o active el protector de pantalla con contraseña después de utilizar activamente el equipo.
f) Únicamente el personal de la Oficina de Sistemas de Información está autorizado para instalar algún tipo de software en el equipo portátil.
g) El usuario del servicio se hará responsable directo de cualquier mal uso, mientras tenga a su cargo el computador portátil y sus accesorios.
h) Todo dispositivo electrónico de almacenamiento que se conecte al equipo debe ser analizado con el antivirus inmediatamente se conecte, no es recomendable acceder al contenido sin ser previamente analizado.
i) Cuando sea necesario el traslado de los equipos portátiles ya sea en las instalaciones del instituto o fuera de ellas debe estar debidamente apagado, y en el bolso asignado. Recuerde asegurar el equipo portátil cada vez que deje de utilizarlo, en lo posible guárdelo en un lugar seguro.
j) Cuando sea necesario el traslado de los equipos portátiles fuera de las instalaciones de la Entidad debe ser registrada tanto la salida como la entrada en la portería del instituto.

**Políticas para el uso de otros dispositivos móviles**

La Entidad establece las condiciones para el uso seguro de los dispositivos móviles (teléfonos inteligentes, tabletas, entre otros) que hagan uso de servicios institucionales, para lo cual se establecen las siguientes directrices:

a) Establecer contraseñas de acceso robustas, mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.
b) Los funcionarios y contratistas no están autorizados a cambiar la configuración, ni la instalación/desinstalación de las aplicaciones móviles de los dispositivos móviles institucionales que se les entregue como recurso para la ejecución de sus obligaciones o funciones.
c) Es responsabilidad del usuario al que se le asignó el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes

inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

d) Los funcionarios y contratistas deben evitar conectar los dispositivos móviles institucionales a puertos USB de computadores públicos, hoteles o cafés internet, terminales, y demás sitios de acceso público.
e) Los funcionarios y contratistas deben notificar los dispositivos móviles institucionales con sospecha de infección por malware la oficina de Sistemas de Información de la Entidad para el proceso de análisis, evaluación y tratamiento.
f) Los dispositivos móviles que son autorizados para salir de las instalaciones por la Entidad deben ser protegidos mediante el uso e implementación de los controles apropiados como: Políticas de restricción en la ejecución de aplicaciones y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, entre otros.
g) Todos los dispositivos móviles propiedad de la Entidad pueden ser monitoreados y sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.
h) Evitar almacenar información de la Entidad que no sea estrictamente necesaria para el desarrollo del trabajo en el dispositivo móvil.
i) Eliminar la información confidencial del dispositivo móvil una vez se haga la actividad que corresponda de acuerdo al desarrollo del trabajo.
j) Mantener el registro actualizado de los dispositivos móviles de la Entidad asignados a los colaboradores, así como el registro de la instalación del software y hardware requerido por el colaborador.
k) Para los dispositivos móviles asignados por la Entidad, se debe notificar a la Oficina de Sistemas de Información la sospecha de infección por virus u otro software malicioso del equipo.
l) Al utilizar el dispositivo móvil en lugares públicos se recomienda mantenerlo siempre vigilado y en caso de robo o pérdida del equipo notificar a la Oficina de Sistemas de Información para la realización del debido proceso.
m) Desactivar en los dispositivos móviles la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no sea necesario.

## 5.3 POLITICAS PARA EL USO DE RECURSOS DE RED

El uso de Internet, impresoras y documentación se concede a los funcionarios como una herramienta que colabora y apoya en la realización de las tareas, por lo tanto cada usuario debe darle un uso apropiado a este servicio estrictamente relacionado con las labores que desempeña en la institución, cualquier uso para otros propósitos no es aceptable. El usuario deberá considerar las medidas de racionalidad y seguridad que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.

**Internet**

a) La utilización del internet se debe hacer de forma segura contando con una disponibilidad de internet compartido el cual se utiliza con fines de trabajo y no sociales.
b) El acceso a internet es de manera laboral, por la tanto queda prohibido el uso de internet para navegar en zonas restringidas y no permitidas como también queda prohibido el uso del internet para el acceso a redes sociales ya que el rendimiento del internet se puede ver afectado por estas conductas.
c) El internet se utiliza con fines de trabajo por lo tanto no se pueden hacer descargas de archivos y software, ya que esto puede afectar el rendimiento de las conexiones a internet, no se debe acceder a la visualización de páginas en línea con contenido inadecuado esto afectara el rendimiento de la computadora y la rapidez de la red.
d) Se encuentra prohibido el acceso a sitios pornográficos, sitios religiosos dedicados a difundir las creencias de alguna religión o secta en particular, acceso a sitios web de alzados en armas o de grupos terroristas a nivel nacional o internacional dedicados a difundir temas relacionados con violencia.
e) El internet inalámbrico se utiliza con el fin de dar soporte únicamente a las computadoras que no pueden tener acceso directo debido a los lugares donde se encuentran o porque los dispositivos no cuente con periféricos de red, por lo tanto, queda prohibido el compartimiento de las claves de acceso a las redes inalámbricas.
f) Los usuarios de la institución deben tener precauciones a la hora de navegar en internet debido a la existencia de software malicioso y virus que se propagan por el internet, los cuales puede ser causante de fallas en los equipos de cómputo y perdida de información.
g) Nunca hacer clic en enlaces que vengan de un remitente desconocido, aunque resulten atractivos, pues lo más seguro es que no se obtenga lo deseado y además infecte con un virus el computador.
h) Al entrar en páginas donde se deba facilitar datos confidenciales, se deben asegurar de acceder con protocolo https, la "s" del final significa Secure (segura) y la transmisión de la información irá cifrada.
i) Comprobar que en el navegador aparece un candado que nos asegure la validez del certificado y que este no ha caducado.
j) Verificar los dominios o links de las páginas web en caso de recibir mensajes de entidades bancarias o ente gubernamental
k) No abrir banners publicitarios

**Seguridad de las Comunicaciones**

La Entidad debe asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de soporte, para lo cual se

establecen las siguientes directrices:

a) La Oficina de Sistemas de Información debe implementar tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red como por ejemplo un firewall de seguridad perimetral.

b) La Oficina de Sistemas de Información realiza el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso de servidor proxy, firewall o control que mejor se ajuste a la necesidad.

c) La Oficina de Sistemas de Información implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Entidad.

d) La Oficina de Sistemas de Información debe aplicar un método para gestionar la seguridad de las redes dividiéndola en dominios de red separados, por ejemplo: Red de dominio de acceso público y red de dominio de computador de escritorio, dominio de servidor), junto con unidades organizacionales (por ejemplo, recursos humanos, finanzas, mercadeo) o alguna combinación (por ejemplo, un dominio de servidor que se conecta a múltiples unidades organizacionales). La separación se puede hacer usando diferentes redes físicas o diferentes redes lógicas (por ejemplo, redes privadas virtuales).

e) No se deben dejar mensajes que contengan información confidencial, en las máquinas contestadoras, ya que éstos pueden ser escuchados por personas no autorizadas, o almacenados incorrectamente como resultado de una marcación incorrecta.

f) La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del activo tipo información involucrada.

g) La Entidad asegura la protección de las redes y la transferencia de información. Para dar cumplimiento se deben firmar acuerdos de confidencialidad y de no divulgación entre la Entidad y entidades externas con las cuales se intercambie información e implementar controles de seguridad al monitoreo de la red.

**Impresoras**

a) Evitar dejar documentos en cola, al haber varios imprimiéndose pueden causar una saturación de las tareas de la impresora.
b) Con las impresoras multifuncionales se debe tener precaución a la hora de enviar documentos a ser escaneados debido a que se debe escoger el

equipo en el cual debe quedar el documento escaneado.

c) Verificar que tanto la impresora como el equipo a la cual se encuentre conectada esté encendido o tenga el cable de red conectado de manera correcta para que su funcionamiento sea el más óptimo.

**Documentación**

a) Precaución de hacer buena utilización de la documentación, debido a que esa documentación es de apoyo y de trabajo de varias personas.

b) Precaución al guardado de una copia de la documentación de forma local, la cual nos ayudara y será de fortaleza si pasa algo o la red no funciona de manera adecuada.

c) Precaución a la hora de compartir documentación en la red en la cual se debe seleccionar los beneficiados para que no sea compartida con todos los usuarios ya que para todos no son de utilidad y pueden generar pérdidas o suministración de documentación a terceros.

d) Precaución a la hora de hacer el guardado de la documentación si está siendo utilizada de forma remota por varias personas las cuales pueden hacer modificación y las cuales no pueden ser guardadas por acciones de otro usuario que la esté trabajando y niegue su guardado.

## 5.4 POLITICA DE CONTROL DE ACCESO

El Instituto Departamental de Salud asigna a cada funcionario en apoyo al cumplimiento de sus labores dando acceso a equipos informáticos, a la red de datos institucional y a documentación, con la cual el empleado puede acceder diferentes elementos que la componen como: servidores de archivos, servidores de bases de datos, impresoras, archivos compartidos en otras estaciones de trabajo, sistemas y aplicaciones Institucionales, entre otros. Por lo anterior, los empleados deben hacer uso de la red y de los servicios relacionados con esta, estrictamente en cumplimiento de las labores institucionales, tomando en consideración la privacidad de otros usuarios y la no saturación de la red por uso indebido del ancho de banda, ningún empleado está autorizado para crear claves, cuentas de usuario, instalar programas y realizar modificaciones a los equipos sin autorización de la persona encargada de la oficina de sistemas de información.

**Sistema Gestión de contraseñas**

Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas. Los usuarios deben cumplir las prácticas de la entidad para el uso de información de contraseñas que se relacionan a continuación:

a) Mantener la confidencialidad de la información de contraseña, asegurándose de que no sea divulgada a ninguna otra parte, incluidas personas externas a la entidad y personal de otras dependencias de la institución no autorizadas

b) Evitar llevar un registro (en papel, en un archivo de software o en un

dispositivo portátil) de contraseña, a menos que se pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado (una bóveda para contraseñas)
c) cambiar la información de contraseña siempre que haya cualquier indicio de que se pueda comprometer la información
d) Se debe seleccionar contraseñas seguras con una longitud mínima suficiente que:

- sean fáciles de recordar;
- no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.);
- no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios);
- estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos;
- si son temporales, cambiarlos la primera vez que se ingrese;

e) No compartir información de contraseña del usuario individual
f) Establecer una protección apropiada de contraseñas cuando se usan éstas como información de contraseña en procedimientos de ingreso automatizados, y estén almacenadas
g) No usar la misma información de contraseña para propósitos de negocio y otros diferentes de estos
h) El sistema debe restringir los tiempos de conexión para brindar seguridad adicional para aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.

**Control de acceso a equipos informáticos**

a) Todos los equipos de cómputo tienen asignado un responsable y un usuario, debe cumplir con la responsabilidad de darle buen uso y funcionamiento a los equipos.
b) Los equipos de cómputo que se encuentren en áreas críticas donde sea de fácil acceso deben tener un seguimiento y deben poseer su respectiva seguridad.
c) Los cuartos de Rack son áreas donde se encuentren los equipos imprescindibles para el funcionamiento y trabajo en los departamentos del instituto, el cual, se encuentra restringido el acceso a los funcionarios ajenos a la Oficina de Sistemas de Información.
d) El servidor de datos, es para almacenamiento de documentos institucionales, estos archivos deben ser productos de las funciones del personal o sirvan como apoyo para la ejecución de dichas funciones.
e) Las impresoras no son para uso personal, se prohíbe la impresión total o parcial de información ajena al Instituto Departamental de Salud.
f) Los equipos con acceso a la red institucional e internet no podrán usar el ancho de banda para ver videos, escuchar música o acceder a redes sociales, ya que el uso del internet es estrictamente necesario para cumplir las labores del cargo.

g) Las diversas páginas web que funcionan como redes sociales, tienen contenido de video, música o contenido para adulto, están estrictamente restringidas.
h) Está restringido el uso de programas de descarga de contenido audiovisual (música, videos, fotos) y software, que no apoye desarrollo de las funciones laborales para cumplir la misión de la institución.

**Control de acceso a la red local**

a) La Oficina de Sistemas de Información es responsable de dar acceso a un punto remoto, en el cual es asignada una dirección IP dentro del rango de direcciones que el instituto tiene para ofrecer conectividad a internet y recursos compartidos.
b) Los usuarios deben hacer utilización de la red local de manera adecuada (no acceder a información ajena y no utilizar recursos de red que no estén permitidos) para que el funcionamiento y la realización de las tareas sean las mejores.
c) La Oficina de Sistemas de Información es el encargado de visualizar y realizar prevención del buen uso de la red.
d) El acceso a los equipos de cómputo especializados como servidores y equipos de red se deben hacer por medio del personal autorizado por la Oficina de Sistemas de Información.
e) Los equipos que son del instituto y sean conectados a la red local, o aquellos que sean conectados a la red inalámbrica debe hacer uso de la misma de manera responsable y con la mejor de las disposiciones para el buen funcionamiento de las redes.
f) El acceso a la red institucional deberá realizarse por medio del dominio IDS con su respectivo usuario y contraseña, los cuales son asignados por el área de sistemas a cada equipo teniendo en cuenta el procedimiento de Ingreso de un nuevo equipo a la red institucional.
g) Los equipos personales que requieran el acceso a la red institucional, debe ser solicitado a la Oficina de Sistemas de Información por medio del formato de solicitud de servicio interno.

**Control de acceso a la documentación**

**a)** El control de acceso a la documentación que es compartida en red se debe hacer de manera segura y con precauciones de guardar una copia en el equipo del usuario.
**b)** La documentación que se encuentre en red se debe compartir con los usuarios beneficiados, la cual, hace parte de sus actividades de trabajo con restricción de acceso a personas ajenas a las actividades que en esta documentación se emplean.
**c)** La información que se encuentre en la red se debe proteger y utilizar solo con fines laborales, no con fines personales ni de lucro, ni transferir a

terceros, los cuales podrían utilizar la información con otros fines como dañar la institución.

**d)** Se considera falta gravísima al detectar los usuarios que vulnere la información contenida en los equipos de cómputo o en la red institucional como borrar carpetas compartidas o no autorizadas.

**Seguridad Física y del Entorno**

La Entidad debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información del Instituto Departamental de Salud de Norte de Santander, para lo cual se establecen las siguientes directrices:

a) Las oficinas administrativas, áreas de procesamiento de información, equipos tecnológicos y de soporte, información de medios físicos entre otros, son base para el cumplimiento de los objetivos de la Entidad, por tanto, se deben establecer y mantener controles para resguardar la seguridad de las instalaciones y ambientes de trabajo, el acceso a las áreas, y demás que procesen información.

b) Los equipos de cómputo que pasen a un estado de retiro o se requieran para la reutilización deberán cumplir los siguientes lineamientos: -Al momento de retirar un equipo en la organización (almacén), el funcionario a cargo del activo, realiza la copia de respaldo de la información almacenada. En el caso de presentarse falla en la realización del proceso, debe enviar al correo sistemasdeinformacion@ids.gov.co la solicitud de apoyo para realización de la misma. -La Oficina de Sistemas de Información realiza el proceso de borrado seguro de la información almacenada en los equipos que van a ser cedidos o reutilizados en la organización.

c) Los funcionarios y contratistas, deben procurar que no se disponga información de la Entidad en los escritorios de los equipos y que esta no estará almacenada y fácilmente copiada o accedida por alguien sin autorización desde un computador desatendido.

d) Para todos los usuarios de las aplicaciones y sistemas de información de la Entidad, es obligatorio que las sesiones sean cerradas al finalizar las actividades y no se deben dejar abiertas o desatendidas.

e) Todos los visitantes, sin excepción, deben registrar su ingreso y salida en la Recepción de la entidad indicando su documento de identidad y la dependencia a la cual se dirige. El personal de Recepción verificará telefónicamente, con la dependencia indicada, que el visitante está autorizado para permanecer dentro de las instalaciones de la Entidad.

f) Las áreas dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

## 5.5 POLÍTICA PARA USO DE SOFTWARE

**Instalación del Software**

**a)** Los usuarios no pueden instalar, suprimir o modificar el software

originalmente entregado en su computador. Es competencia de la Oficina de sistemas de Información.

**b)** Es responsabilidad de la oficina de sistemas de información dar a conocer las bases y los tipos de software que se deben instalar.

**c)** Las cualidades y características del software que se debe instalar en los equipos de cómputo del Instituto deben cumplir con características de soporte para las actividades de desempeño laboral y contar con un licenciamiento.

**d)** En la instalación de software nuevo en los equipos de cómputo la Oficina de Sistemas de Información deben tener estudio pleno y responsabilidad en la instalación ya que puede estar en riesgo tanto la información de trabajo del usuario, también es responsabilidad del usuario realizar las respectivas copias de seguridad de la información.

**e)** Sistemas de Información es el responsable de la instalación de software de seguridad de los equipos de cómputo como los son antivirus, vacunas, privilegios de acceso y otros software que ayuden con la protección del equipo información del usuario. Al no contar con licencia de antivirus se instalarán software libre, el cual no tiene costo ni restricciones.

**f)** La seguridad lógica y física de los equipos compete al funcionario a quien es asignado el equipo.

**g)** Compete al usuario hacer uso propio del software instalado solo con fines laborales, no con fines de lucro personal como también es de responsabilidad dar a conocer novedades que se presenten con el software instalado a la Oficina de Sistemas de Información.

**Actualización del Software**

a) La actualización y adquisición de nuevos software para los equipos de cómputo es de responsabilidad de la Oficina de Sistemas de Información por lo tanto queda prohibido la actualización de software sin previo aviso.

b) Está prohibido la intervención de personal ajeno a la Oficina de Sistemas de Información para realizar instalación o actualizaciones de software.

c) Sistemas de Información deberá hacer seguimiento al software instalados en los equipos de cómputo.

d) Si se presenta una actualización o una notificación del equipo de cómputo al usuario para hacer actualización es de suma responsabilidad del usuario comunicarse con la Oficina de Sistemas de Información para que sea guiado y apoyado para la respectiva actualización.

**Software Legal**

**a)** Los computadores se deben adquirir con la respectiva licencia del Sistema Operativo.

**b)** Es responsabilidad del usuario hacer uso de software legal y con su respectiva licencia.

**c)** Le corresponde al usuario informar y dar a conocer sobre el vencimiento de las licencias del software que posee el equipo de cómputo.

**d)** El usuario es responsable de todo software instalado sin autorización de la Oficina de sistemas de información, como también de las consecuencias que cause la instalación de software ilegal y con virus.

**e)** Se debe informar al Almacén cuando se ha terminado la vida útil del software o la licencia haya caducado y no se actualiza para que sea tenido en cuenta en el Comité para dar de baja al bien intangible.

**Uso de plataformas de Software**

a) Cualquier software que sea de uso institucional debe ser instalado por la Oficina de Sistemas de Información.

b) El software que se usa institucionalmente y que es manipulado por los usuarios, deben hacer utilización del software de manera exclusiva para las labores y actividades trabajo de la institución.

c) El software que requieran ser instalados para el trabajo en red de la institución debe ser evaluado con anticipación como también la capacitación en la utilización a los usuarios.

d) Es responsabilidad del usuario realizar buenas practicas con el software que posee la institución con el fin de aprovechar los beneficios y riquezas que ofrecen el software.( Consultar los manuales de usuario)

e) Se debe dar a conocer por parte de los usuarios a la Oficina de Sistemas de Información las fallas y no funcionamiento correcto de software.

Mecanismo de control de Software

a) Los equipos de la entidad hacen parte de un dominio, y desde el servidor de usuarios, se establecen políticas de seguridad y listas de controles de acceso a sitios web.

b) Perfiles de usuarios con acceso restringido para la instalación y desinstalación de software.

c) Los programas o aplicaciones que los usuarios requieren son instalados por el personal que hace parte de la Oficina de Sistemas de Información.

d) Verificación aleatoria de software instalado en los equipos de las diferentes dependencias u oficinas, en caso de existir software no licenciado se procede a la desinstalación del mismo.

e) Se da instrucciones a los funcionarios sobre el uso del hardware y software, enfatizando en la responsabilidad y consecuencias que conlleva la instalación de software no licenciado.

## 5.6 POLÍTICA USO DE UNIDADES DE ALMACENAMIENTO DE INFORMACIÓN

La información constituye uno de los principales activos de la institución, por tanto el manejo adecuado de la misma es responsabilidad de todos los funcionarios así como

la correcta utilización de los dispositivos que el mercado ofrece para la administración y respaldo información. Por lo tanto, todos los usuarios de tecnologías de información que manipulen dispositivos de almacenamiento deben utilizarlos considerando la importancia de la información que contienen, buscando mecanismos seguros para su almacenamiento o distribución

Teniendo en cuenta la importancia de la información que maneja la institución y la necesidad de resguardar los datos, así como emitir información a otras entidades, surge la necesidad de establecer la normativa para regular el uso de cualquier tipo de unidades de respaldo sean estas internas o externas, entre las que podemos mencionar los quemadores de discos compactos, DVD, memorias USB, Disco Duros interno y externos, almacenamiento en la nube, entre otros; con el objeto de que su uso sea para labores propias de la institución.

Por lo anterior, toda unidad que cuente con dispositivos para la realización de respaldos (computadoras de escritorio, portátiles y servidores) debe velar porque se haga un uso adecuado de esos recursos, utilizándolos únicamente para cumplir con los intereses de la institución, y tomando en cuenta las funcionalidades operativas del equipo.

a) No se permite realizar copia no autorizada de material protegido por derecho de autor.
b) No se permite almacenar información de índole personal como videos, fotos, música entre otros, en los equipos institucionales ni equipos servidores.
c) No se permite modificar, eliminar o copiar un archivo perteneciente a otro Usuario sin el previo consentimiento del dueño del archivo.
d) Todo archivo de índole personal que se encuentre en el servidor de datos, será borrado inmediatamente sin previa autorización.

**Organización de la información en un equipo de cómputo**

a) Sistemas de Información debe crear en los computadores dos particiones. La primera corresponderá al lugar en el cual se instalará el Sistema Operativo, la segunda corresponderá al lugar en el cual se guardará la información del usuario, aunque esto no garantiza la permanencia de la información ni tampoco sea una regla que se deba tener en los computadores, si se facilitan las cosas a la hora de hacer una restauración del computador por daño en el Sistema Operativo
b) El usuario debe guardar toda la información generada en la partición creada por la Oficina de Sistemas de Información, en dado caso, que el equipo no cuente con dicha partición, el usuario deberá crear una carpeta con el nombre del equipo, en el disco local C y guardar toda la información en dicha carpeta.

**Nombre de los archivos**

a) Se recomienda no guardar archivos con nombres muy largos. Es de vital importancia a la hora de realizar una copia de seguridad, pues en ocasiones, los archivos que tienen nombres muy largos ocasionan problemas y no

permiten su manipulación.

b) Es importante nombrar los archivos con nombres que permitan reconocer el contenido. Con el fin de evitar la revisión de todos los archivos que están en el computador abriéndolos, sino que simplemente se pueda limitar a leer el nombre del archivo, y con esto tomar la decisión si se guarda o se elimina.

c) Tener en cuenta que algunos Sistemas Operativos no permiten ingresar unos caracteres especiales al nombre del archivo, por tanto, se sugiere no nombrar archivos o carpetas utilizando caracteres especiales como (#$%&?¡'¿).

**Organización de los Archivos**

a) Se recomienda llevar control y orden de los archivos, con el fin de aprovechar el espacio del equipo de cómputo y facilitar la búsqueda de información.

b) No se recomienda crear demasiadas subcarpetas, ya que al momento de realizar copias de seguridad el sistema operativo incluye la ruta del archivo como si formara parte del nombre del archivo.

c) Grabar cambios de archivos frecuentemente. Al trabajar con documentos de texto, planillas de cálculo u otro archivo, se recomienda guardar los cambios frecuentemente para evitar pérdida de los avances frente a un apagado inesperado del equipo. En lo posible, utilizar versiones de los archivos en la medida que se generan modificaciones en ellos.

**Almacenamiento en la nube**

a) La Oficina de Sistemas de Información da a conocer, a los funcionarios y contratistas, que en la actualidad la institución, mediante alquiler de hosting corporativo incluida plataforma GSuite, dispone de un almacenamiento en la nube de 2TB por cuenta asignada a las dependencias para la gestión documental virtual.

b) La Oficina de Sistemas de Información da conocer a los funcionarios y contratistas los pasos a seguir para un adecuado borrado de la información contenida en los repositorios en la nube.

## 5.7 POLÍTICA DE COPIAS DE SEGURIDAD

La realización periódica de respaldos de la información generada en los sistemas, bases de datos, así como la información residente en los equipos de los funcionarios del Instituto Departamental de Salud de Norte de Santander, es de gran importancia para brindar continuidad de los servicios. Por lo tanto, todos somos responsables de su preservación.

a) Cada funcionario debe salvaguardar la información que se encuentra bajo su responsabilidad, realizando copia de seguridad una vez por semana de los archivos indispensables para el funcionamiento del instituto.

b) Sistemas de Información realiza copias de seguridad de la información contenida en la carpeta destinada para tal fin en la red institucional: \\SERVIDORUSER\DependeciasIDS
c) Sistemas de Información define anualmente un cronograma de pruebas de restauración que permita validar la integridad y disponibilidad de la información almacenada, garantizando la confiabilidad del proceso ejecutado para copias de respaldo.

## 5.8 POLÍTICA DE USO DE TELEFONIA IP

Las tres sedes del Instituto Departamental de Salud de Norte de Santander: Principal, Laboratorio Departamental de Salud Pública y Control de Vectores se encuentra interconectada con la misma central telefónica IPPBX, utilizando la tecnología VoIP que permite realizar llamadas telefónicas a través de la conexión de Internet.
Se deben tener en cuenta las siguientes consideraciones:

a) Los teléfonos IP deben estar conectados a la red de datos y al estabilizador de energía.
b) Las llamadas locales son ilimitadas, las cuales, se marca el número directamente.
c) Las llamadas locales extendidas y a móviles celulares son para extensiones autorizadas; las cuales, se marca el número directamente.
d) Las llamadas larga distancia nacionales son para extensiones autorizadas, marcando 08+indicativo+número
e) Grupo de extensiones: Las oficinas que cuenten con más de una extensión puede tomar la llamada de cualquier extensión, marcando *8
f) Las oficinas con teléfonos digitales cuentan con mensajería de voz.
g) Transferencia de llamadas entre extensiones: De acuerdo al teléfono instalado debe realizar la siguiente operación:
    a. Teléfono tradicional: flash + extensión + #
    b. Teléfono GRANDSTREAM: + extensión + transferir
h) Teniendo en cuenta la importancia de satisfacer tanto los requisitos del cliente como los legales, según Numeral 5.5.3 Comunicación Interna de la NTC-GP 1000:2009 se debe asegurar que la comunicación se efectúa considerando la eficacia, la eficiencia y la efectividad del Sistema de Gestión de la Calidad, por tal motivo, deberán actualizar los datos del número telefónico de la IP-PBX establecidos en los pies de página de los registros establecidos en el Sistema Integrado de Gestión de la Entidad.

## 5.9 POLITICA DE USO DE CORREOS ELECTRONICOS

Se debe tener en cuenta los siguientes lineamientos para el uso del correo electrónico institucional del Instituto departamental de Salud de Norte de Santander:

a) Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Código de

Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

b) Toda información institucional que se quiera comunicar a través de correo electrónico, se debe hacer a través de las cuentas de correo institucionales asignadas a las dependencias u oficinas o el correo institucional de la alta dirección.
c) El sistema de correo electrónico institucional debe ser usado únicamente para propósitos laborales.
d) El servicio de correo electrónico de la Institución no debe ser utilizado para enviar correo Spam (basura digital).
e) Es necesario crear una rutina diaria de limpieza de correos leídos, los cuales, deben ser archivados de acuerdo a la TRD institucional; esto es de vital importancia para su correcto funcionamiento.
f) Si desea almacenar los correos de una cuenta institucional configurada como alias o contar con un backup (copia) de los mismos, es necesario hacer el redireccionamiento de la cuenta a una cuenta externa, ya sea (gmail, hotmail, yahoo u otra), la solicitud la puede realizar a la oficina de sistemas de información o por correo electrónico sistemas@ids.gov.co
g) Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar los lineamientos y recomendaciones para dicho tipo de documentos, tales como:
    - ✓ Iniciar su correo con un saludo formal.
      Ejemplo: Buenos días o Doctor Julián. Cordial saludo.
    - ✓ Nombrar al destinatario de correo por su nombre o profesión.
    - ✓ Evitar el uso de palabras que puedan resultar ofensivas.
    - ✓ Escribir puntualmente.
    - ✓ No extenderse demasiado.
    - ✓ Al final del correo agradecer por la atención prestada y firmar. La firma debe contener nombre y apellidos completos, cargo dependencia, nombre completo de la entidad, dirección de la oficina, teléfono de contacto, correo electrónico.
h) Los usuarios del correo electrónico institucional no deben enviar mensajes personales u ofensivos; mensajes cadenas o mensajes que se relacionen con actividades ilegales y no éticas, o que atenten contra el buen nombre de la Institución.
i) Los correos institucionales no deben ser inscritos en ninguna página para acceder a información en la web, ya que estas páginas usan los correos para enviar correos Spam o publicidad.
j) Los usuarios no deben utilizar una cuenta de correo electrónico que pertenezca a otra dependencia o línea. En caso de ausencias o vacaciones,

se debe recurrir a la Oficina de Sistemas de Información como mecanismo alterno para el envío de correos.

k) No abrir correos electrónicos de remitentes desconocidos, sin asunto, o cuyo asunto resulte sospechoso.

l) No abrir archivos adjuntos o links desconocidos que envíen a través de correo electrónico.

## 5.10 POLITICA DE USO PARA FIRMAS DIGITALES

En caso que algún funcionario cuente con firma digital para fines institucionales debe tener en cuenta:

a) Utilizar la clave privada y el certificado digital emitido tan sólo para los fines establecidos y de acuerdo con los condicionamientos establecidos en el contrato celebrado.

b) Será responsabilidad del funcionario el uso indebido que éste o terceros hagan del mismo.

c) Responder por la custodia de la clave privada y de su soporte físico (si aplica) evitando su pérdida, revelación, modificación o uso no autorizado. Especialmente, el suscriptor deberá abstenerse, sin importar la circunstancia, de anotar en el soporte físico del certificado digital el código de activación o las claves privadas, ni tampoco en cualquier otro documento que el suscriptor conserve o transporte consigo o con el soporte físico.

d) Solicitar la revocación del certificado digital que le ha sido entregado cuando se cumpla alguno de los supuestos previstos para la revocación de los certificados digitales.

e) Abstenerse en toda circunstancia de revelar la clave privada o el código de activación del certificado digital, así como abstenerse de delegar su uso a terceras personas.

f) Asegurarse de que toda la información contenida en el certificado digital es cierta y notificar inmediatamente a Sistemas de Información en caso de que se haya incluido cualquier información incorrecta o inexacta o en caso de que por alguna circunstancia posterior la información del certificado digital no corresponda con la realidad. Asimismo, deberá comunicar de manera inmediata el cambio o variación que haya sufrido cualquiera de los datos que aportó para adquirir el certificado digital, aunque éstos no estuvieran incluidos en el propio certificado digital para realizar el respectivo reporte a la empresa contractual.

g) Se deberá notificar de inmediato la pérdida, robo o falsificación del soporte físico y cualquier intento de realizar estos actos sobre el mismo, así como el conocimiento por otras personas del código de activación o de las claves privadas, solicitando la revocación del certificado digital.

h) Abstenerse de monitorear, alterar, realizar ingeniería inversa o interferir en cualquier otra forma la prestación de servicios de certificación digital.

i) Conservar el dispositivo de firma digital en un lugar seguro.

j) No digitar la clave más de tres veces de manera errada, ya que se bloquea el dispositivo, lo que conlleva a un proceso de reingreso que tiene un costo que será asumido por el funcionario.

k) En caso de olvidar la clave, implica el reingreso del certificado digital que tiene

un costo que será asumido por el funcionario.

## 5.11 POLITICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

La Entidad establece directrices para asegurarse que los funcionarios y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad de la información, para lo cual se establecen las siguientes directrices:

a) El área que realiza la contratación de personal en el Instituto departamental de Salud de Norte de Santander debe realizar las verificaciones de los antecedentes (procuraduría, contraloría, policía) de los candidatos al cargo, la formación académica, experiencia y demás información que se requiera, de acuerdo a las leyes, reglamentos de la Entidad y ética pertinente.
b) Todo funcionario y contratista debe recibir inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Entidad.
c) La Entidad establece directrices a través de la oficina de sistemas de información para que los funcionarios y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad y privacidad de la información.
d) Todos los funcionarios y contratistas deben firmar un acuerdo de confidencialidad y no divulgación, donde se especifiquen la responsabilidad con el acceso y gestión de la información confidencial, de datos personales, derechos de autor, entre otra que tenga implicaciones legales.
e) Se debe especificar en el proceso de contratación las sanciones que conlleva el uso indebido de la información de la Entidad y Comunicar a los funcionarios y contratistas las obligaciones que deben cumplir con la información del Instituto departamental de Salud de Norte de Santander al finalizar el contrato o relación laboral.
f) El incumplimiento o la violación de las políticas de seguridad de la información de la Entidad, por parte de los Colaboradores o Terceros, se les aplicará lo establecido en el proceso de investigaciones disciplinarias.

## 5.12 POLITICA DE GESTIÓN DE ACTIVOS

La Entidad debe desarrollar estrategias de trabajo para optimizar el uso de los recursos de seguridad, establecer los métodos de identificación clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades y manteniendo mecanismos acordes par el control de riesgos de la información, para lo cual se establecen las siguientes directrices:

a) Cada activo de información del Instituto departamental de Salud de Norte de Santander debe tener un responsable que debe velar por su seguridad. Los propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y requerimientos legales de retención.
b) La Entidad debe establecer los niveles de clasificación de la información de acuerdo a la normatividad Legal Colombiana y brindar protección a la información de acuerdo con su importancia para la organización.
c) Es responsabilidad de la dependencia de Planeación y Sistemas de

Información la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.

d) Todos los activos de información deben contar con un responsable, que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.

e) Los funcionarios y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Entidad.

## 5.13 POLÍTICA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El Instituto Departamental de Salud propende porque la Seguridad de la Información sea parte integral de los sistemas de información dentro del ciclo de vida de desarrollo de los sistemas de información y en la adquisición de aquellos que presten servicios a la Entidad, para lo cual se establecen las siguientes directrices:

a) Se establece el procedimiento de desarrollo seguro de software, la revisión técnica y de seguridad de las aplicaciones para detectar vulnerabilidades antes de salir a producción y la aplicación del procedimiento gestión de cambios.

b) La Entidad garantiza que los sistemas de información estén asociados a lineamientos, procesos, buenas prácticas y demás requisitos que sirvan para regular los desarrollos de software internos en un ambiente controlado, así mismo se identifican y gestionan los posibles riesgos referentes a seguridad de la información durante todo el ciclo de vida del software.

c) La Entidad asegura que se diseñe e implemente los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.

d) La Entidad establece controles técnicos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.

e) La Entidad exige al proveedor mediante los contratos, que éste cuente con los controles de seguridad de la información sobre los ambientes de desarrollo y de pruebas.

f) Los datos de pruebas que se utilicen durante todo el ciclo de vida de los sistemas de información deben ser seleccionados, utilizados y eliminados de forma segura.

## 5.14 POLITICA DE RELACIONES CON LOS PROVEEDORES

La Entidad debe controlar que toda relación con proveedores, y en particular aquellos que tienen acceso a la información, está suficientemente protegida, para lo cual se establecen las siguientes directrices:

a) Para proveedores críticos de tecnología, así como de procesos misionales, la Entidad exige que cuente con planes de continuidad de negocio y recuperación de desastres definidos e implementados, de modo que proveedor contratado puedan responder ante eventuales escenarios que afecten el suministro de servicios o productos a la Entidad.
b) La protección de la información, debe contemplarse antes, durante y a la finalización del servicio. Para dar este cumplimiento se deben establecer cláusulas contractuales en materia de seguridad y privacidad de la información y determinar qué controles de seguridad son de obligatorio cumplimiento en las relaciones los proveedores de servicios tecnológicos.
c) Cualquier cambio que se realice con algún proveedor crítico de TI o de los procesos misionales, debe aplicarse mediante el procedimiento de gestión de cambios establecido en la Entidad.
d) La Entidad realiza revisiones periódicas al cumplimiento de las Políticas de Seguridad y Privacidad de la Información a los Proveedores.

## 5.15 POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD

La Entidad debe asegurarse que todos los colaboradores conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información, para lo cual se establecen las siguientes directrices:

a) Para reportar cualquier incidente de seguridad el funcionario o contratista deberá comunicarse con la Oficina de Sistemas de Información, enviando correo a sistemasdeinformacion@ids.gov.co, para registrar el incidente con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.
b) Todos los funcionarios y contratistas deben conocer el método de reporte de eventos e incidentes de seguridad de la información
c) En la gestión del incidente y cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables o comunicar a un ente competente para que realice el debido proceso.
d) La Entidad establece y ejecuta procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.
e) La Entidad debe establecer y poner a disposición de los colaborados el formato o mecanismos de reporte de eventos e incidentes de seguridad y privacidad de la información.
f) La Oficina de Sistemas de Información debe llevar en una bitácora el registro de los incidentes de seguridad de la información reportados y atendidos y el establecimiento de indicadores relacionados a la gestión de los incidentes de seguridad y privacidad de la información.

## 5.16 POLITICA DE CUMPLIMIENTO

La Entidad gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente, para lo cual se establecen las siguientes directrices:

a) Se debe analizar los requisitos legales aplicables a la información, incluyendo los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros y los delitos informáticos y brindar los lineamientos que permitan dar cumplimiento a la normatividad legal.
b) La Entidad asegura el conocimiento y cumplimiento de las obligaciones legales en materia de seguridad de la información. Por lo anterior, garantiza el cumplimiento de los derechos de propiedad intelectual de terceros controlando la adquisición y uso del software en la Entidad. Debe determinar las responsabilidades para gestionar la protección de datos personales.
c) La Entidad propende por la implementación de medidas de seguridad y privacidad de la información con el fin de asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.

## 6. SENSIBILIZACIÓN Y COMUNICACIÓN

### 6.1. TOMA DE CONCIENCIA

Brindar lineamientos para que los servidores públicos, contratistas y proveedores de la Entidad reciban la educación y formación en toma de conciencia adecuada, y actualizaciones sobre las políticas de seguridad y privacidad de la información.
La Oficina de Recursos Humanos y el supervisor del contrato, deberán velar por que los servidores públicos, contratistas y proveedores de la Entidad, que desempeñen funciones en el mismo reciban entrenamiento y actualización periódica en materia de Seguridad de la Información.
Será responsabilidad de Recursos Humanos, incorporar la aplicación de las políticas de seguridad de la información en su plan de capacitación institucional, y velar por la correcta inducción de los funcionarios nuevos en materia de seguridad de la información.

### 6.2. COMUNICACIÓN

El Instituto Departamental de Salud de Norte de Santander establece para la comunicación permanente de todas las políticas, procedimientos u otros documentos que hagan parte del Modelo de Seguridad y Privacidad de la Información (MSPI), los siguientes canales accesibles y formales: Correo Electrónico, página web institucional, comunicación impresa, charlas y capacitaciones. El presente manual de políticas de Seguridad y Privacidad de la Información, será comunicado a todas las partes interesadas de la Entidad.
Todas las políticas, procedimientos y demás documentos relacionados con la seguridad y privacidad de la información serán publicados en la página web institucional https://ids.gov.co/web/
Será responsabilidad de Recursos Humanos, incorporar la aplicación de las políticas de seguridad de la información en su plan de capacitación institucional, y velar por la correcta inducción de los funcionarios nuevos en materia de seguridad de la información.
La periodicidad para el desarrollo de actividades está establecida en el plan de comunicaciones de seguridad y privacidad de la información de la entidad.

## 7. EVALUACIÓN DEL DESEMPEÑO

### 7.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

El Instituto Departamental de Salud de Norte de Santander, debe asegurar que la seguridad y privacidad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales, para lo cual se establecen las siguientes directrices:

Seguimiento de tareas, actividades o acciones asignadas en reuniones de comités donde se traten los temas de seguridad y privacidad de la información.

Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y demás normas de seguridad y privacidad de la información.

Generación de Informe de resultados de las revisiones del Modelo de Seguridad de la Información al interior de los procesos.

Seguimiento y presentación de los resultados del último ciclo de auditoría interna al MSPI (informe de Auditoría Interna).

Realizar los cambios en las cuestiones internas y externas que sean pertinentes al MSPI.

Analizar propuestas o mejoras al MSPI por parte de los servidores públicos y contratistas.

Estado de acciones correctivas y de mejora (se evalúa la eficacia de las acciones), para seguridad y privacidad de la Información sólo aplican las acciones correctivas y de mejora.

Gestionar obtener la realimentación de las partes interesadas, respecto a la implementación de seguridad y privacidad de la información.

Gestionar, analizar y documentar los resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos.

Identificar las vulnerabilidades y amenazas no tratadas adecuadamente en la valoración previa de los riesgos.

Revisión y actualización anual en caso de que aplique de la política general, la revisión de las políticas específicas de seguridad, de objetivos de Seguridad de la Información (su contenido y cumplimiento en los diferentes procesos) por medio de planes de acción.

### 7.2. REVISIÓN POR LA DIRECCIÓN

La dirección debe revisar el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Entidad a intervalos planificados, ya que se tiene que asegurar la idoneidad, la adecuación, la eficiencia y la alineación continua con los objetivos estratégicos de la Entidad, la revisión por la dirección tiene que planificarse y realizarse una vez al año el análisis de los resultados de la Evaluación y Desempeño.

## GLOSARIO

**Accidente: Es un suceso repentino no deseado que produce consecuencias negativas ya sea en las personas, las instalaciones, las máquinas o el proceso.**

**Administrador**: Esla persona o programa encargado de gestionar, realizar el control, conceder permisos, etc. de todo un sistema informático o red de ordenadores

**Almacenamiento en la nube. o** almacenamiento cloud. Es un almacenamiento fuera del sitio que mantiene un tercero. El almacenamiento en la nube guarda los datos de manera segura en una base de datos remota para no guardar tus datos y archivos en el disco duro del computador ni en otro dispositivo de almacenamiento.

**Ancho de banda**: Máxima cantidad de datos que pueden pasar por un camino de comunicación en un momento dado, normalmente medido en segundos. Cuanto mayor sea el ancho de banda, más datos podrán circular por ella al segundo.

**Computador:** Es un dispositivo de computación de sobre mesa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU.

**Contraseña:** Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).

**Dominio:** El conjunto de computadoras conectadas en una red que confían a uno de los equipos de dicha red, la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.
**Equipo personal:** Se entiende como equipo personal todo equipo perteneciente a un dueño diferente al Instituto Departamental de Salud de Norte de Santander.
**Incidente:** Es un suceso repentino no deseado que ocurre por las mismas causas que se presentan los accidentes, sólo que por cuestiones del azar no desencadena lesiones en las personas, daños a la propiedad, al proceso o al ambiente.

**Firma Digital:** es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad).

**Mensaje de Datos:** La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

**Periféricos:** Es la denominación genérica para designar al aparato o dispositivo auxiliar e independiente conectado a la CPU de una computadora.

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

**Proveedor:** Toda persona natural o jurídica que proporciona materia prima para el desarrollo de las actividades de la Entidad

**Red:** Conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

**Servidor:** Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

**Software:** Todos los componentes no físicos de un PC (Programas).

**Spam:** Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

**Usuario:** Toda persona, funcionario (empleado, contratista, temporal), que utilice los sistemas de información de la empresa debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

**Virus:** Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar serios problemas a los sistemas infectados. Al igual que los virus en el mundo animal o vegetal, pueden comportarse de muy diversas maneras. (Ejemplos: caballo de Troya y gusano).

**Visitante:** Toda aquella persona que ingresa a las instalaciones de la Entidad, para realizar actividades que no requieren el manejo de activos de información como reuniones, entrega de correspondencia, solicitudes de información, entrevistas, entre otras.

**LUIS ARMANDO ROJAS CAICEDO**
P.U. Líder de Sistemas de Información

**Elaboró y Proyectó: Yaruth Núñez** Yaruth Núñez S.
**Revisó : Armando Rojas C.**