E.S.E
SALUD del TUNDAMA

MUNICIPIO DE DUITAMA
EMPRESA SOCIAL DEL ESTADO SALUD DEL TUNDAMA

Resolución 1460 del 30 de Octubre de 2015

"Por la cual se adopta la Política de Confidencialidad y Seguridad de la Información"

LA GERENTE DE LA EMPRESA SOCIAL DEL ESTADO SALUD DEL TUNDAMA

En uso de sus Facultades Legales, Estatutarias y,

C O N S I D E R A N D O:

Que el Decreto 1011 del 2006, por la cual establece el sistema obligatorio de garantía de la calidad de la atención en salud del sistema general de seguridad social en salud.

Que la resolución 2003 del 2014, Por la cual establece los estándares mínimos de habilitación.

Que la resolución 2082 y Decreto 903 del 2014, Por la cual establece las normas de acreditación.

Que la Ley 603 del 2000, por la cual se reglamenta la protección de los derechos de autor en Colombia. Recuerde.

Que la Ley 1273 del 5 de Enero 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.

Que la Ley 1341 del 30 de Julio de 2009, Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Que la Ley Estatutaria 1581 de 2012, Por la cual establece la Protección de datos personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 011 de la Corte Constitucional.

Que la 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:

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en

pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Resolución 1460 del 30 de Octubre de 2015

"Por la cual se adopta la Política de Confidencialidad y Seguridad de la Información"

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Que la Ley 527 de 1999, en su artículo 10, señala que: "Los mensajes de datos serán admisibles como medios de prueba y su carga probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil".

Que la Ley 599 de 2000, en su artículo 195, señala que: "El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quién tiene derecho a excluirlo, incurrirá en multa".

RESUELVE:

ARTÍCULO PRIMERO: ADOPCIÓN: Adoptar la política de Confidencialidad y Seguridad de la Información de la E.S.E. Salud del Tundama.

ARTICULO SEGUNDO: OBJETIVOS: La Política de Confidencialidad y Seguridad de la Información de la E.S.E. Salud del Tundama, tendrá como objetivos:

OBJETIVO GENERAL

Definir los criterios relacionados con las herramientas, los equipos, el software, las comunicaciones, leyes, normas, y prácticas que garanticen la seguridad, confidencialidad, disponibilidad de la información, y a su vez puedan ser entendidas y ejecutadas por todos aquellos miembros de la Empresa Social del Estado Salud del Tundama, a fin de obtener uniformidad, calidad, comunicación y racionalidad en el desarrollo informático institucional.

OBJETIVOS ESPECÍFICOS

- Apoyar el crecimiento, desarrollo e implementación del área informática con el propósito de prestar los servicios a los usuarios internos y externos, con mayor oportunidad y calidad.
- Establecer la adquisición de tecnología informática en la Institución.
- Establecer lineamientos generales en procura de la armonía y la comunicación necesaria entre los procesos.
- Representar un marco de referencia técnico que permite lograr

homogeneidad y compatibilidad en las tecnologías de información utilizadas.

- Orientar a los líderes de procesos en la planificación y en el desarrollo de los sistemas de información.

ARTICULO TERCERO: ALCANCE. Las estrategias de seguridad y confidencialidad de la información, involucra a todos los niveles de la organización (Colaboradores, usuarios y sus familias, visitantes, proveedores, y comunidad en general.)

ARTICULO CUARTO: RESPONSABLES.

La política de Confidencialidad y Seguridad de la Información es transversal a todos los procesos de la organización, su cumplimiento y direccionamiento de estrategias se logra a través del grupo de Gerencia de la Información de Acreditación, quien formula, coordina, realiza seguimiento, planes de mejoramiento y evaluación de la estrategia de Confidencialidad y Seguridad de la Información.

ARTÍCULO QUINTO: DEFINICIONES: La E.S.E SALUD DEL TUNDAMA, adopta la terminología para la política de Confidencialidad y Seguridad de la Información:

- **Políticas:** Son guías dadas por la administración superior y que delimitan el área dentro del cual una decisión puede ser adoptada. Las políticas pueden ser consideradas como guías de pensamiento en la adopción de decisiones y por lo tanto permiten cierto grado de libertad.

- **Amenaza:** Es una situación o acontecimiento que puede causar daño a los bienes informáticos; puede ser una persona, un programa malicioso o un suceso natural o de otra índole que representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema.

- **Análisis de riesgo:** Es un proceso dirigido a determinar la posibilidad de que las amenazas se materialicen sobre los bienes informáticos e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar.

- **Bienes informáticos:** Elementos, componentes del sistema que deben ser protegidos para evitar la ocurrencia de una amenaza.

- **Impacto:** Es el daño producido por la materialización de una amenaza.

- **Riesgo:** Probabilidad de que una amenaza se materialicé sobre una

vulnerabilidad del sistema informático, causando un impacto negativo en la organización.

- **Riesgo residual:** Es el riesgo que queda después de aplicados controles de seguridad para minimizarlo.
- **Riesgo aceptable:** El riesgo se encuentra en un nivel que se puede aceptar, sin necesidad de tomar otras medidas de control diferentes a las que se poseen.
- **Seguridad:** Es usada para minimizar los riesgos a que están sometidos los bienes informáticos.
- **Sistema informático:** Es el conjunto de bienes informáticos de que dispone una entidad para su correcto funcionamiento para la consecución de sus objetivos.
- **Vulnerabilidad:** En un sistema informático es un punto o aspecto susceptible de ser atacado o de dañar su seguridad; representan las debilidades o aspectos fiables o atacables en el sistema informático y califican el nivel de riesgo del mismo.
- **Informática:** Es la ciencia de la información automatizada, todo aquello que tiene relación con el procesamiento de datos, utilizando las computadoras y/o los equipos de procesos automáticos de información. Es la ciencia que se encarga de la automatización del manejo de la información.
- **Freeware:** (Software de libre distribución). Aquel que no requiere ningún tipo de licencia para su funcionamiento. Sin embargo, sus derechos de copia no pueden ser incorporados a ningún tipo de desarrollo de software. Normalmente se adquiere vía Internet.
- **Hardware:** Es la parte física de un computador y más ampliamente de cualquier dispositivo electrónico.
- **Licencia de Software:** Una licencia de software es un contrato entre el titular del derecho de autor (propietario) y el usuario del programa informático (usuario final), para utilizar éste en una forma determinada y de conformidad con unas condiciones convenidas.
- **Shareware o Liteware:** (Software de uso restringido). Aquel que se puede instalar sin licencia como versión inicial de prueba, pero, el usuario tiene que pagar por la licencia de uso definitivo. En algunas ocasiones las versiones Shareware, traen opciones deshabilitadas para obligar al usuario a adquirir la licencia definitiva.
- **Software:** Se refiere al equipamiento lógico o soporte lógico de un computador, comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica.
- **Software de dominio público:** Aquel que no tiene derechos de autor, ya que los autores desean compartirlo con la comunidad mundial de desarrolladores. Es de libre uso y puede ser incorporado a cualquier desarrollo de software no comercial.
- **Software ilegal:** Toda copia o uso no autorizado de un programa de computador en cualquier forma distinta a la permitida por las leyes de derechos

de autor o la estipulada en la licencia de software.

- **Control del Software Instalado:** Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre. El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

- **Copia de Seguridad:** es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales; etc.

- **Seguridad:**

Realza la propiedad de algo donde no se registran peligros, daños ni riesgos. Es algo firme y certero.

- **Confidencialidad:**

Es una cualidad de confidencial, es decir es una acción segura y recíproca entre dos o más individuos; es además una propiedad de la información que pretende garantizar el acceso solo a las personas autorizadas.

- **Acceso no autorizado**

Es producto de la explotación de una vulnerabilidad en algún sistema para acceder a algún tipo de información.

- **Perdida de información**

Es la falta o ausencia de algún tipo de información que se tenga de las personas.

- **Deterioro**

Es la disminución o pérdida de la calidad o la importancia gradual de algo.

- **Archivos**

Es un conjunto de documentos producidos o recibidos por toda persona física o moral, y por todos los servicios u organismos públicos o privados, en el ejercicio de su actividad. Son conservados para sus necesidades.

- **Historia clínica**

Es el documento médico legal que contiene todos los datos e información de un usuario.

- **Claves de acceso**

Es una contraseña que las personas emplean para acceder a un servicio, sistema o programa.

- **Backups**

Es una copia de seguridad o copia de respaldo, es decir, una copia de datos de tal forma que estas puedan restaurar un sistema después de una perdida de información.

- **Control documental**

Es un requisito que establece las bases para elaborar, mantener y actualizar el soporte documental.

ARTÍCULO SEXTO: COMPROMISO:

La E.S.E. Salud del Tundama se compromete a un eficiente uso de los recursos y al manejo de la información de los usuarios y su familia, enfocados en los parámetros que garanticen la confiabilidad, confidencialidad, Privacidad y seguridad de la información".

ARTÍCULO SEPTIMO: PASOS PARA LA SENSIBILIZACIÓN Y CAPACITACIÓN EN LA E.S.E SALUD DEL TUNDAMA:

Se desarrollan programas de Capacitación para informar y/o comunicar del manejo de la confidencialidad y la seguridad de la información de la E.S.E. Salud del Tundama.

- Directivas y funcionarios de los diferentes procesos que responden por la información procesada siendo responsables de su protección.
- Personal de informática, que domina los aspectos técnicos necesarios para la implementación de los controles de seguridad.
- Líderes de procesos, quienes a partir de su responsabilidad custodian los bienes informáticos.

La Política Seguridad de la Informática será revisada a intervalos programados o ante surgimiento de cambios significativos para asegurar su actualización, adecuación y efectividad. Algunos procedimientos de seguridad que se implementan son:

- De administración de cuentas de usuarios.
- De asignación y cancelación de permisos de acceso a los servicios.
- De asignación y cancelación de derechos y privilegios.
- De asignación de contraseñas.
- De realización de auditorías.
- De acceso a las áreas.

Se debe establecer claramente las áreas de las cuales los colaboradores son responsables, teniendo en cuenta:

- Definir y documentar los niveles de autorización.

- Identificar y definir los bienes informáticos y los procesos de seguridad asociados a cada proceso.
- Asignar el responsable de cada bien informático.

SOCIALIZACIÓN DE LA POLITICA

- Se realizará la adopción de la política mediante acto Administrativo.
- Se publicará la política en INTRANET, para el acceso de todos los colaboradores y usuarios de la Empresa Social del Estado Salud del Tundama.
- Se realiza entrega en medio magnético a cada líder de proceso para que este se encargue de socializarla con cada uno de los integrantes de su grupo.
- Se realizará retroalimentación (Feedbak) con cada uno de los trabajadores de la Institución, mediante actividades lúdicas.
- Se publicarán tips sobre seguridad informática, en los boletines entregados en la Institución.
- Se realizarán Socializaciones con todos los colaboradores de la Institución, para concientizar sobre la necesidad de la seguridad Informática.
- La preparación del personal para el cumplimiento de sus obligaciones en cuanto a la seguridad informática.
- Capacitar a los usuarios en las medidas y procedimientos que se van a implantar.
- Se reforzará con las capacitaciones mensuales y quincenales establecidas por la Institución.

ARTÍCULO OCTAVO: IMPLEMENTACION DE LA POLITICA DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN DE LA E.S.E SALUD DEL TUNDAMA:

NORMAS DE SEGURIDAD INFORMÁTICA

Adóptense para la Empresa Social del Estado Salud del Tundama, las normas, como prácticas y procedimientos orientados a mantener la operación segura de la información en cuanto a eficacia, eficiencia, confiabilidad, integridad, exactitud, disponibilidad, legalidad, confidencialidad, autorización, protección física y propiedad.

NORMA 1: PREVENCIÓN, DETECCIÓN Y ELIMINACIÓN DE SOFTWARE ILEGAL O INNECESARIO:

OBJETIVO: Garantizar que todo el software utilizado en la Empresa Social del

Estado Salud del Tundama esté debidamente licenciado y/o autorizado para su uso.

Prevención:

- Todo el software instalado en los computadores de la Empresa Social del Estado Salud del Tundama debe ser legalmente adquirido y debe contar con la correspondiente licencia de uso.
- Todo proceso de adquisición que incluya software debe ser analizado, sugerido por el grupo de Gerencia de la Información y por el Comité Coordinador del Sistema de Control Interno y por el Comité de Compras.
- Al software instalado en los componentes tecnológicos de la Empresa Social del Estado Salud del Tundama que no esté respaldado por un concepto previo de los responsables de la información, no se le brindará ningún tipo de soporte.
- Todos los funcionarios de la Empresa Social del Estado Salud del Tundama deben conocer las implicaciones que tiene el instalar software ilegal en los computadores de la Empresa.
- Ningún tipo de software, incluyendo el catalogado como de libre distribución debe ser instalado en los componentes tecnológicos de la Empresa Social del Estado Salud del Tundama sin previa autorización. La no aplicación de esta directriz será sancionada disciplinariamente. Los inventarios de software, hardware y licencias deberán permanecer actualizados.

Detección: El Técnico Operativo debe realizar revisiones periódicas y de selección aleatoria a los computadores de la Empresa Social del Estado Salud del Tundama, con el fin de verificar que solamente esté instalado software autorizado.

Eliminación: Todas las copias de software instaladas y no autorizadas deben ser eliminadas. La violación de estas normas ocasionará sanciones disciplinarias.

NORMA 2: PROPIEDAD DE LA INFORMACIÓN:

OBJETIVO: Determinar que toda la información almacenada en los sistemas de cómputo de la Empresa Social del Estado Salud del Tundama es propiedad de ella. Establece que:

- Toda la información almacenada en los sistemas de cómputo de la Empresa Social del Estado Salud del Tundama pertenece a ella.
- Todos los sistemas de cómputo de la Empresa Social del Estado Salud del Tundama están sujetos a revisiones periódicas por parte del responsable del área de sistemas o por el personal que la Empresa delegue para dicho fin.
- Es responsabilidad de los funcionarios garantizar los derechos de la

confidencialidad y seguridad de la Información de la Empresa Social del Estado Salud del Tundama.

- Se prohíbe el uso de la información de la Empresa Social del Estado Salud del Tundama. con propósitos comerciales o personales.
- Toda información generada por y para la Empresa Social del Estado Salud del Tundama es propiedad de ella a menos que la relación contractual aprobada por la Gerencia especifique lo contrario.
- Ningún tipo de información referente a la Empresa Social del Estado Salud del Tundama debe ser compartida con externos, solamente se hará cuando las características del trabajo lo requieran.

NORMA 3: COPIAS DE SEGURIDAD. Backup

OBJETIVO: Garantizar la custodia y conservación de la información, los datos relevantes y originales que se realiza con el fin de disponer de un medio de recuperarlos del software de propiedad de la Empresa Social del Estado Salud del Tundama.
Se Establece:

- El área de sistemas de la Empresa Social del Estado Salud del Tundama, debe realizar diariamente una (1) juego de copias de seguridad de la información generada por los programas del sistema informático software administrativo, financiero y Asistencial o por la aplicación que lo amplíe o sustituya. De la información generada en otros programas se deberán hacer copias de seguridad con una periodicidad no mayor a un mes (1) mes en el área de Administrativa.
- Las copias de seguridad se deben guardar en custodia así: un (1) juego en la oficina del Técnico Operativo (Sistemas) y el otro juego lo custodiará la Gerencia de la Empresa Social del Estado Salud del Tundama por fuera de las instalaciones físicas de la Institución.
- Las copias de seguridad se guardarán por un término no inferior a un año.

ARTÍCULO NOVENO: INTEGRACIÓN CON OTRAS POLÍTICAS Y CON LA PLANEACIÓN ESTRATÉGICA DE LA E.S.E SALUD DEL TUNDAMA:

La Política de Confidencialidad y Seguridad de la Información de la E.S.E SALUD DEL TUNDAMA, se articula con la Visión Institucional por cuanto la misma busca una atención humanizada, segura y centrada en el usuario y su familia y con la Misión Institucional ya que es objetivo de la E.S.E. SALUD DEL TUNDAMA, es contar con un equipo humano comprometido con la calidad, seguridad, innovación, responsabilidad social, y la atención centrada en las personas y sus familias.

ARTICULO DECIMO: PARTICIPACIÓN DEL PACIENTE Y SU FAMILIA Y LA COMUNIDAD EN LA COGESTIÓN DE LA POLÍTICA DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN DE LA E.S.E SALUD DEL TUNDAMA:

La E.S.E SALUD DEL TUNDAMA, favorece la integración del Usuario y su familia en el cumplimiento de la confidencialidad y seguridad de su información, por lo tanto que nuestros colaboradores le han enseñado y lo hace a través de las siguientes estrategias:

- Capacitar, educar al usuario y su familia, reforzando su conocimiento en temas de confidencialidad y seguridad de su información.
- Se Establece dentro de los Derechos de los usuarios: "A que se le Garantice la custodia y confidencialidad de su información".

ARTICULO DECIMO PRIMERO: RECURSOS PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN EN LA E.S.E SALUD DEL TUNDAMA:

En la Planeación Presupuestal de la E.S.E SALUD DEL TUNDAMA, se incluirán los recursos requeridos para garantizar la implementación de la presente Política, asegurando el apoyo financiero, físico, tecnológico y de Talento Humano para el logro de los objetivos aquí planteados.

ARTICULO DECIMO SEGUNDO: INDICADORES QUE MIDEN LA POLÍTICA DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN DE LA E.S.E SALUD DEL TUNDAMA

Es necesario lograr diagnosticar correctamente qué está pasando y qué es necesario corregir para poder gestionar. Mediante el proceso de revisión para comprobar la conformidad con los patrones establecidos para medir el rendimiento y la eficacia de la Política de Confidencialidad y Seguridad de la información, para lo cual se deben considerar las siguientes acciones:

- Revisiones periódicas de los indicadores seleccionados.
- Revisiones de los riesgos residuales y riesgos aceptables.
- Realización de auditorías internas.
- Comunicación de los resultados de las auditorias.

Los indicadores permiten verificar el correcto funcionamiento de la Política Seguridad de la Informática, cada indicador debe tener a sociado valores que representen las metas a cumplir. Al definir y valorar el cumplimiento de los indicadores se tendrá en cuenta el daño derivado de la ocurrencia de un incidente y su posible impacto en los objetivos. La información referente a estos es la base de la retroalimentación del sistema.

Algunos posibles indicadores pueden ser:

- Tiempo de servicio sin interrupciones.
- Cantidad de incidentes computacionales.
- Velocidad real.
- Cantidad de conformidades detectadas.
- Virus detectados en el sistema.
- Mantenimientos preventivos ejecutados.
- Claves Asignadas
- Acceso de la Información

ARTICULO DECIMO TERCERO: DOCUMENTOS DE REFERENCIA:

- Manual de Acreditación en Salud Ambulatorio y Hospitalario en Colombia, versión 003.
- http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- http://www.aliatuniversidades.com.mx/bibliotecasdigitales/pdf/sistemas/Politica_y_legislacion_informatica.pdf
- http://redyseguridad.fi-proyectos/seguridad/DefinicionPolitica.php
- http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

ARTICULO DECIMO CUARTO: VIGENCIA Y DEROGATORIAS. La presente resolución rige a partir de la fecha de su expedición y deroga las demás disposiciones que le sean contrarias.

COMUNIQUESE Y CÚMPLASE

Dada en Duitama a los treinta (30) días del mes de Octubre del 2015.

LUCILA ESPERANZA PEREZ PRECIADO