E.S.E.
SALUD del TUNDAMA

MUNICIPIO DE DUITAMA
EMPRESA SOCIAL DEL ESTADO SALUD DEL TUNDAMA

Resolución 1034 del 29 de septiembre de 2020

"Por medio de la cual se modifica la resolución 1460 del 30 de octubre de 2015, y se actualiza a la Política de Confidencialidad y Seguridad de la Información y Protección de Datos Personales"

LA GERENTE DE LA EMPRESA SOCIAL DEL ESTADO SALUD DEL TUNDAMA

En uso de sus facultades legales y estatutarias y,

CONSIDERANDO:

Constitución política, Artículo 15, Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

Ley 1266 de 2008 (Ley de Habeas Data), Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

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.

Decreto reglamentario 1377 de 2013, Establece la obligación para los responsables del tratamiento de los datos personales de desarrollar políticas relacionadas con el tratamiento de los datos personales a su cargo.

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 3100 de 2019, Por la cual se definen los procedimientos y condiciones de inscripción de los prestadores de servicios de salud.

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

Que la Resolución 5095 de 2018, Por medio de la cual se adopta el manual de acreditación en salud ambulatorio y hospitalario de Colombia

Resolución 1034 del 29 de septiembre de 2020

Por medio de la cual se establece la política de Confidencialidad, Seguridad la Información y protección de datos personales

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

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 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 2691: 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 A el artículo 240 de este Código.

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".

Resolución 512 de marzo 14 de 2019: Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información

Política de seguridad de la información MIPG - Decreto Único Reglamentario 1078 de 2015, del sector de las Tecnologías y Comunicaciones -TIC, se define el componente de seguridad y privacidad de la información, como parte integral de la Estrategia Gobierno en Línea -GEL, la cual en el MEN se ha adoptado.

Decreto 1008 de 2018. - Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Resolución 1034 del 29 de septiembre de 2020

Por medio de la cual se establece la política de Confidencialidad, Seguridad la Información y protección de datos personales

Decreto 1151 de 2008, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Lineamientos generales de la Estrategia de Gobierno en línea.

Por lo antes expuesto,

RESUELVE:

ARTÍCULO PRIMERO: COMPROMISO: Establecer las medidas generales para garantizar los niveles de seguridad y privacidad adecuados para la protección de datos personales, con el fin de evitar posibles adulteraciones, pérdidas, consultas, usos o accesos no autorizados, aplicable a los datos personales registrados en cualquier base de datos (suministrados por todos nuestros usuarios, colaboradores, proveedores, trabajadores y contratistas) que administre la ESE Salud del Tundama.

ARTICULO SEGUNDO: OBJETIVOS:

- Definir los criterios relacionados con las herramientas, los equipos, el licenciamiento de software, las comunicaciones, leyes, normas, y prácticas que garanticen confidencialidad, seguridad la información y protección de datos personales, así como la disponibilidad de la información, y a su vez puedan ser entendidas y ejecutadas por todos aquellos miembros de la ESE Salud del Tundama, a fin de obtener uniformidad, calidad, comunicación y racionalidad en el desarrollo informático institucional.
- Implementar un marco de referencia técnico que permite lograr homogeneidad y compatibilidad en las tecnologías de información utilizadas y las establecidas en Gobierno Digital.
- Establecer los lineamientos para la protección de los datos personales recopilados por la ESE Salud del Tundama, que permitan garantizar a nuestros usuarios su derecho a conocer, actualizar y rectificar la información que se encuentre registrada en nuestras bases de datos.
- Garantizar los lineamientos para obtener la autorización de los titulares (usuarios, colaboradores, proveedores, trabajadores y contratistas), efectuar el tratamiento de los datos personales, las finalidades de uso, los derechos que le asisten a ellos, los canales de atención, así como los procedimientos internos para el tratamiento.

ARTÍCULO TERCERO: ALCANCE: La política confidencialidad, seguridad de la información y protección de datos personales es transversal a todos los procesos de la ESE Salud del Tundama, buscando que la información sea custodiada, garantizando la privacidad de nuestros usuarios, colaboradores, proveedores, trabajadores y contratistas.

ARTICULO CUARTO: IMPLEMENTACIÓN, Para llevar a cabo la implementación de la Política de Confidencialidad y Seguridad de la Información y Protección de Datos Personales en la E.S.E. Salud del Tundama, se toma como base la metodología Planear, Hacer, Verificar y Actuar "PHVA" y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos, dentro de las ACTIVIDADES se contemplan:

1) Elaborar la Política de Confidencialidad y Seguridad de la Información y Protección de Datos Personales

Resolución 1034 del 29 de septiembre de 2020

Por medio de la cual se establece la política de Confidencialidad, Seguridad la Información y protección de datos personales

2) Elaborar el Procedimiento de Confidencialidad y Seguridad de la Información y Protección de Datos Personales
3) Realizar la socialización a los colaboradores de la ESE Salud del Tundama de la política y procedimiento de Confidencialidad y Seguridad de la Información y Protección de Datos Personales.
4) Evaluar la adherencia al cumplimiento de la política y procedimiento de Confidencialidad y Seguridad de la Información y Protección de Datos Personales.

ARTÍCULO QUINTO: RESPONSABLES: La política de confidencialidad, seguridad de la información y protección de datos personales 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, quien formula, coordina, realiza seguimiento, planes de mejoramiento y evaluación de la estrategia de Confidencialidad y Seguridad de la Información.

Es responsabilidad de la Gerencia de la información hacer uso de la política, como parte de sus herramientas de seguridad de la información y de gestión, de definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento.

ARTÍCULO SEXTO: La presente resolución rige a partir de su fecha de expedición y deroga las demás disposiciones que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE

Dada en Duitama a los veintinueve (29) días del mes de septiembre de 2020

CATHERINE VAN ARCKEN MARTINEZ
Gerente

Proyectó: Edwin A Romero A
Revisó: Sandra Torres Barinas