POLITICA DE SEGURIDAD DIGITAL

E.S.E HOSPITAL SAN LUCAS DE EL MOLINO

ISABEL PAULINA APONTE DIAZ
GERENTE

AÑO 2024

INTRODUCCION

La dependencia de las tecnologías de la información y las comunicaciones interconectadas globalmente ha puesto en el centro de la discusión la necesidad de trabajar en políticas y/o estrategias nacionales de seguridad digital. Esta necesidad es alimentada por el aumento de incidentes y ataques digitales con potenciales consecuencias catastróficas para la protección de la seguridad de la información, por tanto, de las personas.

Siendo la seguridad digital una discusión cada vez más crítica, hay que reconocer que la sociedad civil y los grupos de interés público no son suficientemente considerados, algo que desequilibra el debate y lo ubica en un tema enfocado en los sistemas o vagos conceptos de seguridad nacional, en lugar de las personas.

Sin embargo, la seguridad digital está intrínsecamente relacionada con las personas, pues la forma en cómo se definen e implementan las políticas de regulación del comportamiento en línea y la seguridad de la información tienen profundas implicaciones para los derechos humanos, en especial la privacidad, la libertad de expresión o la libre asociación.

Es así que la Política de seguridad digital está enfocada a contrarrestar las amenazas cibernéticas, siendo la gestión del riesgo la parte fundamental de esta política, la seguridad digital por ser la información el activo más importante de la organización, es necesario protegerla frente a los posibles riesgos derivados del uso de las nuevas tecnologías, para garantizar la seguridad de la información. Por lo tanto, las entidades, organismos y órganos de control deberán analizar las particularidades de funcionamiento de cada entidad y adoptar las políticas de protección y mitigación que resulten pertinentes a sus necesidades, adoptando el enfoque de gestión de riesgos al que hace referencia el CONPES 3854 de Seguridad Digital o aquella norma que lo modifique o sustituya.

El presente documento se encuentra la formulación de la Política de Seguridad Digital para la ESE Hospital San Lucas de El Molino, la cual se diseña bajo los lineamientos del Modelo Integrado de Planeación y Gestión -MIPG, en el marco de su implementación.

1. JUSTIFICACION

En el Decreto 1499 de 2017 y el Manual de MIPG se encuentra la Dimensión Gestión con Valores para Resultados donde la entidad debe tener en cuenta acciones relevantes dentro de su organización asociadas a aspectos considerados de la “Ventanilla hacia adentro” haciendo necesario la implementación y adopción de una política de Seguridad digital, la cual debe desarrollarse con lineamientos contenidos en el CONPES 3854 de 2016 Política Nacional de Seguridad digital.

Que el numeral 8 del artículo 2 de la Ley 1341 de 2009 establece que el Gobierno Nacional fijará los mecanismos y condiciones para garantizar la masificación del Gobierno en Línea, con el fin de lograr la prestación de servicios eficientes a los ciudadanos, así mismo, la citada Ley determinó que es función del Estado intervenir en el sector de las TIC, con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo de dichos ector; así como reglamentar las condiciones en que se garantizará el acceso a la información en línea, de manera abierta, ininterrumpida y actualizada.

El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, ha incrementado la participación digital de los ciudadanos, generando nuevas formas para atentar contra su seguridad y la del Estado, por ende, es necesario fortalecer las capacidades de las instituciones para identificar, gestionar el riesgo y atender las situaciones para brindar protección en el ciberespacio.

A través de la política de seguridad digital se han propuesto estrategias que permiten resolver problemas, generar diagnósticos más rápidamente, así como comparar diferentes escenarios posibles para prevenir riesgos cibernéticos en la plataforma dispuesta para la ESE Hospital San Lucas de El Molino.

Con la implementación de la Política de Seguridad de la Información, la ESE Hospital San Lucas de El Molino adopta un compromiso obligatorio de protección a la información frente a una amplia gama de amenazas. Contribuyendo a minimizar los riesgos asociados de daño y asegurar el eficiente cumplimiento de las funciones de la entidad apoyadas en un correcto uso de los Sistema de información.

2. OBJETIVO

Diseñar estrategias para mejorar las capacidades de los funcionarios de la ESE Hospital San Lucas de El Molino en materia de seguridad digital, en todas sus actividades en el entorno digital, en un marco de cooperación, colaboración y asistencia.

2.1 OBJETIVOS ESPECIFICOS

- Salvaguardar los activos tecnológicos y custodiar la información producida en la ESE Hospital San Lucas de El Molino.
- Definir lineamientos en materia de seguridad de la información.
- Promover la cultura de la seguridad de la información a los servidores públicos, contratistas, ciudadanos y público en general.
- Capacitar al personal de la entidad en buenas practicas digitales.
- Orientar a la ciudadanía en general sobre el uso responsable del medio digital.
- Fortalecer la capacidad de la administración en materia de prevención de riesgos digitales.

3. ALCANCE

La Política de Seguridad Digital en la ESE Hospital San Lucas de El Molino busca garantizar que la entidad identifique el peligro de los riesgos de su entorno digital con el fin de desarrollar nuevas capacidades frente a sistemas de seguridad digital que permiten que la entidad tenga un manejo confiable y seguro de la información.

4. MARCO LEGAL

Numero	Año	Descripción
Constitución Política de Colombia	1991	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 23	1982	Derechos de autor
Ley 527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 594	2000	Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100de 2004. Por medio del cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

Ley 603	2000	Esta Ley se refiere a la protección de los derechos de autor en Colombia. El software en un archivo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
Ley 962	2005	Simplificación y Racionalización de Tramite. Atributos de seguridad en la información electrónica de entidades públicas.
Ley 1150	2007	Seguridad de la información electrónica en contratación en línea.
Ley 1266	2008	Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273	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.
Ley 1341	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.
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Ley 1712	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la información Pública Nacional y se dictan otras disposiciones.
Ley 1928	2018	Por medio de la cual se aprueba el “Convenio sobre la Ciberdellncuencia, adoptado el 23 de noviembre de 2001, en Budapest”
Decreto 2693	2012	Estrategia de Gobierno en Línea. Ministerio de tecnologías de la Información y las comunicaciones.
Decreto 1377	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
Decreto 103	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de tecnologías de la Información y las Comunicaciones.
Resolución 500 del 10 de Marzo	2021	“Por la cual se establecen 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”
Documento Conpes 3854	2016	Política Nacional de Seguridad Digital

5. DEFINICIONES

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligue o genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Lineamientos: Directriz o disposición establecida por el Ministerio TIC, que debe ser implementada por las entidades públicas para el desarrollo de la Política de Gobierno Digital y se desarrolla a través de estándares, guías, recomendaciones o buenas prácticas.

Estándar: Es el conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Un estándar se construye a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular, implican uniformidad y normalización y es de obligatorio cumplimiento.

Arquitectura: Este habilitador busca que las entidades apliquen en sugestión un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades Institucionales y de gestión TI. El habilitador de Arquitectura soporta su uso e implementación en el Marco de Referencia de Arquitectura Empresarial del Estado, que es el instrumento que establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza la ruta de implementación que una entidad pública debe realizar.

Seguridad de la Información: Este habilitador busca que las entidades públicas incorporen la Seguridad de la información en todos sus procesos, tramites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad, y privacidad de la información, así como la protección de los datos personales que tratan las entidades públicas en cumplimiento de la normatividad de protección de datos personales; este habilitador tiene un soporte en el MSPI.

Confidencialidad: La información no se pone a disposición, ni se revela a individuos, entidades o procesos autorizados.

MSPI: Modelo de Seguridad y Privacidad de la Información.

Riesgo: Posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

Servidor: Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

Múltiples partes interesadas: el Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades.

Bajo el enfoque de la política nacional de seguridad digital:

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

Entorno digital abierto: entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica.

Incidente digital: evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

Resiliencia: es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.

6. DIAGNOSTICO

Teniendo como base el diligenciamiento del cuestionario del Formulario Único de Reporte de Avance a la Gestión, FURAG, aplicado para la vigencia 2021, se puede evidenciar que la Empresa Social del Estado ESE Hospital San Lucas de El Molino presenta el 43,1% de avance en la elaboración, aprobación e implementación de la política de Seguridad Digital, tal como se evidencia en la gráfica.

7. PRINCIPIOS POLITICA DE SEGURIDAD DIGITAL

La Política nacional de gobierno digital recomienda que se debe tener en cuenta dos tipos de principios que son: generales y operativos. Los principios generales están dirigidos a las múltiples partes interesadas quienes, directa o indirectamente, desarrollan algunas o todas sus actividades socioeconómicas en el entorno digital. Los principios operativos están dirigidos a los líderes o tomadores de decisiones, quienes por su alto nivel en las organizaciones deben enfocar sus acciones hacia la adopción del marco general de gestión del riesgo de seguridad digital.

Principios Generales:

Conocimiento, capacidades y empoderamiento: Las múltiples partes interesadas deben entender los riesgos de seguridad digital. Deben ser conscientes de que el riesgo de seguridad digital puede afectar el logro de sus objetivos económicos y sociales, y el de otros. Deben estar educados al respecto, poseer las habilidades necesarias para entender el riesgo, administrarlo y evaluar su impacto.

Responsabilidad: Las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales.

Derechos humanos y valores fundamentales: Las múltiples partes interesadas deben gestionar los riesgos de seguridad digital de manera transparente y compatible con los derechos humanos y los valores fundamentales. La implementación de la gestión de riesgos de seguridad digital debe ser compatible con la libertad de expresión, el libre flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales. Las organizaciones deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de seguridad digital.

Cooperación: Las múltiples partes interesadas deben cooperar, incluso más allá de sus fronteras, a nivel regional e internacional.

Principios operativos:

Evaluación De Riesgos Y Ciclo De Tratamiento: la evaluación de riesgos debe llevarse a cabo de manera sistemática y continua, evaluando las posibles consecuencias de las amenazas y las vulnerabilidades digitales en las actividades económicas y sociales en juego. El tratamiento del riesgo debería tener como objetivo reducir el riesgo a un nivel aceptable en relación con los beneficios económicos y sociales.

Medidas De Seguridad: los líderes y tomadores de decisiones deben asegurarse de que las medidas de seguridad sean apropiadas y proporcionales al riesgo, y deben tener en cuenta su potencial impacto, negativo o positivo, sobre las actividades económicas y sociales que tienen por objeto proteger. La evaluación de riesgos de seguridad digital debe guiar la selección, operación y mejora de las medidas de seguridad para reducir el riesgo a niveles aceptables.

Innovación: los líderes y tomadores de decisiones deben asegurarse de que la innovación sea considerada como parte integral de la reducción del riesgo de seguridad digital. Esta debe fomentarse tanto en el diseño y funcionamiento de la economía, y de las actividades sociales basadas en el entorno digital, como en el diseño y el desarrollo de las medidas de seguridad.

Preparación Y Continuidad: con el fin de reducir los efectos adversos de los incidentes de seguridad, y apoyar la continuidad y la capacidad de recuperación de las actividades económicas y sociales, deben adoptarse preparaciones y planes de continuidad. El plan debe identificar las medidas para prevenir, detectar, responder y recuperarse de los incidentes y proporcionar mecanismos claros de escalamiento.

Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos en Colombia, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de la intimidad y los datos personales y la privacidad, así como los principios fundamentales consagrados en la Constitución Política de Colombia. En caso de limitación a estos derechos, debe ser bajo medidas excepcionales y estar conforme con la Constitución Política y los estándares internacionales aplicables. Estas medidas, deben ser proporcionales, necesarias y estar enmarcadas en la legalidad.

Adoptar un enfoque incluyente y colaborativo que involucre activamente a las múltiples partes interesadas, y que permita establecer condiciones para el desarrollo eficiente de alianzas, con el fin de promover la seguridad digital del país y sus habitantes, y aumentar la capacidad de resiliencia nacional frente a eventos no deseados en el entorno digital.

Asegurar una responsabilidad compartida entre las múltiples partes interesadas, promoviendo la máxima colaboración y cooperación. Lo anterior, teniendo en cuenta el rol y el grado de responsabilidad de cada parte para gestionar los riesgos de seguridad digital y para proteger el entorno digital.

La ESE Hospital San Lucas de El Molino estable las siguientes acciones para mantener el estado de implementación de esta Política:

- Revisión de la Política de Seguridad Digital y mecanismos que permitan verificar su cumplimiento.
- Revisión y aprobación de los activos y Riesgos de Seguridad Digital.
- Realizar campañas de concientización en temas de Seguridad Digital teniendo en cuenta los diferentes roles definidos dentro de la “Matriz roles y responsabilidades” del Sistema de Gestión de la Seguridad de la Información SGSI.
- Revisión de indicadores asociados a los objetivos del Sistema de Gestión de la Seguridad de la Información SGSI, con el fin de verificar su cumplimiento y alineación.

8. LINEAMIENTOS GENERALES DE LA POLÍTICA

- La **ESE Hospital San Lucas de El Molino,** asignara responsabilidades frente a la seguridad de la información que serán definidas, compartidas, publicadas y aceptadas por cada uno de los proveedores, socios de la Entidad o terceros.

- La **ESE Hospital San Lucas de El Molino,** verificará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- **ESE Hospital San Lucas de El Molino**, protegerá la información creada, procesada, transmitida o resguardada por los procesos de la Entidad, con el fin de minimizar los impactos financieros, operativos o legales a causa de los usos deesta y las amenazas originadas por parte del personal.

- Toda información que provenga de un archivo externo de la Entidad o que deba ser descargado tiene que ser analizado con el antivirus institucional vigente.

- Todo usuario de los recursos TIC, **NO** debe visitar sitios restringidos de manera explícita o implícita, o sitios que afecten la productividad de la Institución; como el acceso desde la Entidad a sitios relacionados con la pornografía, juegos, redes sociales no autorizadas, etc.

- Minimizar el uso de dispositivos extraíbles para compartir archivos aprovechando los recursos compartidos del servidor de la entidad o haciendo uso del servicio de internet.

- Todo usuario de los recursos TIC debe advertir e informar a la Secretaria de Gobierno y/o oficina de Gobierno en Línea o quien haga sus veces, de las medidas específicas de protección para evitar el acceso a personal no autorizado, y/o establecer el sistema de respaldo para la misma.

9. POLÍTICAS DE SEGURIDAD DE GOBIERNO DIGITAL

La ESE Hospital San Lucas de El Molino, se compromete a administrar los riesgos de seguridad y privacidad de la información para generar, implementar y monitorear los controles que permitan mantener la confidencialidad, integridad y disponibilidad de sus activos de información en cumplimiento de los requisitos aplicables. La protección de la información; busca la disminución del impacto generado sobresus activos, por los riesgos identificados de manera sistemática con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados

Para dar cumplimiento a la policita de gobierno digital la administración de Pisba ha definido los siguientes parámetros:

- Cada funcionario de la ESE Hospital San Lucas de El Molino, tendrá un usuario con contraseña personal e intransferible de los aplicativos, correo electrónico, plataformas institucionales y demás para el desempeño de sus funciones.
- El correo electrónico, claves de internet, y chat son de carácter personal e intransferible, es deber de cada uno de los usuarios mantener el uso de

estas y de sus contraseñas, por ningún motivo se debe permitir a otra persona acceder a estos recursos.

- La contraseña definida por cada usuario debe contener los estándares de seguridad definidos en el plan de seguridad y privacidad de la información.

- La entidad deberá restringir el acceso a los sitios relacionados con redes sociales, con el fin de aumentar la velocidad de acceso y el riesgo de virus. Si algún funcionario por motivos de trabajo requiere acceso a ellos, deberá enviarla solicitud a la Gerencia.

- Tendrán acceso a redes sociales un grupo de usuario, teniendo en cuenta sus funciones.

- Toda información que se publique o divulgue por cualquier medio de internet de cualquier funcionario, contratista o colaborador que sea creado a nombre personal como redes sociales, se considera fuera del dominio de la ESE Hospital San Lucas de El Molino, por lo tanto, su integridad, confiabilidad, disponibilidad y daños y perjuicios que se puedan generar, serán de completa responsabilidad de la persona que las haya generado.

- No debe descargarse juegos ni aplicativos en ninguno de los equipos de la administración.

- Los equipos de cómputo y de comunicaciones de la Entidad deben utilizarse únicamente para asuntos de carácter institucional.

- El uso e información de cada equipo es responsabilidad del funcionario asignado.

9.1 LINEAMIENTOS PARA MEDIOS REMOVIBLES

Son medios removibles todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores, para lo cual se establecen los siguientes lineamientos.

- Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales.

- El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la ESE Hospital San Lucas de El Molino y deben ser usados únicamente para el cumplimiento de la misión de la Entidad.

- El manejo, configuración, y actualización de la página institucional es exclusivamente del área responsable de sistemas, o del personal que deleguela Gerencia para tal fin.

- Los usuarios deben tratar los mensajes de correo electrónico, chat y archivos adjuntos como información de propiedad de la ESE Hospital San Lucas de El Molino.

- Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

- Cuando un funcionario que tiene asignada una cuenta de correo de la entidad, deberá entregar a la Gerencia los usuarios y password asignados, de igual manera dicha información debe entregarse cuando exista un proceso de empalme.

9.2 PRIVACIDAD Y CONFIDENCIALIDAD

9.2.1 Política de Tratamiento de Datos Personales

Los datos personales que los ciudadanos, usuarios, servidores públicos, proveedores suministren a la ESE Hospital San Lucas de El Molino, en cualquiera de sus procesos, serán utilizados para la prestación del servicio solicitado y serán incorporados en una base de datos cuya responsabilidad y manejo está a cargo del Municipio de Pisba. Los datos personales suministrados serán administrados de forma confidencial y con la finalidad de brindar los servicios y el soporte requerido por el usuario, con las debidas garantías constitucionales, legales y demás normas aplicables a la protección de datos personales.

La ESE Hospital San Lucas de El Molino, transferirá la información a un tercero únicamente si está obligado a hacerlo por orden de autoridad administrativa o judicial.

La ESE Hospital San Lucas de El Molino, se abstiene de ceder, vender o compartir los datos de carácter personal recolectados, sin la expresa autorización del usuario.

La ESE Hospital San Lucas de El Molino, no responderá en ningún caso y bajo ninguna circunstancia,por los ataques o incidentes contra la seguridad de su sitio web o contra sus sistemas de información; o por cualquier exposición o acceso no autorizado,fraudulento o ilícito a su sitio web y que afecten la confidencialidad, integridad o autenticidad de la información publicada o asociada con los

contenidos y servicios que se ofrecen en él.

9.2.2 Tratamiento de los datos

El Tratamiento de los datos se realizará para:

La vinculación, desempeño de funciones o prestación de servicios, retiro o terminación.

Para seguridad de las personas, los bienes e instalaciones de la entidad.

Para los fines relacionados con el desarrollo el proceso de gestión contractual de productos o servicios que la entidad requiera para su funcionamiento de acuerdo a la normatividad vigente.

9.2.3 Derechos de los titulares

Conocer, actualizar y rectificar sus datos personales frente al responsable y encargado del tratamiento. Este derecho se podrá ejercer entre otros ante datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

Solicitar prueba de la autorización otorgada al Municipio como responsable y encargado del tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de laLey 1581 de 2012.

Ser informado por el Municipio como responsable del tratamiento y encargado del tratamiento, previa solicitud, respecto del uso que les ha dado a los datos personales del Titular.

Presentar ante el Municipio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.

Revocar la autorización y/o solicitar la supresión del dato personal cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

La revocatoria y/o supresión procederá cuando el Municipio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a la Ley 1581 de 2012 y a la Constitución.

9.2.4 Autorización del titular

Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa, expresa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

Casos en que no se requiere la autorización: La autorización del Titular no será necesaria cuando se trate de:

- *Información requerida por la ESE Hospital San Lucas de El Molino en ejercicio de sus funciones legales opor orden judicial.*
- *Datos de naturaleza pública.*
- *Casos de urgencia médica o sanitaria.*
- *Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.*
- *Datos relacionados con el Registro Civil de las Personas.*

9.2.5 Acuerdo de confidencialidad

Implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

10. SEGURIDAD DE COMPUTADORES Y PORTÁTILES

Para lograr un alto rendimiento y salvaguarda de computadores y portátiles, la ESE Hospital San Lucas de El Molino ha definido los siguientes parámetros.

- Los computadores de mesa, portátiles, y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la aprobación del Jefe del área.
- El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de la ESE Hospital San Lucas de El Molino.

- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.

- Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previniendo así la pérdida involuntaria de información, derivada del proceso de reparación.

- Los equipos de la ESE Hospital San Lucas de El Molino sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

- Debe respetarse y no modificar la configuración de hardware y software establecida por la oficina o área de sistemas.

- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en computadores que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN o WAN de la ESE Hospital San Lucas de El Molino.

- A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón, es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente a la oficina de las TIC y poner el computador en cuarentena hasta que el problema sea resuelto.

- No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por la oficina o are de sistemas de la ESE Hospital San Lucas de El Molino.

- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario.

- El personal que utiliza un computador portátil que contenga información confidencial de la institución, no debe dejarlo desatendido, sobre todo cuando esté de viaje.

- El área de Sistemas, no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de la ESE Hospital San Lucas de El Molino.

- Se prohíben que los equipos estén en contacto con piso, el usuario debe disponerlo (computador y/o Portátil) sobre el escritorio.

- Los recursos de Gobierno Digital, utilizados para el procesamiento de la información deben ser ubicados en sitios estratégicos, que faciliten el trabajo compartido, el trabajo colaborativo, la optimización de recursos.

11. ESTRATEGIAS

Para la implementación de la Política, la ESE Hospital San Lucas de El Molino ha definido las siguientes estrategias.

- Habilitar y mejorar la provisión de servicios digitales de confianza y calidad
- Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías procesos e información.
- Tomar decisiones basadas en datos a partir del aumento en el aprovechamiento de la información.
- Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto.
- Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de tecnologías de la Información.

ISABEL PAULINA APONTE DIAZ
GERENTE