Código:	PE01 PO 57	**POLÍTICA SEGURIDAD DIGITAL**	Metrosalud®
Versión:	02		
Vigente a partir de:	23/09/2024		
Página:	1 de 5		

Descripción de la política

(Describe el compromiso que la institución está dispuesta a cumplir, cuál es la posición de la administración o qué es lo que se desea regular. Debe responder al Qué, Cómo, Para qué)

La ESE Metrosalud asume el compromiso adoptar e implementar la política de Seguridad Digital estableciendo las reglas, los lineamientos, estrategias y mecanismos para garantizar la seguridad y disponibilidad de los activos informáticos, definiendo controles que permitan mitigar los riesgos de delitos informáticos a los que se exponen los usuarios de la Subred al conectarse a la red de datos mediante un dispositivo digital.

Responsable Institucional

(La Unidad Administrativa responsable de liderar la política, el cargo del responsable institucional y el cargo del Gestor institucional de política)

Unidad Administrativa: Dirección Sistemas de Información

Líder de política: Director Sistemas de Información

Gestor de política: Profesional Universitario (analista software)

Marco normativo

(Directriz gerencial o normatividad que soporta la política)

- Modelo Integrado de Planeación y Gestión (MIPG)
- Constitución Política Colombiana 1991, artículos 2, 123 y 209 ✓ Ley 1437 de 2011 "Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo".
- Lay 962 de 2005, racionalización de trámites y procedimientos administrativos.
- Acuerdo 279 de 2007. Lineamientos de política para la promoción y uso del software libre en el sector público.
- Decreto 619 establece la estrategia del gobierno electrónico.

Lineamientos para implementación

(Define cuáles son las estrategias y/o lineamientos de la ESE Metrosalud para el desarrollo e implementación de la política y lograr su propósito y los mecanismos que usará para dar a conocerla)

En la ESE Metrosalud, esta política se implementa a través de:

- Proceso Gestión del sistema de información
- La implementación del PE02 MA 429 MA MANUAL SISTEMA DE GESTIÓN DE RIESGOS

El esquema que resume el desarrollo de la política en la ESE Metrosalud es el siguiente ciclo de actividades:

La política de seguridad digital incluye el concepto de seguridad digital en la implementación y desarrollo del Plan de Seguridad y Privacidad de la Información, teniendo en cuenta la normatividad vigente y los eventuales cambios que se puedan presentar.

Para el desarrollo de una cultura de seguridad digital se establece un proceso de capacitación permanente en seguridad de la información y seguridad digital a todos los colaboradores y demás grupos de interés externos que se identifiquen.

Los lineamientos pretenden fortalecer la infraestructura en hardware y software que permita prevenir, atender y controlar los eventos de seguridad digital que se puedan presentar en el desarrollo de las actividades propias de la entidad. En el marco de la gestión de riesgos se incluirán los identificados con eventos de seguridad informática derivados de las debilidades de los sistemas de información y demás plataformas informáticas, mediante la implementación de estrategias de mejoramiento continuo.

La protección de la información busca reducir el impacto de la materialización de los riesgos digitales sobre los activos de información con el fin de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de valor identificados.

Articulación con los planes institucionales:

Para el desarrollo de la política la ESE Metrosalud definirá los planes operativos necesarios que le permitan lograr los objetivos programáticos de las respectivas vigencias. Estos planes se articularán con los objetivos estratégicos y con las estrategias institucionales dando pie a la aparición del plan de acción de la Dirección de Talento Humano o quien haga sus veces.

El Plan de acción de la vigencia soporta las acciones básicas de planeación relacionadas con la política. Este plan cuenta con un método de formulación, seguimiento y evaluación estandarizada. De igual forma con una frecuencia de seguimiento y evaluación determinada. Ver:

PE01 ME 74 ME METODOLOGÍA FORMULACIÓN Y DESPLIEGUE DE PLANES, PROGRAMAS Y PROYECTOS INSTITUCIONALES
PE01 DT 446 DT DOCUMENTO TÉCNICO LINEAMIENTOS PARA FORMULACIÓN PLAN ACCIÓN

Adicionalmente Metrosalud cuenta con:

PE01 PL 19 PL PLAN TRATAMIENTO RIESGOS SEGURIDAD Y PRIVACIDAD INFORMACIÓN

Indicadores

(Defina los indicadores que va a utilizar para medir el cumplimiento de la política)

Cumplimiento del plan de seguridad y privacidad de la información

Cumplimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información

Seguimiento y evaluación

(Describe cómo se realizará el seguimiento y evaluación de la política. Detalla la frecuencia de seguimiento y evaluación, responsables, informes o reportes y comités o grupos de trabajo donde se analizará el desempeño de la política)

Seguimiento a la política:

La implementación de la política estará determinada por el seguimiento sistemático de los indicadores definidos para medir la Política de Seguridad Digital.

Como resultado del seguimiento se elaborará un informe ejecutivo semestral que dé cuenta del avance de la implementación de la política y los aspectos relevantes que han afectado esta.

Responsable: Director Sistemas de información.
Frecuencia: Semestral.
Mecanismo de seguimiento: Indicadores de la política.
Resultado: Informe del desempeño de los indicadores.
Comité o equipo de trabajo donde se analiza: Comité Institucional de Gestión y Desempeño

Evaluación de la política:

La política se evaluará cada año mediante el uso de mecanismos o instrumentos de evaluación y/o autoevaluación definidos por el DAFP y/o el ente regulador de la política estatal.

En caso de no estar estandarizados los mecanismos y/o instrumentos, estos se desarrollarán en correspondencia con los estándares y criterios establecidos en las normas técnicas o legales vigentes y se llevará a cabo como una autoevaluación de un elemento organizacional a través del aplicativo del sistema integrado de gestión.

Responsable: Director Sistemas de Información - Jefe Oficina Asesora de Planeación y desarrollo Organizacional.
Frecuencia: Anual.
Mecanismo de evaluación: Formulario Único Reporte de Avances a la Gestión FURAG – Formulario Autoevaluación de la Política.
Resultado: Informe de Autoevaluación de la política.
Comité o equipo de trabajo donde se analiza: Comité Institucional de Gestión y Desempeño.

En el marco de las líneas de defensa:

Línea Estratégica:

El Gerente (O quien haga sus veces) determina y direcciona la política de Atención Centrada en el usuario y su aplicación en todos los niveles jerárquicos de la estructura.

Primera línea de defensa:
Servidores que hacen parte de la ejecución de los procesos, procedimientos, planes y programas relacionados directamente con el propósito misional.
Director de Sistemas de Información – Responsable del proceso de gestión del sistema de información y de los planes que se implementen en desarrollo de la política de seguridad digital.
Equipos de trabajo de las UPSS (O quienes hagan sus veces). A través del seguimiento a los Procesos, Procedimientos, Programas, Planes y proyectos que tienen relación con la política de Seguridad Digital o a través de los indicadores definidos.

Segunda línea de defensa:
Mediante el monitoreo al seguimiento y evaluación realizado por la Oficina Asesora de Planeación y Desarrollo Organizacional (O quien haga sus veces, por el Comité de Gerencia y el Comité Institucional de Gestión y Desempeño a la aplicación de indicadores o puntos de control.

Tercera Línea:
A través de la evaluación de los elementos de la política mediante auditoría independiente y objetiva por parte de la Oficina de Control Interno y Evaluación, que realice una evaluación de aseguramiento sobre la efectividad, implementación y adecuada operación de la política de Seguridad Digital en Metrosalud.

ELABORADO POR:	
Anderson Ospina Sierra	Cargo: Director Sistemas de Información
Santiago Zapata García	Cargo: Profesional Universitario (Analista Software)

CONTROL DE ACTUALIZACIÓN

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO O AJUSTE	RAZÓN DEL CAMBIO O AJUSTE	RESPONSABLE DEL CAMBIO O AJUSTE
01	01/10/2019	Se crea la política para el seguridad de la información para soportar las directrices institucionales relacionadas con	Con el propósito de formalizar las políticas institucionales y responder a requerimientos normativos.	Director Sistemas de Información

CONTROL DE ACTUALIZACIÓN

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO O AJUSTE	RAZÓN DEL CAMBIO O AJUSTE	RESPONSABLE DEL CAMBIO O AJUSTE
		manejo de información.		
02	23/09/2024	Se ajusta la denominación de la política de seguridad de la información por Seguridad Digital. Además, se ajusta la política en los siguientes aspectos: 1. Establecer el direccionamiento estratégico- ESE Metrosalud 2. Definición de los planes institucionales – ESE Metrosalud 3. Despliegue del plan de desarrollo, planes y programas institucionales	De conformidad con los lineamientos del Modelo Integrado de Planeación y Gestión del estado Colombiano y el sistema de gestión de riesgos de la ESE Metrosalud.	Director Sistemas de Información