PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

ADRIANA MARIA VALÁSQUEZ ARANGO

Gerente (E) ESE Metrosalud

Dirección Operativa de Talento Humano

28/01/2026

Versión [06]

Contenido

1. PLATAFORMA ESTRATÉGICA Y CONTENIDO INSTITUCIONAL 3
2. OBJETIVOS 5
3. MARCO NORMATIVO 5
4. DESARROLLO DEL PLAN 5
5. DOCUMENTOS RELACIONADOS: 12
6. ANEXOS: 12

1. PLATAFORMA ESTRATÉGICA Y CONTENIDO INSTITUCIONAL

Plataforma Estratégica

Organigrama institucional. Ver enlace:

http://www.metrosalud.gov.co/metrosalud/organigrama

Mapa de procesos. Ver enlace:

http://www.metrosalud.gov.co/metrosalud/estructura-de-procesos

Deberes y Derechos de los usuarios. Ver enlace

http://www.metrosalud.gov.co/usuarios/derechos-y-deberes

- **POLÍTICAS RELACIONADAS**.

Política de Gestión de la Tecnología

Con el fin de garantizar una adecuada ejecución en los procesos de evaluación para la adquisición de tecnología biomédica y vigilancia tecnológica, la ESE Metrosalud se compromete en la implementación de un Sistema de Gestión de Tecnología, que brinde la orientación estratégica y permita la adquisición, instalación, uso y mantenimiento seguro y eficiente de las tecnologías en salud acorde a las necesidades de los pacientes y a la complejidad de los servicios ofertados por la institución, en sus etapas de promoción, prevención, diagnóstico, tratamiento y rehabilitación, que permita responder a los objetivos de desarrollo institucional, que sea segura para los pacientes, costo efectiva, que cumpla con estándares de calidad y con la normatividad legal vigente.

La política de gestión de la tecnología orientará los parámetros para la evaluación de tecnologías en salud de acuerdo con el ciclo de vida para la evaluación de tecnologías sanitarias comprendido desde la planeación, selección, adquisición, instalación, uso, mantenimiento y calibración, hasta su disposición final.

Política de seguridad digital

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.

Política de gestión de riesgos

La ESE Metrosalud se compromete a gestionar los riesgos de gestión u operativos, riesgos de corrupción, opacidad y fraude y riesgos de lavado de activos y financiación del terrorismo, riesgos de proliferación de armas de destrucción masiva, desarrollando y poniendo en operación mecanismos efectivos que contemplan la identificación, análisis, valoración, tratamiento y monitoreo de los riesgos, que actúen sobre las situaciones que impiden el normal desarrollo de los procesos y las funciones, orientando la toma de decisiones oportuna con el fin de asegurar el cumplimiento de los objetivos institucionales, mitigar el impacto negativo de los riesgos para los usuarios, familia, servidores, proveedores, comunidad y grupos de interés y aprovechar el impacto positivo de los mismos.

Para todo lo anterior, el Gerente de la ESE Metrosalud, dispondrá los recursos humanos, financieros, técnicos, tecnológicos y logísticos que sean necesarios para la gestión de los riesgos LA/FT/PADM y COF (Lavado de Activos, Financiación del Terrorismo, Proliferación de Armas de Destrucción Masiva, y Corrupción, Opacidad, Fraude).

2. OBJETIVOS

Objetivo General

Identificar los riesgos de los componentes informáticos y de la gestión de información mediante la aplicación de la metodología institucional con el fin de salvaguardar los activos de Información, el control de acceso y la gestión de usuarios.

Objetivos Específicos

- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.
- Generar Conciencia a todos los funcionarios sobre la importancia de gestionar de manera adecuada, los riesgos inherentes a cada proceso.
- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

3. MARCO NORMATIVO

No aplica

4. DESARROLLO DEL PLAN

ALCANCE

Este plan suministra los principios y directrices para la gestión de riesgos en los sistemas de información, de una manera sistemática, secuencial y lógica, a través de una serie de pasos o etapas, que van desde la definición del "contexto del riesgo" y del "contexto organizacional" hasta el "tratamiento del riesgo" enfocado a los sistemas de información de la ESE Metrosalud.

4.1 FORMULACIÓN

ÁMBITO DE APLICACIÓN

La gestión del riesgo es el término aplicado a un método lógico y sistemático, iterativo, compuesto por una serie de pasos que, si se ejecutan secuencialmente, permiten la mejora continua en la toma de decisiones.

Esta metodología puede aplicarse a todo plan, programa, proyecto o proceso de la organización.

ROLES Y RESPONSABILIDADES EN LA GESTIÓN DEL RIESGO

Unidad Administrativa Responsable	Unidad Administrativa Corresponsable	Proceso
Subgerencia Administrativa y Financiera	Dirección de Sistemas de Información	Gestión de la Información

ANALISIS DE RIESGOS PARA EL SISTEMA DE INFORMACION EN LA E.S.E METROSALUD

La E.S.E Metrosalud, ha venido implementando un conjunto de soluciones informáticas que han hecho que sus procesos asistenciales y administrativos tengan una gran dependencia de su infraestructura informática, aumentando la vulnerabilidad ante la probabilidad de ocurrencia de riesgos que afecten la disponibilidad de la infraestructura informática y la información.

Queremos identificar los riesgos asociados a nuestro sistema de información y para ello desarrollaremos una serie de actividades, como la identificación de escenarios sujetos a control, que son las tareas o procesos macro del área de sistemas y las actividades que las componen. Desde la parte técnica de sistemas se identifican los riesgos asociados a esos componentes y con esta información se realiza una calificación; básicamente consiste en indagar con grupos de usuarios del sistema de información sobre el daño y las pérdidas que cierto problema puede causar y asignar una probabilidad de ocurrencia y una impacto de pérdida; no obstante, la condición técnica del administrador del sistema, en materias de seguridad informática puede tener aquí la última palabra a la hora de evaluar los impactos de cada amenaza, basándonos en los siguientes aspectos:

- La evaluación de los riesgos inherentes a los procesos informáticos.
- La evaluación de las amenazas o causas de los riesgos.
- Los controles utilizados para minimizar las amenazas a riesgos.
- La asignación de responsables a los procesos informáticos.
- La evaluación de los elementos del análisis de riesgos.

CALIFICACIÓN DEL RIESGO

El riesgo se califica en función de su probabilidad de ocurrencia y el impacto que tenga sobre el sistema de información en caso de que se materialice el riesgo, se califica en la escala de alto A, medio M, y bajo B, para determinar su peso.

Se Pondera la probabilidad de ocurrencia Vs el impacto o costo, según la siguiente tabla:

ALTO+ALTO = ALTO

ALTO+MEDIO = ALTO

ALTO+BAJO = MEDIO

MEDIO+MEDIO = MEDIO

MEDIO+BAJO = BAJO

BAJO+BAJO = BAJO

La calificación definitiva nos mostrará los riesgos de probabilidad de ocurrencia alto y de mayor impacto, sobre este grupo se realiza un trabajo de identificación de controles que permitan mitigar su probabilidad de ocurrencia.

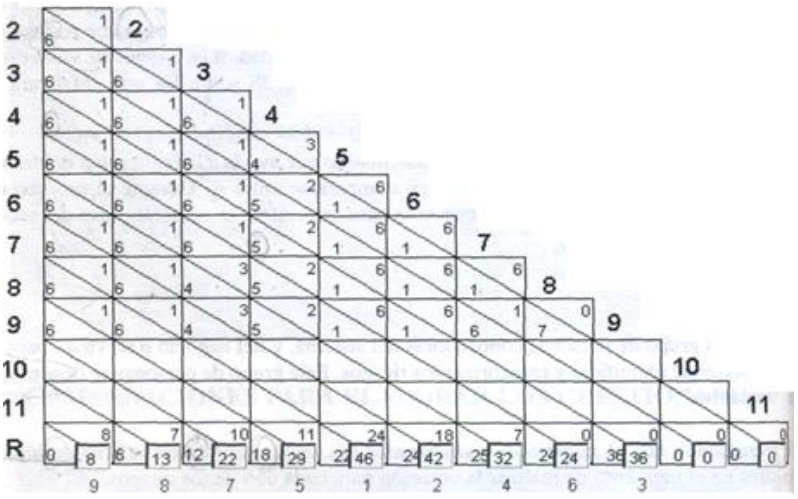
DESCRIPCION DEL METODO

Al tener la selección de los riesgos, requerimos dar un orden de prioridad, para determinar la vulnerabilidad Alta y Media Alta, aplicando el Principio de Pareto.

Usamos un modelo matemático para comparar entre si los riesgos, un grupo de personas conocedoras del sistema califican cada riesgo, no se pueden abstener de votar, la lista de riesgos debe estar previamente establecida. El grupo tendrá en cuenta si es posible o no que se presente el riesgo y en qué forma podría presentarse el riesgo para nuestro sistema en el E.S.E METROSALUD

Hacemos una comparación de la magnitud del impacto negativo (Económico o aspectos que afecten la misión de la institución) que tendría la ocurrencia de un riesgo con respecto a la ocurrencia de cada uno de los demás riesgos. Se compara cada uno de los riesgos que conforman el modelo contra los demás, mediante votación.

El resultado de la votación se registra en un gráfico así:



A cada uno de los riesgos seleccionados se le asigna un número. Estos números se ubican tanto en la parte izquierda de cada fila como en la parte superior de la columna. Cada celda se divide en "a" y "b" en "b" se registra el valor de las filas y en "a" el de las columnas.

Una vez terminada la votación se totalizan los resultados en la fila identificada con la letra "R" (Resultados) de la siguiente manera:

Celda R:

R

- En la sección "a" de la celda "R" se anota la sumatoria de los puntajes registrados en las secciones superiores ("a") de todos los cuadros pertenecientes a esa columna.
- En la sección "b" de la celda "R" se anota la sumatoria de los puntajes registrados en las secciones inferiores ("b") de todos los cuadros pertenecientes a la fila identificada con el número que encabeza la respectiva columna.
- En el cuadro "c" que se encuentra en la parte inferior derecha de cada uno de los cuadros de la fila de resultados, se contabiliza la sumatoria de las dos secciones que lo conforman ("a'V'b").
- En la parte inferior del gráfico se numera cada uno de los riesgos, en orden ascendente, luego de comparar todos sus totales entre sí. Esta es la categorización de los riesgos.

El puntaje máximo que puede obtener un riesgo, se calcula con la siguiente fórmula:

- PMP = Np x (Ra - 1) En donde:
- PMP: Puntaje máximo que puede obtener un riesgo.
- Np: Número de participantes Ra: Riesgos aplicables

Este puntaje máximo PMP se toma como base para establecer los intervalos que se utilizarán para categorizar los puntajes obtenidos por cada uno de los riesgos. Teniendo la calificación de los riesgos, se determina según el principio de pareto teniendo en cuenta el puntaje PMP.

VULNERABILIDAD	PORCENTAJE
ALTA	80% - 100%
MEDIA ALTA	60% - 80%
MEDIA	40% - 60%
MEDIA BAJA	20% - 40%
BAJA	0% - 20%

Un riesgo crítico será solo si su vulnerabilidad es alta o media alta, y sobre estos se establecerán los controles necesarios y suficientes para mitigar su impacto.

IDENTIFICACION DE LOS CONTROLES

Se realiza mediante la lluvia de controles, y se clasifica el control de acuerdo a 3 categorías (Preventivo, detectado o correctivo), que tienen un valor de 3, 2, 1 respectivamente.

Para cada riesgo se debe plantear una fórmula o mezcla de controles, cuyos requisitos son:

- La mezcla debe tener uno de cada clase.
- Cuando se selecciona el control se debe especificar la categoría para su implementación (un control puede ser de varias categorías para la mezcla)
- La mezcla de controles debe ser mayor que 2 para garantizar que es necesario y suficiente.

Mezcla de controles = (Sumatoria de los valores de los controles preventivos + valores de los controles detectados + valores de los controles correctivos) / Total de controles

Si mz<2 Los controles son insuficientes para mitigar el riesgo

Si mz =2 Los controles son necesarios pero mejorables

Si mz >2 Los controles son necesarios y suficientes

ANALISIS DE RIESGOS E.S.E METROSALUD

- **ACTIVIDADES INHERENTES A LA GESTION INFORMATICA (ESCENARIOS SUJETOS A CONTROL)**

1. Políticas de seguridad de la información
2. Plan de contingencias
3. Administración de proveedores
4. Administración de red de datos
5. Administración de red eléctrica
6. Plan estratégico de sistemas
7. Sistema de documentación de procesos y procedimientos

- **ACTIVIDADES SUJETAS A CONTROL POR ESCENARIOS**

Políticas de seguridad de la información

1. Asignación de nombres de usuario
2. Asignación de claves de usuario
3. Normas de acceso físico
4. Definición de firewall
5. Almacenamiento de los Backup
6. Capacitación a usuarios
7. Divulgación de las políticas

Plan de contingencias

1. Administración de las copias de seguridad
2. Definición de prioridad de los recursos sensitivos
3. Simulación del plan de contingencias
4. Definición de eventos críticos
5. Protección al hardware
6. Protección al software
7. Definición del equipo de contingencia

Administración de proveedores

1. Análisis del proveedor
2. Análisis financiero
3. Análisis técnico
4. Elaboración del documento de selección

Administración de red de datos

1. Definición de políticas
2. Elaboración de planos
3. Definición del tipo de red (Direccionamiento)
4. Definición de la topología
5. Elaboración de esquema de mantenimiento

Administración de red eléctrica

1. Definición de políticas
2. Elaboración mapa de la red
3. Selección del sistema de protección
4. Elaboración del esquema de mantenimiento

Plan estratégico de sistemas

1. Análisis del sistema actual
2. Definición de estrategias
3. Definición de actividades

Sistema de documentación de procesos y procedimientos

1. Definición de medios de difusión
2. Elaboración de estándares de terminología
3. Elaborar sistema de seguimiento a su ejecución

4.2 IMPLEMENTACIÓN Y DESPLIEGUE

Se divulgará a través del software Almera, se publicará en la página web (Ítem transparencia) y se socializará al personal de la Dirección de sistemas de información.

4.3 SEGUIMIENTO – MONITOREO

Para dar cumplimiento al Decreto 612 de 2018, se realizará el respectivo seguimiento a cada una de las actividades mencionadas anteriormente.

La ESE METROSALUD, generará los mecanismos e instrumentos necesarios que brinden las garantías para el desarrollo del Plan de riesgos de seguridad y privacidad de la información.

La ESE METROSALUD, implementará con los diferentes equipos de trabajo, los distintos procedimientos que permitan tener la documentación actualizada y disponible como guía para las buenas prácticas.

El seguimiento al plan se realizará a través del software Almera y se apoyará en la matriz de seguimiento de actividades plan adjunta.

Utilice el Utilice la matriz de seguimiento de actividades.

4.4 EVALUACIÓN

El seguimiento se realizará en el aplicativo Almera trimestralmente con reportes de avance del mismo. Se obtendrá el nivel de cumplimiento del plan a través del software Almera.

La evaluación estará a cargo de la Dirección de sistemas de información y se articulará en el reporte del seguimiento y evaluación al plan de acción de la vigencia.

5. DOCUMENTOS RELACIONADOS:

No aplica

6. ANEXOS:

No aplica

ELABORADO POR:	
Anderson Ospina Sierra	Director de Sistemas de Información
Jorge Adrian Ceballos Gallo	Profesional Universitario
Santiago Zapata García	Profesional Universitario infraestructura

CONTROL DE ACTUALIZACIÓN

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO O AJUSTE	RAZÓN DEL CAMBIO O AJUSTE	RESPONSABLE DEL CAMBIO O AJUSTE
01 Almera	22/01/2019	Se crea el plan en el software Almera.	Actualización de la documentación en el nuevo software.	Director Sistemas de Información
02 Almera	30/01/2019	Se crea el plan en correspondencia con la estructura documental.	Se crea el plan para responder a requerimientos normativos.	Director Sistemas de Información
03 Almera	23/01/2023	Se crea el plan en correspondencia con la estructura documental.	Se crea el plan para responder a requerimientos normativos.	Director Sistemas de Información
04 Almera	20/01/2024	Se crea el plan en correspondencia con la estructura documental.	Se crea el plan para responder a requerimientos normativos.	Director Sistemas de Información

05 Almera	27/01/2025	Se crea el plan en correspondencia con la estructura documental.	Se crea el plan para responder a requerimientos normativos.	Director Sistemas de Información
06 Almera	28/01/2026	Se crea el plan en correspondencia con la estructura documental.	Se crea el plan para responder a requerimientos normativos.	Director Sistemas de Información