



PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022

MARTHA CECILIA CASTRILLON SUAREZ

Gerente ESE Metrosalud

Dirección sistemas de información

27/01/2022

Versión [02]



Alcaldía de Medellín

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2021		
Página:	2 de 21		

Contenido

PLATAFORMA ESTRATÉGICA Y CONTENIDO INSTITUCIONAL.....	4
1. LINEAMIENTOS DE POLÍTICA	4
2. INTRODUCCIÓN.....	5
3. OBJETIVOS.....	6
3.1. OBJETIVO GENERAL.....	6
3.2. OBJETIVOS ESPECÍFICOS.....	6
4. ALCANCE	6
5. DESARROLLO DEL PLAN	7
5.1. FORMULACIÓN.....	7
5.1.1. ÁMBITO DE APLICACIÓN.....	7
5.1.2. ROLES Y RESPONSABILIDADES EN LA GESTIÓN DEL RIESGO	7
5.1.3. POLÍTICA DE GESTION DEL RIESGO	7
5.1.4. ANALISIS DE RIESGOS PARA EL SISTEMA DE INFORMACION EN LA E.S.E METROSALUD	7
5.1.5. CALIFICACIÓN DEL RIESGO.....	8
5.1.6. DESCRIPCION DEL METODO	9
5.1.7. IDENTIFICACION DE LOS CONTROLES.....	11
5.1.8. ANALISIS DE RIESGOS E.S.E METROSALUD.....	12
• ACTIVIDADES INHERENTES A LA GESTION INFORMATICA (ESCENARIOS SUJETOS A CONTROL).....	12
5.2. IMPLEMENTACIÓN Y DESPLIEGUE	13
5.3. SEGUIMIENTO – MONITOREO	13
5.4. EVALUACIÓN.....	14
6. DEFINICIONES Y CONCEPTOS	15

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	3 de 21		

PLATAFORMA ESTRATÉGICA Y CONTENIDO INSTITUCIONAL

Misión, Visión Ventaja competitiva, Promesa de valor, Objetivos corporativos, Competencias corporativas. Ver enlace

<http://www.metrosalud.gov.co/metrosalud/institucional>

Principios y valores corporativos. Ver enlace:

<http://www.metrosalud.gov.co/metrosalud/principios-y-valores>

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>

1. LINEAMIENTOS DE POLÍTICA

Política de gestión de riesgos:

La ESE Metrosalud se compromete a gestionar los riesgos de gestión u operativos, riesgos de corrupción y riesgos de lavado de activos y financiación del terrorismo, 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.

Política de seguridad de información:

En Metrosalud estamos comprometidos con garantizar la seguridad, confidencialidad, oportunidad y accesibilidad de la información, a través del uso adecuado de los activos y recursos tecnológicos, mediante la identificación, priorización, aplicación e implementación de controles que permitan mitigar la pérdida de información útil,

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	5 de 21		

Generando confiabilidad, veracidad y validez de los datos a los usuarios, servidores, proveedores y demás partes interesadas, mejorando constantemente la calidad de la información y cumpliendo con los requisitos legales vigentes.

2. INTRODUCCIÓN

Administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	6 de 21		

3. OBJETIVOS

3.1. 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.

3.2. 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.

4. 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.

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	7 de 21		

5. DESARROLLO DEL PLAN:

5.1. FORMULACIÓN

5.1.1. 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.

5.1.2. 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

5.1.3. POLÍTICA DE GESTION DEL RIESGO

La ESE Metrosalud se compromete a gestionar los riesgos, desarrollando y poniendo en operación mecanismos efectivos, que actúen sobre las situaciones que impiden el normal desarrollo de los procesos y las funciones, con el fin de asegurar el cumplimiento de los objetivos misionales y mitigar el impacto negativo de las decisiones tomadas frente a los usuarios, familia, servidores, proveedores, comunidad y grupos de interés.

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	8 de 21		

5.1.1. 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 un 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.

5.1.2. 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.

Código:	PE01 PL 19
Versión:	02
Vigente a partir de:	30/01/2020
Página:	9 de 21

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



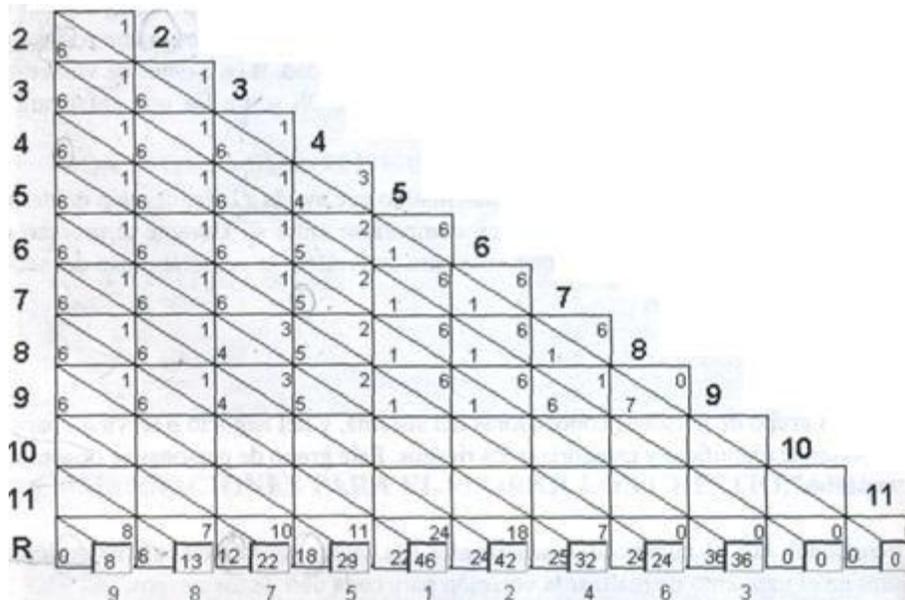
5.1.3. DESCRIPCIÓN DEL METODO

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

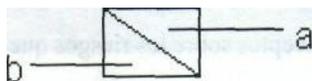
Hacemos una comparación de la magnitud del impacto negativo (Económico o aspectos que afecten la misión de la institución) que tendría la ocurrencia de un riesgo con respecto a la ocurrencia de cada uno de los demás riesgos. Se compara cada uno de los riesgos que conforman el modelo contra los demás,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

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	10 de 21		



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 subcuadro "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 ("aVb").
- 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:

- $PMP = Np \times (Ra - 1)$ 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.

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	11 de 21		

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.

5.1.4. IDENTIFICACION DE LOS CONTROLES

Se realiza mediante la lluvia de controles, y se clasifica el control de acuerdo a 3 categorías (Preventivo, detectivo 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 detectivos + 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

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	12 de 21		

5.1.5. 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 types backups
6. Capacitación a usuarios
7. Divulgación de las políticas

Plan de contingencias

1. Administración de los cartuchos de type backups
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

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	13 de 21		

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

5.2. 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.

5.3. 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.

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	14 de 21		

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 practicas.

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.

5.4. 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.

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	15 de 21		

6. DEFINICIONES Y CONCEPTOS

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

Acciones asociadas: son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar, compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.

Administración de riesgos: conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

Amenaza: situación externa que no controla la entidad y que puede afectar su operación

Análisis del riesgo: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

Asumir el riesgo: opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.

Causa: medios, circunstancias y/o agentes que generan riesgos.

Calificación del riesgo: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

Compartir o transferir el riesgo: opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

Consecuencia: efectos que se pueden presentar cuando un riesgo se materializa.

Contexto estratégico: son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

Control: acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

Control preventivo: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

Control correctivo: acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	16 de 21		

Debilidad: situación interna que la entidad puede controlar y que puede afectar su operación.

Evaluación del riesgo: resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

Evitar el riesgo: opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.

Frecuencia: ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

Identificación del riesgo: etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos

Impacto: medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

Mapa de riesgos: documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

Materialización del riesgo: ocurrencia del riesgo identificado

Opciones de manejo: posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar, compartir o transferir el riesgo residual).

Plan de contingencia: conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio

Probabilidad: medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

Procedimiento: conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

Proceso: conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	17 de 21		

Riesgo: eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

Riesgo de corrupción: posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

Riesgo inherente: es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

Riesgo institucional: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

- Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
- Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
- Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
- Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

Riesgo residual: nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

Valoración del riesgo: establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.



Código:	PE01 PL 19
Versión:	02
Vigente a partir de:	30/01/2020
Página:	18 de 21

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

ELABORADO POR:

Nombre: Jaime Alberto Henao Acevedo	Cargo: Director Sistemas de Información
Nombre: Gustavo Alonso Morales Correa	Cargo: Profesional Universitario
Nombre: Leonardo Juan Salgado Agudelo	Cargo: Profesional Universitario

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

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	19 de 21		

Código:	F0103010118	MATRIZ DE SEGUIMIENTO DE ACTIVIDADES PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN												
Versión:	1													
Vigente a partir de:	12/12/2018													
Página:	1 de __													
N°	Nombre de la Actividad	Acciones o Tareas principales	Indicador o Producto	Meta	Fecha inicio	Fecha final	Avance Programado						Responsable de la Actividad	% Cumplimiento
							B1	B2	B3	B4	B5	B6		
1	Red de datos sin las condiciones técnicas requeridas para soportar los componentes del sistema de información en algunos puntos de atención.	Proyecto de segmentación de la red elaborado e implementado (Para CS, UH, Sacatin)	Red de datos segmentada por Vlan. Documento de configuración de la red de datos	1	01/03/2022	31/12/2022							Director Sistemas de Información	
2	Hacking Ético	Test a la red de datos	Informe de vulnerabilidades y plan de remediación.	1	01/05/2022	30/11/2022							Director Sistemas de Información	
		Análisis de vulnerabilidad a la publicación de aplicativos WEB	Informe de vulnerabilidades y plan de remediación.	1	01/05/2022	30/11/2022							Director Sistemas de Información	

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	20 de 21		

Código:	F0103010118	MATRIZ DE SEGUIMIENTO DE ACTIVIDADES PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	1		
Vigente a partir de:	12/12/2018		
Página:	1 de __		

N°	Nombre de la Actividad	Acciones o Tareas principales	Indicador o Producto	Meta	Fecha inicio	Fecha final	Avance Programado						Responsable de la Actividad	% Cumplimiento
							B1	B2	B3	B4	B5	B6		
3	Migración de servidores a Datacenter TIE3	Migración de Sistemas Operativos y establecimiento de Línea Base.	Sistema Operativo con hardening	100%	01/03/2022	31/07/2022							Director Sistemas de Información	
4	Entrega de la Historia clínica a personas no autorizadas o sin cumplimiento de requisitos legales.	Crear forma para validación de impresión de historia clínica.	Indicador de oportunidad para la resolución 256	1	01/03/2022	31/05/2022							Director Sistemas de Información	
		Implementar restricción de impresión desde un privilegio	Impresión autorizada por privilegios de usuario	100%	01/04/2022	31/05/2022							Director Sistemas de Información	
5	Acceso lógico no autorizado	Difusión de las Políticas de sistemas de información	Soportes de los medios de difusión institucional usados para divulgar las políticas de sistemas de información	100%	01/03/2022	31/12/2022							Director Sistemas de Información	

Código:	PE01 PL 19	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	02		
Vigente a partir de:	30/01/2020		
Página:	21 de 21		

Código:	F0103010118	MATRIZ DE SEGUIMIENTO DE ACTIVIDADES PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Versión:	1		
Vigente a partir de:	12/12/2018		
Página:	1 de __		

N°	Nombre de la Actividad	Acciones o Tareas principales	Indicador o Producto	Meta	Fecha inicio	Fecha final	Avance Programado						Responsable de la Actividad	% Cumplimiento
							B1	B2	B3	B4	B5	B6		
		Unir el 100% de los equipos al directorio activo y ampliar el alcance de las políticas.	Gestión centralizada de las políticas del dominio	100%	01/01/2022	31/12/2022							Director Sistemas de Información	