PLAN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

LEOPOLDO ABDIEL GIRALDO VELÁSQUEZ

Gerente ESE Metrosalud

Dirección sistemas de información

30/07/2018

Versión [01]

Alcaldía de Medellín

Contenido

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

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.

OBJETIVOS

Objetivo general

Identificar los riesgos de los componentes informáticos y de la gestión de información médiate 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.

ALCANCE

Esta guía metodológica suministra los principios y directrices para la gestión del riesgo, 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".

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.

DEFINICIONES

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.

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.

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.

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

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.

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.

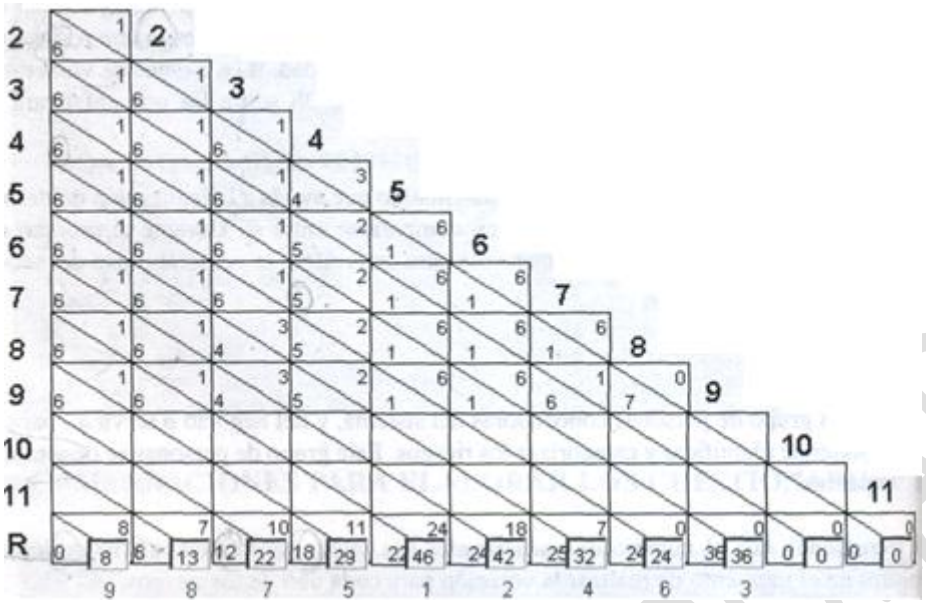
DESCRIPCION DEL METODO

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 la 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 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 ("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, 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<2Los 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 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

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

ELABORADO POR:	
Jaime Alberto Henao	Cargo: Director Operativo de Sistemas de Información