1. INTRODUCCIÓN

La Administración de riesgos es un método sistemático que permite establecer a las entidades sean públicas o privadas, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos en función de la tecnología, equipos, infraestructura etc., asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todo el equipo de la empresa de Salud ESE del Municipio de Soacha, en cumplimiento de sus funciones, está expuesto a riesgos, por lo tanto, se hace necesario establecer una estructura y metodología en conjunto con lo dictaminado por el Ministerio de las TIC's, para identificar las causas y consecuencias evitando la materialización de los eventos detectados, teniendo como fin la seguridad de la información bajo los principios de Integridad, Disponibilidad y Confidencialidad de la información.

2. OBJETIVOS

2.1 Objetivo general

Establecer la estructura metodológica para la administración de riesgos en la empresa de Salud ESE del Municipio de Soacha.

2.2 Objetivos específicos

- Generar pautas para la determinación de los riesgos en la empresa de Salud ESE del Municipio de Soacha.
- Fomentar el uso y apropiación de la Política de Seguridad vigente en los funcionarios y contratistas de la empresa de Salud ESE del Municipio de Soacha.
- Involucrar y comprometer a todos los funcionarios y contratistas en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

3. ALCANCE

El presente documento está enfocado en mejorar la estrategia para el análisis, diseño, ejecución y control de los riesgos, generados en las actividades cotidianas por el uso frecuente de información en la empresa de Salud ESE del Municipio de Soacha.

La mitigación de los riesgos como debe ser establecida bajo un proceso estructurado y sistemático es por ello que esta guía contiene desde la definición de los roles y responsabilidades hasta los formatos que deben ser diligenciados en el proceso de identificación.

4. DEFINICIONES

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

- **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 empresas mediante figuras como outsourcing, seguros, sitios alternos.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **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.
- **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.
- **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
- **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 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.

- **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.

5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de diversos factores, aun así, la participación de la alta dirección en este caso la gerencia, permite que el proceso se desarrolle con mayor fluidez y efectividad es por ello que en la identificación de los roles no solo se observa el equipo técnico que hará las labores de análisis y tratamiento del riesgo.

- Gerencia: aprueba las directrices para la administración del riesgo en la empresa.
- Servidores públicos y contratistas: ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la empresa.
- Quien haga las veces de Control Interno: debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.

6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Empresa de Salud ESE del Municipio de Soacha, adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, mediante el apoyo de la Gerencia en conjunto con funcionarios y contratistas es por ello que se comprometen a:

1. Conocer y cumplir la política de seguridad de la información.
2. Replicar con sus equipos de trabajo fortaleciendo el trabajo mancomunado con la oficina de tecnología fortaleciendo la conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.

3. Aprobar la revisión frecuente de los procesos y procedimientos para la identificación de nuevos riesgos o control de los existentes.
4. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto

Para mitigar y lograr lo mencionado anteriormente es necesario que sean asignados recursos humanos, presupuestales y tecnológicos que permitan cerrar las brechas detectadas y mejorar los controles existentes.

7. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

7.1 Identificación de riesgos

En esta fase del documento el objetivo es evaluar todos los activos que se encuentran, considerando las áreas existentes entre ellos y realizando una valoración sobre estos. De esta forma se definirá claramente un punto de salida de todos los activos, sean estos tangibles o no, dentro de la compañía y pudiendo analizar a qué amenazas podrían estar expuestos estos activos.

Una vez disponemos de un listado de las amenazas reales que pueden afectar a nuestros activos, estaremos en disposición de poder realizar la evaluación del impacto que sufrirá la compañía en caso de que se materialicen estas amenazas.

El impacto, junto con los resultados anteriormente explicados dará una serie de datos que nos permitirán priorizar el plan de acción y, al mismo tiempo, evaluar como se ve modificado este valor una vez se apliquen las contramedidas o bien, el riesgo que estamos dispuestos a asumir.

Como resultado de esta fase, podremos obtener:

- Un análisis detallado de los activos relevantes de seguridad de la empresa.
- Un estudio de las posibles amenazas sobre los sistemas de información, así como su impacto.
- El resultado final, será el impacto potencial que tendrá la materialización de las diferentes amenazas a las que están expuestos nuestros activos.

7.1.1 Inventario de activos

El primer punto para el análisis es estudiar los activos vinculados a la información. Es habitual agrupar los activos por grupos

- [L] Lugar
- [HW] Hardware
- [SW] Software
- [COM] Red
- [O] Organización
- [P] Personal

8. Dimensiones de seguridad

Desde el punto de vista de la seguridad, junto a la valoración de los activos, se ha de indicar cuál es el aspecto de la seguridad más crítico. Esto será de gran ayuda en el momento de pensar en posibles medidas de prevención, ya que serán enfocadas en aquellos aspectos más críticos.
Una vez identificados los activos, se ha de realizar la valoración de los mismos. Esta valoración mide la criticidad a las cinco dimensiones de la seguridad de la información gestionada por el proceso de la Empresa de Salud ESE del Municipio de Soacha. Esta valoración nos permitirá, valorar el impacto que tendrá la materialización de la amenaza sobre la parte del activo expuesto.
El valor que reciba el activo puede ser propio o acumulado. El valor propio se asignará a la información, quedando el resto de activos subordinados a las necesidades de explotación y protección de la información. De esta manera, los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos. Cada activo de información puede tener un valor diferente en cada uno de las diferentes dimensiones para la empresa que deseamos analizar. Por esto, se ha de tener presente siempre que representa cada dimensión.
Las cinco dimensiones de las que se habla son:

- **[C] Confidencialidad**. Únicamente las personas autorizadas tienen acceso a la información sensible o privada.
- **[I] Integridad**. La información y los métodos de procesamiento de esta información son exactos y completos, y no se han manipulado sin autorización
- **[D] Disponibilidad**. Los usuarios que están autorizados pueden acceder a la información cuando lo necesiten.

Una vez detalladas las tres dimensiones se ha de tener presente la escala en que se realizarán las valoraciones. En este caso se utilizará una escala de valoración de 1 – 4 siguiendo los siguientes criterios.

Tabla 1: Tabla de valoración

VALOR	CLASIFICACIÓN
1	Zona de Riesgo Bajo (B)
2	Zona de Riesgo Moderado (M)
3	Zona de Riesgo Alto (A)
4	Zona de Riesgo Extremo (E)

9. Análisis de amenazas

Las amenazas pueden afectar diferentes aspectos de la seguridad de los activos, por tanto, uno de nuestros objetivos es el análisis de qué amenazas pueden afectar los activos de la Empresa. Una vez hecho esto se ha de estimar la vulnerabilidad de cada activo respecto a las amenazas potenciales.
El primer paso para realizar este análisis es disponer de una tabla de amenazas, para obtener este listado de amenazas las cruzaremos con los activos que hemos detallado en el punto anterior.
En último lugar, para valorar el impacto de las amenazas en los activos que tenemos definidos, deberemos asignar valores al impacto que produciría en la empresa la materialización de la amenaza, este valor será estimado de 1 – 5 y se define en la siguiente tabla:

Tabla 2: Valoración de Impacto

VALOR	IMPACTO
1	Insignificante
2	Menor
3	Moderado
4	Mayor
5	Catastrófico

10. AMENAZAS

Tabla 3: Clasificación Amenazas

ACTIVO	AMENAZA
[L] Lugar	Daño en los equipos y servidores por falta de un Equipo climatización centro de datos
	Mal estado de Equipos extintores
[HW] Hardware	Daño de Equipos de Escritorio
	Daño, o fuga de información Equipos Portátiles
	Daño de Impresoras
	Daño, o fuga de información Servidor Aplicaciones
	Daño, o fuga de información Servidor backup
	Daño, o fuga de información Servidor Bases de datos
	Malware, troyano, gusanos, descargas o visitas a través de Unidades extraíbles
	Daño Aplicación Sistemas Operativos
[SW] Software	Daño o alteración Aplicaciones ofimática
	Eliminación o Divulgación Base de datos de Contraseñas
	Suplantación o eliminación Correo electrónico
	Alteración, eliminación o Divulgación Programas de administración (contabilidad, manejo de personal, etc.)
	Daño o alteración Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)
	Alteración, eliminación o Divulgación Programas manejo documental
	Daño o alteración Servidor Antivirus
[COM] Red	Daño de Equipos de la red cableada (router, switch, etc.)
	Daño de Equipos de la red inalámbrica (router, punto de acceso, etc.)
	Malware, troyano, gusanos, descargas o visitas a través de Navegación en Internet
[O] Organización	Alteración o eliminación Archivo de Gestión
	Alteración o eliminación Archivo de talento Humano
	Alteración o eliminación Bases de datos internos
	Alteración o eliminación Contables
	Alteración o eliminación Contractuales

	Alteración o eliminación Financieros
	Alteración o eliminación Jurídicos
	Alteración o eliminación Licencias y Permisos
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Administrativos
[P] Personal	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de gerencia y subgerentes
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Administrativos
	Acceso no autorizado a sistemas, compartir contraseñas, Manejo Inadecuado de equipos, negligencia por falta de conocimiento por parte de Contratistas
	Acceso no autorizado a personal ajeno, Manejo Inadecuado de equipos, negligencia en la prestación del servicio por parte de Servicio de vigilancia

11. Evaluación del riesgo

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

Tabla 4: Valoración del Riesgo

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Raro	B	B	B	M	M
Improbable	B	M	M	A	A
Moderado	B	M	A	A	E
Probable	M	A	A	E	E
Casi certeza	M	A	E	E	E

12. Valoración de los riesgos

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo y definir la opción de manejo del riesgo. Lo anterior de acuerdo con la evaluación de controles y Valoración del riesgo.

13. Identificación de controles

Es crucial para la implementación adecuada de un SGSI la aplicación de controles existentes según la norma ISO 27001. Estos salen como resultado del análisis de riesgo efectuado en la etapa inicial, en la mayoría de los casos para la aplicación de los controles es necesario personal experto en diversas áreas pues si bien es cierto que la implantación de un sistema de seguridad de la información está ligada al personal encargado de TI según la norma se trabaja sobre los dominios existentes los cuales incluyen desde recursos humanos hasta la legislación.

Para cada uno de los dominios existen controles que deberán ser aplicados para la mitigación del riesgo depende de la clasificación inicial.

14. Manejo de riesgos

Estructuralmente la Empresa de Salud ESE del Municipio de Soacha manejara los riesgos identificados de la siguiente manera:

14.1 Controles técnicos

Estos controles se basan prácticamente en la gestión operativa y de aseguramiento, de zonas físicas, accesos, manipulación de hardware y software, accesos a sitios web, manejo de la información, etc. Esta es la fase de la implementación de mayor cuidado y costo, pues en este proceso es donde está en juego la información y el éxito de la implantación del sistema de gestión y la mitigación del riesgo.

14.2 Implementar programas de capacitación y sensibilización

Es ideal que se programen las fechas desde el inicio y las respectivas capacitaciones y sensibilizaciones, pues de esto depende en gran parte el éxito de la implementación del sistema. Al aplicar algunos controles se deberá realizar el debido seguimiento para verificar y cuantificar la funcionalidad del mismo, sin embargo, esto no aplica para todos los controles; Es ahí donde la sensibilización entra a jugar un papel fundamental en la empresa pues por desconocimiento los trabajadores pueden interferir el funcionamiento real del control, pues si bien es cierto que el sistema

puede ser estable los usuarios son parte fundamental del éxito de cada uno.

14.3 Implementación de procedimiento de manejo de incidentes de seguridad

Cuando se habla de incidente informático, se hace referencia a un suceso que se presentó o que tiene una gran posibilidad de darse en un momento determinado. Este suceso puede ser llevado a cabo a voluntad o accidental. Dependiendo de la gravedad de la situación este puede afectar el funcionamiento normal de la empresa. Por lo general el manejo del incidente implica que este se debe solucionar en el menor tiempo posible para evitar una afectación mayor y se debe buscar documentar cada uno de los eventos presentados y el tiempo que transcurrió entre cada uno de ellos, con el fin de poderlo analizar posteriormente y aplicar correcciones del caso para que en un futuro este no se vuelva a presentar o al menos su impacto sea lo menor posible. Para ello, se pueden seguir los pasos ideales para mantener el orden adecuado.

14.3.1 Preparación

En este punto, se debe tener una lista de chequeo la cual ayuda a organizar la reacción ante un incidente, para esto es necesario tener conceptos claros como son:

- Políticas. Si estas existen, se debe determinar que está permitido y que no. Conducto regular de comunicación, lista de contactos, la posibilidad o no de dar información a terceros, quien está en capacidad de hacerlo entre otros.
- Recurso humano. No basta con saber que se cuenta con determinadas áreas dentro de la empresa, se necesita saber quiénes son las personas que están capacitadas para afrontar un incidente, sus números de teléfono, el escalamiento en la comunicación, entre otros.
- Información: El manejo que se le debe dar a la misma, forma de almacenamiento, importancia según el negocio, confidencialidad, integridad y disponibilidad.
- Software – Hardware: Con que elementos contamos como antivirus, firewall, ubicación de los mismos, servidores, etc.
- Comunicaciones. Con que elementos cuenta la empresa para llevar a cabo la prestación de los servicios ante un incidente, medios de comunicación alternos, etc.
- Ups – Plantas Electrices – controles: Determinar claramente cuáles son los dispositivos que cuenta la empresa, cuales son principales y cuáles de respaldo, el comportamiento de los mismos, tiempos de funcionamiento, plan de contingencia entre otros.
- Formatos o Plantillas. Se debe contar con elementos para registras los sucesos, el tiempo en que ocurren, como se afrontaron, observaciones, etc.

14.3.2 Detección y análisis

La detección se puede dar por llamada de un usuario, cliente, administrador, etc., alarma presentada por algún dispositivo dispuesto para ello, como un firewall, IPS. Alteración de información, observación, medios informativos, caída de un sistema, base de datos, etc.
Una vez detectado se procede a analizar el impacto del mismo, con ello se disponen los elementos

que se requieran para solucionar el impase. Determinar si no son falsos positivos, validar la evidencia en este caso ver logs de registros, bitácoras.

14.3.3 Contención

En esta fase se procede a neutralizar el incidente, para ello es necesario tener cautela de no eliminar evidencia que posteriormente nos ayude a analizar el origen, el posible atacante, desde cuando está llevando a cabo el proceso, en fin, información que posteriormente se estudiara. Aquí se toman decisiones de como plantear la estrategia de contención, fundamentados en importancia del activo, disponibilidad para la operación de la empresa, elementos alternos o sustitutos, grado del ataque.

14.3.4 Erradicación y Recuperación

Con base en la información tomada en la detección y contención es necesario tomar las medidas del caso para que no se vuelvan a presentar. Es posible que la empresa tenga que invertir en elementos de protección adicionales. Pero esta decisión debe ser fundamentada en hechos y datos, ser lo más objetivos posibles. En el proceso de recuperación puede ser necesario restaurar las copias de respaldo, cambio de contraseñas, cambios de direcciones IPs.

14.3.5 Reporte y cierre

Se hace necesario llevar a cabo un informe en el cual se documente los procesos realizados, siendo muy claros en los pasos llevados a cabo. Esta información puede servir más adelante para resolver nuevos impases o determinar si las decisiones tomadas fueron acordes al incidente.

Se debe generar un documento el cual debe estar redactado por el equipo que afronto el incidente, estas lecciones aprendidas se analizaran posteriormente la cual se informara y hará los aportes para prevenir futuras situaciones. Por último, dar a conocer las recomendaciones del caso y llevar a cabo las implementaciones a que haya lugar. Es bueno, volver a hacer una revisión periódica tanto a las decisiones tomadas como las inversiones hechas por la empresa. Con ello evitamos que una solución planteada hoy mañana sea obsoleta y se nos presente un incidente nuevamente.