TABLA DE CONTENIDO

1. INTRODUCCIÓN
2. OBJETIVOS
   2.1 OBJETIVO GENERAL
   2.2 OBJETIVOS ESPECÍFICOS
3. ALCANCE
4. DEFINICIONES
5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO
   - Sponsor del proyecto (Subgerencia Administrativa y Financiera)
   - Director del proyecto (Referente de Tecnología)
   - Director de riesgos (Referente de Tecnología)
   - Responsable de riesgos (Técnicos soporte del Departamento de Tecnología)
   - Miembro del equipo del proyecto (Técnicos soporte del Departamento de Tecnología: a cargo de Ing. Joao E Pinzon P)
   - Interesados o stakeholders (funcionarios de la ESE Municipal de Soacha Julio Cesar Peñaloza)
   - Consultores y proveedores demás contratistas de otros campos de la E.S.E. Municipal de Soacha Julio Cesar Peñaloza
6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO
7. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO
   7.1 IDENTIFICACIÓN DE RIESGOS
   7.2 MEDICIÓN O EVALUACIÓN
   7.3 CONTROL Y MITIGACIÓN
   7.4 MONITOREO
   7.5 INVENTARIO DE ACTIVOS
8. DIMENSIÓN DE SEGURIDAD
   8.1. LA DISPONIBILIDAD DE LA INFORMACIÓN
   8.2. LA INTEGRIDAD DE LA INFORMACIÓN
   8.3. LA CONFIDENCIALIDAD DE LA INFORMACIÓN

9. ANALISIS DE AMENAZAS
10. AMENAZAS
    10.1 ALGUNAS DE LAS MÁS RELEVANTES AMENAZAS
    10.2 CONTROLES QUE SE DEBEN IMPLEMENTAR PARA MITIGAR EL RIESGO
11. EVALUACION DEL RIESGO
    11.1. ANALIZANDO LOS RIESGOS INFORMÁTICOS
    11.2. REDUCIENDO LOS RIESGOS INFORMÁTICOS
12. VALORACION DEL RIESGO
13. IDENTIFICACION DE CONTROLES
14. MANEJO DE RIESGOS
    14.1. CONTROLES TÉCNICOS
    14.2 IMPLEMENTAR PROGRAMAS DE CAPACITACIÓN Y SENSIBILIZACIÓN
15. BIBLIOGRAFIA

1. INTRODUCCIÓN

El presente documento define las medidas de seguridad identificadas para desarrollar durante el año, el plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información, seguridad digital y continuidad de la operación en la E.S.E. Municipal de Soacha Julio César Peñaloza. 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 e infraestructura, asociados con una actividad, función o proceso de tal forma que permita minimizar riesgos y maximizar oportunidades. Todos los funcionario y/o contratistas de la E.S.E. Municipal de Soacha Julio César Peñaloza, 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 negativos, teniendo como fin la seguridad de la información bajo los principios de Integridad, Disponibilidad y Confidencialidad de la información.

Para la E.S.E. Municipal de Soacha Julio César Peñaloza, a través de su Modelo Integrado de planeación y gestión, se compromete a mantener una cultura de la gestión del riesgo asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos, regulando los riesgos de los procesos y proyectos luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados y fortaleciendo las medidas de control y la eficiencia a lo largo del proyecto para optimizar de manera continua y oportuna, la respuesta a los riesgos, además de los riesgos de seguridad y privacidad de la Información y Seguridad Digital de manera Integral. La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los usuarios de la E.S.E. Municipal de Soacha Julio César Peñaloza.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Adoptar e implementar los lineamientos del Modelo de Seguridad y Privacidad de la Información y la Estrategia de seguridad digital conforme a lo establecido por el Gobierno Nacional con el fin de fortalecer la integridad, confidencialidad y disponibilidad de los activos de información y el tratamiento de sus riesgos. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad y para cada una de ellas se define el nombre de la medida, el objetivo, la justificación, el responsable de cada medida y sus respectivas prioridades. Las medidas presentes en este documento se definieron teniendo en cuenta la información del análisis de riesgos, el cual brindó información acerca de las necesidades en cuanto a la seguridad de la información y proporcionó las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución, la estructura metodológica para la administración de riesgos en la E.S.E. Municipal de Soacha Julio César Peñaloza.

2.2 OBJETIVOS ESPECÍFICOS

- ✓ Generar pautas para la determinación de los riesgos tecnológicos en la E.S.E. Municipal de Soacha Julio César Peñaloza.
- ✓ Fomentar el uso y aplicación de la Política de Seguridad y privacidad de la información vigente con los funcionarios y/o contratistas de la E.S.E. Municipal de Soacha Julio César Peñaloza.
- ✓ Involucrar y comprometer a todos los funcionarios y/o contratistas en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.
- ✓ Definir y aplicar los lineamientos para tratar de manera integral los riesgos de seguridad y privacidad de la Información; seguridad digital y continuidad de la operación, de esta manera alcanzar los objetivos y metas institucionales,

protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información de acuerdo con los contextos establecidos en la

- ✓ Fortalecer y apropiar conocimiento referente a la gestión de riesgos de seguridad y privacidad de la información; seguridad digital y continuidad de la operación.

3. ALCANCE

Realizar una eficiente gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación, que permita integrarlo en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. 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 E.S.E. Municipal de Soacha Julio César Peñaloza. La mitigación de los riesgos como debe ser establecida bajo un procedimiento 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; basándonos en este alcance logramos identificar falencias, brechas que brindan seguridad a los funcionarios de la E.S.E. Municipal de Soacha Julio César Peñaloza, donde se evidencia que cada proceso tiene información relevante y los funcionarios brindan la seguridad de la misma para un trabajo idóneo.

4. DEFINICIONES

- ✓ **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- ✓ **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- ✓ **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- ✓ **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- ✓ **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las

actividades y tareas requeridas para el logro de objetivos de los procesos de una Entidad

ELABORADO POR	REVISADO POR	APROBADO POR
Ing. Joao Enrique Pinzon Pinzon Referente de tecnología	Claudia Puello Castro Referente de Calidad Julia Andrea De Ávila Heredia Jefe de Oficina Asesora de Planeación y Gestión Interna	María Victoria Herrera Roa Gerente

- ✓ **Reducir o mitigar:** corresponde a la protección en el momento en que se presenta el riesgo; se encuentra en esta categoría los planes de emergencia, planes de continencia, mantener copias de respaldo.
- ✓ **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.
- ✓ **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- ✓ **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.
- ✓ **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:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- ✓ **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
- ✓ **Sponsor:** Es una persona o una organización que patrocina, apoya o financia una actividad o proyecto, habitualmente con fines publicitarios.
- ✓ **Stakeholders:** significa ‘interesado’ o ‘parte interesada’, y que se refiere a todas aquellas personas u organizaciones afectadas por las actividades y las decisiones.

- ✓ **Bugs:** Esta palabra inglesa, cuya traducción literal es “bicho”, se usa para nombrar a los errores que se producen en un programa informático.
- ✓ **Crackers:** Del inglés to crack, que significa romper o quebrar se utiliza para referirse a las personas que rompen o vulneran algún sistema de seguridad.
- ✓ **Hackers:** Habitualmente se les llama así a técnicos e ingenieros informáticos con conocimientos en seguridad y con la capacidad de detectar errores o fallos en sistemas informáticos para luego informar los fallos a los desarrolladores del software encontrado vulnerable o a todo el público.
- ✓ **Backup:** del inglés: back up, “respaldo”, “refuerzo”, respaldo, copia de seguridad o copia de reserva a una copia de los datos originales de un sistema de información o de un conjunto de software (archivos, documentos, etc.
- ✓ **Troyano:** en la mayoría de los casos, crean una puerta trasera (en inglés backdoor) que permite la administración remota a un usuario no autorizado, a un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.
- ✓ **Need-to-know:** conocer la necesidad para el acceso a la información específica, su conocimiento o su posesión necesaria para tener acceso a ese recurso con el fin de realizar su trabajo.
- ✓ **Switch** nace en un término de origen inglés y puede ser traducido al español como interruptor, conmutador, vara o látigo, según cada contexto.

5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

- **Sponsor del proyecto (Subgerencia Administrativa y Financiera)**

El sponsor del proyecto es la persona que autoriza y destina los recursos personales y económicos para su ejecución, sus roles en la gestión de riesgos son:

- ✓ Proveer los recursos necesarios para poder implementar las acciones dentro del proceso de gestión de riesgos.
- ✓ Gestionar los recursos y presupuesto asignados a la gestión de riesgos informáticos.
- ✓ Apoyar al referente de tecnología en el proceso de gestión de riesgos.
- ✓ Gestionar y solucionar los asuntos que exceden de las responsabilidades al

referente de tecnología.
- ✓ Definir los criterios a nivel de los objetivos del proyecto, ayudando a evaluar los riesgos y las acciones planificadas respecto a estos.

- **Director del proyecto (Referente De Tecnología)**

Cómo responsable del proyecto se encarga de planificar y ejecutar la gestión de riesgos; lo que implica las siguientes responsabilidades:

- ✓ Definir los diferentes roles en la gestión de riesgos y asignarlos a las personas implicadas.
- ✓ Dirigir y seguir el proceso de identificación y gestión de riesgos.
- ✓ Integrar la gestión de riesgos en el plan de gestión de proyecto.
- ✓ Resolución de conflictos y dar continuidad al proceso.

- **Director de riesgos (Referente De Tecnología)**

Este rol aparece como figura independiente, sus roles en la gestión de riesgos son:

- ✓ Actuar como líder en los procesos de identificación y gestión de riesgos; asumiendo responsabilidades en la ejecución y dirección de estos procesos.
- ✓ Dar soporte a los miembros del equipo del proyecto implicados en la gestión de riesgos, es bueno que tenga un perfil de especialista en este ámbito.
- ✓ Gestionar y mantener el registro de riesgos y las reuniones periódicas de gestión de riesgos.

- **Responsable de riesgos (Técnicos soporte del Departamento de Tecnología):**

Cada riesgo considerado relevante para la E.S.E. debe incluir un responsable. Estos responsables forman parte del equipo y asumen este rol de forma adicional a sus tareas habituales. Sus roles en la gestión de riesgos son:

- ✓ Ayudar en la definición de las acciones a tomar frente al riesgo del que son responsables.

- ✓ Implementar y controlar las acciones definidas para el riesgo del que son responsables.
- ✓ Evaluar y reportar la evolución de las acciones y el riesgo a lo largo del proyecto.

- **Miembro del equipo del proyecto (Técnicos soporte del Departamento de Tecnología**

La gestión de riesgos es un proceso que debe implicar a todos los integrantes del proyecto, cada uno asumiendo diferentes roles y responsabilidades, pero colaborando en identificar los riesgos y aplicar las acciones que correspondan deben asumir las siguientes tareas:

- ✓ Aportar los conocimientos técnicos y experiencia para soportar en la identificación y evaluación de riesgos y en la definición de acciones.

- ✓ Dar soporte y participar en la implementación de las acciones definidas.

- **Interesados o stakeholders (Funcionarios de la ESE Municipal de Soacha Julio Cesar Peñaloza)**

Aquí estaríamos hablando de los funcionarios y/o contratistas, que por tanto no se espera que participen directamente en la ejecución o seguimiento. No obstante, estos pueden ayudarnos a identificar riesgos relacionados con sus necesidades y objetivos.

- **Consultores y proveedores demás contratistas de otros campos de la E.S.E. Municipal de Soacha Julio Cesar Peñaloza**

Aunque estos podrían incluirse en el grupo anterior, los consultores y proveedores que hayan sido contratados para participar en un determinado proyecto deben aportar una implicación superior a la que esperamos de un interesado. En referencia a la gestión de riesgos, esta implicación queda plasmada en soportar las tareas de identificación, evaluación y definición de las acciones a realizar, aportando información o juicio como expertos.

El éxito de la administración del riesgo depende de diversos factores, aun así, la participación de 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.

6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La administración del riesgo tiene un papel importante en la E.S.E. Municipal de Soacha Julio César Peñaloza, debido al dinamismo y constantes cambios, que el mundo globalizado de hoy exige; estos cambios hacen que la E.S.E. Municipal de Soacha Julio César Peñaloza deba enfrentarse a factores internos y externos que pueden crear incertidumbre sobre el logro de sus objetivos. La Gestión del Riesgo es el proceso que comprende el establecimiento y aplicación de las políticas, procedimientos, metodología e instrumentos que permiten brindar una seguridad razonable para controlar y responder a los acontecimientos potenciales, por lo tanto, la administración del riesgo es una herramienta de gestión que le permite establecer mecanismos adecuados para identificar, valorar y minimizar el impacto de la amenaza. La política de administración del riesgo determina la posición de la alta dirección frente al manejo de los riesgos, en las que se fijan los lineamientos con relación a la calificación de éstos, la forma de administrarlos y la protección de los recursos, estableciéndose guías de acción para que todos los funcionarios y/o contratistas las apliquen en los procesos.

La E.S.E. Municipal de Soacha Julio César Peñaloza, adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de administración del riesgo, mediante el apoyo de la Gerencia y en conjunto con referentes, es por ello que se comprometen a:

- ✓ Conocer y cumplir la política de seguridad de la información.
- ✓ Capacitar a los funcionarios y/o contratistas por medio del trabajo mancomunado con el área de tecnología, fortaleciendo la conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
- ✓ Aprobar la revisión frecuente de los procedimientos para la identificación de nuevos riesgos o control de los existentes.
- ✓ Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

- ✓ Estar a la vanguardia de los delitos informáticos a los que se pueda ver expuesta la entidad.
- ✓ Generar monitores constantes en la recopilación de información y esta sea salvaguardada como repositorios fundamentales de la ESE.

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

Se debe realizar con anterioridad a la ejecución de cualquier proceso con el fin de identificar los riesgos que podría manifestarse, así como, aquellos riesgos en potencia que de ocurrir se van a transformar en una serie de obstáculos de cara al logro de los objetivos definidos.

Una vez disponemos de un listado de las amenazas reales que pueden afectar a nuestros activos y sus respectivos subyacentes, estaremos en disposición de poder realizar la evaluación del impacto que sufrirá la E.S.E. Municipal de Soacha Julio César Peñaloza en caso de que se materialicen estas amenazas. El impacto, junto con los resultados esperados o no 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 medidas más adecuadas o bien, el riesgo y las consecuencias que estamos dispuestos a asumir. Como resultado de esta fase, podremos obtener:

- ✓ Un análisis detallado de los activos relevantes de seguridad de la E.S.E. Municipal de Soacha Julio César Peñaloza.
- ✓ 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.

7.2 MEDICIÓN O EVALUACIÓN

Una vez que los riesgos de los diferentes procesos han sido identificados, el siguiente paso es evaluar la posibilidad de materialización en función de la frecuencia con la que suceden, así como; definir el impacto que podrían generar en caso de ocurrencia. Como resultado establecemos el llamado riesgo inherente, que no es más que el nivel de riesgos que presenta una actividad concreta, sin aplicarle ningún tipo de control.

7.3 CONTROL Y MITIGACIÓN

Se busca definir las medidas de control que permitan reducir la probabilidad de ocurrencia y/o los impactos ocasionados por los riesgos inherentes detectados. Tras esta etapa la E.S.E. Municipal de Soacha Julio César Peñaloza, obtiene el riesgo conocido como residual, que es el riesgo que resulta tras la aplicación de los oportunos controles que hayan sido considerados.

7.4 MONITOREO

Aquí, se lleva a cabo el seguimiento adecuado a los riesgos con el fin de ir analizando su evolución**.**

7.5 INVENTARIO DE ACTIVOS

El primer punto para el análisis, es estudiar los activos vinculados a la información, los activos se agrupan en un archivo llamado A-TICSI-F008 MATRIZ TECNOLOGIA

8. DIMENSIÓN DE SEGURIDAD

La seguridad de la información se articula sobre tres dimensiones, que son los pilares sobre los que aplicar las medidas de protección de la información:



8.1. LA DISPONIBILIDAD DE LA INFORMACIÓN

Hace referencia a que la información esté accesible cuando la necesitemos. Algún ejemplo de falta de disponibilidad de la información es: - cuando nos es imposible acceder al correo electrónico corporativo debido a problemas con el acceso a Internet, o bien, cuando la Base de Datos del sistema de información sufre una falla de servicio, en el que el sistema cae impidiendo accesos. Ambos tienen implicaciones serias para la seguridad de la información.

8.2. LA INTEGRIDAD DE LA INFORMACIÓN

Hace referencia a que la información sea correcta y esté libre de modificaciones y errores. La información ha podido ser alterada intencionadamente o ser incorrecta y nosotros podemos basar nuestras decisiones en ella. Ejemplos: Ataques contra la integridad de la información son la alteración malintencionada en los archivos de trabajo almacenados en el servidor mediante la explotación de una vulnerabilidad, o la modificación de un reporte de los diferentes departamentos por error humano.

8.3. LA CONFIDENCIALIDAD DE LA INFORMACIÓN

Implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como need-to-know. Con este término se hace referencia a que la información solo debe ponerse en conocimiento de los usuarios autorizados para su acceso. para este caso se generan políticas de acceso a las carpetas. La importancia

de contar con información confiable evita la pérdida o el robo de información confidencial, la divulgación no autorizada a través de las redes sociales o el acceso por parte de un usuario no autorizado a información crítica de la E.S.E. Municipal de Soacha Julio César Peñaloza ubicada en carpetas sin permisos asignados.

9. ANALISIS DE AMENAZAS

En la E.S.E. Municipal de Soacha Julio César Peñaloza se analiza el impacto de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad, de un activo de información, evaluando de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades e impactos en los activos.

Además de riesgo en sí, es necesario analizar también sus consecuencias potenciales, que son muchas y de distinta gravedad: desde una simple dispersión de la información a la pérdida o robo de datos relevantes o confidenciales.

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 E.S.E. Municipal de Soacha Julio César Peñaloza. La materialización de la amenaza, este valor será estimado en la siguiente tabla:

VALOR / COLOR
Riesgo Residual Extremo
Riesgo Residual Alto
Riesgo Residual Moderado
Riesgo Residual Bajo

10. AMENAZAS

Desde un hacker remoto o de un programa descargado de forma gratuita: los ataques se pueden ver reflejados de la siguiente manera:

1. Malware
2. Virus

3. Gusanos
4. Troyanos
5. Spyware
6. AdWare
7. Ransomware
8. Doxing
9. Phishing
10. Denegación de servicio distribuido (DDoS)
11. Inyección SQL o SQL Injection
12. Whaling o "caza de ballenas"

Las principales amenazas de un sistema de información que vulneran los equipos de cómputo pueden ser lógicas, físicas o emprendidas por usuarios.

Para la E.S.E. Municipal de Soacha Julio César Peñaloza la seguridad informática juega un papel esencial, dado que nos asegura que todos los recursos del sistema de información se resguardan de la forma que se tenía prevista desde un principio, así como que el acceso a la información allí contenida o su modificación únicamente por aquellas personas que se encuentran acreditadas y dentro de los límites de su autorización.

10.1 ALGUNAS DE LAS MÁS RELEVANTES AMENAZAS SON:

Lógicas: son los errores de programación (bugs) o los canales cubiertos, presentados como vías de comunicación que permitirán a un proceso transferir información, de manera que viole la política de seguridad del propio sistema. Igualmente, durante el desarrollo de aplicaciones grandes o sistemas operativos es bastante habitual que se inserten atajos en los sistemas habituales de autenticación de programa o núcleo del sistema que se está desarrollando. Los tres elementos más vulnerables frente a las amenazas de un sistema de información y que hemos de proteger al máximo son el software, el hardware y datos.

Usuarios: los funcionarios y/o contratistas de la E.S.E. Municipal de Soacha Julio César Peñaloza, podría comprometer la seguridad de los equipos, exfuncionarios descontentos con la entidad que podrían aprovechar las debilidades de un sistema. Junto a ellos, podemos incluir los crackers, que se refiere a las personas que intentan obtener acceso no autorizado a los recursos de la red con intención maliciosa y por supuesto los hackers

o piratas informáticos.

Finalmente, podríamos señalar un tercero tipo que alude a las amenazas físicas como puedan se los robos, sabotajes, catástrofes naturales, condiciones atmosféricas o de suministro eléctricos.

10.2 CONTROLES QUE SE DEBEN IMPLEMENTAR PARA MITIGAR EL RIESGO:

PASO 1: Debe tener definido el responsable de llevar a cabo la actividad de control. (referente trasversal) debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas.)
PASO 2: Debe tener una periodicidad definida para su ejecución. El control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.)
PASO 3: Debe indicar cuál es el propósito del control, ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, comparar, revisar, cotejar). o detectar la materialización del riesgo, con el objetivo de llevar acabo los ajustes y correctivos en el diseño del control o en su ejecución.
PASO 4: Debe establecer el cómo se realiza la actividad de control. de tal forma que se pueda
evaluar si la fuente u origen de la información que sirve para ejecutar el control, es confiable para la mitigación del riesgo.
PASO 5: Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones.
PASO 6: Debe dejar evidencia de la ejecución del control. La evidencia ayuda a que se pueda revisar la misma información por parte de terceros y llegue a la misma conclusión de quien ejecutó el control, se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos y descritos anteriormente.

ACTIVO	AMENAZA
[L] Lugar	*Daño en los equipos y servidores por falta de un Equipo climatización centro de datos*
	Mal estado de Equipos extintores
	Fuga o escape de gas
	Rotura de tubería de agua
	Terremoto daño en edificio
[HW] Hardware	*Daño de Equipos de Computo*
	Daño de Impresoras
	Daño, o fuga de información Servidor Aplicaciones, Base de Datos o Dominio
	Daño, o fuga de información en Disco de backup
	Malware, troyano, gusanos, descargas o visitas a través de Unidades extraíbles
[SW] Software	*Daño o alteración Aplicaciones ofimática*
	Eliminación o Divulgación Base de datos de Contraseñas
	Suplantación o eliminación de información total o parcial de Correo electrónico
	Alteración, eliminación o Divulgación en el ERP de la organización
	Daño o alteración de la telefonía IP
	Daño o alteración en el Antivirus
	Daño o alteración parcial o total de la información contenida en los equipos de computo
[COM] Red	*Daño de Equipos de la red cableada (router, switch, etc.)*
[O] Organización	*Alteración o eliminación total o parcial de los Archivos de Gestión*
	Alteración o eliminación total o parcial de los Archivos de talento Humano
	Alteración o eliminación total o parcial de los archivos de la Bases de datos internos
	Alteración o eliminación total o parcial de los archivos Contables
	Alteración o eliminación total o parcial de los documentos Contractuales

	Alteración o eliminación total o parcial de documentos Financieros
	Alteración o eliminación total o parcial de documentos Jurídicos
	Alteración o eliminación total o parcial de Licencias y Permisos
	Acceso no autorizado a sistemas
	Compartir contraseñas
	Negligencia por falta de conocimiento por parte de usuarios
[P] Personal	*Acceso no autorizado a sistemas, por negligencia o desconocimiento*
	Divulgación de información sensible para la organización
	Extracción no autorizada de información.

11. EVALUACION DEL RIESGO

En la E.S.E. Municipal de Soacha Julio César Peñaloza la evaluación de los riesgos y detección de los problemas informáticos es esencial para la administración de los bienes informáticos y resguardo de la inversión económica representada en cada equipo de cómputo o información de importancia. Al igual que el resto de equipos médicos o el mobiliario, los computadores se van amortizando y pierden valor, pero este proceso puede verse acelerado si no se les presta la debida atención en mantenimiento informático.

11.1. ANALIZANDO LOS RIESGOS INFORMÁTICOS

Una vez calculado el precio de los bienes de equipo que están en juego, es importante analizar todos los orígenes de los problemas informáticos, como, por ejemplo:

- ✓ Desconocimiento de los usuarios sobre las buenas prácticas de seguridad.
- ✓ Evaluación del riesgo de sufrir ataques informáticos de terceros.
- ✓ Evaluación del riesgo de que los equipos resulten infectados por virus.
- ✓ Tiempo de vida de los equipos informáticos y otros dispositivos.
- ✓ Prácticas en cuanto a copias de seguridad.
- ✓ Protocolo de actuación ante problemas informáticos (Plan de contingencia informático).

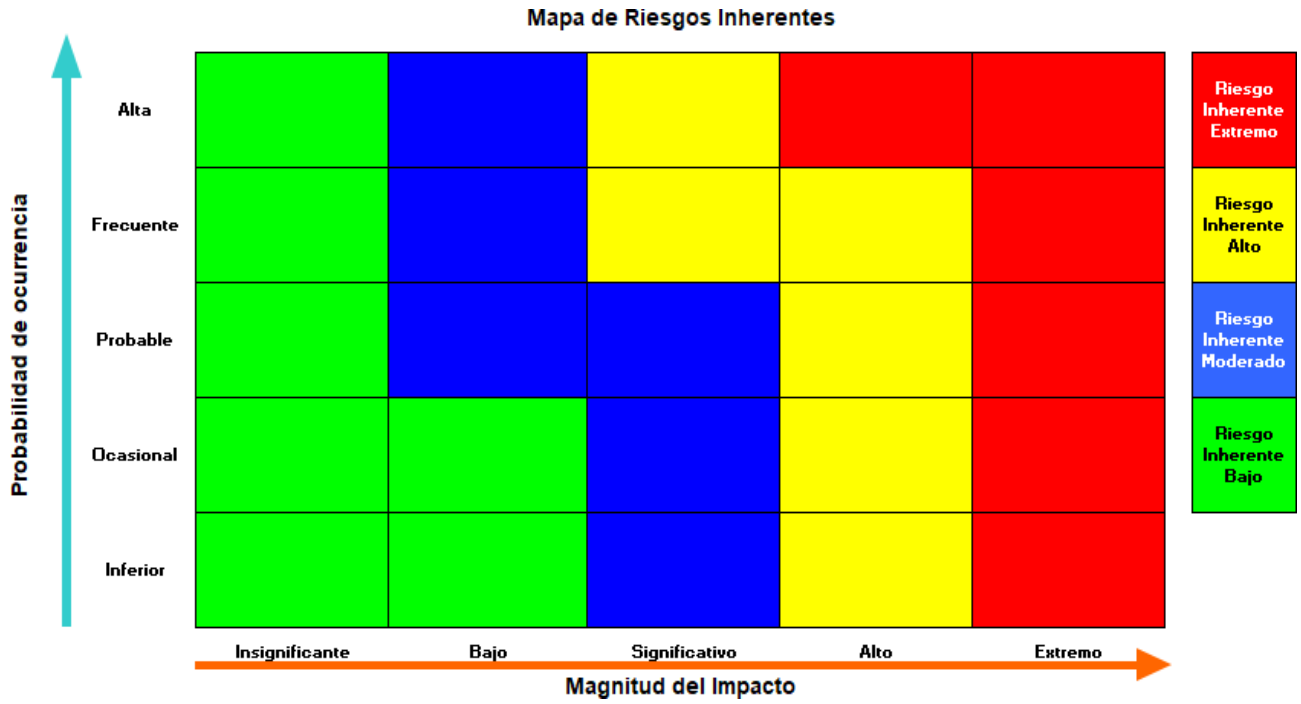
Se evalúa el riesgo real que puede significar para la organización que se produjera

algún problema informático que afectara total o parcialmente al valor de los equipos.

11.2. REDUCIENDO LOS RIESGOS INFORMÁTICOS

El presupuesto destinado a informática se orienta a las necesidades de la E.S.E. Municipal de Soacha Julio César Peñaloza, habrá gastos que son variables e imprescindibles, pero otros en cambio no están ni siquiera contemplados y estos gastos imprevistos podrían evitarse aplicando las técnicas de mantenimiento correctivo y preventivo adecuados. Lo importante es que los gastos en el área de informática de la E.S.E. Municipal de Soacha Julio César Peñaloza se reduzcan a final de año, reduciendo el número de imprevistos.

Se comparan 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.



ELABORADO POR	REVISADO POR	APROBADO POR
Ing. Joao Enrique Pinzon Pinzon Referente de tecnología	Claudia Puello Castro Referente de Calidad Julia Andrea De Ávila Heredia Jefe de Oficina Asesora de Planeación y Gestión Interna	María Victoria Herrera Roa Gerente

12. VALORACION DEL RIESGO

Es el producto de confrontar la evaluación del riesgo y los controles preventivos o correctivos**:** cronograma mantenimiento preventivo y correctivo de tecnologia 2024 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. IDENTIFICACION DE CONTROLES

Por control podemos entender el conjunto de normas, técnicas, acciones y procedimientos que interrelacionados e interactuando entre sí con los sistemas y subsistemas organizacionales y administrativos, permite evaluar, comparar y corregir aquellas actividades que se desarrollan en las organizaciones, garantizando la ejecución de los objetivos y el logro de las metas institucionales. El control actúa sobre las personas, situaciones específicas, fuentes de información y organizaciones, las cuales requieren con urgencia el diseño de estrategias que le permitan controlar y corregir los resultados de sus actividades.

14. MANEJO DE RIESGOS

Estructuralmente la E.S.E. Municipal de Soacha Julio César Peñaloza, desarrolla estrategias de seguridad y mitigación de riesgos, implementa programas de seguridad y gestiona incidentes.

Maneja los riesgos identificados de la siguiente manera:

- ✓ Se identifica las normas y directrices de seguridad aplicables a la infraestructura tecnológica.
- ✓ Proporciona un enfoque prioritario, flexible, repetible, basado en el rendimiento.
- ✓ Se ayuda a los funcionarios y/o contratistas a identificar, evaluar y gestionar el

riesgo informático.

- ✓ Se prioriza la innovación técnica.
- ✓ Se brinda capacitación en lo referente a los ciberataques o delitos informáticos.
- ✓ Se orienta para medir el desempeño de la implementación del plan de seguridad informática.
- ✓ Se Identifican las áreas de mejora que se debe abordar mediante la colaboración y asesoría del departamento de tecnología.

En este documento se evidencia la importancia que la E.S.E. Municipal de Soacha Julio César Peñaloza le da a contar con un plan de riesgo, priorizado, flexible, centrado en los resultados y que permita las comunicaciones y la seguridad informática.

La gestión de riesgos es el proceso continuo de identificación, evaluación y respuesta al riesgo.

Para gestionar el riesgo, la ESE Municipal de Soacha Julio Cesar Peñaloza comprende la probabilidad de que ocurra un evento y los posibles impactos resultantes. Con esta información, se determina el nivel aceptable de riesgo para lograr los objetivos organizacionales y expresa esto como su tolerancia al riesgo. Con una comprensión de la tolerancia al riesgo, se priorizan las actividades de la seguridad en las TIC y esto permite tomar decisiones informadas sobre los gastos de seguridad. La implementación de programas de gestión de riesgos ofrece a la capacidad de cuantificar y comunicar los ajustes de los programas de seguridad. Se opta por manejar el riesgo de diferentes maneras:

- ✓ Mitigación de riesgos
- ✓ La transferencia del riesgo
- ✓ La evasión del riesgo
- ✓ La aceptación del riesgo.

Dependiendo del impacto potencial en la prestación de los servicios críticos. Se pueden utilizar los procesos de gestión de riesgos para permitir informar y priorizar las decisiones con respecto a la seguridad. Se admite evaluaciones de riesgos recurrentes y validación de impulsores comerciales para ayudar a la organización a seleccionar objetivo y actividades de seguridad informática que reflejen los resultados deseados. Por lo tanto, se brinda la capacidad de seleccionar dinámicamente la gestión de riesgos de seguridad

para los entornos de TI. Es entonces una política adaptable para proporcionar una implementación flexible y basada en el riesgo que se puede utilizar con una amplia gama de procesos de gestión.

Las funciones del aérea de tecnología son:

- ✓ Identificar.
- ✓ Proteger
- ✓ Detectar
- ✓ Responder
- ✓ Mantener
- ✓ Estabilizar
- ✓ Recuperar.

Estas funciones ayudan a la organización a expresar su gestión del riesgo de seguridad TI organizando información, habilitando decisiones de gestión de riesgos, abordando amenazas y mejorando actividades previas. Estas funciones también se alinean con las metodologías existentes para la gestión de incidentes y ayudan a mostrar el impacto de las inversiones en seguridad cibernética.

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 E.S.E. Municipal de Soacha Julio César Peñaloza pues por desconocimiento los funcionarios y/o contratistas pueden interferir en el funcionamiento real del control del sistema.

15. BIBLIOGRAFIA

- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información: https://www.funcionpublica.gov.co/documents/418537/38169866/2021-01-30_Plan_tratamiento_riesgos_seguridad_informacion_v3.pdf/91994a8c-eda2-02b2-8c02-4c5dde38a3d6?t=1612127235836

- Manual de gobierno digital https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf

- Guía para la administración del riesgo y el diseño de controles en entidades públicas https://www.mincit.gov.co/temas-interes/documentos/guia-para-la-administracion-del-riesgo-y-el-diseno.aspx

E.S.E. Municipal de Soacha Julio César Peñaloza	**ESE MUNICIPAL DE SOACHA JULIO CESAR PEÑALOZA**	
MACROPROCESO: APOYO	**Plan:** **TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**	**CODIGO: A-TCSI-PL 003**
PROCESO: GESTIÓN DE TECNOLOGÍA, INFORMACIÓN Y COMUNICACIONES		**VERSION: 5**
SUBPROCESO: SISTEMAS		**FECHA: 29/01/2024**

MODIFICACIONES Y CAMBIOS

VERSIÒN	ELABORADO POR	REVISADO POR	APROBADO POR	MOTIVO DE LA MODIFICACIÓN	FECHA ACTUALIZACIÓN
1	JOAO ENRIQUE PINZON PINZON Líder de Tecnología	SANDRA BALLEN Líder de Calidad	KARIN JOHANNA MENDOZA ESPITIA Gerente	CREACION	24/01/2020
2	JOAO ENRIQUE PINZON PINZON Líder de Tecnología	JULIA ANDREA DE AVILA HEREDIA Jefe Oficina Asesora de Planeación	MARIA VICTORIA HERRERA ROA Gerente	ACTUALIZACION	24/01/2021
3	JOAO ENRIQUE PINZON PINZON Líder de Tecnología	JULIA ANDREA DE AVILA HEREDIA Jefe Oficina Asesora de Planeación	MARIA VICTORIA HERRERA ROA Gerente	ACTUALIZACION	25/01/2022
4	JOAO ENRIQUE PINZON PINZON Referente de Tecnología	LILY YOHANNA AVILA GARZÓN Apoyo Profesional de Planeación CLAUDIA PUELLO CASTRO Referente de Calidad	MARIA VICTORIA HERRERA ROA Gerente	ACTUALIZACION	26/01/2023
5	JOAO ENRIQUE PINZON PINZON Referente de Tecnología	JULIA ANDREA DE AVILA HEREDIA Jefe Oficina Asesora de Planeación y Gestión Interna CLAUDIA PUELLO CASTRO Referente de Calidad	MARIA VICTORIA HERRERA ROA Gerente	ACTUALIZACION	29/01/2024
6	DEYBER BECERRA Referente de Tecnología		WALDETRUDES AGUIRRE RAMÍREZ Gerente	ACTUALIZACION	25/01/2025
7	YAMID LEÓN Referente de Tecnología				22/01/2025

DOCUMENTOS RELACIONADOS

No	NOMBRE	CÓDIGO
1	ACTA RESPONSABILIDAD COMPONENTES Y USUARIOS TECNOLÓGICOS	A-TICSI F 005
2	PROCEDIMIENTO COPIAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	A-TICSI-PC 003
3	MATRIZ TECNOLOGÍA	A-TICSI-F008

ELABORADO POR	REVISADO POR	APROBADO POR
Ing. Joao Enrique Pinzon Pinzon Referente de tecnología	Claudia Puello Castro Referente de Calidad Julia Andrea De Ávila Heredia Jefe de Oficina Asesora de Planeación y Gestión Interna	María Victoria Herrera Roa Gerente

4		
5		
7		
Lugar y Tiempo de Archivo: De acuerdo a las Tablas de Retención Documental de la Empresa de Salud ESE del Municipio de Soacha		

ELABORADO POR	REVISADO POR	APROBADO POR
Ing. Joao Enrique Pinzon Pinzon Referente de tecnología	Claudia Puello Castro Referente de Calidad Julia Andrea De Ávila Heredia Jefe de Oficina Asesora de Planeación y Gestión Interna	María Victoria Herrera Roa Gerente