E.S.E. Municipal de Soacha Julio César Peñaloza	E.S.E. MUNICIPAL DE SOACHA JULIO CÉSAR PEÑALOZA	
MACROPROCESO: APOYO	**Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información**	**CODIGO:**
PROCESO: SISTEMAS INTEGRADOS DE GESTIÓN		**VERSION: 1**
SUBPROCESO: GESTIÓN INFORMACION		**FECHA: 22/03/2020**

TABLA DE CONTENIDO

1. INTRODUCCIÓN 2
2. OBJETIVOS 2
   2.2 Objetivo general 2
   2.2 Objetivos específicos 3
3. ALCANCE 3
4. DEFINICIONES 4
5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO 7
   - Sponsor del proyecto (SUBGERENCIA ADMINISTRATIVA) 7
   - Director del proyecto (LIDER DE TECNOLOGIA) 7
   - Director de riesgos (LIDER DE TECNOLOGIA) 8
   - Responsable de riesgos Técnicos soporte del Departamento de Tecnología 8
   - Miembro del equipo del proyecto Técnicos soporte del Departamento de Tecnología 9
   - Interesados o stakeholders (Funcionarios de la ESE) 9
   - Consultores y proveedores (demás contratistas de otros campos de la ESE) 10
6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO 10
7. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO 11
   7.1 Identificación de riesgos 11
   7.2 Medición o evaluación 12
   7.3 Control y mitigación 12
   7.4 Monitoreo 12
7.5 Inventario de activos 12
8. DIMENSIÓN DE SEGURIDAD 13
8.1. La disponibilidad de la información 13
8.2. La integridad de la información 13
8.3. La confidencialidad de la información 13
9. ANALISIS DE AMENAZAS 14
10. AMENAZAS 15
11. EVALUACION DEL RIESGO 17
11.1. Analizando los riesgos informáticos 17
11.2. Reduciendo los riesgos informáticos 17
12. VALORACION DEL RIESGO 18
13. IDENTIFICACION DE CONTROLES 18
14. MANEJO DE RIESGOS 19
14.1. Controles técnicos 20
14.2 Implementar programas de capacitación y sensibilización 21

1. INTRODUCCIÓN

El presente documento define las medidas de seguridad identificadas para desarrollar durante el año 2021 y con seguimiento periódico hasta el 31 de diciembre de 2021 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 a las entidades minimizar riesgos y maximizar oportunidades. Todo el equipo 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 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

Al establecer el Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos. El Plan de Tratamiento de Riesgo 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 de sistemas de información vigente en los funcionarios y contratistas de la E.S.E. Municipal de Soacha Julio César Peñaloza.
- 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.
- 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 entidad.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos 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 integrar 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 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. basándonos en este alcance logramos identificar falencias, brechas que brindan seguridad a los funcionarios de la ESE, donde se evidencia que cada proceso tiene información relevante y los funcionarios brindan la seguridad de la misma para un trabajo idóneo.

4. DEFINICIONES

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 del sector TIC, 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 a este fenómeno y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los 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. Se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

- **Evitar**: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.
- **Prevenir**: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.
- **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 equipos de protección personal, ambiental, de acceso mantener copias de respaldo.
- **Dispersar**: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos.
- **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.
- **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**: 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
- **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 de una empresa.
- **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)

El sponsor del proyecto es la persona que lo 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 del proyecto.
- Soportar al director del proyecto en el proceso de gestión de riesgos y darle autoridad para ello.
- Gestionar y solucionar los asuntos que exceden de las responsabilidades del director del proyecto.
- 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 (LIDER DE TECNOLOGIA)

Cómo responsable del proyecto es el responsable 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. En los proyectos de mayor tamaño, esto puede incluir asignar un director de gestión de riesgos, aunque en proyectos menores esta función la asume el propio director del proyecto o algún miembro del equipo.

- 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 (LIDER DE TECNOLOGIA)

Este rol aparece como figura independiente únicamente en proyectos de gran envergadura, siendo lo más habitual que sus responsabilidades sean asumidas por el director del proyecto o algún miembro del equipo. Sus roles en la gestión de riesgos son:

- Actuar como referente y 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. En este sentido 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.

- Gestionar los recursos y presupuesto asignados a la gestión de riesgos.

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

Cada riesgo considerado relevante para el proyecto debe incluir un responsable. Estos responsables forman parte del equipo del proyecto 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. De esta forma, los miembros del equipo del proyecto que no estén implicados en los roles anteriores 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 interesados que no forman parte de los grupos anteriores, y que por tanto no se espera que participen directamente en la ejecución o seguimiento del proyecto. No obstante, estos pueden ayudarnos a identificar riesgos relacionados con sus necesidades y objetivos.

Consultores y proveedores (demás contratistas de otros campos de la ESE 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 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.

6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Administración del Riesgo tiene un papel preponderante 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 Institución 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, que puedan los objetivos y resultados institucionales. Por lo tanto, la Administración del Riesgo es una Herramienta de Gestión que le permite a la institución 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 usuarios y 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 en conjunto con funcionarios y contratistas es por ello que se comprometen a:

- Conocer y cumplir la política de seguridad de la información.
- 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.
- Aprobar la revisión frecuente de los procesos y 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.

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

Debe realizarse 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 organización 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 de los mismos (en función de la frecuencia con la que los mismos suceden) así como, definir el impacto que los mismos podrían generar en caso de ocurrencia. Como resultado de esta segunda etapa, 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

En esta tercera etapa, 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 organización, obtiene el conocido como riesgo residual, que es el riesgo que resulta tras la aplicación de los oportunos controles que hayan sido considerados por la organización.

7.4 Monitoreo

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

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

7.5 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] Persona

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. Algunos ejemplos de falta de disponibilidad de la información son: 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 ERP de la institución sufre una falla de servicio, en el que el sistema «cae» impidiendo accesos legítimos. 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 de ataques contra la integridad de la información son la alteración malintencionada en los archivos de trabajo almacenados en un Servidor mediante la explotación de una vulnerabilidad, o la modificación de un reporte del departamento de facturación por un empleado malintencionado o 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. 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 de información confidencial o el acceso por parte de un usuario no autorizado a información crítica de la compañía 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 en la organización 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 de 1 – 5 y se define en la siguiente tabla:

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

10. AMENAZAS

Desde un hacker remoto o de un programa descargado de forma gratuita, las principales amenazas de un sistema informático 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 de la organización se resguardan de la forma que se tenía previsto 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.

Algunas de las más relevantes amenazas son:

Lógicas: se entiende que 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 informático y que hemos de proteger al máximo son el software, el hardware y los datos.

Usuarios: el propio personal de la E.S.E. Municipal de Soacha Julio César Peñaloza, podría comprometer la seguridad de los equipos, exempleados 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 tercer tipo que alude a las **amenazas físicas** como puedan ser los robos, sabotajes, catástrofes naturales, condiciones atmosféricas o de suministro eléctrico.

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.)*
	Daño de Equipos de la red inalámbrica (router, punto de acceso, 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 capital. 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 online.
- 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 organización. 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 predictivo y preventivo adecuadas. Lo importante, a la postre, es que los gastos en el área de informática de la organización 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.

Matriz de Riesgos						
		Consecuencia				
		1. Leve	2. Menor	3. Moderado	4. Alto	5. Extremo
Probabilidad	E - Casi cierto (frecuente)	M	M	A	E	E
	A - Probable	B	M	A	A	E
	M - Posible	B	M	M	A	A
	B - No muy común	B	B	M	M	A
	L - Raro	L	L	B	B	M

12. VALORACION DEL RIESGO

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos**:** CRONOGRAMA MTO PREVENTIVO Y CORRECTIVO TECNOLOGIA A jun 2021) 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, cosas, 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 y remediación. Maneja los riesgos identificados de la siguiente manera:

- Se identifica las normas y directrices de seguridad aplicables en todos los sectores de infraestructura crítica.
- Se Proporciona un enfoque prioritario, flexible, repetible, basado en el rendimiento y rentable.
- Se ayuda a los usuarios y colaboradores de infraestructura crítica a identificar, evaluar y gestionar el riesgo informático.
- Se prioriza la innovación técnica.
- Se Brinda orientación en lo referente a la tecnología y se permite a los sectores críticos de la organización beneficiarse de la misma.

Se orienta para medir el desempeño de la implementación del marco 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 marco basado en el 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 sistemas son:

Identificar.
Proteger
Detectar
Responder
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 el aprender de 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 trabajadores pueden interferir el funcionamiento real del control, pues si bien es cierto que el sistema