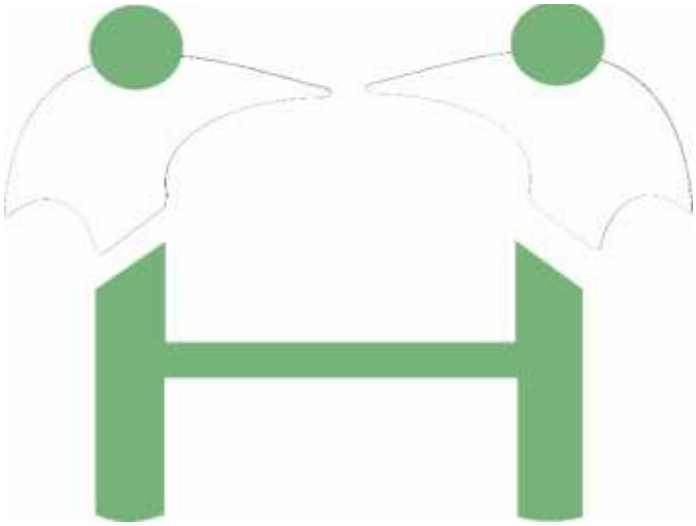
HOSPITAL SAN ANTONIO DE CHIA



DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

"TIC"

Plan de tratamiento de riesgos de seguridad y privacidad de la información.

Chía - 2018

Carrera 10 No. 8-24 Chia, Cundinamarca. PBX 091- 595 12 30/ Fax 863 08 28
E-mail: hchia21@telecom.com.co – Web : http://esehospitalchia.gov.co

TABLA DE CONTENIDO

1. OBJETIVO

Garantizar la continuidad de las operaciones de la institución y que dependen directamente de los sistemas de información de la institución, como el software de gestión financiera y asistencial Dinámica Gerencial.Net, en caso de fallo.

Establecer y definir los procedimientos a seguir, en caso del fallo en alguno de los componentes de la red de datos o del sistema general de información, con el fin de dar continuidad a los procesos informáticos.

Establecer estrategias de recuperación de servicios en caso de contingencia en el menor tiempo posible y los mecanismos físicos a utilizar en caso de tiempo prolongados de inactividad del sistema.

1.2 Objetivos Específicos

- Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en la ESE Hospital San Antonio de Chía, para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.

2. ALCANCE

Este plan de contingencia es una herramienta que abarca todas las áreas del hospital que cuenten con sistema de información y recursos informáticos. Comienza desde el análisis de los posibles riesgos a que están sujetos los equipos y la red de datos, se pretende reducir la posibilidad de ocurrencia de éstos y establecer los procedimientos para dar solución en caso que se presentara algún evento.

3. RESPONSABLES

Alta gerencia, subgerencias, líderes de procesos, área de las TIC

4. TERMINOLOGÍA

- **Hardware**: Es la parte física del computador y permite definir no sólo a los componentes físicos internos (disco duro, placa madre, microprocesador, circuitos, cables, etc.), sino también a los periféricos (escáners, impresoras).

- **Software:** Es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora.

- **Firewall**: Es un sistema diseñado para bloquear el acceso no autorizado de comunicaciones. Se trata de un dispositivo configurado para permitir, limitar, cifrar y descifrar el tráfico de mensajes entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos se utilizan para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet especialmente intranets.

- **Datos**: En general se consideran datos todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (Bases de Datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colecciones de bits.

- **Aplicaciones**: Son los archivos y programas con sus correspondientes manuales de usuario y/o técnicos desarrollados o adquiridos por la entidad.

- **Amenaza:** Cualquier evento que pueda interferir con el funcionamiento de un computador o causar la difusión no autorizada de información confiada a un computador. Ejemplo: Fallas del suministro eléctrico, virus, saboteos o descuido del usuario

- **Base de Datos**: Es un conjunto de datos organizados, entre los cuales existe una correlación y que además están almacenados con criterios independientes de los programas que los utilizan. Entre sus principales características se encuentran brindar seguridad e integridad a los datos, proveer lenguajes de consulta, de captura y edición de los datos en forma interactiva, proveer independencia de los datos.

- **Seguridad**: Se refiere a las medidas que se toman con el objeto de preservar la integridad de sus datos o información procurando que no sean modificados, destruidos o divulgados ya sea en forma accidental, no autorizada o intencional.

- **Sistemas de Información**: Es el almacenamiento de los datos de una organización. Pueden ser registros en archivos de Word y Excel, o pueden ser complejos como una aplicación de software con base de datos.

- **Acceso a la Información Pública**

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control
De sujetos obligados. (Ley 1712 de 2014, art

- **Activo**

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, Personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información**

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

- **Archivo**

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Amenazas**

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo**

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría**

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Autorización**

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- **Bases de Datos Personales**

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Ciberseguridad**

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio**

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control**

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos**

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales**

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos**

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a

su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados**

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- **Datos Personales Mixtos**

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles**

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Declaración de aplicabilidad**

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Derecho a la Intimidad**

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos**

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.
(Ley 1581 de 2012, art 3)

- **Gestión de incidentes de seguridad de la información**

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada**

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada**

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Plan de continuidad del negocio**

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos**

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad**

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Responsabilidad Demostrada**

Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos**

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **Riesgo**

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información**

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI**

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Titulares de la información**

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **Trazabilidad**

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un Individuo o entidad. (ISO/IEC 27000).

5. MARCO LEGAL

- Acceder los datos personales que hayan sido objeto de Tratamiento conforme a lo dispuesto en la Ley 1581 de 2012 y en el Decreto 1377 de 2013 y en las demás normas que los modifiquen, adicionen o complementen.
- Solicitar prueba de la autorización otorgada al Responsable del Tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 en el Decreto 1377 de 2013 y en las demás normas que los modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la Constitución, a la Ley 1581 de 2012 y a las demás normas que la reglamenten, modifiquen o subroguen.

6. CONTENIDO DEL PLAN

Este plan de contingencia es una herramienta que abarca todas las áreas del hospital que cuentan con un sistema de información y recursos informáticos. Comienza desde el análisis de los posibles riesgos a que están sujetos los equipos y la red de datos, se pretende reducir la posibilidad de ocurrencia de estos y establecer los procedimientos para dar solución en caso que se presente un evento.

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la **E.S.E. Hospital San Antonio de Chía**, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar

Ilustración 1 – Marco de Seguridad y Privacidad de la Información

Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC

7. ACTIVIDADES

1. Realizar Diagnóstico
2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
3. Realizar la Identificación de los Riesgos con los líderes del Proceso.
   3.1. Entrevistar con los líderes del Proceso
4. Valorar del riesgo y del riesgo residual
5. Realizar Mapas de calor donde se ubican los riesgos
6. Plantear al plan de tratamiento de riego aprobado por los líderes

7.1 IDENTIFICACIÓN DE RIESGOS (DIAGNOSTICO)

Subdivisión de riesgos según estructura organizacional de red:

1. Riego a nivel del servidor.
2. Riesgos de la red física.
3. Riesgo a nivel de los equipos de cómputo.
4. Riesgos de la información.
5. Riesgos del servicio de internet.

7.1.1 Riesgo a nivel del servidor.

- Corte del fluido eléctrico: debido a fallos a nivel municipal, cambios en el sistema interno y externo o adecuaciones eléctricas sin previo aviso.
- Daño físico en la infraestructura del servidor, ocasionado por incendios, terremotos, inundaciones o calamidades de índole natural.
- Daño de los discos duros.
- Pérdida de la información ocasionada por virus informático.
- Pérdida de información por sabotaje o mal manejo por parte del usuario.
- Falla general o parcial en la base de datos del sistema de información.
- Daño del sistema operativo.
- Problemas con el cableado estructurado.
-

7.1.2 Riesgos de la red física.

- Ruptura del cableado estructurado.
- Desconocimiento de la estructura de la red.
- Ampliación improvisada de red.
- Daño en los switch o router de comunicación.
- Daños en los patch Cord y pash panel de los rack de comunicación.
- Pérdida de conectividad en los puntos de red.

7.1.3 Riesgos a nivel de los equipos de cómputo.

- corte del fluido eléctrico: debido a fallos a nivel municipal, cambio en el sistema interno y externo o adecuaciones eléctricas sin previo aviso.
- Daño físico en la infraestructura ocasionado por incendios, terremotos, inundaciones o calamidades de índole natural.
- Daño de los discos duros.
- Pérdida de la información ocasionada por virus informáticos.
- Pérdida de información por sabotaje o mal manejo por parte del usuario.
- Daño del sistema operativo.
- Problemas con el cableado estructurado, pérdida de información por robo.

7.1.4 Riesgos de la información.

- Falla general o parcial en la base de datos del sistema de información.
- Pérdida de información ocasionada por virus informático.
- Pérdida de información por sabotaje o mal manejo por parte del usuario.
- Pérdida de información por robo.

7.1.5 Riesgos del servicio de internet.

- Interrupción del servicio de internet producido por el servidor web.
- Fallos producidos por los proveedores de internet.
- Mala utilización del servicio de internet.
- Caída del hosting de la página web.

8 PLAN DE CONTINGENCIA DE ACUERDO AL RIESGO

8.1.1 A nivel del servidor.

Si hay falla en el sistema eléctrico:

- Se cuenta con una planta eléctrica que soporta el eléctrico en caso de cortes de energía.

- El servidor tiene dos ups conectadas cada una a una fuente redundante que permite el soporte eléctrico en algún fallo y de manera independiente por 20 minutos.

- Además se cuenta con un sistema de energía regulada, con capacidad de 20 KVA de potencia, lo que permite la conmutación instantánea y el soporte eléctrico suficiente para accionar la planta eléctrica, con una autonomía de más de 30 minutos.

- Daño físico en la infraestructura del servidor, ocasionado por incendios, terremotos, inundaciones o calamidades de índole natural.

- El servidor cuenta con un extintor ubicado estratégicamente y debidamente recargado.

- Existen 2 equipos configurados con todas las aplicaciones necesarias, aptos para funcionar como gestores de bases de datos en caso de que alguno falle.

- El área donde están ubicados los servidores cumple con las condiciones necesarias de ventilación, espacio adecuado, único para el proceso, que garantiza la continuidad del servicio, mediante protocolos propios de la institución a nivel de seguridad.

8.1.2 Daño de los discos duros del servidor.

- Para protección de la información, el servidor está programado para hacer 3 copias diarias en diferentes horarios de la base de datos comprimida diariamente y guardada en un disco externo y es quemada en un DVD, resguardado en la oficina de sistemas.

- El sistema realiza cada tres horas copia de la base de datos y un tarea programada la copia en otro equipo de la red.
- Diariamente se hace mantenimiento general de los discos duros: liberación del espacio, eliminación de archivos temporales.

8.1.3 Pérdida de información ocasionada por virus informático

- Se mantienen unidades de almacenamiento con backups de la información del servidor con el fin de resguardarla cuando sea necesario.

- Igualmente existen backups diarios del sistema de información Dinámica Gerencial, almacenada y resguardada en la oficina de sistemas.

8.1.4 Pérdida de información por sabotaje o mal manejo por parte del usuario

- Existen políticas de seguridad que no permiten el acceso de los usuarios al servidor.

- Cuando hay retiro del personal de sistemas, inmediatamente se cambian las claves del servidor y los aplicativos.

8.1.5 Falla general o parcial en la base de datos del sistema de información.

- Diariamente se realizan backups del sistema de información, la cual es resguardada en la oficina de sistemas en unidades de almacenamiento específicas.

- Se restablece la copia generada en el equipo de computo auxiliar.

8.1.6 Problemas con el cableado estructurado.

- Identificación del fallo por medio del mapeo del cableado.
- Reemplazo de los patsh cort y conectores de red.

8.2 Riesgo de la red física.

8.2.1 Ruptura del cableado

- Identificación del fallo por medio del mapeo del cableado.
- Reemplazo de los patsh cort y conectores de red.

8.2.2 Desconocimiento de la estructura de red.

- Mapeo de cableado entres nodos para identificación de red.
- Registro documental de punto de red en archivo.

8.2.3 Daño de los switch o router de comunicación.

- Prueba y reemplazo de switch o intercomunicadores de red de manera temporal.

8.2.4 Daños en los patch Cord y Pash panel de los rack de comunicación.

- Identificación del punto afectado e independización de los puntos del pash panel afectado.

8.2.5 Pérdida de conectividad en los puntos de red.

- Mapeo e identificación de cableo, cambio de cableado del punto de red, instalación de equipo inalámbrico.

8.3 Riesgo a nivel de los equipos de cómputo.

8.3.1 Corte del fluido eléctrico: debido a fallos a nivel municipal, cambios en el sistema interno y externo o adecuaciones eléctricas sin previo aviso.

Se cuenta con una planta eléctrica

- para garantizar el servicio en caso de corte eléctrico.

- La mayoría de equipos cuenta con conexión a la red regulada.

8.3.2 Daño físico en la infraestructura ocasionado por incendios, terremotos, inundaciones o calamidades de índole natural.

- Se tienen pólizas que garantizan la reposición de las maquinas, la información del aplicativo es resguardar desde el servidor.

8.3.3 Daño de los discos duros.

- Se realiza backup‘s de la información de cada equipo cuando son intervenido en la oficina por causas de reinstalación y formateo de equipos de cómputo, las cuales se encuentran en un disco específico para esto y discos compactos.

8.3.4 Pérdida de información ocasionada por virus informático.

- Todos los equipos tienen instalado un antivirus, el cual se actualiza y se analizan los equipos automáticamente por políticas y gestión de dominio.

- Se tiene como instructivo general, vacunar todas las memorias antes de abrirlas en los equipos, para verificar que no estén infectadas.

8.3.5 Pérdida de la información por sabotaje o mal manejo por parte del usuario.

- Existe control de acceso a la información en el sistema operativo con contraseñas que permiten acceder a una información determinada, son parámetros de administrador, lo que también permite controlar el acceso a descargar archivos ejecutables que atenten contra la seguridad de la información.

- Se generan y autorizan los roles y permisos de acceso a los módulos y consultas del sistema de información.
- En caso de presentarse algún tipo de error, como acceso a los módulos y consultas del sistema de información y teniendo los permios respectivos, se aplican los correctivos de acuerdo a las especificaciones del cargo.

- Al retirarse el personal, el departamento de sistemas se encarga de realizar el bloqueo de acceso al sistema, para evitar posibles saboteos.

- Se tiene herramientas software que monitorizan la actividad de los usuarios en sistema.

8.3.6 Daño del sistema operativo.

- Restauración de la copia de seguridad de la base de datos en el equipo temporal del servidor y revisión del daño.

8.3.7 Problemas con el cableado estructurado.

- Identificación del punto de fallo y conexión de equipo temporal, mientras de identifica el fallo.

- Se acude al mapa de distribución de equipos, se identifica el esquipo afectado y se realiza la corrección necesaria para el funcionamiento de los dispositivos como: disco duro, enlaces de red, cables y logs.

8.4 Riesgos de la pérdida de la información.

8.4.1 Falla general o parcial de la información y de la base de datos del sistema de información.

- Se realiza restauración de backup´s de la información de cada equipo, los cuales se encuentran en un disco específico para esto, no es periódica y solo se realiza a los equipos del área administrativa, los equipos asistenciales no poseen información importante para ser guardada.

8.4.2 Pérdida de información ocasionada por virus informático.

- Se haca mantenimiento e los equipos, vacunación y borrado de archivos temporales.

8.4.3 Pérdida de información por sabotaje o mal manejo por parte del usuario.

- Se realiza restauración de backup´s de la información de los equipos, los cuales se encuentran en un disco específico para esto.

8.4.4 Pérdida de la información por robo

- La institución cuenta con vigilancia privada, quienes cuentan con protocolos de acceso y salida del personal
- Para la protección de datos ante este riesgo, se realiza restauración de la copia de la información de cada equipo y se mantiene en la oficina de sistemas.

- Se cuenta con pólizas que garantizan la restitución de los equipos.

8.5 Riego en el servicio de internet.

8.5.1 Interrupción del servicio de internet producido por el servidor Web.

- Si hay falla en el servidor Web inmediatamente se instala el aplicativo indicado para el servicio (CProxy) en otro equipo, para mantener a todos los usuarios en línea.

8.5.2 Fallos producidos por los proveedores de internet.

- Existen un directorio telefónico de proveedores que permiten una comunicación rápida para dar solución al problema.

- Si el servicio Web, deja d funcionar, el hospital cuenta con un servicio adicional de internet.

8.5.3 Mala utilización del servicio de internet.

- El departamento de sistemas, tiene a su cargo la tarea de realizar los filtros necesarios para el buen manejo del servicio y evitar el acceso a redes sociales que trastorna el eficiente desempeño de los funcionarios.

8.5.4 Caída del hosting de la página web.

- Se acude al directorio telefónico de proveedores, para solicitar el restablecimiento del servicio.

- Se hace copia de datos de los archivos que comprende la página web en otro equipo y en un CD, resguardado en la oficina de sistemas.

9 CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por el la **E.S.E. Hospital San Antonio de Chía**

- Revisión y/o Modificación de la actual Política de Seguridad.
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

10 CRONOGRAMA

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

Actividad	Abril				Mayo				Junio				Julio				Agosto				Septiembre			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Realizar Diagnóstico																								
Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información																								
Realizar la Identificación de los Riesgos con los lideres del Proceso Entrevista con los lideres del Proceso																								
Valoración de riesgo riesgo residual Mapas de calor donde se ubican los riesgos																								
Mapas de calor donde se ubican los riesgos																								
Seguimiento y control																								

11 SEGUIMIENTO y EVALUACIÓN

Al finalizar cada etapa se realizará una reunión con la Subgerente de Proyectos y la Secretaría General para presentar el informe del avance del proyecto y de esta manera evaluar todos los pasos se han ido realizado.

12 ENTREGABLES

- Política de Seguridad

13 MARCO LEGAL

Ley 87 De 1993, Articulo 2° Literal a y f: donde indica:

Proteger los recursos de la organización, buscando si adecuada administración ante posibles riesgos que los puedan afectar.

Definir y aplicar medidas, para prevenir los riesgos, detectar y corregir las desviaciones que se presentan en la organización y que pueden afectar el logro de sus objetivos.

Item	Estrategia (Que se quiere lograr)	Actividades (Acciones para la ejecución del Plan)	Responsable (Quien lo debe hacer)
1	Avance en el cronograma	Valoracion Riesgo residual	Lider TIC
2	Avance en el cronograma	Mapa de calor	Lider TIC

14 ANEXOS

FORMATO PLAN DE ACTIVIDADES

APROBACIÓN DEL DOCUMENTO		
Elaboró	**Revisó**	**Aprobó**
Firma: Nombre: Andres Cubillos Cargo: Ing de Sistemas	Firma: Nombre: Ana Isabel Parra Cargo: Subgerente Administrativa	Firma: Nombre: Rosemberg Rinc Cargo: Gerente

CONTROL DE CAMBIOS			
Fecha	**Versión**	**Cambio**	**Motivo**