CONTENIDO

1. INTRODUCCIÓN

En la actualidad el Hospital San Vicente de Paul Empresa Social del Estado de Filandia Quindío, cuenta con una unidad funcional de sistemas de información donde se procesan todas las transacciones, dentro del proceso de mejoramiento continuo se establece la necesidad de realizar identificación, análisis y evaluación de riesgos y de establecer políticas, procesos, procedimientos y controles que permitan reaccionar ante una posible materialización de los mismos a través del presente plan de tratamiento de riesgo de seguridad y privacidad de la información

La información que se genera a través de los sistemas de información, son de vital importancia para el correcto funcionamiento de cada uno de los procesos institucionales y el cumplimiento de los objetivos misionales, es por ello que la seguridad y privacidad de la información se convierten en atributos indispensables para evitar cualquier posibilidad de alteración, mal uso, pérdida, entre otros eventos, que puedan significar una alteración para el normal desarrollo en la prestación de servicios de salud.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Desarrollar el plan de tratamiento de riesgo seguridad y privacidad de la información, que permita minimizar el riesgo de pérdida de información en el Hospital San Vicente de Paul E.S.E de Filandia Quindío

2.2. OBJETIVOS ESPECÍFICOS

- Establecer políticas, procesos y/o procedimientos de seguridad y privacidad de la información tanto asistencial como administrativa que permitan, para el cliente interno la confiabilidad y veracidad en la generación de informes y para el cliente externo, la garantía de la custodia y privacidad de su información.
- Fortalecer el uso de tecnologías de la información dentro de la institución con el fin de garantizar la seguridad y privacidad de la misma
- Proporcionar al funcionario los procedimientos y conceptos básicos del uso y cuidado de los equipos de cómputo y periféricos en general
- Optimizar el uso de los recursos informáticos.
- Propender a la satisfacción tanto del usuario interno como externo, brindando los respectivos suministros para el almacenamiento y conservación de la información.

3. NORMATIVIDAD

- Ley 23 de 1982 establece la legitimidad de los derechos de autor y la propiedad intelectual.
- Resolución 1995 de 1999. Establece las normas para el manejo de la Historia Clínica.
- Ley 594 de 2000 Reglamenta parcialmente los decretos nacionales por medio de las cuales se dicta la Ley general de archivo.
- Ley 962 de 2005. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos procedimientos administrativos.
- Ley 734 regula el Código Único Disciplinarios.

- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales de habeas data y se regula el manejo de la información en bases de datos personales
- Ley 1581 de 2012. Por medio de la cual de dictan las disposiciones generales para la protección de datos personales.
- Decreto 2364 de 2012. Por medio del cual se reglamenta el uso de firma electrónica.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Ley 1712 de 2014. Por medio de la cal se establece la ley de transparencia y acceso a la información pública.
- Resolución 3564 de 2015. Por medio de la cual se reglamentan los aspectos relacionados con la ley de transparencia y acceso a la información pública.
- Decreto 1078 de 2015. Decreto único reglamentario del sector de las tecnologías de la información y las comunicaciones.
- Acuerdo 03 de 2015 del Archivo General de la Nación. Por el cual se establecen lineamientos generales sobre la gestión de documentos electrónicos.

4. ALCANCE

Dirigido a todos los colaboradores que están involucrados en el manejo de información tanto física como automatizada

5. JUSTIFICACIÓN

El Hospital San Vicente de Paul E.S.E, al ser una institución que ofrece un servicio tan indispensable como es el de la salud y en donde el flujo de información es

constante e importante para el funcionamiento administrativo, el objetivo es no poner en riesgo la seguridad y privacidad de la misma.

Por medio de este plan de tratamiento de riesgos de seguridad y privacidad de la información, se establecen los procesos o procedimientos a seguir respecto a cualquier indisponibilidad de los servicios, riesgo de pérdida de información o riesgo en la vulnerabilidad de la seguridad y privacidad de la misma

6. DEFINICIONES

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.

Activo: Cualquier cosa que tiene valor para la organización. Para el caso específico del presente plan, existen los siguientes activos: información; software, como programas informáticos; físico, como computadores; servicios; personas, y sus calificaciones, habilidades y experiencia; e intangibles, como reputación e imagen

Activo de información: Conocimiento o información que tiene valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la institución.

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo con base en su probabilidad e impacto de ocurrencia.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones.

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.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona/entidad autorizada.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de Seguridad de la Información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

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.

Gestión de riesgos: Proceso de identificar, analizar y responder a factores de riesgo en beneficio de los objetivos.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros, como pérdida de reputación o implicaciones legales.

Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Incidente de seguridad de la información: Un evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Probabilidad: Medida para estimar la ocurrencia del riesgo.

Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

7. ANÁLISIS DE RIESGOS

El Hospital San Vicente de Paul E.S.E de Filandia Quindío pretende, a través del presente documento, identificar, gestionar y establecer controles para la mitigación de los riesgos institucionales, riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico.

Para poder establecer las acciones se seguirán los puntos siguientes:

Identificación del riesgo: Determinar los posibles riesgos que causen una pérdida potencial de información o que impliquen un riesgo de seguridad y privacidad de la misma y comprender el cómo, dónde y porqué podría ocurrir dicha pérdida.

Identificación de los activos: Para nuestro caso específico documentos de tipo físico o informático que por sus características requieran protección, seguridad y privacidad.

Identificación de las amenazas: Identificar las causas que puedan causar riesgos en la seguridad, privacidad o pérdida de la información institucional. Las causas pueden ser de origen natural o humano y pueden ser accidentales o

deliberadas, en todo caso se tendrán en cuenta de manera minuciosa todas aquellas amenazas que afecten el correcto desarrollo de las funciones institucionales y puedan ocasionar riesgos institucionales de cualquier tipo

Así las cosas, la documentación asociada al presente plan son

- Matriz de riesgos
- Inventario de activos de información
- Plan de seguridad y privacidad de la información
- Política de seguridad informática
- Política de tratamiento de datos personales
- Plan de contingencia por áreas

7.1. CLASIFICACIÓN DEL RIESGO

La clasificación del riesgo se establece de dos formas:

1. de acuerdo al impacto sobre los procesos y según la importancia dentro del correcto flujo de las actividades tanto administrativas como asistenciales

Impacto Catastrófico: Las consecuencias pueden afectar totalmente el hospital, produciendo daños irrecuperables y afectar completamente la imagen de la institución. A nivel de pacientes la afectación es alta produciendo daños irreparables en la salud y la vida misma del paciente.

Impacto Mayor: Las consecuencias de los riesgos pueden afectar de manera importante los procesos y servicios del Hospital y afectar la imagen institucional. A nivel de los pacientes puede existir un nivel medio de afectación que implique altos costos, pérdida importante de tiempo o cancelación definitiva de servicios

Impacto Moderado: Las consecuencias de los riesgos afectan parcialmente los procesos y servicios del hospital pero la perdida y daños son menores y o afectan la imagen institucional. A nivel de los pacientes puede existir un nivel mínimo de afectación que puede corresponder a tiempo, costos o reprocesos

Impacto Menor: Las consecuencias de los riesgos afectan levemente al hospital pero pueden pasar desapercibidas para los pacientes y no afectan la prestación del servicio ni la imagen institucional.

Impacto leve: Las consecuencias de los riesgos no afectan a ningún proceso del hospital

2. de acuerdo a la probabilidad de ocurrencia del riesgo

Probabilidad de ocurrencia remota: Improbable que ocurra (No ha ocurrido en los últimos cinco años)

Probabilidad de ocurrencia rara: posible que ocurra en algún momento (puede ocurrir al menos una vez en los últimos cinco años)

Probabilidad de ocurrencia ocasional: probablemente ocurrirá (puede suceder al menos una vez en los últimos dos años).

Probabilidad de ocurrencia frecuente: probablemente ocurrirá en la mayoría de las circunstancias (al menos una vez en el último año)

Probabilidad de ocurrencia casi segura: se espera que el evento ocurra en la mayoría de las circunstancias (más de una vez al año)

7.2. IDENTIFICACIÓN DE LOS RIESGOS

Se pueden identificar 3 clases de riesgos inherentes de seguridad de la información:

Pérdida de la Confidencialidad: Pérdida de la propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.

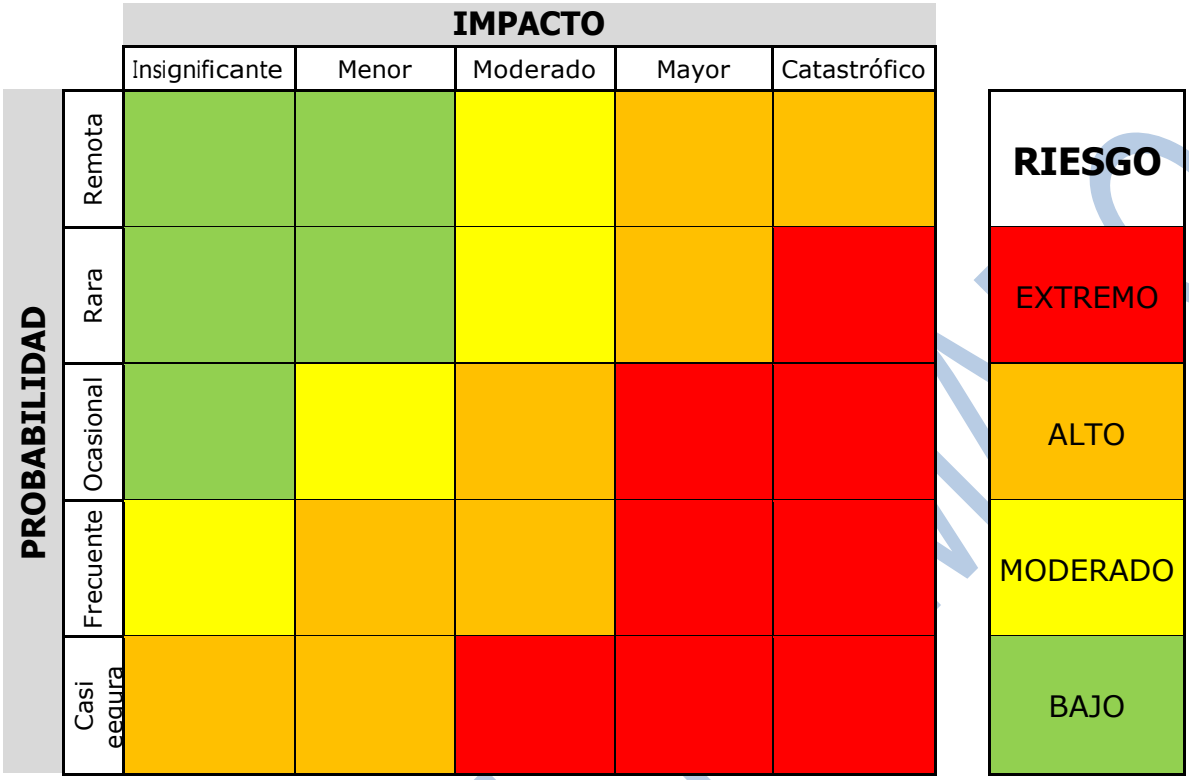
Pérdida de la Integridad: Pérdida de la propiedad de contar con información exacta y completa, o que pudo haber sido sin ser manipulada o alterada por personas o procesos no autorizados.

Pérdida de la Disponibilidad: Pérdida de la cualidad o condición de la información de encontrarse a disposición de quienes requieran acceder a ella, ya sean personas, procesos o aplicaciones.

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Teniendo en cuenta las amenazas comunes, las amenazas dirigidas por el hombre la vulnerabilidad común. Usando como referencia el Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas.

7.3. EVALUACIÓN DE LOS RIESGOS

La evaluación del riesgo se realizará a través de una matriz de calor de acuerdo al impacto y a la probabilidad de ocurrencia del mismo de la siguiente manera:



7.4. TRATAMIENTO DE LOS RIESGOS

Para el manejo de los riesgos se analizarán las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos y cambios físicos entre otros.

Se plantearán controles empleando como referencia los controles del "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", con el fin de mitigar/tratar los riesgos de seguridad de la información.

El tratamiento de riesgos implica tomar decisiones basadas en los resultados de la identificación de riesgos y su análisis. La política de gestión de riesgos está determinada por las siguientes opciones de tratamiento:

ZONA DE RIESGO	DESCIPCION	TRATAMIENTO
EXTREMO	En esta zona de riesgo extrema debe siempre y de manera simultánea: evitarse el riesgo, reducirlo y compartir o transferir el riesgo. Los puntos de control deben ser más estrictos	* Reducir el riesgo * Corregir la probabilidad de riesgo * Compartir las acciones correctivas * Transferir para plan de mejoramiento y seguimiento
ALTO	En esta zona de riesgo alta debe siempre evitar, reducir y compartir las acciones correctivas del riesgo	* Reducir el riesgo * Corregir la probabilidad de riesgo * Compartir las acciones correctivas
MODERADO	Evaluada la probabilidad e impacto es posible asumir el riesgo, pero siempre acompañado de acciones para reducirlo y evitarlo en lo posible.	* Asumir el riesgo * Reducir el riesgo
BAJO	Dada su baja probabilidad de presentación, es posible asumir el riesgo, sin embargo debe de realizarse un seguimiento	*Asumir el riesgo

7.5. MONITOREO, MEDICIÓN, REVISIÓN Y EVALUACIÓN E LOS RIESGOS

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación:

En primera instancia el seguimiento se debe llevar a cabo por el responsable del proceso (Gerencia).

Segundo momento de seguimiento por parte del Subgerente (Procesos asistenciales, procesos administrativos y financiero).

La Oficina de Control Interno comunicará y presentará luego del seguimiento y evaluación, los resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas

Una vez por semestre, los líderes de cada uno de los procesos deben monitorear su respectivo mapa de riesgos realizando los ajustes que considere necesarios ante los riesgos presentados y justificar dichos cambios ante las oficinas de planeación y control interno.

Cada responsable de proceso realizará una autoevaluación a la gestión del riesgo, determinando la efectividad de sus controles para minimizar el riesgo, a su vez la Oficina de Control Interno realizará su propio informe de evaluación de riesgos y controles de segundo orden.

El informe de seguimiento a los riesgos institucionales consolidado por la Oficina de Control Interno es publicado en la página web y se constituye como un insumo para la gestión y mejoramiento institucional y en una de las bases principal de revisión de cumplimiento del presente plan.

8. BIBLIOGRAFIA

Guía 7 gestión de riegos. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

Guía 8 controles de seguridad y privacidad de la información. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.