E.S.E HOSPITAL ANA SILVIA MALDONADO JIMENEZ DE COLOMBIA - HUILA

Plan De Tratamientos De Riesgos De Seguridad Y Privacidad De La Información

Colombia, Enero de 2025

TABLA DE CONTENIDO

1. INTRODUCION

La institución en su que hacer diario utiliza TIC en cuanto a captura, procesamiento y reporte de información tanto internamente como externamente para comunicarse con los diferentes actores del sistema de salud, lo cual implica que la institución sea vulnerable a ataques mal intencionados o mala manipulación de la información lo que acarrea problemas económicos, legales, y administrativos por lo cual este documento busca establecer un línea de trabajo que permita a la entidad sortear los riesgos que lo rodean y lograr que su información este segura.

La información que genera constantemente el Hospital Ana Silvia Maldonado Jiménez de Colombia - Huila, es crucial para su correcto desempeño y cumplimiento de los objetivos organizacionales, 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.

2.1. Objetivo General

Desarrollar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información el cual sea una guía para el control y minimización de los de los riesgos y así proteger la privacidad de la información y los datos tanto de los procesos como de las personas vinculadas con la información de la institución.

2.2. Objetivos Específicos

- Lograr un diagnóstico real de la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información

- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y Mintic para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información

- Optimización de los recursos de la institución en la aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

El Hospital Ana Silvia Maldonado Jiménez de Colombia – Huila, proporcionará una metodología establecida por la Institución para el tratamiento de riesgos de amenazas de la información interna, donde se orientara sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis y valoración de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

La estructura organizacional de los procesos responsables de la realización del plan es la siguiente:

GERENTE
ASESORES
EQUIPO ADMINISTRATIVO
EQUIPO ASISTENCIAL

5. MARCO NORMATIVO

- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales
- Ley 594 de 2000 - Ley General de Archivos
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

- Decreto 2364 de 2012 - Firma electrónica
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales
- Ley 527 de 1999 - Ley de Comercio Electrónico
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información

6.1 Contexto de La Gestión Del Riesgo De Seguridad Y Privacidad De La Información

Corresponde a una visión general de los riesgos que pueden afectar el cumplimiento de los objetivos en este caso para la seguridad y privacidad de la información se analiza información de la estructura organizacional, del modelo de operación por procesos, del cumplimiento de planes y programas, de los recursos físicos y tecnológicos, entre otros. Para establecer el contexto para la gestión del riesgo es necesario definir los criterios de riesgo de seguridad y privacidad de la información:

Criterios De Evaluación Del Riesgo

Para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización se tienen en cuenta los siguientes aspectos.

- El valor estratégico del proceso de información para la entidad.
- La criticidad de los activos de información involucrados en el proceso.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

Criterios De Impacto.

Los criterios de impacto del riesgo se especifican en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información de los procesos.
- Brechas en la seguridad dela información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información).
- Operaciones deterioradas
- Perdida del negocio y del valor financiero
- Alteración de planes y fechas limites
- Daños para la reputación
- Incumplimiento de los requisitos legales.

El Hospital Cuenta Con Los Siguientes Criterios

El riesgo inherente es importante porque la diferencia entre este y el riesgo residual proporciona una medida de la necesidad y la eficacia del tratamiento del riesgo actual. Si la diferencia entre el riesgo inherente y el residual es pequeña, el riesgo no necesita ser tratado o el tratamiento es ineficaz.

- Para calcular el riesgo residual es necesario primero evaluar la efectividad de los controles.

- Los responsables de los procesos, son los propietarios de sus riesgos y les corresponde rendir cuentas sobre su gestión, ellos deben realizar la medición de sus controles en términos de eficiencia, eficacia y efectividad para

determinar la pertinencia, la necesidad de ajuste o modificación en caso de presentarse.

- Corresponde a todos los responsables de procesos y líderes de proyectos identificar e implementar acciones preventivas cuando el cálculo del riesgo residual los ubique en zona de riesgo inaceptable o importante.

- Cuando el cálculo del riesgo residual los ubique en zona de riesgo aceptable, tolerable o moderado, no requerirá implementar acciones preventivas, sin embargo, se debe continuar con la aplicación de los controles establecidos y el monitoreo permanente del comportamiento del riesgo.

- Cuando el impacto de la materialización del riesgo residual sea mayor o catastrófico, los responsables de los procesos y proyectos deben establecer planes de contingencia que permitan proteger la institución en caso de su ocurrencia.

- Los procesos en los que se hayan identificado riesgos que no posean controles, deben diseñarse los mismos para evitar la materialización del riesgo o establecer acciones preventivas para eliminar la causa del posible riesgo.

6.2 Identificación del Riesgo

Para la identificación y evaluación se toma como base el contexto estratégico que reconoce las situaciones de riesgo de origen interno y externo para la entidad; luego se procede a la identificación de los riesgos, reconociendo variables como agentes generadores, causas, efectos entre otros, para realizar posteriormente la calificación de los riesgos. El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas recolectan datos de entrada para esta actividad.

Categorías De Riesgos

ET: Estratégicos: Relacionados a lineamientos, políticas, estrategias o directrices no adecuadas o no convenientes para la Entidad.

OP: Operativo: Relacionado a procesos, conductas o actividades inapropiadas, contrarias al deber ser o que presente una posible brecha frente a la calidad esperada.

FA: Financiero: Relacionado con la asignación, suficiencia o recaudo de recursos económicos que puedan afectar a corto, mediano o largo plazo financieramente a los procesos o la entidad.

TEC: Tecnológico: Relacionado al uso, manejo o disposición de equipos biomédicos, industriales o de cómputo y periféricos.

Identificación De Las Vulnerabilidades

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes. Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas.

Identificación De Las Consecuencias

Para la identificación de las consecuencias es necesario tener:

- Lista de activos de información y su relación con cada proceso de la entidad.
- Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

Se deben identificar las consecuencias operativas de los escenarios de incidentes en términos de:

- Tiempo de investigación y reparación
- Pérdida de tiempo operacional
- Pérdida de oportunidad
- Salud y seguridad
- Costo financiero
- Imagen, reputación y buen nombre.

6.3 Análisis de Riesgo

Determinar las consecuencias o efectos de la posible ocurrencia del riesgo teniendo en cuenta los objetivos del Hospital, las consecuencias pueden darse en personas, bienes materiales o intangibles como la imagen y prestigio corporativo.

Para realizar el análisis se utiliza las siguientes tablas para evaluar la probabilidad y el impacto:

CALIFICACIÓN		VARIABLE
1	**Remota**	Improbable que ocurra (No ha ocurrido en los últimos cinco años)
2	**Raro**	Posible que ocurra en algún momento (puede ocurrir al menos una vez en los últimos cinco años)
3	**Ocasional**	Probablemente ocurrirá (puede suceder al menos una vez en los últimos dos años).
4	**Frecuente**	Probablemente ocurrirá en la mayoría de las circunstancias (al menos una vez en el último año)
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias (más de una vez al año)

6.4 Evaluación del Riesgo

En la fase de evaluación se toman las decisiones sobre las acciones futuras basadas en el conocimiento del riesgo que se ha obtenido durante la fase de análisis. En la mayoría de las ocasiones, el criterio para tomar la decisión de, si se debe tratar el riesgo y cómo hacerlo, depende de los costes/beneficios de aceptar el riesgo y/o de implantar los controles pertinentes. El criterio de "tan bajo como razonablemente sea posible" es un clásico de este enfoque de criterio.

Esta última etapa es la valoración del riesgo y se realiza de manera tal que permita establecer la probabilidad de su ocurrencia y el impacto sobre la operación del hospital. Para facilitar la calificación y evaluación a los riesgos, a continuación, se presenta una matriz que contempla un análisis cualitativo, para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad).

		IMPACTO
Muy Bajo	**1**	Los efectos de materialización del riesgo no son significativos.
Bajo	**2**	Los efectos de materialización del riesgo son poco significativos.
Moderado	**3**	Los efectos de materialización del riesgo pueden significar aspectos moderados.
Alto	**4**	Los efectos de materialización del riesgo son significativos e importantes.
Muy Alto	**5**	Los efectos son catastróficos, como muerte, lesiones incapacitantes o liquidación de la empresa.

7. TRATAMIENTO Y SEGUIMIENTO DEL RIESGO

Para el manejo de los riesgos se deben analizar 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. 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:

Zonas o niveles de criticidad e intervención del riesgo		Tratamiento
Zona de Riesgo Baja	Dada su baja probabilidad de presentación, es posible asumir el riesgo, pero deben planearse acciones para reducirlo en caso que se presente.	Asumir el riesgo
Zona de Riesgo Moderada	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
Zona de Riesgo Alta	En esta zona de riesgo alta debe siempre evitar, reducir, compartir o transferir el riesgo.	Reducir el riesgo, evitar, compartir o transferir
Zona de Riesgo Extrema	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, evitar, compartir o transferir

Seguimiento De Riesgo

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. 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. Semestralmente se realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

- Cumplimiento de las políticas y directrices para la administración del riesgo: metodología de Administración del Riesgo (diseño y funcionamiento).
- Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.
- Los resultados de la evaluación y las observaciones de la persona que haga las veces de auditor deben ser presentados, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización

8. CONTROL DE RESPONSABILIDADES

APROBÓ

Nombre: EDUARDO MAHECHA REYES
Cargo: Gerente E.S.E
Fecha: ENERO DE 2025