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

E.S.E. HOSPITAL SAN JUAN DE DIOS
SANTA FE DE ANTIOQUIA
Camino a la excelencia con respeto y humanización

2021

Contenido

INTRODUCCIÓN

La información que genera constantemente el Hospital San Juan de Dios de Santa Fe de Antioquia 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.

De acuerdo a lo mencionado anteriormente, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información –MSPI-, un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Es por esto que el Hospital San Juan de Dios adopta la metodología "Guía de Riesgos" del Departamento Administrativo de la Función Púbica y como herramienta metodológica la utilizada por la Unidad Nacional para la Gestión del Riesgo de Desastres de la Presidencia de la República, además ha incorporado como referente la Norma ISO 31000 con el objetivo de generar buenas prácticas de gobierno corporativo y del mejoramiento continuo en la gestión de riesgos.

El Hospital San Juan de Dios acoge la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, maximizar rendimientos y cuidar la seguridad del paciente.

1. OBJETIVO

Vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información con la Metodología de riesgos del DAFP.

2. EJECUCIÓN DEL PLAN

Para la realización del plan de tratamiento de riesgos de seguridad y privacidad de la información se utilizó la Guía 7 Gestión de riesgos y la Guía 8 Controles de seguridad de la información.

2.1. ESTABLECER EL CONTEXTO PARA 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 de la 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.

CRITERIOS DE ACEPTACIÓN DEL RIESGO

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo y se podrían considerar los siguientes elementos:

- Criterios del negocio
- Aspectos legales y reglamentarios
- Operaciones
- Tecnología
- Finanzas
- Factores sociales y humanitarios

El Hospital San Juan de Dios 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.

Ejemplo contexto

CONTEXTO						
EVENTO (RIESGO)		**CAUSA**				**Consecuencia (Lo que podría ocasionar)**
		CONTEXTO INTERNO		**CONTEXTO EXTERNO**		
N° Riesgo	**Puede suceder …**	**Tipo**	**Debido a..**	**Tipo**	**Debido a…**	
R1	Interrupción de la operación del sistema de información de SERVINTE	Máquinas-equipos	Caída del enlace hacia los servidores SERVINTE, Obsolescencia tecnológica (ej:servidores) Falta de mantenimiento a los equipos.	Tecnológicos	Caída del fluido eléctrico, falta de equipos de refrigeración y/o inconvenientes por humedad, accesos no autorizados, No disponibilidad del servicio por parte de proveedor.	No continuidad en el proceso de atención integral en salud y procesos de apoyo a través de la herramienta SERVINTE Pérdida de la información durante la contingencia (Historia Clínica), Pérdidas financieras . Subfacturación por falta del sistema SERVINTE Posible ocurrencia de eventos adversos

2.2. VALORACIÓN 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.

A partir de los factores internos y externos, se determinan los agentes generadores del riesgo de seguridad y privacidad de la información sus causas y sus consecuencias: pérdida, daño, perjuicio o detrimento.

Para los riesgos de seguridad y privacidad se debe tener en cuenta:

IDENTIFICACIÓN DEL RIESGO

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.

IDENTIFICACIÓN DE LOS ACTIVOS

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar acabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas) Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

IDENTIFICACIÓN DE CONTROLES EXISTENTES

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo la duplicidad de controles, además de esto mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.

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.

NOTA: Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, entre otros.

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.

IDENTIFICACION DEL RIESGO						
N° DEL RIESGO	**RIESGO**	**CLASIFICACIÓN**	**SUCATEGORÍA**	**CAUSAS**	**DESCRIPCION DEL RIESGO**	**CONSECUENCIAS POTENCIALES**
R1	Interrupción de la operación del sistema de información de SERVINTE	Operativo	Tecnológico	Caída del enlace hacia los servidores SERVINTE, Obsolescencia tecnológica (ej:servidores) Falta de mantenimiento a los equipos. . Caída del fluido eléctrico, falta de equipos de refrigeración y/o inconvenientes por humedad, accesos no autorizados, No disponibilidad del servicio por parte de proveedor.	A causa de problemas con la infraestructura, el canal, la red de suministro eléctrico o problemas con los proveedores se puede causar una falta de disponibilidad de la herramienta que podría causar retrasos o reprocesos en los procesos asistenciales e inactividad de operaciones en procesos administrativos	No continuidad en el proceso de atención integral en salud y procesos de apoyo a través de la herramienta SERVINTE Pérdida de la información durante la contingencia (Historia Clínica), Pérdidas financieras . Subfacturación por falta del sistema SERVINTE Posible ocurrencia de eventos adversos

2.3. ANÁLISIS DE RIESGOS

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:

Criterios para clasificar la probabilidad de ocurrencia del riesgo

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)

Criterios para la calificación del impacto del riesgo

Calificación		Variable
1	**Insignificante**	Las consecuencias de los riesgos, si ocurren no afectan a ningún proceso del Hospital.
2	**Menor**	Las consecuencias de los riesgos, si ocurren, afectan levemente al Hospital y pueden pasar desapercibidas para el paciente y no afectan la prestación del servicio ni la imagen institucional. En equipos o instalaciones daños por cuantía menor a 150 SMLMV.
3	**Moderado**	Las consecuencias de los riesgos pueden afectar parcialmente los procesos y servicios del Hospital, pero las pérdidas y daños son menores y no afectan la imagen institucional. En los pacientes puede aumentar la estancia o el nivel de complejidad de cuidados para 1 o 2 pacientes; en los visitantes puede requerirse atención sin hospitalización para 1 o 2 de ellos; en la personal pérdida de tiempo y restricciones por enfermedad o lesiones.

		En equipos o instalaciones daños por cuantía de 150 a 450 SMLMV.
4	**Mayor**	Las consecuencias de los riesgos pueden afectar de manera importante los procesos y servicios del Hospital y afectarse igualmente la imagen institucional. En los pacientes puede producirse discapacidad, desfiguramiento, requerir intervención quirúrgica y aumento de la estancia o del nivel de complejidad en cuidados para 3 o más pacientes; en los visitantes puede requerirse hospitalización para 1 o 2 de ellos; en la personal hospitalización de 1 o 2 de ellos. En equipos o instalaciones daños por cuantía de 450 a 1500 SMLMV.
5	**Catastrófico**	Las consecuencias pueden afectar totalmente al Hospital produciendo daños irrecuperables y afectarse la imagen institucional de manera grave. El resultado en pacientes puede ser muerte o discapacidad grave, suicidio, violación, reacción-hemofílica post-transfusional, cirugía en sitio equivocado, rapto de niños, entrega de niños a familia equivocada; en visitantes puede producirse muerte o requerirse hospitalización para más de 3 personas; en el personal puede producir muerte u hospitalización de 3 o más personas. En equipos o instalaciones daños por cuantía superior a 1500 SMLMV.

2.4. EVALUACIÓN DE RIESGOS

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).

Probabilidad					
Casi seguro (5)					
Frecuente (4)					
Ocasional (3)					
Raro (2)					
Remota (1)					
	Insignificante (1)	**Menor (2)**	**Moderado (3)**	**Alto (4)**	**Catastrófico (5)**
Impacto					

Criterios para la evaluación del riesgo

Las categorías relacionadas con el Impacto son: insignificante, menor, moderado, alto y catastrófico. Las categorías relacionadas con la Probabilidad son: remota, raro, ocasional, frecuente, casi seguro.

2.5. TRATAMIENTO DE RIESGOS

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 Bajo	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

La gestión del riesgo está alineada con el modelo de mejoramiento institucional y es una de las fuentes de mejora. Para el tratamiento de los riesgos se implementan planes de mejoramiento, especialmente en los casos que se identifican nuevos riesgos, cuando es necesario rediseñar los controles existentes o definir unos nuevos controles.

2.6. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad, por sus siglas en ingles Statement of Applicability (SoA), es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información.

- La declaración de aplicabilidad se debe realizar luego del tratamiento de riesgos, y a su vez es la actividad posterior a la evaluación de riesgos.
- La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación, los que se hayan descartado, de igual manera se debe justificar por qué algunas medidas han sido excluidas (las innecesarias y la razón del por qué no son requerías por la Entidad).

		Objetivo de control o control seleccionado Si/No	Razón de la Selección	Objetivo de control o control Implementado Si/No	Justificación de exclusión	Referencia	Aprobado por la alta dirección Firma director de la entidad
Dominio	A.5 Políticas de seguridad de la información						
Objetivo de control	A. 5.1 Directrices establecidas por la dirección para la seguridad de la información						
Control	A. 5.1.1 Políticas para la seguridad de la información						
Control	A. 5.1.2 Revisión de las políticas para seguridad de la información						

3. COMUNICACIÓN Y CONSULTA

La comunicación es muy importante porque permite que todas las partes interesadas emitan su propio juicio sobre los riesgos; es importante tener en cuenta que las percepciones variarán en cuanto a los valores, necesidades, suposiciones, conceptos y preocupaciones de los interesados.

4. MONITOREO Y REVISIÓN

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 (Director, Jefe, Líder). 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

Por lo menos cada semestre, 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.

5. MECANISMOS DE SEGUIMIENTO Y VERIFICACIÓN

Los atributos establecidos para valorar el desempeño de la gestión de riesgos es una parte de la evaluación global de la institución y de la medición del desempeño de las áreas y de las personas.

Las valoraciones integrales de toda la institución y particulares por proceso, proyecto o estrategia correspondiente a la disminución del nivel de vulnerabilidad, por lo que se tiene el siguiente indicador:

Índice de riesgo residual por proceso: Expresado como proporción o porcentaje de la reducción de los valores estimados de probabilidad e impacto, luego de aplicar las medidas de gestión de riesgos para cada proceso o proyecto.

Formula:

RIESGO INHERENTE – **EFECTIVIDAD GESTIÓN DEL RIESGO** = RIESGO RESIDUAL

RIESGO CONTROLADO

Meta: Índice de riesgo residual por proceso: Menor de 25

Por lo menos cada semestre, 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.

Se tiene dispuesto en la intranet el Mapa de los riesgos tanto clínicos como administrativos segregados por procesos y responsables para su debida consulta y gestión, este engloba la totalidad de los riesgos a

gestionar alojados en una tabla de Excel debidamente clasificados y valorados

Nivel de Madurez de la Gestión del Riesgo

Herramienta utilizada para capturar y evaluar las prácticas de riesgos de la institución y proporcionar realimentación en forma de una calificación de Madurez de la Gestión de Riesgos. El índice se calcula en base a preguntas relacionadas con las actuales prácticas de gestión de riesgos, la estructura de gobierno corporativo y el proceso de toma de decisiones de la empresa.

Meta: Nivel de Madurez de la Gestión del Riesgo: Mayor de 3.0

6. 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.

7. SEGUIMIENTO, CONTROL Y MEJORA

Las acciones y actividades articuladas al plan de acción de acuerdo a lo estipulado en el decreto 612 de 2018.