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

INTRODUCCIÓN

El Hospital Infantil Concejo de Medellín en busca de la mejora continua tiene adoptada la gestión del riesgo bajo la metodología para la administración del riesgo del Departamento Administrativo de la Función Púbica y dentro de esta gestión es de vital importancia el seguimiento de los riesgos relacionados con la seguridad y privacidad de la información pues para que un sistema sea fiable es crucial conocer las vulnerabilidades y amenazas a los que se enfrenta en el normal desarrollo en la prestación de servicios de salud.

OBJETIVO

Incluir en la gestión de riesgos institucionales la identificación y análisis de los riesgos relacionados con la seguridad de la información.

1. ALCANCE DEL DOCUMENTO

2. MARCO NORMATIVO

NORMA	CONTENIDO
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Norma internacional ISO 31000:2018	Sistemas de gestión del riego
Norma internacional ISO 27000:2013	Seguridad de la información
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

3. ANÁLISIS DE RIESGOS

1. 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 y por qué podría ocurrir está perdida.

2. 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.

3. 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.

4. 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.
Los controles que se planifican para implementar de acuerdo con los planes de implementación de tratamiento de riesgo, se deberían considerar en la misma forma que aquellos que ya están implementados.

5. 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.

6. 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.

Criterios para clasificar la probabilidad de ocurrencia del riesgo

CALIFICACIÓN		VARIABLE
1	**Remota**	Improbable que ocurra (puede ocurrir alguna vez en 5 a 30 años)
2	**Raro**	Posible que ocurra (puede ocurrir alguna vez en 2 a 5 años)
3	**Ocasional**	Probablemente ocurrirá (puede suceder varias veces entre 1 y 2 años)
4	**Frecuente**	Puede ocurrir inmediatamente o en un breve periodo (varias veces en un año)

Criterios para la calificación del impacto del riesgo

CALIFICACIÓN		VARIABLE
1	**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.

2	**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 el personal, pérdida de tiempo y restricciones por enfermedad o lesiones. En equipos o instalaciones daños por cuantía de 150 a 450 SMLMV.
3	**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 el personal, hospitalización de 1 o 2 de ellos. En equipos o instalaciones daños por cuantía de 450 a 1500 SMLMV.
4	**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.

4. EVALUACIÓN DE RIESGOS

La evaluación del riesgo se realiza con la metodología institución de gestión del riesgo que es la adoptada del Departamento Administrativo de la Función Púbica.

Criterios para la evaluación del riesgo

	Impacto			
Probabilidad	Menor (1)	Moderado (2)	Alto (3)	Catastrófico(4)
Remota (1)	1	2	3	**4**
Raro (2)	2	4	6	**8**
Ocasional (3)	3	6	**9**	**12**
Frecuente (4)	4	**8**	**12**	**16**

Acorde los criterios descritos en la tabla anterior, se definen las siguientes zonas de riesgo y la actuación mínima subsecuente una vez sean valorados.

Zonas o niveles de criticidad e intervención del riesgo

Zonas		Calificación según: criticidad del riesgo
Zona de Riesgo Bajo (1, 2)	Dada su baja probabilidad de presentación, es posible asumir el riesgo, pero deben planearse acciones para reducirlo en caso que se presente.	Aceptable
Zona de Riesgo Medio (3, 4, 6)	Evaluada la probabilidad e impacto es posible asumir el riesgo, pero siempre acompañado de acciones para reducirlo y evitarlo en lo posible. Si el impacto está localizado en zona de riesgo medio, pero es catastrófico (puntaje 4) debe compartirse o transferirse y tratarse como riesgo de Zona Alta.	Tolerable
Zona de Riesgo Alta y Extrema (8, 9, 12,16)	En esta zona de riesgo alta debe siempre y de manera simultánea: evitarse el riesgo, reducirlo y compartir o transferir el riesgo. Los puntos de control deben ser más estrictos en zonas de puntaje 12 y 16.	Inaceptable

5. 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

6. SEGUIMIENTO, CONTROL Y MEJORA

Las acciones y actividades articuladas al plan de acuerdo a lo estipulado en el decreto 612 de 2018 se realizará el seguimiento en comité de Gestión y Desempeño.