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

INTRODUCCION

LA Unidad de Salud de Ibagué en busca de la mejora continua implementa un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados el manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma.

La institución en su quehacer 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 lograr que su información este segura.

OBJETIVOS

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.

OBJETIVOS ESPECIFICOS

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 Min tic 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

ALCANCE

El plan de tratamiento de riesgos de seguridad y privacidad de la información aplica a todos los procesos administrativos y misionales de la Unidad de Salud de Ibagué

RESPONSABLE

La oficina de Sistemas de La Unidad de Salud de Ibagué

MARCO CONCEPTUAL

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).

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.

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)

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).

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).

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 publica
- 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
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de
- Tecnologías de la Información y las Comunicaciones
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

DESCRIPCION DEL PLAN

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, las siguientes etapas recolectan datos de entrada para esta actividad

Categoría 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.

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

CL: Clínico: Relacionados a condiciones patológicas de pacientes atendidos en la Unidad de salud de Ibagué.

Identificación de Riesgos:

Normalmente se identifican los riesgos como eventos o situaciones no deseadas que se pretenden evitar, por tal razón la identificación de riesgos inicia con términos como: Ausencia, No adherencia, Inadecuada, No suficiencia, entre otros.

Una vez se identifique el riesgo, debe complementarse para obtener el contexto del riesgo, ya que éste puede presentarse en un área, en un horario, por parte de un grupo de colaboradores, o en unas circunstancias específicas que ayudarán más adelante a determinar las acciones a tomar. Estos son algunos ejemplos de preposiciones a utilizar: al, durante, en, sobre, con, hacia, de, mediante, entre otros.

Descripción de Causas:

Se describen las causas asociadas al riesgo identificado, pueden ser intrínsecas: atribuidas a personas, métodos, materiales, equipos, instalaciones, directamente involucradas en el proceso o externas: cuando provienen del entorno en el que se desarrolla el proceso.

Consecuencias:

Se describen los efectos asociados a la materialización del riesgo, que incidan sobre el objetivo del proceso o la Entidad. Pueden agruparse en: Daños a pacientes o trabajadores, Pérdidas económicas, Perjuicio de la imagen, Sanciones legales, reproceso, Demoras, Insatisfacción, entre otras.

Barreras de Seguridad Existentes:

Se describen los controles implementados o barreras que existen actualmente para evitar la materialización del riesgo se pueden encontrar en los protocolos o procedimientos documentados en las guías de reacción inmediata.

Valoración del Riesgo:

Se mide en cuanto a probabilidad e impacto para obtener un dato cuantitativo que permita su comparación y priorización, como se muestra en las siguientes escalas de valoración:

PROBABILIDAD		
Remota	1	La probabilidad de ocurrencia es muy baja, casi nula
Poco Probable	2	Puede ocurrir bajo circunstancias excepcionales
Probable	3	Puede ocurrir con cierta frecuencia
Ocasional	4	Ocurre algunas veces
Frecuente	5	La ocurrencia se da de manera comun en circunstancias actuales

IMPACTO		
Muy bajo	1	Los efectos de materializacion del riesgo no son significativos
Bajo	2	Los efectos de materializacion del riesgo son poco significativos
Moderado	3	Los efectos de materializacion del riesgo pueden significar aspectos moderados
Alto	4	Los efectos de materializacion del riesgo son significativos e importantes
Muy Alto	5	Los efectos son catastroficos, como muerte, lesiones incapacitantes o liquidacion de la empresa

	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		IMPACTO				

NIVEL DE RIESGO	MEDIDAS RESPUESTA
BAJA	ASUMIR EL RIESGO Y CONTINUAR MONITORIZANDOLO
ACEPTABLE	REDUCIR EL RIESGO PARA LLEVARLO A ZONA BAJA
ALTA	EVITAR-COMPARTIR-TRANSFERIR POR MEDIO DE UN PLAN DOCUMENTADO
INACEPTABLE	EVITAR-COMPARTIR-TRANSFERIR POR MEDIO DE UN PLAN DOCUMENTADO

U.S.I.
Unidad de Salud de Ibagué E.S.E.
Nuestros servicios al alcance de todos

IBAGUÉ VIBRA

PROCESO	DESCRIPCIÓN	EVENTO ADVERSO	CAUSA	CONSECUENCIA	PRBABILIDAD	IMPACTO	EVALUACIÓN	ACCIÓN	RESPONSABLE
Gestión de la información y tics	Revisión e instalación de equipos de computo	Instalación de cableria en mal estado	Deterioro de cables por conStante uso.	deficiente funcionalidad de equipos.	3	3	M	Mantenimiento frecuente a equipos de cómputo e instalación elé ctrica	Oficina de sistemas y apoyo hospitalaria
	Copias de seguridad efectivas	Disco duro no apto para realizar copias de seguridad confiable.	No realización de copias de seguridad, sin efectividad total	Pérdida ecónomica	3	4	A	Adquisición de equipo Corporativo con capacidad de información	Oficina de sistemas
	Equipos de cómputo aptos para el funcionamiento	Daño de equipos y perdida de información.	Equipos de cómputo con baja capacidad para almacenamiento de información y capacidad	Pérdida ecónomica	3	4	A	Adquisición de equipos corporativos tipo servidor de alta funcionalidad.	Oficina de sistemas
Gestión clinica	Diligenciamiento de historias clínicas	historias clínicas incompletas	Falta de datos personales	Archivo histórico clínico incompleto	5	3	M	Auditoria de histórias clínicas; capacitación a personal médico para correcto diligenciamiento de historias clínicas	AUDITORIA CONCURRENTE
	Procesos de custodia de documentos de archivo de gestión, central e historico e Historia clínica física	Deterioro de documentos	Material de baja resistencia	Perdida de información	2	2	B	Digitalizar totalmente las historias clínicas	AUDITORIA CONCURRENTE
GESTION FINANCIERA	Proceso de diligenciamiento de comprobantes que afecten el módulo de contabilidad	Datos erróneos	Datos diligenciados de manera errónea	AFECTACION EN LOS TIEMPOS DE ENTREGA DE LOS ESTADOS FINANCIEROS	2	2	A	ARREGLO DE PARAMETROS EN LOS DISTITNTOS MODULOS QUE AFECTEN LA PARTE CONTABLE	SISTEMAS Y AREA FINANCIERA