Hospital San Rafael de Fusagasugá
"Hospital humano, hospital comprometido"

2020

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

Ing. Javier Antonio Melo R.

E.S.E. HOSPITAL SAN RAFAEL DE FUSAGASUGÁ

31/01/2020

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

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

Elaborado por:
JAVIER ANTONIO MELO RIVERA
LIDER PROCESO DE GESTION TECNOLOGICA

EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN RAFAEL DE FUSAGASUGÁ
MACROPROCESO SUB GERENCIA ADMINISTRATIVA
PROCESO GESTION TECNOLOGICA
AÑO 2020

TABLA DE CONTENIDO

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

1. INTRODUCCIÓN

El Hospital San Rafael de Fusagasugá, en busca de la mejora continua implementa un método sistemático que permita identificar, analizar, evaluar, tratar, monitorear y socializar los riesgos asociados el manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma. El Hospital San Rafael de Fusagasugá en sus actividades utiliza tecnologías de Información y Comunicación para el ejercicio de recibo, revisión, consolidación, validación, análisis y envío 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 o mala manipulación de la información lo que trae consigo problemas a la institución por lo tanto este documento busca establecer un mecanismo que permita a la entidad mitigar los riesgos que existen

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Establecer un plan de tratamiento de riesgos de seguridad y privacidad de la información para así lograr proteger la información institucional y mitigar los riesgos que en ella existen.

2.2. OBJETIVOS ESPECIFICOS

- Realizar un diagnóstico de la situación actual de la institución en cuanto a seguridad y privacidad de la información.
- Identificar la ubicación y propietarios de los activos de información a través del inventario del mismo.
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información

3. ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional

4. CONTENIDO

4.1. DEFINICIONES

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

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).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

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. (ISO/IEC 27000).

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).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

Privacidad: Derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

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).

4.2. METODOLOGIA

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información, se utiliza el ciclo continuo PHVA, tradicional en los sistemas de gestión de la calidad.

- Plan (planificar): establecer el SGSI.
- Hacer: implementar y utilizar el SGSI.
- Verificar: monitorizar y revisar el SGSI.
- Actuar: mantener y mejorar el SGSI

4.3. ACTIVIDADES PROPUESTAS

- Realizar Diagnóstico.
- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
- Valoración del riesgo y del riesgo residual.
- Realizar Mapas de calor donde se ubican los riesgos.
- Plantear al plan de tratamiento de riego aprobado por los lideres

4.4. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por El Hospital San Rafael De Fusagasugá.

- Creación de la Política de Seguridad.
- Aspectos organizativos de la seguridad de la información.
- Seguridad Ligada a los recursos humanos.
- Revisión del Control de acceso.
- Seguridad en la operativa.
- Seguridad en las telecomunicaciones.
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

4.5. CRONOGRAMA

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION																																
ACTIVIDAD	abr-20				may-20				jun-20				jul-20				ago-20				sep-20				oct-20				nov-20				dic-20			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1. Realizar diagnostico																																				
2. Realizar la identificación de los riesgos con los líderes de proceso																																				
3. Valorar el riesgo y el riesgo residual																																				
4. Realizar Mapa de calor donde se ubican los riesgos																																				
5. Plantear plan de tratamiento de riesgo aprobado por los lideres																																				
6. Seguimiento y control																																				

5. BIBLIOGRAFÍA

http://www.eafit.edu.co/institucional/reglamentos/tratamiento-proteccion-datos-personales/Paginas/definiciones.aspx

https://eq2b.com/riesgo-amenaza-y-vulnerabilidad-iso-27001/

6. APROBACIÓN, CONTROL Y DISPOSICIÓN DEL DOCUMENTO

6.1. APROBACIÓN

	Nombre	Cargo	Fecha	Firma
Elaboró				
Revisó				
Aprobó				

6.2. CONTROL DE CAMBIOS Y REVISIONES

Versión	Descripción del cambio o revisión	Nombre	Fecha	Firma

6.3. CONTROL DE COPIAS

Copias	Nombre de quien recibe	Cargo	Fecha	Firma

6.4. CONTROL Y DISPOSICIÓN DE REGISTROS DOCUMENTALES

Identificación		Área de almacenamiento	Conservación		Disposición final
Código	Nombre del documento		Archivo de gestión	Archivo central	