Hospital San Rafael de Fusagasugá

"Hospital humano, hospital comprometido"

2021

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

SISTEMAS

E.S.E. HOSPITAL SAN RAFAEL DE FUSAGASUGÁ

27/01/2021

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

Elaborado por:
SOLUCIONES INTEGRALES Y DESARROLLOS INFORMÁTICOS SAS
Sistemas

EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN RAFAEL DE FUSAGASUGÁ
GESTIÓN DE APOYO
GESTIÓN DE RECURSOS FÍSICOS
AÑO 2021

Aprobación: 27-ENE-2021

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La E.S.E. 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 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 las actividades encaminadas al tratamiento de los riesgos de seguridad y privacidad de la información, que permitan la protección de la información institucional y la mitigación de los riesgos que en ella existen.

2.2. OBJETIVOS ESPECIFICOS

- Realizar un diagnóstico de la situación actual de la institución en cuanto a los riegos en seguridad y privacidad de la información.
- Gestionar los riesgos referentes a la seguridad y privacidad de la información.
- Actualizar 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 tratamiento de riesgos de seguridad y privacidad de la información contempla desde el diagnóstico de la situación actual en entidad hasta el seguimiento a los controles establecidos, y aplica a todos los procesos de la E.S.E. Hospital San Rafael de Fusagasugá en su sede central, sedes adscritas, centros y puestos de salud que 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).

CAUSA: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

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).

CONSECUENCIA: Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

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).

IMPACTO: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

NIVEL DE RIESGO: Valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del nivel del riesgo poder ser probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación.

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: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: 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. METODOLOGÍA

Para establecer y gestionar el tratamiento de riesgos de la seguridad de la información es necesario contar con un diagnóstico de la situación actual de la estructura de riesgos identificados, relacionados con el modelo de operación de procesos.

Así las cosas, la metodología que se usará será la suministrada por parte de la función pública en su guía para la administración del riesgo y el diseño de controles en entidades públicas la cual consta de tres pasos:

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS:

- Lineamiento de la política.
- Clasificación de la información.
  - Público
  - Uso interno
  - Uso Privado
  - Confidencial

IDENTIFICACIÓN DE RIESGOS QUE AFECTEN LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN:

- Análisis de los objetivos.
- Identificación de los puntos de riesgo.
  - DA, BD, CORREO, SHP
  - Servidores.
  - Almacenamiento.
  - Redes de datos.
- Identificación de área de impacto.
- Identificación de factores de riesgos.
- Descripción del riesgo.
- Clasificación del riesgo.

VALORACIÓN DE RIESGOS:

- Análisis de los riesgos.
- Evaluación del riesgo.
  - Evaluación del riesgo inherente: cuando hay ausencia de controles

PROBABILIDAD	Frecuente	2	3	3	4	4
	Ocasional	2	2	3	3	4
	Probable	1	2	2	3	3
	Poco Probable	1	2	2	2	3
	Remota	1	1	1	2	2
		Muy bajo	Bajo	Medio	Alto	Muy Alto
		IMPACTO				

Se presentan las zonas de riesgo las cuales se tienen que trabajar para mitigar los riesgos identificados por medio de controles.

Inaceptable	**Se requiere una acción inmediata.** Riesgo extremo, se requiere acción inmediata. Planes de Tratamiento requeridos, implementados y reportados a la Alta Dirección.
Importante	**Se requiere una pronta atención:** Riesgo alto requiere atención de la Alta Dirección. Planes de Tratamiento requeridos, implementados y reportados a los Líderes funcionales.
Tolerable	**Se administra con procedimientos normales de control:** Riesgo moderado, requiere atención del área involucrada, definición de procedimientos y controles de mitigación.
Aceptable	**Genera menores efectos que pueden ser fácilmente remediados:** Riesgo aceptable – Administrado con procedimientos normales de control.

- Estrategias para mitigar el riesgo.
- Monitoreo y revisión.

4.3. ACTIVIDADES PROPUESTAS

- Actualizar el diagnóstico.
- Determinar los riesgos que van a ser incluidos en el plan de tratamiento de riesgos.
- Aplicación de la metodología de administración de riesgos.
- Establecimiento y ejecución de controles.
- Realizar mapas de calor donde se ubican los riesgos.
- Asignación de las funciones en el grupo de trabajo para realizar la gestión de los riesgos.

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 operatividad.
- 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.

5. BIBLIOGRAFÍA

- Departamento administrativo de la función pública 2018. Decreto 612 de 2018, "por el cual se fijan directrices para la integración de los planeas institucionales y estratégicos al plan de acción por parte de las entidades del estado". Bogotá, Colombia.
- Universidad EAFIT 2021. Política de tratamiento de protección de datos personales de los titulares Medellín, Colombia. Retrived from. Https://www.eafit.edu.co/institucional/reglamentos/tratamiento-proteccion-datos-personales/paginas/politica-tratamiento-datos-personales.aspx
- Ministerio de tecnologías de la información y las comunicaciones 2016. Procedimientos de la seguridad de la información. Bogotá, colombia. Retrived from. Https://www.mintic.gov.co/gestionti/615/articles-5482_g3_procedimiento_de_seguridad.pdf
- Departamento administrativo de la función pública 2020. Guía para la administración del riesgo y el diseño de controles a entidades públicas Bogotá, Colombia. Retrived from. Https://www.funcionpublica.gov.co/documents/28587410/34298398/2020-12-16_guia_administracion_riesgos_dise%c3%b1o_controles_final.pdf/fa179c5e-45bb-dffd-027c-043d4733c834?t=1609857497641

6. ANEXOS

- Formato de cronograma 2021 de plan de tratamiento de riesgos de seguridad y privacidad de la información.

7. APROBACIÓN, CONTROL Y DISPOSICIÓN DEL DOCUMENTO

7.1. APROBACIÓN

	Nombre	Cargo	Fecha	Firma
Elaboró	SOLUCIONES INTEGRALES Y DESARROLLOS INFORMÁTICOS SAS	SISTEMAS	27-ENE-2021	
Revisó	DIEGO ANDRES CUCAITA MORALES	PROFESIONAL APOYO PLANEACIÓN	27-ENE-2021	
	JULIÁN NIETO BELTRÁN	PROFESIONAL APOYO PLANEACIÓN		
	JAIRO BOBADILLA MONTENEGRO	PROFESIONAL PROCESO PLANEACIÓN		
	ISIDRO ALBERTO GONZÁLEZ RODRÍGUEZ	SUBGERENTE ADMINISTRATIVO		
Aprobó	ANDRÉS MAURICIO GONZÁLEZ CAYCEDO	GERENTE	27-ENE-2021	

7.2. CONTROL DE CAMBIOS Y REVISIONES

Versión	Descripción del cambio o revisión	Nombre	Fecha	Firma
01	Creación del documento	JAVIER ANTONIO MELO RIVERA	03-SEP-2018	
02	Actualización de documento a la vigencia, se estructura el documento	SOLUCIONES INTEGRALES Y DESARROLLOS INFORMÁTICOS SAS	27-ENE-2021	

7.3. CONTROL DE COPIAS

Copias	Nombre de quien recibe	Cargo	Fecha	Firma
Original	JAIRO BOBADILLA MONTENEGRO	PROFESIONAL PROCESO PLANEACIÓN	27-ENE-2021	

7.4. CONTROL Y DISPOSICIÓN DE REGISTROS DOCUMENTALES					
Identificación		Área de almacenamiento	Conservación		Disposición final
Código	Nombre del documento		Archivo de gestión	Archivo central	
SS-MA-02 V02	Plan de tratamiento de riesgos de seguridad y privacidad de la información	Planeación institucional	2	8	Conservación total

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

Identificación		Área de almacenamiento	Conservación		Disposición final
Código	Nombre del documento		Archivo de gestión	Archivo central	
SGMA-02 V02	Plan de tratamiento de riesgos de seguridad y privacidad de la información	Plataforma institucional	2	6	Conservación total