



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

2022

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



SISTEMAS

**E.S.E. HOSPITAL SAN RAFAEL
DE FUSAGASUGÁ**

31/01/2022



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

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

Elaborado por:
Soluciones Integrales y Desarrollos Informáticos S.A.S.
Sistemas

**EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN RAFAEL DE FUSAGASUGÁ
GESTIÓN DE APOYO
GESTIÓN DE RECURSOS FÍSICOS
AÑO 2022**



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

TABLA DE CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVOS	3
2.1. OBJETIVO GENERAL	3
2.2. OBJETIVOS ESPECÍFICOS	3
3. ALCANCE.....	3
4. CONTENIDO	3
4.1. DEFINICIONES.....	3
4.2. MARCO NORMATIVO.....	5
4.3. METODOLOGIA.....	6
4.4. ACTIVIDADES PROPUESTAS.....	7
4.5. CUMPLIMIENTO DE IMPLEMENTACIÓN	7
5. BIBLIOGRAFÍA	7
6. ANEXOS	7
7. APROBACIÓN, CONTROL Y DISPOSICIÓN DEL DOCUMENTO.....	8
7.1. APROBACIÓN.....	8
7.2. CONTROL DE CAMBIOS Y REVISIONES.....	8
7.3. CONTROL DE COPIAS	8
7.4. CONTROL Y DISPOSICIÓN DE REGISTROS DOCUMENTALES	8



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

1. INTRODUCCIÓN

Dentro del desarrollo de distintas actividades se utilizan tecnologías de Información y Comunicación logrando así 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

Mediante la implementación del plan de tratamiento de riesgos de seguridad y privacidad de la información se pretende establecer los lineamientos que son base fundamental para apoyar la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo mitigar riesgos para la información.

La E.S.E. Hospital San Rafael de Fusagasugá trabaja en el fortalecimiento de la seguridad de la información, con el fin de fortalecer la información como un activo importante garantizándole protección y privacidad tanto a ciudadanos, funcionarios y en general a la entidad.

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 ESPECÍFICOS

- Mejorar las buenas prácticas de gestión de la seguridad y privacidad aplicables para la E.S.E. Hospital San Rafael de Fusagasugá.
- 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 de Riesgos de Seguridad y Privacidad se hace extensivo a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional esto con el ánimo de crear estrategias para generar una cultura que actuar de manera preventiva contribuyendo en la toma de decisiones esto con el fin de prevenir incidentes que afecten en la operación diaria de la entidad o se vean afectaciones en el cumplimiento de los objetivos planes y programas del Hospital San Rafael.

4. CONTENIDO

4.1. DEFINICIONES

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)



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

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

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

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Nivel de riesgo: Es el 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.

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 auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (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,



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

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.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

4.2. MARCO NORMATIVO

- DECRETO 612 DE 2018 "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado."
- NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001 tecnología de la información. Técnicas de seguridad Sistemas de gestión de la seguridad de la información (SGSI)
- Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales."
- LEY 1712 DE 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."
- Políticas técnicas de seguridad de la información Función Pública 2020 La declaración de la Política de Seguridad de la Información institucional busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión, consolidada en los procedimientos, guías, instructivos y publicaciones, así como la asignación de roles y responsabilidades
- Decreto 103 de 2015, 2019 Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
- Decreto 1494 de 2015 2019 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
- Decreto 1008 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Decreto 2573 de 2014 2018 Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
- Decreto 1377 de 2013 2018 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- Decreto 2609 de 2012. 2017 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Ley estatutaria 1581 de 2012, 2017 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
- Ley 1474 de 2011 2017 Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.



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

- Decreto 4632 de 2011 2017 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 1273 de 2009, 2016 Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
- Ley 527 de 1999 2015 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.

4.3. METODOLOGIA

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.



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

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

4.4. ACTIVIDADES PROPUESTAS

- Actualizar lineamientos de Gestión del Riesgo y metodología de gestión del riesgo.
- Identificación de riesgos de privacidad y seguridad de la información que se incluirán dentro del mapa de riesgos
- Aplicación de la metodología de administración de riesgos
- Aceptación y aprobación de riesgos.
- Establecimiento y ejecución de controles.
- Identificar la ubicación de los riesgos dentro del mapa de calor
- Asignación de las funciones en el grupo de trabajo para realizar la gestión de los riesgos.
- Seguimiento de actividades ejecutadas para el tratamiento de riesgos

4.5. 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.

- Sensibilización de cumplimiento de la Política de privacidad y 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

- <http://www.eafit.edu.co/institucional/reglamentos/tratamiento-proteccion-datos-personales/Paginas/definiciones.aspx>
- <https://eq2b.com/riesgo-amenaza-y-vulnerabilidad-iso-27001/>
- https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf
- 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



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 INTEGRALES S.A.S.	SISTEMAS	31-ENE-2022		
Revisó	DIEGO ANDRÉS CUCAITA MORALES	PROFESIONAL DE APOYO PLANEACIÓN INSTITUCIONAL	31-ENE-2022		
	JAIRO BOBADILLA MONTENEGRO	PROFESIONAL PLANEACIÓN			
	ISIDRO ALBERTO GONZÁLEZ RODRÍGUEZ	SUBGERENTE ADMINISTRATIVO			
Aprobó	ANDRÉS MAURICIO CAICEDO CAYCEDO	GERENTE	31-ENE-2022		
7.2. CONTROL DE CAMBIOS Y REVISIONES					
Versión	Descripción del cambio o revisión	Nombre	Fecha	Firma	
1	Creación del documento	JAVIER ANTONIO MELO RIVERA	03-SEP-2018		
2	Actualización de documento a la vigencia, se estructura el documento	SOLUCIONES INTEGRALES Y DESARROLLOS INFORMÁTICOS S.A.S.	27-ENE-2021		
3	Se actualiza el plan de tecnologías de la información y las comunicaciones PETIC al contexto actual del hospital.	SOLUCIONES INTEGRALES Y DESARROLLOS INFORMÁTICOS S.A.S.	31-ENE-2022		
7.3. CONTROL DE COPIAS					
Copias	Nombre de quien recibe	Cargo	Fecha	Firma	
Original	JAIRO BOBADILLA MONTENEGRO	PROFESIONAL PLANEACIÓN	31-ENE-2022		
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 V03	Plan de tratamiento de riesgos de seguridad y privacidad de la información	Planeación institucional	2	8	Conservación Total