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

LIZ ALIETH MATEUS SANTAMARÍA
Gerente

LEYLA PAOLA REY AVENDAÑO
Subdirectora Administrativa y Financiera

ORLANDO SANCHEZ URIBE
Jefe Oficina Asesora Jurídica

Proyectó:
FÉLIX ACELASMEJÍA
CPS MIPG

Revisó:
EDWIN RENÉ MUÑOZ
Profesional de Sistemas

FLORIDABLANCA
2019

Tabla de contenido

1. Introducción

La gestión del riesgo se ha convertido en una herramienta fundamental para controlar los impactos negativos en cualquier actividad que se ejecute, aun cuando el riesgo siempre permanece inherente a cada proceso, se hace necesario planificar herramientas que coadyuven a minimizar las posibilidades de su materialización.

La ESE CLINICA GUANE además de manejar información producida por si quehacer diario, también tiene la responsabilidad de custodiar registros de propiedad del cliente, consignados éstos en la historia clínica. Ante esta necesidad de administrar el riesgo, la entidad formula el Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información, cuyo plan de acción se ha planteado de acuerdo a los recursos disponibles para la presente vigencia.

2. Política del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2.1. Conceptualización

La gestión del riesgo de seguridad y privacidad de la información se hará efectivo acorde a la política trazada para tal fin en el Manual Integrado de Administración del Riesgo de la entidad, cuyo soporte metodológico se fundamenta en las metodologías de identificación,

valoración y evaluación de riesgos diseñados por el Departamento Administrativo de la Función Pública –DAFP-.

En consecuencia, se hace necesario incorporar los parámetros definidos en el presente plan al Manual Integrado de Administración del Riesgo de la ESE CLÍNICA GUANE Y SU RIS.

2.1. Objetivos

Establecer roles y responsabilidades del riesgo de seguridad y privacidad de la información con el fin de integrarlos en el Manual Integrado de Administración del Riesgo de la ESE CLINICA GUANE.

Identificar los riesgos de seguridad y privacidad de la información con el fin de administrarlos de acuerdo a la política integrada de riesgos de la entidad.

Definir los criterios de la política específica del riesgo de seguridad y privacidad de la información para incorporarla en el Manual Integrado de Administración del Riesgo.

3. Marco Legal

RESOLUCIÓN 1995 DE 1999: Por la cual se establecen normas para el manejo de la Historia Clínica. El Artículo 1 señala: "a) La Historia Clínica es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley… d) Historia Clínica para efectos archivísticos: Se entiende como el expediente conformado por el conjunto de documentos en los que se efectúa el registro obligatorio del estado de salud, los actos médicos y demás procedimientos ejecutados por el equipo de salud que interviene en la atención de un paciente, el cual también tiene el carácter de reservado"

LEY 594 DE 2000: Mediante la cual se establecen las reglas y principios generales que regulan la función archivística del Estado. En el Artículo 3 define el concepto de Archivo en los siguientes términos: "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".

NTC-ISO31000 DE 2011: interpreta que la eficiencia del control interno está en el manejo de los riesgos, es decir: el propósito principal del control es la reducción de los mismos,

propendiendo porque el proceso y sus controles garanticen de manera razonable que los riesgos están minimizados o se están reduciendo.

LEY 1581 DE 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Esta ley estatutaria tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

En la conceptualización de términos contemplados en el Artículo 3, define: "Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales; Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

DECRETO 1377 DE 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

El Artículo 3 señala: "Además de las definiciones establecidas en el artículo 3° de la Ley 1581 de 2012, para los efectos del presente decreto se entenderá por: 1. Aviso de privacidad: Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

2. Dato público: 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.

3. Datos 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…"

ISO 27001 DE 2013: Norma técnica emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

LEY 1712 DE 2014: Mediante la cual se regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

4. Diagnóstico

Actualmente la ESE CLINICA GUANE Y SU RED INTEGRAL DE SALUD carece de una política específica para la administración del riesgo de seguridad y privacidad de la información, sin embargo, existen procedimientos para proteger a sus usuarios en cuanto a los registros contenidos en la historia clínica.

En cuanto a la información propia de la entidad, no existe institucionalizada una política que administre el riesgo para la protección de la información y ésta se encuentra coadministrador por una entidad externa mediante la modalidad de contratación de servicios.

Ante este panorama, se hace indispensable formalizar una política de seguridad y privacidad de la información con su respectiva matriz de riesgos con el fin de dar cumplimiento a la normatividad vigente e integrarla en el Manual Integrado de Administración de Riesgos de la institución.

5. Plan de Gestión para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información

El Plan de Acción para el tratamiento del riesgo de seguridad y privacidad de la información se determinó teniendo en cuenta las necesidades institucionales y la asignación de recursos económicos disponibles para el efecto.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – 2019				
ACCION	**RESPONSABLE**	**INDICADOR**	**META**	**PRESUPUESTO**
Identificar Roles y responsabilidades del riesgo	Subdirección Administrativa - CPS Apoyo Sistemas	Informe Roles y responsabilidades del riesgo	Informe Roles y responsabilidades del riesgo	5% CPS Apoyo Sistemas = $1.530.000
Identificación de los riesgos TI de la entidad	Subdirección Administrativa - CPS Apoyo Sistemas	Matriz de riesgos	Matriz de riesgos	5% CPS Apoyo Sistemas = $1.530.000
Implementar políticas de administración del riesgo	Subdirección Administrativa - CPS Apoyo Sistemas	Manual Integrado de riesgo actualizado	Manual Integrado de riesgo actualizado	5% CPS Apoyo Sistemas = $1.530.000

CONTROL DE CAMBIOS

FECHA	RESPONSABLE	CAMBIO	VERSION	ARCHIVO
2018/07/31	Subdirección Adminsitrativa y Financiera	No Aplica	01	
2019/01/28	Subdirección Administrativa y Financiera	Revisión y ajustes	02	