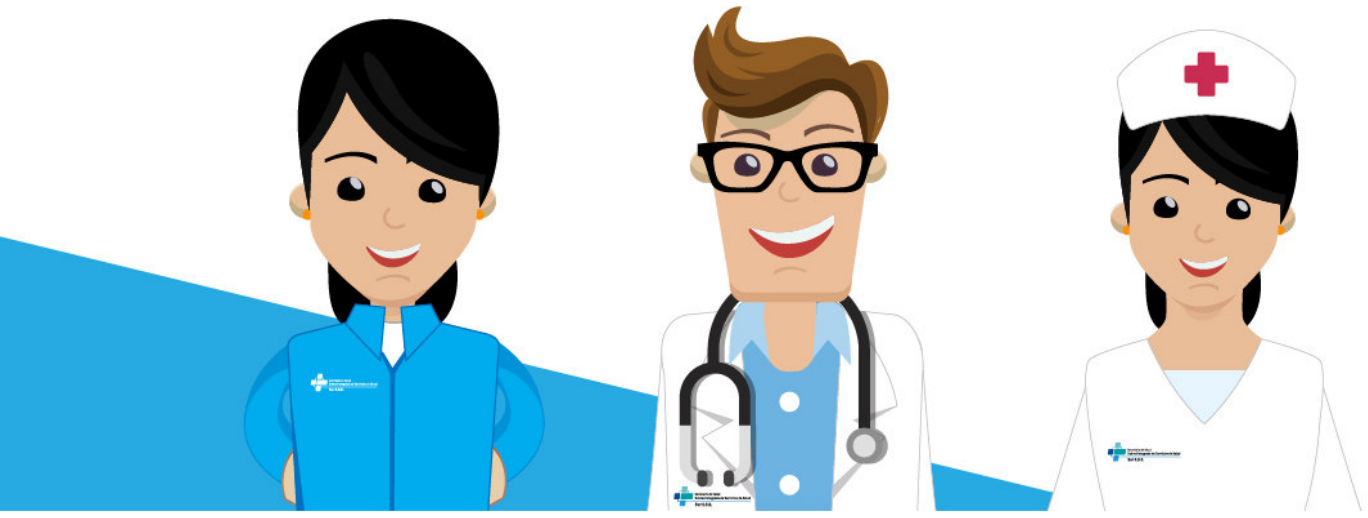
Subred Integrada de Servicios
de Salud Sur E.S.E

PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
GI-TICS-PP-06 V1



1. INTRODUCCIÓN:

El objetivo primordial del Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, es garantizar que éstos sean conocidos, gestionados y tratados por la Entidad de una forma documentada, sistemática, estructurada, repetible y eficiente, para lo cual es esencial identificar y valorar los riesgos que pueden afectar la seguridad y privacidad de la información, y por consiguiente establecer los mecanismos más convenientes para protegerla.

Lo anterior implica, que la Entidad requiere conocer el estado actual de sus activos de información, clasificarlos, priorizarlos y determinar su valor en caso de pérdida de información, y conocer los posibles riesgos que puedan afectar la seguridad y privacidad de los mismos y de esta forma determinar las medidas orientadas a minimizar el impacto en caso de presentarse la materialización de una amenaza.

En la medida que se tenga una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, la Entidad puede establecer controles y medidas efectivas, viables y transversales, con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad de su información, para lo cual es necesario definir los lineamientos que se deben seguir, para el análisis y evaluación de los riesgos de Seguridad de la Información de la Entidad.

2. OBJETIVO:

Definir lineamientos internos que orienten a la institución en la correcta identificación, análisis, valoración y seguimiento de los riesgos de Seguridad y Privacidad de la Información, que puedan afectar el logro de los objetivos institucionales o la atención centrada en el usuario, en el marco del desarrollo de los procesos, proyectos y/o planes, para minimizar su ocurrencia mediante acciones de control efectivas.

3. ALCANCE:

Los lineamientos presentados en este documento, son aplicables a todos los procesos de la Subred Integrada de Servicios de Salud Sur E.S.E., con alcance a los colaboradores de todos los niveles del orden asistencial o administrativos.

DESDE: La identificación de los Riesgos de Seguridad y privacidad de la información.

HASTA: El seguimiento y mejora de la gestión de riesgos de Seguridad y privacidad de la información.

4. DEFINICIONES:

ACTIVO DE INFORMACIÓN: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

AMENAZA: Es la causa potencial de un daño a un activo de información.

ANÁLISIS DE RIESGOS: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

CAUSA: Razón por la cual el riesgo sucede.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible a personas no autorizados

CONTROLES: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

DISPONIBILIDAD: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

IMPACTO: Consecuencias de que la amenaza ocurra.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos.

PROBABILIDAD DE OCURRENCIA: Posibilidad de que se presente una situación o evento específico.

RIESGO: Grado de exposición de un activo que permite la materialización de una amenaza.

RIESGO INHERENTE: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

RIESGO RESIDUAL: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

VULNERABILIDAD: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

5. RESPONSABLES:

El responsable de la elaboración y actualización del presente Plan, es la Oficina de Sistemas de Información TICS (Tecnología de Información y Comunicación en Salud), quien a su vez se encargará de la evaluación y adherencia del mismo, de manera anual.

6. NORMATIVIDAD APLICABLE:

NORMA	AÑO	DESCRIPCIÓN	EMITIDA POR
Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.	MINTIC
NTC / ISO 27001	2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).	Icontec
NTC/ISO 31000	2009	Gestión del Riesgo. Principios y directrices	Icontec

7. CONTENIDO DEL PLAN /Y/O PROGRAMA:

La metodología para la administración de Riesgos de la Subred Integrada de Servicios de Salud Sur E.S.E., se enfoca en primera instancia en la premisa de promover una cultura de riesgos con orientación de resultados frente al control o mitigación de riesgos que puedan afectar la gestión institucional, o puedan afectar las necesidades de los usuarios durante la prestación del servicio, con base en la aplicación de 4 FASES.

7.1 FASE 1. IDENTIFICACIÓN:

Fase en la cual se identifica en primera instancia, los riesgos en seguridad y privacidad de la información de acuerdo a los activos de información identificados en la institución.

7.2 FASE 2. ANÁLISIS Y VALORACIÓN:

Una vez identificado, se procede a realizar el Análisis y Valoración de estos Riesgos, lo que implica establecer su probabilidad de ocurrencia y su nivel de impacto, calificándolo y evaluándolo a fin de determinar la zona de riesgo inicial (riesgo inherente) y determinar la capacidad de la institución para su manejo.

ANÁLISIS Y VALORACIÓN DEL RIESGO								
PROBABILIDAD	IMPACTO	RIESGO INHERENTE / ZONA DE RIESGO	CONTROLES EXISTENTES			CALIFICACIÓN DE LOS CONTROLES	RIESGO RESIDUAL / ZONA DE RIESGO	TRATAMIENTO DEL RIESGO: - EVITAR - REDUCIR - COMPARTIR O TRANSFERIR - ASUMIR
			NATURALEZA DE LOS CONTROLES					
			PREVENTIVOS	CORRECTIVOS	DETECTIVOS			

Fuente Matriz de Riesgos- Oficina Asesora de Desarrollo Institucional Subred Integrada de Servicios de Salud Sur

7.3 FASE 3. DISEÑO PLAN DE ADMINISTRACIÓN DEL RIESGO:

En esta fase se formulan las propuestas de acciones o controles a implementar, las cuales deberán estar enfocadas a la causa del Riesgo. Bajo este contexto, se formulan las acciones de mitigación del riesgo, determinando fecha, mecanismos de medición o seguimiento del desarrollo de la misma y responsable, teniendo en cuenta el ciclo PHVA para su formulación. Así mismo se identifica el indicador el cual se orienta a medir el desempeño del riesgo identificado. Se sugiere en primera instancia revisar los indicadores ya existentes y si alguno se correlaciona con el riesgo identificado con el fin de asociarlo. Las estrategias o acciones definidas deben articularse con las barreras de seguridad o acciones ya existentes en la organización.

ACCIONES A IMPLEMENTAR	FECHA CUMPLIMIENTO	INDICADOR DEL RIESGO	RESPONSABLE (ÁREA / CARGO)

Fuente Matriz de Riesgos Subred Integrada de Servicios de Salud Sur E.S.E.

7.4 FASE 4. SEGUIMIENTO DE LOS RIESGOS:

En esta fase se realiza seguimiento desde las tres líneas de defensa:

7.4.1 La de primer Orden el Jefe de Oficina de sistemas de información TICS durante la aplicación de las acciones de seguimiento manteniendo trazabilidad y/o documentación respectiva de todas las actividades realizadas, para garantizar de forma razonable, que dichos riesgos no se materializarán y por ende que los objetivos del proceso se cumplirán.

7.4.2 En el seguimiento de segundo orden la Oficina Asesora de Desarrollo Institucional. - Gerencia del Riesgo, revisa las evidencias de cumplimiento reportadas por el primer orden y valida los resultados de los indicadores.

7.4.3 En el tercer orden, la Oficina de Control Interno como evaluador independiente de la administración del riesgo, realizará el seguimiento a los indicadores establecidos revisando el resultado general del riesgo, según verificación integral realizada por Control Interno y se describe las recomendaciones a lugar.

8 CONTROL DE CAMBIOS:

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
2017-08-08	1	Creación del documento para la Subred integrada de Servicios de Salud Sur E.S.E

9 BIBLIOGRAFÍA:

https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

DI-GRI-MA-01 MANUAL ADMINISTRACION DEL RIESGO, Subred Integrada de Servicios de Salud Sur E.S.E.

ELABORADO POR	REVISADO POR	CONVALIDADO	APROBADO
Nombre: Andrea Fernanda Baro Moreno	Nombre: Jhon Alexander Cepeda Zafra	Nombre: María Clara León Dugand	Nombre: Jhon Alexander Cepeda Zafra
Cargo: Profesional especializado TICS	Cargo: Jefe Oficina sistemas de Información TICS	Cargo: Profesional Administrativo Oficina de Calidad	Cargo: Jefe Oficina sistemas de Información TICS
Fecha: 2020-01-20	Fecha: 2020-01-21	Fecha: 2020-01-22	Fecha: 2020-01-24