2022

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD D ELA INFORMACION

INSTITUTO DEPARTAMENTAL DE SALUD DE NARIÑO

Oficina de Sistemas de Información
Grupo TIC – IDSN 30-12-2021

FIRMAS Y REVISIONES

Título	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Departamental de Salud de Nariño - IDSN
Autor	Oficina de Sistemas de Información – Grupo TIC – IDSN
Tema	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
Fecha de elaboración	Octubre a diciembre 2021
Formato	PDF
Versión	2.0
Palabras relacionadas	Gobierno Digital, Arquitectura empresarial, tecnología, TIC, sistemas de información, infraestructura TI, Plan Estratégico de Tecnologías de la Información y Comunicación – PETI, Modelo de seguridad y privacidad de la información – MSPI, Sistema de gestión de seguridad de la información

NOMBRE	VERSIÓN	AUTOR	FECHA
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Departamental de Salud de Nariño - IDSN	2.0	Oficina de Sistemas de Información – Grupo TIC – IDSN	Diciembre 2021

CONTROL DE CAMBIOS

COMITÉ	ACTA DE APROBACIÓN	FECHA
Comité de Gestión y Desempeño Institucional	Acta No.	Fecha

CONTENIDO

ÍNDICE DE ILUSTRACIONES

1. OBJETIVO GENERAL

Presentar el Plan de Tratamiento para los riesgos de seguridad y privacidad de la información, identificados en los procesos incluidos en el alcance del SGSI del Instituto Departamental de Salud de Nariño, en adelante IDSN.

2. OBJETIVOS ESPECÍFICOS

- Identificar los riesgos asociados a los procesos que hacen parte del alcance del SGSI
- Calcular el nivel de riesgo
- Establecer el plan de tratamiento de riesgos
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos

3. MARCO LEGAL

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

4. MARCO TEÓRICO

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto el IDSN. Es recomendable contar con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla. El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la metodología emitida por el

Instituto Departamental de Salud de Nariño, en su versión vigente.
A continuación, se presenta las actividades generales para la implementación del Plan:

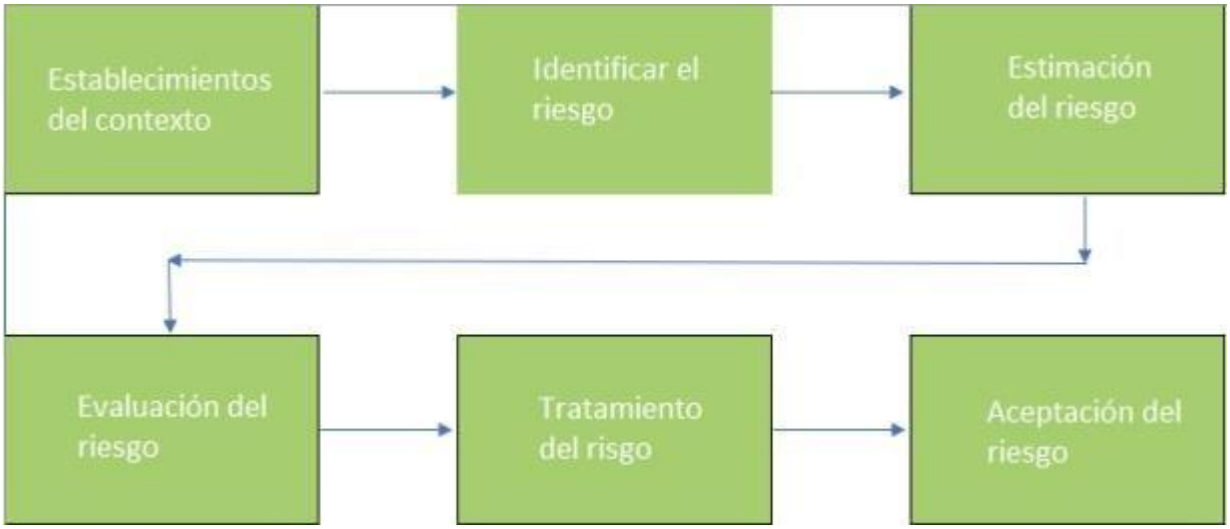

Ilustración 1. Estructura general de la metodología de riesgos

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

Ilustración 2. Ciclo PHVA y la gestión de riesgos

5. ACTIVIDADES

El Plan de Tratamiento de riesgos de seguridad y privacidad de la información está

compuesto por los siguientes Hitos o actividades:

5.1 PROGRAMACIÓN Y AGENDAMIENTO DE ENTREVISTAS

En esta fase se seleccionan los procesos incluidos en el alcance del SGSI del IDSN y se procede a programar y a agendar a los líderes de proceso para la identificación de riesgos.

5.2 ENTREVISTA CON LOS LÍDERES DE PROCESO

Se entrevista a cada líder de proceso, se explica la metodología y en conjunto se procede a realizar la identificación de los riesgos, los cuales se consignan en la Matriz de Riesgos.

5.3 IDENTIFICACIÓN Y CALIFICACIÓN DE RIESGOS

En esta fase, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.

5.4 VALORACIÓN DEL RIESGO RESIDUAL

En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

5.5 MAPAS DE CALOR DONDE SE UBICAN LOS RIESGOS

Luego se procede a ubicar los riesgos en un mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

5.6 PLAN DE TRATAMIENTO DE RIESGOS

Cada líder de proceso debe aprobar e implementar el plan de tratamiento de riesgos propuesto.

5.7 SEGUIMIENTO Y CONTROL

El seguimiento y control se realiza de acuerdo a la **GUÍA PARA LA ADMINISTRACIÓN DE RIESGO.**

6. CRONOGRAMA

HITOS	1	2	3	4	5	6	7	8	9	10	11	12
5.1 PROGRAMACION Y AGEN DAMIENTO DE ENTREVISTAS.												
5.2 ENTREVISTA CON LOS LIDERES DE PROCESO.												
5.3 IDENTIFICACION Y CALIFICACION DE RIESGOS.												
5.4 VALORACION DEL RIESGO RESIDUAL.												
5.5 MAPAS DE CALOR DONDE SE UBICAN LOS RIESGOS.												
5.6 PLANES DE TRATAMIENTO DE RIESGOS.												
5.7 SEGUIMIENTO Y CONTROL.												

7. GLOSARIO

Activo: Cualquier elemento que tenga valor para la organizacion.

Análisis del riesgo: Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.

Causa: Elemento específico que origina el evento.

Contexto externo: Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).

Contexto interno1: Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).

Controles: Procesos, políticas y/o actividades que pueden modificar el riesgo.

Criterios de riesgos2: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.

Evaluación del Riesgo: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.

Evento: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.

Fuente: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.

Gestión del riesgo3: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Identificación del riesgo4: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.

Riesgo aceptable: Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.

Riesgo residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento.

Riesgo: Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de sus objetivos.