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

REFORESTADORA INTEGRAL DE ANTIOQUIA RIA S.A. 2023

Tabla de contenido

1. INTRODUCCIÓN

Nos encontramos ya en la 4° revolución industrial, en donde se reconoce el protagonismo de la información en sus procesos productivos, por tanto, la importancia de tener su información adecuadamente identificada y protegida, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

En la actualidad, el activo más importante de cualquier empresa después del talento humano es la información, es por ello, que es de vital importancia, velar por la seguridad y protección de este activo tan valioso, por o tanto hay que Gestionar eficazmente la seguridad de la información y riesgos de seguridad digital de los sistemas de información de la entidad, así como en los activos que participan en sus procesos y que se encuentran expuestos, permite garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de Seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del Sistema de Gestión de Seguridad de la Información y en concordancia a la normativa aplicable.

2. OBJETIVOS

General

Establecer las políticas, procedimientos y metodologías para identificar, analizar, valorar, monitorear, medir y controlar los riesgos de mayor probabilidad de ocurrencia, con el fin de proteger los activos de información, el manejo de medios, control de acceso y gestión de usuarios, que puedan afectar el cumplimiento de la misión y los objetivos de la Reforestadora Integral de Antioquia.

Específicos

- Consolidar una administración de riesgos acorde con las necesidades de la Entidad.
- Proteger los activos de información de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad.
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.
- Establecer el plan de tratamiento de riesgos.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos.

3. MARCO NORMATIVO

NORMA	DESCRIPCION
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Informacióny las Comunicaciones.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de lapolítica de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitadospor tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales
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.
Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4	Riesgos de Gestión, Corrupción y Seguridad DigitalFunción Pública octubre 2018

4. PROCESO DE RIESGOS DE SEGURIDAD DE LAINFORMACION

Modelo de gestión de riesgos de seguridad de la información diseñado bajo la norma ISO/IEC 31000 como en la ISO 27005 para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:

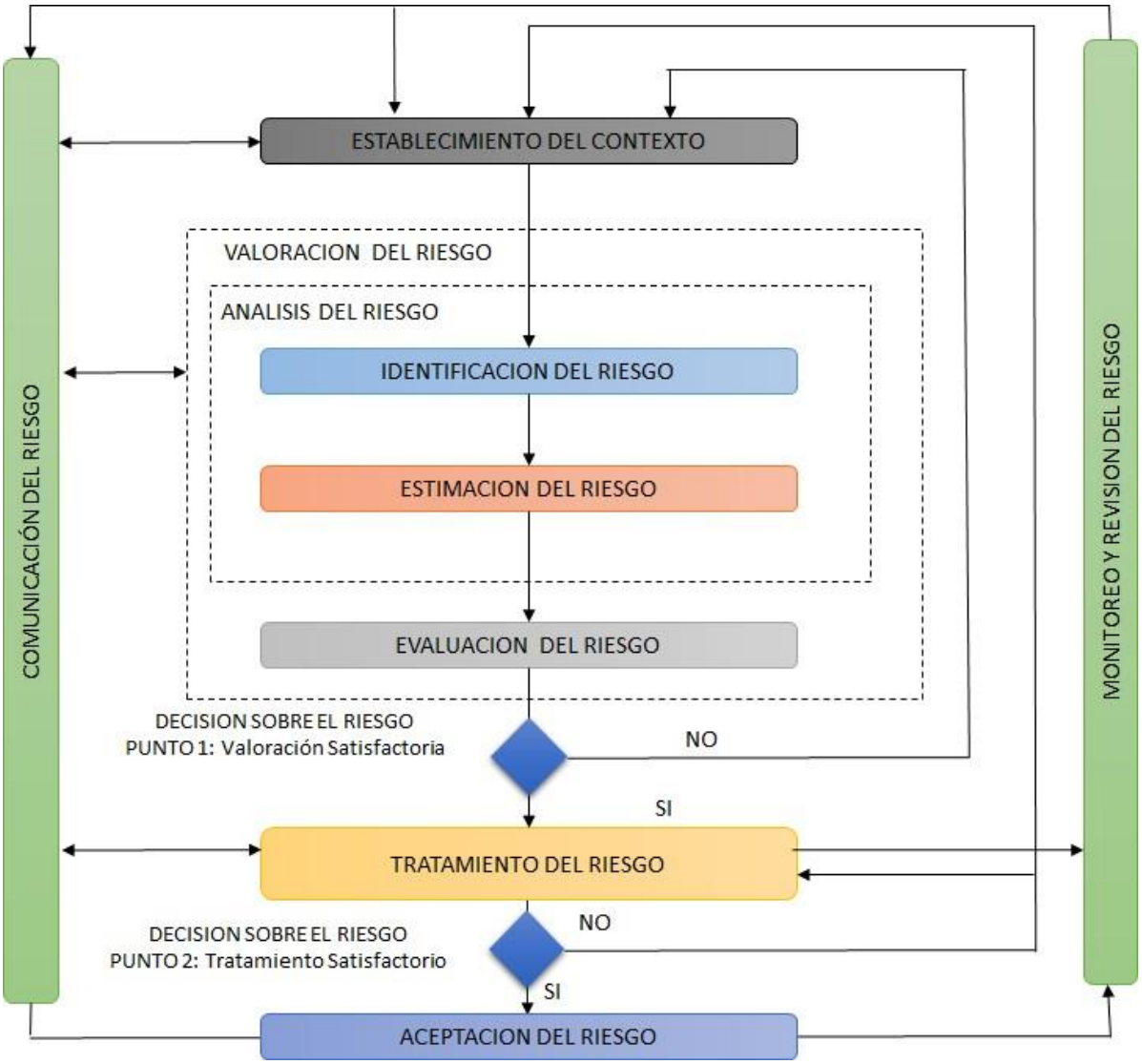

Imagen 1: VISION PROCESO DE RIESGOS DE SEGURIDAD

Tomado de la norma ISO/IEC 27005

Se debe identificar y gestionar muchas actividades, por lo que se considera como proceso a cualquier actividad queconsume recursos y que, además, su gestión promueva la transformación de entradas ensalidas. El enfoque basado en procesos consiste en que la organización identifique las actividades del funcionamiento de esta y la interacción entre las actividades; así, para la gestión de la Seguridad de la Información se hace énfasis en la importancia de la Norma ISO 27001:2013.

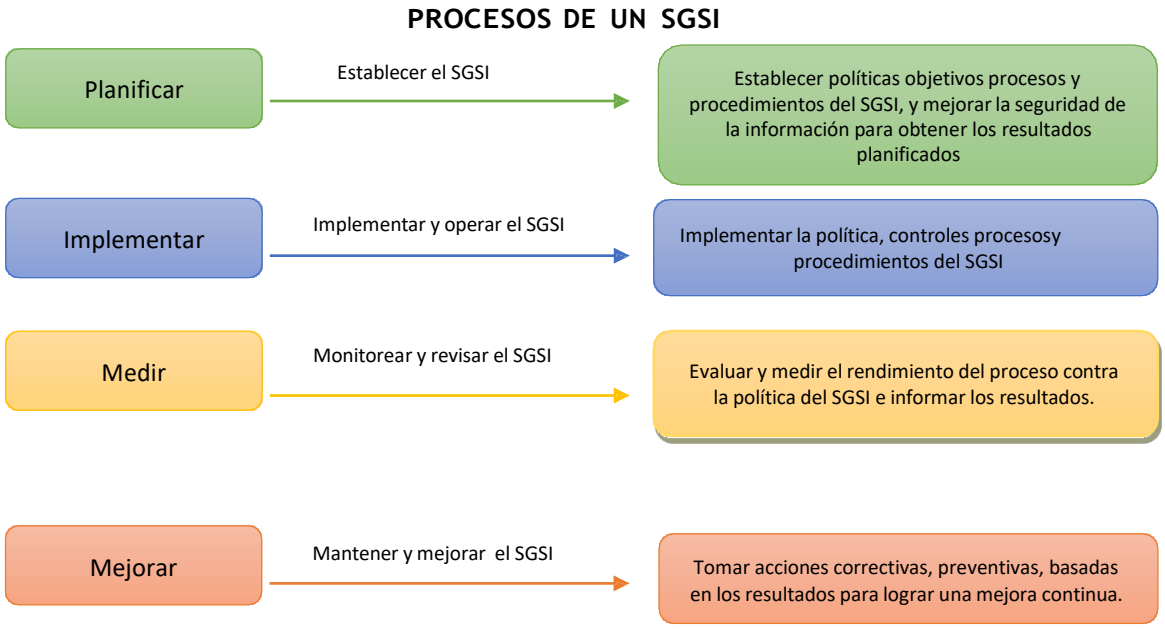

Imagen 2: enfoque basado en procesos

5. RECONOCER LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Se pretende detectar los riesgos de seguridad de la información y establecer el grado de riesgo al que está expuesto la entidad en la seguridad de la información y establecer los pasos a seguir:

6. CRITERIOS DE EVALUACION DE RIESGOS DE SEGURIDAD

La evaluación de los riesgos de seguridad de la información se enfocará en:

- Lo crítico que sean los activos de información involucrados en el proceso.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la Reforestadora Integral de Antioquia.

7. Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
  - Pérdida delnegocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación

- Incumplimiento de los requisitos legales, reglamentarios o contractuales

8. VALORACION DE LOS RIESGOS

Antes de realizar una valoración de riesgos de seguridad de la información se determinan los de activos de información de los procesos, a través de un inventario de los mismos y el cual será base para la valoración de los riesgos de seguridad de la información.

Se deben identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la entidad, esta fase consta delas siguientes etapas:

1.1.1 Programación y Agendamiento de Entrevistas

En esta fase se seleccionan los procesos incluidos en el alcance del SGSI de la entidad y se procede a programar y a agendar a los directivos de las dependencias y grupos internos de trabajo que conforman los procesos, para la identificación de riesgos.

1.1.2 Entrevista con los Directivos

Se define con cada directivo cual será la metodología y se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se establecen en la Matriz de Riesgos.

1.1.3 Identificación y Calificación de Riesgos

En esta etapa el área de sistemas evalúa los controles existentes o si no los hay comenzarlos a implementar para calcular el nivel de riesgo.

1.1.4 Valoración del Riesgo Residual

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

1.1.5 Mapas De Calor Donde Se Ubican Los Riesgos

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

9. CRONOGRAMA

Fase	Actividades	Responsable	Fecha Inicio	Fecha Final
Fase 1 Identificación y valoración de Activos	Identificación de Activos de Información. Clasificación de Activos de Información. Valoración de Activos de Información.	Área Sistemas	Febrero 2023	Abril 2023
Fase 2 Identificación deAmenazas y Vulnerabilidades	Identificación de Amenazas y Vulnerabilidades.	Área Sistemas	Mayo 2023	Mayo 2023
Fase 3 Determinació nde Riesgos	Determinación del Impactos de lasamenazas por activo Determinación de **Probabilidad** de Ocurrencia por	Área Sistemas	Junio 2023	Junio 2023
Fase 4 Análisis de Riesgos	Cálculo de Riesgos Identificación de Riesgos superiores al NRA	Área Sistemas	Julio 2023	Julio 2023
Fase 5 Gestión de Riesgos	Determinación de ControlesTratamiento de Riesgos Diseño de controles Priorización de Controles	Área Sistemas	Agosto 2023	Septiembre 2023
Fase 6 Planificación de controles	Implementación de Controles que no requieren recursos. Planificación de Controles	Área Sistemasy áreas responsables	Octubre 2023	Noviembre 2023
Fase 7 Monitoreo	Medición de la eficacia de los controles	Equipo Sistemas y áreas responsables	Diciembre 2023	N/A