

**Plan de Tratamiento para los riesgos de seguridad y privacidad de la información
2020**

EMPRESA FÉRREA REGIONAL

1. OBJETIVO

Presentar el Plan de Tratamiento para los riesgos de seguridad y privacidad de la información, de la Empresa Férrea Regional

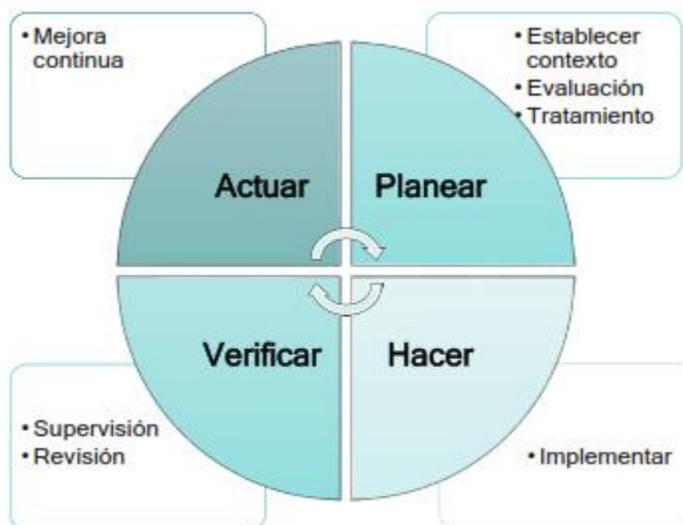
2. OBJETIVOS ESPECÍFICOS

- 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 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 la Empresa Férrea Regional. Las técnicas tradicionales están encaminadas a 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.

La gestión del riesgo dentro de la seguridad de la información se enmarca dentro del ciclo de planear, hacer, verificar y actuar



4. ACTIVIDADES

El Plan de Tratamiento de riesgos de seguridad y privacidad de la información está compuesto por los siguientes Hitos o actividades:

4.1 PROGRAMACIÓN Y AGENDAMIENTO DE ENTREVISTAS

En esta fase se procede a programar y a agendar a los líderes de proceso para la identificación de riesgos.

4.2 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.

4.3 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.

4.4 VALORACIÓN DEL RIESGO RESIDUAL

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

4.5 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.

4.6 PLAN DE TRATAMIENTO DE RIESGOS

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

4.7 SEGUIMIENTO Y CONTROL

El seguimiento y control se realiza de acuerdo a la programación prevista

5. CRONOGRAMA VIGENCIA

| HITOS | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|--|---|---|---|---|---|---|---|---|---|----|----|----|
| PROGRAMACIÓN Y AGENDAMIENTO DE ENTREVISTAS | | ■ | ■ | | | | | | | | | |
| ENTREVISTA CON LOS LÍDERES DE PROCESO | | | | ■ | ■ | | | | | | | |
| IDENTIFICACIÓN Y CALIFICACIÓN DE RIESGOS | | | | | ■ | | | | | | | |
| VALORACIÓN DEL RIESGO RESIDUAL | | | | | ■ | ■ | | | | | | |
| MAPAS DE CALOR DONDE SE UBICAN LOS RIESGOS | | | | | ■ | ■ | | | | | | |
| PLAN DE TRATAMIENTO DE RIESGOS | | | | | | | ■ | ■ | | | | |
| SEGUIMIENTO Y CONTROL | | | | | | | | ■ | ■ | ■ | ■ | ■ |

