PLAN DE SEGURIDAD Y PRIVACIDAD EN LA INFORMACIÓN

2020

EMPRESA FÉRREA REGIONAL

1. INTRODUCCIÓN

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la Política de Gobierno Digital. Forma parte del componente de Seguridad y Privacidad de la Información, acorde con las mejores prácticas de seguridad y estándares internacionales.

En el ámbito del propósito de la Empresa Férrea Regional S.A.S., en el cual, la gestión de la seguridad propone ser concebidas en el marco de la gestión de la organización determinado por las necesidades, objetivos, los requisitos de seguridad planteados por la estrategia de gobierno.

2. OBJETIVOS

Establecer las acciones estratégicas, encaminadas a fortalecer la seguridad y privacidad de la información de la Empresa Férrea Regional S.A.S, mediante la planeación de actividades para la mejora continua de la de seguridad de la información las cuáles serán gestionadas por los servidores públicos o contratistas de la EFR.

2.1. OBJETIVOS ESPECÍFICOS

1. Definir los elementos normativos sobre los temas de protección de la información.

2. Gestionar los riesgos de seguridad y privacidad de la información, de manera integral

3. Mitigar los incidentes de Seguridad y Privacidad de la Información.

4. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad de la información de la EFR.

5. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.

6. Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información.

2.2. ALCANCE DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

Aplica a toda la Empresa Férrea Regional y sus involucrados, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y compartan, utilicen, recolecten, procesen, intercambien o consulten su información, y todas las personas relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación. Así mismo, esta lo dispuesto en este documento y su implementación.

2.3. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD EN LA INFORMACIÓN

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualización de metodología e instrumento de levantamiento de activos de información	área de informática
		Validar activos de información en el instrumento levantado en la vigencia anterior	área de informática
		Identificar nuevos activos de información en cada dependencia	área de informática
	Reporte Datos Personales	Reportar al área encargada información recolectada en el instrumento de activos de información, correspondiente a bases de datos	área de informática
		Revisar y actualizar el procedimiento para la planificación y control operacional.	área de informática
		Implementar o fortalecer los controles de seguridad.	área de informática
Gestión de Riesgos	Sensibilización	Realizar la Implementación del plan de tratamiento de riesgos.	área de informática
		Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información.	área de informática

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE
Gestión de Incidentes de Seguridad de la Información	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	área de informática