Unidad del Servicio de Empleo

UNIDAD ADMINISTRATIVA ESPECIAL DEL SERVICIO PÚBLICO DE EMPLEO

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

El empleo es de todos

Mintrabajo

Unidad del Servicio Público de Empleo
Cra 69 No. 25B – 44 piso 7 Bogotá D.C.
PBX: (57 1) 7560009
www.serviciodeempleo.gov.co

Nombre del documento	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	
Estado del documento:	Versión liberada	
Responsables:	Nombre	Empresa
	Secretaria General Subdirección de Desarrollo y Tecnología	Unidad del Servicio Público de Empleo

Control de Versiones del Documento

Versión	Creación	Liberación	Descripción Cambio
1.0	Diciembre 2018	Enero 2019	Versión inicial
2.0	Octubre 2019		
3.0	Enero 2020	Enero 2020	Actualización

Unidad del Servicio Público de Empleo
Cra 69 No. 25B – 44 piso 7 Bogotá D.C.
PBX: (57 1) 7560009
www.serviciodeempleo.gov.co

Unidad del Servicio de Empleo

Contenido

Unidad del Servicio Público de Empleo
Cra 69 No. 25B – 44 piso 7 Bogotá D.C.
PBX: (57 1) 7560009
www.serviciodeempleo.gov.co

1. OBJETIVOS

1.1 Objetivo General

Establecer las políticas y procedimientos para ser usados sobre los sistemas de información en el caso de una contingencia, procurando proteger y asegurar la funcionalidad de los activos de la Unidad del SPE.

1.2 Objetivos específicos.

- Gestionar un plan que permita controlar y minimizar los riesgos de seguridad y privacidad de la información, relacionados a los procesos TIC existentes, de tal manera que se definan y apliquen los controles con los cuales se busca mitigar los riesgos de seguridad de la información en La Unidad del SPE.
- Formular e implementar controles y acciones encaminadas a prevenir y administrar los riesgos.
- Establecer a través de una adecuada administración del riesgo base confiable para la toma de decisiones y planificación de la Entidad.
- Asegurar la capacidad de supervivencia de La Unidad del SPE ante eventos que atenten con la existencia de la información vital.
- Proteger y conservar los activos de cómputo e información de la empresa, de riesgos, desastres naturales o actos mal intencionados.
- Reducir la probabilidad de las pérdidas a un mínimo de nivel aceptable, a un costo razonable y asegurar la adecuada recuperación.
- Asegurar que existan controles adecuados para reducir el riesgo por fallas o mal funcionamiento tanto del equipo, como del software, de los datos y de los medios de almacenamiento.
- Comunicar a todo el personal activo de La Entidad (funcionarios y contratistas) los pasos a seguir en caso de cualquier riesgo.

2. ALCANCE

El presente documento, proporciona la metodología establecida por la Entidad para la administración y gestión de los riesgos a nivel de procesos de seguridad y privacidad de la información; además, orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

3. PLAN DE TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE INFORMACIÓN

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información –SGSI, La Unidad del SPE busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

Así pues, se garantiza el tratamiento de los riesgos de seguridad de la información y la gestión de riesgo positivo u oportunidad, acorde con lo establecido en el Lineamiento de Administración de Riesgos.

El plan de tratamiento de riesgos y privacidad de la información es el instrumento de gestión para el buen manejo de las Tecnologías de la Información y las Comunicaciones. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la institución. Así mismo, este plan de tratamiento de riesgo y privacidad de la información sigue el conocido ciclo de vida iterativo "plan-do-check-act", es decir, "planifica-actúa-comprueba-corrige". Surge de un análisis de riesgos, donde entre otras amenazas se identifican aquellas que afectan a la continuidad de la operación de La Entidad.

El plan de tratamiento de riesgos y privacidad de la información deberá ser revisado anualmente, o antes si se materializa una amenaza.

4. ACTIVIDADES QUE DESARROLLAR SOBRE RIESGOS DE SEGURIDAD DE LA INFORMACION

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
Definir el marco de seguridad y privacidad de la información.	Definir las acciones a implementar a nivel de seguridad y privacidad y de mitigación del riesgo de Seguridad de la Información.	Secretaria General Subdirección de Desarrollo y Tecnología
Ejecutar el plan de Seguridad y privacidad de la Información. Aplicar y mejorar la seguridad y privacidad de la información.	Ejecutar el cronograma de Seguridad y privacidad de la Información.	Secretaria General Subdirección de Desarrollo y Tecnología
Aplicar y mejorar la seguridad y privacidad de la información	Análisis, seguimiento y evaluación del desempleo de las actividades relacionadas con la seguridad y privacidad de la información, realizando correctivos necesarios de ser requeridos.	Secretaria General Subdirección de Desarrollo y Tecnología

5. ACTIVIDADES QUE DESARROLLAR SOBRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO	DESCRIPCIÓN DEL RIESGO
Gestión de información	Afectación de la información por ataques cibernéticos. Falta de acceso a la información que permita dar continuidad a los procesos de la entidad. Información inadecuada en el sistema de gestión de información Falta de un plan de contingencias para preservar la información Hurto de documentación. Daño de activos documentales durante la administración, custodia y conservación en el Archivo Central. Fuentes de datos no confiables. Incumplimiento de los criterios de capacidad, disponibilidad, continuidad, seguridad de los servicios tecnológicos.

6. MARCO LEGAL

Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.

Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

7. REQUISITOS TÉCNICOS

Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información. MINTIC.

Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018