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

VIGENCIA 2024

WALTER DE JESUS CUARTAS VASQUEZ
Director General (E)
Escuela Contra la Drogadicción

TABLA DE CONTENIDO

INTRODUCCIÓN

En Colombia se viene adelantando la implementación de la política de gobierno digital, tal como lo establece La Presidencia de la Republica y el Ministerio de Tecnologías de la Información y las Comunicaciones a través del Decreto 767 de 2022, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2,libro 2, como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual se ha articulado con el Modelo Integrado de Planeación y Gestión, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otraspolíticas esenciales para la gestión pública en Colombia.

El Manual de la política de Gobierno Digital expedido por el MinTIC establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Según el manual, la implementación de la política de gobierno digital se ha definido en dos componentes: TIC para el estado y TIC para la sociedad, que son habilitados por cuatro elementos transversales: Arquitectura, Cultura y Apropiación, Seguridad y Privacidad de la Información y Servicios Ciudadanos Digitales. Estos seis elementos, se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

El manual en mención, precisa que el habilitador de Seguridad y Privacidad de la Información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, tramites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El documento denominado Modelo de Seguridad y Privacidad de la Información (MSPI), expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción de este, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos

La adopción e implementación del Modelo de Seguridad y Privacidad de la información en las

entidades públicas toma como sustento el estándar NTC ISO 27001:2013, así como principios regulatorios definidos por el Gobierno Nacional, tal como la Ley 1712 de 2014 o la Ley 1581 de 2012; así mismo, apoyan su enfoque en la implementación de un ciclo de identificación, valoración tratamiento de riesgos de seguridad y privacidad de la información, para lo cual se ha expedido desde el Departamento Administrativo de la Función Pública la guía para la administración del riesgo y el diseño de controles en entidades públicas, como referente para abordar los riesgos de gestión, corrupción y de seguridad de la información. La adopción de prácticas de gestión de riesgos en las entidades públicas permitirá fortalecer la toma de decisiones en cuanto a la implementación de controles de acuerdo con el plan de tratamientos definido. Estos referentes constituyen el fundamento para la definición del plan de tratamiento de riesgos de seguridad y privacidad de la información de la Escuela Contra La Drogadicción - ECD sobre activos de información que aportan al logro de los objetivos organizacionales.

1. MARCO LEGAL

Ley 909 de 2004: "Por la cual se expiden normas que regulan el empleo público, la carrera administrativa, gerencia pública y se dictan otras disposiciones".

Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales".

Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

Decreto Ministerial 1078 de 2015: "Por medio del cual se expide el Decreto ÚnicoReglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Decreto Presidencial 1083 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticasde Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

Decreto Presidencial 612 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 Presidencial 767 de 2022: "Por el cual se establecen los lineamientos generales de la Política 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".

Resolución Ministerial 00500 de 2021: "Por la cual se establecen los lineamientosy estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital".

ISO/IEC 27001:2013: Tecnología de la información-Técnicas de seguridad – Sistemas de Gestión de la Seguridad de la Información (SGSI) – Requisitos

2. OBJETIVOS

Establecer un marco de acción para aportar al tratamiento de riesgos de seguridad y privacidad de la información, sobre los activos de información que soportan el cumplimiento de los objetivos organizacionales, conducentes a preservar la confidencialidad, integridad y disponibilidad de la

información institucional, en atención al contexto organizacional de la entidad, las capacidades y recursos disponibles, para fortalecer la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

La planeación se enfocará en fortalecer la implementación de acciones para el tratamiento de riesgos de seguridad y privacidad de la información de acuerdo a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Función Pública, enfocados a la seguridad de los activos de información de la Escuela Contra La Drogadicción, como un aporte a las actividades que realizará la entidad en torno a la Seguridad y Privacidad dela Información institucional, teniendo en cuenta las capacidades y recursos disponibles, para mejorar la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

3. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIAD DE ACTIVOS DE INFORMACION POR CATEGORIAS

Según lo expuesto en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo dela Función Pública, el tratamiento de riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, por lo tantodicha planeación en este caso en particular, hace alusión al tratamiento de riesgos de Seguridad y Privacidad de la Información enfocado en la seguridad de la información sobre los activos de información a cargo de la Escuela Contra La Drogadicción, para lo cual se realizan un conjunto de actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados. En atención a lo anterior, a continuación,se describen las actividades más relevantes orientadas al tratamiento de riesgosde Seguridad y Privacidad de la Información.

El desarrollo de las actividades para lograr su consecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al apetito de riesgo institucional y a las orientaciones de la alta dirección, en cuanto al apetito de riesgo institucionales que han adoptadopara afrontar el desarrollo y cumplimiento de las actividades planificadas.

Para el desarrollo de las actividades, la Escuela Contra La Drogadicción contará con un equipo humano dispuesto para adelantar actividades de sensibilización, capacitación y atención de inquietudes de las áreas a través de cronogramas definidos.

La ECD ha establecido unos tiempos en los cuales sebrindará y apoyará el seguimiento al desarrollo de los planes de seguridad y privacidad de la información que las dependencias presenten y así tratar las actividades pertinentes a los procesos relacionados al diligenciamiento de los planes de seguridad y privacidad de la información

4. CRONOGRAMA

Actividad	Responsable	E	F	M	A	M	J	J	A	S	O	N	D
Actualizar el inventario de activos de información de la Institución conforme al modelo del MINTIC o del **Conglomerado Público** disponibles, y según sea adecuado a las condiciones de la ECD	Ingeniero												
Caracterizar las amenazas y vulnerabilidades Según el modelo seleccionado (del MINTIC o del **Conglomerado Público**)	Ingeniero												
Realizar la Adquisición e implementación decontroles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada Dependencia.	Todas las áreas de la Escuela		X	X	X	X	X	X	X	X	X	X	X
Realizar los procesos requeridos para el seguimiento a la operación de los controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia.	Todas las áreas de la Escuela		X	X	X	X	X	X	X	X	X	X	X
Realizar el seguimiento a las actividades de identificación y operación de controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada área.	Área de sistemas			X			X			X			X

Elaboró: Cristian Zuluaga	Revisó: Gerardo Vanegas Jaramillo	Aprobó: Luis Fernando Otalvaro
Firma:	Firma:	Firma:
Cargo: Profesional apoyo.	Cargo: Subdirector A y F	Cargo:

WALTER CUARTAS VASQUEZ
Director General (E)
Escuela Contra La Drogadicción
Presidente Comité de Gestión y Desempeño