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

PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

BOGOTÁ
Enero de 2024

CONTROL DE CAMBIOS

VERSION	FECHA	DESCRIPCIÓN DEL CAMBIO
1	Enero /2023	Elaboración del documento “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información”.
2	Enero /2024	Ajuste Plan de trabajo – Cambio de vigencia

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece las actividades requeridas para la gestión de los riesgos de seguridad y privacidad de la información, en función de la implementación de controles que permitan a la entidad disminuir la probabilidad y el impacto de materialización de este tipo de riesgos, con el fin de preservar la seguridad e integridad de los activos de información de la Entidad.

En este sentido, acorde con lo establecido en el Modelo de Seguridad y Privacidad de la Información – MSPI, en la Guía No. 7 – Guía de Gestión de Riesgos y Guía No. 8 – Controles de Seguridad y Privacidad de la Información, en el presente Plan se estipulan directrices, fechas de ejecución y responsables para lograr un adecuado proceso de administración y evaluación de los riesgos de seguridad y privacidad de la información.

2. OBJETIVO

Establecer los lineamientos para la adopción de medidas y acciones encaminadas a modificar, reducir o eliminar riesgos a los que están expuestos los activos de información que soportan la prestación de servicios de TI de Computadores para Educar de acuerdo con lo establecido en el Modelo de Privacidad y Seguridad de la Información – MSPI, la Guía No. 7 – Guía de Gestión de Riesgos y la Guía No. 8 – Controles de Seguridad y Privacidad de la Información.

3. ALCANCE

Los requisitos, lineamientos y acciones establecidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información son aplicables de forma anualizada a los procesos estratégicos, misionales, de apoyo y de control y evaluación, por lo cual deberán ser conocidos y cumplidos por todos los Colaboradores, contratistas y terceras partes vinculadas a la Entidad que accedan a los activos de información, sistemas de información e instalaciones físicas de la Entidad.

4. GENERALIDADES DEL PLAN

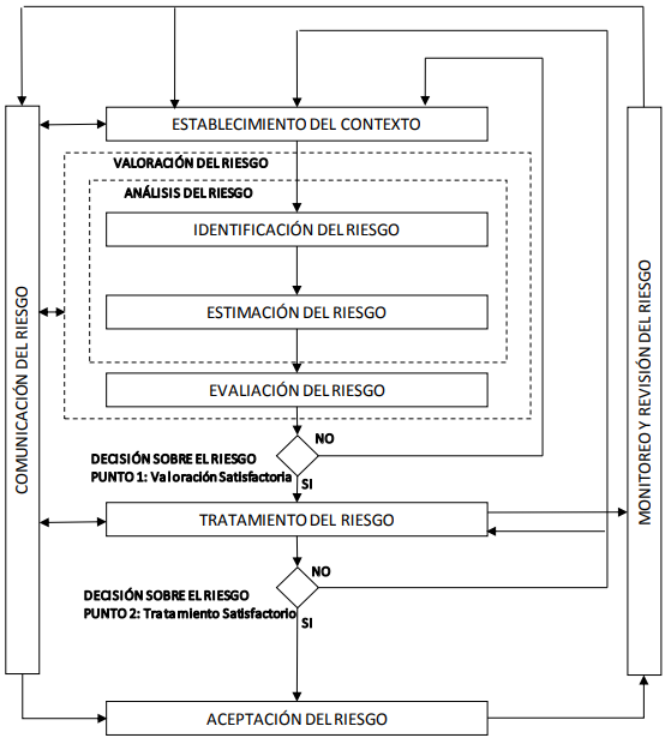
4.1 Desarrollo metodológico

Este plan en particular hace alusión al tratamiento de riesgos de seguridad y privacidad de la información enfocado en la seguridad informática sobre los activos de tecnologías de información frente a ciberamenazas.

El plan de tratamiento de riesgos de seguridad y privacidad de la información de Computadores para Educar, relaciona actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados para el tratamiento de los riesgos tomando como referencia metodológica lo establecido en la Guía No. 7 – Guía de Gestión de Riesgos del MinTIC, alineado con el manual de riesgos y oportunidades de la entidad y la guía de administración del riesgo del DAFP.

A continuación, se describe el proceso general para la gestión del riesgo:

- Proceso para la administración del riesgo en seguridad de la información



Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

La administración de riesgos de seguridad y privacidad de la información propone una gestión iterativa en cuanto a las actividades de valoración del impacto y el tratamiento de los riesgos identificados.

Establecimiento del alcance, contexto y criterios

El establecimiento del contexto permite relacionar los aspectos externos e internos que impactan que se deben tener en cuenta para gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad de Computadores para Educar. A partir del contexto es posible establecer las posibles causas de los riesgos a identificar. De esta forma para la definición del contexto se seguirá la metodología dispuesta por la entidad que inicia con la revisión del análisis de matriz FODA realizado por la entidad en la vigencia para posteriormente realizar un análisis mas detallado basado en los activos de cada proceso y en la transversalidad de las actividades que ejecutan.

Identificación del riesgo

Mediante la identificación y formalización de un inventario de activos de información, COMPUTADORES PARA EDUCAR reconoce cuáles son los activos de información críticos para la entidad siguiendo los lineamientos establecidos en la Guía para el Inventario de Activos (GTI-005-G), de igual forma es necesario considerar otros aspectos como la plataforma tecnológica, sistemas de información, locaciones y en general cualquier aspecto que se pueda identificar en el que la explotación de una vulnerabilidad pudiera poner en riesgo los activos de información de la entidad .

Evaluación de Riesgos

La evaluación de riesgos pretende priorizar los riesgos identificados de acuerdo con el nivel de criticidad obtenido, evaluando y determinando la probabilidad, el impacto y controles existentes de acuerdo con las vulnerabilidades y amenazas identificadas. Esta evaluación se realiza acorde a la metodología para la administración de riesgos emitida por el Departamento Administrativo de la Función Pública (DAFP) y que se adoptó por computadores para Educar en el manual de riesgos y oportunidades.

Tratamiento de riesgos

Teniendo en cuenta el nivel inherente del riesgo se determinarán las siguientes opciones de tratamiento:

• **Aceptar el riesgo:** no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo.

• **Evitar el riesgo:** se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca. Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.

• **Reducir el riesgo:** se adoptan medidas para reducir la probabilidad o el impacto del riesgo o ambos, esto conlleva a la implementación de controles. El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

• **Compartir el riesgo:** Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. En este caso, no es posible transferir la responsabilidad del riesgo.

5. PLAN DE TRABAJO

El plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se actualiza y aprueba anualmente, el seguimiento se realiza conforme a lo definido en el plan de trabajo que se muestra a continuación el cual se ejecuta en las sedes de Computadores para Educar.

Gestión de Riesgos			
Revisar y actualizar los lineamientos de riesgos de seguridad de la información	02/2024	06/2024	Equipo SGSI, Subdirección TI y Oficina asesora de planeación
Socializar manual de riesgos de seguridad de la información	04/2024	05/2024	Equipo SGSI
Identificar y Analizar Riesgos Seguridad de la información	04/2024	05/2024	Subdirección TI, Oficina Asesora de Planeación
Consolidar matriz de riesgos de seguridad de la Información	05/2024	06/2024	Equipo SGSI, Oficina asesora de planeación
Definir el plan de Tratamiento de riesgos	05/2024	06/2024	Equipo SGSI, Oficina asesora de planeación
Aceptar y aprobar matriz de riesgos	06/2024	07/2024	Comité de Gestión y desempeño
Realizar seguimiento, monitoreo de los riesgos identificados	01/2024	12/2024	Subdirección de TI, Oficina Asesora de Planeación

Actualizar y socializar los procedimientos de seguridad cuando se requiera	01/2024	12/2024	Equipo SGSI y Subdirección de TI

6. SEGUIMIENTO Y MEDICIÓN

Se realizará monitoreo periódico de los activos, vulnerabilidades, probabilidades, impactos y amenazas, validando que las acciones que se están llevando a cabo y evaluando la eficiencia en su implementación. La medición se realiza principalmente mediante el porcentaje de ejecución de actividades definidas en el tratamiento de riesgos de seguridad de la información identificados.