Plan de acción de Tratamiento de Riesgos de Seguridad Digital de la Política de Seguridad Digital

Oficina de Riesgos

Fecha de elaboración: 01 diciembre 2022

Versión 1

MINISTERIO DE EDUCACIÓN NACIONAL

Contenido

1. Introducción

El ICETEX en busca de la mejora continua implementa un método que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos de seguridad digital asociados al manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma. La Entidad en su operación utiliza permanentemente tecnología en captura, procesamiento y reporte de información tanto interna como externamente para comunicarse con las diferentes partes interesadas, lo cual implica que la Entidad sea vulnerable a ataques mal intencionados o mala manipulación de la información, lo que puede acarrear problemas económicos, legales, administrativos y de continuidad, por lo cual este documento busca establecer un línea de trabajo que permita a la Entidad sortear los riesgos que lo rodean y lograr que su información este segura.

En atención a lo anterior y siguiendo los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG, se establece el Plan de acción de Tratamiento de Riesgos de Seguridad Digital del ICETEX para la vigencia 2023, donde se define la estrategia de la gestión de riesgos de seguridad digital, incorporando la revisión de los controles de la norma ISO27001 y medidas de seguridad de la información que estén acordes al entorno operativo de la Entidad, a través de metodologías que prevengan la afectación de cualquier activo de información en cuanto a confidencialidad, integridad, disponibilidad y privacidad, cumpliendo con los requisitos normativos, los documentos del Sistema de Gestión de Seguridad Digital y del Programa Integral de Protección de Datos Personales y las propuestas a oportunidades de mejoras identificadas en la gestión del año 2022.

Este documento se encuentra articulado con el Plan de acción de seguridad y privacidad de la información, el Plan estratégico de tecnología de la información y comunicación (PETIC) y se desarrolla de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones.

2. Descripción

Nombre del Plan de Acción	Plan de acción de Tratamiento de Riesgos de seguridad Digital
Nombre y código rubro presupuestal	312001020
Presupuesto asignado ($)	$137.642.076
Área responsable	Oficina de Riesgos
Política MIPG y otros	8. Seguridad digital
Proceso	Gestión de Riesgos No Financieros
Fecha inicio del proyecto	02/01/2023
Fecha fin del proyecto	29/12/2023

3. Objetivo Estratégico

Fortalecer los procesos, la tecnología, la cultura y el gobierno corporativo para atender las necesidades de los usuarios y los lineamientos de las políticas públicas

4. Objetivo General

Este plan establece una guía para el control y minimización de los de los riesgos de seguridad digital y así proteger la privacidad de la información y los datos tanto de los procesos como de las personas vinculadas con la información de la Entidad.

4.1 Objetivos Específicos

- Lograr un diagnóstico real de la situación actual de la institución en materia de riesgos de seguridad digital.
- Optimización de los recursos de la institución en la aplicación del Plan de acción de Tratamiento de Riesgos de Seguridad Digital.
- Asegurar la gestión de riesgos de seguridad digital en todos los procesos y proyectos de la Entidad.

5. Alcance

El plan de acción de tratamiento de riesgos de seguridad digital aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

6. Justificación

Para definir las actividades del presente plan se analizó la situación actual vs la deseada, buscando en todo momento una alineación con la normativa de seguridad y privacidad de la información. A continuación, se ilustra el análisis para la definición del plan de acción de tratamiento de riesgos de seguridad digital para el año 2023:

Situación actual

Dentro de las revisiones a algunos controles específicos de la norma ISO27001 se ha identificado necesidades de fortalecer la efectividad y diseño de éstos, toda vez que no garantizan la debida protección a la información, siendo necesario continuar generando verificaciones a todo el Sistema de Gestión de Seguridad Digital y se logren medidas mitigantes de riesgo a la información.

Dentro del análisis de diagnóstico al Programa Integral de Datos Personales que se emitió en el año 2022, se consideraron varias acciones encaminadas a fortalecer la gestión de riesgos para garantizar la debida confidencialidad de los datos personales de nuestros beneficiarios, deudores solidarios, becarios, funcionarios, contratistas, entre otros, que es necesario continuar y fortalecer en el año 2023.

Situación deseada

El Sistema de Gestión de Seguridad Digital como proceso transversal pretende apoyar el logro de las metas institucionales, aportando desde la perspectiva de seguridad de la información en todos los procesos y proyectos en los que se encamine la Entidad.

Contar con controles que aseguren la debida confidencialidad, integridad, disponibilidad y privacidad de la información, para lo cual se verificarán los controles de la norma ISO27001 en los procesos, identificado su diseño y efectividad. De igual manera se debe asegurar el cierre de brechas en la implementación de controles, encontradas en las auditorías y revisiones internas.

Se espera contar con un esquema robusto de monitoreo y respuesta a incidentes de seguridad digital que permita responder adecuadamente y minimizar el impacto en la Entidad.

Adicionalmente, es importante implementar controles para proteger la privacidad de la información en todas las dependencias, acorde con el programa integral de protección de datos personales.

7. Cronograma de actividades

Teniendo en cuenta que el Modelo Integrado de Planeación y Gestión (MIPG) así como el cumplimiento de los requisitos normativos que incluyen los riesgos que puedan afectar a cualquier activo de información en cuanto a confidencialidad, integridad, disponibilidad y privacidad, en el presente plan se incorporan las actividades de monitoreo de riesgos de seguridad digital, la revisión de controles buscando identificar su grado de diseño y efectividad, la gestión de incidentes de seguridad digital desde la prevención hasta su corrección, en concordancia con el Sistema de Gestión de Seguridad Digital y el Programa Integral de Protección de Datos Personales. El Plan de acción de Tratamiento de Riesgos para el año 2023, está conformado por las siguientes actividades:

N°	Categoría / Actividad / Tarea	Fecha Inicio	Fecha Fin
1.	**Contratación del personal**	**02/01/2023**	**30/01/2023**
1.1.	Elaboración de Estudio y del pliego de condiciones	02/01/2023	30/01/2023
1.2	Perfeccionamiento del contrato	02/01/2023	30/01/2023
2.	**Cronograma**	**01/02/2023**	**28/02/2023**
2.1.	Elaboración estructura desglose de trabajo del equipo de seguridad	09/01/2023	13/01/2023
3.	**Monitoreo de riesgos por proceso**	**13/02/2023**	**30/11/2023**
3.1.	Desarrollo de monitoreo de riesgos	13/02/2023	30/11/2023
3.2.	Elaboración de planes de tratamiento de riesgos que no cumplen con el nivel de tolerancia	13/02/2023	30/11/2023
3.3.	Seguimiento de plan de acción de controles que requieren mejora	13/02/2023	30/11/2023
3.4	Revisión de resultado de plan de acción de controles que requieren mejora	13/02/2023	30/11/2023
3.5	Cierre de plan de acción de controles que requieren mejora	**13/02/2023**	30/11/2023
3.6	Elaboración de declaración de aplicabilidad	**13/02/2023**	30/11/2023
4	**Gestión de incidentes**	**02/01/2023**	**29/12/2023**
4.1.	Identificación de eventos de riesgos e incidentes	02/01/2023	29/12/2023
4.2.	Gestión de eventos e incidentes de riesgos de seguridad digital	02/01/2023	29/12/2023
4.3.	Seguimiento de plan de acción de incidentes	02/01/2023	29/12/2023
4.4.	Cierre de plan de acción de incidentes	02/01/2023	29/12/2023
5.	**Revisión de controles de normas**	**13/02/2023**	**30/11/2023**
5.1.	Revisión del diseño y eficacia de los controles de la ISO 27001 correspondiente a 14 dominios y 114 controles	13/02/2023	30/11/2023
5.2.	Socialización de resultados de revisión de controles en su diseño y eficacia de la ISO 27001 correspondiente a 14 dominios y 114 controles	13/02/2023	30/11/2023
5.3	Emisión de plan de acción de controles que requieren mejora	13/02/2023	30/11/2023
5.4.	Seguimiento de plan de acción de controles que requieren mejora	13/02/2023	30/11/2023
5.5.	Revisión de resultado de plan de acción de controles que requieren mejora	13/02/2023	30/11/2023
5.6	Cierre de plan de acción de controles que requieren mejora	13/02/2023	30/11/2023

8. Hitos

Nº	Hito o producto esperado	Fecha Entrega
1.1.	Pliego de condiciones de prestación de servicios	30/01/2023
1.2	Contrato de prestación de servicios	30/01/2023
2.1.	Cronograma de trabajo	13/01/2023
3.1.	Acta de monitoreo de riesgos de cada proceso de acuerdo con los nuevos controles de la norma ISO 27001.	30/11/2023
3.2.	Planes de tratamiento de riesgos que no cumplen con el nivel de tolerancia	30/11/2023
3.3.	Acta de seguimiento de plan de acción de controles que requieren mejora	30/11/2023
3.4	Plan de acción de controles cerrado sobre riesgos que requieren mejora	30/11/2023
3.5	Plan de acción con el cierre mejoras de controles	30/11/2023
3.6	Declaración de aplicabilidad de acuerdo con el esquema de controles de la norma ISO27001.	30/11/2023
4.1.	Documento que evidencia el evento de riesgos e incidentes	29/12/2023
4.2.	Reporte de eventos e incidentes de riesgos de seguridad digital	29/12/2023
4.3.	Plan de acción de incidentes	29/12/2023
4.4.	Plan de acción de incidentes cerrado en el sistema de gestión de riesgos	29/12/2023
5.1.	Informe de revisión de control	30/11/2023
5.2.	Informe revisión de controles en su diseño y eficacia de la ISO 27001 correspondiente a 14 dominios y 114 controles	30/11/2023
5.3	Plan de acción de controles que requieren mejora	30/11/2023
5.4.	Acta de Seguimiento de plan de acción de controles que requieren mejora	30/11/2023
5.6	Plan de acción cerrado de controles que requieren mejora en el sistema de gestión de riesgos	30/11/2023

9. Seguimiento y evaluación

Con el fin de garantizar un seguimiento y evaluación al plan de acción, se establece el siguiente indicador:

Identificación del grado de diseño y efectividad de controles de seguridad digital = No. controles revisados /No. controles planeados de revisión

Seguimiento a planes de acción: Planes de acción gestionados / Planes de acción abiertos

Gestión de incidentes de seguridad = No. incidentes gestionados /No. Incidentes identificados

10. Anexos

Marco normativo que aplica al Plan de acción de Tratamiento de Riesgos de Seguridad Digital del ICETEX

Las siguientes son las referencias normativas aplicables a la seguridad digital de la Entidad:

- Ley 1581 de 2012– Protección de Datos Personales.
- Ley 1712 de 2014– Transparencia y Derecho de Acceso a la Información Pública.
- Ley 2088 de 2021. Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".
- Decreto 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 2106 de 2019, establece la disposición de una estrategia de seguridad digital acorde con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones- MInTic.
- Decreto 1377 de 2013 (Compilado en el Decreto 1081 de 2015), por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 103 de 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y el acceso a la información pública.
- Decreto 886 de 2014, Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
- Decreto 1008 de 2018 – Política de Gobierno Digital (MinTIC).
- Decreto 338 de 2022, contiene lineamientos generales para fortalecer la gobernanza de la seguridad digital.
- Superintendencia Financiera de Colombia:
  - ✓ Circular Básica Jurídica 029 de 2014 Parte 1, Título II, Capítulo I – Canales, medios, seguridad y calidad en el manejo de información de prestación de servicios financieros,
  - ✓ Circular Básica Jurídica 029 de 2014 Parte 1, Título IV, Capítulo V – Requerimientos mínimos para la gestión del riesgo de ciberseguridad
  - ✓ Circular Básica Jurídica 029 de 2014 Parte 1, Título I, Capítulo VI – Reglas relativas al uso de servicios de computación en la nube.

- ✓ Circular Externa 033 de 2020. Instrucciones relacionadas con la Taxonomía Única de Incidentes Cibernéticos – TUIC, el formato para el reporte de métricas de seguridad de la información y ciberseguridad y el protocolo de etiquetado para el intercambio de información Traffic Light Protocol (TLP).

- MINTIC: Modelo de Seguridad y Privacidad Digital (MSPI) de la Estrategia de Gobierno Digital.
- NTC-ISO-IEC 27001 – norma técnica colombiana – Sistema de Gestión de Seguridad de la Información.
- Modelo Integrado de Planeación y Gestión – Dimensión Seguridad Digital.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital
- CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital.
- Directiva presidencial 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Directiva presidencial 02 de 2022. Lineamientos para el uso de servicios en la nube, actualización de catálogos de servicios, sistemas de información, bases de datos, activos de información, infraestructura; Implementar una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos, conformación de un equipo o Grupo de Seguridad Digital.
- Resolución 500 de 2021. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
- Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”.
- Resolución 460 de 2022 “Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación”.