Plan de acción de Seguridad y Privacidad de la Información de la Política de Seguridad Digital

Oficina de Riesgos

Fecha de elaboración: 01 diciembre 2022

Versión 1

MINISTERIO DE EDUCACIÓN NACIONAL

Tabla de Contenido

1. Introducción

El ICETEX identifica la información como uno de los activos más importantes y críticos para el desarrollo de sus funciones, en la gestión de los procesos continuamente se está procesando, gestionando, almacenando, custodiando, transfiriendo e intercambiando información valiosa que no debe ser divulgada a personal no autorizado, suceso que puede poner en riesgo la gestión pública. La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos institucionales, así como para mantener el cumplimiento normativo aplicable a la Entidad, además traslada confianza a las partes interesadas.

En atención a lo anterior y siguiendo los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG, se establece el Plan de acción de Seguridad y Privacidad de la Información del ICETEX para la vigencia 2023, que define la hoja de ruta de la estrategia de seguridad digital para gestionar y proteger la información suministrada a la Entidad y generada por la misma de las diferentes amenazas que pueden afectar la integridad, disponibilidad, confidencialidad y privacidad de la información; mediante la planeación de actividades para la mejora continua del Sistema de Gestión de Seguridad Digital – SGSD 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 Tratamiento de Riesgos de Seguridad Digital y 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 Seguridad y Privacidad de la información
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

Definir las actividades y roles necesarios para implementar el Modelo de Seguridad y Privacidad de la Información para el año 2023, siguiendo la metodología sugerida por el MINTIC - Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, el Departamento Administrativo de Función Pública, con el fin de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información.

4.1 Objetivos Específicos

- Planificar el desarrollo y seguimiento de las actividades que conforman el Sistema de Gestión de Seguridad digital.
- Desarrollar y mantener el Programa Integral de Protección de Datos Personales.
- Implementar las oportunidades de mejora identificadas al Sistema de Gestión de Seguridad Digital.

5. Alcance

El Plan de acción de Seguridad y Privacidad de la Información contempla las actividades requeridas por la normativa en la materia, la atención a las necesidades de las áreas en temas de seguridad y privacidad de acuerdo con nuestro Modelo de Seguridad y Privacidad, la Políticas de Seguridad Digital y de Protección de Datos Personales y el Programa Integral de Protección de Datos Personales.

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 Seguridad y Privacidad de la Información 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 estos, 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 cubrir la reglamentación colombiana en la materia y garantizar la debida confidencialidad de los datos personales de nuestros beneficiarios, deudores solidarios, becarios, funcionarios, contratistas, entre otros.

Respecto a los resultados del FURAG del año 2021, se obtuvo un puntaje de 97,8% para la Política de Seguridad Digital, encontrando que para la vigencia 2023 es necesario la mejora continua en adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la Entidad tales en implementar la guía para la identificación de infraestructura crítica cibernética.

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 digital en todos los procesos y proyectos en los que se encamine la Entidad.

Como segundo aspecto, procura dar estricto cumplimiento a las políticas y procedimientos de seguridad digital, bajo un enfoque de sensibilización y concienciación de todas las partes interesadas, destacando el compromiso de la alta dirección con las estrategias de seguridad de la información.

En tercer lugar, 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. También se deben cerrar las brechas en la implementación de controles, encontradas en las auditorías y revisiones internas. Adicionalmente, es importante implementar controles para proteger la privacidad de la información en todas las dependencias, según el Programa Integral de Protección de Datos Personales.

7. Cronograma de actividades

A continuación, se relacionan el cronograma de actividades del Plan de Acción de Seguridad y Privacidad de la Información para el año 2023:

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.	**Planes estratégicos**	**01/02/2023**	**28/02/2023**
2.1.	Plan estratégico	01/02/2023	28/02/2023
2.2.	Plan de capacitación y comunicación	01/02/2023	28/02/2023
2.3.	Elaboración estructura desglose de trabajo del equipo de seguridad	09/01/2023	13/01/2023
3.	**Capacitación y sensibilización de seguridad de la información y protección de datos personales**	**01/03/2023**	**15/12/2023**
3.1.	Capacitación funcionarios, contratistas, proveedores y beneficiarios	15/02/2023	15/12/2023
3.2.	Sensibilización a funcionarios y contratistas	15/02/2023	15/12/2023
3.3	Pruebas de ingeniería social	01/07/2023	15/12/2023
4	**Conceptos de seguridad y de datos personales**	**02/01/2023**	**29/12/2023**
4.1.	Revisión de acuerdos estratégicos y contratos	02/01/2023	29/12/2023
4.2.	Conceptos específicos requeridos por las áreas	02/01/2023	29/12/2023
5.	**Actualizar y consolidación del inventario activos de información de la entidad**	**01/03/2023**	**15/12/2023**
5.1.	Actualizar inventario de activos de información de la entidad	15/02/2023	15/12/2023
5.2.	Generar y publicar documentos de instrumentos de gestión	01/0112023	15/12/2023
6.	**Desarrollar comité de seguridad de la información**	**01/04/2023**	**15/12/2023**
6.1.	Elaborar informe de comité de seguridad de la información	01/04/2023	15/12/2023
6.2.	Realizar comité de seguridad de la información	01/04/2023	15/12/2023
7.	**Revisión y actualización de políticas, procedimientos del sistema de gestión de seguridad digital**	**01/03/2023**	**15/12/2023**
7.1.	Revisión y actualización de políticas de seguridad digital y protección de datos personales	15/02/2023	15/12/2023
7.2.	Revisión y actualización de procedimientos del sistema de gestión de seguridad digital	15/02/2023	15/12/2023
8.	**Seguimiento a indicadores del Modelo de Seguridad y Privacidad**	**01/03/2023**	**15/12/2023**
8.1.	Reportar los resultados los indicadores del Modelo de Seguridad y Privacidad	01/03/2023	15/12/2023
9.	**Revisión y seguimiento de cumplimiento de políticas de seguridad de la información de los principales proveedores**	**01/03/2023**	**15/12/2023**
9.1.	Revisión y seguimiento de cumplimiento de políticas de proveedores	15/02/2023	15/12/2023
10.	**Revisión y seguimiento de cumplimiento de normativa**	**01/03/2023**	**15/12/2023**
10.1.	Revisión de cumplimiento de ISO27001, SFC, Ley 1581	01/03/2023	30/06/2023
10.2	Seguimiento de cumplimiento de ISO27001, SFC, Ley 1581	01/07/2023	15/12/2023
11.	**Análisis de Vulnerabilidades**		
11.1.	Contratación empresa prestadora de servicio de Ethical Hacking	01/03/2023	31/03/2023
11.2.	Elaboración de pruebas de vulnerabilidades	03/04/2023	31/10/2023
11.3	Seguimiento a planes de remediación	03/04/2023	31/10/2023
11.4	Re-test y Resultados de re-test	01/11/2023	17/11/2023
12.	**Registro de bases de datos personales**	06/02/2023	31/03/2023
12.1	Recolección de bases de datos de las áreas	06/02/2023	31/03/2023
12.2	Actualización de bases de datos personales ante la SIC	06/02/2023	31/03/2023
13.	**Atención de auditoria al SGSD**	**01/03/2023**	**15/12/2023**
13.1	Establecer planes de acción a hallazgos identificados	01/03/2023	15/12/2023
13.2	Desarrollo de planes de acción a hallazgos identificados	01/03/2023	15/12/2023
14.	**Aprobación en Junta Directiva**	**08/07/2023**	**15/12/2023**
14.1.	Presentación en Junta Directiva semestral	08/07/2023	29/12/2023
14.2.	Firma y publicación de acuerdo de junta	29/07/2023	29/12/2023

8. Hitos

Nº	Hito o producto esperado	Fecha Entrega
1.1.	Estudio y del pliego de condiciones	30/01/2023
1.2	Contrato de prestación de servicios	30/01/2023
2.1.	Plan estratégico	28/02/2023
2.2.	Plan de capacitación y comunicación	28/02/2023
2.3.	Cronograma de trabajo	13/01/2023
3.1.	Resultados de Capacitación funcionarios y contratistas, y documento divulgado de capacitación a proveedores y beneficiarios	15/12/2023
3.2.	Piezas de Sensibilización a funcionarios y contratistas	15/12/2023
3.3.	Informe de resultado de ingeniería social	15/12/2023
4.1.	Matriz de riesgos de acuerdos estratégicos y contratos	29/12/2023
4.2.	Conceptos específicos requeridos por las áreas	29/12/2023
5.1.	Inventario de activos de información de la entidad	15/12/2023
5.2.	Instrumentos de gestión	15/12/2023
6.1.	Informe del comité de seguridad de la información	15/12/2023
6.2.	Acta del comité de seguridad de la información	15/12/2023
7.1.	Actualización de políticas de seguridad digital y protección de datos personales.	15/12/2023
7.2.	Procedimientos nuevos o actualizados del sistema de gestión de seguridad digital	15/12/2023
8.1.	Informe de indicadores del Modelo de Seguridad y Privacidad	15/12/2023
9.1.	Informe de cumplimiento de políticas de proveedores	15/12/2023
10.1.	Autodiagnóstico de cumplimiento normativo	30/06/2023
10.2.	Resultado de seguimiento de cumplimiento normativo	30/06/2023
11.1	Contrato de servicio de Ethical Hacking	31/03/2023
11.2	Informe de pruebas de vulnerabilidades	31/10/2023
11.3	Acta de seguimiento a planes de remediación	31/10/2023
11.4	Resultados de re-test	17/11/2023
12.1	Inventario de bases de datos de las áreas	31/03/2023
12.2	Evidencia de actualización de bases de datos personales ante la SIC	31/03/2023
13.1	Planes de acción propuestos a hallazgos identificados	15/12/2023
13.2	Evidencia de planes de acción gestionados	15/12/2023
14.1.	Presentación en Junta Directiva semestral	29/12/2023
14.2.	Acuerdo de junta directiva	29/12/2023

9. Seguimiento y evaluación

Con el fin de garantizar un seguimiento y evaluación al plan de acción, se establece los siguientes indicadores:

% Cumplimiento Plan de Acción = Nº Actividades Ejecutadas / Nº Actividades Planificadas

Pruebas de Ethical Hacking= No. Vulnerabilidades con seguimiento /No. Vulnerabilidades identificadas

Concienciación en Seguridad Digital = (Número de personas capacitadas / Número total de personas) *100

10. Anexos

Marco normativo que aplica al Plan de acción de Seguridad Privacidad de la Información 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".