



Plan de Seguridad y Privacidad de la Información – 2023

Dirección de Tecnología e Información



Contenido

Introducción	3
Objetivos	4
Objetivo General	4
Objetivos específicos	4
Definiciones	5
Generalidades	7
Alcance del Documento	7
Marco Normativo	7
Desarrollo del Plan de Seguridad y Privacidad de la Información	9
Metodología de implementación	9
Mapa de Ruta	10

Introducción

El Instituto Colombiano para la Evaluación de la Educación – Icfes, Empresa estatal de carácter social del sector Educación Nacional, que se enfoca en ofrecer el servicio de evaluación de la educación en todos sus niveles y adelantar investigaciones sobre factores que inciden en la calidad educativa, con la finalidad de brindar información para el mejoramiento y la toma de decisiones en la calidad de la educación, propone el siguiente Plan de Seguridad y Privacidad de la Información para la vigencia 2023.

Siendo consiente que la seguridad de la información debe ser un componente crítico y fundamental dentro de la estrategia de institucional de las entidades a nivel nacional, por ello el Instituto Colombiano para la Evaluación de la Educación - Icfes, presenta a los grupos de interés y a la ciudadanía el presente plan donde reconoce su importancia para el sector educación y ha identificado la información como uno de los activos más importantes y críticos para el desarrollo de sus funciones.

El Plan de Seguridad y Privacidad de la Información se elaboró teniendo en cuenta los lineamientos del Manual de Política de Gobierno Digital y del Modelo de Privacidad y Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones y cuenta con un conjunto de actividades basadas en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) para crear condiciones de uso confiable en el entorno digital y físico de la información, mediante un enfoque basado en la identificación de activos, la gestión de riesgos, el establecimiento de controles para mitigar las posibles afectaciones a los activos y la gestión de la continuidad tecnológica que apoyan la evaluación de la educación en todos sus niveles y las investigaciones sobre factores que inciden en la calidad educativa del país.

Este plan se define teniendo en cuenta el contexto, las necesidades de la organización, las buenas prácticas y la normatividad vigente como: la NTC (Norma Técnica Colombiana) ISO 27001:2013, ISO 27701:2020, ISO 22301:2019, lo establecido en el Decreto 1008 de 14 de junio 2018 *“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”*, la Resolución 1519 de 2022 *“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”* y la 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”* dentro del cual se establecen para las entidades del estado los Habilitadores Transversales: *Seguridad de la Información, Arquitectura de TI y Servicios Ciudadanos Digitales.*

Objetivos

Objetivo General

Definir las acciones para incrementar el nivel de madurez de seguridad y privacidad de la Información del Icfes, de acuerdo con las estrategias de Gobierno Digital, MIPG, requerimientos de la entidad, disposiciones legales y buenas prácticas vigentes, tendientes a garantizar la integridad, confidencialidad, disponibilidad y privacidad de la información institucional.

Objetivos específicos

- Fortalecer y optimizar la gestión de seguridad y privacidad de la información al interior del Icfes, apoyando el cumplimiento de los objetivos estratégicos del Instituto.
- Gestionar los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación tecnológica que puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de la información.
- Identificar, clasificar y mantener actualizados los activos de información del Icfes.
- Reportar y gestionar los eventos e incidentes de seguridad de la información que afecten o puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de manera oportuna y pertinente reduciendo su impacto y propagación.
- Atender los requerimientos de seguridad de la información, seguridad digital y ciberseguridad establecidos por las diferentes entidades a nivel nacional y requisitos de legales.
- Fortalecer la cultura, el conocimiento y las habilidades de los colaboradores en los temas de seguridad y privacidad de la información en el Icfes.
- Desarrollar estrategias que permitan la continuidad de los servicios tecnológicos prestados por el Icfes, frente a situaciones adversas que impidan el normal funcionamiento y prestación de estos.

Definiciones

Activos de Información: Son los recursos necesarios para que una empresa o un negocio funcione y consiga los objetivos que se ha propuesto la alta dirección. (ISO 27001). En relación con la privacidad y seguridad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal (MSPI - MINTIC). Son, entre otros, las bases de datos, los archivos, los manuales, las aplicaciones, así como el hardware y software que se tiene el Instituto para desarrollar su objeto.

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del MSPI de una organización.

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Disponibilidad: propiedad de la información de ser accesible, utilizable y recuperable a demanda por una entidad.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO27001:2013 e ISO31000:2019.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Incidente de seguridad de la información: Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.

Integridad: propiedad de la información de ser completa, exacta e inalterada exactitud y completitud.

Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten ser protegidos de potenciales riesgos.



ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable.

MSPI: Modelo de Seguridad y Privacidad de la Información propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los componentes de la Política de Gobierno Digital.

Plan de continuidad del negocio (BCP): Orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos: Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles para proteger la misma.

Política de seguridad de información: Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.

Riesgo de seguridad y privacidad: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de probabilidad y consecuencias.

Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI): Parte del sistema de gestión general del Instituto, basada en un enfoque hacia los riesgos globales del negocio, cuyos fines son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad y privacidad de la información.

Generalidades

Alcance del Documento

El presente Plan de Seguridad y Privacidad de la Información aplica a todos los procesos definidos en el Instituto Colombiano para la Evaluación de la Educación – Icfes, donde haya recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, para el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

Marco Normativo

Ley 1324 de 2009 “Por la cual se fijan parámetros y criterios para organizar el sistema de evaluación de resultados de la calidad de la educación, se dictan normas para el fomento de una cultura de la evaluación, en procura de facilitar la inspección y vigilancia del Estado y se transforma el ICFES”.

Ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre 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”.

CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano.

Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.

Guía para la administración del riesgo y el diseño de controles en entidades públicas. RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL año 2020.

CONPES 3995 de 2020 - Política Nacional De Confianza y Seguridad Digital



Resolución interna 255 de 2020 “Por la cual se adoptan las Políticas de Tratamiento de la Información de Datos Personales del Instituto Colombiano para la Evaluación de la Educación - Icfes y se dictan otras disposiciones”.

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 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 interna 666 de 2021 “Por la cual se actualiza el Registro de Activos de Información, el Índice de Información Clasificada y Reservada y el Esquema de Publicación de Información del Icfes para la vigencia de 2021.”.

Resolución interna 485 de 2022 “Por la cual se actualiza la Política y el Manual de Políticas de Seguridad y Privacidad de la Información del Sistema de Gestión de Seguridad de la Información – SGSI del Instituto Colombiano para la Evaluación de la Educación – Icfes y se deroga la Resolución 000391 del 12 de agosto de 2020”.

Resolución interna 486 de 2022 “Por la cual se actualiza el Manual de Políticas de Tratamiento de la Información de Datos Personales del Instituto Colombiano para la Evaluación de la Educación – Icfes y se deroga la Resolución 000278 del 22 de abril de 2016”.

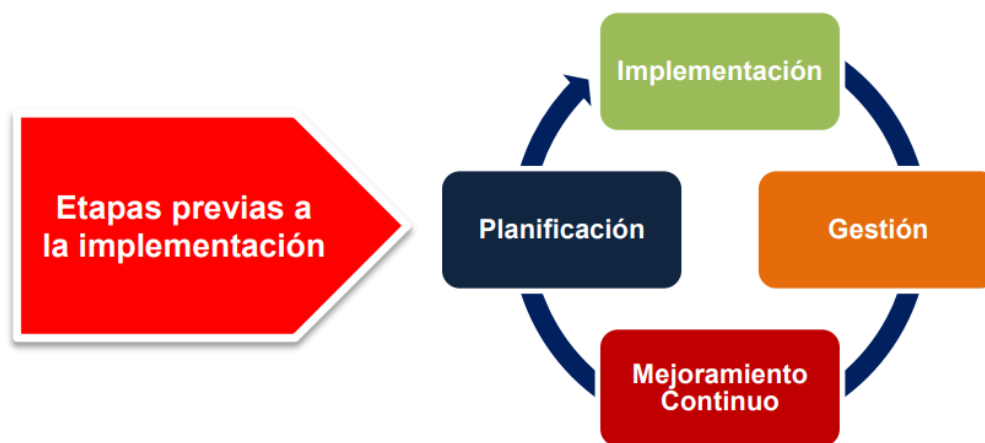
Norma Técnica Colombiana ISO27001

Norma Técnica Colombiana ISO31000

Desarrollo del Plan de Seguridad y Privacidad de la Información

Metodología de implementación

La metodología de implementación del Plan de Seguridad y Privacidad para el Instituto Colombiano para la Evaluación de la Educación – Icfes, está basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y lo establecido en el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC y se ejecuta a través del mapa de ruta definido a continuación:





Mapa de Ruta

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
1. Activos de información					
1.1	Actualización de la información de los Instrumentos de gestión de la información pública	Junio	Agosto	Todos los procesos Icfes – acompañan Equipo Seguridad de la Información	Matrices de activos
1.2	Publicación Instrumentos de gestión de la información pública	Septiembre	Octubre	Oficina Asesora de Planeación y Equipo Seguridad de la Información	Registro de Activos de Información, Índice de Información Clasificada y Reservada y Esquema de Publicación en la página web y datos abiertos
1.3	Seguimiento y mejora de la implementación de las estrategias para el etiquetado de los activos de tipo información en medio físico, electrónico y en Sistemas de Información	Marzo	Diciembre	Subdirección de Abastecimiento y Servicios General, Dirección de Tecnología e Información, Subdirección de Desarrollo de Aplicaciones, Subdirección de Información y Equipo Seguridad de la Información	Informe de actividades realizadas
1.4	Definir lineamientos para la gestión y uso de los activos de información del instituto	Abril	Julio	Equipo Seguridad de la Información	Documentos, procedimientos guías aprobados en Daruma
1.5	Definir y socializar los lineamientos y controles sobre áreas seguras	Abril	Julio	Equipo Seguridad de la Información	Documentos, procedimientos guías aprobados en Daruma
2. Riesgos de Seguridad y Privacidad de la Información					
2.1	Identificación y Análisis de Riesgos Seguridad de la información	Junio	Agosto	Todas las áreas y acompañamiento de Equipo Seguridad de la Información	Matrices de riesgos
2.2	Definición del Tratamiento de Riesgos Seguridad de la Información	Junio	Agosto	Todas las áreas y acompañamiento de Equipo Seguridad de la Información	Plan de Tratamiento de Riesgos de Seguridad de la Información
2.3	Control y Seguimiento a la implementación de los planes de tratamiento	Enero	Diciembre	Oficina de Control Interno apoya Equipo de Seguridad	Informe de Auditoria de Riesgos
3. Concienciación y Sensibilización en Seguridad y Privacidad de la Información					
3.1	Definición del Plan de Concienciación en Seguridad y Privacidad	Enero	Febrero	Equipo Seguridad de la Información	Documento Plan de Concienciación en Seguridad y Privacidad



3.2	<i>Ejecución del Plan de Concienciación en Seguridad y Privacidad.</i>	<i>Febrero</i>	<i>Diciembre</i>	<i>Equipo Seguridad de la Información y acompañan Oficina Asesora de Comunicaciones y Mercadeo y Subdirección de Talento Humano</i>	<i>Informe de ejecución Plan de Concienciación en Seguridad y Privacidad</i>
3.3	<i>Entrenamientos y/o Sensibilizaciones en temas Seguridad y Privacidad de la información.</i>	<i>Febrero</i>	<i>Diciembre</i>	<i>Equipo Seguridad de la Información</i>	<i>Listado de asistencia, certificado participantes. Informe de las acciones realizadas.</i>
3.4	<i>Análisis de resultados del Plan de Concienciación en Seguridad y Privacidad.</i>	<i>Noviembre</i>	<i>Diciembre</i>	<i>Equipo Seguridad de la Información</i>	<i>Informe de resultados Plan de Concienciación en Seguridad y Privacidad</i>

4. Protección de Datos Personales

4.1	<i>Seguimiento a la implementación y cumplimiento del Manual de Protección de Datos Personales</i>	<i>Febrero</i>	<i>Diciembre</i>	<i>Oficina Asesora Jurídica y acompaña Equipo Seguridad de la Información</i>	<i>Informe de Seguimiento y Recomendaciones.</i>
4.2	<i>Actualización del Registro de Base de Datos en la SIC</i>	<i>Enero</i>	<i>Marzo</i>	<i>Equipo Seguridad de la Información acompaña Oficina Asesora Jurídica</i>	<i>Actualización del Registro en la SIC</i>

5. Sistema de Gestión de Seguridad y Privacidad de la Información

5.1	<i>Apoyo en la definición, actualización e implementación de los lineamientos y controles asociados a Seguridad y Privacidad de la Información</i>	<i>Enero</i>	<i>Diciembre</i>	<i>Equipo Seguridad de la Información</i>	<i>Documentos, procedimientos, guías, manuales, formatos, políticas.</i>
5.2	<i>Revisión de la implementación y cumplimiento de los controles de seguridad establecidos.</i>	<i>Junio</i>	<i>Diciembre</i>	<i>Equipo Seguridad de la Información</i>	<i>Herramienta de medición y autodiagnóstico del MSPI semestral</i>
5.3	<i>Identificar acciones de mejoramiento para fortalecer la implementación y cumplimiento de los controles de seguridad</i>	<i>Enero</i>	<i>Diciembre</i>	<i>Equipo Seguridad de la Información</i>	<i>Planes de Trabajo Cronogramas</i>
5.4	<i>Revisión por la Dirección</i>	<i>Marzo</i>	<i>Mayo</i>	<i>Oficina Asesora de Planeación y Equipo Seguridad de la Información</i>	<i>Acta de Revisión por la Dirección</i>
5.5	<i>Gestionar y apoyar la ejecución de la auditoria de certificación al Sistema de Gestión de Seguridad y Privacidad de la Información</i>	<i>Abril</i>	<i>Julio</i>	<i>Equipo Seguridad de la Información</i>	<i>Plan de auditoria</i>
5.6	<i>Definir y ejecutar los planes de mejoramiento de acuerdo con las auditorías realizadas</i>	<i>Febrero</i>	<i>Diciembre</i>	<i>Todos los procesos y acompaña Equipo Seguridad de la Información</i>	<i>Planes de Mejoramiento, evidencias de cierre</i>



5.7	Gestión y cierre oportuno de los incidentes y eventos de seguridad de la Información	Enero	Diciembre	Equipo Seguridad de la Información	Registro y documentación de las acciones sobre la gestión de los incidentes y/o eventos de seguridad presentados.
5.8	Reporte y Seguimiento al cumplimiento de los indicadores asociados al SGSPI	Enero	Diciembre	Equipo Seguridad de la Información	Informe semestral de medición de los indicadores internos del SGSPI.
5.9	Realizar ejercicios y simulaciones para fortalecer el reporte y gestión de incidentes de seguridad y privacidad de la información	Febrero	Diciembre	Equipo Seguridad de la Información	Informe de Resultados de las actividades realizadas.
5.10	Apoyar la integración del SGSPI al sistema de gestión de calidad del Instituto	Abril	Octubre	Oficina Asesora de Planeación y Equipo de Seguridad	Plan de Trabajo

6. Continuidad de TI – Continuidad del Negocio

6.1	Actualizar el análisis de impacto al negocio – BIA para los activos críticos de la DTI	Marzo	Mayo	DTI, SI y SDA	Documento de análisis de impacto al negocio – BIA
6.2	Actualización del Plan de Continuidad de TI	Abril	Junio	Equipo Seguridad de la Información – DTI	Plan de Continuidad de TI - DRP
6.3	Apoyo en la planeación y seguimiento de las pruebas definidas en el Plan de Continuidad de TI	Febrero	Diciembre	Equipo Seguridad de la Información – DTI - Subdirección de Información	Informe de resultados de las pruebas realizadas
6.4	Analizar los resultados de la aplicación de la estrategia de Continuidad de TI y gestionar las acciones de mejora identificadas con el fin de fortalecer los planes y documentación	Febrero	Diciembre	Equipo Seguridad de la Información – DTI	Informe de resultados de las pruebas realizadas

7. Seguridad Informática

7.1	Realizar análisis de vulnerabilidades y retest a los sistemas de información e infraestructura de TI	Junio	Octubre	Equipo Seguridad	Informes de los análisis de vulnerabilidades
7.2	Seguimiento a la remediación de las vulnerabilidades identificadas	Febrero	Diciembre	Equipo Seguridad	Informe de Seguimiento y Cierre de Vulnerabilidades.
7.3	Implementación y afinamiento de las herramientas de seguridad: DLP, Antivirus, Seguridad en Office, Firewall, WAF, SIEM.	Febrero	Diciembre	Equipo Seguridad – Dirección de Tecnología e Información	Herramientas productivas
7.4	Seguimiento periódico a las actividades reportadas por las	Enero	Diciembre	Equipo Seguridad – Dirección de Tecnología e Información	Reportes seguimiento herramientas (DLP,



	<i>herramientas de monitoreo de seguridad informática</i>				<i>Seguridad Office 365, WAF, Firewall, Antivirus, SIEM)</i>
--	---	--	--	--	--