



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Oficina Asesora de Planeación.



Contenido

Introducción.....	3
Objetivos.	4
Objetivo General.....	4
Objetivos Específicos.	4
Alcance.....	5
Definiciones.	6
Marco Normativo.....	7
Responsables.	8
Desarrollo del Plan.....	9
Fase Previa Diagnostico MSPI.....	9
Estado Actual.....	10
Fase de Planificación.....	10
Diagnóstico del MSPI.	10
Fase de Implementación.....	11
Fases de Gestión y Mejoramiento Continuo.....	11
Mapa de Ruta.....	12
Recursos	19
Medición.....	19
Control de Cambios	19



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 2026.

Siendo consiente que la seguridad y privacidad 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.

La articulación del Sistema Inteligente para la Gestión Organizacional (SIGO), abarca las estrategias de seguridad de la información dentro de su integralidad para la óptima operación del instituto como parte de la estrategia institucional, considerando la relevancia de cada componente en la organización.

El Plan de Seguridad y Privacidad de la Información tiene 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 y la gestión de riesgos para el establecimiento de controles que permitan mitigar las posibles afectaciones a los activos, y la gestión de la continuidad tecnológica para responder a los requerimientos del negocio.

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 y 2022, 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, la cual hace parte de la Política de Gobierno Digital reglamentada por el Decreto 1078 de 2015, indica que las entidades señaladas en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015 son sujetos obligados a cumplir con la Política de Gobierno Digital, y como tal, deben definir lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital y establecer los lineamientos y estándares para la estrategia de seguridad digital.

Objetivos.

Objetivo General.

Establecer y encaminar las actividades orientadas a fortalecer el tratamiento de la información que es generada, tratada y custodiada por la entidad; con el fin de elevar su nivel de confianza con sus grupos de interés, mediante la preservación de su confidencialidad, integridad y disponibilidad, así como también la adopción de las buenas prácticas, el cumplimiento de la política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información y el marco legal que le sea aplicable, alineado dentro del Sistema Inteligente para la Gestión Organizacional (SIGO).

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.
- Identificar, clasificar y mantener actualizados los activos de información del Icfes.
- 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.



- 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.
- Definir y divulgar a los colaboradores de la entidad, las políticas, documentación asociada y buenas prácticas que permitan consolidar una cultura institucional en torno a la seguridad de la Información.
- Realizar el seguimiento a las acciones que permitan reducir las brechas de cumplimiento de la Política de Gobierno Digital con el autodiagnóstico del Modelo Integrado de Planeación y Gestión (MIPG), frente a relacionado con el habilitador transversal de seguridad y privacidad de información.
- Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, gobierno digital y protección de datos personales.

Alcance.

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.



Definiciones.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001).

Activo de Información: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de la entidad. (CONPES 3854 de 20116).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27001).

Incidente de Seguridad de la Información: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (ISO/IEC27035, 2012).

Partes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de



actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

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”.
- CONPES 3701 de 2011 –Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- 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 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.
- CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano.
- 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
- Norma Técnica Colombiana ISO27701
- Norma Técnica Colombiana ISO22301

Responsables.

Todas las áreas y procesos de la entidad son responsables del cumplimiento de los lineamientos y actividades definidas en este plan.

La Oficina Asesora de Planeación como parte de la segunda línea de defensa y siendo la dependencia responsable de liderar el desarrollo e implementación del Sistema de Gestión se encargará de revisar y adecuar la metodología de administración de riesgos propuesta por el Instituto para la Evaluación de la Educación Superior ICFES.

El equipo de la Dirección de Tecnologías de Información será el encargado de brindar acompañamiento en el desarrollo e implementación del componente de Administración del Riesgo de Seguridad y Privacidad de la Información, este deberá recoger iniciativas, responsabilidades y armonizar los diferentes ejercicios para la implementación de un proceso más efectivo. El equipo de seguimiento y evaluación está conformado Seguridad de la Información de la Oficina Asesora de Planeación, quienes velarán por la adecuada elaboración e implementación del mapa de riesgos de cada proceso, promoviendo su apropiación, entendimiento y evaluación del mismo.

Desarrollo del Plan.

El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC definió el Modelo de Seguridad y Privacidad -MSPI el cual fue facilitado a las entidades del Estado colombiano con el fin de que estos lo adopten e incrementen el nivel de madurez en los temas de seguridad y privacidad de la información. De acuerdo con lo anterior, la metodología de implementación del Plan de Seguridad y Privacidad del Icfes, está basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y lo establecido en el MSPI y se ejecuta a través del mapa de ruta definido a continuación:

Ilustración 1. Modelo de Operación del MSPI - tomado de MinTIC



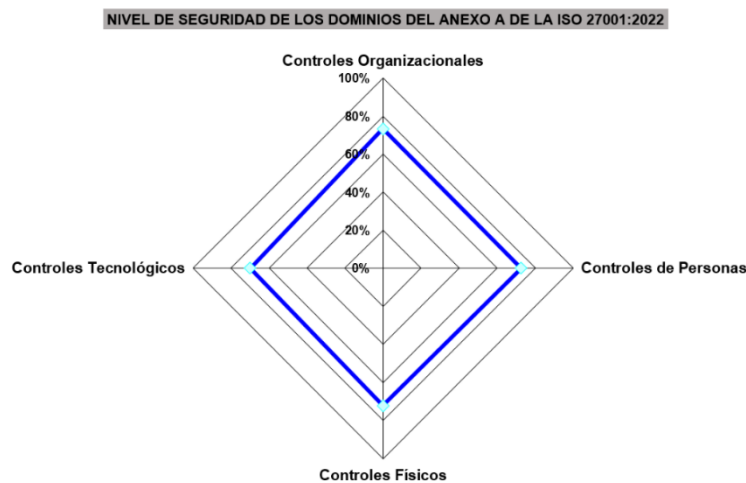
Fase Previa Diagnostico MSPI.

Esta fase permite por medio del uso de herramientas de diagnóstico, actividades de reconocimiento y valoración de controles de seguridad de la información, identificar cual es el estado actual de la Entidad en temas de seguridad y privacidad; el resultado de este de diagnóstico permitirá establecer el nivel de madurez en cuanto a seguridad y privacidad de la información, y así definir la hoja de ruta para las actividades en las siguientes fases del modelo.

Estado Actual.

Teniendo en cuenta la calificación de FURAG, el Icfes se encuentra en un puntaje de 92,3 en seguridad digital, esto se ve reflejado en el esfuerzo realizado por la entidad para apoyar la implementación del SGSPI y la alineación con el Sistema Inteligente para la Gestión Organizacional (SIGO), por lo que viene adelantando la actualización de las políticas y manual de políticas de seguridad y privacidad de la información, esto ha permitido revisar y avanzar en la identificación de los activos de información de la Entidad, de manera que a través del análisis de riesgo se pueda clasificar y aplicar controles que permitan mejorar el nivel de riesgo de estos activos.

Ilustración 2. Niveles de seguridad ISO 27001:2022



Fase de Planificación.

Esta fase está estrechamente relacionada con el resultado dado en la fase de diagnóstico y el estado actual del Icfes, esta fase permite la identificación de las acciones claves que van a definir y orientar las actividades para los propósitos de seguridad y privacidad.

Diagnóstico del MSPI.

El nivel de implementación del MSPI permitirá al Icfes establecer la estrategia a desarrollar para la vigencia 2026 para implementar y mejorar la seguridad y privacidad de la información, para los procesos misionales, estratégicos, de control y de apoyo de la Entidad y toda la infraestructura que los soporte.

A corte de noviembre de 2026, el avance general en el ciclo PHVA, de acuerdo con la medición del instrumento de identificación de la línea base de seguridad, proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones, se cuenta con un estado de implementación de la siguiente manera:



Evaluación de Efectividad de Controles Anexo A		
Ítem	Dominio	Evaluación de efectividad del control
A.5	Política de Seguridad de la Información	Optimizado
A.6	Organización de la Seguridad de la Información	Optimizado
A.7	Seguridad de los Recursos Humanos	Optimizado
A.8	Gestión de Activos	Optimizado
A.9	Control de Acceso	Optimizado
A.10	Criptografía	Gestionado
A.11	Seguridad Física y del Entorno	Optimizado
A.12	Seguridad de las Operaciones	Optimizado
A.13	Seguridad de las Comunicaciones	Optimizado
A.14	Adquisición, Desarrollo y Mantenimiento de Sistemas	Gestionado
A.15	Relaciones con los Proveedores	Gestionado
A.16	Gestión de Incidentes de Seguridad de la Información	Optimizado
A.17	Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio	Optimizado
A.18	Cumplimiento	Optimizado
Promedio de Evaluación de Controles		Optimizado

Fase de Implementación.

El Sistema de Gestión de Seguridad de la Información inicialmente se adoptó en 2017 y mediante las Resoluciones 000391 del 12 de agosto de 2020 y 00486 del 23 de agosto de 2022 basadas en la NTC-ISO-IEC 27001 se actualizó definiendo el conjunto de políticas, procedimientos, guías y formatos para proteger la confidencialidad, integridad, disponibilidad y privacidad de la información del Icfes.

Fases de Gestión y Mejoramiento Continuo.

Esta fase se lleva a cabo la implementación, medición y mejoramiento continuo de los requisitos base presentados el Modelo de Seguridad y privacidad de la información – MSPI y la norma ISO/IEC 27001 en su versión 2022; de la misma forma llegar a la implementación de los controles, que por normativa o por resultado de la identificación de riesgos deban ser implementados.

Estas actividades permiten que el Icfes cumpla con los requisitos normativos, optimice y fortalezca el sistema a través del análisis y gestión de los siguientes temas en el marco de seguridad: gestión de activos, gestión de comunicaciones y operaciones, gestión de recursos humanos, gestión de terceros, gestión de seguridad física, gestión de la continuidad de negocio, control de acceso lógico, cumplimiento regulatorio estrategia de



seguridad en aplicaciones, estrategia de seguridad de datos y estrategia de seguridad tecnológica, entre otros.

Mapa de Ruta.

A continuación, se listan las actividades que el Icfes planea realizar para la vigencia 2026 en temas de seguridad y privacidad de la información:

Ítem	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
1. Activos de información					
1.1	Identificación y actualización de activos de información	Febrero	Abril	Todos los procesos Icfes - acompañan Equipo Seguridad de la Información	Matrices de activos
1.2	Actualización de Instrumentos de gestión de la información pública	Junio	Septiembre	Equipo Seguridad de la Información	Registro de Activos de Información e Índice de Información Clasificada y Reservada
1.3	Publicación Instrumentos de gestión de la información pública	Septiembre	Septiembre	Equipo Seguridad de la información	Registro de Activos de Información, Índice de Información Clasificada y Reservada Publicación en la página web
1.4	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	100% de los Sistemas de Información con etiquetado de información.

Ítem	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
				Información	
1.5	Actualizar lineamientos para la gestión y uso de los activos de información del instituto	Junio	Septiembre	Equipo Seguridad de la Información	Documentos, procedimientos guías aprobados en Daruma
1.6	Actualizar 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	Agosto	Noviembre	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	Agosto	Noviembre	Todas las áreas y acompañamiento de Equipo Seguridad de la Información	Plan de Tratamiento de Riesgos de Seguridad de la Información
2.3	Seguimiento a la implementación de los planes de tratamiento	Enero	Diciembre	Equipo de Seguridad	Informe trimestral de seguimiento de los planes de tratamiento
3. Concienciación y Sensibilización en Seguridad y Privacidad de la Información					



Ítem	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
3.1	Definición del Plan de Concienciación en Seguridad y Privacidad	Enero	Marzo	Equipo Seguridad de la Información	Documento Plan de Concienciación en Seguridad y Privacidad
3.2	Ejecución del Plan de Concienciación en Seguridad y Privacidad.	Marzo	Diciembre	Equipo Seguridad de la Información y acompañan Oficina Asesora de Comunicaciones y Mercadeo y Subdirección de Talento Humano	Informe de ejecución Plan de Concienciación en Seguridad y Privacidad
3.3	Entrenamientos y/o Sensibilizaciones en temas Seguridad y Privacidad de la información.	Marzo	Diciembre	Equipo Seguridad de la Información	Listado de asistencia, certificado participantes.
					Informe de las acciones realizadas.
3.4	Análisis de resultados del Plan de Concienciación en Seguridad y Privacidad.	Noviembre	Diciembre	Equipo Seguridad de la Información	Informe de resultados Plan de Concienciación en Seguridad y Privacidad
4. Protección de Datos Personales					
4.1	Seguimiento a la implementación y cumplimiento del Manual de Protección de Datos Personales	Febrero	Diciembre	Equipo Seguridad de la Información	Informe de Seguimiento y Recomendaciones
4.2	Diagnóstico sobre el estado de cumplimiento y madurez del Icfes frente a los principios y disposiciones de la Ley de	Marzo	Junio	Equipo Seguridad de la Información	Informe con resultado de diagnóstico

Ítem	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
	protección de datos personales.				
4.3	Definición a seguimiento a la ejecución del plan de cierre de brechas según diagnóstico.	Abril	Diciembre	Equipo Seguridad de la Información	Plan de Brechas - Informes de seguimiento trimestral
4.4	Apoyo en la definición de los lineamientos de propiedad intelectual	Mayo	Julio	Equipo Seguridad de la Información acompaña Oficina Asesora Jurídica	Documentos, procedimientos guías aprobados en Daruma
5. Sistema de Gestión de Seguridad de la Información					
5.1	Apoyo en la definición y/o actualización de documentación asociada a Seguridad y Privacidad de la Información	Enero	Diciembre	Equipo Seguridad de la Información	Documentos, procedimientos guías.
5.2	Actualización de lineamientos de seguridad como apoyo a la ejecución de los procesos	Enero	Diciembre	Equipo Seguridad de la Información	Documentos, procedimiento guías, correos.
5.3	Revisión de la implementación y cumplimiento de los controles de seguridad establecidos.	Junio	Diciembre	Equipo Seguridad de la Información	Herramienta de medición y autodiagnóstico del MSPI semestral

Ítem	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
5.4	Ejecución del plan de cierre de brechas identificado y pendiente de la vigencia anterior sobre el estado de implementación del SGSPI	Enero	Diciembre	Equipo Seguridad de la Información con el apoyo de los responsables de las actividades	Informes Trimestrales de ejecución.
5.5	Gestionar y apoyar la ejecución de la auditoria de certificación al Sistema de Gestión de Seguridad y Privacidad de la Información	Abril	Julio	Equipo Seguridad de la Información	Plan de auditoria
5.6	Definir los planes de mejoramiento de acuerdo con las auditorías realizadas	Febrero	Diciembre	Todos los procesos y acompaña Equipo Seguridad de la Información	Planes de Mejoramiento
5.7	Ejecución de las actividades de los planes de mejoramiento correspondientes al SGSPI	Febrero	Diciembre	Equipo Seguridad de la Información	Registro de evidencia y cierre de planes
5.8	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.

Ítem	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
5.9	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.
6. Continuidad de TI – Continuidad del Negocio					
6.1	Realizar el análisis de impacto al negocio – BIA para los activos críticos de la DTI	Septiembre	Noviembre	Equipo Seguridad de la Información con la Dirección de Tecnología e Información y sus subdirecciones.	Documento de análisis de impacto al negocio – BIA
6.2	Definición del Plan de Continuidad de TI	Abril	Agosto	Equipo Seguridad de la Información	Plan de Continuidad de TI
6.3	Realizar la planeación y ejecución de las pruebas definidas en el Plan de Continuidad de TI	Febrero	Diciembre	Dirección de tecnología e Información y sus subdirecciones – acompaña equipo de seguridad de la 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	Septiembre	Diciembre	Equipo Seguridad de la Información y Dirección de tecnología e Información y sus subdirecciones	Informe de resultados de las pruebas realizadas
7. Seguridad Informática					

Ítem	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
7.1	Solicitar a la DTI la contratación para realizar hacking Ethico e ingeniería social y retest a los sistemas de información	Mayo	Octubre	Dirección de Tecnología e Información	Informes de resultado de vulnerabilidades
7.2	Remediación de las vulnerabilidades identificadas en los diferentes análisis	Febrero	Diciembre	Responsables de los CI de la Dirección de tecnología e Información y sus subdirecciones	Reportes de Cierre de Vulnerabilidades.
7.3	Seguimiento a la remediación de las vulnerabilidades identificadas	Febrero	Diciembre	Equipo Seguridad de la información	Informe de Seguimiento del estado y cierre de Vulnerabilidades.
7.4	Verificación y afinamiento del SOC SaaS con la definición de casos, seguimiento y atención de incidentes	Enero	Diciembre	Equipo de Infraestructura de la Subdirección de Información	Informe mensual de incidentes y alertas y remediaciones
7.5	Implementación y afinamiento de las herramientas de seguridad	Febrero	Diciembre	Equipo de Infraestructura de la Subdirección de Información	Herramientas productivas
7.6	Seguimiento periódico a las actividades reportadas por las herramientas de monitoreo de seguridad informática	Enero	Diciembre	Equipo de Infraestructura de la Subdirección de Información	Reportes seguimiento mensual de las herramientas (DLP, Seguridad Office 365, WAF, Antivirus, entre otros)



Recursos

Equipo seguridad de la información – Oficina Asesora de Planeación, equipo de apoyo seguridad de la información – Dirección Tecnologías de la Información, Áreas y/o personal del Instituto para la Evaluación de la Educación Superior que se requieran para el apoyo o ejecución de las actividades.

Medición

La medición del plan se realizará de forma trimestral según las actividades del trimestre, las que tiene duración todo el año se revisará y reportará avance en los trimestres, pero el cierre se dará en el último corte.

Control de Cambios

CONTROL DE CAMBIOS		
VERSIÓN	DESCRIPCIÓN	FECHA
0	Versión de consulta para la ciudadanía, acorde con el decreto 612 de 2018	29/12/2025
1	Versión aprobada en Comité Institucional de Gestión y Desempeño, acorde con el decreto 612 de 2018	29/01/2026

Aprobó: Alejandro Restrepo Mejía - Jefe de la Oficina Asesora de Planeación.

Revisó: Alejandro Restrepo Mejía - Jefe de la Oficina Asesora de Planeación.

Proyectó: Franklin Esteban Gil Espinal – Contratista Equipo técnico Seguridad de la Información de la Oficina Asesora Planeación.