PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE

Dirección de Tecnología e Información

Versión 2.0

Enero 2024

Contenido

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 2024.

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.

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 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.

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.

- 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.

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.

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

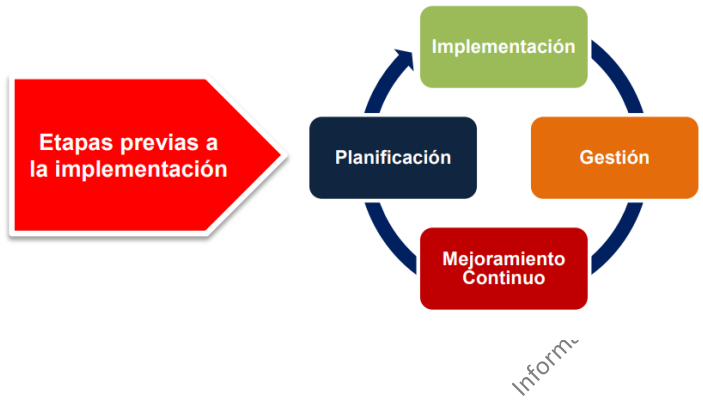
RESPONSABLES

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

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



1. FASE PREVIA - DIAGNOSTICO DEL 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.

1.1 Estado Actual

Teniendo en cuenta la calificación de FURAG, el Icfes se encuentra en un puntaje de 88,5 en seguridad digital, esto se ve reflejado en el esfuerzo realizado por la entidad para apoyar la implementación del SGSPI, por lo que viene adelantando la actualización de las

políticas y manual de políticas de seguridad y privacidad de la información, esto ha permitido 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.

2. 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.

2.1 Diagnóstico del MSPI

El nivel de implementación del MSPI permitirá al Icfes establecer la estrategia a desarrollar para la vigencia 2023 para implementar y mejorar la seguridad y privacidad de la información, para los procesos (20 procesos) misionales, estratégicos, de control y de apoyo de la Entidad y toda la infraestructura que los soporte.

A corte de noviembre de 2023, 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:

Ilustración 2.Evaluación de Efectividad de los Controles

No.	Evaluación de Efectividad de controles	
	DOMINIO	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLÍTICAS 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 EVALUACIÓN DE CONTROLES		OPTIMIZADO

3. FASE 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.

La estructura del Sistema de Gestión de Seguridad y Privacidad de la Información se presentará a través de la estructura que se presenta a continuación:

Ilustración 3. Estructura del Sistema de Seguridad y Privacidad de la Información

4. 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 sus versiones 2013 y 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.

4.1 Mapa de Ruta

A continuación, se listan las actividades que el Icfes planea realizar para la vigencia 2024 en temas de seguridad y privacidad de la información:

Tabla 1. Actividades en Seguridad y Privacidad de la Información 2024

	1. Activos de información				
No	***Actividad***	***Fecha de inicio***	***Fecha final***	***Responsable***	***Producto o resultado esperado***
1.1	*Identificación y actualización de activos de información*	*Mayo*	*Julio*	*Todos los procesos Icfes - acompañan Equipo Seguridad de la Información*	*Matrices de activos*
1.2	*Actualización de Instrumentos de gestión de la información pública*	*Agosto*	*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 Información*	*100% de los Sistemas de Información con etiquetado de información.*
1.5	*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*
1.6	*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				
No	***Actividad***	***Fecha de inicio***	***Fecha final***	***Responsable***	***Producto o resultado esperado***
2.1	*Identificación y Análisis de Riesgos Seguridad de la información*	*Agosto*	*Octubre*	*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*	*Octubre*	*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				
No	***Actividad***	***Fecha de inicio***	***Fecha final***	***Responsable***	***Producto o resultado esperado***
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	*Ejecución del Plan de Concienciación en Seguridad y Privacidad.*	*Febrero*	*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.*	*Febrero*	*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				
No	***Actividad***	***Fecha de inicio***	***Fecha final***	***Responsable***	***Producto o resultado esperado***
4.1	*Seguimiento a la implementación y*	*Febrero*	*Diciembre*	*Equipo Seguridad de la Información*	*Informe de Seguimiento y Recomendaciones.*

	cumplimiento del Manual de Protección de Datos Personales				
4.2	*Diagnóstico sobre el estado de cumplimiento y madurez del Icfes frente a los principios y disposiciones de la Ley de protección de datos personales.*	*Febrero*	*Abril*	*Equipo Seguridad de la Información*	*Informe con resultado de diagnostico*
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	*Actualización del Registro de Base de Datos en la SIC*	*Enero*	*Marzo*	*Equipo Seguridad de la Información acompaña Oficina Asesora Jurídica*	*Actualización del Registro en la SIC*
4.5	*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*
4.6	*Revisión y elaboración de los protocolos para la autorización impresa y electrónica de tratamiento de datos de usuarios, proveedores y empleados y demás documentos para la transmisión o transferencia de información que contenga datos personales con terceros.*	*Mayo*	*Octubre*	*Equipo Seguridad de la Información*	*Documentos, procedimientos guías aprobados en Daruma*
	5. Sistema de Gestión de Seguridad de la Información				
No	***Actividad***	***Fecha de inicio***	***Fecha final***	***Responsable***	***Producto o resultado esperado***
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	*Definición 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*

5.4	*Ejecución del plan de cierre de brechas identificado por la consultoría 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	*Revisión por la Dirección*	*Marzo*	*Mayo*	*Oficina Asesora de Planeación y Equipo Seguridad de la Información*	*Acta de Revisión por la Dirección*
5.6	*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*
5.7	*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*
5.8	*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*
5.9	*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.*
5.10	*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.*
5.11	*Realizar ejercicios y simulaciones para fortalecer el reporte y gestión de incidentes de seguridad y privacidad de la información*	*Julio*	*Diciembre*	*Equipo Seguridad de la Información*	*Informe de Resultados de las actividades realizadas.*
	6. Continuidad de TI – Continuidad del Negocio				
No	***Actividad***	***Fecha de inicio***	***Fecha final***	***Responsable***	***Producto o resultado esperado***
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*	*Octubre*	*Noviembre*	*Equipo Seguridad de la Información*	*Plan de Continuidad de TI*
6.3	*Realizar la planeación y ejecución de las pruebas*	*Febrero*	*Diciembre*	*Dirección de tecnología e*	*Informe de resultados de las pruebas realizadas*

	definidas en el Plan de Continuidad de TI			*Información y sus subdirecciones – acompaña equipo de seguridad de la información*	
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*	*Noviembre*	*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				
No	***Actividad***	***Fecha de inicio***	***Fecha final***	***Responsable***	***Producto o resultado esperado***
7.1	*Contratación para realizar hacking Ethico e ingeniería social y retest a los sistemas de información*	*Junio*	*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	*Implementación 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

Para el presente Plan, se relacionan los recursos humanos, tecnológicos, y financieros, necesarios para su ejecución:

Tabla 2 Recursos Necesarios para el Plan

Tipo Recurso	***Cantidad***	***Valor***
Recursos humanos	*4*	*$414.000.000*
Material de sensibilización y concientización	*1*	*$30.000.000*
Capacitaciones – entrenamientos	*2*	*$60.000.000*
Contratación Auditoria de Certificación	*1*	*$35.000.000*
Contratación EH – Ingeniería Social	*1*	*$200.000.000*
Contratación DLP	*1*	*$150.000.000*
Contratación herramientas de seguridad informática		*$600.000.000*

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:

Tabla 3. Medición del Plan

Trimestre	***Cantidad actividades***	***Formula***
Primer	*3*	*Cantidad actividades cumplidas del periodo transcurrido en la vigencia / Total actividades planeadas (40)*

Segundo	*7*	
Tercero	*4*	
Cuarto	*5*	
Toda la vigencia	*21*	
Total actividades	***40***	