INSTITUTO COLOMBIANO PARA LA EVALUACIÓN DE LA EDUCACIÓN – ICFES Dirección: Calle 26 No. 69-76, Torre 2, piso 16. Edificio Elemento, Bogotá D.C., Colombia. Líneas de atención al usuario: Bogotá 601 5144370

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Oficina Asesora de Planeación.

INSTITUTO COLOMBIANO PARA LA EVALUACIÓN DE LA EDUCACIÓN – ICFES Dirección: Calle 26 No. 69-76, Torre 2, piso 16. Edificio Elemento, Bogotá D.C., Colombia. Líneas de atención al usuario: Bogotá 601 5144370

Índice

Introducción

El Plan de Tratamiento de Riesgos de Seguridad de la Información del Instituto para la Evaluación de la Educación Superior ICFES, genera una estrategia, actividades y acciones preventivas para mitigar los riesgos y mantener su valoración en un residual aceptable para el Instituto, identificando, analizando, evaluando, tratándose y rastreando periódicamente los riesgos de seguridad de la información en cada uno de los procesos del instituto. Este plan de tratamiento, es la línea estratégica que pretende desarrollar y fortalecer en el instituto la cultura organizacional de entendimiento del riesgo y su contexto, generando así la prevención del mismo a todo nivel, comprendiendo las nuevas modalidades de ciberataques dirigidos a entidades públicas, privadas, proveedores de servicios de la OAP, DTI y demás actores que conforman el ecosistema de la información pública, reservada y clasificada, convirtiéndola en un blanco para los ciberdelincuentes que buscan apoderarse de esta, causando traumatismos en la operación, pérdida, robo, destrucción y caída o deterioro de los servicios orientados al instituto y al ciudadano.

El Instituto Colombiano para la Evaluación de la Educación - ICFES, presenta a los grupos de interés, y a la ciudadanía el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2025, donde se establece 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 gestión de riesgos, preservando la confidencialidad, integridad, privacidad y disponibilidad de la información de la entidad para mitigar las posibles afectaciones a los activos que apoyan la evaluación de la educación en todos sus niveles y las investigaciones sobre factores que inciden en la calidad educativa del país.

Objetivos

Objetivos Generales

Realizar el Tratamiento de Riesgos de Seguridad de la Información del ICFES, para prevenir y mitigar los eventos de seguridad de la información del instituto, alineado al Sistema Inteligente para la Gestión Organizacional (SIGO) y a la metodología de Gestión del Riesgo de la Entidad, conforme a los lineamientos y directrices emitidos por el Departamento Administrativo de la Función Pública – DAFP y el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, para la gestión y tratamiento de los riesgos de seguridad de la información, preservando la confidencialidad, integridad y disponibilidad.

Objetivos Específicos

- Involucrar a la Alta Dirección en la gestión proactiva, pertinente y oportuna de los riesgos de seguridad y privacidad de la información.
- Identificar, mitigar y gestionar los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de manera articulada con los riesgos de corrupción y gestión, de acuerdo con el Modelo Integrado de Planeación y Gestión y del Sistema Inteligente para la Gestión Organizacional (SIGO).
- Realizar un efectivo análisis y proteger de los riesgos que afectan los activos del instituto en cuanto a confidencialidad, integridad, privacidad y disponibilidad de la información.
- Hacer seguimiento a la implementación y cumplimiento de los controles y planes de tratamiento definidos, documentando las evidencias y resultados de las acciones realizadas.

Alcance

El plan de tratamiento de riesgos de seguridad aplica a toda la Entidad, se enfoca en gestionar y tratar todos los riesgos de seguridad de la información, en especial los que se encuentran en la zona de riesgo Extremo, Alto o Moderado, los cuales superan la viabilidad de riesgo aceptable en el instituto, con la finalidad de generar mecanismos de prevención y mitigación de los mismos, fortalecer la toma de decisiones y la prevención frente a la materialización de incidentes de seguridad de la información que puedan afectar el logro de los objetivos institucionales.

Un adecuado tratamiento y gestión de los riesgos debe contar con la participación activa de todas las áreas del instituto, con el fin de conocer, apropiar e implementar las directrices y lineamientos definidos y realizar el seguimiento o monitoreo correspondiente de acuerdo a la Política de Riesgos de la Entidad.

Definiciones

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Impacto: consecuencias que puede ocasionar a la organización la materialización del riesgo.

Control o Medida: Medida que permite reducir o mitigar un riesgo.

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.

- Decreto 612 de 4 de abril 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.

- 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 presente plan está alineado y contribuye al logro de la misión, visión, mega y demás elementos del direccionamiento estratégico del Icfes, los cuales se estipulan en el Plan Estratégico Institucional y el Plan de Seguridad de la Información.

Articulación con el contexto estratégico	
Objetivo estratégico al que aporta:	Fortalecer análisis y divulgación de información relevante para grupos de interés. Mejorar los procesos administrativos. Generar una cultura de calidad e innovación en todos los niveles de la organización. Fortalecer el uso de la tecnología.
Gestión y Desempeño Institucional - MIPG	Política Gobierno Digital. Política de Seguridad Digital. Política de Gestión Documental. Política de Transparencia, acceso a la información pública y lucha contra la corrupción. Gestión del conocimiento y la innovación.

Metodología de Implementación

La metodología para la identificación, evaluación y gestión de riesgos de los sistemas de gestión vigentes del Icfes se basa en la NTC-ISO 31000, la Guía para la administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública – DAFP, principalmente en lo dispuesto en su Anexo 4 - Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas del Ministerio de Tecnología de la Información y las comunicaciones y la cual se encuentra definida en el política de gestión de riesgos de la entidad DES -PT001 y el manual de gestión integral de riesgos DES -MN002, estos documentos tiene como objetivo generar un lineamiento para la gestión del riesgo del Icfes, que permita la mejora continua y el cumplimiento de los objetivos institucionales mediante el tratamiento de controles fortaleciendo el desempeño de los procesos y la transparencia en la gestión Institucional y aplica para todos los procesos del instituto.

Por lo anterior de manera articulada con la Oficina Asesora de Planeación se realiza la gestión de todos los riesgos en el Icfes, ya sean de gestión, corrupción, contratación, seguridad, privacidad, seguridad digital, ciberseguridad y continuidad, las actividades de identificación y análisis de los riesgos la realizan con los líderes de cada proceso como propietarios de los activos, por lo cual deben garantizar porque los custodios de las información cumplan con los controles establecidos para procurar la confidencialidad, integridad, privacidad y disponibilidad de la información institucional.

El objetivo del análisis es identificar los riesgos, evaluar la pertinencia de los controles y determinar el tratamiento del riesgo que lo lleve a un nivel aceptable, teniendo en cuenta el siguiente esquema:

Ciclo en la Gestión del Riesgo

[Grafica] Ciclo en la Gestión del Riesgo: DES -PT001

El propósito es permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo, lo que implica definir el alcance del proceso, y comprender los contextos externo e interno. Se establece un contexto del proceso con los siguientes aspectos:

Establecimiento del Contexto

- **Definir el alcance:** Se deben considerar los objetivos de la gestión de riesgos que deben estar alineados con los objetivos de la organización.
- **Contextos externo e interno:** Es necesario realizar el análisis de necesidades y requerimientos de los entornos externo e interno en los cuales opera el Instituto y debería reflejar el entorno específico.
- **Definición de los criterios del riesgo:** Se debe establecer la cantidad y el tipo de riesgo que se pueden o no gestionar. También deben definirse los criterios para valorar la importancia del riesgo y para apoyar los procesos de toma de decisiones.

Evaluación del Riesgo

- **Identificación del Riesgo:** El propósito es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir al Instituto lograr sus objetivos, por lo que es necesario contar con información pertinente, apropiada y actualizada.
- **Análisis de Riesgos:** El propósito es comprender la naturaleza del riesgo y sus características incluyendo el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos.
- **Valoración del riesgo:** El propósito es apoyar a la toma de decisiones, pues implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional.

Tratamiento del Riesgo

El tratamiento del riesgo consiste en seleccionar y aplicar las medidas adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos, para lo cual se definen medidas de respuesta ante los riesgos (asumir, reducir, compartir, trasferir o evitar), luego se definen acciones de mitigación de riesgos (actividades o tareas, responsables, plazo de ejecución y seguimiento).

El tratamiento del riesgo implica la preferencia para la modificación de los riesgos y la aplicación del mismo, una vez empleado el tratamiento otorga controles o los modifica, es importante incluir las opciones de análisis, evaluación, desarrollo e implementación que se deben tener en cuenta para el tratamiento del riesgo. Después de definir qué opción (es) de manejo se le va (n) a dar a los riesgos, se deben establecer las actividades de control, responsables, tiempo, indicadores que midan la efectividad de las acciones de control y acciones de contingencia.

Comunicación y Consulta

La comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones. Esto debería facilitar un intercambio de información basado en hechos, oportuno, pertinente, exacto y comprensible, teniendo en cuenta la confidencialidad e integridad de la información, así como el derecho a la privacidad de las personas.

Seguimiento y Revisión

El propósito es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

La revisión de las actividades que se ejecutan se verificará por medio de los planes de tratamiento, identificando la gestión, avances y resultados con relación a los efectos de los cambios de nivel de riesgo que puede perjudicar en las consecuencias y el riesgo se pueda materializar, de tal manera es necesario la revisión continua para adquirir información para la valoración del riesgo e identificar los riesgos emergentes.

Mapa de Ruta

A continuación, se listan las actividades que el Icfes planea realizar para la vigencia 2025 para el tratamiento de los riesgos de seguridad y privacidad de la información:

Ítem	Actividad	Inicio	Fin	Responsable	Producto o resultado esperado
Riesgos de Seguridad y Privacidad de la Información					
1	Seguimiento a la ejecución de los planes de tratamiento definidos en la vigencia anterior.	Febrero	Diciembre	Equipo Seguridad de la Información	Informe Trimestral de Planes de Tratamiento
2	Identificación, documentación, análisis y valoración de Riesgos de seguridad en la herramienta institucional	Julio	Octubre	Todas las áreas acompañamiento de Equipo Seguridad de la Información	Matrices de Riesgos
3	Definición de planes de tratamiento para la mitigación de los riesgos	Septiembre	Noviembre	Todas las áreas acompañamiento de Equipo Seguridad de la Información	Planes de tratamiento
4	Revisión y cierre de los planes de tratamiento de riesgos	Febrero	Diciembre	Todas las áreas acompañamiento de Equipo Seguridad de la Información	Actas de reunión - correos Electrónicos – Cierre Planes en Daruma
5	Informe de cierre de los riesgos de seguridad y privacidad de la información	Noviembre	Diciembre	Equipo Seguridad de la Información	Informe final riesgos de seguridad y privacidad de la información

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.

ELIZABETH BLANDÓN BERMÚDEZ

Directora General Icfes

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.