PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2022

Dirección de Tecnología e Información

Versión 1

Índice

1. Introducción

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 2022, 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.

El análisis de riesgos de los activos de información nos permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad, privacidad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis. Los escenarios de riesgo presentes en nuestra época obligan a que las entidades como el Icfes cuenten con un proceso integral de gestión de riesgos orientado a darle la confianza necesaria a la ciudadanía que se cuenta con instituciones seguras, confiables y que estas tienen resiliencia frente a los diferentes factores externos causantes de inestabilidad política, afectación de la información y conflictos sociales.

2. Objetivos

01. Objetivo General

02. Objetivos específicos.

2. Objetivos

Objetivo general

Establecer las actividades necesarias para mantener la integridad, confidencialidad, disponibilidad y privacidad de la información a través de la gestión de los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y Continuidad del Instituto Colombiano para la Evaluación de la Educación – Icfes.

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 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.
- Realizar un efectivo análisis 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.

3. Generalidades

01. Contexto estratégico.
02. Alcance.
03. Contexto normativo.
04. Definiciones.

3. Generalidades.

Contexto estratégico

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, PETI 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

Alcance

El presente plan aplica en todos los procesos del 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.

Contexto 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

Contexto normativo

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

- 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.

- Ley 1955 de 2019 Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. “Pacto por Colombia, Pacto por la Equidad”

- 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 interna 391 de 2020 “Por la cual se adopta la nueva 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 dictan otras disposiciones”.

- Resolución interna 397 de 2020 “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 2020”.

- 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”.

- Norma Técnica Colombiana ISO27001
- Norma Técnica Colombiana ISO27005
- Norma Técnica Colombiana ISO31000

Definiciones

- **Activo de información:** La información imprescindible o de alto valor para el instituto es llama Activo de Información, su protección es uno de los objetivos del SGSI. (Ej: Información, sistemas de información, servicios, hardware, software y personas)
- **Amenaza:** Peligro latente de que un evento pueda causar un incidente no deseado, presentando daños y/o pérdidas a los activos de información.
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia**: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Control**: Acción o medida que modifica nivel del riesgo
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad.
- **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.
- **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.
- **Integridad:** propiedad de exactitud y completitud.
- **Impacto**: Efecto negativo o positivo que provocaría en caso de que materializara el riesgo.

Definiciones

- **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, es la combinación del impacto y posibilidad.
- **Privacidad**: Es el aspecto que se ocupa de la capacidad que una organización o individuo tiene para determinar el tratamiento que se les da a los datos de recolecta o produce.
- **Probabilidad**: Posibilidad de materialización del riesgo analizado. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Riesgo:** Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos del Icfes. Se expresa en términos de probabilidad y consecuencias (impacto).
- **Riesgo Inherente**: Es el nivel de riesgo sin implementar controles.
- **Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo después de aplicar los controles.
- **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.
- **Vulnerabilidad:** Es una debilidad, deficiencia o falta de control en los procesos, tecnología o administración.

4. Desarrollo del Plan de Seguridad y Privacidad de la Información.

01. Ciclo de la Gestión de Riesgos.
02. Establecimiento de contexto.
03. Valoración y Análisis del Riesgo.
04. Tratamiento del Riesgo.
05. Comunicación de Riesgos.
06. Monitoreo – Información de riesgos y revisión.

4. Desarrollo del Plan de Seguridad y Privacidad de la Información.

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 PDE -PT001 y el manual de gestión integral de riesgos PDE -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 de la Gestión de Riesgos

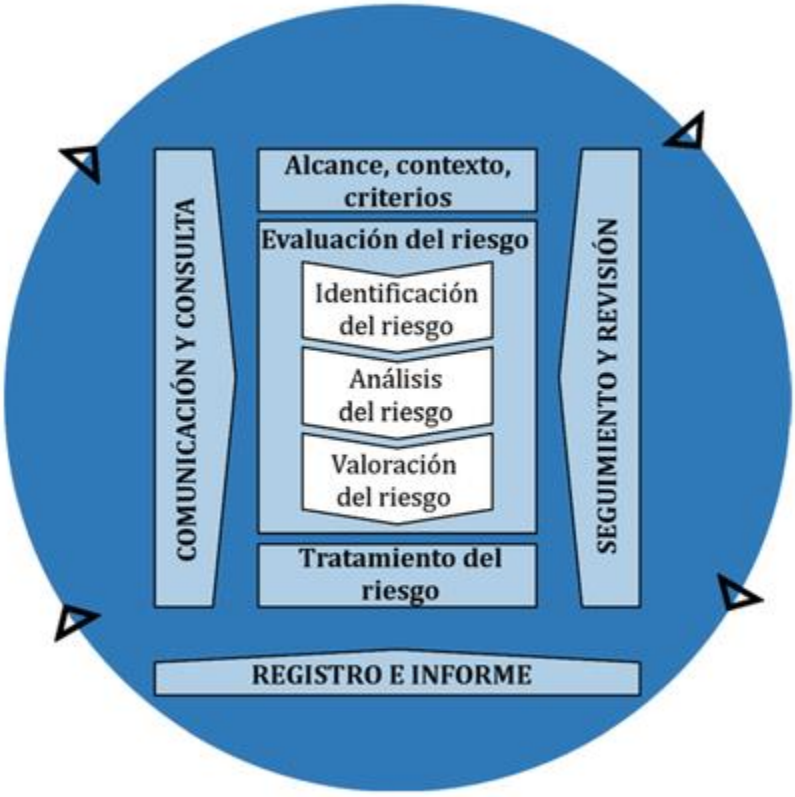

Ilustración 1 - Ciclo de la Gestión de los Riesgos - ISO 31000:2019

Alcance, Contexto y Criterios

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:

- **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)

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.

3. Mapa de ruta

3. Mapa de Ruta.

No	Actividad	Fecha inicio	Fecha final	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*	*Junio*	*Agosto*	*Todas las áreas acompañamiento de Equipo Seguridad de la Información*	*Matriz de Riesgos*
3	*Definición de planes de tratamiento para la mitigación de los riesgos*	*Junio*	*Agosto*	*Todas las áreas acompañamiento de Equipo Seguridad de la Información*	*Planes de tratamiento*
4	*Gestión y seguimiento a la ejecución de los planes de tratamiento definidos*	*Enero*	*Diciembre*	*Todas las áreas acompañamiento de Equipo Seguridad de la Información y OCI*	*Actas de reunión - correos Electrónicos - Reporte de Evidencias*
5	*Informe de cierre de los riesgos de seguridad y privacidad de la información*	*Diciembre*	*Diciembre*	*Equipo Seguridad de la Información*	*Informe final riesgos de seguridad y privacidad de la información*