PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Versión 1.0

Instituto Colombiano para la Evaluación de la Educación
ICFES

Bogotá, julio de 2018

FORMATO PRELIMINAR AL DOCUMENTO

Título:	**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**				
Fecha dd/mm/aaaa:	31/07/2018				
Resumen:	Este documento tiene como objetivo establecer políticas, actividades y acompañamiento para la Gestión de Riesgos de Seguridad y Privacidad de la Información, así mitigar la afectación a la confidencialidad, integridad y disponibilidad de la información del Instituto Colombiano para la Evaluación de la Educación – ICFES.				
Palabras claves:	Confidencialidad, Integridad, Disponibilidad, Seguridad de la Información y riesgo				
Formato:	DOC	**Código:**	No aplica	**Versión:**	1.0
Autor (es):	Sergio Carreño Pérez Profesional de la Dirección de Tecnología e Información				
Revisó:	Eliécer Vanegas Murcia Director de Tecnología e Información Carlos Cardona López Subdirector de Información				
Aprobó:	Eliécer Vanegas Murcia Director de Tecnología e Información Carlos Cardona López Subdirector de Información				
Información adicional:	No aplica				
Ubicación:	Calle 26 No.69-76, Torre 2.				

CONTROL DE CAMBIOS

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	31/07/2018	Versión inicial

TABLA DE CONTENIDO

1. INTRODUCCIÓN....5
2. OBJETIVO GENERAL....5
2.1. OBJETIVOS ESPECIFICOS....5
3. ALCANCE....5
4. RESPONSABILIDADES....6
5. METODOLOGÍA....6
6. TIEMPO DE EJECUCIÓN – CRONOGRAMA DE ACTIVIDADES....7
7. PRESUPUESTO....8
8. GESTIÓN DEL RIESGO DEL PLAN....8

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es 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 y disponibilidad de la información del Instituto Colombiano para la Evaluación de la Educación – ICFES y el establecimiento de controles para mitigar las posibles afectaciones, todo esto basado en la Norma Técnica Colombiana ISO31000:2011, las políticas creadas para la protección del entorno digital y cibernético en el CONPES 3854 de 2016 y 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", dentro del cual se establecen para las entidades del estado los Habilitadores Transversales: *Seguridad de la Información*, Arquitectura de TI y Servicios Ciudadanos Digitales.

2. OBJETIVO GENERAL

Establecer políticas, actividades y acompañamiento para la Gestión de Riesgos de Seguridad y Privacidad de la Información, así mitigar la afectación a la confidencialidad, integridad y disponibilidad de la información del Instituto Colombiano para la Evaluación de la Educación – ICFES.

2.1. OBJETIVOS ESPECIFICOS

a. Minimizar el riesgo en los procesos de la entidad respecto a la integridad, confidencialidad y disponibilidad de la información.

b. Cumplir la normatividad legal vigente en la Política de Gobierno Digital establecida por el MinTic y demás legislación aplicable al ICFES.

c. Asignar y usar eficazmente los recursos para el tratamiento del riesgo.

3. ALCANCE

El presente documento, está destinado a orientar a las áreas y colaboradores del ICFES para la identificación de riesgos, implementación de controles y seguimiento a los mismos preservar la confidencialidad, integridad y disponibilidad de la información que reciban, generen y procesen en medio físico o digital, con el fin de mitigar la afectación ante posibles amenazas.

4. RESPONSABILIDADES

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se encuentra bajo cada área que haya identificado los riesgos asociados a Información, adicionalmente la Dirección de Tecnología e Información asigna profesionales para crear lineamientos y herramientas para facilitar la identificación y el tratamiento de estos, de acuerdo a las funciones establecidas en el decreto 5014 de 2009, en relación a definir, coordinar y controlar las políticas, estrategias, procedimientos y actividades de seguridad informática de la empresa.

5. METODOLOGÍA

A continuación, se describen las etapas y actividades preliminares contempladas en la formulación y ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del ICFES, así poder atender las necesidades de mitigación de impactos asociados a la información física y digital en la Entidad:

Etapa 1. Identificación de requerimientos para mantener la confidencialidad, integridad y disponibilidad de la información.

Etapa 2. Diagnosticar el estado actual de la información, tipo, medio de almacenamiento, cumplimiento legal, responsables de la recepción, generación, procesamiento y eliminación.

Etapa 3. Definir y/o formular la estrategia a aplicar para mitigar la afectación a la información de la entidad, así como los responsables y fases de implementación. En este punto, el ICFES estableció el Sistema de Seguridad de la Información, basado en la Norma Técnica Colombiana ISO27001:2013, a su vez se estableció una metodología de riesgos basada en la Norma Técnica ISO3001 e ISO27005.

Etapa 4. Definir y/o ajustar políticas, manuales, procedimientos e instructivos asociados a los riesgos de la información del ICFES basado en buenas prácticas internacionales.

Etapa 5. Revisar y/o ajustar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de acuerdo con las mejores prácticas y exigencias legales asociadas a la mitigación de riesgos de la información, así como la integración con los diferentes planes vigentes y su armonización con el Modelo Integrado de Planeación y Gestión.

Etapa 6. Definir las directrices frente a la identificación y tratamiento de riesgos de la información del ICFES.

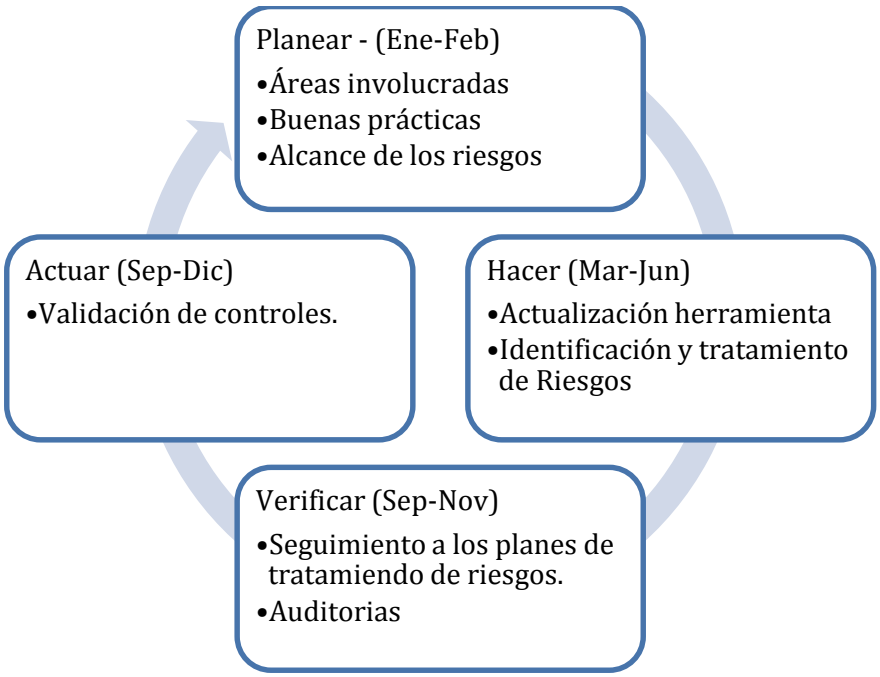
Etapa 7. Formalizar y socializar a las áreas de la Entidad los riesgos y los tratamientos establecidos para el cuidado de la información.

Para aplicar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en el ICFES se disponen de los siguientes recursos:

RECURSOS	VARIABLE
Humanos	Dirección de Tecnología e Información a través de la Subdirección de Información es responsable coordinar y controlar las políticas, estrategias, procedimientos y actividades de seguridad de la información del ICFES.
Técnicos	Herramienta para la identificación de riesgos y controles.
Logísticos	Socialización y transferencia de conocimiento sobre el cuidado de la información institucional.
	Gestión del cambio
Financieros	Plan de inversión continuada al talento humano y tecnológico requerido para el cuidado de la información institucional.
	Auditorias
	Mejora continua

6. TIEMPO DE EJECUCIÓN – CRONOGRAMA DE ACTIVIDADES

La ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es de manera permanente en la Entidad, con revisión y actualización periódica, basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar), con el siguiente ciclo de implementación para el año 2018:



7. PRESUPUESTO

El presupuesto para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que hace parte del Sistema Gestión de Seguridad de la Información, está incluido dentro del rubro asignado a la Dirección de Tecnología e Información coordinar y controlar las políticas, estrategias, procedimientos y actividades de seguridad de la información de la empresa, aportando con el talento humano en la creación de políticas, herramientas y acompañamiento, las áreas asignan responsables para la identificación y tratamiento de riesgos.

8. GESTIÓN DE RIESGO DEL PLAN

A continuación, se evalúan los riesgos para la ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en el ICFES, así:

CAUSA	RIESGO	PROBABILIDAD	IMPACTO	CONSECUENCIA
Errores en la planificación	Incumplimiento en los objetivos establecidos	Menor	Mayor	Incumplimientos legales y sanciones
Falta de recursos económicos	Incumplimiento en los objetivos establecidos	Posible	Mayor	Incumplimientos legales y reprocesos
Falta de ejecución de acciones del plan de Seguridad y Privacidad.	Exposición a pérdida o fuga de información sensible de la entidad.	Probable	Mayor	Incumplimientos legales y sanciones.