Imagen que contiene persona, interior, pared, captura de pantalla

Descripción generada automáticamente

# Versión 2

# Plan de Seguridad y Privacidad de la Información - Icfes

Contenido

[Plan de Seguridad y Privacidad de la Información - Icfes 1](file:///C:\Users\Diego\Downloads\10.%20Plan%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informacion%20(1).docx#_Toc42710541)

[Introducción 3](#_Toc42710542)

[Objetivos 4](#_Toc42710543)

[Objetivo General: 4](#_Toc42710544)

[Objetivos específicos: 4](#_Toc42710545)

[Definiciones 5](#_Toc42710546)

[Generalidades 8](#_Toc42710547)

[Alcance del Documento 8](#_Toc42710548)

[Marco Normativo 8](#_Toc42710549)

[Desarrollo del Plan de Seguridad y Privacidad de la Información 10](#_Toc42710550)

[Metodología de implementación 10](#_Toc42710551)

[Mapa de Ruta 11](#_Toc42710552)

# 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, presenta el Plan se Seguridad y Privacidad de la Información para la vigencia 2020.

Siendo consiente que la seguridad 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 Plan de Seguridad y Privacidad de la Información para la vigencia 2020, 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 gestión de riesgos y el establecimiento de controles 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. Este modelo propone un proceso continuo de tratamiento de riesgos con el fin de gestionarlos de acuerdo al contexto de la organización, teniendo como referentes la NTC (Norma Técnica Colombiana) ISO 27001:2013 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.

# Objetivos

## Objetivo General:

Definir las acciones para mejorar el nivel de madurez del Sistema de Gestión de Seguridad y Privacidad de la Información del Icfes, de acuerdo con las estrategias de Gobierno Digital, MIPG, requerimientos de la entidad y disposiciones legales vigentes, tendientes a garantizar la integridad, confidencialidad, disponibilidad y privacidad de la información institucional.

## Objetivos específicos:

* Hacer uso eficiente y seguro de los activos de información para garantizar la continuidad de la prestación de los servicios de TI.
* Apoyar la identificación y clasificación de los activos de información del instituto, así como el análisis, valoración y tratamiento de los riesgos de seguridad de la información, privacidad, ciberseguridad y seguridad digital.
* 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.
* Fortalecer la cultura, responsabilidad, conductas y hábitos sobre la seguridad y privacidad de la información en todos los colaboradores del Icfes.
* Atender los requerimientos de seguridad de la información, seguridad digital y ciberseguridad establecidos por las diferentes entidades a nivel nacional y requisitos de legales.

# Definiciones

**Activos de Información:** Son los recursos necesarios para que una empresa o un negocio funcione y consiga los objetivos que se ha propuesto la alta dirección. (ISO 27001).En relación con la privacidad y seguridad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal (MSPI - MINTIC). Son, entre otros, las bases de datos, los archivos, los manuales, las aplicaciones, así como el hardware y software que se tiene el Instituto para desarrollar su objeto.

**Amenaza:** Posible causa de un riesgo.

**Auditoria:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del MSPI de una organización.

**CSIRT**: Equipo de respuestas ante incidentes de seguridad.

**Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

**Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el MSPI de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma ISO 27001:2013.

**Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

**Disponibilidad:** propiedad de la información de ser accesible, utilizable y recuperable a demanda por una entidad.

**Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO27001:2013 e ISO31000:2013.

**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.

**Ingeniería Social:** Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial o reservada de una entidad.

**Integridad:** propiedad de la información de ser completa, exacta e inalterada exactitud y completitud.

**Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

**ISO 27001:** Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Actual la segunda publicación de 2013.

**MSPI:** Modelo de Seguridad y Privacidad de la Información propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los componentes de la Política de Gobierno Digital.

**Plan de continuidad del negocio (BCP):** Orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

**Plan de tratamiento de riesgos:** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles para proteger la misma.

**Política de seguridad de información**: Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.

**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.

**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.

**Sistema de Gestión de Seguridad de la Información:** Parte del sistema de gestión general del Instituto, basada en un enfoque hacia los riesgos globales del negocio, cuyos fines son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

**Vulnerabilidad:** condiciones o factores que se tienen o no y cuya explotación puede implicar una amenaza.

# Generalidades

## Alcance del Documento

El presente Plan de Seguridad y Privacidad de la Información aplica a 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 1955 de 2019 Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. “Pacto por Colombia, Pacto por la Equidad”

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.

Guía para la administración del riesgo y el diseño de controles en entidades públicas. RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL año 2018.

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.

Resolución interna 887 de 2016 “Por la cual se adopta el Sistema de Gestión de Seguridad de la Información (SGSI) del Instituto Colombiano para la Evaluación de la Educación – ICFES”.

Resolución interna 042 de 2018 por el cual se actualiza el Registro de Activos de Información, el Índice de Información Clasificada y Reservada y el Esquema de Publicación de la Información.

Resolución interna 278 de 2016 “Por el cual se adopta el Manual de Políticas y Procedimientos de Protección de Datos y se implementa la Política Pública de Protección de Datos Personales”.

Norma Técnica Colombiana ISO27001:2013.

Norma Técnica Colombiana ISO31000:2013

# Desarrollo del Plan de Seguridad y Privacidad de la Información

## Metodología de implementación

La metodología de implementación del Plan de Seguridad y Privacidad para el Instituto Colombiano para la Evaluación de la Educación – Icfes, está basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y lo establecido en el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC y se ejecuta a través del mapa de ruta definido a continuación:



# Mapa de Ruta

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***No*** | ***Actividad*** | ***Fecha de inicio*** | ***Fecha final*** | ***Responsable*** | ***Producto o resultado esperado*** |
| ***1. Activos de información*** | | | | | |
| *1.1* | *Actualización de Instrumentos de gestión de la información pública* | *Enero* | *Julio* | *Todos los procesos Icfes – acompañan Equipo SGSI* | *Matrices de activos* |
| *1.2* | *Publicación Instrumentos de gestión de la información pública* | *Julio* | *Agosto* | *Oficina Asesora de Planeación y Equipo SGSI* | *Registro de Activos de Información, Índice de Información Clasificada y Reservada y Esquema de Publicación en la página web* |
| ***2. Riesgos de Seguridad y Privacidad de la Información*** | | | | | |
| *2.1* | *Identificación y Análisis de Riesgos Seguridad de la información* | *Julio* | *Diciembre* | *Todas las áreas y acompañamiento de Equipo SGSI* | *Matrices de riesgos* |
| *2.2* | *Definición del Tratamiento de Riesgos Seguridad de la Información* | *Julio* | *Diciembre* | *Todas las áreas y acompañamiento de Equipo SGSI* | *Plan de Tratamiento de Riesgos de Seguridad de la Información* |
| *2.3* | *Seguimiento a la implementación de los planes de tratamiento* | *Julio* | *Diciembre* | *Equipo de Seguridad* | *Informe trimestral de seguimiento de implementación de los planes de tratamiento* |
| ***3. Plan de concienciación en Seguridad y Privacidad de la Información*** | | | | | |
| *3.1* | *Definición del Plan de Concienciación en Seguridad y Privacidad* | *Enero* | *Febrero* | *Equipo SGSI* | *Documento Plan de Concienciación en Seguridad y Privacidad* |
| *3.2* | *Ejecución del Plan de Concienciación en Seguridad y Privacidad.* | *Febrero* | *Diciembre* | *Equipo SGSI 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* | *Inducción y reinducción en Seguridad y Privacidad de la información.* | *Marzo* | *Diciembre* | *Equipo SGSI* | *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 SGSI* | *Informe de resultados Plan de Concienciación en Seguridad y Privacidad* |
| ***4. Protección de Datos Personales*** | | | | | |
| *4.1* | *Revisión de Requisitos Legales de Seguridad y Privacidad* | *Abril* | *Agosto* | *Oficina Asesora Jurídica y acompaña Equipo SGSI* | *Actualización del Normograma* |
| *4.2* | *Validación y actualización del registro de Bases de Datos en el RNBD* | *Febrero* | *Diciembre* | *Equipo SGSI* | *Registro de BD ante la SIC* |
| *4.3* | *Definición de la Política y Aviso de privacidad de protección de datos personales* | *Febrero* | *Mayo* | *Oficina Asesora Jurídica y acompaña Equipo SGSI* | *Política y Aviso de privacidad de protección de datos personales* |
| *4.4* | *Definición del Manual de Protección de Datos Personales* | *Junio* | *Diciembre* | *Oficina Asesora Jurídica y acompaña Equipo SGSI* | *Manual de Protección de Datos Personales* |
| ***5. Dominios de la Norma ISO 27001:2013*** | | | | | |
| *5.1* | *Revisión de Manual y Políticas y Procedimientos de Seguridad del Sistema de Gestión de Seguridad de la Información.* | *Enero* | *Julio* | *Equipo SGSI* | *Documentos Manual, Políticas y Procedimientos de Seguridad de la Información.* |
| *5.2* | *Definición de lineamientos de seguridad como apoyo a la ejecución del proceso de Gestión de Tecnología e Información* | *Enero* | *Diciembre* | *Equipo SGSI* | *Documentos, procedimiento guías.* |
| *5.3* | *Definición de lineamientos de seguridad como apoyo a la ejecución de los diferentes procesos.* | *Enero* | *Diciembre* | *Equipo SGSI* | *Documentos, procedimiento guías.* |
| *5.4* | *Revisión de los controles de la norma ISO 27001:2013* | *Junio* | *Diciembre* | *Equipo SGSI* | *Herramienta de medición y autodiagnóstico del MSPI semestral* |
| ***6. Auditorías al Sistema de Gestión de Seguridad de la Información*** | | | | | |
| *6.1* | *Participar en las Auditorías al Sistema de Gestión de Seguridad de la Información* | *Junio* | *Diciembre* | *Áreas parte del alcance de auditoria y acompaña Equipo SGSI* | *Actas de participación en el Plan de auditoria* |
| *6.2* | *Definir los planes de mejoramiento de acuerdo con las auditorías realizadas* | *Febrero* | *Diciembre* | *Áreas parte del alcance de auditoria y acompaña Equipo SGSI* | *Planes de Mejoramiento* |
| *6.3* | *Realizar seguimiento a la ejecución de los planes de mejoramiento* | *Febrero* | *Diciembre* | *Áreas parte del alcance de auditoria y acompaña Equipo SGSI* | *Informe seguimiento a la ejecución de los planes de mejoramiento* |
| ***7. Gestión de Incidentes de Seguridad de la Información*** | | | | | |
| *7.1* | *Gestión y cierre oportuno de los incidentes de seguridad de la Información* | *Enero* | *Diciembre* | *Equipo SGSI* | *Registro y documentación de las acciones sobre la gestión de los incidentes presentados.* |
| ***8. Indicadores del Sistema de Gestión de Seguridad de la Información*** | | | | | |
| *8.1* | *Definición de los indicadores del Sistemas de Gestión de Seguridad de la Información* | *Junio* | *Julio* | *Equipo SGSI* | *Indicadores de gestión* |
| *8.2* | *Reporte de información de los indicadores del Sistema de Gestión de Seguridad de la Información* | *Enero* | *Diciembre* | *Equipo SGSI* | *Resultado de la medición* |
| ***9. Seguridad Informática*** | | | | | |
| *9.1* | *Realizar análisis de vulnerabilidades a los sistemas de información e infraestructura de TI* | *Marzo* | *Diciembre* | *Equipo SGSI* | *Vulnerabilidades Identificadas.* |
| *9.2* | *Seguimiento a la remediación de las vulnerabilidades identificadas* | *Enero* | *Diciembre* | *Equipo SGSI* | *Cierre de Vulnerabilidades.* |
| *9.3* | *Seguimiento periódico a las actividades reportadas por las herramientas de monitoreo de seguridad informática* | *Mayo* | *Diciembre* | *Equipo SGSI - DTI* | *Reportes seguimiento herramientas (DLP, Seguridad Office 365, WAF, Imperva, Antivirus, DDOS, DA, VPN)* |
| ***10. Continuidad de TI*** | | | | | |
| *10.1* | *Realizar el análisis de impacto al negocio – BIA para los activos críticos de la DTI* | *Julio* | *Agosto* | *Equipo SGSI - DTI* | *Documento de análisis de impacto al negocio – BIA* |
| *10.2* | *Definir los Escenarios de afectación para los servicios de TI* | *Agosto* | *Octubre* | *Equipo SGSI - DTI* | *Riesgos de Continuidad de TI* |
| *10.3* | *Definición del Plan de Continuidad de TI* | *Agosto* | *Octubre* | *Equipo SGSI - DTI* | *Plan de Continuidad de TI* |
| *10.4* | *Realizar la planeación, ejecución y evaluación de las pruebas definidas en el Plan de Continuidad de TI* | *Agosto* | *Diciembre* | *Equipo SGSI - DTI* | *Informe de resultados de las pruebas realizadas* |