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

Descripción generada automáticamente

**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020**

**Dirección de Tecnología e Información**

1. **Introducción.**
2. **Objetivos.**
   1. Objetivo General.
   2. Objetivos Específicos.
3. **Generalidades.**
   1. Contexto estratégico.
   2. Alcance.
   3. Contexto normativo.
   4. Definiciones.
4. **Desarrollo del Plan de Seguridad y Privacidad de la Información.**
   1. Ciclo de la Gestión de Riesgos.
   2. Establecimiento de contexto.
   3. Valoración y Análisis del Riesgo.
   4. Tratamiento del Riesgo.
   5. Comunicación de Riesgos.
   6. Monitoreo – Información de riesgos y revisión.
5. **Mapa de ruta.**

**Índice**

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 2020, 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.

1. **Introducción**

**2. Objetivos**

1. Objetivo General
2. Objetivos específicos.



* Involucrar a la Alta Dirección en la gestión proactiva, pertinente y oportuna de los riesgos de Seguridad y Privacidad de la información, Seguridad digital, ciberseguridad y Continuidad, que apoyan el cumplimiento de los objetivos estratégicos del instituto.
* 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 más críticos 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.

**Objetivo general**

**Objetivos específicos**

Establecer las actividades necesarias para mantener la integridad, confidencialidad y disponibilidad 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.

**2. Objetivos**

1. Contexto estratégico.
2. Alcance.
3. Contexto normativo.
4. Definiciones.

**3. Generalidades**

**3. Generalidades.**



| 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 |

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.

**Contexto estratégico**



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.

**Alcance**



**Contexto normativo**

* Ley 44 de 1993 “por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.” (Derechos de autor).
* Ley 527 de 1999 “por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.
* 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.



* 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”.
* NTC-ISO\IEC 27001
* GTC-ISO\IEC 27002
* NTC-ISO\IEC 27005
* NTC-ISO 31000

**Contexto normativo**



* **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**



**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.

1. Ciclo de la Gestión de Riesgos.
2. Establecimiento de contexto.
3. Valoración y Análisis del Riesgo.
4. Tratamiento del Riesgo.
5. Comunicación de Riesgos.
6. Monitoreo – Información de riesgos y revisión.

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

**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.

Esta política 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, Seguridad y Privacidad de la información, 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 velar 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**

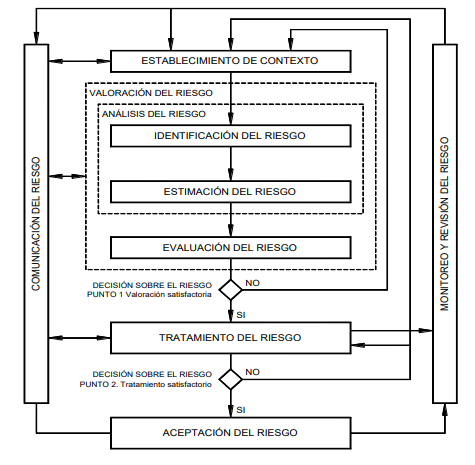


Ilustración 1 - Ciclo de la Gestión de los Riesgos - ISO 31000:2009



Se establece un contexto del proceso con los siguientes aspectos:

* **Contexto del Proceso:** Se determinan las características o aspectos esenciales del proceso y sus interrelaciones.
* **Diseño del proceso:** Claridad en la descripción del alcance y objetivo del proceso.
* **Interrelación con otros procesos:** Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
* **Transversalidad:** Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.

1. Riesgos de corrupción.
2. Racionalización de trámites.
3. Estrategia de rendición de cuentas.
4. Mecanismos para la transparencia y acceso a la información.
5. Mecanismos para mejorar la atención al ciudadano.

**Establecimiento de contexto**



**Establecimiento de contexto**

* **Procedimientos asociados:** Pertinencia en los procedimientos que desarrollan los procesos.
* **Responsables del proceso:** Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
* **Comunicación entre los procesos:** Efectividad en los flujos de información determinados en la interacción de los procesos.

Y luego se establece el tipo de proceso: Misional, Estratégicos, de Apoyo y Evaluación y Control.



**Valoración y análisis del riesgo**

Se realiza la identificación de los riesgos sus causas, vulnerabilidades, amenazas (identificación, descripción, tipo), consecuencias y se determina la clase de riesgo basados en la probabilidad e impacto, todo esto asociado a aquellos eventos o situaciones que puedan afecten los activos de información interrumpiendo el normal desarrollo de los procesos.



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)

**Tratamiento del riesgo**



**Información de riesgos y revisión**

Los riesgos identificados traen consigo controles que incluyen el monitoreo de los eventos correspondientes, invirtiendo los recursos de acuerdo a la criticidad del riesgo asociado, las responsabilidades del monitoreo comprenden todos los aspectos del proceso para la gestión del riesgo con el fin de:

* Garantizar que los controles son eficaces y eficientes tanto en el diseño como en la operación.
* Obtener información adicional para mejorar la valoración del riesgo.
* Analizar y aprender lecciones a partir de los eventos.
* Detectar cambios en el contexto externo e interno, incluyendo los cambios en los criterios de riesgo y en el riesgo mismo que puedan exigir revisión de los tratamientos del riesgo y las prioridades.

Participan todos los procesos e involucran a todos los colaboradores para el levantamiento de los mapas de riesgo, contando con el aporte de los colaboradores con mayor experticia tanto para la identificación como para el tratamiento de riesgos. Cuando se identifica un riesgo el Instituto suministra, comparte u obtiene información a través de un diálogo con las partes involucradas con respecto a la gestión del riesgo. La información está relacionada con la existencia, la naturaleza, la forma, la probabilidad, el significado, la evaluación, la aceptabilidad y el tratamiento de la Gestión de riesgo.

**Comunicación de riesgos**

**3. Mapa de ruta**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***No***  **3. Mapa de Ruta.** | **Actividad** | **Fecha inicio** | **Fecha final** | **Responsable** | **Producto o resultado esperado** |
| ***Riesgos de Seguridad y Privacidad de la Información*** | | | | | |
| *1* | *Socialización de la metodología para el Análisis de Riesgos de Seguridad y Privacidad de la información, Seguridad digital, ciberseguridad y Continuidad y registro en la herramienta institucional* | *Febrero* | *Marzo* | *Equipo SGSI* | *Evidencias de Sensibilización* |
| *2* | *Identificación, documentación y Análisis de Riesgos* | *Abril* | *Junio* | *Todas las áreas y acompañamiento de Equipo SGSI* | *Matriz de Riesgos* |
| *3* | *Definición de planes de tratamiento para la mitigación de los riesgos* | *Abril* | *Junio* | *Todas las áreas y acompañamiento de Equipo SGSI* | *Planes de tratamiento* |
| *4* | *Publicación de riesgos de seguridad de*  *Seguridad y Privacidad de la información, Seguridad digital, ciberseguridad y Continuidad* | *Julio* | *Agosto* | *Equipo SGSI* | *Link de transparencia* |
| *5* | *Gestión y seguimiento a la ejecución de los planes de Tratamiento definidos* | *Agosto* | *Diciembre* | *Todas las áreas y acompañamiento de Equipo SGSI* | *Actas de reunión / correos*  *Electrónicos / Reporte de Evidencias* |
| *6* | *Validación y medición de la efectividad de los controles y planes implementados* | *Febrero* | *Diciembre* | *Equipo SGSI* | *Informe parcial de ejecución de controles* |
| *7* | *Informe de Seguimiento y gestión de los riesgos de Seguridad y Privacidad de la información, Seguridad digital, ciberseguridad y Continuidad* | *Noviembre* | *Diciembre* | *Equipo SGSI – Oficina de Control Interno* | *Informe Final de la gestión de riesgos* |
| *8* | *Presentación de los riesgos en la revisión por la Dirección.* | *Junio* | *Diciembre* | *Equipo SGSI* | *Acta de Reunión* |