

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página 1 de 18

<b>Firma de Autorizaciones</b>		
<b>Elaboró</b>	<b>Revisó</b>	<b>Aprobó</b>
María Alejandra Suarez Contratista Oficina Asesora de Planeación	Lira Pineda Contratista Oficina Asesora de Planeación  Miguel Leonardo Calderón Marín Jefe Oficina Asesora de Planeación y Finanzas	<b>Comité Institucional de            Gestión y Desempeño</b>
<b>Control de Cambios</b>		
<b>Fecha</b>	<b>Descripción</b>	
Noviembre de 2018	Creación del documento	
Febrero de 2019	Se incluye fecha de aprobación de la política.	
Mayo de 2019	Se actualiza el alcance y la política de seguridad y privacidad de la información y se incluye como herramienta para su implementación la firma del compromiso de cumplimiento de las políticas TIC del IDEP	
Noviembre de 2021	Se reestructura la Política de seguridad y privacidad de la información y se incluye el manejo de la información según las TRD.	
Abril de 2023	Se actualiza la Política de seguridad y privacidad de la información por el cambio de sede.	
Agosto de 2024	Se alinea la política a la estructura documental de la entidad, estableciendo actividades mediables y ejecutables para la vigencia 2024	

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página <b>2</b> de <b>18</b>

## TABLA DE CONTENIDO

<b>1</b>	<b>OBJETIVO .....</b>	<b>3</b>
<b>2.</b>	<b>ALCANCE .....</b>	<b>3</b>
<b>3.</b>	<b>REFERENCIAS NORMATIVAS.....</b>	<b>3</b>
<b>4.</b>	<b>DOCUMENTOS ASOCIADOS.....</b>	<b>4</b>
<b>5.</b>	<b>DEFINICIONES .....</b>	<b>4</b>
<b>6.</b>	<b>DECLARACIÓN DE LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN .....</b>	<b>7</b>
<b>6.1.</b>	<b>Roles y Responsabilidades.....</b>	<b>8</b>
<b>6.2.</b>	<b>Políticas Organizacionales.....</b>	<b>11</b>
<b>6.3.</b>	<b>Política del Recurso Humano .....</b>	<b>14</b>
<b>6.4.</b>	<b>Políticas de Control Físico.....</b>	<b>15</b>
<b>6.5.</b>	<b>Políticas de Control Tecnológico .....</b>	<b>16</b>
<b>7.</b>	<b>VIGENCIA .....</b>	<b>18</b>

 <p><b>ALCALDÍA MAYOR DE BOGOTÁ D.C.</b> EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>Política de Seguridad y Privacidad de la Información</b></p>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página 3 de 18

## 1 OBJETIVO

Establecer directrices para gestionar la seguridad de la información/digital en el Instituto para la Investigación Educativa y el Desarrollo Pedagógico IDEP, garantizando la protección adecuada de los activos de información, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información y sus activos relacionados.

## 2. ALCANCE

Las políticas de seguridad de la información aplican a todos los procesos del IDEP y deben ser cumplidas y aplicadas por los directivos, funcionarios, contratistas y terceros relacionados con el IDEP.

## 3. REFERENCIAS NORMATIVAS

Normatividad	Entidad	Descripción
Acuerdo 002 de 2023	Comisión Distrital de Transformación Digital	Por la cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.
Resolución 500 de 2021	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	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.
Decreto 620 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Directiva 002 de 2020	Presidencia de la Republica	Medidas para atender la contingencia generada por el covid-19, a partir uso de las tecnologías la información y las telecomunicaciones - TIC
CONPES 3995 de 2020.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política Nacional de Confianza y Seguridad Digital.
Decreto 612 de 2018	Presidencia de la Republica	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
CONPES 3854 de 2016.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política de Seguridad Digital del Estado Colombiano

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página 4 de 18

Normatividad	Entidad	Descripción
Ley 1581 de 2012	Congreso de Colombia	Por la cual se dictan disposiciones generales para la protección de datos personales

#### 4. DOCUMENTOS ASOCIADOS

- Plan de Seguridad y Privacidad de la Información
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones

#### 5. DEFINICIONES

Las definiciones que se relacionan a continuación fueron tomadas de la Ley 1581 de 2012, el modelo de seguridad y privacidad de la información y la serie ISO 27000

- **Activo de información:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- **Amenaza:** causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.
- **Análisis de riesgos:** proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
- **Anonimizar el dato:** eliminar o sustituir algunos nombres de personas (naturales o jurídicas); direcciones y demás información de contacto que no sea de carácter público.
- **Autenticidad:** propiedad de que una entidad es lo que afirma ser. (ISO 27000).
- **Ciberespacio:** ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).
- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.
- **CoICERT:** Grupo de Respuesta a Emergencias Cibernéticas de Colombia
- **Custodio de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado, que tiene la responsabilidad de administrar y hacer efectivos los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.
- **Dato público:** es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos


	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página 5 de 18

en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Etiquetado de la información:** Acción de agregar etiquetas visibles a documentos y datos que indiquen su clasificación y cualquier restricción de acceso o manejo
- **Evento de seguridad de la información:** ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.
- **Gestión de incidentes de seguridad de la información:** proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.
- **Información electrónica:** La información electrónica se refiere a cualquier dato o contenido que es creado, almacenado, procesado, o transmitido usando dispositivos electrónicos. Esto incluye una amplia gama de formatos y medios, tales como:
  - Documentos escaneados: Documentos físicos que se han convertido en imágenes digitales mediante un escáner.
  - Archivos electrónicos: Archivos almacenados en formatos electrónicos, como documentos de texto (DOCX, PDF), hojas de cálculo (XLSX), y presentaciones (PPT).
  - Correos electrónicos: Mensajes enviados y recibidos a través de sistemas de correo electrónico.
  - Bases de datos: Conjuntos de datos almacenados en sistemas de gestión de bases de datos.

La característica principal de la información electrónica es que depende de dispositivos electrónicos para ser creada, almacenada y gestionada.


- **Información digital:** La información digital es un subconjunto de la información electrónica y se refiere específicamente a datos y contenidos que están codificados en formato binario, lo que permite su procesamiento y manipulación por sistemas computacionales. Ejemplos de información digital incluyen:
  - Archivos digitales: Todos los tipos de archivos que están en formato digital,

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página 6 de 18

- como imágenes (JPEG, PNG), audio (MP3, WAV), y video (MP4, AVI).
- Contenido web: Páginas web, blogs, y otros contenidos disponibles en internet.
- Datos en sistemas digitales: Información almacenada y procesada en sistemas digitales, como bases de datos relacionales y sistemas de información.

La característica distintiva de la información digital es que está codificada en un formato que puede ser fácilmente procesado por computadoras y otros dispositivos digitales.

- **Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la información.
- **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 27000)
- **Inteligencia Artificial (IA):** es una rama de la informática que se centra en la creación y el uso de sistemas capaces de realizar tareas que normalmente requieren la inteligencia humana. Estas tareas pueden incluir el aprendizaje, el razonamiento, la resolución de problemas, la percepción y el uso del lenguaje. La IA puede ser utilizada en una variedad de aplicaciones.
- **Modelo de Seguridad y Privacidad de la Información -MSPI-:** Es el modelo que imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.
- **No repudio:** servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).
- **Plan de recuperación ante desastres (DRP):** Plan de connotación técnica, que describe cómo se deben de ejecutar diferentes acciones para reestablecer la operación de tecnologías de información y comunicaciones, después de una situación de interrupción o de crisis, catalogada como desastrosa.  
Es parte de la planificación de la continuidad del negocio y se aplica a los aspectos de una organización que dependen de una infraestructura de TI para funcionar.
- **Propietario de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.
- **Riesgo de seguridad de la información:** posibilidad de que una amenaza

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página 7 de 18

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 consideraciones.


- **Seguridad digital:** según la norma ISO/IEC 27001, se refiere al conjunto de prácticas y controles diseñados para proteger la información y los sistemas de información de una organización contra amenazas internas y externas
- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información física, electrónica y digital.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basado en un enfoque de gestión y de mejora a un individuo o entidad.
- **Trazabilidad:** cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sea asociada de modo inequívoco a un individuo o entidad. Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas.
- **Tecnologías de información y comunicaciones (TIC):** Son herramientas, relacionadas con los dominios del conocimiento de la ingeniería de sistemas, electrónica, telemática o similares; que se utilizan, desarrollan y apropian en las instituciones, para mejorar y lograr efectividad y eficiencia en la ejecución de sus procesos misionales y de soportes.

Las Tecnologías de Información y Comunicaciones (TIC) se refieren al uso de tecnologías de computación y telecomunicaciones, sistemas y herramientas para facilitar la forma en que se crea, recopila, procesa, transmite y almacena la información

## 6. DECLARACIÓN DE LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto para la Investigación Educativa y el Desarrollo Pedagógico (IDEP) entiende la importancia de una gestión eficiente de la información, por ello es esencial la implementación de medidas, controles e instrumentos que aseguren y demuestren una adecuada gestión de los riesgos relacionados con la seguridad y privacidad de la información. La entidad establecerá un marco de confianza que respalde el cumplimiento de nuestras responsabilidades con el Estado y la ciudadanía, en cumplimiento con la normativa vigente y en consonancia con nuestra misión y visión institucional.

El IDEP se compromete a proteger y salvaguardar sus activos de información, minimizando el impacto de los riesgos identificados; el enfoque se centra en mantener un

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página <b>8</b> de <b>18</b>

nivel de exposición que garantice la integridad, confidencialidad y disponibilidad de la información, de acuerdo con las necesidades de nuestros diversos grupos de interés.

En este sentido, el IDEP implementará una política de seguridad y privacidad de la información, respaldada por directrices alineadas con las necesidades de la entidad y los requisitos regulatorios. Esta política abarca toda la información gestionada en el contexto de los procesos y proyectos de la entidad, destacando el compromiso de la Dirección en la implementación del Modelo de Seguridad y Privacidad de la Información

### **6.1. Roles y Responsabilidades**

A continuación, se describen los roles y responsabilidades de la seguridad de la información para el Instituto para la Investigación Educativa y el Desarrollo Pedagógico (IDEP):

#### **Comité Institucional de Gestión y Desempeño**

Es la instancia encargada de realizar la revisión, seguimiento y aprobación de la implementación, mantenimiento y mejora continua del Modelo Integrado de Planeación y Gestión, entre ellos el Sistema de Gestión de Seguridad de la Información (SGSI), cuando la entidad tome decisiones respecto a su implementación.


#### **Oficial de Seguridad de la Información**

El oficial de seguridad de la información o quien sea delegado por la Dirección será el encargado de las siguientes responsabilidades

- Responsable de presentar al Comité Institucional de Gestión y Desempeño la documentación, estrategias y propuestas para el mantenimiento y fortalecimiento del SGSI, así como liderar la implementación, mantenimiento y mejora de este con el fin de fomentar una cultura de la seguridad de la información en el IDEP.
- Definir y apoyar la implementar las políticas y controles de seguridad de la información, entre otras y asociadas a la seguridad y privacidad de la información institucional.
- Reportar incidentes a las instancias correspondiente (CoICERT, SIC) como primer canal de contacto.

#### **Oficina Asesora de Planeación**

Responsable de apoyar a los líderes de proceso en la realización de los cambios necesarios en los procesos y la operación de la Entidad para ajustarlos y alinearlos al

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página <b>9</b> de <b>18</b>

Modelo Integrado de Planeación y Gestión (MIPG) y al Sistema de Seguridad de la Información (SGSI), así como apoyar el proceso de su documentación.

### **Líderes de Proceso y Equipos de Trabajo**

Encargados de cumplir con las políticas, lineamientos, procesos y procedimientos del Sistema de Gestión de Seguridad de la Información (SGSI). Los líderes de procesos y equipos de trabajo son responsables de velar por la protección de los activos de información y controlar la producción, desarrollo, mantenimiento, uso, seguridad y actualización de estos.

### **Proceso de Gestión Tecnológica**


Este proceso se encuentra a cargo de la Oficina Asesora de Planeación y tendrá a cargo lo siguiente:

- Implementar las políticas y controles de seguridad informática, en lineamiento con las políticas y demás directrices que se establezcan.
- Gestionar los incidentes de seguridad informática.
- Supervisar las acciones de mejora continua en el Sistema de Gestión de Seguridad de la Información (SGSI).
- Proponer al Comité Institucional de Gestión y Desempeño la política institucional de seguridad y privacidad de la información y coordinar su implementación a través del Oficial de Seguridad.
- Monitorear el cumplimiento de las directrices definidas en la política institucional de seguridad y privacidad de la información.
- Definir e implementar la estrategia de continuidad para los servicios tecnológicos, o el plan de recuperación ante desastres de la plataforma tecnológica.
- Presentar al Comité Institucional de Gestión y Desempeño los resultados obtenidos en la implementación de la política de seguridad y privacidad de la información.

### **Subdirección Administrativa y Financiera**

Esta subdirección a través de sus funciones deberá:

- Coordinar la seguridad y los accesos físicos en las instalaciones del IDEP.
- Gestionar los activos físicos de la entidad a través de procedimientos y lineamientos.
- Atender los incidentes y eventos de seguridad que se presenten en los activos de información físicos.

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página <b>10</b> de <b>18</b>

- Atender, gestionar y direccionar las PQRSD (Petición, Queja, Reclamo, Sugerencia, Denuncia, Felicitación, Agradecimiento y Acción de Tutela) que lleguen al IDEP dentro de los términos legales vigentes. Además de dar a conocer al ciudadano las políticas del Sistema de Gestión de Seguridad de la Información (SGSI) cuando sea requerido.
- Coordinar y ejecutar los programas de Inducción y Reinducción dentro del Plan Institucional de Capacitación, donde se comunicará a los servidores públicos y contratistas los lineamientos de seguridad de la información, las obligaciones respecto al cumplimiento de las políticas de seguridad y privacidad de la información y la protección de datos personales.
- Orientar los lineamientos para que se reporte oportunamente el retiro de funcionarios.
- Definir las directrices necesarias para la implementación de la política de gestión documental del IDEP, incluyendo la gestión de documentos electrónicos y mecanismos de firma digital, electrónica y/o complementarios; en consideración a las directrices de los organismos competentes en la materia.

### **Oficina Jurídica**

Es la dependencia responsable de atender asuntos de carácter legal, frente al cumplimiento de la normatividad relacionada con la seguridad de la información, protección de datos personales, transparencia y acceso a la información pública, entre otras.

Incorporar en el modelo de los contratos cláusulas y obligaciones sobre el cumplimiento de las políticas de seguridad, privacidad y confidencialidad, sus procedimientos y los acuerdos de confidencialidad correspondientes.

Verificará el cumplimiento de la presente política en la gestión de todos los contratos o acuerdos del IDEP con colaboradores o terceros.

### **Oficina de Control Interno**

El jefe de la Oficina de Control Interno velará por:

- Evaluar y realizar seguimiento al cumplimiento de las políticas, planes y requisitos de seguridad de la información, auditar el SGSI y presentar los hallazgos correspondientes.

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página 11 de 18

## Oficina de Control Disciplinario Interno

El jefe de la Oficina de Control Disciplinario velará por:

- Llevar a cabo las investigaciones necesarias por incumplimiento de los lineamientos y políticas definidas en seguridad de la información para el IDEP.

## 6.2. Políticas Organizacionales

### Gestión de Activos de Información


El IDEP, con el liderazgo de la Dirección General y el trabajo articulado con la Oficina Asesora de Planeación a través del proceso de gestión tecnológica y las demás dependencias, realizará la identificación, clasificación y etiquetado de los activos de información digitales y electrónicos del Instituto, mediante la metodología que se establezca.

- Los funcionarios y contratistas deberán evitar la divulgación, modificación, retiro y destrucción no autorizada de información almacenada en los medios accesibles.
- Todo funcionario y contratista que se desvincule temporal o definitivamente del IDEP deberá realizar la devolución de activos de información que tenga asignados y en custodia, físico o virtual, al supervisor o jefe inmediato, de acuerdo con los lineamientos definidos para tal fin.
- La información almacenada en los equipos de cómputo es responsabilidad de quien use el equipo; la Oficina Asesora de Planeación a través del Proceso de Gestión Tecnológica hará mantenimiento a dichos equipos y eliminará los archivos en intervalos planificados.
- El IDEP definirá el acuerdo de confidencialidad de la información, el cual debe ser adoptado por los interesados que tengan acceso a activos de información institucional durante la ejecución contractual.

### Control de Acceso

La Oficina Asesora de Planeación a través del Proceso de Gestión Tecnológica en articulación con las áreas gestionará lo siguiente:

- La creación, reactivación o desactivación de usuarios de la red o de los sistemas de información, así como la asignación de roles y permisos, será responsabilidad del proceso de gestión tecnológica, conforme al procedimiento establecido para tal fin.
- Los supervisores de contratistas con acceso a las plataformas tecnológicas de la entidad deben informar a la Oficina Asesora de Planeación, a través del Proceso

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página <b>12</b> de <b>18</b>

de Gestión Tecnológica, sobre cualquier novedad relacionada con la suspensión o terminación contractual, para que se realicen las modificaciones de acceso necesarias.

- La Oficina Asesora de Planeación a través del Proceso de Gestión Tecnológica gestionará el control de acceso mediante usuario y contraseña a la red de la entidad, correo electrónico y a los sistemas de información administrados, diligenciando por cada usuario el formato dispuesto para tal fin.
- En caso de retiro temporal o definitivo de cualquier servidor público o contratista, se deberá deshabilitar los privilegios en los sistemas y actualizarlos en caso de encargos o suplencia temporal, previa solicitud por correo electrónico enviada por el jefe inmediato y/o supervisor al Jefe de la Oficina Asesora de Planeación.
- La Oficina Asesora de Planeación a través del Proceso de Gestión Tecnológica debe mantener actualizada la documentación relacionada con la administración de usuarios y monitoreará la asignación de permisos y roles otorgados a los usuarios.
- Las contraseñas serán de uso personal e intransferible y deberán ser cambiadas con frecuencia. Se evitará que las contraseñas sean fáciles de recordar o basadas en información personal, y se garantizará que no sean vulnerables a ataques de diccionario. Si son temporales, deberán ser cambiadas la primera vez que se ingrese.
- Es responsabilidad del funcionario o contratista el uso dado a su usuario y contraseña.
- La Oficina Asesora de Planeación a través del Proceso de Gestión Tecnológica asegurará la configuración el servicio de autenticación para que trimestralmente el sistema solicite al usuario cambio de contraseña.
- No se recomienda el uso de la opción 'recordar contraseña en las plataformas tecnológicas'.
- La instalación de software en los equipos de cómputo del IDEP será realizada a través del usuario del administrador de la red. Toda solicitud deberá gestionarse a través de la Oficina Asesora de Planeación a través del Proceso de Gestión Tecnológica, quien aprobará su instalación.

## **Seguridad de la información para el uso de servicios en la nube**

El IDEP deberá:

- Mantener la confidencialidad de la información almacenada en la nube mediante controles de acceso sólidos y autenticación segura.
- Garantizar la integridad de los datos almacenados en la nube mediante prácticas de cifrado y medidas de seguridad contra la alteración no autorizada.
- Asegurar la disponibilidad constante de los datos y servicios en la nube mediante copias de seguridad periódicas, probadas y planes de recuperación ante desastres de la plataforma tecnológica, adecuados a las necesidades de la entidad.
- Evaluar y gestionar de forma regular los riesgos asociados al uso de servicios en la nube, implementando medidas preventivas y correctivas según sea necesario.

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página 13 de 18

Los usuarios de servicios en la nube utilizarán exclusivamente los aprobados por el proceso de gestión tecnológica.

### **Cumplimiento normativo, Privacidad y protección de datos personales**

- Propender la identificación, documentación y cumplimiento de las obligaciones legales, estatutarias y demás normatividad vigente relacionadas con seguridad y privacidad de la información, orientada a la protección de los datos personales de sus colaboradores, beneficiarios y partes interesadas.
- Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software registrados, patentados y los desarrollados internamente por la entidad.
- Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación en la materia.
- Realizar revisión del SGSI al momento de su implementación, para identificar su adecuada implementación y operación conforme a las políticas definidas.

### **Relación con los Proveedores**

El IDEP debe:

- Establecer y documentar los requisitos de seguridad y privacidad de la información con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información del IDEP.
- Cuando sea el caso, requerir al proveedor planes de continuidad de negocio, certificaciones asociadas a la seguridad y privacidad de la información y planes de recuperación ante desastres; que permitan garantizar el cumplimiento de los postulados de confidencialidad, integridad y disponibilidad de la información, así como la continuidad de las operaciones de acuerdo con los acuerdos de niveles de servicios contratados.
- Realizar seguimiento, revisión y auditoría regular de la prestación de servicios de los proveedores.

### **Gestión de Eventos e Incidentes de Seguridad de la Información**

El IDEP debe:

- Establecer las responsabilidades y procedimientos de gestión para una respuesta rápida, eficaz y ordenada ante los eventos e incidentes de seguridad de la información. Todos los colaboradores deben reportar los eventos e incidentes de seguridad de la información a la Oficina Asesora de Planeación a través del

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página <b>14</b> de <b>18</b>

Proceso de Gestión Tecnológica tan pronto como tengan conocimiento de estos o sospechen de alguno.

- Definir y aplicar procedimientos para preservar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información con el fin de ser utilizado en la reducción de la posibilidad o el impacto de incidentes futuros.
- Definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información de los incidentes de seguridad de la información que pueda servir como evidencia.

### **Aspectos de Seguridad de la Información en la Continuidad de los Servicios TI**

El IDEP deberá:

- Determinar los aspectos de la continuidad de la gestión de la seguridad de la información en situaciones adversas, durante una crisis o desastre, incluyendo el cumplimiento de los requisitos de disponibilidad.
- Identificar, documentar, implementar y mejorar de manera continua los procesos para asegurar el nivel de continuidad requerido por el IDEP.
- Verificar a intervalos planificados los controles de continuidad implementados, validando su adecuado funcionamiento.

### **6.3. Política del Recurso Humano**

Los funcionarios, contratistas, proveedores y cualquier persona que tenga acceso a los recursos tecnológicos y activos de información institucional deben propender por la protección, confidencialidad, integridad y disponibilidad de la información manejada, cumpliendo con los estándares establecidos:


#### **Proceso de selección, durante y después del cargo:**

- Integrar los principios de seguridad de la información en los procesos de selección y contratación.
- Establecer los acuerdos de confidencialidad y no divulgación de la información.

#### **Gestión de la Información:**

- Todos los funcionarios, contratistas y cualquier persona que tenga acceso a los recursos tecnológicos son responsables de salvaguardar la información confidencial y crítica de la entidad.
- Los líderes de proceso deben fomentar una cultura de seguridad de la información y proporcionar el apoyo necesario para su implementación.

#### **Formación y Concientización:**

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página 15 de 18

- Se proporcionará formación regular sobre seguridad de la información a todos los empleados.
- Todos los funcionarios, contratistas y cualquier persona que tenga acceso a los recursos tecnológicos deben estar al tanto de las políticas, normativas y procedimientos relacionados con la seguridad de la información.

#### **Uso Apropiado de los Recursos:**

- Los funcionarios, contratistas y cualquier persona que tenga acceso a los recursos tecnológicos deben utilizar los recursos de información de manera responsable y ética.
- Se deben seguir las pautas establecidas para el uso de dispositivos, sistemas y datos del IDEP.
- Se debe utilizar el almacenamiento y repositorio institucional de información, manteniéndola organizada en los medios respectivos para asegurar su portabilidad y acceso dentro del instituto.

#### **Gestión de Acceso:**

- El acceso a la información estará restringido según las funciones y responsabilidades laborales.
- Se deben seguir los protocolos de autenticación y autorización para acceder a sistemas y datos sensibles.

#### **Reporte de Incidentes:**

- Todos los incidentes relacionados con la seguridad de la información deben ser reportados inmediatamente al oficial de seguridad por los medios establecidos.

#### **Acceso remoto a los activos de información:**

- Utilizar conexiones VPN seguras para acceder a los recursos de la organización desde ubicaciones remotas, en caso de ser requerido.
- Implementar sin excepción el doble factor de autenticación para fortalecer la autenticación y garantizar el acceso autorizado a sistemas y datos institucionales. En los casos que puedan ser parametrizables.
- Mantener actualizados los sistemas operativos y aplicaciones con los últimos parches de seguridad.
- Hacer uso de las herramientas de ofimática dispuesta por la entidad, para transferencia, comunicación y almacenamiento de la información institucional.

#### **6.4. Políticas de Control Físico**

El IDEP, a través de la Subgerencia de Gestión Administrativa, velará por:

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página <b>16</b> de <b>18</b>

- Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información.
- Diseñar y aplicar la protección contra desastres naturales, ataques maliciosos y accidentes para evitar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre.


Así mismo, el proceso de gestión tecnológica:

- Deberá establecer y ejecutar los planes de mantenimiento de equipos.
- Apoyará los lineamientos sobre la disposición o reutilización segura de los equipos de cómputo.

## 6.5. Políticas de Control Tecnológico

**Seguridad de las Operaciones:** El IDEP, a través del Proceso de Gestión Tecnológica, velará por:

- Documentar, aplicar y poner a disposición los procedimientos de operación de los servicios tecnológicos.
- Hacer seguimiento y gestión a los cambios en las instalaciones y sistemas de procesamiento de información que afectan la seguridad de la información.
- Separar los ambientes de desarrollo, prueba y producción para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.
- Hacer seguimiento al uso de los recursos tecnológicos, hacer los ajustes y proyecciones de los requisitos sobre la capacidad futura.
- Asegurar que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
- Implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
- Hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
- Elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
- Registrar las actividades del administrador y del operador del sistema, revisándolas con regularidad.
- Sincronizar los relojes de todos los sistemas de procesamiento de información con una única fuente de referencia de tiempo.
- Implementar políticas para controlar la instalación de software en los equipos de cómputo.

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página 17 de 18

- Obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades y tomar las medidas apropiadas para tratar el riesgo asociado.


**Seguridad de las comunicaciones:** Asegurar la protección de la información en las redes e infraestructura de procesamiento de información, a través de documentación y controles efectivos que permitan conexiones seguras para los fines institucionalmente establecidos.

**Uso y aplicación de herramientas o componentes de Inteligencia Artificial – IA:** El IDEP propenderá por el uso ético y responsable de herramientas, sistemas de información o componentes tecnológicos basados en Inteligencia Artificial para mejorar la productividad y acceso al conocimiento de sus colaboradores. En el uso de estas herramientas y tecnologías, los colaboradores serán responsables en todo momento por la salvaguarda de la información institucional, personal y de la protección y buen uso de los derechos de propiedad intelectual de las fuentes de datos y de información con las que interactúen y de los propios del IDEP. Los colaboradores del IDEP no podrán publicar o suministrar información institucional a motores o herramientas de inteligencia artificial o terceros de tipo gratuita.

**Desarrollo y Mantenimiento de Sistemas:** De manera armónica durante el desarrollo y mantenimiento de los sistemas de información, se tendrán en cuenta los siguientes aspectos:

- Conocer e implementar la guía de estilo e imagen institucional en aspectos en los que aplique para el desarrollo de los sistemas de información.
- Garantizar ambientes seguros de desarrollo, pruebas y producción.
- Todo sistema de información o desarrollo de software debe poseer un plan de pruebas de calidad que incluya pruebas de seguridad.
- Establecer y documentar la arquitectura para sistemas de información seguros.
- Generar las copias de seguridad de acuerdo con los lineamientos que defina el proceso de gestión tecnológica.
- Mantener actualizada la documentación de los desarrollos realizados y estándares que se emplearán.
- Establecer un plan para el análisis y tratamiento de vulnerabilidades en los sistemas de información.
- Establecer como obligación específica a los proveedores en sus contratos la entrega de la documentación necesaria para la administración y funcionamiento de los sistemas de información.

**Criptografía y Prevención de fuga de datos:** La entidad adoptará mecanismos de cifrado avanzados para asegurar la confidencialidad de la información, comprometiéndose a utilizar algoritmos robustos y actualizados que cumplan con los estándares de seguridad. Además, implementará un conjunto integral de medidas destinadas a prevenir la fuga de

	<b>Política de Seguridad y Privacidad de la Información</b>	Código: PO-GT-12-01
		Versión: 6
		Fecha de Aprobación: 01/08/2024
		Página <b>18</b> de <b>18</b>

datos. Esto incluye el fortalecimiento de los controles de acceso, garantizando que solo el personal autorizado tenga acceso a información sensible, y el establecimiento de protocolos estrictos para la transferencia segura de dicha información, tanto interna como externamente.

## 7. VIGENCIA

La presente política de seguridad y privacidad de la información cuenta con la revisión y aprobación del Comité Institucional de Gestión y Desempeño del 01/08/2024. Será revisada a intervalos planificados, o cuando se produzcan cambios significativos en los procesos, infraestructura física o tecnológica, o todo aspecto que afecte la misionalidad del Instituto para la Investigación Educativa y el Desarrollo Pedagógico (IDEP).