## Tabla de Contenido

# INTRODUCCIÓN

El Ministerio de las Culturas, las Artes y los Saberes (en adelante el "Ministerio" o la "Entidad"), con el fin de lograr el cumplimiento normativo de las diferentes estrategias y legislaciones que le aplican a las Entidades del Estado en el desarrollo de sus funciones, para los temas relacionados con la administración y protección de la información en cada una de sus dimensiones como la disponibilidad, integridad y confidencialidad, ha elaborado una serie de acciones para la implementación de un Subsistema de Gestión de Seguridad de la Información (SGSI) alineado con los objetivos estratégicos de la Entidad.

Este documento describe la política general de seguridad y privacidad de la información, los lineamientos generales, los requerimientos legales y las responsabilidades tanto de la alta dirección como de los propietarios de los activos y en general todos los funcionarios, contratistas y terceros que intervengan en la generación, tratamiento y almacenamiento de la información del Ministerio.

## 0. LISTA DE VERSIONES

| VERSIÓN | FECHA | RAZÓN DE LA ACTUALIZACIÓN |
|---|---|---|
| 0 | 18/10/2024 | Creación del documento resultado de la actualización de la Política, el cual anteriormente era Documento interno código DI-GSI-003 Nombre Política General de Seguridad y privacidad de la Información V5.<br>Se actualizó la estructura conforme la actualización de la ISO 27001:2022, en<br>*Políticas Organizacionales<br>* Política del Recurso Humano<br>* Políticas de Control Físico<br>* Políticas de Control Tecnológico<br>Se complementó la redacción de la Política general de seguridad y privacidad de la información y se suprimieron los roles y responsabilidades de los usuarios externos.<br>La presente política fue revisada y aprobada en el marco del 3er. Comité Institucional de Gestión y Desempeño (Revisión por la Dirección), llevado a cabo el 4/10/2024.<br>**Nota.** El documento hasta en versión 4, pertenecía al proceso Mejoramiento Continuo con código DI-OPL-003. |

## 1. OBJETIVO GENERAL

Establecer las directrices y lineamientos requeridos para proteger la información y los sistemas de información donde se administra, produce, procesa y/o transforma la información del Ministerio y de los ciudadanos en los diferentes procesos; ante cualquier amenaza que pueda comprometer la confidencialidad, disponibilidad e integridad de dicha información.

## 2. OBJETIVOS ESPECÍFICOS

### 2.1. Gestionar los riesgos

Gestionar los Riesgos de seguridad de la información de forma oportuna por medio de controles, ayudando a reducir los impactos negativos de su materialización.

### 2.2. Reducir los incidentes

Reducir los Incidentes de Seguridad de la Información que afecten el normal funcionamiento del Ministerio.

### 2.3. Fomentar cultura

Fomentar una cultura y apropiación de seguridad y privacidad de la información en los colaboradores del Ministerio frente al SGSI, con el fin

de que estos tomen conciencia de sus deberes y responsabilidades al proteger los activos de información, controlar los riegos y reducir el impacto que pueda generar su materialización.

## 3. ALCANCE

La Política General de Seguridad y Privacidad de la información aplica para todos los procesos, sedes, colaboradores y terceros del Ministerio. En consecuencia, es responsabilidad de estos cumplir todos los lineamientos establecidos en el Subsistema de Gestión de Seguridad de la Información (SGSI).

## 4. DEFINICIONES

**Auditabilidad:** Propiedad que asegura que cualquier acción sobre cualquier objeto de seguridad puede examinarse a fin de establecer las responsabilidades reales de la operación.

**Autenticación:** Garantía de que una parte de una transacción informática no es falsa. La autenticación normalmente lleva consigo el uso de una contraseña, un certificado, un número de identificación personal u otra información que se pueda utilizar para validar la identidad en una red de equipos.

**Colaborador:** Empleado, contratista, practicante, proveedor y en general cualquier persona que tenga acceso a información del Ministerio y tenga un vínculo contractual con el mismo.

**Criptografía:** Arte o técnica de escribir con clave secreta o de un modo enigmático.

**No repudio:** Este servicio evita que las entidades que se comunican puedan denegar el haber participado en parte o en toda la comunicación.

**Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

**Procedimiento:** Documento que describe la forma específica de llevar a cabo a una actividad o un proceso.

**Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.

**Seguridad de la Información:** Preservación de la confidencialidad, disponibilidad e integridad de la información (ISO/IEC 27000) independiente de su medio de conservación, transmisión o formato.

**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, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

## 5. MARCO NORMATIVO

- Decreto 338 de 2022. "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".
- Decreto 1499 de 2017 (Ver Decreto 1893 de 2021). Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

## 6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El MINISTERIO reconoce la importancia de gestionar efectivamente la información. Por ello, se compromete a establecer, implementar, mantener y mejorar continuamente un Subsistema de Gestión de Seguridad de la Información (SGSI) que garantice la confidencialidad, disponibilidad e integridad de la información. Esto se logrará mediante la gestión de riesgos, incidentes de seguridad y el cumplimiento de requisitos legales y regulatorios, apoyando así la formulación, coordinación e implementación de la política cultural del Estado colombiano para estimular y promover el desarrollo de procesos,

proyectos y actividades culturales y artísticas que reconozcan la diversidad y protejan el patrimonio cultural de la nación.

Esta política se aplica a la entidad según se defina en el alcance, guiada por los siguientes principios que fundamentan el desarrollo de acciones y la toma de decisiones en torno al SGSI:

- Minimizar el riesgo en las funciones críticas de la entidad.
- Cumplir con los principios de seguridad de la información.
- Preservar la confianza de los ciudadanos, colaboradores y otras entidades.
- Apoyar la innovación tecnológica.
- Proteger los activos de información.
- Establecer políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en funcionarios, terceros, contratistas y demás partes que tengan interacción con el Ministerio.
- Garantizar la continuidad de las tecnologías de la información frente a incidentes.

Con base en lo anterior, establece los siguientes lineamientos para la implementación de la política de seguridad y privacidad del SGSI del Ministerio:

## 6.1. Roles y Responsabilidades

A continuación, se describen los roles y responsabilidades de la seguridad de la información para el Ministerio de las Culturas, las Artes y los Saberes:

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

Como representante de la alta dirección del Ministerio el comité es la Instancia encargada de realizar la revisión, seguimiento y aprobación de la implementación, mantenimiento y mejora continua del Subsistema de Gestión de seguridad de la Información - SGSI.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Responsable de presentar al Comité Institucional de Gestión y Desempeño la documentación, estrategia 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 Ministerio.

Acompañar a las áreas en la Administración del Riesgo, realizando la revisión, análisis y consolidación de la información.

OFICINA ASESORA DE PLANEACIÓN

A través del Sistema integrado de gestión institucional es responsable de asesorar a las áreas en la realización de los cambios a que haya lugar en los procesos, procedimientos, instructivos y formatos de la Entidad para ajustarlos y alinearlos con el Modelo Integrado de Planeación y Gestión - MIPG, el Sistema de Gestión de Seguridad de la Información – SGSI, así como apoyar el proceso de su documentación.

GRUPO GESTIÓN DE SISTEMAS E INFORMÁTICA

- Implementar las políticas y controles de Seguridad informática
- 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 los linimentos definidos en la política institucional de seguridad y privacidad de la información.
- Definir e implementar la estrategia de continuidad para los servicios tecnológicos

GRUPO DE GESTIÓN HUMANA

Encargado de 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.

GRUPO DE CONTRATOS Y CONVENIOS

Encargado de la inclusión y supervisión de cláusulas de seguridad de información en los contratos y verificación de los acuerdos de niveles de servicio; dictar lineamientos para que se reporte oportunamente el retiro de colaboradores.

GRUPO DE GESTIÓN ADMINISTRATIVA Y SERVICIOS

Encargado de coordinar la seguridad y los accesos físicos a las diferentes sedes del Ministerio, gestionar los incidentes de seguridad de la información que no sean informáticos.

OFICINA ASESORA JURÍDICA

- Realizar la asesoría 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.

- Responsable de verificar el cumplimiento de la presente política en la gestión de todos los contratos u acuerdos del Ministerio con colaboradores o terceros.
- Responsable de asesorar en materia legal al Ministerio en temas de seguridad de la información.

OFICINA DE CONTROL INTERNO

Responsables de evaluar y realizar seguimiento al cumplimiento de las políticas, planes y requisitos de Seguridad de la información, auditar el SGSI y presentar los hallazgos.

GRUPO DE CONTROL INTERNO DISCIPLINARIO

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

GRUPO DE SERVICIO AL CIUDADANO

Responsable de dar a conocer al ciudadano las políticas del Subsistema de Gestión de Seguridad de la Información – SGSI.

JEFE – COORDINADOR

Encargado de dar a conocer las políticas de seguridad y privacidad de la información de la información, en el proceso de Inducción al Puesto de Trabajo en el Formato F-GGH-036 INDUCCIÓN Y ENTRENAMIENTO EN EL PUESTO DE TRABAJO. Formato que debe ser remitido al Grupo de Gestión Humana y reposar en la historia laboral de cada funcionario.

SUPERVISOR DE CONTRATO

Encargado de dar a conocer las políticas de seguridad y privacidad de la información del Ministerio, a contratistas y colaboradores en condición de prestación de servicios, con el formato F-GCC-015 FORMATO DE INDUCCIÓN PARA EL DESARROLLO DE LAS OBLIGACIONES CONTRACTUALES Formato que debe ser remitido al Grupo de Contratos y Convenios.

COLABORADORES

- Cumplir con las políticas, lineamientos, procesos, procedimientos y asistir a las sensibilizaciones o capacitaciones del Sistema de Gestión de seguridad de la información SGSI
- Firmar y respetar acuerdos de confidencialidad y contratos que especifiquen las obligaciones respecto a la seguridad de la información.

## 6.2. Políticas Organizacionales

**Gestión de Activos de Información**

- Minculturas con el liderazgo de la Dirección y el trabajo articulado del Grupo Gestión de Sistemas e Informática y los procesos institucionales, realizarán la identificación, clasificación y etiquetado de los activos de información del Ministerio mediante la metodología que se establezca.
- Los funcionarios y contratistas deberán evitar la divulgación, modificación, retiro y destrucción no autorizados de información almacenada en los medios accesibles.
- La información creada, desarrollada o gestionada por los colaboradores del Ministerio se considera un activo fundamental y será propiedad de la entidad. Su divulgación o entrega a terceros estará sujeta a la normativa legal vigente.
- Todo funcionario y contratista que se desvincule temporal o definitivamente del Ministerio 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 portátiles es responsabilidad de quien use el equipo, el Grupo Gestión de Sistemas e Informática hará mantenimiento a dichos equipos y eliminará los archivos en intervalos planificados.

- A través del Grupo de Gestión de Sistemas e Informática se desarrollarán e implementarán procedimientos y lineamientos adecuados para el etiquetado de la información, de acuerdo con el esquema de clasificación adoptado por el Ministerio.

**Control de Acceso**

- La creación, reactivación o desactivación de usuarios de la red o sistemas de información; al igual que los roles y permisos otorgados, los realizará el Grupo de Gestión de Sistemas e Informática a través del procedimiento establecido para tal fin.
- El Grupo de Gestión de Sistemas e Informática gestionará el control de acceso a la red de la Entidad, al correo electrónico y a los sistemas de información que administre, a través de usuario y contraseña.

En caso de retiro temporal o definitivo de cualquier colaborador, se deberán deshabilitar sus privilegios en los sistemas y actualizarlos en caso de encargos o suplencias temporales. Esta acción se realizará previa solicitud por correo electrónico enviada por el jefe inmediato y/o supervisor al Grupo de Gestión de Sistemas e Informática.

- El Grupo de Gestión de Sistemas e Informática 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, deberán ser cambiadas con frecuencia. Evitar que las contraseñas sean fáciles de

recordar; no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.); no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios); estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos; si son temporales, cambiarlos la primera vez que se ingrese.

- Es responsabilidad del funcionario o contratista el uso dado a su usuario y contraseña.
- El administrador de la red/infraestructura configurará el servicio de autenticación para que trimestralmente el sistema solicite al usuario cambio de contraseña.
- No es recomendable el uso de la opción 'recordar contraseña'.
- La instalación de software en los equipos de cómputo del Ministerio será realizada a través del usuario del administrador de la red. Toda solicitud al respecto debe gestionarse a través del Grupo de Gestión de Sistemas e Informática quien aprobará su instalación.

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

El Ministerio velera por:

- Únicamente se seleccionarán proveedores de servicios en la nube que cumplan con estándares de seguridad reconocidos y que hayan sido

evaluados y aprobados por el Grupo de Gestión de Sistemas e Informática

- Mantener la confidencialidad de la información almacenada en la nube a través de 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 y planes de recuperación ante desastres.
- Evaluar y gestionar de forma regular los riesgos asociados al uso de servicios en la nube, implementando medidas preventivas y correctivas según sea necesario.
- Los colaboradores utilizarán exclusivamente servicios en la nube aprobados y licenciados por la entidad.

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

- Promover la identificación, documentación y cumplimiento de las obligaciones legales, estatutarias y demás normativas vigentes relacionadas con la seguridad de la información, así como de cualquier requisito de seguridad.

- 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 patentados.
- Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación en materia.
- Definir e implementar una política de privacidad, tratamiento y protección de datos personales.

## Relación con los Proveedores

El Ministerio debe:

- Establecer y documentar los requisitos de seguridad de la información con los proveedores que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la entidad.
- Cuando sea el caso, requerir al proveedor planes de continuidad y recuperación de desastres que le permitan prestar en forma continua el servicio contratado.
- Realizar seguimiento y revisar con regularidad la prestación de servicios de los proveedores.

## Gestión de Incidentes de Seguridad de la Información

El Ministerio debe:

- Establecer responsabilidades y procedimientos para una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. Todos los colaboradores deben reportar cualquier incidente o sospecha de incidente de seguridad al Grupo de Gestión de Sistemas e Informática tan pronto como tengan conocimiento de ello
- Definir y aplicar procesos para preservar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información con el fin de ser usado 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 Ministerio debe:

- Determinar los aspectos de la continuidad de la gestión de la seguridad de la información en situaciones adversas, durante una crisis o desastre entre ellas el cumplimiento de los requisitos de disponibilidad.

- Identificar, documentar, implementar y mejorar de manera continua los procesos y procedimientos para asegurar el nivel de continuidad requerido por el Ministerio.
- 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:

**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 son responsables de salvaguardar la información confidencial y crítica de la entidad.

- Los jefes/coordinadores de área, así como líderes de proceso deben fomentar una cultura de seguridad de la información y proporcionar el apoyo necesario para su implementación.

## Formación y Concientización

- Se proporcionará formación regular sobre seguridad de la información a todos los empleados.
- Todos los colaboradores deben estar al tanto de las políticas, normativas y procedimientos relacionados con la seguridad de la información.

## Uso Apropiado de los Recursos

- Los colaboradores deben utilizar los recursos de información de manera responsable y ética.
- Se deben seguir las pautas establecidas para el uso de dispositivos, sistemas de información, recursos tecnológicos y datos del Ministerio.

## 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 de la información o a la mesa de ayuda.

**Trabajo en casa**

- Utilizar conexiones VPN seguras para acceder a los recursos de la organización desde ubicaciones remotas.
- Implementar sin excepción el doble factor de autenticación para fortalecer la autenticación y garantizar el acceso autorizado a sistemas y datos institucionales.
- Mantener actualizados los sistemas operativos y aplicaciones con los últimos parches de seguridad.
- Hacer uso de las herramientas de Microsoft 365 para transferencia, comunicación y almacenamiento de la información institucional.

## 6.4. Políticas de control físico

El Ministerio de las Culturas, las Artes y los Saberes a través del Grupo de Gestión Administrativa y de Servicios velará por:

- 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 medidas de protección contra desastres naturales, ataques maliciosos y accidentes, para evitar daños por incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre.

Así mismo desde el Grupo de Gestión de Sistemas e Informática

- Se deberán establecer y ejecutar planes de mantenimiento de equipos.
- Se apoyarán los lineamientos sobre la disposición o reutilización segura de los equipos de cómputo.

## 6.5 Políticas de control tecnológico

**Seguridad de las Operaciones**

El Ministerio a través del Grupo de Gestión de Sistemas e Informática velará por:

- Documentar, aplicar y poner a disposición los procedimientos de operación de los servicios tecnológicos.
- Realizar el seguimiento y gestión a los cambios en las instalaciones y sistemas de procesamiento de información que afectan la seguridad de la información.
- Hacer seguimiento al uso de los recursos tecnológicos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.

- Asegurarse que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
- Implementar controles de detección, prevención y de 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 procedimientos para controlar la instalación de software en sistemas operativos
- 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.

## Desarrollo y Mantenimiento de Sistemas

Establecer las directrices generales para el desarrollo y mantenimiento de sistemas de información. De manera armónica, durante estas actividades se tendrán en cuenta los siguientes aspectos:

- Implementar la guía de estilo e imagen institucional en los aspectos aplicables al desarrollo de sistemas de información.
- Garantizar ambientes seguros de desarrollo, pruebas y producción.
- Incluir un plan de pruebas de calidad, que contemple pruebas de seguridad, para todo sistema de información o desarrollo de software.
- Establecer y documentar una arquitectura segura y principios de ingeniería para los sistemas de información.
- Mantener actualizada la documentación de los desarrollos realizados y los estándares empleados.
- Desarrollar un plan para el análisis y tratamiento de vulnerabilidades en los sistemas de información.

- Incluir en los contratos de proveedores la obligación específica de entregar la documentación necesaria para la administración y funcionamiento de los sistemas de información.
- Establecer la transferencia de conocimiento como una obligación específica en los contratos, cuando corresponda.

**Criptografía y Prevención de fuga de datos.**

El Ministerio 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 para prevenir la fuga de datos, incluyendo:

- Fortalecer los controles de acceso para garantizar que solo el personal autorizado tenga acceso a información sensible.
- Establecer protocolos estrictos para la transferencia segura de información, tanto interna como externamente.

## 7. VIGENCIA

La presente política de seguridad y privacidad de la información ha sido revisada y aprobada por el Comité Institucional de Gestión y Desempeño, y está vigente a partir de su aprobación.

Será revisada a intervalos planificados o cuando ocurran cambios significativos en los procesos, infraestructura física o tecnológica, o cualquier aspecto que afecte la misionalidad del Ministerio de las Culturas, las Artes y los Saberes.