TABLA DE CONTENIDO

0. LISTA DE VERSIONES

VERSION	FECHA	RAZON DE LA ACTUALIZACION
0	20/01/16	Elaboración del documento. Revisado y aprobado por el Comité de Desarrollo Administrativo Institucional, según consta en acta del 16 de diciembre de 2015.
1	16/05/17	1. Se presenta la actualización del presente documento y se aprueba por el Comité de Desarrollo Administrativo Institucional, según consta en acta del 14 de junio de 2017. 2. Se actualiza el nombre del documento de "POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN" por "POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN". 3. Se ajusta el alcance del documento de "al Ministerio de Cultura y a la ciudadanía en general" a "Esta política aplica a todos los colaboradores del Ministerio de Cultura. De acuerdo a esto, es responsabilidad de los mismos cumplir todos los lineamientos establecidos en el Subsistema de Gestión de Seguridad de la Información (SGSI).". 4. Se modifica el objetivo inicial y se adicionan los requeridos acorde con los lineamientos NTC-ISO 27001:2013. 5. Se modifica el ítem 4. "Condiciones generales" y se reemplaza por lineamientos de la política general de Seguridad y Privacidad de la Información. 6. Se eliminan definiciones que no se usan en el documento. 7. Se formula la política de seguridad y privacidad de la información del Ministerio de Cultura. 8. Se modificar los lineamientos ajustándolos con la GTC-ISO27002, descritos del numeral 4.1 al 4.13. 9. Se modifica el ítem de "Aprobación" por "Vigencia".

0. INTRODUCCIÓN

El Ministerio de Cultura 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 implantación 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 de Cultura.

1. OBJETIVOS

- 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 de Cultura y de los ciudadanos en los diferentes procesos; ante cualquier amenaza que pueda comprometer la confidencialidad, disponibilidad e integridad de dicha información.
- Gestionar los Riesgos de seguridad de la información de forma oportuna por medio de controles, ayudando a reducir los impactos negativos de su materialización.
- Reducir los Incidentes de Seguridad de la Información que afecten el normal funcionamiento del Ministerio de Cultura.
- Fomentar una Cultura de Seguridad de la información en el Ministerio para que todos los Colaboradores tomen conciencia de sus deberes y responsabilidades frente al SGSI.

2. ALCANCE

Esta política aplica a todos los colaboradores del Ministerio de Cultura. De acuerdo a esto, es responsabilidad de los mismos cumplir todos los lineamientos establecidos en el Subsistema de Gestión de Seguridad de la Información (SGSI).

3. DEFINICIONES

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

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

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).

4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El **MINISTERIO DE CULTURA**, se compromete con el establecimiento, implementación, mantenimiento y mejora continua de un Subsistema de Gestión de Seguridad de la Información (SGSI) que garantice la confidencialidad, disponibilidad e integridad de la información por medio de la gestión de riesgos, incidentes de seguridad y en cumplimiento de los requisitos legales y regulatorios, apoyando la formulación, coordinación e implementación de la política cultural del Estado colombiano para estimular e impulsar el desarrollo de procesos, proyectos y actividades culturales y artísticas que reconozcan la diversidad y promuevan la valoración y protección del patrimonio cultural de la nación.

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

4.1 Dispositivos móviles y teletrabajo

- Se debe garantizar la seguridad del teletrabajo y el uso de dispositivos móviles del Ministerio y de los dispositivos móviles personales dentro de las instalaciones.
- Se debe documentar e implementar procedimientos medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

4.2 Seguridad del Recurso Humano

- Se debe asegurar que los colaboradores comprenden sus responsabilidades y son idóneos para el desempeño de sus funciones u obligaciones contractuales.
- Se debe llevar a cabo una verificación de antecedentes alineada con los requisitos legales que apliquen para cada colaborador.
- Los acuerdos contractuales con los colaboradores deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.
- La alta dirección debe exigir a todos los colaboradores la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por el Ministerio.
- Se debe establecer y ejecutar un programa de sensibilización en seguridad y privacidad de la información, acorde con las políticas y procedimientos pertinentes del Ministerio, teniendo en cuenta la información que se debe proteger, y los controles que se han implementado.

- Se debe definir, comunicar a los colaboradores y hacer cumplir las responsabilidades y los deberes de seguridad de la información que permanecen válidos aún después de la terminación contrato o cambio de empleo.

4.3 Activos de información

- Se debe mantener un inventario de activos de información actualizado, alineado con los requisitos legales y regulatorios, en donde se registren los propietarios, responsables, custodios y clasificación de los mismos.

- Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por el Ministerio.

- Se debe documentar e implementar procedimientos para que los colaboradores realicen la devolución de todos los activos que sean de propiedad del Ministerio, al terminar su contrato, acuerdo o retiro de la Entidad.

- Se debe disponer en forma segura de los medios de almacenamiento de información cuando ya no se requieran, utilizando procedimientos formales.

4.4 Control de Acceso

- Se deben documentar e implementar políticas que permitan limitar el acceso a información y a instalaciones de manejo de información, que permita el acceso a las redes, sistemas y servicios para los que tengan autorización formal previa, con especial atención a los accesos privilegiados, implementando un procedimiento formal de registro, ajuste, cancelación y revisión periódica de accesos.

- El Ministerio de Cultura debe implementar mecanismos de autenticación adecuada para los ingresos seguros a sistemas o aplicaciones, las credenciales de acceso deben mantenerse en secreto por parte de los colaboradores, de igual forma serán personales y de uso exclusivo.

4.5 Controles criptográficos

- Se debe contemplar el uso apropiado y eficaz de la criptografía en los sistemas y aplicaciones para proteger la confidencialidad, autenticidad e integridad de la información.

4.6 Seguridad física y del entorno

- Se debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

- Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el ingreso a personal autorizado.

- Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes para evitar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre.

- Se deben realizar acciones para prevenir la pérdida, daño, robo o compromiso de activos de información y la interrupción de las operaciones de la organización; los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las posibilidades de acceso no autorizado, protegidos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro, el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debe estar protegido contra interceptación, interferencia o daño.

- Todos los colaboradores del Ministerio de Cultura deben bloquear los equipos de cómputo cuando estén desatendidos, cerrar las sesiones de las aplicaciones o servicios de red cuando ya no se necesiten, adoptar la política de escritorio limpio de papeles y medios de almacenamiento removibles y tener la pantalla del computador despejada, libre de archivos o accesos directos a los programas.

4.7 Seguridad de las Operaciones

El Ministerio de Cultura debe:

- Asegurar las operaciones de las instalaciones de procesamiento de información; los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.

- Controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los 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.

- Implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada de los colaboradores, para proteger al Ministerio de Cultura contra códigos maliciosos.

- Realizar copias de respaldo (Backup) de la información, software e imágenes de los sistemas, y probarlas regularmente de acuerdo con una política de copias de respaldo definida.

- Elaborar, conservar y revisar regularmente los registros acerca de actividades de los usuarios, operadores y administradores, excepciones, fallas y eventos de seguridad de la información y protegerlos contra alteración y acceso no autorizado.

- Sincronizar todos los relojes de los sistemas de procesamiento de información con una única fuente de referencia de tiempo.

- Controlar la instalación y actualización de aplicaciones o servicios en los servidores.

- 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.

- El Grupo de Gestión de Sistemas e Informática a través de la mesa de ayuda, son los únicos autorizados para instalar o desinstalar cualquier tipo de programa de los equipos de los colaboradores propendiendo por el cumplimiento legal en materia de derechos de autor.

4.8 Seguridad de las comunicaciones

- Se debe asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información, documentar y hacer cumplir acuerdos de confidencialidad o no divulgación de información del Ministerio de Cultura.

4.9 Adquisición, desarrollo y mantenimiento de sistemas

- Se debe incluir la seguridad de la información como parte integral de los sistemas de información durante todo su ciclo de vida, como requisito para nuevos sistemas de información o mejoras a los mismos, estableciendo y aplicando reglas para el desarrollo de software o sistemas.

- Documentar y aplicar procedimientos formales para el control de cambios en los sistemas de información, contar con ambientes de desarrollo, pruebas y producción separados y seguros.

4.10 Relaciones con los proveedores

- Se deben documentar y acordar los requisitos de seguridad de la información para mitigar los riesgos asociados con los activos de información a los que tengan acceso o suministren los proveedores.

- Se debe hacer seguimiento, revisión y auditoria a la prestación de servicios de los proveedores en cuanto a términos y condiciones de seguridad de la información.

4.11 Gestión de incidentes de seguridad de la información

- Se debe establecer las responsabilidades y procedimientos de gestión para una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
- Todos los colaboradores deben reportar los incidentes de seguridad de la información a la mesa de ayuda del Grupo de Sistemas e Informática tan pronto como tengan conocimiento del mismo o sospechen de alguno.
- Se definir y aplicar procedimientos para preservar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para ser usado en la reducción de la posibilidad o el impacto de incidentes futuros.
- Se deben 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.

4.12 Aspectos de seguridad de la información de la gestión de continuidad de negocio

- El Ministerio debe establecer, documentar, implementar y mantener procesos, procedimientos y controles donde se determinen sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas.
- Se debe verificar por lo menos anualmente los controles establecidos para la continuidad de la gestión de la seguridad de la información para asegurar que son válidos y eficaces.
- Las instalaciones de procesamiento de información se deben implementar con redundancia en cumplimiento de los requisitos de disponibilidad.

4.13 Cumplimiento

- Se debe garantizar el cumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
- Se debe definir e implementar una política de privacidad, tratamiento y protección de información de datos personales.
- El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa del Ministerio de Cultura, incluyendo

lo establecido en las normas que competen al Gobierno Nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

- La presente Política se debe publicar y socializar a las partes interesadas del MINISTERIO DE CULTURA, debe esta soportada en las políticas específicas de seguridad y privacidad de la información, las cuales serán parte integral del presente documento y se deberá revisar mínimo una vez al año.

5. Roles y Responsabilidades

A continuación se describen los roles y responsabilidades de la seguridad de la información para el Ministerio de Cultura:

• **Comité de Desarrollo Administrativo Institucional**: Instancia encargada de realizar la revisión, seguimiento y aprobación de la implementación, mantenimiento y mejora del SGSI.

• **Oficial de Seguridad de la Información**: Responsable de presentar al Comité de Desarrollo Administrativo Institucional la documentación, estrategia y propuestas para el mantenimiento y fortalecimiento del SGSI, así como liderar la implementación, mantenimiento y mejora del mismo con el fin de fomentar una cultura de la seguridad de la información en el Ministerio de Cultura.

• **Oficina Asesora de Planeación – Equipo del Sistema Integrado de Gestión**:

- Responsable de asesorar a las áreas para realizar los cambios a que haya lugar en los procesos, procedimientos, instructivos y formatos del Ministerio para ajustarlos y alinearlos con el Sistema de Gestión de Calidad - SGC y el Sistema de Gestión de Seguridad de la Información - SGSI, así como apoyar el proceso de documentación del SGSI.

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

• **Grupo Gestión de Sistemas e Informática**: Implementar las políticas y controles de Seguridad informática en los recursos de tecnologías de información y comunicaciones, atender los incidentes de seguridad informática y supervisar las acciones del proveedor de seguridad.

• **Grupo de Gestión Humana**: Encargado de la administración de los procesos y capacitaciones de seguridad de la información asociados con los funcionarios del Ministerio.

• **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, dicta 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 de Cultura, 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.

• **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 Atención al Ciudadano**: Encargado de realizar seguimiento a la implementación de la política de protección de datos personales (Ley 1581 de 2012 y Decreto 1377 de 2013), y presentar al Comité de Desarrollo Administrativo Institucional el nivel de cumplimiento de la misma.

• **Colaboradores**: Cumplir con las políticas, lineamientos, procesos, procedimientos y asistir a las sensibilizaciones o capacitaciones del Sistema de Gestión de seguridad de la información.

6. VIGENCIA

La presente política cuenta con la revisión y aprobación del Comité de Desarrollo Administrativo Institucional y se encuentra vigente a partir de su publicación a través del aplicativo del Sistema Integrado de Gestión Institucional.