TABLA DE CONTENIDO

0. LISTA DE VERSIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
0	20/Ene/2016	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/May/2017	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. Se actualiza el nombre del documento de "POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN" por "POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN". Se ajusta el alcance del documento de "al Ministerio y a la ciudadanía en general" a "Esta política aplica a todos los colaboradores del Ministerio. 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).". Se modifica el objetivo inicial y se adicionan los requeridos acorde con los lineamientos NTC-ISO 27001:2013. Se modifica el ítem 4. "Condiciones generales" y se reemplaza por lineamientos de la política general de Seguridad y Privacidad de la Información. Se eliminan definiciones que no se usan en el documento. Se formula la política de seguridad y privacidad de la información del Ministerio. Se modificar los lineamientos ajustándolos con la GTCISO27002, descritos del numeral 4.1 al 4.13.

		Se modifica el ítem de "Aprobación" por "Vigencia".
2	06/02/2019	Actualización logos Ministerio Actualización etiquetada de información
3	28/Ago/2020	• Actualización objetivo general • Actualización numeración objetivos específicos • Actualización de título 5.1 dispositivos móviles cambia por Seguridad organizacional • Actualización de controles criptográficos 5.5 • Actualización título 6.10 "Grupo de atención al ciudadano" por "Grupo de servicio al ciudadano" • Actualización de redacción capítulo 5 • Actualización del ítem controles criptográficos. • Inclusión de software seguro en adquisición, desarrollo y mantenimiento de sistemas • Se agrega capitulo Usuarios Externos • Actualización del capítulo 6.5 Responsabilidades del Grupo de Gestión Humana. • Se incluye responsabilidades para jefes, coordinadores y supervisores de contrato. Capítulo 6.12, 6.13.
4	24/10/2022	• Cambio de logo. • Se incluye el reporte de los incidentes de seguridad por parte de los usuarios del ministerio, el cual se encuentra establecido en el procedimiento P-OPL-030 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN • Definición de roles y responsabilidades.

1. 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.

2. OBJETIVOS

2.1 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.

2.2 OBJETIVOS ESPECÍFICOS

2.2.1 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.

2.2.2 Reducir los incidentes

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

2.2.3 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. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El MINISTERIO, 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:

5.1 SEGURIDAD ORGANIZACIONAL

Se debe realizar una asignación de responsabilidades para la seguridad de la información, generar contacto con autoridades y grupos de interés en seguridad de la información.

Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles del Ministerio y personales dentro de las instalaciones.

Documentar e implementar procedimientos para tomar medidas de seguridad de soporte, con el fin de proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares donde se realiza teletrabajo.

5.2 SEGURIDAD DEL RECURSO HUMANO

Los colaboradores deben comprender 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.

En los acuerdos contractuales con los colaboradores se debe establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.

La alta dirección debe exigir a todos los colaboradores el cumplimiento de las políticas y procedimientos de seguridad de la información establecidos por el Ministerio.

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 implementados.

Definir y comunicar a los colaboradores la responsabilidad de cumplir con los deberes de seguridad de la información que permanecen válidos después de la terminación contrato o cambio de empleo.

5.3 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 estos.

Desarrollar e implementar un conjunto adecuado de procedimientos y lineamientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por el Ministerio.

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.

Disponer en forma segura de los medios de almacenamiento de información cuando ya no se requieran, utilizando procedimientos formales.

La información que sea creada, desarrollada o gestionada por los colaboradores del Ministerio es catalogada como como un activo

fundamental y será propiedad de la entidad. Su divulgación o entrega a terceros estará sujeta a la normatividad legal vigente.

5.4 CONTROL DE ACCESO

Documentar e implementar políticas que permitan limitar el acceso a información y a instalaciones de manejo de información, así como realizar un procedimiento formal de registro, ajuste, cancelación y revisión periódica de accesos a las redes, sistemas y servicios de la Entidad.

El Ministerio debe implementar mecanismos de autenticación adecuada para el ingreso seguro a sistemas o aplicaciones; las credenciales de acceso deben ser personales de uso exclusivo y mantenerse en secreto por parte de los colaboradores.

5.5 CONTROLES CRIPTOGRÁFICOS

Se debe contemplar el uso apropiado y eficaz de la criptografía en la infraestructura de red, por ende, todo sistema de información y servicio tecnológico debe incluir parámetros de seguridad basado en usuarios y roles según se requiera con el fin de proteger la confidencialidad, autenticidad e integridad de la información.

En el caso de servicios web misionales o de alto impacto los accesos se deben realizar adoptando medidas de conexión segura.

5.6 SEGURIDAD FÍSICA Y DEL ENTORNO

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información del Ministerio.

Proteger las áreas seguras mediante controles de acceso apropiados para permitir el ingreso solo al personal autorizado.

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.

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 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.

5.7 SEGURIDAD DE LAS OPERACIONES

El Ministerio 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 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.

5.8 SEGURIDAD DE LAS COMUNICACIONES

Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información, a través de documentación y controles efectivos que permitan conexiones seguras para los fines institucionalmente establecidos.

5.9 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

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 lineamientos de software seguro.

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.

Todo requerimiento de instalación de software libre debe estar previamente validado por el Subsistema de Gestión de Seguridad de Información – SGSI.

5.10 RELACIONES CON LOS PROVEEDORES

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.

Hacer seguimiento, revisión y auditoria a la prestación de servicios de los proveedores en cuanto a términos y condiciones de seguridad de la información.

5.11 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

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 de este o sospechen de alguno, lo establecido en el procedimiento P-OPL-030 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

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.

5.12 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 los requisitos

para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas.

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.

5.13 CUMPLIMIENTO

Garantizar el cumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

Definir e implementar una política de privacidad, tratamiento y protección 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, 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, debe estar 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.

6. 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:

6.1 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.

6.2 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.

6.3 OFICINA ASESORA DE PLANEACIÓN

6.3.1 Sistema integrado de gestión institucional

Responsable de asesorar a las áreas en la realización de 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, el Sistema de Gestión de Seguridad de la Información – SGSI y la protección de datos personales, así como apoyar el proceso de su documentación.

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

6.4 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.

6.5 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, con el apoyo del Sistema Integrado de Gestión Institucional – SIGI.

6.6 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.

6.7 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.

6.8 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.

6.9 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.

6.10 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.

6.11 GRUPO DE SERVICIO AL CIUDADANO

Responsable de atender, gestionar o direccionar las PQRSD que lleguen al Ministerio dentro de los términos legales vigentes.

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

6.12 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.

6.13 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 ELDESARROLLO DE LAS OBLIGACIONES CONTRACTUALES Formato que debe ser remitido al Grupo de Contratos y Convenios.

6.14 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.

6.15 USUARIOS EXTERNOS

Todos los usuarios externos deben estar autorizados por un colaborador, quien será el responsable del uso adecuado de los activos de información y los recursos tecnológicos del Ministerio.

Las cuentas de estos usuarios no deben tener caducidad superior a 3 meses renovables conforme las necesidades del usuario.

No es permitido el acceso a sistemas de información y recursos tecnológicos a usuarios invitados o no registrados.

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 y se encuentra vigente a partir de su publicación a través del aplicativo del Sistema Integrado de Gestión Institucional.

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 Ministerio.