Plan de Seguridad y Privacidad de la Información

Ministerio de Cultura

Contenido

1. INTRODUCCIÓN 3
2. OBJETIVOS 4
OBJETIVO GENERAL 4
OBJETIVOS ESPECÍFICOS 4
3. CONTEXTO INSTITUCIONAL 5
MISIÓN 5
VISIÓN 5
CONTEXTO ESTRATÉGICO 6
POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 6
4. ALCANCE 7
5. OPERACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI 8
CICLO DE OPERACIÓN 8
GESTIÓN DEL SGSI 8
6. ESTRATEGIAS 9
ACTIVOS DE INFORMACIÓN 9
RIESGOS 10
CONTROLES 11
GESTIÓN DE INCIDENTES 11
CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN 12
CULTURA 12
MEJORA CONTINUA 13
7. REFERENCIAS 13

1. INTRODUCCIÓN

El Ministerio de Cultura con el fin de preservar la seguridad de la información que genera y custodia y en cumplimiento normativo de las diferentes estrategias del Gobierno Colombiano, se compromete a establecer un Subsistema de Gestión de Seguridad de la Información a través de la resolución número 1872 de 2018, - "Mediante la cual se conforma el Sistema Integrado de Gestión Institucional – SIGI del Ministerio de cultura."-, artículo 3° por el cual se conforman los subsistemas, específicamente en el numeral 4 – Subsistema de Gestión de Seguridad de la Información (SGSI): tiene por propósito preservar la confidencialidad, integridad, disponibilidad y privacidad de la información, mediante la gestión de riesgos de seguridad de la información, mejores prácticas, estándares nacionales y la normatividad vigente. además, el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital., el cual cita: "Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las Entidades del estado, y de los servicios que prestan al ciudadano"

Conforme a lo expuesto y dando cumplimiento con lo establecido en el Decreto 612 de 2018, se genera el presente documento con el Plan de Seguridad y Privacidad de la Información.

2. OBJETIVOS

OBJETIVO GENERAL

Establecer el Plan de Seguridad y Privacidad de la información a través de actividades que permitan establecer, implementar, operar, monitorear, revisar y mejorar continuamente el Subsistema de Gestión de Seguridad de la Información – SGSI, conforme con los lineamientos establecidos en el componente Seguridad de la Información de la Política de Gobierno Digital, el Plan Estratégico Institucional y en cumplimiento de la normatividad vigente aplicable, alineadas con la NTC/IEC ISO 27001:2013.

OBJETIVOS ESPECÍFICOS

- Definir las fases del ciclo de operación del modelo de seguridad y privacidad de la información.
- Fortalecer la gestión del Subsistema de Gestión de Seguridad de la Información – SGSI de acuerdo con la normatividad vigente aplicable.

3. CONTEXTO INSTITUCIONAL

El Ministerio de Cultura es la entidad rectora del sector cultural colombiano la cual tiene como objetivo formular, coordinar, ejecutar y vigilar la política del Estado en materia cultural de modo coherente con los planes de desarrollo, con los principios fundamentales y de participación contemplados en la Constitución Política y en la ley y le corresponde formular y adoptar políticas, planes generales, programas y proyectos del sector.

Al Ministerio de Cultura le corresponde liderar el proceso de coordinación intersectorial para fortalecer las instituciones públicas, privadas y mixtas, orientadas a la promoción, defensa, divulgación y desarrollo de las actividades culturales y creativas y promover adecuadamente el potencial de la economía cultural y creativa (economía naranja).

MISIÓN

Formular, coordinar e implementar 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.

VISIÓN

En el 2022 el Ministerio de Cultura será reconocido en el ámbito nacional e internacional por su contribución a la transformación social y económica, a partir de una política con enfoque territorial y poblacional que fortalece la protección del patrimonio, el ejercicio de los derechos culturales y el desarrollo de la economía naranja impulsando la labor de los creadores y gestores culturales.

CONTEXTO ESTRATÉGICO

El plan enmarcado en este documento contribuye al cumplimiento de los objetivos estratégicos, los cuales se encuentran establecidos en el Plan Estratégico Institucional -PEI.

CONTEXTO ESTRATÉGICO ARTICULADO	
Objetivo Estratégico al que Contribuye	8.Fortalecer la capacidad de gestión y desempeño institucional y la mejora continua de los procesos, basada en la gestión de los riesgos, el manejo de la información y la evaluación para la toma de decisiones
Modelo Integrado de Planeación y Gestión - MIPG	Política Gobierno Digital Política de Seguridad Digital Política de Gestión Documental Política de Transparencia, acceso a la información pública y lucha contra la corrupción

Tabla 1 Contexto Estratégico, Fuente: Plan Estratégico Ministerio de Cultura.

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dentro de su compromiso con la contribución al incremento de la transparencia en la gestión pública, el uso de las mejores prácticas en seguridad de la información y la importancia de velar por la confidencialidad, integridad y disponibilidad de la información, la Entidad adoptó la Política General de Seguridad y Privacidad de la Información (DI-OPL-003) en donde:

“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 lineamientos para la implementación de la política de seguridad y privacidad del SGSI del MINISTERIO DE CULTURA”

4. ALCANCE

El Ministerio de Cultura, entendiendo la importancia de gestionar adecuadamente la información hace extenso el cumplimiento y aplicabilidad de su plan de seguridad de la información a todos los procesos y subprocesos con el fin de apoyar el desarrollo de la misión institucional.

5.OPERACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI

Son gestiones propias del SGSI las siguientes:

CICLO DE OPERACIÓN

Ilustración 1 Ciclo de operación del modelo de seguridad y privacidad de la información, Fuente: MinTic - https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

GESTIÓN DEL SGSI

Ilustración 2 Gestión del Subsistema de Gestión de Seguridad de la Información - SGSI, Fuente: archivo SGSI, Ministerio de Cultura

6. ESTRATEGIAS

Una vez identificadas las estrategias se establece el siguiente plan, con el fin de realizar su implementación y gestión.

ACTIVOS DE INFORMACIÓN

ACTIVIDADES	TAREAS	ENTREGABLES
Publicación actualización activos de información 2020	Generación de RAID con activos de información a publicar en www.datos.gov.co	Matriz RAID con activos de información
	Generación de RAID con índice de información clasificada y reservada a publicar en www.datos.gov.co	Matriz RAID con índice de información clasificada y reservada
	Publicación de activos de información en la página web institucional.	Correo electrónico de solicitud cargue de matrices
	Informar sobre actualización activos de información 2020	Correo electrónico
Levantamiento actualización activos de información 2021	Generación de pieza gráfica para sensibilización	Pieza gráfica
	Actualizar guía para el levantamiento, clasificación y actualización de activos de información – G-OPL-012. Incluye parámetros para identificar infraestructuras criticas	Documento publicado y aprobado en ISOLUCION
	Actualización de formato para el registro, clasificación y actualización de activos de información F-OPL-097	Documento publicado y aprobado en ISOLUCION
	Socialización de guía para el levantamiento, clasificación y actualización de activos de información – G-OPL-012.	Correo electrónico
	Emisión de oficio o correo electrónico solicitando la actualización de activos de información a los líderes de proceso y subprocesos.	Correo electrónico o radicado de AZ digital

ACTIVIDADES	TAREAS	ENTREGABLES
	Revisión de los activos de información reportados en el formato F-OPL-097	Correo electrónico
	Retroalimentación y correcciones de lo reportado en el formato para registro, clasificación y actualización de activos de información	Correo electrónico / actas de mesa de trabajo
	Recepción de formato final y oficio de aceptación por parte de los líderes de proceso y subprocesos	Oficio físico y digital con aceptación de activos
	Actualización de matriz en la caracterización del proceso	Cargue de matriz en ISOLUCION como registro

RIESGOS

ACTIVIDADES	TAREAS	ENTREGABLES
Actualización de documentación	Evaluar las estrategias de seguridad digital para integrar la gestión de riesgos digitales	Actualización guía G-OPL-019
	Socialización una vez actualizada la documentación, según el caso.	Correo electrónico y pieza gráfica
Identificación de riesgos de seguridad de la información y seguridad digital	Identificación, análisis y evaluación del riesgo.	Matriz de riesgo
	Retroalimentación y ajustes	Correo electrónico / actas mesa de trabajo
Aceptación de riesgos identificados	Aceptación y aprobación de los riesgos identificados.	Matriz de riesgo
	Elaboración planes de manejo	Matriz de riesgo
	Cargue de los riesgos identificados en la herramienta ISOLUCION	Matriz de riesgo
Seguimiento planes de tratamiento	Seguimiento a los planes de manejo establecidos por cada uno de los procesos y subprocesos, con sus respectivas evidencias.	Matriz de riesgo
Evaluación de riesgos residuales	Evaluar el riesgo residual de los riesgos identificados	Matriz de riesgo / actas mesa de trabajo

CONTROLES

FASE	ACTIVIDADES	TAREAS	ENTREGABLES
Gobierno Digital	Comando Conjunto Cibernético - CCOC	Participación en las reuniones convocadas por CCOC	Correo electrónico / actas
		Cumplimiento de requerimientos infraestructuras críticas del gobierno	Correo electrónico / actas
Controles NTC/IEC ISO 27001:2013	Revisión y actualización Matriz de aplicabilidad	Definición, actualización de controles aplicados en la matriz.	Matriz de Aplicabilidad
Indicadores SGSI	Actualización de Indicadores	Revisar y actualizar según el caso las formulas y metas de los indicadores para la vigencia 2021	ISOLUCION módulo medición
	Gestión de indicadores	Reporte y seguimiento de los indicadores	ISOLUCION módulo medición -
Gestión de Vulnerabilidades	Apoyo implementación Data Loss Prevention - DLP	Establecer reglas de acuerdo con la clasificación de la información y diccionario de palabras	Correo electrónico – Formato de reglas / actas
	Solicitud de ejecución de pruebas de penetración – Ethical Hacking a los portales institucionales.	Coordinar con el Grupo de Sistemas para ejecutar pruebas con el proveedor de la solución.	Correo electrónico / actas
	Plan remediación de vulnerabilidades	Establecer plan de remediación de vulnerabilidades	Correo electrónico / actas
		Ejecución plan de remediación.	Correo electrónico / actas

GESTIÓN DE INCIDENTES

ACTIVIDADES	TAREAS	ENTREGABLES
Actualización y publicación de documentos relacionados: Procedimiento gestión de incidentes de seguridad de la información y Guía de incidentes de seguridad de la información	Actualizar la guía de acuerdo con tiempos de solución y el procedimiento conforme a los cambios organizacionales.	Actualización guía G-OPL-015
	Creación de formato institucional para el reporte de incidentes	Documentos aprobado y cargado en ISOLUCION
	Publicar documentos actualizados en ISOLUCION	Documentados cargados en ISOLUCION (flujo de aprobación)

ACTIVIDADES	TAREAS	ENTREGABLES
Socialización del procedimiento de gestión de incidentes y Guía de incidentes de seguridad de la información.	Socializar el procedimiento y guía de incidentes de seguridad de la información el equipo de mesa de ayuda y Grupo de sistemas	Acta mesa de trabajo
PONAL / CSIRT / Comando Conjunto Cibernético - CCOC	Socialización de boletines información y de gestión para la prevención de incidentes de seguridad.	Correo electrónico
Eventos/vulnerabilidades	Realizar seguimientos a las herramientas de seguridad informática validando comportamientos anómalos en seguridad de la información	Correo electrónico / actas mesa de trabajo

CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

ACTIVIDADES	TAREAS	ENTREGABLES
Documentar análisis de impacto de la operación	Revisar y actualizar el análisis de impacto del negocio	BIA
Documentar estrategias de continuidad	Establecer las estrategias que permitan continuar con la operación institucional	cronogramas, árbol de comunicaciones, documento final con plan de continuidad del negocio
Establecer el plan de continuidad del negocio	Crear documentación del plan de continuidad del negocio para Museo Nacional, biblioteca Nacional y Palacio Echeverry	BIA, cronogramas, árbol de comunicaciones, documento final con plan de continuidad del negocio
	Formalizar y publicar el plan de continuidad	ISOLUCION
	Socializar el plan.	Correo electrónico / actas

CULTURA

ACTIVIDADES	TAREAS	ENTREGABLES
Plan de cultura en seguridad de la información	Elaborar la matriz de cultura y apropiación de seguridad de la información	Matriz con plan de sensibilización

ACTIVIDADES	TAREAS	ENTREGABLES
Ejecución de plan de seguridad de la información.	Llevar a cabo las estrategias que fomenten la cultura organizacional en materia de seguridad de la información	Correo electrónico, piezas gráficas
Análisis del plan de seguridad de la información	Ejecutar tarea programada que permita medir la apropiación del SGSI en la Entidad.	Correo electrónico, actas mesa de trabajo

MEJORA CONTINUA

FASE	ACTIVIDADES	TAREAS	ENTREGABLES
Acciones Correctivas y Oportunidades de Mejora	Seguimiento de las acciones correctivas y oportunidades de mejora	Revisar y documentar las acciones correctivas y oportunidades de mejora reportadas en ISOLUCION	Seguimientos ISOLUCION módulo riesgos
	Reportar oportunidades de mejora de acuerdo con las visitas de inspección	Cargar en ISOLUCION las oportunidades de mejora que se requieran de acuerdo con las visitas de inspección realizadas a los procesos y subprocesos.	ISOLUCION módulo riesgos
Auditorías Internas y Externas	Apoyo en las auditorias que se realicen al SGSI	Participar y asesorar las auditorias que se realicen al SGSI.	Correo electrónico / actas

7. REFERENCIAS

- Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Ley 1712 de 2014. “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”
- Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado: de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015 sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, (“11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital)
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política de Seguridad Digital del Estado Colombiano
- Guía para la administración de los riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo para la Función Pública - DAFP
- resolución número 1872 de 2018, - “Mediante la cual se conforma el Sistema Integrado de Gestión Institucional – SIGI del Ministerio de cultura.”-, artículo 3° por el cual se conforman los subsistemas, específicamente en el numeral 4 – Subsistema de Gestión de Seguridad de la Información (SGSI)