SAN GIL

Instituto de **Cultura y Turismo**

POLITICAS O LINEAMIENTOS INTERNOS DE CIBERSEGURIDAD

Contenido

1. INTRODUCCIÓN

La ciberseguridad se ha convertido en un pilar fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información en las entidades públicas. En el Instituto de Cultura y Turismo de San Gil, reconocemos la importancia de proteger nuestros activos digitales y la información sensible frente a amenazas cibernéticas cada vez más complejas.

Este documento establece los lineamientos internos de ciberseguridad, orientados a mitigar los riesgos tecnológicos, promover una cultura de seguridad digital entre los colaboradores, y garantizar la continuidad de las operaciones institucionales. Su contenido está alineado con la normativa nacional vigente, como el Modelo de Seguridad y Privacidad de la Información del Estado Colombiano (MSPI), el Modelo Integrado de Planeación y Gestión (MIPG), y las recomendaciones de estándares internacionales como ISO/IEC 27001.

2. OBJETIVOS

Objetivo general:
Establecer los lineamientos y responsabilidades para la implementación, mantenimiento y mejora de la ciberseguridad en el Instituto de Cultura y Turismo de San Gil, permitiendo gestionar un nivel de ciber riesgo aceptable en concordancia con los objetivos institucionales.

Objetivos específicos:

- Promover el uso seguro y responsable de los sistemas de información y activos digitales.
- Proteger los ciberactivos críticos frente a accesos no autorizados, pérdida de datos o interrupciones.
- Fortalecer la cultura organizacional frente a la seguridad de la información y ciberseguridad.
- Prevenir, detectar, responder y recuperar ante incidentes cibernéticos.
- Cumplir con la normativa nacional e internacional relacionada con la protección de datos, seguridad digital y gestión del riesgo.

3. ALCANCE

Los presentes lineamientos son aplicables a:

- Todos los servidores públicos, contratistas, pasantes, proveedores y terceros que accedan a los sistemas, redes o plataformas digitales del Instituto, ya sea de manera física o remota.
- Toda la infraestructura tecnológica, software, sistemas de información y activos digitales considerados críticos o estratégicos para el funcionamiento institucional.
- Las actividades relacionadas con el desarrollo, administración, mantenimiento, operación y uso de los recursos tecnológicos.

4. PRINCIPIOS ORIENTADORES DE LA CIBERSEGURIDAD

La implementación de esta política se sustenta en los siguientes principios, los cuales guían todas las acciones, decisiones y medidas de seguridad digital dentro del Instituto:

- **Confidencialidad:** Garantizar que la información solo sea accesible por personal autorizado.
- **Integridad:** Asegurar la exactitud, consistencia y no alteración no autorizada de la información.
- **Disponibilidad:** Mantener la accesibilidad y operatividad de los sistemas y activos digitales cuando se requieran.
- **Legalidad:** Cumplir con la normativa vigente en materia de seguridad digital, protección de datos personales y acceso a la información pública.

- **Prevención:** Implementar medidas proactivas que reduzcan la probabilidad de ocurrencia de incidentes de ciberseguridad.
- **Responsabilidad compartida:** Fomentar la corresponsabilidad de todos los funcionarios y contratistas en la protección de los recursos digitales.
- **Mejora continua:** Evaluar y actualizar de forma periódica los controles, protocolos y procedimientos de ciberseguridad.

5. ORGANIZACIÓN PARA LA CIBERSEGURIDAD: ROLES Y RESPONSABILIDADES

Para la efectiva implementación de la presente política, se establecen los siguientes roles:

Rol	Responsabilidades
Dirección General	- Liderar el compromiso institucional con la ciberseguridad. - Aprobar excepciones y actualizaciones a la política. - Proveer los recursos necesarios para su implementación.
Responsable de Ciberseguridad / Área TIC	- Diseñar e implementar controles técnicos y procedimientos de ciberseguridad. - Monitorear los riesgos y reportar incidentes. - Realizar simulacros y pruebas técnicas. - Documentar delegaciones de autoridad en caso de ser necesarias.
Área de Talento Humano	- Coordinar programas de capacitación, sensibilización y cultura de ciberseguridad. - Mantener el registro de formación por perfiles de rol.
Servidores públicos y contratistas	- Cumplir los lineamientos establecidos. - Participar activamente en las capacitaciones. - Reportar cualquier sospecha o incidente de seguridad.
Proveedores y terceros	- Cumplir con los lineamientos de acceso seguro cuando interactúen con sistemas del Instituto. - Firmar compromisos de confidencialidad y responsabilidad en el uso de activos digitales.
Comité de Control Interno / Planeación	- Verificar el cumplimiento y efectividad de los controles establecidos. - Incorporar los resultados del seguimiento a la política en el ciclo de mejora institucional.

6. LINEAMIENTOS DE CIBERSEGURIDAD

6.1. Acceso y protección de activos digitales

- Todo acceso a los sistemas de información del Instituto deberá estar autenticado, registrado y sujeto a control de privilegios.
- Los perfiles de usuario serán asignados según el principio de **mínimo privilegio**, y revisados periódicamente.
- Se restringirá el acceso a ciberactivos críticos únicamente al personal autorizado.
- Los accesos remotos requerirán mecanismos de autenticación reforzada (como doble factor).

6.2. Gestión de riesgos de ciberseguridad

- Todos los proyectos institucionales que involucren activos tecnológicos deberán realizar una **valoración de riesgos de ciberseguridad**, documentada y alineada con la política de gestión del riesgo institucional.
- La valoración debe contemplar amenazas, vulnerabilidades y probabilidad de impacto, y derivar en planes de tratamiento que incluyan al menos una de las siguientes acciones:
  - Evitar el riesgo
  - Mitigarlo (reducir impacto o probabilidad)
  - Transferirlo
  - Aceptarlo, si es residual y justificado

6.3. Prevención y protección ante malware

- Se deben implementar herramientas actualizadas de detección y prevención de malware en todos los equipos que gestionen información institucional.
- El correo electrónico y los dispositivos USB serán monitoreados y restringidos según criterios técnicos.
- Se realizarán campañas periódicas de concientización sobre ingeniería social, phishing y amenazas emergentes.

6.4. Gestión de incidentes

- El Instituto contará con un **protocolo de respuesta a incidentes de ciberseguridad**, que incluirá:
  - Notificación oportuna del incidente
  - Clasificación del evento
  - Acciones de contención, mitigación y recuperación
  - Reporte y análisis posterior (lecciones aprendidas)
- Este protocolo deberá ser probado al menos una vez al año mediante simulacros o ejercicios de escritorio.

6.5. Conexiones temporales y dispositivos externos

- Las conexiones temporales dentro de los perímetros de seguridad digital deben ser autorizadas y registradas.
- Todo dispositivo externo (como portátiles o memorias) debe ser verificado antes de conectarse a los sistemas institucionales.

6.6. Copias de seguridad y recuperación

- Los activos críticos deben contar con esquemas de **respaldo periódico (backup)** que permitan la restauración ante pérdida de datos o fallas técnicas.
- Estos backups deben almacenarse en entornos seguros y ser probados periódicamente para garantizar su funcionalidad.

6.7. Capacitación y cultura organizacional

- Todo el personal nuevo deberá recibir formación en ciberseguridad como parte del proceso de inducción.
- Se realizarán mínimo dos jornadas anuales de actualización o sensibilización en temas de seguridad digital.

7. SEGUIMIENTO Y CONTROL

Para garantizar la efectividad y sostenibilidad de esta política, el Instituto de Cultura y Turismo de San Gil establecerá mecanismos sistemáticos de seguimiento, control y mejora, enmarcados en el Modelo Integrado de Planeación y Gestión (MIPG) y en el ciclo PHVA (Planear, Hacer, Verificar, Actuar).

7.1. Indicadores de gestión

Se definirá una batería de indicadores para monitorear la implementación de la política de ciberseguridad, que podrá incluir:

- Porcentaje de funcionarios y contratistas capacitados.
- Número de incidentes reportados y gestionados.
- Tiempo promedio de atención a incidentes.
- Cumplimiento del plan de respaldo y recuperación.
- Nivel de implementación de controles preventivos.

7.2. Seguimiento periódico

- El área TIC, en articulación con Planeación y Control Interno, realizará un informe semestral que detalle los avances, dificultades, y recomendaciones en la implementación de esta política.
- Dicho informe deberá presentarse ante la Dirección General y el Comité de Coordinación del Sistema de Control Interno.

7.3. Auditoría interna y evaluación

- Como parte de la evaluación institucional, la política de ciberseguridad será objeto de revisión en las auditorias internas, en concordancia con el componente de gestión de riesgos del MIPG.
- Se promoverá la evaluación participativa mediante encuestas, focus group u otros mecanismos, que permitan recoger percepciones del personal frente a la cultura de ciberseguridad.

7.4. Mejora continua

- Los resultados del seguimiento, las auditorías y los incidentes gestionados deberán derivar en acciones correctivas y preventivas.
- La política se revisará anualmente y será ajustada en función de:
  - Cambios normativos o tecnológicos
  - Evolución de las amenazas
  - Cambios organizacionales o estratégicos
  - Lecciones aprendidas de eventos reales o simulados

8. EXCEPCIONES

Cualquier excepción a los lineamientos establecidos en esta política deberá ser:

- **Solicitada por escrito**, justificando la necesidad y alcance de la excepción.
- **Revisada y aprobada** por la Dirección General del Instituto de Cultura y Turismo de San Gil, con el respaldo del área TIC y/o el Comité de Coordinación del Sistema de Control Interno.
- **Documentada formalmente**, indicando:
  - Nombre del solicitante
  - Descripción de la excepción
  - Periodo de validez
  - Riesgos asociados y controles compensatorios
- **Revisada periódicamente** para verificar si se mantiene vigente o debe modificarse.

9. DISPOSICIONES GENERALES

- Esta política hace parte integral del sistema de gestión institucional y se articula con los documentos del MIPG, la política de protección de datos personales y el plan estratégico de TI del Instituto.
- Todos los servidores públicos, contratistas, proveedores y terceros que interactúen con activos digitales del Instituto están obligados a cumplir esta política.
- El incumplimiento de lo aquí dispuesto podrá derivar en sanciones administrativas, disciplinarias o legales, según la gravedad del hecho y conforme al régimen aplicable.
- La presente política deberá ser socializada a todo el personal mediante jornadas de inducción, boletines o medios digitales oficiales.

10. CONTROL DE VERSIONES Y VIGENCIA

Versión	Fecha de aprobación	Responsable de la actualización	Descripción del cambio
1.0	[Fecha actual]	Área TIC / Dirección General	Versión inicial de la política

Esta política entra en vigencia a partir de la fecha de su aprobación y deberá ser revisada anualmente o cuando haya cambios tecnológicos, normativos o estratégicos que así lo requieran.