

POLITICA SE SEGURIDAD DE LA INFORMACION

INSTITUTO DE CULTURA Y TURISMO DE SAN GIL

1. GENERALIDADES

La política de seguridad informática busca implementar una serie de medidas de índole técnica y de organización, que garanticen la seguridad, confidencialidad y disponibilidad de la información, así como garantizar la seguridad de las tecnologías de la información que a su vez puedan ser intensidades y ejecutadas por todos aquellas personas que interactúan haciendo uso de los servicios asociados a ellos.

2. ALCANCE

Este manual de políticas de seguridad se elaboró de acuerdo al análisis de riesgos y de vulnerabilidades del Instituto de Cultura y Turismo de San Gil, por consiguiente el alcance de estas políticas se encuentra sujeto a esta entidad. Esta política es aplicable a todo el personal de la entidad, al igual que a todos sus recursos tecnológicos.

3. OBJETIVOS

Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos del Instituto de Cultura y Turismo de San Gil.

Los objetivos que se deseen alcanzar luego de implantar las Políticas de Seguridad son los siguientes:

- Establecer un esquema de seguridad con perfecta claridad y transparencia.
- Que se aumente la calidad en la prestación del servicio.
- Todos los empleados se convierten en interventores del sistema de seguridad.

4. VIGENCIA

La documentación presentada como Políticas de Seguridad entrara en vigencia desde el momento en que sean aprobadas por la Dirección. Esta normativa debe ser revisada y actualizada conforme a las exigencias del Instituto de Cultura y Turismo de San Gil o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

5. FRECUENCIA DE EVALUACIÓN DE LAS POLÍTICAS

Las políticas planteadas en este documento se evaluarán con una frecuencia semestral.

6. POLITICAS DE SEGURIDAD FÍSICA

6.1 Acceso Físico

6.1.1. Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

6.1.2. Las visitas internas o externas podrán acceder así las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de sistemas o con permiso de esta área.

6.1.3. Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido.

6.2 PROTECCIÓN FÍSICA

6.2.1. Centros de Cableado

Los centros de cableado deberán:

- Tener una puerta de acceso de vidrio transparente, para favorecer el control del uso de los recursos de cómputo.
- Ser un área restringida, tener un sistema de control de acceso que garantice la entrada solo al personal autorizado.
- No debe poseer instalaciones eléctricas en mal estado.
- Respaldo de energía redundante.
- Contar con extintor de incendio adecuado y cercano al centro de cableado.

6.3 INSTALACIONES DE EQUIPOS DE COMPUTO

La instalación de equipos de cómputo se hará de acuerdo a los siguientes lineamientos:

- Los equipos de uso de la entidad se instalaran en lugares adecuados, aquellos sitios lejos del tráfico de personas.
- Las instalaciones eléctricas y de comunicaciones estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales.
- No se permitirán instalaciones eléctricas improvisadas o sobrecargadas.

6.4 RESPALDOS

- Las bases de datos del Instituto de Cultura y Turismo de San Gil serán respaldadas periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.
- Los respaldos de información deberán ser almacenados en lugares seguros.

- Para reforzar la seguridad de la información, los funcionarios y contratistas, bajo su criterio deberán hacer respaldos de la información en sus discos duros frecuentemente, dependiendo de la importancia y frecuencia de cambio; y en las unidades de almacenamiento asignadas por la entidad “La Nube” (Google Drive), los respaldos serán responsabilidad absoluta de los usuarios.

6.5 RECURSOS DE LOS USUARIOS

6.5.1. Uso

- Los funcionarios y contratistas deberán respetar, cuidar y hacer un uso adecuado de los recursos de cómputo y red del Instituto de Cultura y Turismo de San Gil, de acuerdo con las políticas que en este documento se mencionan.
- Los funcionarios y contratistas deberán solicitar apoyo al área de sistemas ante cualquier duda en el manejo de los recursos de cómputo de la entidad.
- El correo electrónico no se deberá usar para envío de materiales de uso no institucional o innecesarios para envíos de correos masivos (entiéndase por correo masivo todo aquí que sea ajeno a la institución, tales como cadenas, publicidad y propaganda comercial, política, social, etcétera).

6.5.2. Derechos de Autor

- Queda estrictamente prohibido copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor.
- No está permitido para los funcionarios y contratistas instalar ningún programa en su computadora sin autorización estricta de la dirección o la oficina de sistemas.
- No se permitirá que un empleado realice copias no autorizadas de programas informáticos.
- No se permitirá que un empleado cargue o descargue programas informativos no autorizados de internet, dentro de los cuales también incluyen programas que puedan utilizarse para comercializar trabajos protegidos por los derechos de autor.
- No se permitirá a funcionario o contratista, realice intercambios de archivos digitales de música (MP3) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.
- Si se encuentran copias sin licencias, están serán eliminadas y de ser necesario reemplazadas por copias con licencia.
- Los usuarios utilizarán los programas informáticos solo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.

7. POLITICAS DE SEGURIDAD LOGICA

7.1. Red

- Las redes de datos tiene como finalidad principal ayudar en el intercambio de información dentro de la entidad, entre oficinas hacia afuera.
- Ninguna persona podrá copiar, alterar o destruir la información que se encuentra en los equipos sin el consentimiento explícito del responsable del equipo.
- No se permiten que se utilicen los servicios de la red para labores que no sean propias de la entidad.
- No estará permitido el uso de programas analizadores para monitorear redes ajenas al Instituto de Cultura y Turismo de San Gil y no se deberán realizar análisis de la red desde equipos externos a la entidad.

7.2 Servidores

La oficina de sistemas de la Alcaldía Municipal de San Gil tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectado a la red.

Los servidores que proporcionen servicios a través de la red e internet deberán:

- Las 24 horas del día los 365 días del año.
- Recibir mantenimiento preventivo mínimo dos veces al año.

7.3 Renovación de equipos

Cuando en alguna de las áreas se requiera de un equipo de cómputo, bien sea por sustitución o para mejorar el desempeño y la calidad del servicio, se deberá realizar una consulta al área de sistemas a fin de que se seleccione el equipo adecuado, sin el visto bueno de la oficina de sistemas no podrá liberar una orden de compra.

7.4 Usuarios y dependencias

- La dirección precisara los servicios de internet a ofrecer a los funcionarios y contratistas.
- Todos los funcionarios y contratistas que tengan acceso a un sistema de información o a la red de datos, tendrán un identificador de usuario y contraseña.
- El funcionario o contratista, definirá su contraseña conforme al procedimiento establecido y será responsable de la confidencialidad de la misma.
- Los funcionarios y contratistas son responsables del uso de su identificador de usuario y contraseña.

- Los funcionarios y contratistas no deben dar a conocer bajo ningún motivo si identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

7.5 Antivirus

Todos los equipos de cómputo conectado a la red del Instituto de Cultura y Turismo de San Gil deben tener instalado y debidamente actualizado la solución antivirus.

7.6 Uso del antivirus por parte de los funcionarios y contratistas

- En ningún momento y bajo ninguna circunstancia el usuario debe desinstalar el antivirus de su computadora, pues esto ocasionaría un potencial riesgo de seguridad.
- En caso de problemas con algún virus, el usuario deberá notificarlo a la oficina de sistemas con el fin de buscar una solución.

8. ACTUALIZACIONES EN LA POLITICA DE SEGURIDAD

Debido a la evolución de las amenazas de seguridad, el Instituto de Cultura y Turismo de San Gil se reserva el derecho de modificar estas políticas planteadas en este documento cuando lo crea necesario. Los cambios realizados en estas políticas serán divulgados a todos los funcionarios y contratistas de la entidad. Es responsabilidad de cada uno de los funcionarios y contratistas la lectura y conocimiento de la Política de Seguridad más reciente.

8.1. Disposiciones

- Las políticas enmarcadas en este documento entraran en vigor a partir del día de su difusión.
- Las políticas que están planteadas en este documento podrán ser modificadas o ajustadas conforme a las necesidades que se vayan presentando.