POLITICAS O LINEAMIENTOS INTERNOS DE CIBERSEGURIDAD

INSTITUTO DE CULTURA Y TURISMO DE SAN GIL

1. OBJETIVO

Email: ict@sangil.gov.co
Tel: 3204988239-3045387449
Calle 12 No 10-31
www.turismosangil.com

Definir los detalles de cómo se debe implementar la Política de ciberseguridad en el Instituto de Cultura y Turismo de San Gil, que se consiguen con la aplicación de estos controles de ciberseguridad, para gestionar un nivel de ciber riesgo aceptable.

2. ALCANCE

Estos lineamientos son aplicables a todos los colaboradores, proveedores, contratistas, terceras partes, que ingresan física o remotamente a los perímetros de seguridad y accedan a ciber activos críticos propiedad de ICT.

3. DESCRIPCIÓN DE LOS LINEAMIENTOS

3.1 Organización para la ciberseguridad

3.1.1 Responsable de ciberseguridad

- Implementar y documentar el procedimiento de delegación de la autoridad.
- El responsable de ciberseguridad puede delegar la autoridad para acciones específica, esta delegación debe estar documentada, incluyendo el nombre del titular del delegado, las acciones específicas a delegar y la fecha de delegación; aprobado por el responsable de ciberseguridad y actualizado máximo treinta (30) días de cualquier cambio de delegación.

3.1.2 Evaluaciones y planes para el personal

El personal que tiene acceso lógico autorizado o acceso físico o escoltado a ciberactivos críticos, incluyendo contratistas deben tener una evaluación de riesgos de personal que cumplan con planes de concientización, capacitación y entrenamiento.

3.1.3 Programa de entrenamiento y capacitación

Debe contar con un programa de entrenamiento y capacitación según el rol desempeñado y su criticidad, este debe contener los siguientes elementos:

- Políticas o lineamientos de ciberseguridad.
- Controles de acceso físico y control de visitantes.
- Controles de acceso electrónicos.
- Manejo de ciberactivos críticos, información y su almacenamiento.
- Gestión de incidente de ciberseguridad, notificaciones iniciales de acuerdo con el procedimiento de respuesta a incidentes.
- Procedimiento de recuperación para ciberactivos críticos.

- Riesgos de ciberseguridad asociados con la interconectividad e interoperabilidad de ciberactivos críticos.

3.2 Tratamiento y Gestión del Ciber riesgo

Generación, transmisión y distribución, talento humano y soluciones organizaciones son responsables de analizar y realizar el tratamiento de los ciber riesgos con base en los objetivos de negocio y alineados con la política de gestión de riesgos.

En los proyectos o nuevas adquisiciones se debe realizar la identificación de los activos críticos y ciber activos críticos, los riesgos, vulnerabilidades y el nivel de gestión de ciberseguridad en la operación para establecer un plan de ciberseguridad.

Periódicamente se debe realizar una valoración del riesgo para contemplar los cambios en los requisitos de ciberseguridad y la situación de riesgos, tales como cambio en los activos críticos y ciber activos críticos, las amenazas, las vulnerabilidades y los impactos. Se debe decidir cuándo un riesgo es aceptable, ya sea por motivos de objetivos de negocio o por costes no rentables.

Los posibles tratamientos a los riesgos identificados incluyen:

- Evitar el riesgo.
- Disminuir la probabilidad de ocurrencia.
- Disminuir el impacto.
- Transferir los riesgos.
- Retener los riesgos.

3.3 Administración de conexiones temporales

Documentara e implementara procedimientos de administración de conexiones temporales dentro del perímetro de seguridad electrónica.

3.4 Herramientas de prevención

Utilizar herramientas de prevención contra software malicioso (malware), donde será técnicamente factible, para detectar, prevenir, disuadir y mitigar la introducción, exposición y propagación de malware a todos los ciberactivos dentro de los perímetros de seguridad electrónica.

3.5 Pruebas y simulacros

Los planes de respuesta a incidentes deben probarse mínima una (1) al año. Una prueba o simulacro del plan de respuesta a incidentes puede comprender desde una prueba de escritorio a un ejercicio operativo completo que simule un incidente real.

Los planes de respuesta a incidentes deben revisarse, actualizarse y comunicarse para reflejar los cambios, procedimientos de mejoramiento y lecciones aprendidas de la ejecución de los mismos.

Tecnología debe disponer de registros documentales de las pruebas o simulacros que se realicen periódicamente y las acciones de mejora como resultados de las pruebas, así como, documentación de la divulgación de los mismos.

4. EXCEPCIONES

Las excepciones a cualquiera de los lineamientos de ciberseguridad deben ser aprobados, la cual puede requerir autorización del director del Instituto de Cultura y Turismo de San Gil, todas las excepciones a la política deben ser formalmente documentadas, registradas y revisadas.

Email: ict@sangil.gov.co
Tel: 3204988239-3045387449
Calle 12 No 10-31
www.turismosangil.com