INSTITUTO MUNICIPAL DE CULTURA Y TURISMO DE TENJO (IMCTT)

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024 - 2027

Contenido

1. Introducción 4

1.1. Objetivo principal 5

1.2. Objetivos específicos 5

2. Marco Normativo 6

3. Alcance 7

4. Políticas de Seguridad y Privacidad 9

4.1. Política de Acceso y Autorización 9

4.2. Política de Respaldo y Recuperación 9

4.3. Política de Monitoreo y Auditoría 9

4.4. Política de Gestión de Incidentes 9

4.5. Política de Manejo de Datos Personales 10

5. Controles de Seguridad 10

5.1. Controles Técnicos 10

5.2. Controles Físicos 11

5.3. Controles Administrativos 11

5. Política de Privacidad de la Información 12

5.1. Manejo de Datos Personales 12

5.2. Transparencia y Comunicación 13

5.3. Derechos de los Individuos 14

6. Concientización y Formación en la Seguridad de la Información 15

6.1. Sesiones de Concientización 15

6.2. Sesiones de Formación 15

7. Evaluación y Mejora Continua 15

7.1. Revisiones Periódicas 15

7.2. Adaptación a Cambios..... 16

1. Introducción

El Instituto Municipal de Cultura y Turismo de Tenjo (IMCTT) asume el compromiso de salvaguardar la integridad, confidencialidad y disponibilidad de la información que gestiona, reconociendo su valor estratégico en el cumplimiento de nuestra misión cultural y turística. La seguridad y privacidad de la información se erigen como pilares fundamentales para el fortalecimiento de la confianza de nuestros colaboradores, visitantes, y la comunidad en general.

En este contexto, el presente Plan de Seguridad y Privacidad de la Información establece un marco integral que aborda las políticas, procedimientos y controles necesarios para garantizar la protección efectiva de nuestros activos de información. Conscientes de los desafíos y riesgos constantes en el entorno digital actual, este plan se configura como una guía estratégica para mitigar amenazas, preservar la confidencialidad de la información y asegurar la continuidad de nuestras operaciones.

A través de la implementación de medidas técnicas, físicas y administrativas, el IMCTT busca establecer una cultura de seguridad y privacidad arraigada en cada nivel de nuestra organización. Además, este plan reconoce la importancia de respetar la privacidad de los datos personales, cumpliendo con las normativas vigentes y fomentando la confianza de quienes confían en nosotros con su información personal.

El compromiso con la mejora continua se refleja en la evaluación periódica de nuestros procesos, la adaptación a las evoluciones tecnológicas y la capacitación constante de nuestro personal. La seguridad y privacidad de la información no son metas estáticas, sino un viaje dinámico que abordamos con diligencia y responsabilidad.

Por lo tanto, invitamos a todos los miembros del IMCTT a comprometerse activamente con la implementación de este plan, reconociendo que la seguridad y privacidad de la información son responsabilidades compartidas. Al hacerlo, no solo fortalecemos la resiliencia de nuestra organización, sino que también reafirmamos nuestro compromiso con la confianza y la excelencia en la gestión de la información.

1.1. Objetivo principal

Garantizar la seguridad y privacidad de la información del Instituto Municipal de Cultura y Turismo de Tenjo (IMCTT), fortaleciendo la confianza en la gestión de la información y asegurando la integridad y disponibilidad de los activos de información esenciales para la misión cultural y turística de la institución.

1.2. Objetivos específicos

- Refuerzo de la Confidencialidad Implementar controles de acceso avanzados y políticas de autorización.
- Mejora de la Integridad de los Datos: Desarrollar y aplicar controles técnicos para prevenir alteraciones no autorizadas de la información.

- Aseguramiento de la Disponibilidad Continua: Implementar medidas para garantizar la alta disponibilidad de sistemas y datos críticos.
- Promoción de Concientización en Seguridad: Desarrollar programas de concientización y formación en seguridad de la información para todo el personal del IMCTT.

2. Marco Normativo

Normativa	Fecha	Contexto
Directiva Presidencial 02	Feb 24, 2022	Implementación segura de la Política de Gobierno Digital del MinTIC.
Decreto 338	Mar 8, 2022	Establece lineamientos generales para fortalecer la gobernanza de la seguridad digital.
Resolución 746	Mar 11, 2022	Fortalece el Modelo de Seguridad y Privacidad de la Información.
Decreto 767	May 16, 2022	Establece lineamientos generales de la Política de Gobierno Digital.
Directiva Presidencial 03	Mar 15, 2021	Lineamientos para el uso de Servicios en la Nube, Inteligencia Artificial, Seguridad digital y Gestión de Datos.
Resolución 500	Mar 10, 2021	Establece lineamientos y estándares para la estrategia de seguridad digital y adopta el modelo de seguridad y privacidad.
Conpes 3995	Jul 1, 2020	Política Nacional de Confianza y Seguridad Digital.
Resolución 1519	Aug 24, 2020	Define estándares y directrices para la publicación de información, acceso a la información, accesibilidad web, seguridad digital, y datos abiertos.
Decreto 612	Apr 4, 2018	Fija directrices para la integración de planes institucionales y estratégicos.

Decreto 1008	Jun 14, 2018	Establece lineamientos generales de la política de Gobierno Digital.
Resolución 2140	Oct 19, 2017	Adopta el Modelo Integrado de Planeación y Gestión y crea instancias administrativas en el Ministerio de Ambiente y Desarrollo Sostenible.
Conpes 3854	Apr 11, 2016	Política Nacional de Seguridad Digital.
Decreto 103	Jan 20, 2015	Reglamenta parcialmente la Ley 1712 de 2014.
Ley 1712	Mar 6, 2014	Crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
Decreto 886	May 13, 2014	Reglamenta el artículo 25 de la Ley 1581 de 2012 sobre el Registro Nacional de Bases de Datos.
Ley 1581	Oct 17, 2012	Dicta disposiciones generales para la protección de datos personales.

3. Alcance

El alcance del Plan de Seguridad y Privacidad de la Información del Instituto Municipal de Cultura y Turismo de Tenjo (IMCTT) abarca la totalidad de los procesos, sistemas y activos de información bajo la responsabilidad de la institución. Este plan se extiende a todas las áreas y departamentos del IMCTT, incluyendo, pero no limitándose a:

- Sistemas de Información:

  Todos los sistemas informáticos y aplicaciones utilizados para el procesamiento, almacenamiento y transmisión de datos en el IMCTT.

- Datos Sensibles:

Información relacionada con eventos culturales, patrimonio, datos de visitantes, y cualquier otra información considerada sensible para el cumplimiento de la misión cultural y turística del IMCTT.

- Personal:

Todos los colaboradores, contratistas y terceros que tienen acceso a los sistemas y datos gestionados por el IMCTT.

- Procesos Operativos:

Procesos internos y operativos que involucran la manipulación, gestión y acceso a la información.

- Instalaciones Físicas:

Áreas físicas que albergan servidores, dispositivos de almacenamiento y otros activos de información críticos.

El alcance de este plan busca establecer un marco integral que proteja la confidencialidad, integridad y disponibilidad de la información manejada por el IMCTT, garantizando la seguridad de los activos de información y el respeto a la privacidad de los datos personales.

4. Políticas de Seguridad y Privacidad

4.1. Política de Acceso y Autorización

- Establecer niveles de acceso basados en roles y responsabilidades.
- Implementar autenticación de dos factores para cuentas críticas.
- Revisar y actualizar periódicamente los privilegios de acceso.

4.2. Política de Respaldo y Recuperación

- Realizar copias de seguridad programadas de los datos críticos.
- Almacenar copias de seguridad en ubicaciones seguras y fuera de las instalaciones principales.
- Realizar pruebas regulares de recuperación para validar la efectividad del plan.

4.3. Política de Monitoreo y Auditoría

- Establecer registros de auditoría detallados para actividades críticas.
- Monitorear proactivamente eventos de seguridad y anomalías.
- Realizar auditorías de seguridad internas y externas periódicas.

4.4. Política de Gestión de Incidentes

- Documentar y reportar incidentes de seguridad de manera oportuna.
- Mejorar continuamente las respuestas a incidentes basándose en lecciones aprendidas.

4.5. Política de Manejo de Datos Personales

- Obtener consentimiento informado para la recolección y procesamiento de datos personales.
- Establecer períodos de retención de datos y procedimientos para su eliminación segura.
- Garantizar la confidencialidad y seguridad de los datos personales.

5. Controles de Seguridad

5.1. Controles Técnicos

5.1.1. Firewalls y Antivirus

- Mantener firewalls actualizados y configurados para bloquear tráfico no autorizado.
- Implementar soluciones antivirus en todos los dispositivos para detectar y prevenir software malicioso.

5.1.2. Actualización de Software y Sistemas

- Establecer un programa de gestión de parches para sistemas y software críticos.
- Realizar pruebas de compatibilidad antes de aplicar actualizaciones en entornos de producción.

5.1.3. Encriptación de Datos

- Encriptar datos confidenciales durante su transmisión a través de redes seguras.
- Implementar encriptación en repositorios de almacenamiento de datos sensibles.

5.2. Controles Físicos

5.2.1. Acceso Restringido a Áreas Críticas

- Implementar sistemas de control de acceso físico, como cerraduras electrónicas.
- Registrar y monitorear el acceso a áreas críticas.

5.2.2. Respaldo Físico de Copias de Seguridad

- Establecer un proceso seguro para transportar y almacenar copias de seguridad en ubicaciones externas.
- Garantizar la integridad de las copias de seguridad almacenadas físicamente.

5.3. Controles Administrativos

5.3.1. Programas de Formación en Seguridad

- Implementar programas de formación en seguridad de la información para todo el personal.
- Incluir sesiones de actualización periódicas sobre las políticas y procedimientos de seguridad.

4.3.1. Políticas de Uso Aceptable

- Desarrollar políticas claras que especifiquen cómo se deben utilizar los sistemas y datos.
- Comunicar y hacer cumplir estas políticas mediante la capacitación y auditorías internas.

5. Política de Privacidad de la Información

5.1. Manejo de Datos Personales

5.1.1. Principios Básicos

- Obtener el consentimiento informado antes de la recolección de datos personales.
- Limitar la recolección de datos a lo estrictamente necesario para los fines específicos.
- Garantizar la exactitud y actualización de los datos personales recolectados.

5.1.2. Consentimiento Informado

- Obtener un consentimiento claro y específico antes de recolectar, procesar o compartir datos personales.
- Proporcionar información transparente sobre el propósito de la recolección y el uso previsto de los datos.

5.1.3. Retiro del Consentimiento

- Proporcionar mecanismos claros para que los individuos retiren su consentimiento en cualquier momento.
- Respetar la decisión de retirar el consentimiento y ajustar el manejo de los datos en consecuencia.

5.1.4. Retención y Eliminación de Datos

- Establecer periodos de retención claros y justificables para los datos personales recolectados.
- Revisar y actualizar periódicamente los periodos de retención según las necesidades y regulaciones.
- Implementar procedimientos seguros para la eliminación de datos personales al finalizar su periodo de retención.
- Garantizar que la eliminación se realice de manera irreversible y documentada.

5.2. Transparencia y Comunicación

5.2.1. Políticas de Privacidad

- Publicar y mantener políticas de privacidad accesibles para informar a los individuos sobre cómo se manejan sus datos personales.
- Incluir detalles sobre los derechos de los individuos con respecto a sus datos personales.

5.2.2. Comunicación de Incidentes

- Notificar a las partes afectadas y autoridades pertinentes en caso de una brecha de seguridad que pueda comprometer datos personales.
- Proporcionar información clara y oportuna sobre la naturaleza del incidente y las medidas tomadas.

5.3. Derechos de los Individuos

5.3.1. Acceso a Datos Personales

- Garantizar que los individuos tengan acceso a sus propios datos personales.
- Facilitar el ejercicio de otros derechos, como rectificación, limitación del procesamiento y portabilidad de datos.

5.3.2. Respuesta a Solicitudes

- Establecer procedimientos eficientes para responder a las solicitudes de derechos de los individuos en un plazo razonable.
- Designar un punto de contacto responsable de manejar estas solicitudes.

6. Concientización y Formación en la Seguridad de la Información

6.1. Sesiones de Concientización

- Temas de actualidad en seguridad de la información.
- Amenazas cibernéticas y tácticas comunes.
- Casos de estudio y lecciones aprendidas.

6.2. Sesiones de Formación

- Fundamentos de seguridad de la información.
- Prácticas seguras en el uso de sistemas y datos.
- Procedimientos de respuesta a incidentes.

7. Evaluación y Mejora Continua

7.1. Revisiones Periódicas

- Evaluar la efectividad de los programas mediante revisiones regulares.
- Ajustar y actualizar contenido y métodos de formación según las tendencias y necesidades emergentes.

7.2. Adaptación a Cambios

- Mantenerse al tanto de las evoluciones en amenazas de seguridad y tecnologías emergentes.
- Ajustar programas de concientización y formación en consecuencia.