



# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## 2025

**Instituto Municipal de Cultura y Turismo de Cajicá**





## Tabla de contenido

1.	<b>INTRODUCCIÓN</b> .....	3
2.	<b>CONTEXTO ESTRATEGICO INSTITUCIONAL</b> .....	3
3.	<b>ALCANCE</b> .....	3
4.	<b>OBJETIVO GENERAL</b> .....	4
5.	<b>OBJETIVOS ESPECÍFICOS</b> .....	4
6.	<b>DEFINICIONES BÁSICAS</b> .....	4
7.	<b>MARCO NORMATIVO</b> .....	8
8.	<b>DIAGNÓSTICO</b> .....	9
9.	<b>PLAN DE ACCIÓN ANUAL</b> .....	9
10.	<b>CRONOGRAMA</b> .....	10
11.	<b>SEGUIMIENTO Y MONITOREO</b> .....	10
12.	<b>REFERENCIAS</b> .....	10





## 1. INTRODUCCIÓN

Actualmente, entidades y organizaciones de todo tipo se enfrentan a un aumento significativo de incidentes de seguridad de información, que derivan en pérdidas financieras, de imagen, corrupción y filtración de datos o que generan reprocesos administrativos. Esta realidad crea la necesidad de implementar, mantener y mejorar de manera continua un Plan de Seguridad de Información donde se diseñen, documenten, implementen y monitoreen controles basados en gestión de riesgos que minimicen la probabilidad y el impacto de ocurrencia.

El plan de seguridad de información del Instituto Municipal de Cultura Y Turismo de Cajicá (IMCTC) consolida la normatividad, el alcance, y las metodologías implantadas en la entidad para salvaguardar de manera eficiente la información Institucional, y describe las acciones que se llevan a cabo con el objetivo de mitigar los riesgos identificados durante la ejecución de las actividades institucionales.

## 2. CONTEXTO ESTRATEGICO INSTITUCIONAL

### Misión

Somos una entidad descentralizada que planea, direcciona, ejecuta y evalúa las políticas, planes, programas y proyectos culturales, bibliotecarios, patrimoniales y turísticos del Municipio de Cajicá, desde el reconocimiento y visibilización de la diversidad cultural del municipio, el fortalecimiento de las prácticas de lectura, escritura y oralidad, la salvaguarda, protección, conservación y divulgación del patrimonio material e inmaterial y la promoción de Cajicá como destino turístico, a partir de procesos de planeación, articulación, desarrollo y evaluación encaminados al reconocimiento del Instituto a nivel regional y nacional por la calidad de los servicios y el impacto en la comunidad.

### Visión

Liderar la formulación, ejecución y evaluación de políticas, planes, programas y proyectos culturales, bibliotecarios, patrimoniales y turísticos a nivel municipal, departamental, nacional e internacional, por medio de procesos innovadores de la gestión pública de la cultura a través del fomento de las prácticas culturales, el impulso de las prácticas de la lectura, escritura y oralidad, el rescate y apropiación de los bienes y manifestaciones de interés cultural y la promoción de Cajicá como destino turístico, contribuyendo a la transformación cultural y el desarrollo social, económico y comunitario de la población.

## 3. ALCANCE

Este Plan aplica a toda la entidad, funcionarios y contratistas del IMCTC. Todas las personas cubiertas por el alcance y aplicabilidad deberán dar





cumplimiento al Plan de Seguridad y Privacidad de la Información.

#### **4. OBJETIVO GENERAL**

Definir los controles necesarios para garantizar la seguridad de la información del IMCTC.

#### **5. OBJETIVOS ESPECÍFICOS**

Objetivo 1: Promover la centralización de datos a través del uso de las herramientas informáticas institucionales implementadas y/o controladas por el IMCTC, para facilitar los procesos de backup y restauración de datos.

Objetivo 2: Registrar, clasificar, cuantificar y evaluar el reporte de incidentes que involucren riesgos de seguridad a la información, e identificar los puntos críticos que se deben atender con mayor prioridad.

Objetivo 3: Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo de información.

Objetivo 4: Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el Plan de Tratamiento de Riesgos y Privacidad de la Información.

#### **6. DEFINICIONES BÁSICAS**

**Activo de información:** Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

**Adware:** Es cualquier programa que automáticamente va mostrando publicidad al usuario durante su instalación o durante su uso y con ello genera beneficios a sus creadores. Aunque se asocia al malware, no tiene que serlo forzosamente, ya que puede ser un medio legítimo usado por desarrolladores de software que lo implementan en sus programas, generalmente en las versiones shareware, haciéndolo desaparecer en el momento en que adquirimos la versión completa del programa. Se convierte en malware en el momento en que empieza a recopilar información sobre el equipo donde se encuentra instalado.

**Antivirus:** Es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como malware. Es un proceso mediante el cual la organización determina e nivel de exposición y la predisposición a la pérdida de un elemento o grupo de elementos ante una amenaza específica. Para solucionar estos inconvenientes es posible aplicar distintos métodos para llevar a cabo la evaluación de fallas en la infraestructura de una organización.

**Análisis de riesgos:** Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que





se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

**Autenticación:** Procedimiento para comprobar que alguien es quién dice ser cuando accede a un equipo o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

**Backup:** Copia de seguridad que se realiza sobre archivos o aplicaciones contenidas en un equipo con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

**Biometría:** La biometría es un método de reconocimiento de personas basado en sus características fisiológicas (huellas dactilares, retinas, iris, cara, etc.) o de comportamiento (firma, forma de andar, tecleo, etc.).

**Bluesnarfing:** La técnica consiste en aprovecharse de las vulnerabilidades de la tecnología Bluetooth de tus dispositivos móviles. Sin tu conocimiento, alguien más se conecta a tu celular, por ejemplo, y puede robar información como tu lista de contactos, mensajes de texto, correo electrónico y más

**Bug:** Es un error o fallo en un programa de dispositivo o sistema de software que desencadena un resultado indeseado.

**Bulo:** También llamados hoax, son noticias falsas creadas para su reenvío masivo ya sea a través de redes sociales, mensajería instantánea o correo electrónico, con el fin de hacer creer al destinatario que algo es falso.

**Certificado digital:** Un certificado digital es un fichero informático generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.

**Cookie:** Una cookie es un pequeño fichero que almacena información enviada por un sitio web y que se almacena en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

**Ciberseguridad:** Conjunto de tecnologías, procesos y prácticas diseñados para proteger redes, computadoras, programas y datos de ataques, daños o accesos no autorizados. La ciberseguridad trata de trabajar en robustos sistemas que sean capaces de actuar antes, durante y después, no sirve solo para prevenir, sino también dar confianza a los clientes y al mercado, pudiendo así reducir el riesgo de exposición del usuario y de los sistemas.

**Criptografía:** La criptografía es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado.

**Denegación de servicio, DDos, DoS:** Es un tipo de vulnerabilidad muy utilizada con la que se persigue conseguir acceso remoto al sistema atacado. Un desbordamiento de búfer intenta aprovechar





defectos en la programación que provocan un error o el cuelgue del sistema. Un desbordamiento de búfer provoca algo similar a lo que ocurre cuando llenamos un vaso más allá de su capacidad: éste se desborda y el contenido se derrama.

**Exploit:** Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto.

**Firewall:** Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios.

**Gusano, Worm:** Es un programa malicioso (o malware) que tiene como característica principal su alto grado de «dispersabilidad», es decir, lo rápidamente que se propaga.

**IDS:** Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un equipo o a una red.

**Ingeniería social:** Las técnicas de ingeniería social son tácticas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima

**Inyección SQL:** Es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso. IPS Siglas de Intrusion Prevention System (sistema de prevención de intrusiones). Es un software que se utiliza para proteger a los sistemas de ataques y abusos. La tecnología de prevención de intrusos puede ser considerada como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es una tecnología más cercana a los firewall.

**Malware:** Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software.

**Metadatos:** Los metadatos son el conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión. Los metadatos es una información que enriquece el documento al que está asociado.

**Parche de seguridad:** Un parche de seguridad es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del software tras la detección de una vulnerabilidad en el software y pueden





instalarse de forma automática o manual por parte del usuario.

**Pentest (Pentesting):** Una prueba de penetración es un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software, o deficiencias operativas en las medidas de seguridad.

**PCI DSS:** PCI DSS (del Inglés Payment Card Industry Data Security Standard) es, como su nombre indica un Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago.

**Pharming:** Ataque informático que aprovecha una vulnerabilidad del software de los servidores DNS y que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad.

**Phishing:** Estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta.

**Política de seguridad:** Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riesgos a los que están expuestos.

**Puerta trasera (Backdoor):** Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema. Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos.

**Ransomware:** El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico.

**Sniffer:** Un sniffer es un programa que monitorea la información que circula por la red con el objeto de capturar información. Las tarjetas de red pueden verificar si la información recibida está dirigida o no a su sistema.

**Spoofing:** Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de malware. Los ataques de seguridad en las redes usando técnicas de spoofing ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.

**Spam:** También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). Spyware. Es un malware que recopila información de un equipo y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del equipo. El término spyware también se utiliza más ampliamente para referirse a otros productos como adware, falsos antivirus o troyanos.





**Troyano:** Se trata de un tipo de malware o software malicioso que se caracteriza por carecer de capacidad de autoreplicación. Generalmente, este tipo de malware requiere del uso de la ingeniería social para su propagación.

**Virus:** Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios: Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.

**Vulnerabilidad:** Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. Los agujeros de seguridad pueden ser aprovechadas por atacantes mediante exploits, para acceder a los sistemas con fines maliciosos. Las empresas deben ser conscientes de estos riesgos y mantener una actitud preventiva, así como llevar un control de sus sistemas mediante actualizaciones periódicas.

**Zero-day:** Vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes, son desconocidas por los fabricantes y usuarios. No existe un parche de seguridad para solucionarlas y son muy peligrosas ya que el atacante puede explotarlas sin que el usuario sea consciente de que es vulnerable.

**Zombie:** Es el nombre que se da a las computadoras controladas de manera remota por un ciberdelincuente. Generalmente se utiliza la computadora zombie para realizar actividades ilícitas a través de Internet como el envío de comunicaciones electrónicas no deseadas, o la propagación de otro malware.

## 7. MARCO NORMATIVO

- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 1266 de 2008. Disposiciones generales Habeas Data.
- Ley 1581 de 2012. Disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Transparencia y Acceso a la información Pública Nacional.
- Decreto 4170 de 2011. Creación de la ANCP-CCE.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 1083 de 2015. Único Reglamentario del Sector Función Pública, con las modificaciones y adiciones introducidas a partir de su fecha de su expedición.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo con las modificaciones y adiciones introducidas a partir de su fecha de su expedición





## 8. DIAGNÓSTICO

El IMCTC recopila, almacena y procesa información sensible en el marco de sus actividades. Por este motivo, el IMCTC destina recursos para establecer una política que describa de forma detallada los controles y actividades llevadas a cabo con el objetivo que funcionarios, contratistas y usuarios de sus servicios confíen en que su información personal y la que generan debido a su interacción con la entidad, está resguardada y no es objeto de filtraciones, robo o alguna otra situación que comprometa su privacidad.

El IMCTC cuenta con infraestructura física de tipo empresarial para la atención de los servicios de conectividad internos LAN Y Wifi, compuesta por redes de datos Cat7, Switch administrables L3, Access Point AC1750, Firewall y canal dedicados para navegación y publicación de servicios.

La infraestructura lógica está compuesta por Servicios DNS, DHCP, segmentación vLAN, enrutamiento de puertos, controlador de dominio, gestión de cuentas de usuario individual con asociación de información contractual para acceso a las herramientas de colaboración.

## 9. PLAN DE ACCIÓN ANUAL

### ESTRATEGIAS

Promoción del conocimiento de las características y el uso correcto de las herramientas informáticas disponibles y solicitudes de soporte  
Llevar a cabo implementaciones enfocadas en la protección de los datos

### META

Garantizar que contratistas y funcionarios conozcan las herramientas informáticas dispuestas por el IMCTC y el uso adecuado de las mismas, así como velar por la integridad de la información de cada usuario del dominio institucional.

### INDICADORES

Una estrategia anual de promoción de información sobre el uso de las herramientas informáticas institucionales.

Número de acciones para garantizar la integridad de la información.





## 10. CRONOGRAMA

ACTIVIDAD	RESPONSABLE	ENTREGABLE	FECHA DE INICIO	FECHA DE FINALIZACIÓN	PERIODICIDAD
Actividades de promoción, envío de información por correo electrónico y/o capacitaciones presenciales.	Contratista Área de tecnología	Listas de asistencia, evidencias de envío de información	01/02/2025	28/12/2025	Mensual
Gestión de Tickets de asistencia técnica a través de la mesa de ayuda.	Contratista Área de tecnología	Registro mensual de tickets	01/02/2025	28/12/2025	Mensual
Aplicación de métodos técnicos estándar para la protección de los datos.	Contratista Área de tecnología	Informe de actividades	01/02/2025	28/12/2025	Mensual

## 11. SEGUIMIENTO Y MONITOREO

El seguimiento de los planes institucionales se realizará de acuerdo con el formato EST-PIC-MN-002-FM-003, correspondiente al seguimiento de planes, programas y proyectos. Trimestralmente, se deberá reportar el estado de avance de cada plan.

## 12. REFERENCIAS

Glosario de Términos Seguridad Informática <https://safemode-cl.blogspot.com/2006/07/glosario-de-terminos-de-seguridad.html>

Seguridad de la información: Aspectos a tener en cuenta

<https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/>

