# POLÍTICA DE SEGURIDAD DIGITAL

Instituto Municipal de Cultura y
Turismo de Cajicá

## INTRODUCCIÓN

El Instituto Municipal de Cultura y Turismo de Cajicá hace uso de una plataforma informática para generar, recibir, almacenar, procesar y compartir información, en el marco de la ejecución de sus actividades. Esto le permite garantizar la transparencia de sus operaciones, hacerse eficiente frente a los usuarios de sus servicios y mantenerse en una ruta de constante modernización e implementación de nuevas tecnologías. Por tanto, es evidente la necesidad de establecer lineamientos para salvaguardar la información institucional y proporcionar privacidad a quienes hacen uso constante de dichos datos.

El presente documento tiene la finalidad de plasmar las Políticas de Seguridad Digital implementadas para el Inscultura.

## ALCANCE

La Política de Seguridad Digital aplica para todas las funciones institucionales que requieren acceso a los recursos informáticos disponibles. Ésta debe cumplirse por todos los funcionarios, contratistas, proveedores y terceros de cualquier naturaleza que hagan uso de los servicios digitales, desde todo tipo de dispositivos. Esto con el fin de mantener niveles de seguridad sobre la información.

## DEFINICIONES

Recurso informático: Todo equipo, dispositivo, plataforma o herramienta habilitada para el procesamiento de información digital.

Acción Correctiva: Medida orientada a eliminar la causa de cualquier amenaza, evento, riesgo o vulnerabilidad asociada a la seguridad de la información.

Acción Preventiva: Medida orientada a prevenir cualquier amenaza, evento, riesgo o vulnerabilidad asociada a la seguridad de la información.

Activo de Información: Datos o información que tienen un valor para una Entidad.

Amenaza: Circunstancia, suceso o persona con el potencial para dañar un sistema mediante la destrucción, divulgación, modificación de datos o negación de servicios.

Análisis de Riesgo: Método cualitativo o cuantitativo para la evaluación del impacto de riesgo en la toma de decisiones.

Aplicaciones: Es todo software que se utiliza para la gestión o manejo de la información.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona en cualquiera de los sistemas de información de la entidad.

Backup: Parámetros que determinan que equipo o que información debe incluirse en una copia de respaldo dentro de la entidad.

Confidencialidad: Mantener la información oculta a individuos, entidades o procesos no autorizados.

Control: Procedimiento, procesos, políticas que permiten mantener el riesgo de la seguridad de la información por debajo del riesgo presente.

Denegación de Servicio: Es una acción iniciada por un ataque a un sistema objetivo, que provoca la denegación a los usuarios legítimos forzando su cierre o conllevando a una inoperatividad.

Disponibilidad: Mantener la información accesible a quien la necesita en el momento que la necesite.

Dispositivo: Es un ordenador que se puede utilizar para acceder a los servicios de red, computador Tablet, Smartphone.

Evento: Suceso identificado en un sistema, estado que deja al descubierto una brecha de seguridad.

Ingeniería Social: Método utilizado para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la divulgación de información.

Integridad: Prevenir la modificación no autorizada de la información.

Política: Medidas necesarias para garantizar la seguridad de las tecnologías de la información.

Riesgo: Posibilidad de que ocurra un contra tiempo.

Seguridad de la Información: Según ISO 27002 es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguridad Informática: Encargada de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de gestión de seguridad de la información seguro y confiable.

Seguridad Física: Limites mínimos que se deben cumplir en cuanto a los perímetros de seguridad, de forma que se puedan establecer controles.

Seguridad Lógica: Integrar mecanismos y procedimientos que permitan monitorear el acceso a los activos de la información.

Usuario: Cualquier persona que haga uso de los servicios de red proporcionados por la entidad tales como equipos de cómputo, sistemas de información y redes.

Virus: Es un tipo de software o aplicación que tiene como objetivo alterar el normal funcionamiento de los equipos tecnológicos, sin permiso o conocimiento de los usuarios.

Vulnerabilidad: Condición de un sistema que lo hace susceptible a una amenaza

## MARCO NORMATIVO

El Instituto Municipal de Cultura y Turismo de Cajicá opera dentro del marco legal aplicable en Colombia en materia de Seguridad y Privacidad de la Información, teniendo como objetivo, asegurar la integridad, confidencialidad y disponibilidad de la Información en la Entidad y actuar de acuerdo a las políticas establecidas para las entidades públicas.

## OBJETIVOS

### Objetivo general

Asegurar la integridad de la información institucional, disponer los datos en el momento y lugar en que los usuarios lo requieran y garantizar el acceso únicamente a las personas autorizadas según la naturaleza de sus funciones.

### Objetivos específicos

- Identificar las plataformas y herramientas tecnológicas oficiales para la generación y procesamiento de información institucional, en la cuales se garantizará la integridad, disponibilidad y confidencialidad de los datos.
- Definir los parámetros generales de uso de las plataformas y herramientas tecnológicas por parte de los usuarios.
- Especificar los medios y técnicas implementadas para el almacenamiento de datos a corto, mediano y largo plazo.

## POLÍTICA DE SEGURIDAD DIGITAL

### Herramientas Informáticas Institucionales

Todas las herramientas y plataformas para procesamiento de datos en el Instituto Municipal de Cultura y Turismo de Cajicá, estarán implementadas bajo los dominios *culturacajica.gov.co* y *turismocajica.gov.co*. Las herramientas y/o plataformas de terceros y que se ofrecen para uso institucional deberán incluir un subdominio de fácil identificación institucional. Los usuarios deben abstenerse de ingresar información institucional en herramientas que no correspondan a estos dominios puesto que se considerará información no controlada, violando la presente Política de Seguridad Digital.

El Instituto garantizará la integridad y privacidad de los datos contenidos en las siguientes plataformas.

- ✓ *mail.culturacajica.gov.co*

ofrece servicios de correo electrónico y calendario institucional para los dominios culturacajica.gov.co y turismocajica.gov.co, y es accesible mediante aplicaciones para dispositivos móviles, clientes para Windows y Mac y un entorno web desde el cual se podrá cambiar la contraseña de la cuenta. Los usuarios deberán usar esta plataforma para:

- Enviar y recibir correo electrónico con información institucional. Así mismo, la cuenta opera como identificador para el acceso de los usuarios a los otros servicios de la red institucional.
- Crear invitaciones a eventos y reuniones. Está disponible la programación de fechas, horas, días completos y la aceptación interactiva de los invitados, así como mostrar en tiempo real el estado de los usuarios del dominio durante la programación propuesta. Es posible la descripción de las actividades, inserción de notas y el envío de documentos.
- Gestionar la contraseña de la cuenta. El usuario podrá cambiar la contraseña de su cuenta todas las veces que desee siempre y cuando se cumpla la política de contraseñas.

✓ *cloud.culturacajica.gov.co*

es la plataforma aprobada para el almacenamiento de archivos en un entorno de nube. Permite el almacenamiento y edición de documentos, compartición de información con usuarios del dominio dentro de la misma plataforma y la creación de links públicos para la compartición de información con usuarios externos. La plataforma está concebida como un entorno de almacenamiento de corto plazo dada la facilidad de uso y su escasa cuota de espacio por usuario establecida en 20 GB. Los usuarios deben usar esta plataforma en los siguientes casos:

- Cuando se requiere almacenar información institucional. El software integrado en el servicio permite editar documentos como hojas de cálculo, documentos de texto y presentaciones.
- Compartir información con otros usuarios.
- Realizar edición colaborativa en tiempo real sobre un documento.
- Adjuntar links de archivos o carpetas que superan el tamaño permitido por el servicio de correo electrónico para envío de adjuntos.
- Generación de encuestas y obtención de resultados.

✓ *Servidor de archivos*

Espacio de almacenamiento de red concebido para el almacenamiento a largo plazo de la información institucional. Se alinea con las tablas de retención documental establecidas por el Área de Archivo y su acceso se controla mediante políticas de directorio activo.

**Política de contraseñas**

Las contraseñas de usuario en el entorno del Instituto deben cumplir con los siguientes requisitos.

- Tener mínimo 10 caracteres incluyendo números, letras mayúsculas y minúsculas, - y al menos un carácter especial.
- La contraseña no puede ser igual a alguna utilizada en las últimas 10 modificaciones.

- Se debe tener en cuenta que, una vez cambiada la contraseña, esta se modificará para todos los servicios asociados.
- La duración máxima de una contraseña es de 12 meses.
- La cuenta institucional está ligada a la duración del contrato y se bloqueará de forma automática una vez éste llegue a su fecha de vencimiento.

**Creación y asignación de cuentas**

La creación o reasignación de cuentas institucionales debe ser solicitada por la Dirección a la mesa de ayuda mediante el formato de asignación de cuentas. Esto asegura que la información contractual esté verificada.

La mesa de ayuda creará la cuenta ingresando las fechas de vigencia del contrato y notificará los datos de acceso al usuario, mediante correo electrónico, a la dirección personal registrada en el contrato.

**Backups y protección ante desastres informáticos**

Los servidores del Instituto Municipal de Cultura y Turismo de Cajicá están bajo una estricta vigilancia por parte del área de Gestión de Recursos Informáticos, que vela por la seguridad de las operaciones mediante controles al hardware y software instalado, así como las comunicaciones en redes locales e internet. Se utilizan variados métodos de filtrado de contenido, detectores antispam, antivirus, acl, etc. para el acceso a los datos.

Los soportes de almacenamiento utilizan técnicas de redundancia de información a nivel de hardware, software, versionamiento de archivos y rutinas de generación de backups que garantizan la integridad de los contenidos y la recuperación en caso de desastres.

**Mesa de ayuda**

Es un servicio implementado por el área de Gestión de Recursos Informáticos que consiste en la generación y seguimiento de casos mediante tickets de servicio. Los tickets de servicio permiten el seguimiento en tiempo real de los avances a las soluciones y la verificación de los tiempos de respuesta para cada una de las solicitudes realizadas por los funcionarios y contratistas del instituto.

Toda solicitud de soporte o asistencia técnica debe realizarse mediante correo electrónico a *soporte@culturacajica.gov.co*, detallando la necesidad y los datos de contacto para que el personal se comunique en caso de ser necesario.

El sistema enviará una notificación automática al momento de la creación del caso y cada vez que se registre algún avance en la solución del mismo hasta el cierre.

**Acceso a redes y uso de internet**

Se proporcionará a los funcionarios y contratistas acceso a la red informática local con una serie de servicios que incluyen navegación por internet, servicios de correo electrónico, almacenamiento cloud, impresión y demás.

El uso de estos servicios tiene como principal utilidad servir como herramienta para cumplir las tareas asignadas y la actividad laboral. Además, se debe regir por los principios de buenas prácticas, la moral y ética, así como en procura de un mejor desempeño y productividad de quien lo haga.

El uso de los recursos informáticos considerado inaceptable puede comprender la pérdida del acceso, dar lugar a la revocación de permisos y/o las sanciones legales aplicables.

En cuanto a la navegación por Internet, se considera uso inaceptable:

- Descargar material con expresa y manifiesta propiedad intelectual u otros derechos necesarios para dicha descarga o uso, sin los permisos necesarios, las licencias que correspondan o cualquier otro formalismo que deba cumplirse y se omita intencionalmente.
- Utilizar Internet para almacenamiento, divulgación o transmisión de cualquier información, archivos, documentos, imágenes, sonidos u obras que puedan infringir el marco normativo vigente referido a propiedad intelectual, marcas o patentes.
- Involucrarse o participar de cualquier manera en actividades ilícitas en cualquier sitio y desde cualquier dispositivo conectado a la red desde el servicio de Internet.
- Divulgación de información deliberadamente falsa, sensible o difamatoria sobre personas o instituciones en cualquier sitio o herramienta disponible en línea (correo electrónico, webs, wiki, redes sociales, chat, foros, etc.).
- Hacer uso del servicio de Internet sin contar con herramientas básicas de resguardo y seguridad, instaladas en el computador o dispositivo a emplear, a saber: antimalware y las actualizaciones del sistema operativo que posea el computador o dispositivo. La validación de estas condiciones será determinada y pueden consultarse con el área de gestión de recursos Informáticos.
- Hacer uso de herramientas de software instaladas que habiliten servicios potencialmente riesgosos para el Instituto. La validación de estas condiciones debe consultarse con el área de gestión de recursos Informáticos.
- El uso del servicio de Internet en situaciones que afecten la dignidad humana, tengan carácter discriminatorio u ofensivo, sean usados para amenazar y generar persecuciones a personas o empresas, generen situaciones de acoso laboral, sexual, contrarias a la moral, pornografía o similares.

El Instituto Municipal de Cultura y Turismo de Cajicá se reserva el derecho de establecer la prioridad para la prestación del servicio de acceso a Internet y demás servicios informáticos en función de las necesidades propias.

## LÍNEA BASE

El Instituto Municipal de Cultura y Turismo de Cajicá cuenta actualmente con recursos informáticos representados en computadores, licencias de software,

servidores, servicios de virtualización, servicios web y demás. Esta política de Seguridad Digital está encaminada a la optimización del uso de dichos recursos y la implementación de otros con medidas que aporten fluidez en términos de seguridad.

La generación de un ambiente de trabajo digital seguro es importante para la reputación de la entidad y el desempeño institucional.

## FORMULACIÓN Y APROBACIÓN

La presente Política de Seguridad Digital es formulada por el área de Gestión de Recursos Informáticos del Instituto. En este documento se detallan los elementos más importantes para la gestión de la seguridad informática y se establecen los lineamientos generales para el uso de los recursos disponibles.

Esta política debe ser aprobada y publicada por parte de la Dirección y será actualizada conforme a la evolución de los sistemas de almacenamiento y procesamiento de información instalados.

**HÉCTOR EMILIO MONCADA GARZÓN**

**Director Ejecutivo**

| | NOMBRES Y APELLIDOS | FIRMA | ÁREA |
|---|---|---|---|
| **Proyectó:** | Carlos Julio Murcia | | CPS Recursos Informaticos |
| **Revisó:** | Daniel Edgardo Baena | | Técnico Administrativo |
| **Revisó:** | Shirley Jiménez Rodríguez | | Profesional Universitario |
| **Revisó y aprobó:** | Héctor Emilio Moncada Garzón | | Director Ejecutivo |
| Los firmantes, manifestamos expresamente que hemos estudiado y revisado el presente acto administrativo, y por encontrarlo ajustado a las disposiciones constitucionales, legales y reglamentarias vigentes, lo presentamos para su firma bajo nuestra responsabilidad. | | | |