1. OBJETIVO

Desarrollar las actividades necesarias para garantizar la integridad física de los recursos informáticos, así como resguardar la información que se genera en cada uno de los servicios que presta la Alcaldía Municipal de Cajicá.

1.1 OBJETIVOS ESPECIFICOS

- Implementar medidas que brinden integridad, disponibilidad y privacidad de los activos de la información para la Administración Municipal.
- Crear Mecanismos de seguridad que brinden protección de la infraestructura de bienes tangibles como intangibles
- Establecer Normas y Políticas que reduzcan el riesgo de la información, para salvaguardarla de amenazas y vulnerabilidades.
- Establecer actividades que sean acordes con lo establecido en la NTCPG:1000 a fin de cumplir con la disposiciones adoptadas por el Calidad y Control Interno.

2. ALCANCE

El alcance de este Plan, abarca todos los elementos informáticos con que cuenta la institución, y el 100% de la información que se captura a través de los diferentes canales de comunicación definidos por la administración municipal. Este plan de seguridad informático abarca todos aquellos elementos informáticos pertenecientes a la institución

3. DEFINICIONES

CONFIDENCIALIDAD	Propiedad que impide la divulgación de información a personas o sistemas no autorizados.
INTEGRIDAD	Propiedad que busca mantener los datos libres de modificaciones no autorizadas
DISPONIBILIDAD	Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones
AUTENTICACIÓN	Propiedad que permite identificar el generador de la información
RIESGO	Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio
AMENAZA	Cualquier acción o evento que puede ocasionar consecuencias adversas
IMPACTO	Son los resultados y consecuencias de que se materialice un riesgo
SEGURIDAD	Es una forma de protección contra los riesgos
CONTROL	Cualquier acción o proceso que se utiliza para mitigar el riesgo
POLÍTICA	declaración de alto nivel sobre la intención y la dirección de la gerencia
NORMA	Establecer los límites permisibles de acciones y procesos para cumplir con las políticas
CLASIFICACIÓN DE DATOS	El proceso de determinar la sensibilidad y Criticidad de la información
ACTIVO	Cualquier cosa que tenga valor para la administración

COPIA CONTROLADA

4. DOCUMENTOS DE REFERENCIA Y NORMATIVIDAD

ISO 27001. Tecnología de la Información

Decreto 1599 de 2005: "Por el cual se adopta el Modelo Estándar de Control Interno MECI 1000:2005"

NTCISO 9001:2008: Norma Internacional que especifica los requisitos para un sistema de gestión de la calidad.

Decreto 4485 de 2009: "Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad de la Gestión Pública NTCGP 1000 versión 2009"

NTCGP 1000:2009 Norma Técnica de Calidad en la Gestión Pública, la cual establece los requisitos para la implementación de un Sistema Integrado de Gestión aplicable a la rama ejecutiva del poder público y otras entidades prestadoras de servicios en Colombia.

5. DEFINICION DE ACTIVIDADES

5.1. HARDWARE Y SOFTWARE:

Para conseguir dotar a la empresa de un nivel de seguridad de su información conveniente se van a cumplir los siguientes pasos:

- Elaboración de un plano actualizado que contenga la distribución de los equipos que se encuentran en la Administración, teniendo en cuenta las Jerarquías de la información que se debe proteger, según el funcionario.
- Contar con un plano de las diferentes redes eléctricas, telefónicas y datos existentes.
- Elaboración de un inventario del Hardware y Software con que cuenta la institución.
- Elaboración y alimentación permanente de una hoja de vida para cada equipo, en donde se deben evidenciar las características físicas de cada uno y los soportes de lso mantenimiento preventivo y correctivos efectuados.
- Crear barreas de seguridad con aplicaciones de protección, como antivirus, encriptación de claves, y perfiles que eviten programas maliciosos, Intrusos y ataques.

5.2 RIESGOS

- Realizar un análisis de riesgos completo de todo el sistema informático de la administración para evaluar las posibles amenazas que pueden afectarla, las vulnerabilidades de ésta con respecto a los riesgos y consecuencias que estas Amenazas pudieran Generar en el caso de llegar a materializarse. Esto se realizará utilizando la metodología definida por el Departamento Administrativa de la Función Pública (DAFP) para identificación, análisis y valoración de riesgos

5.3 POLITICAS

Las Políticas en Informática son el conjunto de lineamientos enmarcados en el ámbito jurídico y administrativo. Estas normas inciden en la adquisición y el uso de los Bienes y Servicios Informáticos, las cuales se deberán de acatar y desplegar por la totalidad de los integrantes de la Administración municipal. Dentro de estas políticas tenemos las siguientes:

5.3.1 ADQUISICION DE BIENES INFORMÁTICOS

- Toda adquisición de tecnología informática se efectuará a través del Comité de adquisiciones, que contará con la participación de los integrantes del área de sistemas de la Alcaldía municipal.
- Al planear las actividades relativas a la adquisición de Bienes informáticos, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad.
- Para la adquisición de Hardware se deberá tener en cuenta que los equipos o componentes deberán contar con presencia y permanencia demostrada en el mercado nacional e internacional, así como con asistencia técnica y repuestos, deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.
- En la adquisición de Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente.
- Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales, catálogos y sistemas de instalación, los cuales deben reposar en el área de sistemas de la Alcaldía Municipal.

5.3.2 INSTALACION DE EQUIPOS

- La instalación de equipos para uso interno se realizará en lugares adecuados, lejos de polvo y tráfico de personas; conforme a la norma de seguridad e higiene las áreas operativas deberán contar con un croquis actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.
- Las instalaciones eléctricas y de comunicaciones, estarán de preferencia fija o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.

- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.
- Instalación de dispositivos de protección de líneas eléctricas contra sobrecargas
- Revisión periódica de la instalación eléctrica.
- Distribución de extintores a lo largo de toda la dependencia de la empresa, en especial cerca de elementos informáticos críticos
- Se debe evitar mover el equipo mientras está en funcionamiento o activo, evitar golpes o movimientos bruscos que pueden afectar su parte interna.

5.3.3. INFORMACION

- La información almacenada en medios magnéticos se deberá inventariar, anexando la descripción y las especificaciones de la misma, clasificándola de acuerdo con su nivel de importancia dentro de cada proceso.
- Se realizarán backups de acuerdo con la importancia de la información. Para esto se elaborará un cronograma que deberá ser socializado en las diferentes dependencias y se hará seguimiento al cumplimiento del mismo.
- Para la realización de backups, el área de sistemas de la Alcaldía municipal informará a cada funcionario en donde puede ubicar la información a la cual debe realizarse copia de seguridad y el mecanismo para realizarla.
- La información almacenada en medios magnéticos, de carácter histórico, quedará documentada como activos del área de Gestión Documental y estará debidamente resguardada en su lugar de almacenamiento.

5.3.4. FUNCIONAMIENTO DE LOS EQUIPOS DE COMPUTO

- Es responsabilidad del área de sistemas de la Alcaldía Municipal, vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.
- Los servidores públicos, al usar el equipo de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren

la información almacenada.

- Se deberán asignar claves de acceso que permitan el uso solamente al personal autorizado en cada equipo.
- Mantener pólizas de seguros de los recursos informáticos en funcionamiento.
- En determinados casos se autorizará la utilización de dispositivos externos a los procesos informáticos. Por consiguiente, se prohíbe la instalación de software particular en las herramientas tecnológicas de la Administración. Cada usuario se hará responsable del Hardware y Software particular que requiera.

5.3.5. CONTINGENCIAS INFORMATICAS

- En caso de alguna eventualidad se procederá con un plan de contingencia que permita continuar con la operación del área con procedimientos informáticos alternos.
- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Contar con un directorio del personal encargado dentro de la Administración que brinde el soporte según sea necesario. Y el área de Sistemas debe contactar al personal externo, que deba acudir en el momento en que se detecte cualquier anomalía.

5.3.6.IDENTIFICADORES DE USUARIO Y CONTRASEÑAS

- Todos los usuarios con acceso al sistema de información de la Administración, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
- Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente y de Confidencialidad de la información.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información o según lo disponga su jefe directo.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Los identificadores para usuarios temporales se configurarán para un corto período de

tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

5.3.7. RESPONSABILIDADES PERSONALES

- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.
- Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.
- Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.
- Capacitar de manera permanente a los usuarios de la tecnología, en el manejo seguro de la misma.

5.3.8. USO DE MEMORIAS

Los dispositivos de almacenamiento externo como son las memorias USB, siempre deberán ser revisadas antes de abrir cualquier archivo por la oficina de sistemas quien dará la autorización del uso de las misma, esto con el fin de minimizar el riesgo de infección de virus en los equipos de la Alcaldía.

De igual forma el medio extraíble puede contener cualquier tipo de código malicioso, el cual puede modificar, extraer o eliminar la información, si se llegase a presentar este evento, el funcionario asumirá la perdida de información.

5.3.9. RESTRICCIÓN DE PAGINAS DE INTERNET

Se utiliza un servidor de dominio (open dns gratuito) para la restricción de las páginas con contenido inapropiado y redes sociales con excepción de la oficina de prensa y el web máster.

CONTROL DE CAMBIOS		
Fecha	**Versión**	**Tipo de Cambio**
15/05/2015	02	Se anexaron políticas de uso.
02/10/2017	03	Se actualiza el documento

Elaborado por:	Aprobado por:	Adoptado por:
Nombre: Edwin Alberto Zapata Lindarte	Nombre: Edwin Alberto Zapata Lindarte	Nombre: Nydia Corredor Hernández
Cargo: Director TICS-CTEI	Cargo: Director TICS-CTEI	Cargo: Secretaria de Planeación

COPIA CONTROLADA