PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1886
VALOR - TRABAJO - CULTURA

CALARCÁ
ALCALDÍA MUNICIPAL
2016-2019
¡Somos el cambio!

CALARCA - QUINDIO

2018

Contenido

1. GLOSARIO

- **CONFIDENCIALIDAD**: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- **ESTÁNDAR:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la organización antes de crear nuevas políticas.
- **GUÍA:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
- **HARDWARE:** Componentes físicos del ordenador, es decir, todo lo que se puede ver y tocar.
- **LAN:** Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).
- **MEJOR PRÁCTICA:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización.
- **PC:** Computador personal.
- **PROCEDIMIENTO:** Los procedimientos, definen específicamente como las

políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

- **RIESGO:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.
- **ROUTER:** Se trata de un producto de hardware que permite interconectar computadoras que funcionan en el marco de una red a través de varias conexiones (lan y wifi)
- **SOFTWARE:** Estos son los programas informáticos que hacen posible la realización de tareas específicas dentro de un computador.
- **SWITCHES:** son los encargados de la interconexión de equipos dentro de una misma red, o lo que es lo mismo, son los dispositivos que, junto al cableado, constituyen las redes de área local o LAN.
- **TROYANO:** Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.
- **USUARIO**: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la alcaldía municipal de Calarcá

- **VIRUS:** Los virus son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intensión de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador
- **VULNERABILIDAD:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

2. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno digital. Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en el compendio de las normas técnicas colombianas NTC ISO/IEC 27000 vigentes, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

La Alcaldía de Calarcá se guió con los instrumentos aportados por el MINTIC para la realización de este plan.

3. INTRODUCCIÓN

La Política de Seguridad y Privacidad de la Información es la afirmación general que representa la posición de la Alcaldía municipal de Calarcá, con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

En la Alcaldía de Calarcá, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la administración de riesgos y la consolidación de una cultura de seguridad.
Consciente de sus necesidades actuales, la Alcaldía de Calarcá implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios vigentes.

4. JUSTIFICACIÓN

El plan de seguridad y privacidad de la información para la Alcaldía de Calarcá Quindío da cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno digital además establece un modelo a seguir en la Alcaldía de Calarcá para cumplir con un orden y unas políticas establecidas por la Oficina Asesora TIC para llevar un seguimiento y un control a todo lo relacionado con las TIC (Tecnologías de la Información y las comunicaciones) en las diferente dependencias de la Administración.

Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información en las entidades, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación Colombiana.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Establecer un documento que sirva como guía y control para la Administración Municipal relacionado a todos los temas de las TIC enfatizado en la seguridad y privacidad de la Información.

5.2 OBJETIVOS ESPECÍFICOS

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de sus usuarios y servidores públicos.
- Apoyar la innovación tecnológica.
- Implementar el Plan de Copias de seguridad de la información.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, practicantes y usuarios de la administración municipal.
- Garantizar la continuidad de los procesos de la administración frente a incidentes de la plataforma tecnológica.

6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. En el presente Modelo de Seguridad y Privacidad de la Información se contemplan 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno digital, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

7. DESCRIPCIÓN DEL CICLO DE OPERACIÓN

En el presente capítulo se explica el ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Estas, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.

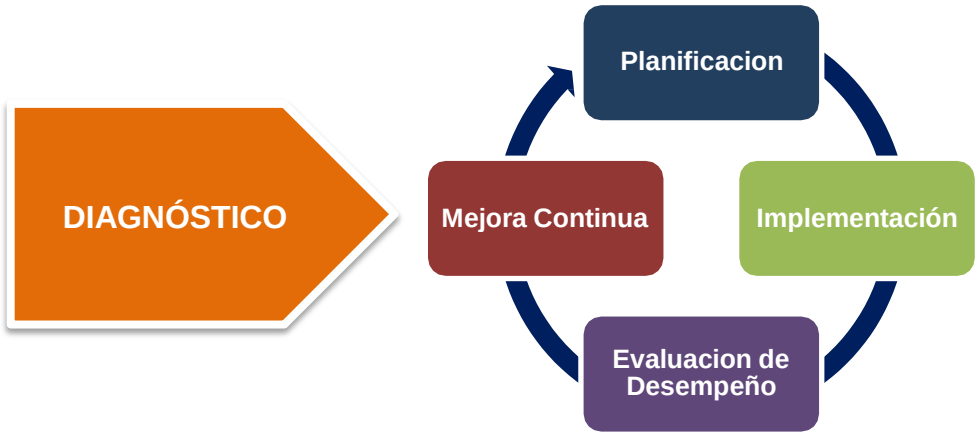

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

8. FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En esta fase se pretende identificar el estado actual de la Alcaldía de Calarcá con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Actualmente la Alcaldía de Calarcá cuenta con las siguientes deficiencias debidamente identificadas y en las cuales se pretender trabajar para la implementación del plan de seguridad y privacidad de la información.

- Negligencia de usuarios/as y decisiones institucionales:
- Falta de inducción, capacitación y sensibilización sobre riesgos
- Mal manejo de sistemas y herramientas
- Utilización de programas no autorizados / software ilegal
- Falta de pruebas de software nuevo con datos productivos
- Perdida de datos
- Infección de sistemas a través de unidades portables sin escaneo
- Manejo inadecuado de datos críticos (codificar, borrar, etc.)
- Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas)
- Compartir contraseñas o permisos a terceros no autorizados
- Transmisión de contraseñas por teléfono
- Acceso electrónico no autorizado a sistemas externos

9. FASE DE PLANIFICACIÓN

La Oficina Asesora Tic pretende por medio de este plan de seguridad y privacidad de la información generar recomendaciones, políticas, controles y operaciones básicas referentes a las TIC.

9.1 Políticas de Seguridad y Privacidad de la Información.

- Los responsables de cada área deberán apoyar al cumplimiento de los lineamientos mencionados en este plan.
- Todo usuario tendrá que cumplir con los lineamientos mencionados en este plan de lo contrario se hará acreedor a una sanción que se designará por el nivel directivo.
- Las medidas anteriores son enunciativas y no limitativas, el área de sistemas se mantendrá en contacto con los usuarios para hacerles saber de las nuevas disposiciones tecnológicas y de procedimientos.

9.2 Procedimientos de Seguridad de la Información.

A continuación se expondrá todos los procedimientos para cumplir a cabalidad con los procesos relacionados a las TIC y definidos por la Oficina Asesora TIC.

9.2.1 COMPUTADORES, PORTATILES, SERVIDORES

Políticas

Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la Alcaldía Municipal de Calarcá sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones.

Controles

- El equipo de cómputo será asignado de acuerdo al puesto o función laboral en su área de trabajo. Siendo el responsable de dicha asignación el Director del Área.
- Cada equipo está preparado con el Hardware y Software básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos.
- En caso de presentar una falla física o lógica se deberá notificar al área de Informática y en el caso de ser requerido enviar el equipo para su revisión y/o reparación de acuerdo al procedimiento establecido.
- En ningún caso el usuario intentará reparar el equipo ó diagnosticarlo, únicamente debe informar de la posible falla.
- El usuario será el único responsable del equipo de cómputo.
- En ningún caso, el usuario tendrá cerca alimentos, bebidas u otros materiales que puedan derramarse sobre el equipo.
- Solo se utilizará el equipo para funciones de interés del área y de ninguna manera para asuntos personales.
- El personal asignado deberá comprobar sus conocimientos o experiencia en el manejo del equipo de cómputo y periféricos básicos.
- En caso de que el usuario no tenga conocimientos y/o experiencia, se notificará al área de sistemas para su correspondiente Capacitación.
- La adquisición de equipo será con cargo al presupuesto de cada área o de la secretaria general, las características técnicas serán proporcionadas por el área de sistemas.
- La solicitud del equipo de cómputo será responsabilidad del área interesada, bajo las características técnicas definidas por el área de sistemas e informando a las áreas relacionadas con la asignación de los recursos.

- Toda recepción de equipo de cómputo por adquisición o donación se realizará a través del Área de Inventarios, con el apoyo del área de sistemas.
- La salida de equipo de cómputo del Almacén, será total responsabilidad del almacén, el cual revisará la integridad física y el área de sistemas instalará la integridad lógica e instalará y preparará el software y hardware correspondiente a las licencias contenidas.
- Cada equipo contiene el software de acuerdo a las necesidades del área de trabajo, El cual No deberá ser alterado.
- Por ningún motivo el usuario instalará software de promoción y/o entretenimiento.
- La adquisición o desarrollo de software será responsabilidad del área de sistemas.
- El usuario deberá reportar de forma inmediata al Área de Sistemas cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, contactos eléctricos con riesgo de incendio u otros.
- El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.
- Es responsabilidad del usuario evitar en todo momento la fuga de la información de la institución que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.
- Cualquier persona que tenga acceso a las instalaciones de la institución, deberá registrar al Momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la Institución, en el área de recepción, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.
- Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la autorización de salida del área de Inventarios anexando el vale de salida del equipo

debidamente por el secretario de la oficina o la equivalente en las dependencias de la institución.

- Los centros de cómputo u oficina de servidores de la Institución son áreas restringidas, por lo que sólo el personal autorizado por el área Sistemas puede acceder a ellos.
- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Área de Sistemas, en caso de requerir este servicio deberá solicitarlo atreves de la mesa de ayuda.
- El Área de Inventarios será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el área de Sistemas.
- El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de la institución.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro en el servidor o equipo, o en su defecto en la carpeta “Mis Documentos” ya que las otras están destinadas para archivos de programa y sistema operativo.
- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.
- Se debe mantener el equipo informático en un entorno limpio y sin humedad.
- Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación al área de Sistemas a través de un plan detallado o una solicitud para el debido acompañamiento del área de sistemas.

- Queda prohibido que el usuario abra o desarme los equipos de cómputo.
- Únicamente el personal autorizado por el Área de Sistemas y Calidad podrá llevar a cabo los servicios y reparaciones al equipo informático.
- El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- El usuario deberá dar aviso inmediato al Área de Sistemas y Calidad, e Inventarios de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.
- El uso de los grabadores de discos externos es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.
- El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se les dé.
- El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, se levantara un reporte de incumplimiento de políticas de seguridad.
- Los equipos de la Alcaldía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- Debe respetarse y no modificar la configuración de hardware y software establecida por el Área de sistemas.
- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el bloqueo de pantalla para que se active al cabo de 20 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además, el usuario debe activarlo manualmente cada vez que se ausente de su oficina.
- Si un computador tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en computadores que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Alcaldía.
- menos que se indique lo contrario, los usuarios deben asumir que todo el software de la institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.
- Los usuarios no deben copiar a un medio removible (como una USB), el software o los datos históricos residentes en las computadoras de la Alcaldía, sin la aprobación previa del área de sistemas o del jefe inmediato.
- No pueden extraerse datos fuera de la institución sin la aprobación previa de la Administración. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.
- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al área de sistemas y poner el computador en cuarentena hasta que el problema sea resuelto.
- Sólo pueden descargarse archivos de redes externas de acuerdo a los procedimientos establecidos.
- Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otras dependencias de la institución.
- No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el área de sistemas
- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de

distribución gratuita o shareware, a menos que haya sido previamente aprobado por el área de sistemas.

- Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.
- No deben usarse USB u otros medios de almacenamiento en cualquier computador de la institución a menos que se haya sido previamente verificado que están libres de virus u otros agentes dañinos.
- Periódicamente debe hacerse el respaldo de los datos guardados en computadores y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de la institución deben guardarse en otra sede, lejos del edificio.
- Los usuarios de computadores son responsables de proteger los programas y datos contra pérdida o daño.
- El área de sistemas será responsable de la generación de las copias de seguridad de los equipos de la entidad y definirá la frecuencia del respaldo.
- Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de la institución.
- No debe dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la institución.
- El personal que utiliza un computador portátil que contenga información confidencial de la institución, no debe dejarlo desatendido, sobre todo cuando esté de viaje.
- Todos los equipos permanecerán en el lugar registrado por el área de almacén.

- Solo los equipos portátiles de propiedad de la Alcaldía del Municipio de Calarcá podrán desplazarse con previa autorización del responsable de la dependencia y bajo la responsabilidad total del usuario.

9.2.2. USO DE INTERNET

Políticas

La alcaldía municipal de Calarcá consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

Controles

- El acceso a internet deberá encontrarse protegido por filtros para disminuir sitios peligrosos que contengan códigos maliciosos o que se encuentren ajenos al servicio, Permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.
- No navegar por sitios no confiables.
- Se prohíbe el uso de sitios de radios online a excepción de sitios institucionales.
- Se prohíbe el uso de intercambio de archivos a través de sistemas o programas de internet, sin que estos cuenten con la debida acreditación y controles de seguridad.
- Se prohíbe el uso de sitios de chat (Messenger, chat, etc.), a menos que este sea de uso institucional.
- Se prohíbe el uso de internet para actividades ilícitas.
- Se prohíbe la descarga que no cumpla con la normativa vigente de copyright y similar.
- Se prohíbe el acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la

calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.

- No compartir sus claves para ingresar a sitios que lo requiera (Bancos, Correo)
- No permitir que el navegador de internet recuerde la contraseña automáticamente.
- Evitar participar en juegos de entretenimiento en línea.
- Si no está navegando por internet, cierre todas las ventanas abiertas.
- Cualquier archivo que se reciba o descargue de internet deberá revisarse con el antivirus para asegurar que no tenga virus.
- Si requiere navegar en algún sitio bloqueado se deberá solicitar al área de sistemas.

9.2.2 MANEJO DE REDES SOCIALES

Políticas

La alcaldía municipal de Calarcá con el fin Definir las pautas generales para asegurar una adecuada protección de la información y un adecuado manejo, en el uso las redes sociales, por parte de los usuarios autorizados.

Controles

- En lo posible la Entidad deberá bloquear todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus. Si algún funcionario por motivos de trabajo requiera acceder a ellos, deberá enviar la solicitud formal al área de sistemas.
- Solo podrán tener acceso a redes sociales un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.
- La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la alcaldía municipal de Calarcá , que sea creado a nombre personal, como redes sociales, twitter®, facebook®,

youtube® likedink® o blogs, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

9.2.3. MANEJO DE IMPRESORAS

Políticas

Estas políticas son necesarias con el fin de Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Controles

- Los documentos que se impriman en las impresoras De la alcaldía municipal de Calarcá deben ser de carácter institucional.

- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la mesa de ayuda de la alcaldía municipal de Calarcá.

9.2.4 MANEJO APROPIADO DE CONTROL DE VIRUS

Políticas

La alcaldía municipal de Calarcá con el fin Definir las pautas generales para asegurar una adecuada protección de la información y un adecuado manejo de los equipos, establece los lineamientos a seguir para proteger los activos de la entidad contra amenazas informáticas.

Controles

- La Entidad deberá definir un producto estándar licenciado entorno de sus estaciones de trabajo, resguardando el correcto funcionamiento de los equipos computo.
- El sistema de actualizaciones y detección diaria deberá estar automatizado.
- Se debe comunicar de cualquier infección por virus que no fue eliminada por el antivirus, al área de sistemas.
- Los usuarios no podrán desinstalar o cambiar el producto de antivirus existente en su equipo.
- Los dispositivos extraíbles, antes de ser usados deben ser escaneados con el antivirus.

9.2.5 SWITCHES Y ROUTERS

Política

El Área de Sistemas es absolutamente responsable del manejo de los dispositivos de red entiéndase por Routers y Switches de los que dispone la institución, velando porque estén dispuestos en lugares seguros y protegidos a nivel físico, así como también a nivel lógico.

Controles

- Las contraseñas predefinidas que traen los dispositivos nuevos, deben cambiarse inmediatamente al ponerse en servicio el dispositivo.
- Se deberá designar al personal que efectuará las actividades de instalación, desinstalación, mantenimiento y conexión física de estos dispositivos.
- Definir procedimientos de recuperación ante eventualidades físicas.
- Definir procedimientos de respuesta, autoridades y los objetivos de la respuesta después de un ataque exitoso, incluir esquemas de preservación de la evidencia.
- Se deberán enumerar protocolos, puertos y servicios a ser permitidos o filtrados en cada interface, así como los procedimientos para su autorización.
- Se deberán identificar los servicios de configuración dinámica de los Routers, y las redes permitidas para accesar a dichos servicios
- Se deben tener plenamente identificados los protocolos de ruteo a utilizar, y los esquemas de seguridad que proveen Seguridad en el Router.

9.2.6. CORREO ELECTRÓNICO INSTITUCIONAL

Política

El correo electrónico es de carácter personal e intransferible, es deber de cada uno de los usuarios mantener el uso de este y de su contraseña siguiendo estas dos premisas y por ningún motivo se debe permitir a otra persona fuera de su dependencia acceder a este recurso. Todo esto para facilitar la comunicación entre funcionarios y terceras partes. Por este motivo la alcaldía municipal de Calarcá proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

Controles

- Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la Alcaldía Municipal de Calarcá. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- El Correo electrónico institucional es de uso exclusivo para actividades relacionadas con la Entidad y queda restringido el uso para otros fines.
- Se prohíbe expresamente el envío de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada pornográfica, difamatoria, racista, música, videos, etc., o que atente contra las buenas costumbres o principios.
- La contraseña de correo debe ser cambiada periódicamente e informar de la nueva contraseña al área de sistemas.
- No abrir link sospechoso llegados por correos electrónicos (bancos, tiendas, etc.).
- No completar datos personales en correos electrónicos sospechosos.
- Eliminar periódicamente los correos no deseados (spam o sospechoso).
- Los Accesos a la red (Internet) serán solo de interés laboral y no personal. Se establecen horarios de uso a fin de no saturar el canal y poder hacer un buen uso del mismo.
- Las páginas de consulta común por su contenido de interés general y de carácter laboral como: DANE, DAFP, presidencia, notinet, soi, www.calarca-quindio.gov.co, gobierno en línea etc. Se pueden consultar en cualquier momento dentro del horario laboral.
- De ninguna manera se podrá acceder a páginas de entretenimiento, pornografía o fuera del contexto laboral.
- El usuario no deberá bajar (ó copiar) archivos sospechoso o con extensiones desconocidas de la red sin autorización del área de sistemas.

- La comunicación estará limitada por las políticas de seguridad del área de Sistemas.
- Solo se enviará y recibirá información de interés laboral.
- En ningún caso de recibir información en archivos adjuntos de dudosa procedencia o que no esté esperando, se notificará al área de sistemas, para analizar y evitar que ingresen virus al sistema.
- Al enviar información el responsable será el usuario correspondiente.
- No se deberá enviar información de tipo estadístico, informativo o información relevante de las acciones de la Dirección, Área de trabajo o del Gobierno Municipal a ningún destino no autorizado.
- Se tienen correos institucionales dentro de la política de austeridad en el gasto público, se recomienda su uso para toda la comunicación interna y ahorrar tinta y papel, igualmente las carpetas compartidas por la LAN para mover y compartir información.k8
- El uso de Internet está limitado por las políticas de seguridad del área de sistemas.

9.2.7. BASES DE DATOS

Política

Es obligación de la Institución y en especial del administrador de la base de datos controlar todo tipo de manejo que se efectué sobre la base de datos y velar por mantenerla protegida contra todo tipo de ataque daño o intrusión sean de naturaleza externa o interna, y en caso de presentarse este tipo de situaciones deben aplicarse los procedimientos correctivos necesarios para restaurar el funcionamiento de la misma sin que ocurra perdida de información.

Es política de la institución prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su

política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

Controles

- Es función del administrador especificar los privilegios que un usuario tiene sobre la base de datos La base de datos debe estar protegida contra el fuego, el robo y otras formas de destrucción.
- Se debe garantizar que los datos sean reconstruidos en caso de daño, efectuando periódicamente un respaldo de la información
- Los datos deben poder ser sometidos a procesos de auditoria. La falta de auditoria en los sistemas de computación ha permitido la comisión de grandes delitos.
- El sistema debe diseñarse a prueba de intromisiones. Los programadores, por ingeniosos que sean, no deben poder pasar por alto los controles.
- El sistema debe tener capacidad para verificar que sus acciones han sido autorizadas. Las acciones de los usuarios deben ser supervisadas, de modo tal que pueda descubrirse cualquier acción indebida o errónea.
- Se deberá demorar la respuesta de la base de datos ante claves erróneas aumentando la demora cada vez y se alertara si hay demasiados intentos.
- Registrar todas las entradas cada vez que un usuario entra, se debe chequear cuándo y desde dónde entró la vez anterior.
- Hacer chequeos periódicos de claves fáciles de adivinar, procesos que llevan demasiado tiempo corriendo, permisos erróneos, actividades extrañas (por ejemplo, cuando usuario está de vacaciones).
- Identificar y autorizar a los usuarios: uso de códigos de acceso y palabras claves, exámenes, impresiones digitales, reconocimiento de voz, barrido de la retina, etc.
- Se deberá contar con un sistema de manejo de autorizaciones con el fin de usar derechos de acceso dados por el terminal, por la operación que puede realizar o por la hora del día.

- Uso de técnicas de cifrado para proteger datos en la base de datos
- Manejo de la tabla de usuarios con código y contraseña, control de las operaciones efectuadas en cada sesión de trabajo por cada usuario y anotadas en la bitácora, lo cual facilita la auditoría de las bases de datos.

9.2.7. RED LAN

Política

Será considerado como un ataque a la seguridad y una falta grave, cualquier actividad no autorizada por el Área de sistemas, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la institución, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.
Por este motivo la alcaldía municipal de Calarcá como responsables de las redes de datos y los recursos de red de la institución, debe propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Controles

- El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reacomodo de cables con el personal de Sistemas.
- La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del Área de Sistemas.
- Todos los cambios en la central telefónica y en los servidores y equipos de red de la institución, incluyendo la instalación del nuevo software, el cambio de direcciones IP, la reconfiguración de Routers y Switches, deben ser documentados y

debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

- El acceso a Internet provisto a los usuarios de la institución es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.
- La solicitud para la conexión de nuevos equipos a la red de la entidad deber hacerse a través del correo de mesa de ayuda, y desde un correo institucional, por ningún motivo se permitirá la conexión de nuevos equipos sin la previa autorización del área de sistemas.
- Solo se pueden conectar a la red los dispositivos móviles que cuenten con la aprobación del área de sistemas, para lo cual debe justificar el motivo por el cual debe conectar este a la red de la alcaldía municipal de Calarcá.
- En caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada por el Área de Sistemas.
- Los usuarios de Internet de la institución tienen que reportar todos los incidentes de seguridad informática al Área de Sistemas inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.
- Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que: Serán sujetos de monitoreo de las actividades que realiza en Internet, ya que Saben que existe la prohibición al acceso de páginas no autorizadas, Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados, y Saben que existe la prohibición de descarga de software sin la autorización del Área de Sistemas
- La utilización de Internet es para el desempeño de su función y no para propósitos personales.

- Los servidores de red y los equipos de comunicación (Routers, switches, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

9.2.8. MANEJO DE CUENTAS DE USUARIOS

- Toda cuenta de acceso que se requiera modificar deberá ser solicitada al área de sistemas.
- El procedimiento de creación de cuentas, debe ser canalizado a través de la mesa de ayuda.
- En caso de tener algún problema al acceder a la cuenta de usuario, el funcionario se debe notificar inmediatamente al área de sistemas y no tratar de solucionarlo.
- El área de sistemas de tener a su disposición todas las contraseñas de los equipos a cargo de la administración municipal de la alcaldía de Calarcá.

9.2.9. OPERACIONES BÁSICAS DE PC

Para el buen uso y funcionamientos de los pc deber seguirse unos pasos para asegurar su buen funcionamiento:

- Para encender el sistema de cómputo verifique que el monitor, CPU, impresora y demás periféricos estén debidamente instalados entre si y conectados a la corriente eléctrica.

- Enseguida identifique los interruptores o botones de encendido y apagado presione o mueva según se requiera.
- Encienda la Impresora, regulador, monitor, y demás periféricos que tenga instalados dejando al final el CPU.
- Para apagar el sistema presione o mueva los interruptores según se requiera en el mismo orden antes mencionado.

Cuando encender y apagar el Sistema:

- Al inicio y fin de las actividades
- En caso de tormentas eléctricas
- Si se presentan fallas eléctricas

9.2.10. CONTRASEÑAS Y EL CONTROL DE ACCESO

Políticas

Controlar el acceso a la información.

Controles

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada, así como tampoco usar números telefónicos ni nombres de familiares. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
- Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al

usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

- Cambiar la contraseña regularmente e informar del cambio a la oficina de sistemas.
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
- Nunca grabar la contraseña en una tecla de función o en un comando de caracteres pre-definido.
- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
- No utilizar la opción de almacenar contraseñas en Internet.
- Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.
- Todas las contraseñas para acceso al Sistema Web con carácter administrativo deberán ser cambiadas al menos cada 6 meses.
- Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.
- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Compañía, pudiendo ser causal de despido.
- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

Parámetros para la creación de una contraseña:

- Contraseñas fuertes que contengan números y letras, mayúsculas y minúsculas.
- Utilizar contraseña que tengan por lo menos 8 caracteres alfanuméricos.
- Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
- No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos

9.2.11. CUMPLIMIENTO SEGURIDAD INFORMÁTICA

Políticas

El Área de sistemas de la Alcaldía Municipal de Calarcá tiene como una de sus funciones la de proponer y revisar el cumplimiento de la política de seguridad, que garanticen acciones preventivas y correctivas para el respaldo de equipos e instalaciones de cómputo, así como la de los bancos de datos de información automatizada en general.

Controles

- Los sistemas desarrollados por personal interno o externo que controle el área de Sistemas y Calidad son propiedad intelectual de la Alcaldía Municipal de Calarcá.
- El Área de sistemas podrá implantar mecanismos de control que permitan identificar tendencias en el uso de los recursos informáticos por parte del personal interno o externo. El mal uso de los recursos informáticos que sea detectado debe ser reportado
- Esta absolutamente prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el área

de sistemas.

- Ningún empleado de la Alcaldía Municipal de Calarcá puede intentar probar fallas en la Seguridad, a menos que estas pruebas sean controladas y aprobadas por el departamento de Informática.
- Se prohíbe absolutamente la escritura, generación, compilación, copia, colección, propagación, ejecución o intento de introducir cualquier tipo de código malicioso o potencialmente dañino conocidos como virus, gusanos o caballos de Troya, diseñados con el único fin de auto replicarse para dañar o afectar el desempeño o acceso a los centros de cómputo, redes o información de la Alcaldía Municipal de Calarcá.
- Los jefes de área o dependencia deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información del DAPRE.

9.2.12. PROCEDIMIENTOS O MANEJO DE INCIDENTES ESTÁNDAR PARA TRATAMIENTO DE FALLOS

Entiéndase por Incidente todo aquel evento extraordinario que ocurra con los activos evaluados de la Alcaldía Municipal de Calarcá: por ejemplo, Mantenimiento preventivo de uno o todos los computadores (Anual o Preventivo), Fallo de Activos, etc. El procedimiento en cualquiera de estos casos se debe registrar teniendo en cuenta los siguientes pasos:

En caso de falla de un activo se debe:

- Enviar un correo electrónico desde el correo institucional de la oficina al correo de mesa de ayuda, donde especifique:
  a) nombre del usuario

b) dependencia donde labora

c) datos de contacto celular, teléfono o extensión

d) la falla que seba a reportar siendo muy claros sobre esta.

- En caso de no poder enviar el correo debe comunicarse en su defecto al número de la mesa de ayuda para la asignación del personal y del número de caso de este.
- En caso de no ser factible ninguna de las opciones anteriores También puede acercarse a la oficina de Mesa de ayuda donde se tomará el servicio y se asignará el técnico.

Es de vital importancia comunicar los fallos a tiempo ya que de esto depende su pronta resolución.

Para el caso de realizar mantenimiento el preventivo anual:

- Se debe pasar el cronograma de actividades de los mantenimientos donde se especifique la dependencia sobre la cual se van a realizar, así como la fecha en que estos se van a efectuar. Lo anterior con la previa autorización del jefe o líder del área de sistemas, o el encargado del área al cual pertenezca.
- Se deben utilizar los formatos pre establecidos para estos procedimientos.
- En caso de algún cambio en el hardware o software del equipo, este debe ser colocado en la hoja de vida del equipo de cómputo.

9.2.13. IMAGEN INSTITUCIONAL

- Todos los equipos podrán tener como imágenes predeterminadas aquellas que sean institucionales.
- En el exterior de todos los equipos se respetará la imagen física de empaque.
- Todos los accesorios de apoyo podrán tener plasmadas imágenes institucionales.
- Cada usuario es responsable del cuidado de su herramienta de trabajo. Por lo que se recomienda limpiar continuamente el equipo externamente.

9.2.14. SEGURIDAD PERSONAL

Recomendaciones Generales:

- Parpadee continuamente para evitar que las pupilas se sequen, especialmente si usa lentes de contacto.
- Cambie periódicamente la dirección de su mirada para descansar el nervio ocular.
- Realice constantemente ejercicios de visión periférica.
- Mantenga limpia la pantalla del monitor para facilitar la lectura y evitar reflejos.
- Ajuste la brillantez de la pantalla.
- Ajuste la posición de la pantalla y las fuentes de iluminación (luz natural y eléctrica).
- Coloque el monitor y los documentos fuente de manera que ambos estén aproximadamente a la misma distancia de sus ojos.
- Si utiliza lentes que sean con un marco completo para leer a una distancia de 50 a 60 centímetros.

10. INVENTARIO DE ACTIVOS DE INFORMACIÓN.

La Alcaldía de Calarcá en el momento no cuenta con un documento establecido para el inventario de activos de información ya que las tablas de retención documental se encuentran en actualización debido a la nueva estructura administrativa de la Alcaldía de Calarcá.

10.1. Integración del MSPI con el Sistema de Gestión documental.

Todo el proceso de Gestión documental de la Alcaldía de Calarcá se encuentra en actualización debido a la nueva estructura administrativa de la Alcaldía de Calarcá y también para dar cumplimiento a lo establecido a nivel nacional por el Archivo General de la Nación

10.2. Identificación, Valoración Y Tratamiento de Riesgos.

Los riesgos en la seguridad de la información de la Administración Municipal se pueden clasificar en tres grupos: Actos originados por la criminalidad común, Riesgos por sucesos de origen físico y riesgos por sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales:

Actos originados por la criminalidad común:

- Sabotaje (ataque físico y electrónico)
- Daños por vandalismo
- Fraude / Estafa
- Robo / Hurto (físico)
- Robo / Hurto de información electrónica
- Virus / Ejecución no autorizado de programas

- Violación a derechos de autor

Riesgos por sucesos de origen físico:

- Incendio
- Inundación
- Sismo
- Polvo
- Falta de ventilación
- Sobrecarga eléctrica
- Falla de corriente (apagones)
- Falla de sistema / Daño disco duro

Negligencia de usuarios/as y decisiones institucionales:

- Falta de inducción, capacitación y sensibilización sobre riesgos
- Mal manejo de sistemas y herramientas
- Utilización de programas no autorizados / software ilegal
- Falta de pruebas de software nuevo con datos productivos
- Perdida de datos
- Infección de sistemas a través de unidades portables sin escaneo
- Manejo inadecuado de datos críticos (codificar, borrar, etc.)
- Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas)
- Compartir contraseñas o permisos a terceros no autorizados
- Transmisión de contraseñas por teléfono
- Acceso electrónico no autorizado a sistemas externos

10.3. Plan de Comunicaciones.

La Oficina Asesora Tic cuenta con un plan de comunicaciones para que estos planes referentes a la seguridad y privacidad de la información sean divulgadas, conocidas, entendidas y sobre todo practicadas constantemente por la Alcaldía de Calarcá, el plan se basa en la capacitación por dependencias por parte del personal de la Oficina Asesora Tic para que todo el personal de la Alcaldía comprenda la importancia de estos planes, una de las estrategias utilizadas es la capacitación personalizada por dependencias para que así se consiga un mejor entendimiento de los planes, este plan de comunicaciones está incluido dentro del Plan Anticorrupción lo que indica que siempre va en pro de una mejora constante de la Alcaldía de Calarcá.

10.4. Plan de transición de IPv4 a IPv6.

La Alcaldía de Calarcá aún no cuenta con un plan de transición de IPv4 a IPv6 ya que además de ser algo muy costoso es la tecnología y el protocolo que se maneja actualmente con el proveedor de Internet.

11. FASE DE IMPLEMENTACIÓN

Para la fase de implementación la Oficina Asesora TIC se encargara de hacer un seguimiento continuo de todo lo expuesto en los procedimientos de la seguridad y privacidad de la información anteriormente nombrados, claro está con un apoyo de la Oficina Asesora Tic para que estos procedimientos sean aplicados y practicados correctamente.

12. CON BASE A LOS RESULTADOS DE LA FASE DE PLANEACIÓN, EN LA FASE DE IMPLEMENTACIÓN DEBERÁ EJECUTARSE LAS SIGUIENTES ACTIVIDADES:

12.1. Planificación y Control Operacional.

La Oficina Asesora TIC se encargará de hacer visitas periódicas a las diferentes dependencias para conocer el manejo que se le está dando al Plan de Seguridad y Privacidad de la información y además cuando se presenten casos o daños se le explicara o se le aconsejara acciones que pueden llevar a cabo para que no vuelvan a ocurrir dichos daños o descuidos.

La Oficina Asesora TIC cuenta con una Mesa de ayuda debidamente estructurada y funcionando 100% donde documenta tanto en digital como físico todos los casos que se resuelven en la Alcaldía, esto para generar confianza en los funcionarios y para internamente sacar acciones preventivas de lo que se está presentado y no vuelva a ocurrir.

Además cabe resaltar que en la Hoja de Servicio de Mesa de Ayuda se cuenta con una encuesta de satisfacción que permite evaluar el servicio prestado por la Oficina Asesora TIC y el nivel de solución que se le da a cada caso.

12.2. Indicadores De Gestión.

Los indicadores de gestión con que la Oficina Asesora Tic se encuentra trabajando para medir la eficacia de estos planes son los estipulados dentro del Plan de Desarrollo que constantemente se deben medir y los estipulados por el Plan Anticorrupción que van enfocados a estos planes de TI.

12.3. Plan de Transición de IPv4 a IPv6.

Aun no se tiene un plan para la transición de IPv4 a IPv6 para la Alcaldía de Calarcá.

12.4. Fase de Evaluación de Desempeño

La Oficina Asesora Tic hace evaluaciones periódicas del servicio prestado y de la implementación de estos planes para su constante mejoría en la prestación del servicio y para prevenir o corregir daños que se están presentando y podrían evitarse.

12.5. Plan de Ejecución de Auditorias

El plan de ejecución de auditorías que se está manejando en la Oficina Asesora Tic son los establecidos por la Oficina Asesora de control interno quien hace sus seguimientos y auditorias con todo el plan de mejoramiento pertinente.

13. FASE DE MEJORA CONTINUA

La Oficina Asesora TIC aún no cuenta con un plan de mejoramiento propio ya que no se han plasmado y organizado los resultados de todas las auditorías realizadas por control interno y las visitas realizadas por la oficina asesora TIC, sin embargo se tienen unas metas y unas actividades establecidas para realizar la mejora continua de este plan de seguridad y privacidad de la información que han sido las expuestas anteriormente en otros ítems.

14. MODELO DE MADUREZ

Este es el nivel de madurez del MSPI en el que se encuentran la Alcaldía de Calarcá de acuerdo a la figura 7 suministrada por el MINTIC.

A continuación la figura 7, muestra los diferentes niveles que hacen parte del modelo de madurez y la figura 6 explica cada uno de ellos para su mayor entendimiento.

Figura 7- Niveles de madurez

Tabla 6 – Características de los Niveles de Madurez

Nivel	Descripción
Inexistente	• Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo no están alineados a un Modelo de Seguridad.

Inicial	• Se han identificado las debilidades en la seguridad de la información. • Los incidentes de seguridad de la información se tratan de forma reactiva.
Repetible	• Se identifican en forma general los activos de información. • Se clasifican los activos de información. • Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información.
Definido	• La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. • La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. • La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. • La Entidad tiene procedimientos formales de
Administrado	• Se revisa y monitorea periódicamente los activos de información de la Entidad. • Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. • Se evalúa la efectividad de los controles y medidas
Optimizado	• En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. • Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de

De acuerdo con las figuras 6 y 7 que identifica y explica el nivel de madurez de acuerdo a la seguridad y privacidad de la información la Alcaldía de Calarcá con su Oficina Asesor TIC tiene un nivel de madurez en MSPI de nivel 3 que quiere decir definido ya que cumple con todos los parámetros explicados en la tabla 6 a excepción del plan de transición de IPv4 a IPv6 pero se tiene como meta futura, de resto cumple con todos los parámetros y le falta muy poco para llegar a un nivel 4 ya que habría que tener implementado el modelo IPv6.

15. PRIVACIDAD DE LA INFORMACIÓN

La Alcaldía de Calarcá cuenta con su política de seguridad y privacidad de la información y protección de datos debidamente publicada en su portal web www.calarca.gov.co. A continuación se da a conocer cuál es:

Es interés de la Alcaldía de Calarcá la salvaguardia de la privacidad de la información personal del Usuario obtenida a través del Sitio Web, para lo cual se compromete a adoptar una política de confidencialidad de acuerdo con lo que se establece a continuación:

El Usuario reconoce que el ingreso de información personal, lo realiza de manera voluntaria y ante la solicitud de requerimientos específicos por la Alcaldía de Calarcá para realizar un trámite, presentar una queja o reclamo, o para acceder a los mecanismos interactivos.

El Usuario acepta que a través del registro en el Sitio Web, la Alcaldía de Calarcá recoge datos personales, los cuales no se cederán a terceros sin su conocimiento.

La recolección y tratamiento automatizado de los datos personales, como consecuencia de la navegación y/o registro por el Sitio Web tiene como finalidades las detalladas a continuación: la adecuada gestión y administración de los servicios ofrecidos en el Sitio Web, en los que el Usuario decida darse de alta, utilizar o contratar; el estudio cuantitativo y cualitativo de las visitas y de la utilización de los servicios por parte de los usuarios; el envío por medios tradicionales y electrónicos de información relacionados con la Alcaldía de Calarcá y sus programas y sus entidades adscritas y vinculadas; poder tramitar servicios de gobierno en línea.

La Alcaldía de Calarcá no cederá a terceros los datos personales de los usuarios que se

recogen a través de la página Web sin su consentimiento expreso. Sin perjuicio de lo anterior, el usuario consiente en que se cedan sus datos personales cuando así sea requerido por las autoridades administrativas competentes o por mandato judicial.

El Usuario también comprende que los datos por él consignados harán parte de un archivo y/o base de datos que podrá ser usado por la Alcaldía de Calarcá para efectos de surtir determinado proceso. El Usuario podrá modificar o actualizar la información suministrada en cualquier momento.

La Alcaldía de Calarcá no se responsabiliza por cualquier consecuencia derivada del ingreso indebido de terceros a la base de datos y/o por alguna falla técnica en el funcionamiento y/o conservación de datos en el sistema en cualquiera de los menús de su página web.

La Alcaldía de Calarcá podrá modificar las Políticas de Privacidad aquí contenidos, a su libre elección y en cualquier momento y los mismos estarán vigentes una vez hayan publicado en la página Web.

El Usuario se compromete a revisar periódicamente esta sección para estar informado de tales modificaciones y cada nuevo acceso del usuario a la página será considerado una aceptación tácita de las nuevas condiciones.

(La última actualización de las políticas de seguridad de la información y protección de datos personales fue: 13 de Abril de 2018).

(La construcción de estas políticas para la Alcaldía de Calarcá se ayudan con las publicadas en la página www.mintic.gov.co, adecuadas y modificadas para la Alcaldía de Calarcá).

16. FASE DE DIAGNÓSTICO

Tabla 7 - Metas, Resultados e Instrumentos de la Fase de Diagnostico

Diagnostico			
Metas	Resultados	Instrumentos MSPI	MRAE
Diagnostico	**Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad.**	**Herramienta de diagnóstico.**	
	Documento con el resultado del diagnóstico realizado por la entidad con la clasificación y distinción de los activos		

La Oficina Asesora TIC no cuenta con esta fase aun ya que no se tiene inventarios de activos de información debido a la actualización en la que se encuentra las tablas de retención documental y aun no se tiene organizado todo el material de la fase de implementación para su debido diagnóstico.

17. FASE PLANIFICACIÓN

Tabla 8 - Metas, Resultados e Instrumentos de la Fase de Planificación

Planificación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Planificación	**Documento con la política de privacidad, Debidamente aprobada por la alta dirección y socializada al interior de la entidad.** **Manual de políticas de seguridad y privacidad de la información, aprobada por la alta dirección y socializada al interior de la entidad.** **Documento con el plan de gestión de la privacidad sobre la información, aprobado por la alta dirección de la entidad.**	**Herramienta de diagnóstico.** **Guía No 4 - Roles y Responsabilidades de Seguridad y Privacidad de la Información.** **Guía No 2 – Política General.**	

La Oficina Asesora TIC no cuenta con esta fase ya que ya que no se ha realizado la anterior de Diagnóstico y además se encuentra en proceso de socialización dentro de la entidad y la aprobación por la alta dirección de la entidad.

18. FASE DE IMPLEMENTACIÓN

Tabla 9 - Metas, Resultados e Instrumentos de la Fase de Implementación

Implementación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Implementación	**Documento con los riesgos contra la privacidad identificados y las medidas de solución adoptadas a partir de la implementación del plan de gestión de la privacidad de la información** **Documento que evidencie el registro de las Bases de datos,** **Documento con el índice de información clasificada, reservada, revisada y sus procedimientos ajustados**	**Herramienta de Diagnóstico. Guía No 7 – Gestión de Riesgos.**	

La Oficina Asesora TIC no cuenta con esta fase ya que las tablas de retención documental se encuentran en actualización y no se ha realizado el documento oficial de información clasificada, reservada y revisada. Sin embargo de acuerdo a la tabla 9 se cuenta con el documento de riesgos identificados.

19. FASE DE EVALUACIÓN DEL DESEMPEÑO

Tabla 9 - Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño

Evaluación de Desempeño			
Metas	Resultados	Instrumentos MSPI	MRAE
Evaluación del desempeño	**Documento con los resultados del plan de seguimiento** **Documento con el Plan de auditoría interna y resultados revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces** **Comunicación de los indicadores al público a través de la rendición de cuentas, informe a la PGN y al Congreso de la República.**	**Guía No 16 – Evaluación del Desempeño.** **Guía No 15 – Auditoria.** **Guía No 14 – Plan de Comunicación, sensibilización y capacitación.**	

La Oficina Asesora TIC no cuenta con el plan de mejoramiento establecido sin embargo se hacen actividades para la continua mejora y el buen desempeño de todos los planes relacionados con la seguridad y privacidad de la información.

20. FASE DE MEJORA CONTINUA

Tabla 10 - Metas, Resultados e Instrumentos de la Fase de Mejora Continua

Mejora Continua			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Mejora Continua	**Documento con los resultados del plan de seguimiento** **Documento con los resultados del plan de mejoramiento revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces.** **Documento con el consolidado de las auditorias.**	**Guía No 16 – Evaluación del Desempeño.** **Guía No 17 - Mejora Continua.**	

La Oficina Asesora TIC no cuenta con el plan de mejoramiento establecido sin embargo se hacen actividades para la continua mejora y el buen desempeño de todos los planes relacionados con la seguridad y privacidad de la información.