MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ALCALDÍA MUNICIPIO DE LOS PATIOS

NORTE DE SANTANDER - COLOMBIA

2017

Proyecto: Ing. Blanca Gamboa

TABLA DE CONTENIDO

MANUAL DE NORMAS Y POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

1. OBJETIVO Establecer reglas y lineamientos técnicos para el uso controlado de activos de información que minimice el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información.

2. ALCANCE El Manual de Normas y Políticas de Seguridad Informática de la Alcaldía del Municipio de Los Patios incluye a los funcionarios de las secretarías que componen la estructura de la Entidad y a los que tienen vinculación mediante contrato. Incluye los lineamientos para proteger la información de la alcaldía y los recursos tecnológicos con la que se procesa y se almacena, así como la recuperación de la información mantenida a nivel de medios (discos, memorias, entre otros) para responder a los requerimientos de los procesos de la institución.

3. OBLIGACIONES Es un compromiso de todos los funcionarios, aprendices y terceros vinculados a la Alcaldía del Municipio de Los Patios, conocer el Manual de Normas y políticas de Seguridad informática y es su deber cumplirlas y respetarlas para el desarrollo de cualquier actividad o consulta de sus productos.

4. PROPOSITO El propósito que tiene la Alcaldía del Municipio de Los Patios al establecer el Manual de Normas y políticas de Seguridad Informática es definir las normas y lineamientos a través de este documento para que la gestión de proyectos y recursos informáticos se realice obedeciendo la directriz de seguridad y evitar que se creen vulnerabilidades que impacten la actividad de la Entidad.

5. MARCO LEGAL

Este manual de normas y políticas para la seguridad y privacidad de la información está apoyada con los siguientes decretos:

- Decreto No. 120 de 2016 de la Alcaldía de Los Patios, de la modificación de políticas de seguridad de la información.
- Decreto 040 del 28 de Marzo de 2016, modificación del comité de Gobierno en Línea y anti trámites de la alcaldía municipal de los Patios.
- Decreto 1078 de 2015, Sector de Tecnologías de la Información y las comunicaciones.

ADVERTENCIA

Cualquier funcionario de la Alcaldía de Los Patios, que se encuentre realizando actividades que vayan en contra del Manual de Normas y Políticas de Seguridad Informática, da lugar a que la Entidad realice las investigaciones disciplinarias pertinentes y reportar a los entes de control del estado cuando haya lugar.

6. DEFINICIONES

ACTIVO: Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

APLICACIONES INFORMATICAS: Son las aplicaciones o sistemas de información que reciben este término porque previamente se encuentran clasificados como vital o necesarias para el buen funcionamiento de los procesos y procedimientos misionales.

BRECHA: Término que se utiliza para denominar la diferencia que se observa entre el mecanismo de seguridad que existe y la situación ideal para evitar que germinen vulnerabilidades que impacten el negocio de la Entidad.

BUENAS PRACTICAS INFORMATICAS: Son lineamientos que contiene los principios básicos y generales para el desarrollo de los productos o servicios de la organización para la satisfacción al cliente.

CICLO DE VIDA DE LA INFORMACIÓN DIGITAL: Se refiere a la clasificación y almacenamiento de la información; siendo necesario tener en cuenta los requisitos técnicos y legales; así como tener claro los conceptos de disponibilidad y velocidad que depende de la misma clasificación que varía conforme su valor con el tiempo.

CLASIFICACION DE LAS APLICACIONES: Las aplicaciones se clasifican conforme los procesos de la entidad y son: Misional, Estratégico y de Apoyo.

CLASIFICACION DE LA INFORMACIÓN: Proceso formal que se utiliza para ubicar el nivel a la información de la Entidad con el fin de protegerla; previa estructura de valoración en atención al riesgo que se presume existe si hay una divulgación no autorizada. Generalmente la información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad informática para la Organización.

CLIENTES: Persona natural o usuario que recibe un producto Institucional.

CONFIDENCIALIDAD: Acceso a la información por parte únicamente de quienes sean autorizados.

CORRIENTE ELECTRICA REGULADA: Se utiliza para regular o mantener el voltaje de la red eléctrica para que no afecte el funcionamiento de los recursos informáticos de la Entidad.

DATO: Es una letra, número o símbolo que tiende a convertirse en información.

SECRETARÍAS: Son los grupos que conforman la estructura organizacional de la Entidad.

DISPONIBILIDAD: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

DOCUMENTO: Es el medio físico que contiene la información que se quiere transmitir.

FUNCIONARIO GENERADOR DEL PROCESAMIENTO DE LA INFORMACIÓN: Es cualquier persona que es propietaria de la información y tiene la responsabilidad de custodiarla.

INCIDENTE: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o reducción de la calidad del servicio.

INFORMACIÓN: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y que es guardada en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

INFORMACIÓN DIGITAL: Cuando la información está almacenado en un medio magnético porque cuando se imprime se convierte en documento físico.

INFORMACIÓN SENSIBLE: Es la tipificación que recibe la información que no se considerada de acceso público como por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con Internet o la información informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc.

INTEGRIDAD: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

PROVEEDORES: Negocio o empresa que ofrece servicios a otras empresas o partes de equipos informáticos Ejemplos de estos servicios incluyen: acceso a internet, operador de telefonía móvil, alojamiento de aplicaciones web etc.

FUNCIONARIO ENCARGADO DEL PROCESAMIENTO DE LA INFORMACION: Se utiliza para denominar a la persona autorizada para organizar, clasificar y valorar la información de su dependencia o área conforme al cargo de la estructura organizacional de la Entidad.

REPOSITORIO DE DOCUMENTOS: Sitio centralizado donde se almacena y mantiene información digital actualizada para consulta del personal autorizado.

REQUERIMIENTO: Necesidad de un servicio informático que el usuario solicita a través del mecanismo definido por la organización en los procedimientos normalizados.

SERVICIO: Incluye los servicios profesionales para la instalación, mantenimiento, desarrollo, integración de software y adquisiciones, enajenaciones, arrendamientos y contratación de Hardware y soporte tanto de software como de hardware; así como de la plataforma tecnológica.

SERVICIOS EQUIPOS INFORMÁTICOS: El concepto de Servicio equipos informáticos consiste en dar soporte, de forma integrada y personalizada, a todas estas herramientas que necesita hoy en día el profesional de empresa para realizar su trabajo.

Los elementos del Servicio equipos informáticos son:

• Los dispositivos: PC, portátiles, impresoras, teléfonos, sistemas de videoconferencia, etc.

• La Red de Área Local corporativa (LAN). Así como las comunicaciones de voz incluyendo el teléfono y ahora llega el momento de proporcionar y gestionar los PC y la electrónica de red necesarios para las comunicaciones de datos.

• Las comunicaciones de voz y datos WAN (Red de Área Remota), que incluyen tanto las redes privadas corporativas como el acceso a redes públicas como Internet. La integración de las comunicaciones WAN y estas cada vez se requieren con las comunicaciones LAN.

SISTEMA DE INFORMACIÓN: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

EQUIPOS INFORMÁTICOS: Conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información, en la actualidad no solo una computadora hace referencia al procesamiento de la información. Internet forma parte de ese procesamiento que, quizás, se realice de manera distribuida y remota. El procesamiento remoto, además de incorporar el concepto de telecomunicación, hoy día hace referencia a un dispositivo como un teléfono móvil o una computadora ultra-portátil, con capacidad de operar en red mediante Comunicación inalámbrica.

USUARIO: Persona que utiliza los recursos informáticos y que interactúan de forma activa en un proceso, secuencia, código etc.

7. CONDICIONES GENERALES

- Los jefes de despacho de cada secretaría en la Alcaldía municipal son los responsables de identificar y valorar su información. Todos los servidores públicos deben seguir los lineamientos enmarcados en este documento. La seguridad de la información debe estar enmarcada con los siguientes principios:

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas que estén autorizadas para tener acceso a ella.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad de la información: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Auditabilidad: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples del mismo remitente original.

No repudio: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

8. POLÍTICAS PARA EL CUIDADO DE LOS EQUIPOS INFORMÁTICOS

I. POLÍTICAS PARA EL CUIDADO DE LOS EQUIPOS INFORMÁTICOS DE LA ENTIDAD

1. La Alcaldía del Municipio de Los Patios debe definir los mecanismos para proteger la información, su uso, procesamiento, almacenamiento, difusión; y, es su deber, mantener actualizada la presente política de seguridad de la información.

2. La Alcaldía del Municipio de Los Patios, debe dar los lineamientos para clasificar, valorar y dar tratamiento de la información; así como, los recursos tecnológicos involucrados.

3. La Entidad debe evaluar el costo/beneficio de los mecanismos de seguridad y recuperación de la información así como los recursos tecnológicos involucrados.

4. Todos los usuarios de los recursos informáticos deben proteger, respaldar y evitar accesos de la información a personas no autorizadas; es decir, son responsables de cuidar todos los activos digitales de información propiedad de la entidad.

5. Todos los funcionarios de la entidad deben seguir los procedimientos de respaldo de la información personal y llevar un registro de copias de seguridad.

6. Todos los sistemas de información y recursos tecnológicos utilizados para el procesamiento deben contar con mecanismo de seguridad apropiados.

7. Todo usuario de Equipos informáticos es responsable de la protección de la información a su cargo y no debe compartir, publicar o dejar a la vista, datos como Usuario y contraseñas.

8. Todo usuario de equipos informáticos debe bloquear la sesión de trabajo de su computador al alejarse aunque sea por poco tiempo, minimizando el tiempo que la estación quede sin protección en su ausencia.

9. Toda información que provenga de un archivo externo de la Entidad o que deba ser restaurado tiene que ser analizado con el antivirus institucional vigente.

10. Ningún usuario de los recursos informáticos debe generar, compilar, copiar, almacenar, replicar o ejecutar código de computador malicioso con la intención de causar daño, afectar e interferir con los servicios de cualquier recurso.

11. Todo usuario de los recursos informáticos no debe visitar sitios restringidos por la entidad de manera explícita o implícita, o sitios que afecten la productividad en la Institución; como el acceso desde la Entidad a sitios relacionados con la pornografía, juegos etc.

12. Está prohibido descargar software de uso malicioso o documentos que brinden información que atente contra la seguridad de la información de la Alcaldía.

13. Ningún funcionario debe brindar información no autorizada en ningún sitio ya sea interno o externo de la Entidad.

14. Ningún usuario, debe descargar y/o utilizar información, archivos, imagen, sonido u otros que estén protegidos por derechos de autor de terceros sin la previa autorización de los mismos.

15. Se documentaran y divulgaran los controles que se deben aplicar para el uso adecuado de la información que se maneja en las oficinas desde el punto de vista laboral.

16. Los usuarios no deben descargar software de Internet bajo ninguna circunstancia y en caso de requerirlo debe informar al grupo de soporte de la Entidad.

II. ORGANIZACIÓN DE LA INFORMACION

1. La Alcaldía del Municipio de Los Patios debe tener el control de su información previa organización y administración, conforme la definición de su marco gerencial (funciones y responsabilidades).

2. La oficina asesora de las TIC, debe elaborar los documentos que contenga los lineamientos, guías y procedimientos para organizar, clasificar y valorar la información de la Entidad.

3. Cada dependencia debe determinar cuál es su información sensible y su disponibilidad.

4. Todos los usuarios de los recursos informáticos de la entidad deben ubicar la información que necesita ser respaldada en los lugares previamente constituidos para ello; en caso contrario son responsables de sus actos y consecuencias.

5. La Oficina Jurídica debe verificar que en todos los contratos exista el compromiso de confidencialidad de la información; así como apoyar a la Entidad para que todos los terceros

cumplan con la política de seguridad descrita en este documento; y, prestar la asesoría legal de la seguridad de la información necesaria.

III. CLASIFICACION DE LA INFORMACION

1. La oficina asesora de las TIC, debe documentar el procedimiento de Clasificación de la información como activo de la Entidad, el cual debe prevalecer los principios de la información en las cuales se basa la seguridad como son confidencialidad, integridad y disponibilidad.

2. Todas las secretarías de la Alcaldía del Municipio de Los Patios deben clasificar la información y determinar su sensibilidad y criticidad en los equipos informáticos.

3. Los funcionarios encargados de la información deben clasificar la información de acuerdo con su grado de sensibilidad y criticidad, así como de documentar y mantener actualizada la clasificación, los permisos de acceso a los sistemas de información.

4. Todos los funcionarios deben clasificar, supervisar, proteger y restringir accesos a la información generada en el ejercicio de sus funciones.

5. La oficina asesora de las TIC debe apoyar al responsable de elaborar el inventario de sus activos importantes y/o asociados a cada uno de los sistemas de información; y, luego consolidar en un solo inventario dicha información.

6. La oficina asesora de las TIC, debe anualmente revisar el inventario de sus activos importantes y/o asociados a cada uno de los sistemas de información o cuando exista un cambio que afecte el inventario unificado.

IV. SEGURIDAD DE RECURSOS HUMANOS

1. La oficina asesora de las TIC, debe documentar los lineamientos de seguridad que contribuya a reducir los posibles riesgos que el ser humano pueda cometer voluntaria o involuntariamente; que incluye el uso adecuado de instalaciones y recursos tecnológicos para la seguridad de la información.

2. La Alcaldía del Municipio de Los Patios a través de su secretaría general debe informar al personal nuevo que se vincule o contrate en la Entidad la existencia del Manual de Políticas de seguridad de la información e incluir en los contratos de estos últimos, el compromiso de confidencialidad de la información y la responsabilidad en materia de seguridad.

3. La Alcaldía del Municipio de Los Patios debe capacitar permanentemente a los funcionarios en materia de seguridad de la información y difundir las posibles amenazas y riesgos que afectan los recursos informáticos de la Entidad.

4. La oficina asesora de las TIC, debe realizar permanentemente campañas de seguridad de la información establecidas en el plan de sensibilización, capacitación y comunicación. Estas

actividades del plan van dirigidas a todos los usuarios de los recursos informáticos para evitar que realicen tareas inseguras que conlleven a perdida y destrucción de información y/o activos informáticos en la alcaldía de Los Patios.

5. En el sitio web de la alcaldía de Los Patios www.lospatios-nortedesantander.gov.co se encuentra el documento Plan de Sensibilización, Capacitación y Comunicación a disposición de la comunidad en general, con el fin de facilitar el acceso a la información respectiva.

V. SEGURIDAD FISICA AMBIENTAL

1. La Alcaldía del Municipio de Los Patios debe garantizar la seguridad física en todas las secretarías de la Entidad para prevenir e impedir accesos no autorizados, daños e interferencia a las instalaciones así como a la información que recibe y genera la entidad.

2. Todos los recursos físicos inherentes a los sistemas de información de La Alcaldía del Municipio de Los Patios como las instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc. deben estar protegidos.

3. Los recursos informáticos utilizados para el procesamiento de la información deben estar ubicados en sitios estratégicos con mecanismos de seguridad que permita controlar el acceso solo a las personas autorizadas e incluir en la protección de los mismos los traslados por motivos de mantenimiento u otros escenarios.

4. La Alcaldía del Municipio de Los Patios a través de las diferentes dependencias debe identificar y garantizar el control de los aspectos ambientales que pueden llegar a interferir el correcto funcionamiento de los recursos tecnológicos inherentes en el procesamiento y almacenamiento de la información institucional.

5. Todas las secretarías de la alcaldía municipal deben definir los niveles de seguridad física en las instalaciones de sus oficinas que está bajo su responsabilidad y como encargados del procesamiento de la información son los encargados de aprobar o negar la autorización formal del acceso a las oficinas de su competencia cuando sea requerido.

6. Todos los funcionarios de la Entidad son responsables del uso adecuado de las pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario que realiza.

VI. GESTION DE COMUNICACIONES/OPERACIONES

1. La oficina asesora de las TIC, debe garantizar el correcto funcionamiento y seguridad de las operaciones que se realizan en el Data Center de la Entidad con relación al procesamiento de la información y comunicaciones.

2. La oficina asesora de las TIC, es la encargada de definir las responsabilidades funcionales y operativas con relación al Data Center y de que se documente los procedimientos para su gestión y operación.

3. La oficina asesora de las TIC, y los funcionarios encargados de procesar información de cada una de las secretarías deben definir y documentar los requerimientos para resguardar la información por la cual es responsable.

4. La oficina asesora de las TIC, debe aprobar el procedimiento relacionado con los servicios para transportar la información cuando sea demandado, de acuerdo a su nivel de criticidad.

5. La oficina asesora de las TIC, es la encargada de mantener actualizados los procedimientos operativos identificados en esta Política de seguridad de la información.

6. La oficina asesora de las TIC, debe definir los procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

7. La oficina asesora de las TIC, debe verificar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan.

8. El personal de la oficina asesora de las TIC, debe analizar el posible impacto operativo de los cambios previstos y verificar su correcta implementación.

9. Los responsables de la gestión operativa y de comunicaciones del Data Center deben evaluar los riesgos y determinar los controles que se deben implementar, realizar monitoreo de las actividades y/o la elaboración de registros de auditoría y control periódico de los mismos.

10. La oficina asesora de las TIC, debe efectuar el monitoreo al crecimiento del volumen de la información de los sistemas que se encuentran en operación en el Data Center y evaluar la

capacidad de almacenamiento y procesamiento de los recursos utilizados, con el fin de proyectar el alcance de estos para evitar saturación en los mismos.

11. La oficina asesora de las TIC, es la encargada de evaluar los posibles cuellos de botella, que puedan generar amenaza a la seguridad o a la continuidad del procesamiento; también debe planificar la acción correctiva que corresponda.

12. La oficina asesora de las TIC, debe elaborar y documentar los procedimientos y definir los criterios para aprobar los nuevos sistemas de información, actualizaciones y nuevas versiones e incluir el procedimiento para la ejecución de las pruebas y aprobación final.

13. La oficina asesora de las TIC, deben definir los controles para la protección contra el software malicioso.

14. La oficina asesora de las TIC y los jefes de despacho deben determinar los requerimientos para proteger cada software o dato en función de su clasificación y valor para la entidad o la criticidad de la misma.

15. La oficina asesora de las TIC, debe definir y documentar el protocolo de resguardo de la información.

16. La oficina asesora de las TIC, debe llevar el control de los registros tales como los intentos de acceso a los sistemas, tiempo de inicio y cierre del mismo, errores y medidas correctivas tomadas, entre otras actividades.

17. La oficina asesora de las TIC, es la encargada de documentar e implementar los controles de seguridad de los datos y los servicios conectados en las redes de la Entidad.

18. La oficina asesora de las TIC, es la encargada de administrar y documentar los procedimientos con medios informáticos portátiles, discos, memorias extraíbles entre otros.

19. La oficina asesora de las TIC, es la encargada de definir los procedimientos para la clasificación, manejo y almacenamiento de la Información, restringiendo el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el funcionario encargado del procesamiento de la Información relativa al sistema.

20. La oficina asesora de las TIC, es la encargada de documentar los procedimientos relacionados con el transporte de medios informáticos a fin de proteger la información sensible contra divulgación o modificación no autorizadas.

21. La oficina asesora de las TIC, es la encargada de definir, documentar e implementar los controles relacionados con el uso adecuado del Correo Electrónico para reducir los riesgos de incidentes de seguridad.

22. La oficina asesora de las TIC, es la encargada de definir y documentar las normas y procedimientos relacionados con el uso adecuado del Correo Electrónico que debe incluir protección de archivos adjuntos de correo electrónico, uso de técnicas criptográficas para proteger la confidencialidad e integridad, de los mensajes electrónicos, retención de mensajes que se deben almacenar y como deben ser usados en caso de ser requeridos legalmente.

23. La oficina asesora de las TIC, es la encargada de definir los aspectos operativos para garantizar el correcto funcionamiento del servicio como el tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, definición de los alcances del uso del correo electrónico por parte del personal de la Entidad entre otros.

VII. ACCESO A LOS RECURSOS INFORMÁTICOS

1. La oficina asesora de las TIC, debe documentar y revisar los procedimientos para administrar y controlar el acceso a los sistemas y recursos tecnológicos de la Entidad de acuerdo a las necesidades de seguridad y de sus actividades.

2. Los funcionarios que manejen sistemas de información, deben solicitar a la oficina asesora de las TIC, las credenciales de acceso de las plataformas y velar por la seguridad de estas.

3. Cada secretaría es responsable de mantener la integridad y confidencialidad de los datos de los sistemas de información que maneja.

4. Todo usuario de los recursos informáticos debe notificar al área de sistemas o a quien corresponda, el tipo de información que requiere medidas específicas de protección para evitar el acceso al personal no autorizado.

5. Todos los funcionarios que utilicen medios de almacenamiento de información como CDs, Dvds, Memorias USB, Portátiles, Discos externos deben cumplir las siguientes recomendaciones:

- ✓ Analizar con el antivirus todos los dispositivos extraíbles que contengan información externa de la entidad.
- ✓ Extraer de forma segura los dispositivos extraíbles.
- ✓ Verificar el estado físico de los medios de almacenamiento extraíble, para evitar daños al equipo informático.

6. La oficina asesora de las TIC, debe documentar de manera formal la administración de Contraseñas de Usuario de acceso a los sistemas de información y de aquellas con las cuales se realizan actividades como instalación de plataformas, habilitación de servicios, actualización de software, configuración de componentes informáticos, entre otros; y, que deben encontrarse protegidas por contraseñas con un mayor grado de complejidad de seguridad.

7. El funcionario encargado de generar información debe proteger y controlar el acceso a los datos y servicios de información conforme al procedimiento formal establecido en la Entidad.

8. Los usuarios deben seguir y aplicar las buenas prácticas de seguridad para la selección y uso de contraseñas que la oficina asesora de las TIC, implante y documente.

9. La oficina asesora de las TIC, debe reglamentar el acceso y el personal autorizado para el ingreso a las estaciones de trabajo o servidores.

10. La oficina asesora de las TIC, debe documentar los controles de seguridad que contribuya a disminuir el riesgo de acceso no autorizado a los servicios de red.

11. La oficina asesora de las TIC, debe documentar y controlar la conexión remota y el acceso a los sistemas de información de la Entidad con el fin de minimizar el riesgo de accesos no autorizados.

12. La oficina asesora de las TIC, debe administrar, controlar y documentar los perímetros de seguridad que implemente mediante la instalación y configuración de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios y bloquear el acceso no autorizado.

13. La oficina asesora de las TIC, debe implementar controles relacionados con el ruteo de redes, las conexiones informáticas y los flujos de información. Estos controles deben verificar positivamente las direcciones de origen y destino así como los dispositivos de red tales como Hubs, Switches, Bridges, Módems o Routers que tenga la plataforma tecnológica en la Entidad.

18. La oficina asesora de las TIC, es la encargada de documentar, reglamentar y controlar la Identificación de equipos e información de los funcionarios. Se debe optar por una técnica de autenticación adecuada para verificar y validar la identidad pedida por el usuario.

19. Todos los funcionarios deben aplicar la desconexión por tiempo sin uso temporal de los computadores personales activos en las oficinas o que se active el protector de pantalla con

contraseñas y evite el acceso no autorizado, sin cerrar las sesiones de aplicación o de red si debe abandonar su puesto de trabajo momentáneamente. De igual forma, se debe definir limitaciones en el tiempo de conexión que proporcionen un nivel de seguridad adicional a las aplicaciones de alto riesgo.

20. La oficina asesora de las TIC, debe evaluar los sistemas y determinar lo que son sensibles y requieren de un ambiente informático dedicado o aislado o que sólo debe compartir recursos con los sistemas de aplicación confiables o no tener limitaciones.

21. La oficina asesora de las TIC, debe documentar reglas para el correcto manejo de dispositivos de computación móvil y trabajo remoto que incluyan la protección física necesaria, el acceso seguro y la utilización de los dispositivos en lugares públicos, el acceso a los sistemas de información y servicios a través de estos y la protección contra software malicioso.

22. Todos los funcionarios debe solicitar al área de sistemas o a quien corresponda, la autorización para el trabajo remoto con los sistemas de información de la alcaldía.

23. El comité de seguridad y privacidad de la información, debe evaluar y aprobar las medidas de protección que correspondan a la seguridad de la información, normas y procedimientos existentes.

VIII. ADQUISICION DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

1. La oficina asesora de las TIC, debe documentar los procedimientos para adquirir nuevos desarrollos de software, mejoras o actualizaciones e incluir los mecanismos de control.

2. Las políticas de seguridad informática aplica a todos los sistemas informáticos y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes donde aplique.

3. La oficina asesora de las TIC, junto con el funcionario generador de información deben determinar la criticidad de los equipos informáticos y de la información para definir los requerimientos de protección como métodos criptográficos a ser utilizados.

4. La oficina asesora de las TIC debe incluir controles en los procesos que permita evaluar el avance del sistema, así como detectar las posibles fallas potenciales de diseño y estructural que deben ser corregidos a tiempo antes de que sea implementado.

5. Todo envío de mensajes o correos electrónicos debe ser evaluado con respecto a la información contenida, determinar su clasificación y considerar la implementación de controles de seguridad.

6. La oficina asesora de las TIC, debe evaluar y documentar en que situaciones hay que utilizar sistemas y técnicas criptográficas para proteger la información previo análisis de riesgo efectuado que asegure una adecuada protección de su confidencialidad e integridad.

7. La oficina asesora de las TIC, debe documentar procedimientos relacionados con Servicios de No Repudio con el fin de proporcionar herramientas que evite que se niegue haberla efectuado y resolver alguna discrepancia acerca de la ocurrencia de un evento o acción.

9. La oficina asesora de las TIC, debe proporcionar asesorías al personal de la entidad, en temas de protección adecuada a los sistemas que utilizan para generar, almacenar y archivar claves, minimizar el alto riesgo y que puedan ser protegidas contra modificación, destrucción o copia o divulgación no autorizada.

10. La oficina asesora de las TIC, debe garantizar que los desarrollos y actividades de soporte a los sistemas adquiridos o actualizados se lleven a cabo de manera segura con los controles necesarios para permitir el acceso a los archivos solo al personal autorizado.

15. La oficina asesora de las TIC, debe documentar el procedimiento de Control de Cambios de Datos Operativos con el fin de que cualquier modificación, actualización o eliminación solo se realice a través de los sistemas que los procesan.

16. Todo cambio que requiera efectuarse en el Sistema Operativo debe ser evaluado en La oficina asesora de las TIC, con el fin de analizar el impacto que pueda incidir en el funcionamiento o seguridad de los nuevos sistemas adquiridos o desarrollados bajo este esquema.

17. Se debe reglamentar la adquisición de Software e incluir los controles necesarios para verificar licencias y los requerimientos de seguridad del software establecidos.

IX. INCIDENTES DE SEGURIDAD DE LA INFORMACION

1. Todo el personal de la alcaldía de Los Patios debe mantener informada a la oficina asesora de las TIC, acerca de la ocurrencia de incidentes de seguridad.
2. La oficina asesora de las TIC, debe implementar herramientas y mecanismos necesarios para fomentar una buena comunicación entre las dependencias para conocer las posibles debilidades en materia de seguridad, así como de los incidentes ocurridos, con el fin de minimizar sus efectos y prevenir su reincidencia.
3. La oficina asesora de las TIC debe registrar la información de incidentes de seguridad, evaluar e identificar aquellos que son recurrentes o de alto impacto; así como establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.
4. La oficina asesora de las TIC, debe establecer la periodicidad de las revisiones o auditorias de acuerdo a la evaluación de riesgos que efectúe en conjunto con los funcionarios generadores de la Información.

X. CUMPLIMIENTO DE NORMAS Y POLITICAS DE SEGURIDAD DE LA INFORMACIÓN.

1. La divulgación del Manual de Normas y Políticas de seguridad debe ser transmitido e implementado a través de las diferentes secretarías que conforman la alcaldía

2. Todos los funcionarios de la Alcaldía del Municipio de Los Patios deben estar autorizados por secretaría General y La oficina asesora de las TIC, para el uso de los recursos informáticos, se debe vigilar el uso adecuado de la información y de toda la plataforma tecnológica.

3. La oficina asesora de las TIC, debe brindar capacitación a toda a la Entidad sobre los riesgos y amenazas que puede tener la información el cual se considera un activo valioso para la entidad y la conveniencia de aplicar las políticas de seguridad Informática para evitar vulnerabilidades que impacten a la entidad.

4. La oficina asesora de las TIC, es la encargada de socializar en todas las dependencias los lineamientos aprobados por el Comité de Gobierno en Línea, Seguridad y Privacidad de la Información y Anti trámites sobre los procedimientos de gestión de riesgos, implementación de políticas, mecanismos de control para mejoras en materia de seguridad de la información en la entidad.

5. Todas las dependencias deben adoptar y cumplir las normas y lineamientos que emita el Comité de Gobierno en Línea, Seguridad y Privacidad de la Información y Anti trámites para la administración de las copias de seguridad.

EXCEPCIONES

Toda solicitud de excepción de alguna política de seguridad informática debe ser solicitada a secretaría general y al área de sistemas o a quien corresponda, con la debida justificación y documentación conforme la naturaleza de su cargo o dado por eventos no contemplados en este Manual de Normas y Políticas; previa evaluación del alcance y el impacto. La evaluación de la excepción puede requerir el apoyo de la Oficina Jurídica y/o Secretaría General.