POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ALCALDÍA DE SESQUILÉ

Enero 29 DE 2020

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 Sesquilé

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 [ISOIlEC 13335- 1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la afirmación general que representa la posición de la alcaldía municipal de Sesquilé, 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 Sesquilé, 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 Sesquilé 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.

La Seguridad de la Información en la Entidad se establece con el objetivo de

- 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

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la alcaldía municipal de Sesquilé, así como a la ciudadanía.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

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

POLÍTICAS, CONTROLES, RECOMENDACIONES Y OPERACIONES BÁSICAS 1.

COMPUTADORES, PORTÁTILES, SERVIDORES

1.1. 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 Sesquilé sólo a personas autorizadas para la salvaguardar los equipos de cómputo y de comunicaciones.

1.2. 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 o 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.
- A 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 Sesquilé podrán desplazarse con previa autorización del responsable de la dependencia y bajo la responsabilidad total del usuario.

2. USO DE INTERNET

2.1. Políticas

La alcaldía municipal de Sesquilé 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.

2.2. 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.

3. MANEJO DE REDES SOCIALES

3.1. Políticas

La alcaldía municipal de Sesquilé 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.

3.2. 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 Sesquilé, que sea creado a nombre personal, como redes sociales, twitter®, facebook®, youtube® likedink® WhatsApp 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.

- El personal encargado del manejo de Social Media de la alcaldía de Sesquilé deberá dar oportuno uso a las mismas, informando de manera clara y objetiva a la entidad y a la comunidad sobre todas las interacciones registradas en cada medio dispuesto oficial de la Administración Municipal.

4. MANEJO DE IMPRESORAS

4.1 Políticas

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

4.2 Controles

- Los documentos que se impriman en las impresoras de la alcaldía municipal de Sesquilé 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 Sesquilé.

.

5. MANEJO APROPIADO DE CONTROL DE VIRUS

5.1. Políticas

La alcaldía municipal de Sesquilé 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.

5.2. 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.

6. SWITCHES Y ROUTERS

6.1. 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.

6.2. 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 acceder 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

7. CORREO ELECTRÓNICO INSTITUCIONAL

7.1. 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 Sesquilé 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.

7.2. Controles

- ➢ Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la Alcaldía Municipal de Sesquilé. 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, http://www.sesquile-cundinamarca.gov.co , gobierno Digital etc. Se pueden consultar en cualquier momento dentro del horario laboral.
- De ninguna manera se podrá acceder a páginas de entretenimiento, pornografía dentro o fuera del contexto laboral.
- El usuario no deberá bajar (o copiar) archivos sospechosos 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.

- El uso de Internet está limitado por las políticas de seguridad del área de sistemas.

8. BASES DE DATOS

8.1. 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.

8.2. 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 alertará 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. RED LAN

9.1. 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 Sesquilé 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.

9.2. 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 Sesquilé.

- ✓ 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.

10. 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 Sesquilé.

11. OPERACIONES BÁSICAS DE PC

11.1 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.

11.2 Cuando encender y apagar el Sistema:

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

12. CONTRASEÑAS Y EL CONTROL DE ACCESO

12.1 Política

Controlar el acceso a la información.

12.2 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.

12.3. 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.

13. CUMPLIMIENTO SEGURIDAD INFORMÁTICA

13.1. Política

El Área de sistemas de la Alcaldía Municipal de Sesquilé 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.

13.2. 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 Sesquilé.

- ✓ 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 Sesquilé 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 Sesquilé.

- ✓ 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.

14. 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 Sesquilé: 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:

14.1 en caso de falla de un activo se debe:

1. 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.

2. 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.

3. 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.

14.2. Para el caso de realizar mantenimiento el preventivo anual:

1. 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.

2. se deben utilizar los formatos pre establecidos para estos procedimientos.

3. 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.

15. 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.

16. 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.

17. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL SITIO WEB Y PROTECCIÓN DE DATOS PERSONALES.

ACUERDO ENTRE EL USUARIO Y LA ALCALDÍA MUNICIPAL DE SESQUILÉ

El Sitio Web de la Alcaldía Municipal de Sesquilé está compuesto de varias páginas Web operadas por Alcaldía Municipal de Sesquilé.

El sitio Web Alcaldía Municipal de Sesquilé se le ofrece a Usted condicionado a la aceptación sin excepciones de los términos, condiciones y avisos aquí contenidos. El uso por su parte del sitio Web Alcaldía Municipal de Sesquilé constituye en sí mismo su aceptación a todos sus términos, condiciones y avisos.

MODIFICACIONES A ESTOS TÉRMINOS DE USO

La Alcaldía Municipal de Sesquilé se reserva el derecho a modificar los términos, condiciones y avisos bajo los cuales se ofrece el sitio Web de la Alcaldía Municipal de Sesquilé, incluyendo, pero no limitado a, los cargos asociados por el uso del sitio Web Alcaldía Municipal de Sesquilé

VÍNCULOS A SITIOS DE TERCERAS PARTES

El sitio Web Alcaldía Municipal de Sesquilé puede contener vínculos a otros sitios Web Site ("Sitios Vinculados"). Los Sitios Vinculados no están bajo el control de Alcaldía Municipal de Sesquilé y por tanto Alcaldía Municipal de Sesquilé no es responsable de los contenidos de ningún Sitio Vinculado, incluyendo sin limitaciones, todo vínculo contenido en un Sitio Vinculado, o todo cambio o actualización de un Sitio Vinculado. Alcaldía Municipal de Sesquilé no es responsable de difusiones vía Web ni mediante cualquier otra forma de transmisión recibida desde cualquier Sitio Vinculado. La Alcaldía Municipal de Sesquilé provee estos vínculos solamente para su conveniencia, y la inclusión de estos vínculos no implica aprobación por parte de Alcaldía Municipal de Sesquilé del sitio, ni asociación con sus operadores.

NO USO ILEGAL O PROHIBIDO

Como una condición al uso por su parte del sitio Web Alcaldía Municipal de Sesquilé, Usted garantiza a Alcaldía Municipal de Sesquilé que no usará el sitio Web Alcaldía Municipal de Sesquilé para propósitos ilegales o prohibidos por estos términos, condiciones y avisos. Usted no puede usar el sitio Web Alcaldía Municipal de Sesquilé de tal forma que pudiera dañar, deshabilitar, sobrecargar o deteriorar el sitio Web Alcaldía Municipal de Sesquilé o interferir con el uso y provecho del sitio Web Alcaldía Municipal de Sesquilé por terceras partes. Usted no puede obtener ni intentar obtener material o información utilizando otros medios que aquellos expresa e intencionalmente ofrecidos a tal efecto en el sitio Web Alcaldía Municipal de Sesquilé.

USO DE SERVICIOS DE COMUNICACIÓN

El sitio Web Alcaldía Municipal de Sesquilé puede contener servicios de BBS, áreas de Chat, grupos de usuarios, foros de discusión, comunidades, páginas Web personales, calendarios y/o otras facilidades de mensajería o comunicación, diseñadas para permitirle a Usted comunicarse con el público en general o con un grupo de personas (en adelante, "Servicios de Comunicación"). Usted acepta usar los Servicios de Comunicación sólo para anunciar, enviar o recibir mensajes y material que sea apropiado y relativo al Servicio de Comunicación en particular. A modo de ejemplo, y no limitado a, Usted acepta que cuando utilice un Servicio de Comunicación, no podrá:

- Difamar, abusar, acosar, acechar, amenazar o de alguna forma violar los derechos legales (como los derechos de privacidad y publicidad) de otros.
- Publicar, anunciar, subir, distribuir o diseminar ningún tópico, nombre, material o información, que sea inapropiada, indecente, transgresora, difamatoria, obscena o ilegal.
- Subir archivos que contengan software u otro material protegido por leyes de propiedad intelectual (o derechos de privacidad o publicidad) a menos que Usted sea el propietario o controle los derechos respectivos, o haya recibido el necesario consentimiento expreso.
- Subir archivos que contengan virus, archivos corruptos, o cualquier otro software o programas que puedan dañar la operación del computador de otro.
- Publicar u ofrecer a la venta o a la compra cualquier bien o servicio con propósitos comerciales, excepto en el caso que dicho Servicio de Comunicación permita específicamente ese tipo de mensajes.
- Dirigir o reenviar encuestas, certámenes, cadenas de cartas o esquemas piramidales.
- Bajar archivos subidos por otro usuario de un Servicio de Comunicación cuando Usted tuviera o razonablemente debiera tener conocimiento de que no deban distribuirse legalmente de esa forma.
- Falsificar o eliminar cualquier referencia al autor, referencia legal o avisos o designaciones propietarias o rótulos del origen o fuente del software u otro material contenidos en un archivo que se sube.
- Restringir o inhibir que otros usuarios puedan usar y disfrutar de los Servicios de Comunicación.
- Violar cualesquiera códigos de conducta u otras guías que puedan aplicarse a un Servicio de Comunicación en particular.
- Recoger o cualquier forma de recolectar información acerca de otros, incluyendo direcciones de correo electrónico sin su consentimiento.
- Violar leyes o regulaciones aplicables.

La Alcaldía Municipal de Sesquilé no tiene obligación de monitorear los Servicios de Comunicación. No obstante, Alcaldía Municipal de Sesquilé se reserva el derecho de revisar los materiales anunciados en los Servicios de Comunicación y quitarlos a discreción. Alcaldía Municipal de Sesquilé se reserva el derecho de quitarle a Usted el acceso a cualquiera o todos los Servicios de Comunicación, en cualquier momento sin previo aviso y por la razón que sea.

Alcaldía Municipal de Sesquilé se reserva el derecho en cualquier momento a revelar información cuando sea necesario cumplir con cualesquiera leyes aplicables, regulaciones, procesos legales, pedidos del gobierno, o editar, denegar la publicación, o eliminar cualquier información o material, en su totalidad o en parte, a la sola discreción de Alcaldía Municipal de Sesquilé.

Sea siempre cuidadoso al dar cualquier información personal que lo identifique a Usted o a sus hijos en todo Servicio de Comunicación. La Alcaldía Municipal de Sesquilé no controla ni aprueba el contenido, mensajes, o información encontrada en los Servicios de Comunicación y, por tanto, la Alcaldía Municipal de Sesquilé niega específicamente cualquier responsabilidad en relación con los Servicios de Comunicación y con cualesquiera acciones resultantes de su participación en cualquier Servicio de Comunicación. Los administradores y anfitriones no son voceros autorizados de la Alcaldía Municipal de Sesquilé, y sus puntos de vista no necesariamente reflejan aquellos de la Alcaldía Municipal de Sesquilé.

Los materiales subidos a un Servicio de Comunicación pueden estar sujetos a limitaciones en el uso, reproducción o difusión dispuestas por la persona que los haya subido. Usted es responsable de cumplir con dichas limitaciones si baja esos materiales.

MATERIALES SUMINISTRADOS A La Alcaldía Municipal de Sesquilé O PUBLICADOS EN CUALQUIER SITIO WEB DE la Alcaldía Municipal de Sesquilé

La Alcaldía Municipal de Sesquilé no reclama la propiedad de los materiales que Usted suministre a la Alcaldía Municipal de Sesquilé (incluyendo comentarios y sugerencias) o anuncie, publique, suba, ingrese, envíe o entregue a cualquier sitio Web de la Alcaldía Municipal de Sesquilé o sus servicios asociados (en adelante "Entregas"). Sin embargo, al anunciar, publicar, subir, escribir, suministrar o entregar sus Entregas, Usted está otorgando permiso a la Alcaldía Municipal de Sesquilé, a sus compañías afiliadas y licenciatarios necesarios, para usar dichas Entregas en relación con la operación de sus respectivos negocios en Internet, incluyendo, sin limitaciones, los derechos a copiar, distribuir, transmitir, mostrar públicamente, representar públicamente, reproducir, editar, traducir y dar nuevo formato a su Entrega; y a publicitar su nombre en conexión con su Entrega.

No se pagará ninguna compensación respecto al uso de su Entrega, tal como se describe aquí. Alcaldía Municipal de Sesquilé no tiene ninguna obligación de anunciar, publicar o usar ninguna de las Entregas que Usted pueda suministrar, y puede eliminar o quitar cualquier Entrega que Usted haya suministrado, en cualquier momento y a la sola discreción de la Alcaldía Municipal de Sesquilé.

Por el solo hecho de anunciar, subir, escribir, suministrar o entregar sus Entregas, Usted garantiza y representa que Usted es el propietario o de alguna manera controla todos los derechos de su Entrega, como se describe en esta sección; incluyendo, sin limitaciones, todos los derechos necesarios para que Usted suministre, anuncie, suba, ingrese, entregue o envíe las Entregas.

RENUNCIA DE OBLIGACIÓN

LA INFORMACIÓN, SOFTWARE, PRODUCTOS Y SERVICIOS INCLUIDOS EN, O DISPONIBLES A TRAVÉS DEL SITIO WEB de la Alcaldía Municipal de Sesquilé PUEDEN

CONTENER INEXACTITUDES O ERRORES TIPOGRÁFICOS. PERIÓDICAMENTE SE REALIZAN MODIFICACIONES Y AGREGADOS A LA INFORMACIÓN AQUÍ CONTENIDA. La Alcaldía Municipal de Sesquilé Y/O SUS PROVEEDORES PUEDEN REALIZAR EN CUALQUIER MOMENTO MODIFICACIONES O MEJORAS AL SITIO WEB DE La Alcaldía Municipal de Sesquilé. LOS CONSEJOS QUE PUEDAN RECIBIRSE A TRAVÉS DEL SITIO WEB la Alcaldía Municipal de Sesquilé NO DEBERIAN TENERSE EN CUENTA PARA LA TOMA DE DECISIONES PERSONALES, MÉDICAS, LEGALES O FINANCIERAS Y USTED DEBERÍA CONSULTAR A UN PROFESIONAL PARA EL ASESORAMIENTO ESPECÍFICO Y A LA MEDIDA DE SU SITUACIÓN.

La Alcaldía Municipal de Sesquilé Y/O SUS PROVEEDORES, NO SON REPRESENTACIÓN DE LA CONVENIENCIA, CONFIABILIDAD, DISPONIBILIDAD, ACTUALIDAD, NI LA EXACTITUD DE LA INFORMACIÓN, SOFTWARE, PRODUCTOS, SERVICIOS Y GRÁFICOS RELACIONADOS; CONTENIDOS EN EL SITIO WEB DE Alcaldía Municipal de Sesquilé, SEA CUAL FUERE SU PROPÓSITO. DE ACUERDO AL MÁXIMO ALCANCE PERMITIDO POR LAS LEYES APLICABLES, DICHA INFORMACIÓN, SOFTWARE, PRODUCTOS, SERVICIOS Y GRÁFICOS RELACIONADOS, SE ENTRGAN “COMO SON”, SIN NINGÚN TIPO DE GARANTÍA O CONDICIÓN. Alcaldía Municipal de Sesquilé Y/O SUS PROVEEDORES RECHAZAN POR ESTE MEDIO TODAS LAS GARANTÍAS Y CONDICIONES EN RELACIÓN CON ESTA INFORMACIÓN, SOFTWARE, PRODUSCTOS, SERVICIOS Y GRÁFICOS RELACIONADOS, INCLUYENDO TODAS LAS GARANTÍAS O CONDICIONES IMPLÍCITAS EN LA COMERCIALIZACIÓN, ADECUACIÓN A UN PROPÓSITO ESPECÍFICO, TITULACIÓN Y/O INFRACCIÓN.

DE ACUERDO AL MÁXIMO ALCANCE PERMITIDO POR LAS LEYES APLICABLES, EN NINGÚN CASO la Alcaldía Municipal de Sesquilé Y/O SUS PROVEEDORES SERÁN RESPONSABLES POR NINGÚN DAÑO DIRECTO, INDIRECTO, PUNITIVO, INCIDENTAL, ESPECIAL, CONSECUENTE, O CUALESQUIERA DAÑOS INCLUYENDO, SIN LIMITACIONES, DAÑOS POR PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS SURGIDOS DEL USO, O DE ALGUNA MANERA RELACIONADOS CON EL USO O RENDIMINETO DEL SITIO WEB DE la Alcaldía Municipal de Sesquilé, CON LA DEMORA O LA IMPOSIBILIDAD DE USO DEL SITIO WEB la Alcaldía Municipal de Sesquilé O SUS SERVICIOS RELACIONADOS, LA PROVISIÓN O FALLA EN LA PROVISIÓN DE SERVICIOS, O POR CUALQUIER INFORMACIÓN, SOFTWARE, PRODUCTOS, SERVICIOS Y GRÁFICOS RELACIONADOS OBTENIDOS A TRAVÉS DEL SITIO WEB DE la Alcaldía Municipal de Sesquilé, O DE ALGUNA OTRA MANERA SURGIDOS A PARTIR DEL USO DEL SITIO WEB DE Alcaldía Municipal de Sesquilé, YA SEA QUE SE BASEN EN UN CONTRATO, AGRAVIO, NEGLIGENCIA, ESTRICTA RESPONSABILIDAD, O CUALQUIER OTRA FORMA, AUN CUANDO la Alcaldía Municipal de Sesquilé O CUALQUIERA DE SUS PROVEEDORES HAYAN SIDO AVISADOS ACERCA DE LA POSIBILIDAD DE DAÑOS. COMO EN ALGUNAS JURISDICCIONES NO SE PERMITE LA EXCLUSIÓN O LIMITACIÓN DE RESPONSABILIDAD POR DAÑOS INCIDENTALES O CONSECUENTES, LA

LIMITACIÓN ARRIBA DETALLADA PUEDE QUE NO SE APLQUE A USTED. SI NO SE ENCUENTRA SATISFECHO CON ALGUNA PARTE DEL SITIO WEB DE Alcaldía Municipal de Sesquilé, O CON ALGUNO DE ESTOS TÉRMINOS DE USO, SU ÚNICO Y EXCLUSIVO REMEDIO ES DEJAR DE USAR EL SITIO WEB DE la Alcaldía Municipal de Sesquilé.

CONTACTO DEL SERVICIO: tec.iformatica@sesquile-cundinamarca.gov.co

FINALIZACIÓN/RESTRICCIÓN DE ACCESO

LA Alcaldía Municipal de Sesquilé se reserva el derecho, a su sola discreción, a finalizar su acceso al sitio Web de la Alcaldía Municipal de Sesquilé, así como a sus servicios relacionados o a cualquier parte de éstos, en cualquier momento y sin previa notificación. GENERAL:

De acuerdo al alcance máximo permitido por la ley, este acuerdo está gobernado por las leyes de comercio vigentes en España y por consiguiente Usted consiente como jurisdicción exclusiva Almería en todas las disputas que surjan del uso o relativas al uso del sitio Web de Alcaldía Municipal de Sesquilé. El uso del sitio Web de la Alcaldía Municipal de Sesquilé no está autorizado en jurisdicción alguna que no haga efectivas todas las provisiones de estos términos y condiciones, incluyendo, sin limitaciones, las contenidas en este párrafo. Usted asiente que como resultado de este acuerdo o por el uso del sitio Web de la Alcaldía Municipal de Sesquilé , no existe asociación, joint venture, relación de dependencia o empleo, o relación de agencia alguna, entre Usted y la Alcaldía Municipal de Sesquilé. El cumplimiento de este acuerdo por parte de Alcaldía Municipal de Sesquilé está sujeto a las leyes vigentes y al proceso legal, y nada contenido en este acuerdo constituye una derogación al derecho de Alcaldía Municipal de Sesquilé a obrar de acuerdo a los requisitos, solicitudes o imposiciones legales, del gobierno o de la corte, relacionados con el uso por Usted del sitio Web de Alcaldía Municipal de Sesquilé, o a información recogida o suministrada a Alcaldía Municipal de Sesquilé respecto de dicho uso. En caso que se determinara legalmente que alguna parte de este acuerdo fuera inválida o no exigible de acuerdo a la ley, incluyendo sin limitaciones, el rechazo de garantías y las limitaciones a la responsabilidad establecidas más arriba, entonces la provisión inválida o no exigible se considerará sustituida por una provisión válida y exigible, que se acerque lo más posible a la intención de la provisión original, y el resto del acuerdo continuará en efecto. Salvo lo especificado aquí, este acuerdo constituye el acuerdo completo entre el usuario y Alcaldía Municipal de Sesquilé respecto del sitio Web de Alcaldía Municipal de Sesquilé y reemplaza a todas las comunicaciones y propuestas anteriores o contemporáneas, hayan sido éstas electrónicas, orales o escritas, entre el usuario y Alcaldía Municipal de Sesquilé respecto del sitio Web de Alcaldía Municipal de Sesquilé. Una versión impresa de este acuerdo y de cualquier notificación enviada en forma electrónica, serán admitidas en procedimientos judiciales o administrativos basados en este acuerdo o relacionados con él, y tendrán el mismo alcance y estarán sujetas a las mismas condiciones que otros documentos y registros comerciales generados y mantenidos originalmente en forma impresa. Es el deseo expreso de las partes que este acuerdo y los documentos relacionados sean escritos en español.

DERECHO DE PROPIEDAD Y MARCAS COMERCIALES:

Todos los contenidos del sitio Web de la Alcaldía Municipal de Sesquilé son: y /o sus proveedores. Todos los derechos reservados.

MARCAS COMERCIALES

Los nombres de compañías y productos reales mencionados aquí pueden ser marcas comerciales de sus respectivos propietarios.

Los nombres usados en ejemplos de compañías, organizaciones, productos, personas y eventos descritos aquí son ficticios. No debe asociarse o inferirse relación alguna con ninguna compañía, organización, producto, persona o evento reales.

Cualesquiera derechos no expresamente otorgados aquí son reservados.

Declaración de Privacidad

La Alcaldía Municipal de Sesquilé está comprometida a proteger su privacidad y la tecnología de desarrollo que le brinda la experiencia en línea más potente y segura. Esta Declaración de Privacidad está relacionada con el sitio Web de la Alcaldía Municipal de Sesquilé y abarca la recolección de datos y su uso. Al utilizar el sitio de la Alcaldía Municipal de Sesquilé, Usted acepta las prácticas utilizadas en relación a los datos que se describen en esta declaración.

Recolección de su Información Personal

La Alcaldía Municipal de Sesquilé recolecta información de identificación personal, como su dirección de correo electrónico (e-mail), nombre, dirección del trabajo o de su casa, o su número telefónico. La Alcaldía Municipal de Sesquilé también recaba información demográfica anónima, en el sentido que no es aplicable sólo a Usted, como por ejemplo el código postal, edad, sexo, preferencias, intereses y favoritos.

También existe información acerca del hardware y software de su computador personal, que se recaba automáticamente por la Alcaldía Municipal de Sesquilé. Esta información puede incluir: su dirección IP, tipo de explorador de Internet usado, nombres de dominio, tiempos de acceso y direcciones de sitios Web que hacen referencia a éste. Esta información es utilizada por la Alcaldía Municipal de Sesquilé para la operación del servicio, para mantener la calidad del servicio prestado y para brindar estadísticas generales acerca del uso del sitio la Alcaldía Municipal de Sesquilé.

Por favor tenga en cuenta que si Usted divulga directamente información de identificación personal o datos privados a través de las herramientas públicas de comunicación en línea ofrecidas por la Alcaldía

Municipal de Sesquilé, dicha información puede ser recogida y usada por otros. Nota: La Alcaldía Municipal de Sesquilé no lee ninguna de sus comunicaciones en línea privadas.

La Alcaldía Municipal de Sesquilé lo alienta a que revise las declaraciones de privacidad de otros sitios Web a los que Usted elija vincular desde la Alcaldía Municipal de Sesquilé de manera que pueda comprender cómo recogen éstos su información y si eventualmente la comparten con otros. La Alcaldía Municipal de Sesquilé no es responsable por declaraciones de privacidad ni otros contenidos que se encuentren en sitios Web fuera de la Alcaldía Municipal de Sesquilé y de la familia de sitios Web de la Alcaldía Municipal de Sesquilé.

Utilización de su Información Personal

La Alcaldía Municipal de Sesquilé obtiene y utiliza su información personal para operar el sitio Web de la Alcaldía Municipal de Sesquilé y brindarle los servicios que Usted haya solicitado. La Alcaldía Municipal de Sesquilé también utiliza la información de su identificación personal para informarlo acerca de otros productos o servicios disponibles en la Alcaldía Municipal de Sesquilé y sus subsidiarias. La Alcaldía Municipal de Sesquilé puede también ponerse en contacto con Usted mediante encuestas, para conocer su opinión sobre los servicios prestados actualmente o potenciales servicios a ofrecer en el futuro.

La Alcaldía Municipal de Sesquilé no vende, alquila o arrienda su lista de clientes a terceras partes. Esporádicamente la Alcaldía Municipal de Sesquilé puede contactarlo de parte de socios de negocios externos para ofrecerle alguna oferta particular que pueda ser de su interés. En estos casos, la información de su identificación personal (e-mail, nombre, dirección, teléfono) no es transferida al socio de negocios. Además, la Alcaldía Municipal de Sesquilé sí puede compartir datos con socios confiables que ayudan y/o en los que delega el análisis estadístico, el envío de correo electrónico o postal, la atención al cliente, o los arreglos para la distribución y entrega. Todas estas terceras partes tienen expresamente prohibido el uso de la información personal que pueda identificarlo salvo para poder proveer estos servicios a la Alcaldía Municipal de Sesquilé, y están obligados a mantener la confidencialidad de su información.

La Alcaldía Municipal de Sesquilé no utiliza ni divulga información personal privada como raza, religión o afiliaciones políticas sin su consentimiento expreso.

La Alcaldía Municipal de Sesquilé rastrea los sitios Web y las páginas que visitan nuestros clientes dentro de la Alcaldía Municipal de Sesquilé, para poder determinar cuáles son los servicios de Alcaldía Municipal de Sesquilé más populares. Estos datos son utilizados para presentar contenidos y publicidades personalizadas en el sitio de la Alcaldía Municipal de Sesquilé a clientes cuyo comportamiento indica que tienen un particular interés en un área determinada.

Los sitios Web de la Alcaldía Municipal de Sesquilé divulgarán su información personal, sin notificarlo,

sólo cuando así sea requerido por la ley o cuando se crea de buena fe que dicha acción es necesaria para: (a) conformar edictos legales o el cumplimiento de un proceso legal realizado sobre Alcaldía Municipal de Sesquilé o el sitio; (b) proteger y defender los derechos o propiedad de la Alcaldía Municipal de Sesquilé; y, (c) actuar bajo circunstancias extremas, para proteger la seguridad de los usuarios de la Alcaldía Municipal de Sesquilé, o del público.

Uso de "Cookies"

El sitio Web de la Alcaldía Municipal de Sesquilé utiliza "cookies" para almacenar sus preferencias ayudándolo a personalizar su experiencia en línea. Una cookie es un archivo de texto que es grabado en su disco duro por un servidor de páginas Web. Las cookies no pueden ser utilizadas para ejecutar programas o distribuir virus informáticos a su computadora. Las cookies son asignadas a Usted por el servidor en relación uno-a-uno, y pueden ser leídas únicamente por un servidor miembro del dominio que emitió la cookie para Usted.

Una de las principales ventajas de las cookies es que le ahorran tiempo. El propósito de una cookie es informarle al servidor Web que Usted ha regresado a una página específica. Por ejemplo, cuando Usted personaliza páginas en la Alcaldía Municipal de Sesquilé, o cuando se registra en el sitio Alcaldía Municipal de Sesquilé, la cookie grabada permite al servidor Web de la Alcaldía Municipal de Sesquilé recuperar su información específica en las subsiguientes visitas. Esto simplifica el proceso de registrar su información personal como dirección de cobro, dirección de envío, etc. La próxima vez que regrese al mimo sitio Web de la Alcaldía Municipal de Sesquilé, la información que Usted suministró anteriormente puede ser recuperada de la cookie, y así las opciones que Usted haya personalizado en su visita anterior a la Alcaldía Municipal de Sesquilé estarán disponibles sin necesidad de que deba escribirlas nuevamente.

Usted tiene la posibilidad de aceptar o rechazar cookies. La mayoría de los exploradores de Internet aceptan las cookies automáticamente, pero si lo prefiere Usted puede modificar la configuración para que las rechace. Si escoge que el explorador rechace cookies, es probable que no pueda aprovechar en su totalidad las características interactivas de los servicios ofrecidos en la Alcaldía Municipal de Sesquilé o en los sitios Web que visite.

Seguridad de su Información Personal

La Alcaldía Municipal de Sesquilé asegura su información personal frente al acceso, uso o divulgación no autorizados. La Alcaldía Municipal de Sesquilé mantiene la información de identificación personal que Usted haya provisto, en servidores ubicados en un ambiente controlado y seguro, protegidos del acceso, uso o divulgación no autorizados. En caso de que información personal (como el número de su tarjeta de crédito) sea transmitida a otros sitios Web, ésta se protege mediante el uso de protocolos cifrados como el protocolo SSL (Secure Sockets Layer).

Modificaciones a esta Declaración

La Alcaldía Municipal de Sesquilé podrá ocasionalmente actualizar esta Declaración de Privacidad para reflejar las sugerencias tanto de la compañía como de los clientes. En la Alcaldía Municipal de Sesquilé lo alentamos a que revise periódicamente esta Declaración para estar informado de cómo la Alcaldía Municipal de Sesquilé protege su información.

Información de Contacto

La Alcaldía Municipal de Sesquilé recibe con agrado sus comentarios relativos a esta Declaración de Privacidad. Si Usted cree que la Alcaldía Municipal de Sesquilé no se ha ceñido a esta Declaración, por favor, póngase en contacto con la Alcaldía Municipal de Sesquilé a través de tec.informatica@sesquile-cundinamarca.gov.co. Pondremos nuestros mejores esfuerzos comercialmente razonables para determinar rápidamente el problema y remediarlo cuanto antes.

POLÍTICAS GENERALES

- Los responsables de cada área deberán apoyar al cumplimiento de los lineamientos antes mencionados.
- Todo usuario tendrá que cumplir con los lineamientos antes mencionados 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.

REFERENCIAS

- Ley 1450 de 2011, por el cual se expide el Plan Nacional de Desarrollo 2010-2014, en el artículo N° 55 sobre accesibilidad a servicios de TIC.
- Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones en el artículo 38 sobre Masificación del uso de las TIC y cierre de la brecha digital**.**
- Decreto 2693 de 2012, por el cual se establecen los lineamientos generales de la estrategia de Gobierno Digital de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
- Capítulo IV referente a la Gestión de Documentos Electrónicos de Archivo del Decreto 2609 de 2012, por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, por la cual se

dictan disposiciones generales para la protección de datos personales.

En constancia se firma a los veintinueve (29) días del mes de enero de dos mil veinte (2020).

ORIGINAL FIRMADO

JAIME ADRIÁN RODRÍGUEZ BERNAL
SECRETARIO DE HACIENDA

Fecha de elaboración: 29/01/2020
Dependencia de origen: Secretaría De Hacienda
Quien elaboró: Jose Adonias Parra Marín
Quien revisó: Jaime Adrián Rodríguez Bernal