NIT: 822.001.883-3

EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE SAN JOSE DEL GUAVIARE

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES PETI

SUBGERENCIA ADMIISTRATIVA Y FINANCIERA

SAN JOSE DEL GUAVIARE, 2023

INTRODUCCIÓN

Con la definición de las políticas y estándares de seguridad informática se busca establecer en el interior de la Institución una cultura de calidad operando en una forma confiable.

La seguridad informática, es un proceso donde se deben evaluar y Administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de EMPOAGUAS E.S.P. en materia de seguridad.

Para el desarrollo de este plan se busca estructurarlo en base a ciertos criterios tales como:

- Seguridad institucional
- Seguridad física y del medio ambiente
- Manejo y control centro de cómputo
- Control de usuarios
- Lineamientos legales
- Dominio (EMPOAGUAS .esp)

1. OBJETIVO

Fortalecer la gestión y generación de información y servicios TI en donde responda a las necesidades de información, sistema de información, infraestructura tecnológica, seguridad de la información y al modelo operativo y de procesos propios de EMPOAGUAS E.S.P, para el cumplimiento de sus objetivos misionales.

1.1 OBJETIVOS ESPECIFICOS

- Generar integración y operatividad de los sistemas y servicios de la entidad.
- Ampliar la disponibilidad de los sistemas y servicios en TI.

- Aportar a la transparencia y buen gobierno favoreciendo los medios tecnológicos para llegar los ciudadanos. Y los sistemas de información, de acceso, uso, divulgación.

2. MARCO NORMATIVO

El marco normativo que aplica para la gestión de TI en el estado colombiano es bastante amplio, comprende una serie de leyes, decretos y otras instancias como documentos; a continuación, se señalan algunos de los más relevantes, los cuales representan un avance significativo en cuanto a la evolución de la gestión de TI en el estado colombiano.

- Decreto 415 de 2016: "por el cual se adiciona el decreto único reglamentario del sector de la función pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones"
- Decreto 1078 de 2015 específicamente en su título 9 políticas y lineamientos de tecnologías de la información, capítulo 1. Estrategia de gobierno en línea, cuyo objeto es "definir los lineamientos, instrumentos y plazos de la estrategia de gobierno en línea para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un estado abierto, más participativo y que preste mejores servicios con la colaboración de toda la sociedad".
- Ley 1712 de 2014: "por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".
- El decreto 1081 de 2015, "por el cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones".
- Resolución 3564 de 2015 del ministerio de tecnologías de la información y las comunicaciones, "por la cual se reglamentan aspectos relacionados con la ley de transparencia y acceso a la información pública"

3. DESARROLLO GENERAL

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC´s de todo el personal comprometido en el uso de los servicios informáticos proporcionados por el área de sistemas.

También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal de EMPOAGUAS E.S.P. Facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada por el área de sistemas al personal, al manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información.

3.1 Evaluación de las políticas

Las políticas tendrán una revisión periódica se recomienda que sea semestral para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias.

3.2 Beneficios

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC´s) en la empresa.

4. SEGURIDAD INSTITUCIONAL

Política: Toda persona que ingresa como usuario nuevo a EMPOAGUAS E.S.P. para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como

Cumplir y respetar al pie de la letra las directrices impartidas en el plan de desarrollo tecnologías de la Información.

4.1 Usuarios nuevos

Todo el personal nuevo de la Empresa, deberá ser notificado a el área de sistemas, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo) o en caso

de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático.

4.2 Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir el plan de desarrollo tecnologías de la Información.

4.3 Capacitación en seguridad informática

Todo servidor o funcionario nuevo en EMPOAGUAS E.S.P. deberá contar con la inducción del plan de desarrollo tecnologías de la Información.

4.4 Sanciones

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta dependencia, o de que se le declare culpable de un delito informático.

5. SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE

Política: Para el acceso a los sitios y áreas restringidas se debe notificar al área de sistemas para la autorización correspondiente, y así proteger la información y los bienes informáticos.

5.1 Protección de la Información y de los Bienes Informáticos.

5.1.1 El usuario o funcionario deberá reportar de forma inmediata al área de sistemas cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

5.1.2 El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

5.1.3 Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

5.2 Controles de Acceso Físico

5.2.1 Cualquier persona que tenga acceso a las instalaciones de EMPOAGUAS E.S.P., 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 entidad, en el área de recepción o portería, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

5.2.2 Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá ser retirado de las instalaciones de EMPOAGUAS E.S.P. únicamente con la autorización de salida del área de almacén, anexando el comunicado de autorización del equipo debidamente firmado por el Coordinador Administrativo y Financiero.

5.3 Seguridad en áreas de trabajo Los centros de cómputo de EMPOAGUAS E.S.P. Son áreas restringidas, por lo que solo el personal autorizado por el área de sistemas puede acceder a él.

5.4 Protección y ubicación de los equipos

5.4.1 Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, 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.

5.4.2 El Área de almacén de activos 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.

5.4.3 El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de los funcionarios o servidores de EMPOAGUAS E.S.P.

5.4.4 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.

5.4.5 Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro virtual INF. EMPOAGUAS (\\backup2018) destinada para archivos, diferente de programas y sistemas operativos, que generalmente se guardan en c:\. O bases creadas en partición D:/

5.4.6 Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

5.4.7 Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.

5.4.8 Se debe mantener el equipo informático en un lugar limpio y sin humedad.

5.4.9 El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar una reubicación de cables con el personal del área de sistemas.

5.4.10 Cuando se requiera realizar cambios múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación al área de sistemas a través de un plan detallado.
5.4.11 Queda terminantemente prohibido que el usuario o funcionario distinto al personal del área de sistemas destape los equipos de cómputo.

5.5 Mantenimiento de Equipos

5.5.1 Únicamente el personal autorizado por el área de sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.

5.5.2 Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

5.6 Perdida de Equipo

5.6.1 El servidor o funcionario que tengan bajo su responsabilidad o asignados 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.

5.6.2 El servidor o funcionario deberán dar aviso inmediato al área de Sistemas, y al área de almacén la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

5.6.3 El préstamo de equipos o portátiles tendrá que solicitarse al área de almacén, con el visto bueno del coordinador administrativo y financiero o su Jefe inmediato.

5.7 Uso de Dispositivos Extraíbles

5.7.1 Cada coordinador de Área o dependencia debe reportar al área de sistemas el listado de funcionarios a su cargo que manejan estos tipos de dispositivos, especificando clase, tipo y uso determinado.

5.7.2 El servidor o funcionario usuario que tengan asignados estos tipos de dispositivos serán responsables del buen uso de ellos.

5.7.3 Si algún área o dependencia por requerimientos muy específicos del tipo de aplicación o servicios de información tengan la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por su Jefe inmediato o un superior.
5.7.4 Todo funcionario o servidor de EMPOAGUAS E.S.P. deberá reportar al área de sistemas el uso de las memorias USB asignados para su trabajo y de carácter personal y responsabilizarse por el buen uso de ellas.

5.8 Daño de equipo

5.8.1 El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad.

6. ADMINISTRACIÓN DE OPERACIONES EN LOS CENTROS DE CÓMPUTO

6.1Políticas del centro de cómputo los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica de EMPOAGUAS E.S.P. de igual forma, deberán proteger la información reservada o confidencial que por necesidades empresariales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna empresarial a otras dependencias o redes externas como internet.

6.1.1 Los usuarios y funcionarios de EMPOAGUAS E.S.P. que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

6.1.2 Cuando un funcionario no autorizado o un visitante requieran la necesidad de ingresar a la Sala donde se encuentren los Servidores, debe solicitar mediante comunicado interno debidamente firmada y autorizado por el Jefe inmediato de su área o dependencia y para un visitante se debe solicitar la visita con anticipación la cual debe traer el visto bueno de la gerencia, y donde se especifique tipo de actividad a realizar, y siempre contar con la presencia de un funcionario del área de sistemas.

6.1.3 Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.

6.1.4 El encargado del área de sistemas deberá solicitar a la gerencia los equipos de protección para las instalaciones contra incendios, inundaciones, sistema eléctrico de respaldo, UPS.

6.2Uso de medios de almacenamiento

6.2.1 Los usuarios y servidores de EMPOAGUAS E.S.P. deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

6.2.2 Las actividades que realicen los usuarios y funcionarios en la infraestructura Tecnología de Información y Comunicaciones (TIC´s) de EMPOAGUAS E.S.P. serán registradas y podrán ser objeto de auditoria.

6.3 Adquisición de Software

6.3.1 Los usuarios y funcionarios que requieran la instalación de software que no sea propiedad de EMPOAGUAS E.S.P., deberán justificar su uso y solicitar su autorización por el área de sistemas con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.

6.3.2 Se considera una falta grave el que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de EMPOAGUAS E.S.P., que no esté autorizado por el área de sistemas.

6.3.3 El área de sistemas, tiene a su cargo la tarea de informar periódicamente a los Administrativos, su política institucional contra la piratería de software, utilizando todos los medios de comunicación disponibles: Emails, Carteleras y oficios. Debemos considerar también la publicación de las posibles prohibiciones en las que se puede incurrir.

6.3.4 El control de manejo para las licencias y el inventario de los medios, paquete de CD´s será responsabilidad del área de sistemas en cabeza del Técnico de Sistemas, o su delegado, en caso de ausencia.

6.3.5 El Técnico del área de sistemas tiene la responsabilidad de velar por el buen uso de los equipos de cómputo y del cumplimiento de las políticas de seguridad. A su vez deberán ofrecer mantenimiento preventivo a las computadoras de la Empresa.

6.3.6 En el proceso de reinstalar un programa el técnico debe borrar completamente la versión instalada para luego proceder a instalar la nueva versión que desea, esto siempre y cuando no sea una actualización del mismo.

6.4 Identificación del incidente

6.4.1 El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al área de sistemas lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

6.4.2 Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Directivas Administrativas competentes, el usuario o funcionario deberá notificar a l área de sistemas.

6.4.3 Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de EMPOAGUAS E.S.P. debe ser reportado al área de sistemas.

6.5 Administración de la Red

6.5.1 Los usuarios de las áreas de EMPOAGUAS E.S.P. no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la entidad, sin la autorización del área de sistemas.

6.6 Seguridad para la red

6.6.1 Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el área de sistemas, en la cual los usuarios o funcionarios realicen la exploración de los recursos informáticos en la red de EMPOAGUAS E.S.P., así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

6.7 Uso del correo electrónico

6.7.1 Los usuarios y funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re-direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a EMPOAGUAS E.S.P., a menos que cuente con la autorización del área de sistemas.

6.7.2 Los usuarios y funcionarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de EMPOAGUAS E.S.P. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

6.7.3 Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades.

6.7.4 Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

6.7.5 Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

6.8 Controles contra virus o software malicioso

6.8.1 Para prevenir infecciones por virus informático, los usuarios de EMPOAGUAS E.S.P. no deben hacer uso de software que no haya sido proporcionado y validado por el área de sistemas.

6.8.2 Los usuarios de EMPOAGUAS E.S.P. deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el área de sistemas.

6.8.3 Todos los archivos de computadoras que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

6.8.4 Ningún usuario, funcionario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del área de sistemas.

6.8.5 Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y notificar al área de sistemas para la revisión y erradicación del virus.

6.8.6 Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean

implantadas por el área de sistemas en: Antivirus, Outlook, office, Navegadores u otros programas.

6.8.7 Debido a que algunos virus son extremadamente complejos, ningún Usuario o funcionario de EMPOAGUAS E.S.P., distinto al personal del área de sistemas deberá intentar erradicarlos de las computadoras.

6.9 Controles para la generación y restauración de copias de respaldo (backups)

6.9.1 Procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la empresa. Se deberán considerar como mínimo los siguientes aspectos:

6.9.1.1 Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores.

6.9.1.2 Cada funcionario es responsable directo de la generación de los backups o copias de respaldo de su equipo propio, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups al área de sistemas.

6.9.1.3 Sera responsabilidad de los backups del servidor el encargado del área de sistemas.

6.9.1.4 Las copias de seguridad o Backups se deben realizar al menos una vez a la semana y el último día hábil del mes. Un funcionario del área de sistemas, revisará una vez por semana, el cumplimiento de este procedimiento.

6.10 Planes de contingencia ante desastres

Definición: Se entiende por PLAN DE CONTINGENCIA los procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información. Estos deben prepararse de cara a futuros sucesos.

6.10.1 Disponibilidad de plataformas computacionales, comunicaciones e información, necesarias para soportar las operaciones definidas como de misión crítica de negocio en los tiempos esperados y acordados.

6.10.2 Tener en existencia equipos informáticos de respaldo o evidencia de los proveedores, de la disponibilidad de equipos y tiempos necesarios para su instalación, en préstamo, arriendo o sustitución.

6.10.3 Existencia de documentación de los procedimientos manuales a seguir por las distintas áreas usuarias durante el periodo de la contingencia y entrenamiento a los usuarios en estos procedimientos.

6.10.4 Existencia de documentación de pruebas periódicas de la implementación del plan de recuperación ante desastre para verificar tiempos de respuesta, capitalizando los resultados de la pruebas para el afinamiento del plan.

6.10.5 Actualización periódica del plan de recuperación ante desastre de acuerdo con los cambios en plataformas tecnológicas (hardware,software y comunicaciones), para reflejar permanentemente la realidad operativa y tecnológica de la compañía.

6.10.6 Disponibilidad de copias de respaldo para restablecer las operaciones en las áreas de misión crítica definidas.

6.11 Internet

6.11.1 El acceso a Internet provisto a los usuarios y funcionarios de EMPOAGUAS E.S.P. es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

6.11.2 Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por EMPOAGUAS E.S.P., en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por el área de sistemas.

6.11.3 Los usuarios de Internet de EMPOAGUAS E.S.P. tienen que reportar todos los incidentes de seguridad informática a l área de sistemas inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

4.11.4 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, 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.

- 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 sus funciones y cargo en EMPOAGUAS E.S.P. y no para propósitos personales.

7. ACCESO LOGICO

Política: Cada usuario y funcionario son responsables de los mecanismos de control de acceso que les sean proporcionados; esto es, de su "ID" login de usuario y contraseña necesarios para acceder a la red interna de información y a la infraestructura tecnológica de EMPOAGUAS E.S.P., por lo que se deberá mantener de forma confidencial.
El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de EMPOAGUAS E.S.P., debe ser proporcionado por el dueño de la información, con base en el principio de "Derechos de Autor" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

7.1 Controles de Acceso Lógico

7.1.1 Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.

7.1.2 Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el área de sistemas antes de poder usar la infraestructura tecnológica de la EMPOAGUAS E.S.P.

7.1.3 Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica

de EMPOAGUAS E.S.P., a menos que se tenga el visto bueno del dueño de la información, del área de sistemas y la autorización de su Jefe inmediato.

7.1.4 Cada usuario que acceda a la infraestructura tecnológica de EMPOAGUAS E.S.P. debe contar con un identificador de usuario (ID) único y personalizado. Por lo cual no está permitido el uso de un mismo ID por varios usuarios.

7.1.5 Los usuarios y funcionarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

7.2 Administración de Privilegios

7.2.1 Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados al área de sistemas (Administrador de la Red), para el cambio de privilegios.

7.3 Equipo desatendido

7.3.1 Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados y autorizados por el área de sistemas cuando no se encuentren en su lugar de trabajo.

7.4 Administración y Uso de Contraseñas

7.4.1 La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

7.4.2 Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al área de sistemas para que se le proporcione una nueva contraseña.

7.4.3 Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

7.4.4 Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.

7.4.5 Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, deberá cambiarlo inmediatamente.

7.4.6 Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

7.5 Controles para otorgar, modificar y retirar accesos a usuarios

7.5.1 Cualquier nuevo rol creado por el área de sistemas se deberá analizar y concertar con los coordinadores.

7.5.2 Todo usuario debe quedar registrado en la base de datos usuarios y roles. La creación de un nuevo usuario y/o solicitud para la asignación de otros roles dentro del sistema de EMPOAGUAS E.S.P., deberá de venir acompañado del reporte debidamente firmado por el Jefe inmediato de Área y con el visto bueno del Gerente, de lo contrario no se le dará trámite a dicha requisición.

7.6 Control de Accesos Remotos

7.6.1 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.

8. SERVICIOS TECNOLOGICOS

Con relación a la gestión de los servicios tecnológicos, conectividad y monitoreo, son administrados por el área de sistema en el cual las actividades a realizar se encuentra la plataforma de almacenamiento, respaldos, servidores, aplicaciones, bases de datos, office, seguridad informática y de la información, redes Lan y redes inalámbricas, correos electrónicos de igual forma se tiene contratado soporte especializado para y actualizaciones según acuerdo de servicio tipo platinum *STEFANINI SYSMAN S.A.S.*

9. CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Política: El área de sistemas tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

9.1 Violación de Seguridad Informática

9.1.1 Está 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.
9.1.2 Ningún usuario o funcionario de EMPOAGUAS E.S.P. debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por el área de sistemas.
9.1.3 No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de EMPOAGUAS E.S.P.

9.2 Equipos en el Área ee Administrativa

9.2.1 Las coordinaciones deberán poner a disposición del área de sistemas, la información contractual de los equipos informáticos de Cómputo Escritorio, Portátil y periférica, así como de los servicios de soporte y mantenimiento.

9.2.2 El área de sistemas, será quien valide el cumplimiento de las Condiciones Técnicas de los equipos informáticos de Cómputo Escritorio, Portátiles y Periféricos adquiridos.

9.2.3 El área de sistemas, tendrá bajo su resguardo las licencias de software, CD de software y un juego de manuales originales, así como un CD de respaldo para su instalación, mismos que serán entregados por los coordinadores o el área usuaria de la licencia, para llevar el control de software instalado, para los equipos informáticos de cómputo Escritorio, Portátiles y periféricos al momento de la recepción de los mismos.

9.2.4 Los requerimientos de Equipos Informáticos de Cómputo Escritorio, Portátiles y periféricos, se llevarán a cabo mediante la solicitud y justificación por escrito, firmada por el Jefe inmediato, los cuales serán evaluados por el área de sistemas para su autorización e inclusión en el Plan Anual de Presupuesto correspondiente.

9.2.5 El área de sistemas, es el área encargada de tramitar las asignaciones, reasignaciones, bajas, etc. de equipos informáticos de cómputo Escritorio, Portátiles y periféricos ante el área de almacén encargada del Inventario de Activos para su ejecución, con base a las solicitudes realizadas al respecto y las revisiones de aprovechamiento de los mismos.

9.2.6 Queda prohibido a los usuarios mover los equipos informáticos de cómputo Escritorio, Portátiles y periféricos por su propia cuenta, el usuario deberá solicitar al área de sistemas el movimiento así como informar la razón del cambio y en su caso, requerir la reasignación del equipo.

9.2.7 El área de sistemas deberá elaborar el pase de salida cuando algún bien informático de cómputo Escritorio, Portátiles y periférico requiera ser trasladado fuera de las instalaciones de EMPOAGUAS E.S.P. por motivo de garantía, reparación o evento.

9.2.8 Si algún equipo informático de cómputo Escritorio, Portátiles o periférico es trasladado por el usuario a oficinas distintas al lugar asignado, oficinas externas o foráneas para realizar sus labores, dicho bien estará bajo resguardo del responsable que retira el equipo y el pase de salida quedará a consideración del área de sistemas para su autorización y visto bueno.

9.2.9 Las diferentes Áreas de EMPOAGUAS E.S.P. serán encargadas de proporcionar al área de sistemas, la relación de bienes y equipos que entrarán al proceso de baja, según corresponda. El área de sistemas realizara la evaluación técnica del equipo y definirá la reasignación o baja definitiva del bien que será informada al área de almacén para control de Inventarios de Activos por medio del procedimiento definido por el mismo.

9.2.10 Queda prohibida la baja de equipo de cómputo que no cuente con evaluación técnica por parte del área de sistemas.

9.2.11 El área de sistemas no es responsable de proporcionar asesoría técnica, mantenimiento preventivo o correctivo a equipo de cómputo propiedad del usuario.

9.2.12 El usuario que ingrese equipos de su propiedad a las instalaciones de EMPOAGUAS E.S.P. es responsable de la información almacenada en el mismo, y deberá mantener la privacidad, integridad y respaldos de la misma sin ser esto responsabilidad del área de sistemas.

9.2.13 Queda prohibido instalar software no autorizado o que no cuente con licencia, el área de sistemas deberá realizar las instalaciones de acuerdo con los estándares de EMPOAGUAS E.S.P.

9.2.14 Es responsabilidad del usuario a quien esté asignado el equipo de escritorio o portátil, la información contenida en la misma.

9.2.15 Cuando un usuario cambie de área, el equipo asignado a éste deberá permanecer dentro del área designada originalmente. Será responsabilidad de la nueva área en la que habrá de laborar el usuario, el proporcionarle equipo de cómputo para el desarrollo de sus funciones.

9.2.16 En el caso de reinstalaciones de equipo, el usuario será el responsable de verificar que toda la información y archivos de trabajo estén contenidos en el equipo asignado, el usuario deberá firmar la Solicitud o Asignación del servicio proporcionado por el técnico o ingeniero asignado firmando de conformidad.

9.2.17 El área de sistemas no es responsable de la configuración de dispositivos personales tales como Palms, iPOD y teléfonos celulares propiedad del usuario.

9.2.18 El usuario que requiera la instalación de Software de su propiedad deberá solicitar por escrito al área de sistemas anexando copia de la licencia que compruebe su propiedad o en el caso de software libre el documento probatorio.

9.2.19 El Software autorizado para todos los equipos de cómputo del cual EMPOAGUAS E.S.P. cuenta con Licencia de uso son los siguientes:

- Windows Server 2016 R2
- Stefanini Sysman S.A.S
- Windows 10
- Microsoft Office 2016.
- Microsoft Office 2013.