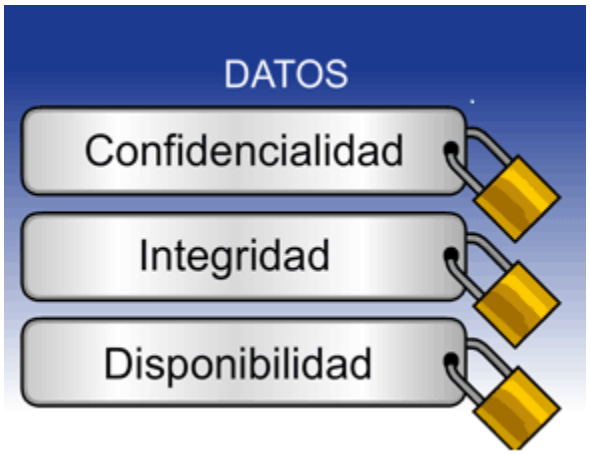
POLITICA DE SEGURIDAD DE LA INFORMACION



EMPRESA DE SERVICIOS PUBLICOS DE ACACIAS ESP

La Política de Seguridad debe cubrir, en la medida de sus posibilidades, todos los aspectos que pudieran poner en peligro la información, sin olvidar las medidas de seguridad física.

CONTENIDO

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA

Propósito

Introducción

Objetivo

Alcance

Beneficios

Que son estándares de seguridad

Que son políticas de seguridad

1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

1.1 Obligaciones de los usuarios

1.2 Acuerdos de uso y confidencialidad

1.3 Entrenamiento en seguridad informática

1.4 medidas disciplinarias

2. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

2.1 Resguardo y protección de la información

2.2 Controles de acceso físico

2.3 Seguridad en áreas de trabajo

2.4 Protección y ubicación de los equipos

2.5 Mantenimiento de equipo

2.6 Pérdida de quipo

2.7 Uso de dispositivos especiales

2.8 Daño del Equipo

3.- POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

3.1 Uso de medios de almacenamiento

3.2 Instalación de software.

3.3 Identificación del incidente

3.4 Administración de la configuración

3.5 Seguridad para la red

3.6 Uso del correo electrónico

3.7 Controles contra código malicioso

3.8 Internet

4.- POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

4.1 Controles de acceso lógico

4.2 Administración de privilegios

4.3 Equipo desatendido

4.4 Administración y uso de contraseña

4.5 Control de accesos remotos

5.- POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

5.1 Derechos de propiedad intelectual

5.2 Revisiones del cumplimiento

5.3 Violaciones de seguridad informática

Glosario de términos

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA PARA USUARIOS

Propósito

El presente documento tiene como finalidad dar a conocer las políticas y estándares de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de la Empresa de Servicios Públicos de Acacías ESPA E.S.P.

Introducción

La Empresa de Servicios Públicos de Acacias ESPA ESP, depende de los sistemas TI (Tecnologías de Información) para alcanzar sus objetivos institucionales. En consecuencia, estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados. Por ello, el objetivo de la seguridad de la información es garantizar la calidad de la información (confidencialidad, integridad, disponibilidad y usos previstos) y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. Esto implica que la organización y su personal deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, (ENS) así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.
El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010 , de 8 de enero , determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos. El cual está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestiones en el ejercicio de sus competencias

La base para que cualquier organización pueda operar de una forma confiable en materia de seguridad Informática comienza con la definición de las políticas y estándares.

La Seguridad Informática, es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. en materia de seguridad.

Toda persona que utilice los servicios que ofrece la red, deberá conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

Este documento se encuentra estructurado en cinco políticas generales de seguridad para usuarios de informática, con sus respectivos estándares que consideran los siguientes puntos:

1. Seguridad de Personal.
2. Seguridad Física y Ambiental.
3. Administración de Operaciones de Cómputo.
4. Controles de Acceso Lógico.
5. Cumplimiento

Objetivo

Establecer y difundir las Políticas y Estándares de Seguridad Informática a todo el personal de la Empresa de Servicios Públicos de Acacías ESPA. E.S.P., para que sea de su conocimiento y cumplimiento en los recursos informáticos asignados y establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y personas que interactúan haciendo uso de los servicios asociados a ellos.

Alcance

El documento describe las políticas y los estándares de seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos de la Empresa de Servicios Públicos de Acacías ESPA E.S.P.

Beneficios

Las políticas y estándares de seguridad informática establecidas dentro de este documento son la base para la protección de los activos tecnológicos e información de la Empresa de Servicios Públicos de Acacías ESPA E.S.P.

Que son Estándares de Seguridad?

Un estándar de seguridad puede ser conceptualizado como la definición clara de un modelo, criterio, regla de medida o de los requisitos mínimos aceptables para la operación de procesos específicos, con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red institucional.

Políticas de Seguridad?

Surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer nuestra política de seguridad requiere un alto compromiso con la organización, para establecer fallas y debilidades en su aplicación, y constancia para renovar y actualizar dicha política.

El objetivo de la **Política de Seguridad de Información** de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad.
Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.

1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política

Todo usuario de bienes y servicios informáticos al ingresar como personal acepta las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., así como el estricto apego al Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

Los usuarios deberán cumplir con lo establecido en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

1.1 Obligaciones de los Usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para usuarios del presente manual.

1.2 Acuerdos de Uso y Confidencialidad

Todos los usuarios de bienes y servicios informáticos de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. deben firmar de aceptación el convenio de confidencialidad y uso adecuado de los recursos informáticos y de información de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., así como comprometerse a cumplir con lo establecido en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

1.3 Entrenamiento en Seguridad Informática

Todo empleado o funcionario de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. deberá contar con la inducción sobre el "Manual de Políticas y Estándares de Seguridad Informática para Usuarios", donde se den a conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento.

1.4 Medidas disciplinarias

1.4.1 Se consideran violaciones graves el robo, daño, acceso no autorizado, divulgación de información reservada o confidencial de la Empresa de Servicios Públicos de Acacias ESPA E.S.P., o de que se le declare culpable de un delito informático.

1.4.2 Cuando la dependencia de Sistemas identifique el incumplimiento al presente Manual remitirá el reporte o denuncia correspondiente a la dependencia de Control Interno de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., para los efectos de su competencia y atribuciones.

2. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Política

Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la Empresa de Servicios Públicos de Acacias ESPA E.S.P. sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones así como las instalaciones y el Centro de Cómputo de la Empresa de Servicios Públicos de Acacias ESPA E.S.P.

2.1 Resguardo y Protección de la Información

2.1.1 El usuario deberá reportar de forma inmediata a la dependencia de Sistemas cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

2.1.2 El usuario tiene la obligación de proteger las unidades de almacenamiento como memorias USB, CD – ROM, cintas magnéticas, DVDs, discos externos, disquetes y tarjetas de memoria, como también computadoras y dispositivos portátiles que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

2.1.3 Es responsabilidad del usuario evitar en todo momento la fuga de la información de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

2.2 Controles de Acceso Físico

2.2.1 Cualquier persona que tenga acceso a las instalaciones de la Empresa de Servicios Públicos de Acacías ESPA 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 Empresa de Servicios Públicos de Acacías ESPA E.S.P, en el área de recepción, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

2.2.2 Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá salir de las instalaciones de la

Empresa de Servicios Públicos de Acacías ESPA E.S.P únicamente con la autorización de salida de la dependencia de Almacén anexando el documento de salida del equipo debidamente firmado por el funcionario de esta dependencia.

2.3 Seguridad en Áreas de Trabajo

La dependencia de Sistemas de la Empresa de Servicios Públicos de Acacías E.S.P. es área restringida, por lo que sólo el personal autorizado por la dependencia de sistemas de la Empresa de Servicios Públicos de Acacías ESP puede acceder a él.

2.4 Protección y Ubicación de los Equipos

2.4.1 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 de la dependencia de Sistemas de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. , en caso de requerir este servicio deberá solicitarlo por escrito a la dependencia de Sistemas.

2.4.2 La dependencia de Almacén de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. es el encargado 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 la dependencia de Sistemas

2.4.3 El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de la Empresa de Servicios Públicos de Acacías ESPA E.S.P.

2.4.4 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.

2.4.5 Es responsabilidad de los usuarios almacenar su información únicamente en la carpeta asignada en el servidor ya que las otras están destinadas para archivos de programa y sistema operativo.

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

2.4.7 Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU u otro equipo que requiera ventilación.

2.4.8 Se debe mantener el equipo informático en un entorno limpio y sin humedad.

2.4.9 El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos.

2.4.10 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 a la dependencia de Sistemas a través de un plan detallado de movimientos debidamente autorizado por el Jefe del área que corresponda.

2.4.11 Queda prohibido que el usuario abra o desarme los equipos de cómputo.

2.4.12 Queda prohibido que el usuario instale o desinstale algún software.

2.4.13 Queda prohibido que el usuario configure o reconfigure el sistema operativo del ordenador.

2.5 Mantenimiento de Equipo

2.5.1 Únicamente el personal autorizado por la dependencia de Sistemas de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

2.5.2 Los usuarios deberán asegurarse de respaldar 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.

2.6 Pérdida de Equipo

2.6.1 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.

2.6.2 El préstamo de laptops, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

2.6.3 El usuario deberá dar aviso inmediato al área de Sistemas o Control interno, Almacén de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

2.7 Uso de Dispositivos Especiales

2.7.1 El uso de los grabadores de discos compactos es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

2.7.2 El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

2.7.3 La asignación de este tipo de equipo será previa justificación por escrito y previa autorización del jefe inmediato correspondiente.

2.7.4 Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por la Subgerencia Administrativa.

2.7.5 Queda prohibido el uso de módems externos en las computadoras de escritorio, excepto cuando lo autorice la Gerencia. Además queda totalmente prohibido el uso de redes Sociales (Facebook, whatsApp, etc.)

2.7.6 Los módems internos deberán existir solo en las computadoras portátiles y no se deberán utilizar dentro de las instalaciones de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. para conectarse a ningún servicio de información externo, excepto cuando lo autorice la Gerencia.

2.8 Daño del Equipo.

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, deberá cubrir el valor de la reposición o reparación del equipo o accesorio afectado. Para tal caso el área de Sistemas determinará la causa de dicha descompostura.

3. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO.

Política

Los usuarios deberán proteger la información que reside y utiliza la infraestructura tecnológica de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de la organización o hacia redes externas como Internet.

Los usuarios de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de troya o gusanos de red.

3.1 Uso de medios de almacenamiento

3.1.1 Toda solicitud para utilizar un medio de almacenamiento de información compartido (File Share), deberá contar con la autorización del área dueña de la información. El personal que requiera estos medios debe justificar su utilización. Dicha justificación deberá de presentarla al Área de Sistemas firmada por su Director de área de adscripción.

3.1.2 Los usuarios de informática de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

3.1.3 En caso de que por el volumen de información se requiera algún respaldo en CD, este servicio deberá solicitarse por escrito al a dependencia de Sistemas con la firma del Director del área correspondiente.

3.1.4 Los usuarios deberán respaldar diariamente la información sensitiva y crítica que se encuentre en sus computadoras personales o estaciones de trabajo

3.1.5 Así mismo el funcionario debe crear una carpeta en una Unidad menos en (C:) con el nombre de la dependencia y seguir guardando toda la información de la Empresa, con el fin de que el Área de Sistemas este guardando los datos.

3.1.6 Es necesario que cada Usuario le coloque clave a su equipo y cada vez que se retire de su PC, bloquear con el fin de que entren intrusos y le puedan borrar o robarle información. Cabe anotar que al colocar clave a su computador la única persona quien debe tener conocimiento de ella es el área de Sistemas o Gerencia si así lo determine y debe guardarla en un sitio seguro. Recuerde su clave de acceso a los diferentes programas o equipos es personal e intransferible y de exclusiva responsabilidad de cada usuario una vez que se le entregue desde el Departamento de Sistemas. El formato de la clave se sugiere sea del tipo alfanumérica (números y letras) sin embargo, por razones de usabilidad para nuestros usuarios se aceptan claves que estén solamente compuestas por letras y con un largo mínimo de 8 caracteres. De igual manera, se sugiere a los usuarios cambiarla de forma periódica con el fin de no correr el riesgo de detección de clave por parte de otra persona (interna o externa al servicio) quien pudiese hacer mal uso de la información que se pudiese obtener al utilizar dicha clave o, por hacer un favor, generar eventos con errores los que serán siempre de responsabilidad del dueño de la clave.

3.1.7 Las actividades que realicen los usuarios en la infraestructura de tecnología de información de la Empresa de Servicios Públicos de Acacias ESPA E.S.P. son registradas y susceptibles de auditoría.

3.2 Instalación de software.

3.2.1 Los usuarios que requieran la instalación de software que no sea propiedad de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., deberán justificar su uso y solicitar su autorización a la Dependencia de

Sistemas, a través de un oficio firmado por su Dirección de adscripción indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación.

3.2.2 Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Empresa de Servicios Públicos de Acacías ESP, que no esté autorizado por la dependencia de Sistemas.

3.3 Identificación del incidente

3.3.1 El usuario que sospeche o tenga conocimiento de la 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.

3.3.2 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 unidades administrativas competentes, el usuario informático deberá notificar al Área de Sistemas.

3.3.3 Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. debe ser reportado al Área de Sistemas.

3.4 Administración de la configuración

Los usuarios de las áreas de la Empresa de Servicios Públicos de Acacías ESP. 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, SSH), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la Empresa de Servicios Públicos de Acacias ESPA E.S.P., sin la autorización del Área de Sistemas.

3.5 Seguridad para la red

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 realicen la exploración de los recursos informáticos en la red de

la Empresa de Servicios Públicos de Acacías ESPA E.S.P., así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

3.6 Uso del Correo electrónico

3.6.1 Los usuarios 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 redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., a menos que cuente con la autorización de la Dirección de Área.

3.6.2 Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de Empresa de Servicios Públicos de Acacías ESP,. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

3.6.3 Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó el Área de Sistemas.

3.6.4 Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

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

3.6.6 La Empresa de Servicios Públicos de Acacías ESPA E.S.P., se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violando políticas de Seguridad Informática de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., o realizado acciones no autorizadas.

3.6.7 El usuario debe de utilizar el correo de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el

desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.

3.6.8 La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito a la dependencia de Sistemas, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del Jefe del área que corresponda.

3.7 Controles contra código malicioso

3.7.1 Para prevenir infecciones por virus informático, los usuarios de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. no deben hacer uso de software que no haya sido proporcionado y validado por el Área de Sistemas.

3.7.2 Los usuarios de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. deben verificar que la información y los medios de almacenamiento, memorias USB, CDs, discos flexibles, discos externos, tarjetas de memoria, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el Área de Sistemas.

3.7.3 Todos los archivos de computadora 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.

3.7.4 Ningún usuario, 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.

3.7.5 Ningún usuario de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software. Tampoco debe probarlos en cualquiera de los ambientes o plataformas de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. El incumplimiento de este estándar será considerado una falta grave.

3.7.6 Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al Área de Sistemas para la detección y erradicación del virus.

3.7.7 Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la Empresa de Servicios Públicos de Acacías ESPA E.S.P. en: Antivirus, Outlook, Office, Navegadores u otros programas.

3.7.8 Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar de manera periódica al Área de Sistemas las actualizaciones del software de antivirus.

3.7.9 Debido a que algunos virus son extremadamente complejos, ningún usuario de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. debe intentar erradicarlos.

3.8 Internet

3.8.1 El acceso a Internet provisto a los usuarios de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

3.8.2 Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la Empresa de Servicios Públicos de Acacías ESPA E.S.P.

3.8.3 Los usuarios con acceso a Internet de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. tienen que reportar todos los incidentes de seguridad informática a la dependencia de Sistemas, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

3.8.4 El acceso y uso de módem en la Empresa de Servicios Públicos de Acacías ESPA E.S.P. tiene que ser previamente autorizado por el Área de Sistemas.

3.8.5 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 de la dependencia de Sistemas.
- La utilización de Internet es para el desempeño de su función y puesto en la Empresa de Servicios Públicos de Acacías ESPA E.S.P. y no para propósitos personales.

4. POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Política

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y contraseña necesarios para acceder a la información y a la infraestructura tecnológica de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., por lo cual deberá mantenerlo de forma confidencial.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., debe ser proporcionado por el dueño de la información, con base en el principio de la "necesidad de saber" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

4.1 Controles de acceso lógico

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

4.1.2 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 Empresa de Servicios Públicos de Acacías ESPA E.S.P.

4.1.3 El acceso a la infraestructura tecnológica de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. para personal externo debe ser autorizado al menos por Director o Jefe de área de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., quien deberá notificarlo por oficio al Área de Sistemas, quien lo habilitará.

4.1.4 Está prohibido que los usuarios utilicen la infraestructura tecnológica de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., para obtener acceso no autorizado a la información u otros sistemas de información de la Empresa de Servicios Públicos de Acacías ESPA E.S.P.

4.1.5 Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., a menos que se tenga la autorización del dueño de la información y del Área de Sistemas.

4.1.6 Cada usuario que acceda a la infraestructura tecnológica de la Empresa de Servicios Públicos de Acacías ESPA E.S.P., debe contar con un identificador de usuario (UserID) único y personalizado, por lo cual no está permitido el uso de un mismo (UserID) por varios usuarios.

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

4.2 Administración de privilegios

Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de la Empresa de Servicios Públicos de Acacías ESPA E.S.P, deberán ser notificados a la dependencia de Sistemas con el visto bueno de su Director o Jefe de área.

4.3 Equipo desatendido

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.

4.4 Administración y uso de contraseña

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

4.4.2 Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito al Área de Sistemas indicando si es de acceso a la red o a módulos de sistemas para que se le proporcione una nueva contraseña.

4.4.3 La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante el Área de Sistemas como empleado de la Empresa de Servicios Públicos de Acacías ESP.

4.4.4 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.

4.4.5 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.

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

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

4.5 Control de accesos remotos

4.5.1 Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno del Área de Sistemas.

4.5.2 La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el Área de Sistemas.

5. POLÍTICAS Y ESTÁNDARES DE 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.

5.1 Derechos de propiedad intelectual

5.1.1 Los sistemas desarrollados por personal interno o externo que controle el Área de Sistemas son propiedad intelectual de la Empresa de Servicios Públicos de Acacías ESPA E.S.P.

5.1.2 Está prohibido por las leyes de derechos de autor y por la Empresa de Servicios Públicos de Acacías ESPA E.S.P., realizar copia no autorizadas de software, ya sea adquirido o desarrollado por la Empresa de Servicios Públicos de Acacías ESPA E.S.P.

5.2 Revisiones del cumplimiento

5.2.1 El Área de Sistemas realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

5.2.2 El Área de Sistemas podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en estas políticas.

5.2.3 Los líderes y responsables de los procesos establecidos en la Empresa de Servicios Públicos de Acacías ESPA E.S.P. deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

5.3 Violaciones de seguridad Informática

5.3.1 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.

5.3.2 Ningún usuario de la Empresa de Servicios Públicos de Acacías ESPA E.S.P. debe probar o intentar probar fallas de la Seguridad Informática o conocidas, a menos que estas pruebas sean controladas y aprobadas por el Área de Sistemas.

5.3.3 Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información. Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación del Área de Sistemas, con excepción de los Órganos Fiscalizadores.

5.3.4 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 la de la Empresa de Servicios Públicos de Acacías ESPA E.S.P.

Glosario de Términos

A	
Termino	**Significado**
Acceso	Es el privilegio de una persona para utilizar un objeto o infraestructura.
Acceso Físico	Es la actividad de ingresar a un área.
Acceso Lógico	Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.
Acceso Remoto	Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación, ya sean telefónicas o por medio de redes de área amplia, que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de

	autenticación.
Aplicación	Acción que se realiza a través de un programa de manera directa con el usuario. Navegadores, Chat, correo electrónico, etc. Son algunos ejemplos de aplicaciones en el medio de Internet.
Antivirus	Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.
Ataque	Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese archivo y lograr afectarlo.
Archivo	Una colección identificada de registros relacionados.
Autorización	Es el proceso de asignar a los usuarios permisos para realizar actividades de cuerdo a su perfil o puesto.

B	
Termino	**Significado**
Base de datos	Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.

C	
Termino	**Significado**
CD	Medio de almacenamiento de información.
Código Malicioso	Hardware, software o firmware que es intencionalmente introducido en un sistema con malicioso o no autorizado. Un caballo de ejemplo de un código malicioso.
Comprimir (zip)	Reducir el tamaño de los archivos sin que éstos pierdan nada de su información. Zip es el nombre de la extensión que contiene un archivo comprimido.
Computadora	Es un conjunto de dispositivos electrónicos que forman una máquina electrónica capaz de procesar información siguiendo instrucciones almacenadas en programas.
Confidencialidad	Se refiere a que la información no sea divulgada a personal no autorizado para su conocimiento.
Control de Acceso	Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo tecnológico.

Copyright	Derecho que tiene un autor, incluido el autor de programa informático, sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas. Aunque este derecho es legalmente irrenunciable puede ser ejercido de Forma tan restrictiva o tan generosa como el autor decida. El símbolo de este derecho es ©.
Correo Electrónico o Email	La funcionalidad es similar a usar el correo normal, pero ahora el individuo puede utilizar una computadora y un software para enviar mensajes o paquetes a otro individuo o grupo de personas a una dirección específica a través de la red o Internet.
Cuentas de Usuario	Es un identificador, el cual es asignado a un usuario del sistema para el acceso y uso de la computadora, sistemas, aplicaciones, red, etc.

D	
Termino	**Significado**
Descargar	Acción de transferir información computarizada computadora a otra.
Descomprimir (unzip)	Acción que se lleva a cabo después de haber comprimido un archivo para regresarlo a su original.
Discos flexibles (diskettes)	Medios de almacenamiento magnéticos de información de 1.44 Mb llamados comúnmente discos de 3 ½.
Discos Ópticos	Los discos ópticos son medios de almacenamiento de información que presentan una capa interna protegida, donde se guardan los bits mediante el uso de un rayo láser, éste al ser reflejado, permite detectar variaciones microscópicas de propiedades "opticoreflectivas" ocurridas como consecuencia grabación realizada en la escritura. Un sistema con lentes encamina el haz luminoso, como un punto en la capa del disco que almacena los datos.
Disponibilidad	Se refiere a que la información esté disponible momento que se requiera.
Dominio	Sistema de denominación de host en Internet. Conjunto de caracteres que identifica y diferentes sitios Web.

E	
Termino	**Significado**
Inscripción	Proceso matemático donde los datos de un protegerlos de accesos no deseados. El término inscripción como tal, no existe en el lenguaje español, el

	término correcto es cifrado de datos.
Estándar	Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.

F	
Termino	**Significado**
Falta administrativa	Es la consecuencia que resulta del incumplimiento de la normatividad.
Freeware (Software Libre	Programas que se pueden bajar desde Internet sin cargo.
FTP	Protocolo de transferencia de Archivos. Es un protocolo estándar de comunicación, que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red

G	
Termino	**Significado**
Gusano	Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.

H	
Termino	**Significado**
Hardware	Se refiere a las características técnicas y físicas de las computadoras.
Help Desk / CAU	Soporte técnico brindado a los usuarios telefónicamente, su función es proveer conocimientos especializados de los sistemas de producción para identificar y asistir en el ámbito / desarrollo de sistemas y en la resolución de problemas.
Herramientas de seguridad	Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.

I

Vigilado Superservicios

Termino	Significado
Impacto	Magnitud del daño ocasionado a un activo en caso de que se materialice una amenaza.
Incidente de seguridad	Cualquier evento que represente un riesgo para la adecuada conservación de la confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.
Integridad	Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional o accidental.
Internet o World Wide Web (www)	Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes en donde cualquier usuarios consulta información de otra computadora conectada a esta red e incluso sin tener permisos necesarios acceder a dichos activos.
Intrusión	Es la acción de introducirse o acceder sin autorización a un activo tecnológico.

L	
Termino	**Significado**
Lenguaje de Programación	Sistema de escritura para la descripción precisa de algoritmos o programas informáticos.

M	
Termino	**Significado**
Maltrato, descuido o negligencia.	Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad de la ESPA E.S.P.
Malware	Código malicioso desarrollado para causar daños en equipos informáticos, sin el consentimiento del propietario. Dentro de estos códigos se encuentran: virus, spyware, troyanos, rootkits, backdoors, adware y gusanos.
Mecanismos de seguridad o de control	Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.
Medios Magnéticos (medios de almacenamiento)	Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (CD´s, DVD´s, etc.)

Vigilado Superservicios

Metodología	Es un conjunto de procedimientos ordenados y documentados que son diseñados para alcanzar un objetivo en particular y comúnmente son divididos en fases o etapas de trabajo previamente definidas.
Módem	Es un aparato electrónico que se adapta una terminal o computadora y se conecta a una red de. Los módems convierten los pulsos digitales de una computadora en frecuencias dentro de la gama de audio del sistema telefónico. Cuando actúa en calidad de receptor, un módem decodifica las frecuencias entrantes.

N	
Termino	**Significado**
"Necesidad de saber" principio	Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidades dentro de la Comisión.
Nodo	Punto principal en el cual se les da acceso a una red a las terminales o computadoras.
Normatividad	Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización

P	
Termino	**Significado**
Página Web	Es un documento o información electrónica capaz de contener texto, sonido, vídeo, programas, enlaces, imágenes, y muchas otras cosas, adaptada para la llamada World Wide Web, y que puede ser accedida mediante un navegador. Esta información se encuentra generalmente en formato HTML o XHTML, y puede proporcionar navegación (acceso) a otras páginas web mediante enlaces de hipertexto.
Parche (patch)	Un parche (algunas veces llamado Fix) son piezas de programación que representan una solución rápida al software o sistema, para incrementar la seguridad o incrementar la funcionalidad del mismo.
Password	Contraseña. Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a un computadora personal, sistema, aplicación o red en particular. Típicamente está compuesto

	de 6-10 caracteres alfanuméricos.

R	
Termino	**Significado**
Respaldo	Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.
Riesgo	Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene.

S	
Termino	**Significado**
Servidor	Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.
Sitio Web	El sitio web es un lugar virtual en el ambiente de internet, el cual proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a él.
Software	Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.
Software Antivirus	Aplicaciones que detectan, evitan y posiblemente eliminan todos los virus conocidos, de los archivos ubicados en el disco duro y en la memoria de las computadoras.
Spyware	Código malicioso desarrollado para infiltrar a la información de un equipo o sistema con la finalidad de extraer información sin la autorización del propietario.
Switch	Dispositivo de red que filtra y direcciona paquetes a las direcciones destinatarias. El switch opera en la capa de enlace de datos del,modelo OSI.

T	
Termino	**Significado**

Tarjeta Inteligente	Es una tarjeta de plástico del tamaño de una tarjeta de crédito, que incorpora un microchip, en el cual se puede cargar datos como números telefónicos anteriormente llamados, pagos realizados a través de medios electrónicos y otro tipo de aplicaciones, las cuales pueden ser actualizadas para usos adicionales.

U	
Termino	**Significado**
UserID	Se denomina al nombre de usuario con el cual accedemos a una página o sistema en el que previamente nos hemos registrado. Este nombre puede estar compuesto de letras, números o signos.
Usuario	Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal o dispositivo (hardware).

V	
Termino	**Significado**
Virus	Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o medios de almacenamiento magnético de computadoras.
Vulnerabilidad	Es una debilidad de seguridad o brecha de seguridad, la cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental.