POLÍTICAS OPERATIVAS DE TECNOLOGÍAS DE LA INFORMACIÓN (TI)

TABLA DE CONTENIDO

Alcance

Establecer un marco de uso de las Tecnologías de Información (TI) de la Empresa de Aseo de Pereira S.A. ESP, que logre satisfacer las necesidades actuales y futuras derivadas de la estrategia del negocio, siguiendo los criterios de innovación, calidad, eficiencia, escalabilidad, y de arquitectura empresarial. Estas políticas son aplicables a todos los colaboradores, consultores, contratistas, terceras partes, que usen las tecnologías de información de la entidad.

Cumplimiento

El cumplimiento de la Política de Tecnologías de la Información (TI) es obligatorio. Toda persona que para el desempeño de sus funciones utilice o tenga acceso a los bienes o servicios informáticos que ofrece la entidad deberá observar lo prescrito en las presentes políticas. La ignorancia del mismo no lo exonera de las responsabilidades asociadas con su incumplimiento.

La omisión de ejercitar o ejecutar cualquier derecho o disposición no constituirá una renuncia de tal derecho o disposición. La Coordinación de Sistemas, o quien haga sus veces, de la Empresa de Aseo de Pereira S.A. E.S.P. vigilará que se acaten las políticas operativas de TI vigentes.

Excepciones

Todas las excepciones a la Política de Tecnologías de la Información (TI), deben ser formalmente documentadas, registradas y revisadas por el Coordinador de Sistemas, o quien haga sus veces, y aprobadas por la Gerencia.

Administración de las políticas

Las modificaciones o adiciones de las Políticas de Tecnologías de la Información (TI) serán propuestas por la Coordinación de Sistemas, o quien haga sus veces, y aprobadas por la Gerencia. Estas políticas deben ser revisadas una vez al año o antes si se considera necesario.

Definiciones

Para efectos del presente documento se entiende por:

Activo: Cualquier cosa que tenga valor para la entidad.

Administrador del sistema. Persona responsable de administrar, controlar, supervisar y garantizar la operabilidad y funcionalidad de los sistemas. Dicha administración está en cabeza del Coordinador de Sistemas de la Empresa de Aseo de Pereira S.A. E.S.P. o quien haga sus veces.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la Organización.

Arquitectura empresarial: Conjunto de elementos organizacionales (estrategia, estructura, procesos más tecnología, personas) que se relacionan entre sí, garantizando la alineación desde los niveles más altos (estratégicos), medios (tácticos),hasta los más bajos (operativos), con el fin de optimizar la generación de productos y servicios que conforman la propuesta de valor entregada a los clientes.

Backup. Copia de seguridad de información en medio digital.

Buzón. También conocido como cuenta de correo, es un receptáculo exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a la empresa.

Chat. (Tertulia, conversación, charla). Comunicación simultánea entre dos o más personas a través de Internet o una Intranet.

Computador. Es un dispositivo de computación de sobremesa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Contraseña o password. Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

Correo electrónico. También conocido como E-mail, abreviación de electronic mail. Consiste en el envío de textos, imágenes, videos, audio, programas, etc., de un usuario a otro por medio de una red. El correo electrónico también puede ser enviado automáticamente a varias direcciones.

Desastre o contingencia: Interrupción de la capacidad de acceso a información y procesamiento de la misma, por medio de equipos de cómputo u otros medios necesarios para la operación normal de un negocio.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Downloads. Descargar, bajar. Transferencia de información desde Internet a una computadora.

Bienes informáticos. Se consideran los siguientes, siendo la Coordinación de Sistemas responsable de su administración.

- Computadores de escritorio y portátiles: conformados por CPU (Discos duros, memorias, procesadores, main board, bus de datos), cables de poder, monitor, teclado, mouse.

- Impresoras, UPS, escáner, lectores, fotocopiadoras, teléfonos, radioteléfonos.

- Equipos de redes comunicaciones como: Switch, Router, Hub, Conversores de fibra y demás equipos de redes y comunicaciones.

Internet. Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.

Intranet. Red privada dentro de una empresa, que utiliza el mismo software y protocolos empleados en la Internet global, pero que solo es de uso interno.

La Entidad: Se refiere a Empresa de Aseo de Pereira S.A. ESP

Megabyte MB. Es bien un millón de bytes ó 1.048.576 bytes.

Políticas: Toda intención y directriz expresada formalmente por la Entidad

Procesos: Se define un proceso como conjunto de actividades que reciben una o más entradas para crear un resultado/producto de valor para el cliente o para la propia empresa.

Red: Se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Puede involucrar otras propiedades como autenticidad, trazabilidad (accountability), no repudio y fiabilidad.

Servidor. Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

SO. (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.

Software. Todos los componentes no físicos de una PC (Programas).

TI: Se refiere a las Tecnologías de Información.

Usuario. Toda persona, funcionario (empleado, contratista, temporal), que utilice los sistemas de información de la empresa debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

UTM. Gestión Unificada de Amenazas (Unified Threat Management). Son dispositivos de red que se encargan de proteger las redes de amenazas y considerados la evolución de un firewall tradicional, ya que incluye productos de seguridad que permiten el desempeño de múltiples funcionalidades de servicios de seguridad en un solo dispositivo, como Firewall, Detección y Prevención de Intrusos, Antivirus y Antispyware de red, VPN, Proxy, Control de Contenido, Balanceo de Cargas, QoS y Reportes

Virus. Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar serios problemas a los sistemas infectados. Al igual que los virus en el mundo animal o vegetal, pueden comportarse de muy diversas maneras. (Ejemplos: caballo de Troya y gusano).

Web Site. Un Web Site es equivalente a tener una oficina virtual o tienda en el Internet. Es un sitio en Internet disponible para ser accesado y consultado por todo navegante en la red pública. Un Web Site es un instrumento avanzado y rápido de la comunicación que facilita el suministro de información de productos o entidades. Un Web Site es también considerado como un conjunto de páginas electrónicas las cuales se pueden accesar a través de Internet.

Políticas Operativas De TI

- Para salvaguardar la información y contar con los datos necesarios para ejecutar y soportar adecuadamente el desarrollo de las actividades, la Coordinación de Sistemas o quien haga sus veces, cuenta con mecanismos de respaldo y monitoreo de la información, tales como:

  - Backups
  - Herramientas tecnológicas para seguimiento y seguridad de las operaciones, tales como antivirus, identificación de conexiones de equipos de cómputo de contratistas y particulares a la red de la entidad, controles de accesos remotos y gestión del acceso de usuarios

- Para garantizar el mejoramiento, continuidad y seguridad en la realización de los procesos que requieren el uso de sistemas de información, la Coordinación de Sistemas o quien haga sus veces valida los requerimientos técnicos y funcionalidad de los mismos, actualiza permanentemente su inventario y el de las licencias de uso de software, adicionalmente, define las acciones de contingencia, en los casos en que se detecte software instalado y no autorizado por la entidad.

- Con el objetivo de mantener condiciones adecuadas de funcionamiento de la plataforma tecnológica e infraestructura de enlace y comunicaciones, la Coordinación de Sistemas o quien haga sus veces:

  - Programa y ejecuta mantenimientos preventivos de tal forma que no afecten la operación de los procesos
  - Cuenta con servicio de Mesa de Ayuda, a través del cual se da soporte oportuno a requerimientos relacionados con TI.
  - Cuenta con respaldo energético a través de UPS
  - Cuenta con un plan de modernización y ajuste tecnológico.
  - Cuenta con niveles de protección y seguridad física en equipos, cableado y centro de datos.
  - Establece y divulga a través de los medios de comunicación disponibles acciones que permiten salvaguardar los activos de la entidad, entre las cuales está el apagado diario de equipos, cuidado de las instalaciones eléctricas y conexiones de red, cuidado físico de equipos.

- Para asegurar una adecuada prestación de los servicios de TI, el proceso ha identificado, documentado y dispuesto a los usuarios, sus procedimientos y ha establecido los registros con los que proporciona evidencia de la conformidad de los mismos.

Políticas y Lineamientos Específicos

1. Sobre los Derechos de Autor, Adquisición de Software y Licencias de Uso

1.1 De Aplicación General
1.2 De Aplicación por Parte del Administrador (Coordinación de Sistemas)
1.3 De Aplicación por Parte del Usuario

1.1. De Aplicación General

1.1.1. En todos los bienes informáticos de la entidad, queda prohibido el uso de software o programas que no cuenten con la licencia correspondiente.

1.1.2. No debe instalarse o utilizarse software o programas de entretenimiento (juegos).

1.1.3. Solamente se permite la reproducción de software o programas como copias de respaldo. Esta actividad la hará el personal de sistemas y queda terminantemente prohibido copiar archivos instaladores de programas en los equipos de cómputo de los usuarios de la Entidad.

1.1.4. Los dispositivos fijos de almacenamiento (Discos duros) de los equipos de cómputo de la Entidad se utilizarán única y exclusivamente para almacenar información de la Institución. Se prohíbe guardar y abrir archivos distintos a los requeridos para la ejecución de actividades pertinentes a las funciones de cada funcionario y/o contratista.

1.1.5. Se prohíbe el almacenamiento de cualquier material protegido por Derechos de Autor (material de audio, video, gráfico, etc.) sin su respectiva licencia.

1.1.6. La inobservancia de estas políticas también puede dar lugar a la aplicación de las sanciones legales y administrativas establecidas en la Ley de Derechos de Autor (Ley 44 de 1993) y derechos conexos.

1.1.7. Los equipos de terceros que sean utilizados al servicio de la Empresa de Aseo de Pereira y sean utilizados al interior de las instalaciones de la Entidad, deberán ser registrados en la Coordinación de Sistemas la primera vez que sean ingresados en la Entidad, y su propietario se hará responsable del licenciamiento del software utilizado en dicho equipo y de los archivos contenidos en el mismo, exonerando de cualquier responsabilidad a la Empresa de Aseo de Pereira de faltas a la Ley de Derechos de Autor (Ley 44 de 1993) y derechos conexos. Si el equipo registrado es reemplazado por otro, se deberá reportar el cambio para su registro.

1.2. De Aplicación por Parte del Administrador (Coordinación de Sistemas)

1.2.1. Llevará el inventario y control de las licencias de software y el medio magnético u óptico en el que se encuentran, adquiridas por la Institución, se responsabilizará de su custodia, considerando licencias individuales en uso, software preinstalado y corporativo.

1.2.2. Revisará y de ser necesario autorizará las solicitudes sobre el uso de software o programas diferentes a los establecidos como estándares.

1.2.3. La instalación del software aprobado, lo realizará solamente el personal autorizado.

1.3. De Aplicación por Parte del Usuario

1.3.1. Quien disponga de bienes informáticos provistos por la Institución, es responsable de controlar que los datos y programas instalados en su equipo, cuenten con la debida autorización.

2. Sobre las Medidas de Seguridad Física

2.1. De Aplicación por Parte del Administrador (Coordinación de Sistemas)

2.1.1. Verificará que las instalaciones físicas donde se ubiquen los bienes informáticos cumplan con las condiciones mínimas de ambientación sugeridas por el fabricante (temperatura, electricidad, humedad, mobiliario, etc.) requeridas para su adecuada conservación y funcionamiento.

2.1.2. Mantendrá los servidores de red y los equipos de comunicaciones como concentradores, enrutadores, firewalls, switches, etc., en cuartos cerrados o en gabinetes con llaves y con restricciones de acceso a personal autorizado, siempre que las instalaciones físicas lo permitan.

2.1.3. Procurará que los accesos de entrada física (puertas, ventanas, paredes de vidrio, ventilación, pared falsa, etc.) existentes en áreas informáticas no estén expuestos a violación accidental o intencional, igualmente los controles físicos limitarán el acceso solo al personal autorizado, siempre que las instalaciones físicas lo permitan.

2.1.4. Procurará la mejor ubicación del Centro de Cómputo y del resguardo de la información procesada, en lugares donde el riesgo de daños sea mínimo o esté

controlado. El acceso será restringido al personal autorizado y de requerirse excepciones éstas serán debidamente autorizadas por el Administrador.

2.1.5. Vigilará las características de la instalación eléctrica del Centro de Cómputo y áreas informáticas, verificando que cumplan con lo recomendado para este tipo de instalaciones. Cualquier inconformidad con las condiciones encontradas deberá ser notificada a instancias superiores para su gestión.

3. Sobre los Bienes Informáticos**.**

3.1 De Aplicación General
3.2 De Aplicación por Parte del Administrador (Coordinación de Sistemas)
3.3 De Aplicación por Parte del Usuario

3.1. De Aplicación General

3.1.1. Toda instalación de bienes informáticos (hardware o software), reconfiguración de los mismos, o de accesorios (DVD-ROM, escáner, drivers, impresoras, etc.) que no forman parte de la configuración original, debe ser autorizado por el administrador de bienes informáticos quién a su vez llevará el control de dichas modificaciones. La instalación la realizará únicamente personal autorizado.

3.1.2. Cuando se quiera instalar accesorios o bienes informáticos (hardware o software) que pertenezcan al usuario, éste deberá solicitar autorización al Administrador de Bienes Informáticos e indicar el objetivo y la duración de la misma. También en este caso, la instalación la realizará personal autorizado.

3.1.3. La Subgerencia Administrativa y Financiera será la responsable del mantenimiento preventivo y correctivo de los recursos informáticos de la institución

3.2. De Aplicación por Parte del Administrador (Coordinación de Sistemas)

3.2.1. Asesorará a la Empresa en la renovación o actualización de la infraestructura informática institucional considerando tanto los requerimientos actuales y futuros de la institución, como la tecnología disponible en el mercado. El reemplazo o actualización de los bienes informáticos será evaluado en función del análisis de costo/beneficio, que asegure la mejor relación en economía, eficacia y eficiencia. El tiempo máximo para la reposición de equipos será de cinco (5) años, dependiendo del uso dado de los mismos, el estado y las necesidades del servicio.

3.2.2. Evaluará las solicitudes y recomendará, a quien corresponda, la provisión de bienes y servicios informáticos necesarios para suplir los requerimientos de automatización de las distintas áreas de la entidad.

3.2.3. Notificará a la Oficina de Recursos sobre todos los bienes informáticos de la Institución, para ser incluidos en el inventario de la entidad y para que sean cubiertos por las pólizas de seguros que amparan los bienes de la empresa.

3.2.4. Verificará que los equipos tengan instalada la última versión de software antivirus que la Institución tenga amparada con la licencia correspondiente.

3.3. De Aplicación por Parte del Usuario

3.3.1. El usuario a quién se le ha asignado bienes informáticos, será responsable por éstos y deberá informar inmediatamente al Administrador y a la Oficina de Recursos sobre cualquier inconveniente que se presente, en especial si algún bien ha sido sustraído o reporta fallas de funcionamiento.

3.3.2. Mantendrá el bien informático en un entorno adecuado, asegurándose que el bien informático no corra riesgos físicos.

3.3.3. Se asegurará de la adecuada alimentación eléctrica al bien informático. Para esto, deberá cerciorarse que los equipos de cómputo estén conectados a la fuente de energía regulada (tomas naranjas) en los sitios que se disponga de ella.

3.3.4. Cuando abandone el área de trabajo, previamente deberá finalizar todos los procesos de sistemas de información, bases de datos, así como el servicio de red y de ser necesario apagará el equipo.

3.3.5. Bajo ninguna circunstancia intentará por sí mismo, la reparación de cualquier equipo o componente de éste.

3.3.6. Revisará que se active la rutina de verificación del software antivirus autorizado por la entidad, cuando se pretenda ingresar información por los medios de almacenamiento externo o de los servicios de Internet.

3.3.7. Procurará la optimización en el uso de los insumos y materiales requeridos para los bienes informáticos a su cargo.

4. Sobre la Seguridad Lógica y Confidencialidad de la Información**.**

4.1 De Aplicación General
4.2 De Aplicación por Parte del Administrador (Coordinación de Sistemas)
4.3 De Aplicación por Parte del Usuario

4.1. De Aplicación General

4.1.1. Las Bases de Datos de la Entidad que deban ser revisadas por personal externo para su evaluación, modificación, recuperación de información o actualización, con el fin de dar solución a alguna dificultad con el uso de las mismas detectada o como adaptación a funcionalidades nuevas en las aplicaciones que trabajan con ellas, se hará en acompañamiento con personal adscrito a la Coordinación de Sistemas, cuando se haga de manera presencial, quien verificará los resultados en la actividad. Al finalizar las tareas pertinentes sobre las bases de datos se hará un registro escrito como evidencia. Si el acceso por parte del contratista se hace de manera remota, el personal de sistemas deberá habilitar previamente el acceso remoto con las herramientas existentes para ello (Escritorio remoto, VPN u otra que se tenga a disposición). En cualquiera de los casos, se hará una copia de seguridad previa para garantizar que se pueda devolver el sistema a su estado inicial.

4.1.2. El usuario acepta que la Empresa de Aseo de Pereira S.A. E.S.P. no está en capacidad de protegerle de ataques o mensajes ofensivos que le pudieren llegar a través de la red de comunicaciones. Por tanto, la Entidad no asume ningún tipo de responsabilidad en este sentido.

4.2. De Aplicación por Parte del Administrador (Coordinación de Sistemas)

4.2.1. La Coordinación de Sistemas y la Asesoría de Control Interno, podrá hacer auditorías aleatorias en cualquiera de los recursos informáticos puestos a disposición de los usuarios internos, para verificar el buen uso de los mismos.

4.2.2. En los casos que se detecten acciones que puedan poner en riesgo la seguridad o los niveles de eficiencia, tanto de la red de datos institucional como de cualquiera de los componentes de la misma, el administrador podrá realizar una auditoría y emitir recomendaciones para prevenir o corregir estas situaciones.

4.2.3. Procurará la creación de copias de seguridad de manera permanente y periódica, a la información que se maneje de manera centralizada (sistemas de información centralizados).

4.2.4. Asesorará a los usuarios en la realización de copias de seguridad de su propia información, usando las herramientas de que disponga la Entidad.

4.3. De Aplicación por Parte del Usuario

4.3.1. Deberá mantener el respaldo de la información requerida para su trabajo, incluyendo en ello, el respaldo de los mensajes de correo electrónico que requiera conservar. La Coordinación de Sistemas no se responsabiliza por la información almacenada en cada uno de los equipos.

4.3.2. Los usuarios velarán por la salvaguarda de las contraseñas asignadas para el ingreso a las distintas aplicaciones y/o servicios electrónicos. El usuario se hará responsable por todas y cada una de las acciones que se hagan con su usuario en los sistemas de información de la Institución.

4.3.3. Los usuarios tendrán derecho a la confidencialidad de su información, con la salvedad de aquellos casos en que se detecten acciones que pongan en riesgo la seguridad tanto de la red de datos institucional como de cualquier otra red, así como para responder ante quejas sobre contenidos que violen los derechos de terceras personas.

4.3.4. Los usuarios deberán cerrar las aplicaciones informáticas a las cuales tienen acceso en caso de ausentarse temporalmente, para evitar que otras personas puedan manipular de una u otra manera la información allí manejada con el usuario que tiene abierta la sesión, asumiendo la responsabilidad el funcionario dueño de la cuenta de lo que de esta manera pueda suceder.

4.3.5. Todos los documentos creados e información generada en los sistemas de información y bienes informáticos de la Institución, son propiedad de la Empresa de Aseo de Pereira S.A. E.S.P., y por lo tanto se prohíbe el borrado de ellos sin la autorización pertinente del Jefe inmediato.

4.3.6. No está permitido obtener copias intencionales de archivos, códigos, contraseñas o información ajena para ser entregada a terceros sin la debida autorización, ni suplantar a otra persona en una conexión que no le pertenece o enviar información a nombre de otra persona sin consentimiento del titular de la cuenta.

4.3.7. Ningún usuario podrá adelantar acciones orientadas a infiltrarse, dañar o atacar la seguridad informática de la Empresa, a través de medio físico o electrónico alguno.

4.3.8. No se debe entorpecer por ningún medio el funcionamiento de los sistemas de información y telecomunicaciones de la Entidad.

5. Sobre el Uso de los Servicios de Información y la Red de Datos Institucional.

5.1 De Aplicación General
5.2 De Aplicación por Parte del Administrador (Coordinación de Sistemas)
5.3 De aplicación por parte del usuario

5.1. De Aplicación General

5.1.1. Todo funcionario que para el desempeño de sus funciones requiera utilizar servicios de información institucionales, deberá poseer una cuenta de usuario, la cual se creará con los permisos, privilegios y restricciones correspondientes según su perfil y necesidades, previa solicitud del jefe inmediato o interventor, la cual se hará de manera escrita, ya sea por medio físico o utilizando las herramientas informáticas que para ello se dispongan en la Entidad y siguiendo los procedimientos que existan para ello.

5.1.2 Cuando un usuario se retira de la Entidad y este tiene por lo menos una cuenta de usuario en alguno de los sistemas de información, el jefe inmediato o interventor deberá informar a la Coordinación de Sistemas para su desactivación mediante el mismo procedimiento mencionado en el literal anterior.

5.1.3. Las cuentas de usuario son individuales e intransferibles y su dueño será responsable de mantener la confidencialidad de las contraseñas de las cuentas, de hacer uso adecuado de las cuentas y de responder por todas las actividades que se realicen con ellas.

5.2. De Aplicación por Parte del Administrador (Coordinación de Sistemas)

5.2.1. Administrará los servicios en la red de datos institucional de manera exclusiva, con el personal del área responsable de los mismos y, en los casos necesarios, con la participación de los proveedores autorizados.

5.2.2. Administrará las cuentas de usuarios de acuerdo a las solicitudes hechas por las distintas áreas.

5.2.3. Mantendrá control sobre el acceso de usuarios a los elementos (físicos y lógicos) de administración de la red de datos institucional.

5.2.4. Vigilará que la infraestructura de la red sea utilizada únicamente en actividades relacionadas con los objetivos institucionales.

5.2.5. Mantendrá información actualizada y disponible sobre el alcance y servicios de la red de datos institucional.

5.2.6. Se asegurará del buen estado de la infraestructura de la red así como del cumplimiento de las normas recomendadas para este tipo de instalaciones.

5.2.7. Ofrecerá los medios y mecanismos para que los usuarios obtengan productos y servicios informáticos de calidad, con los niveles de seguridad adecuados y favoreciendo el máximo aprovechamiento de los recursos informáticos y de comunicaciones disponibles.

5.2.8. Administrará y monitoreará las actividades de red mediante el UTM (Gestión unificadas de amenazas) que se dispone en la Empresa.

5.3. De aplicación por parte del usuario

5.3.1. Hará buen uso del acceso a los recursos y servicios informáticos de acuerdo a las disposiciones y reglamentaciones que para estos fines existan.

5.3.2. Solo podrá utilizar la infraestructura de la red de datos institucional para aquellos servicios que se le haya concedido acceso y únicamente para el desarrollo de actividades relacionadas con su función.

5.3.3. No utilizará los recursos de la red de datos institucional, para anunciar, enviar por correo electrónico o por cualquier otro medio de transmisión electrónica, contenidos ilegales o confidenciales, anuncios no autorizados, materiales promocionales y mensajes que contengan virus que pongan en riesgo los bienes informáticos y datos institucionales o de terceros.

5.3.4. Comprenderá que cualquier material y/o datos descargados de redes externas o de otra manera, sin contar con las protecciones recomendadas, es riesgo para él y la Institución, y que será exclusivamente responsable de cualquier daño al sistema o pérdida de datos que pueda resultar de recibir tal material y/o datos.

6. Sobre Conexión a Otras Redes**.**

6.1 De Aplicación por Parte del Administrador (Coordinación de Sistemas)

6.2 De Aplicación por Parte del Usuario

6.1. De Aplicación por Parte del Administrador (Coordinación de Sistemas)

6.1.1. Velará porque las conexiones entre la red de datos institucional con redes externas, se realicen de la manera más segura posible, de acuerdo a los recursos disponibles en la empresa, para lo cual cada entidad involucrará el equipamiento y los mecanismos de control de acceso que se consideren necesarios.

6.2. De Aplicación por Parte del Usuario

6.2.1. Los usuarios serán responsables de todas las actividades que realicen en redes externas (incluye Internet) desde la red institucional, asumiendo las penalizaciones a que haya lugar, por hacer uso inapropiado de ellas.

7. Sobre la implementación de Herramientas y Otros Servicios Informáticos**.**

7.1 De aplicación General
7.2 De Aplicación por Parte del Administrador (Coordinación de Sistemas)
7.3 De Aplicación por Parte del Usuario.

7.1. De Aplicación General

7.1.1. Toda implementación de herramientas informáticas (hardware o software) deberá ser liderada por el área que se verá afectada y/o la utilizará, desde la definición de necesidades, requerimientos y alcance de la herramienta, hasta el soporte a nivel de usuario en el manejo y definición de parámetros.

7.1.2. Los servicios informáticos (soporte, desarrollo de sistemas informáticos, asesorías, consultorías, mantenimiento, capacitación, etc.) se brindarán en función de los recursos disponibles y de las prioridades establecidas.

7.1.3 Toda implementación de herramientas informáticas deberán contar con el concepto técnico de la Coordinación de Sistemas sobre la viabilidad técnica y la compatibilidad con los demás sistemas implementados en la Entidad.

7.2. De Aplicación por Parte del Administrador (Coordinación de Sistemas)

7.2.1. Prestará todo el apoyo técnico necesario en el área informática, para llevar a cabo las implementaciones que ejecuten las demás áreas de la Institución.

7.2.2. Brindará los servicios informáticos a la Institución y a las entidades que lo solicitaren, procurando el máximo nivel de calidad, eficacia y eficiencia.

7.3 De Aplicación por Parte del Usuario.

7.3.1 Participará activamente en todas y cada una de las etapas del proceso de implementación de herramientas y/o servicios informáticos.

7.3.2 Se responsabilizará del contenido y actualización de los datos que sean requeridos para los sistemas o servicios informáticos que le sean provistos.

8. Sobre la protección eléctrica**.**

8.1. De Aplicación General

8.1.1. La Empresa de Aseo de Pereira S.A. E.S.P. procurará que el cableado eléctrico regulado sea alimentado por Sistemas de Potencia Ininterrumpida (UPS). Solo los equipos de cómputo (CPU y monitor) deben ir conectados en la red regulada (tomas naranjas). Otros dispositivos como impresoras, cargadores, radios, ventiladores, etc., deben ir conectados a la red no regulada (tomas blancas), ya que las UPS pueden sufrir graves daños por sobrecargas de potencia.

8.2. De Aplicación por Parte del Administrador (Coordinación de Sistemas)

8.2.1. Procurará la existencia de un soporte técnico de mantenimiento preventivo y correctivo de las UPS para evitar la carencia del servicio de estos dispositivos por tiempos prolongados.

9. Sobre el Correo Electrónico Institucional

9.1 De Aplicación General

9.1.1 El correo electrónico es un privilegio y se debe utilizar de forma responsable. Su principal propósito es servir como herramienta para agilizar las comunicaciones oficiales que apoyen la gestión institucional de la empresa.

9.1.2 El correo electrónico es un instrumento de comunicación de la empresa y los usuarios tienen la responsabilidad de utilizarla de forma eficiente, eficaz, ética y de acuerdo con la ley, por lo que NO está permitido utilizar el correo institucional con fines políticos, religiosos, sentimentales, comerciales, juegos, ni ninguna clase de actividad mercantil.

9.1.3 El uso del mail es personal y sus claves confidenciales. Por ningún concepto se puede entrar a revisar la información dirigida a otra persona.

9.1.4 La persona que envía el mail es responsable del contenido del mismo, debiendo considerar que la información enviada es irreversible.

9.2 De Aplicación por parte del usuario

9.2.1 El usuario hará buen uso del espacio de almacenamiento asignado para su cuenta de correo, por lo cual velará porque siempre haya espacio disponible en el buzón para recibir nuevos correos. Para esta tarea el usuario deberá almacenar de manera digital los mensajes que considere necesarios para su conservación. La Coordinación de Sistemas no hará respaldo de la información contenida en los buzones de correo.

Elaboró: Orlando Zapata Álvarez
Ing. De Sistemas

Última revisión:

Pereira, 25 de agosto de 2017