PROCESO: Gestión Administrativa

OBJETIVO: Establecer los lineamientos en Políticas de Seguridad tecnológica de Información y de Comunicaciones, permitiendo aplicar las condiciones de uso de los equipos de cómputo (Hardware) y los programas utilizados (Software) pertenecientes al Diagnosticentro S.A.S.

ALCANCE: Es aplicable a todos los empleados y contratistas (usuarios) del CDAR que utilicen equipos de cómputo o dispositivos con acceso a la red interna y/o acceso a internet.

DEFINICIONES

SOFTWARE: Equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas

HARDWARE: Todas las partes físicas de un sistema informático.

COPIA DE SEGURIDAD: Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos o CD`s), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto.

RECUPERACIÓN: Hace referencia a las técnicas empleadas para recuperar archivos a partir de una copia de seguridad (medio externo); esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers.

RESTAURACIÓN: Volver a poner algo en el estado inicial. Una Base de Datos se restaura en otro dispositivo después de un desastre.

GENERALIDADES: Los usuarios del CDAR deben seguir con exactitud las presentes políticas emitidas por la Dirección Financiera Administrativa quien es la encarga de administrar estas políticas a través del contratista de sistemas.

Los usuarios que son clientes y/o visitantes y que hacen uso de la red inalámbrica disponible para ellos, lo harán bajo su propia responsabilidad. El Diagnosticentro S.A.S. no se hace responsable por el contenido, software, aplicaciones e información entre otros, descargado, subido o compartido a través de ésta red.
Este documento integra los aspectos que se relacionan a continuación:

- Políticas para el uso adecuado de las Tecnologías de la Información y las Comunicaciones
- Políticas de contraseñas
- políticas de uso de internet, correo electrónico y administración de la página web
- Políticas para el uso de Software
- Política Institucional
- políticas de administración de acceso de usuarios del servidor en el proceso diagnóstico automotor
- Políticas para el respaldo de la información

- Políticas de mantenimiento de software y Hardware

Estas políticas tienen como propósito proteger y respaldar la información de los empleados, los contratistas y de la entidad; además de propiciar el aumento de la seguridad y el aprovechamiento de la actual tecnología, la cual contribuirá a aumentar la eficiencia en el trabajo y garantizar la continuidad de las operaciones de la empresa.

1. POLÍTICA PARA EL USO ADECUADO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

1.1. Generales

1.1.1. Bajo ninguna circunstancia los usuarios del CDAR, pueden utilizar los recursos informáticos para realizar actividades no permitidas por las normas establecidas o por normas jurídicas nacionales o internacionales.

1.1.2. Para los equipos propiedad del CDAR, la Dirección Financiera Administrativa y Director Técnico son los únicos autorizados para realizar actividades de soporte técnico y cambios de configuración en los equipos de cómputo a través del contratista de sistemas. En el caso de labores de mantenimiento realizadas por terceros, éstas deben estar en conocimiento y aprobadas por la Dirección Financiera Administrativa y de quien haga las veces de interventor del contrato. Para los equipos de cómputo en arrendamiento, la empresa arrendadora es la única responsable y autorizada a realizar labores de mantenimiento, cambio y actualización de hardware o software o en su caso autorizar dichas labores.

1.2. Equipos de Cómputo

1.1.1. El equipo de cómputo, propiedad del CDAR o arrendado, deberá ser utilizado únicamente para actividades relacionadas con los objetivos y metas de la empresa.

1.1.2. La Dirección Financiera Administrativa implementará las acciones y actividades preventivas necesarias para el correcto funcionamiento de los equipos de cómputo.

1.1.3. El Contratista de Sistemas es responsable de la asignación, funcionamiento y distribución de los equipos de cómputo.

1.1.4. La contratación de equipos, materiales y/o servicios relacionados con las TIC, se realizará con base en los fundamentos jurídicos de la contratación de acuerdo a *El Manual de Contratación del CDAR, Resolución 070 de Octubre 06 de 2017, modificada por la resolución 089 de 31 de octubre de 2017*.

1.1.5. Para conectar un equipo portátil, de escritorio o dispositivo móvil (teléfono, celular inteligente, tableta digital, etc.) al equipo o computador perteneciente a la red institucional, que no esté bajo el control administrativo del CDAR (equipos y dispositivos privados de los usuarios del CDAR, computadoras de otras empresas o terceros en general, las cuales no están sujetas a la totalidad de las políticas de seguridad de CDAR y por ende constituyen un riesgo al ser conectadas a la red institucional), se deberá solicitar permiso a la Dirección Financiera Administrativa o Dirección Operativa para que, a través del contratista de sistemas, inspeccione el equipo, compruebe que no constituye un riesgo para la seguridad para la empresa y en tal caso de la autorización.

1.1.6. De presentarse algún incidente (pérdida, robo, daño físico o virtual, etc.) que afecte de manera directa a un equipo de cómputo del CDAR, deberá ser informado a la menor brevedad al Contratista de Sistemas.

1.1.7. Sólo el Contratista de Sistemas está facultado para destapar las computadoras portátiles o cualquier otro equipo de cómputo propiedad del CDAR. Para los equipos de cómputo en arrendamiento, la empresa arrendadora es la única autorizada para destapar los equipos o en su caso autorizar la apertura de ellos.

1.1.8. Todos los equipos de cómputo del CDAR, deben contar con un software antivirus actualizado y un firewall administrado por el contratista de sistemas, con el objetivo de proteger el equipo y su contenido de programas maliciosos.

1.1.9. Los equipos y dispositivos electrónicos ubicados en los pisos bajos de las instalaciones del CDAR deben estar ubicados a una altura de alrededor de 70 cm sobre el nivel del suelo, con el fin de evitar daños en posibles inundaciones.

1.2. Centro de Cómputo

1.2.1. En el Centro de Cómputo del CDAR se alojan los servidores y equipos de comunicación necesarios para la operación de las actividades informáticas de la Institución.

1.2.2. El acceso a los centros de cómputo y los equipos contenidos en él, es restringido y sólo personal autorizado por el Director Técnico o el Director Financiero Administrativo pueden tener acceso a él.

1.2.3. El acceso a los servidores del CDAR, ya sea usando la consola de administración local o una consola de administración remota es restringido a todo el personal. El intento de conexión por alguna persona no autorizada a cualquier consola de administración de los servidores se considera una violación de las políticas de seguridad.

1.3. Propiedad de la Información

1.3.1. Los datos que los usuarios crean y manipulan en los sistemas, aplicaciones y cualquier medio de procesamiento electrónico, durante el desarrollo normal de sus actividades laborales, son propiedad y responsabilidad del CDAR.

1.3.2. Los derechos patrimoniales de un programa de computación, hojas de cálculo (excel), archivos realizados en procesadores de texto (word), presentaciones (power point), macros, y otros documentos locales o en línea, creados por uno o varios usuarios en el ejercicio de sus actividades laborales, corresponden al CDAR.

1.4. Actividades No Permitidas

Las siguientes actividades no están permitidas a los usuarios del CDAR:

1.4.1. Violar los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual, así como archivos multimedia de cualquier tipo (música y video) que no sean de la autoría del usuario.

1.4.2. Distribución o instalación de software sin la licencia de uso adecuado previamente adquirida por el CDAR.

1.4.3. Difundir información identificada como privada o confidencial a través de medios que involucren el uso de tecnologías de información, entre ellas correo electrónico, discos extraíbles, unidades flash (USB).

1.4.4. Introducir software malicioso en la red o en los servidores (virus, worms, ráfagas de correo electrónico no solicitado, entre otros.)

1.4.5. Utilizar la infraestructura tecnológica del CDAR para conseguir o transmitir material con ánimo de lucro

1.4.6. Se prohíbe el uso del sistema de comunicaciones del CDAR con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.

1.4.7. Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios del CDAR.

1.4.8. Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.

1.4.9. Monitorear puertos o realizar análisis del tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad. El contratista de sistemas, responsable de la Seguridad Informática puede realizar estas actividades siempre y cuando tenga la autorización por parte del interventor del contrato.

1.4.10. Ejecutar cualquier herramienta o mecanismo de monitoreo de la red de manera no autorizada.

1.4.11. Burlar mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.

1.4.12. Interferir o negar el servicio a usuarios autorizados con el propósito de lesionar la prestación del servicio o la imagen del CDAR (ejemplo: ataques DoS).

1.4.13. Uso de comandos o programas para el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).

1.4.14. Instalar cualquier tipo de software en los equipos de cómputo de CDAR sin la previa autorización de la Dirección Financiera Administrativa o Dirección Técnica, incluyendo software de dispositivos móviles y teléfonos celulares.

1.4.15. Modificar la configuración del software antivirus, firewall o políticas de seguridad en general implantadas en los equipos de cómputo del CDAR sin consultar previamente con la Dirección Financiera Administrativa o Dirección Técnica, siendo analizada la viabilidad de los cambios solicitados.

1.4.16. Queda estrictamente restringido compartir una carpeta con derecho a todos los usuarios. El contratista de sistemas puede cambiar permisos de recursos compartidos por los usuarios si detecta que éstos no cumplen con las mejores prácticas definidas en los lineamientos internos de seguridad.

1.4.17. Reproducir música de cualquier formato que no esté ubicada en el disco duro de la PC del usuario o en CD. No se permite la reproducción de archivos de música si éstos están ubicados en un recurso compartido de la red privada del CDAR o en cualquier URL de Internet (aplicable para los usuarios que hacen uso del servicio de Internet).

1.4.18. Descargar archivos de multimedia desde Internet.

1.4.19. Reproducir archivos multimedia (música y videos) desde internet

1.4.20. Ver, reproducir, compartir, divulgar, promover o cualquier otra actividad o contenido explícito relacionada con niños, niñas y adolescentes, que vulneren cualquiera de sus derechos.

1.4.21. Acceder a redes sociales o portales P2P.

1.5. Excepciones

Para propósitos de mantenimiento de la red y de seguridad, algunos usuarios del CDAR, pueden estar exentos de seguir algunas de las restricciones anteriores, debido a las necesidades y responsabilidades de su cargo o a eventos programados.

Estas excepciones deben ser solicitadas al Contratista de Sistemas, previa autorización del Director Financiero Administrativo o Director Técnico.

2. POLÍTICAS DE CONTRASEÑAS

2.1. Generales

2.1.1. Todos los usuarios del CDAR requieren de un nombre de usuario y una contraseña para utilizar el equipo de cómputo que tiene asignado y los servicios de red como correo electrónico, impresión, unidades de red, unidades físicas, archivos compartidos y acceso a Internet. La solicitud deberá realizarse a través del correo electrónico sistemas@diagnosticentrorda.com al Contratista de Sistemas.

2.1.2. El software especializado o sistema de información de la revisión Técnico mecánica y de emisiones contaminantes debe contar con protección para el acceso al mismo mediante el uso de contraseñas. Este sistema solicita automáticamente el cambio de contraseña cada 30 días para el personal de pista, en el caso de la Dirección Técnica e ingeniero/a suplente este cambio debe realizarse en un tiempo no mayor a 20 días, los usuarios autorizados deben realizar este cambio para poder seguir ejecutando tareas dentro de dicho sistema de información. Este control se debe llevar en el "Formato Control de Contraseñas" Para el uso de estas contraseñas se debe seguir el requerimiento consignado en el numeral 4.16.2.1 de la NTC 5385.

2.1.3. Todas las contraseñas de los usuarios deben cumplir con ciertos requerimientos de seguridad con el objetivo de evitar que los usuarios elijan contraseñas débiles. Estos requerimientos de seguridad son:

- Mínimo de ocho (8) caracteres alfanuméricos y especiales
- No contener el nombre del funcionario o familiares
- Las contraseñas son personales y conocidas únicamente por el propio usuario el cual será responsable de toda la actividad que se realice con ella.
- Por seguridad, las contraseñas se cambian cada dos meses por el propio usuario.
- El Contratista de Sistemas se reserva el derecho de restablecer en cualquier momento la contraseña de cualquiera de los usuarios del CDAR, con previo aviso para no afectar de ninguna manera la continuidad de sus funciones, si se detecta que ha sido comprometida.
- Todas las demás consignadas en el numeral 4.16.2.1 de la NTC 5385.

3. POLÍTICAS DE USO DE INTERNET, CORREO ELECTRÓNICO Y ADMINISTRACIÓN DE LA PÁGINA WEB

3.1. Administración

Los servicios de acceso a internet y correo electrónico son administrados por el Contratista de Sistemas, quien tomará los reportes de los problemas técnicos y fallas del sistema para su posible atención inmediata. Sin embargo, el proveedor del enlace a Internet es responsable de garantizar la disponibilidad de la conexión, así como de los anchos de banda contratados. El Contratista de Sistemas está facultado para monitorear periódicamente las actividades de cada uno de los usuarios de internet y comunicación por la Red de Datos del CDAR, con la finalidad de vigilar el cumplimiento de las políticas del presente documento, manteniendo la confidencialidad de la información.

3.2. Correo Electrónico

3.2.1. La comunicación institucional realizada por correo electrónico, solo será a través de las cuentas corporativas asignadas (usuario@diagnosticentrorda.com) salvo nuevas cuentas necesarias de crear a través del correo de gmail (usuario@gmail.com).

3.2.2. El correo electrónico es correspondencia privada entre el emisor y el destinatario, por lo tanto, no podrá trasmitirse a través de internet Información considerada como de uso confidencial hacia personal externo del CDAR, salvo instrucción expresa de la Gerencia, del Director Financiero Administrativo y/o por necesidad inherente del cargo y sus funciones.

3.2.3. Cada usuario es responsable del contenido prohibido o sensible de los mensajes enviados, esto incluye entre otros: contenido de material ofensivo, obsceno, contenido infantil sensible, cualquier quebrantamiento de propiedad intelectual, copyright o cualquier información ilegal o criminal.

3.2.4. No está permitida la transmisión de mensajes que puedan crear un medio hostil sobre la raza, edad, sexo, religión, política, nacionalidad, origen, incapacidad u orientaciones personales; comentarios despectivos, noticias informales o mal intencionadas, cadenas de cartas, mensajes masivos de índole personal, y en general cualquier tipo de información que cause congestión en la red o interfiera con el trabajo de otros funcionarios y/o contratistas.

3.2.5. El Contratista de Sistemas establecerá límites para los correos electrónicos que se envíen hacia internet o reciban desde internet de acuerdo a las necesidades de las diferentes áreas y usuarios con el objetivo de evitar el congestionamiento del enlace a internet y por lo tanto la afectación a otros servicios que también se ofrecen utilizando este medio de comunicación.

3.3. Internet

3.3.1. Los empleados y contratistas son responsables de mantener su imagen profesional durante la navegación en internet, así como proteger la imagen y reputación del CDAR.

3.3.2. Ningún usuario tiene acceso a internet de manera automática al conectarse a la Red del CDAR. El usuario para poder ingresar a internet desde otro dispositivo debe solicitarlo a la Dirección Financiera Administrativa o Dirección Técnica, el Contratista de Sistemas, en caso de ser aprobada la solicitud realizará la configuración necesaria en el equipo del usuario y le asignará los privilegios necesarios para el uso del servicio de acuerdo a las actividades que serán desempeñadas.

3.3.3. Los usuarios con equipo externo al CDAR que necesiten conexión a internet y deseen utilizarlo mediante los recursos de conexión destinados para dicho fin, podrán solicitarlo al Contratista de Sistemas para su aprobación y configuración.

3.3.4. No se debe utilizar el acceso a Internet como un medio de participación, acceso y distribución de actividades o materiales que vayan en contra de la Ley.

3.3.5. No acceder, ver o descargar desde sitios de internet: Gráficos, videos, imágenes o cualquier otro material audiovisual que pueda ser percibido como sensible, obsceno, abusivo o que contenga humor inapropiado, lenguaje amenazante, acosante u otra forma de lenguaje objetable dirigido a un individuo o grupo como tampoco material infantil.

3.4. Seguridad

3.4.1. El Contratista de Sistemas es responsable de configurar a los usuarios el servicio correspondiente.

3.4.2. Las cuentas y claves de acceso de los servicios de internet y correo electrónico son personales y confidenciales y se rigen por las políticas de contraseñas definidas en el presente documento.

3.4.3. El usuario notificará inmediatamente al Contratista de Sistemas cualquier uso no autorizado de su cuenta o posible intrusión de seguridad conocida o sospechosa.

3.4.4. El usuario tiene la obligación de usar los servicios con fines institucionales.

3.4.5. Se prohíbe el acceso, descarga o transmisión de material cuyo origen no sea constatado como seguro o de aquél que se desconozca su confiabilidad.

3.4.6. Cualquier archivo o programa obtenido a través de internet o correo electrónico debe revisarse con el software antivirus adquirido por el CDAR.

3.4.7. El usuario tiene la obligación de realizar las descargas habituales del correo electrónico, para evitar que los buzones se saturen, ya que el espacio en el servidor de correo es limitado; siempre y cuando el servicio de correo esté alojado en el servidor del CDAR.

3.4.8. No deberá utilizarse el correo electrónico en suscripciones a listas que saturen la capacidad de almacenamiento de la bandeja de entrada.

3.5. Almacenamiento

3.5.1. El total de la información creada, obtenida o descargada de cualquiera de los servicios deberá ser almacena localmente en el equipo de cómputo del usuario y específicamente en la carpeta “Mis Documentos” no debiendo ser distribuida o transmitida por la red institucional como tampoco en otras carpetas compartidas de la red; salvo sea necesario, se realizará en la carpeta “Pública” destinada para ello.

3.5.2. El área de almacenamiento “Publica” en la red será tratada como de almacenamientos temporales. El Contratista de Sistemas revisará el óptimo aprovechamiento de los recursos compartidos para mantener la

integridad y asegurar que los usuarios utilicen éstos recursos de manera responsable.

3.6. Propiedad y Derechos de Contenidos

3.6.1. La información disponible en internet, incluyendo imágenes, textos, software, música, sonido, fotografía, video, gráficos u otro material contenido, está protegida por derechos de autor, marcas registradas, patentes u otros derechos de propiedad intelectual y leyes. Sólo se permite el uso de este material bajo autorización expresa del autor.

3.6.2. El descargar, cargar, archivar, copiar, imprimir, compartir o enviar cualquier material antes mencionado, debe ser realizado solamente bajo la autorización del autor.

3.6.3. Los usuarios no deben descargar ni instalar ningún tipo de software comercial, opensource, shareware, freeware, apps pagas o gratuitas, controladores de dispositivos externos en las unidades de disco, unidades externas o en cualquier unidad del equipo de cómputo, sin la autorización correspondiente.

3.7. Conducta del Usuario

3.7.1. El usuario es el único responsable del contenido de transmisiones a través de cualquier servicio.

3.7.2. El usuario debe cumplir con las leyes de transmisión de datos técnicos de los países desde los cuales y hacia donde se envían los mensajes de correo electrónico.

3.7.3. El usuario no debe usar el servicio para propósitos ilegales o de entretenimiento.

3.7.4. El usuario debe cumplir con todas las regulaciones, políticas y procedimientos de internet.

3.7.5. La comunicación de los usuarios se debe conducir con respeto y consideración, evitando los abusos y el uso del lenguaje inapropiado.

3.7.6. Se prohíbe el acceso a cualquier fuente de información cuyo contenido no se encuentre relacionado con las actividades del Diagnosticentro S.A.S. o con las actividades del funcionario o contratista.

3.8. Administración y contenido de la página web

La administración de la página web será ejercida por el contratista de sistemas bajo la supervisión del Director Financiero Administrativo

3.8.1. Responsabilidades del administrador del sitio web

- Administrar en contenido publicado en el sitio web
- Actualizar los precios de los servicios o productos ofrecidos por el CDAR
- Publicar y actualizar en la página los contenidos solicitados por los jefes de proceso y representante legal.
- Verificar la disponibilidad de la página en el momento que sea solicitada.
- Verificar la veracidad del contenido publicado en el sitio web.

3.8.2. Actividades NO permitidas

Las siguientes acciones no están permitidas:

- La promoción y/o publicidad de servicios que puedan afectar la imparcialidad del organismo de inspección del Diagnosticentro S.A.S.
- Publicar contenido sin autorización previa del supervisor del contrato

- Publicar contenido que pueda afectar a terceros.
- Publicar contenido explícito o con lenguaje ofensivo.

4. POLÍTICAS DE USO DE SOFTWARE

4.1. Políticas de Administración

El Contratista de Sistemas, bajo la supervisión del interventor del contrato, es el único autorizado para llevar a cabo la administración del software del CDAR, por lo que dentro de sus responsabilidades tiene:

- Mantener bajo resguardo las licencias de uso de software.
- Llevar un control exacto de las licencias en operación y el equipo en el cual se encuentra en uso.
- Establecer políticas y lineamientos para el uso de software, previa aprobación por parte del Gerente y/o el Director Financiero Administrativo.
- Organizar la inspección de los equipos de cómputo en intervalos regulares.
- Difundir a los usuarios las Políticas de Uso de Software con el fin de que conozcan la normatividad.

4.2. Políticas de Instalación

4.2.1. Instalación y Soporte: El contratista de Sistemas es la única persona autorizada y responsable de realizar la instalación del software y proporcionar soporte del mismo en todos los equipos de cómputo del CDAR (propios y en arrendamiento).

Esta responsabilidad abarca equipos de cómputo:

- de Escritorio (propiedad del CDAR y arrendados).
- portátiles (propiedad del CDAR y arrendados).
- ubicados en otras dependencias.
- de propiedad personal de los usuarios del CDAR.

El Contratista de Sistemas se compromete a instalar y proporcionar soporte sobre el software o, en su caso, guiar el proceso de instalación, con el fin de dejarlo operando en las mejores condiciones.

4.3. Software Institucional

De acuerdo con las disponibilidades existentes de software se fijará un estándar para ser utilizado por las áreas usuarias. Todo equipo de cómputo antes de ser entregado por el Contratista de Sistemas al usuario final, cuenta con dicho software básico para el desarrollo de sus funciones. Así mismo existe software adicional utilizado para el desarrollo de las actividades de los funcionarios y equipos de la empresa.

4.3.1. Condiciones bajo las que puede utilizarse Software adicional:

- Software “Preinstalado"
- Software proporcionado por el Contratista de Sistemas con el fin de:
  - Realizar actualizaciones remotas
  - Actualizar software preinstalado
  - Sustituir software preinstalado
  - Accesos o componentes de software instalados en los servidores de información.
  - Software de uso temporal (previo análisis de disponibilidad de licencia).

- Software proporcionado por el Contratista de Sistemas a través de la intranet o por medios no directos (Instalaciones no asistidas).

- Software de Soporte o Complementario: Identifíquese a este software que es propiedad de alguna entidad gubernamental (Ministerios, entes de control, entre otros) y que requiera ser instalado para realizar en tiempo y forma las actividades encomendadas a los usuarios.
- Por otro lado, también se encuentra el software que viene incluido con hardware (cámaras, grabadoras, videograbadoras digitales, unidades de respaldo, unidades de almacenamiento externo, GPS, entre otros) y que sin estas aplicaciones no puedan operar correctamente.

4.3.2. Software que no puede ser instalado:

- Copias ilegales de cualquier programa.
- Software descargado de Internet.
- Software que no se haya identificado como perteneciente al CDAR.
- Instalaciones no autorizadas o no solicitadas al Contratista de Sistemas.
- Software adquirido para uso personal del usuario (sin fines institucionales).
- Software de entrenamiento o esparcimiento.
- Software de dispositivos móviles de uso personal.

4.3.3. Licenciamiento

El software institucional se encuentra amparado por sus respectivas licencias de uso (salvo las aplicaciones libres con fines institucionales), mismas que tienen un proceso de adquisición.

La meta del Contratista de Sistemas es mantener actualizada la información de licenciamiento. Para cumplir con esta meta, se responsabiliza a mantener la disponibilidad de suficiencia, tenencia y conservación de dichas licencias para el software clasificado como:

- Sistemas Operativos
- Conjunto de Aplicaciones (ofimática, contabilidad, operación, entre otros)
- Herramientas Especializadas
- Software de Internet
- Accesorios

4.3.4. Requerimientos de Software

Todo usuario que requiera determinado software instalado en su computadora, deberá solicitarlo al Contratista de Sistemas. El Contratista de Sistemas determinará, de acuerdo a las características del software que resguarda, verificar si existe disponibilidad de licencias para atender la petición o, en caso contrario hacer la solicitud para la adquisición de la misma.

5. POLÍTICA INSTITUCIONAL

El uso de cualquier software sin licencia es ilegal y puede exponer al CDAR a una responsabilidad civil y criminal bajo las Leyes del Derecho de Autor, por lo que el CDAR no permitirá la utilización de software sin licencia o no autorizado por ningún usuario. Así mismo, todo usuario que sea descubierto copiando software o información de manera ilegal o que copie software o información para dárselo a cualquier tercero fuera del CDAR, incluyendo clientes, será sancionado de acuerdo a las circunstancias y leyes vigentes.

6. POLÍTICAS PARA EL RESPALDO DE LA INFORMACIÓN ELECTRÓNICA

6.1. Aspectos Generales

- El contratista de sistemas informara al responsable de cada equipo cómo funciona el programa que realiza las copias de respaldo, la ruta y el horario establecido en el documento itinerario copias de seguridad.
- Las copias de seguridad se realizarán diariamente, semanalmente o de forma mensual según cada caso en particular.
- La información de los archivos contenidos en las copias de seguridad debe ser única y exclusivamente de uso institucional y no personal.
- En caso de requerirse la inclusión o modificación de un servicio de copia de respaldo debe solicitarlo al o contratista de sistemas para su revisión, aprobación e implementación.
- Semanalmente se verificaran las copias comprimidas, para comprobar que se pueden restablecer cuando se necesiten.
- En caso de que algún funcionario necesite copias de sus archivos almacenados en el servidor de backup, esta petición debe ser requerida al contratista de sistemas.
- Se deben realizar copias de respaldo de toda la información esencial del servidor de las pistas. Para asegurar que todo se pueda recuperar tras un desastre o un fallo de los soportes, se tendrán dispositivos de respaldo adecuados.

6.2. Copias de Seguridad Informática

6.2.1. El contratista de sistemas creará una carpeta en los discos duros externos y en el equipo de publica (el computador) donde se almacenara dicha información.

6.2.2. El contratista de sistemas verificara que las copias de seguridad enviadas por cada uno de los funcionarios, sea generada correctamente por el programa.

6.2.3. Se realizara diariamente copias de seguridad del backup de la empresa a una unidad de disco duro externa.

6.2.4. Para el registro de la realización de las copias de seguridad, y verificación de las respectivas pruebas de respaldo, el contratista de sistemas debe diligenciar diariamente el formato GA.24.7.2 ***"Formato Control de Copias de Seguridad".***

Durante la ejecución de los numerales anteriores se tendrán en cuenta los siguientes controles para el **servidor de pistas** de acuerdo a la norma NTC 5385 Numeral 4.16.2.3:

- Almacenar un nivel mínimo de información de respaldo diario, junto a los registros exactos y completos de las copias de seguridad y procedimientos documentados, en una unidad de disco en el mismo servidor.
- En caso de daños por un desastre en la locación del servidor; diariamente se respaldarán desde el servidor de pista, las copias de los días anteriores en un servidor externo en la nube.
- Se debe realizar pruebas a los respaldos diariamente para asegurar que son fiables en caso de necesitar su uso en caso de emergencia este debe quedar registrado en el formato GA.24.7.1 ***"Formato Control de Copias de Seguridad Servidores"***

- Se puede verificar las copias de respaldo del servidor de pista siguiendo los pasos que se encuentran en el manual del Software de pista TECNI-RTM en el ítem "***Instructivo para la realización y verificación de las copias de seguridad de tecni-rtm.***"

6.3. Restauración de las copias de seguridad

- En caso de que algún funcionario requiera la restauración de algún archivo guardado en el servidor como copia de respaldo, deberá solicitar al contratista de sistemas la información que requiere, para su respectiva aprobación el cual debe seguir los pasos del procedimiento "Plan de Contingencia Informática".

7. POLÍTICAS DE MANTENIMIENTO DE SOFTWARE Y HARDWARE

Los equipos de cómputo de la empresa deben estar sometidos a un programa de mantenimiento, registrado en el formato

"Cronograma de Mantenimiento" de modo que se asegure su permanente disponibilidad e integridad.

- El mantenimiento preventivo de los equipos debe ser realizado al menos 2 veces al año y estar sometidos a un mantenimiento regular (limpieza general, verificación de estado de conexiones, verificación de actualizaciones) al menos una vez por mes.
- El mantenimiento será realizado en las instalaciones de la empresa (los equipos no deben ser retirados de las instalaciones físicas) solo por el personal de mantenimiento contratado para tal fin y en las fechas adoptadas en el "cronograma de mantenimiento".
- Los equipos deben de contar con una hoja de vida en la que el contratista debe registrar la información general del equipo, el software instalado con el registro de las respectivas licencias y el historial de labores desarrolladas durante los mantenimientos realizados.

8. DISPOSICIONES ADICIONALES PARA EL HARDWARE Y SOFTWARE DEL ORGANISMO DE INSPECCIÓN VEHICULAR

8.1. Conexiones de Red

Teniendo en cuenta que uno de los requisitos de la resolución 3768 del 26 de Septiembre de 2013 del Ministerio de Transporte, establece como obligatoria la conectividad con el RUNT; y que la forma de establecer esta conexión es mediante un acceso a Internet: En el equipo servidor de la pista está prohibida la navegación libre en internet con el fin de evitar el descargue de información que contenga software malicioso.

Está prohibida la utilización de dispositivos de almacenamiento externo en los equipos de la pista de revisión o en el servidor, en caso de ser requerido, es responsabilidad del usuario administrador ejecutar las acciones a fin de detectar software malicioso y tomar las acciones necesarias para evitar la pérdida de la información.

8.2. Administrador de la Base de Datos

La base de datos debe permitir su administración, seguimiento, monitoreo de las actividades, copias de seguridad y políticas de restauración, gestión de roles o perfiles

de usuarios, los archivos de datos no deben ser accesibles mediante el uso de carpetas compartidas o búsqueda desde un explorador.

Solo El director Técnico y su suplente tendrán acceso a generar reportes previamente diseñados desde esta base de datos, sin embargo no podrá manipular la información, su rol no debe permitir cambiar los datos de las pruebas obtenidas previamente.

9. OTRAS DISPOSICIONES

9.1. El Diagnosticentro S.A.S es responsable, en el marco de compromisos legalmente ejecutables, de la gestión de toda la información obtenida o generada durante la realización de las actividades de inspección. El organismo de inspección debe informar al cliente, con antelación, qué información tiene intención de hacer pública. A excepción de la información que el cliente pone a disposición del público, o cuando haya sido acordado entre el organismo de inspección y el cliente (por ejemplo, con el fin de responder a quejas), toda otra información debe ser considerada información confidencial.

9.2. Cuando el organismo de inspección deba por ley divulgar información confidencial o cuando esté autorizado por compromisos contractuales, el cliente o la persona correspondiente debe ser notificado acerca de la información proporcionada, salvo que esté prohibido por ley.

9.3. La información sobre el cliente obtenido de fuentes distintas al cliente (por ejemplo, una persona que realiza una queja, de autoridades reglamentarias) debe tratarse como información confidencial.

9.4. Los funcionarios del DIAGNOSTICENTRO S.A.S. no podrán usar el nombre y/o la información del OEC en sus redes sociales cuando el objetivo sea lucrarse o hacer negociaciones con terceros.

10. VIGENCIA DE LAS POLÍTICAS

Estas políticas tendrán vigencia a partir de su divulgación y serán revisadas por la Gerencia, el Director Financiero Administrativo y el Director Técnico de acuerdo a los cambios en la infraestructura o evolución tecnológica.

11. SANCIONES

Al detectarse un incumplimiento en las actuales Políticas, se aplicarán los siguientes criterios y sanciones:

11.1. Primera vez

La primera vez que el usuario haya incumplido una de las Políticas, el Contratista de Sistemas notificará por escrito al responsable de la falta y le recordará las políticas vigentes.

11.2. Segunda vez

De presentarse un segundo incumplimiento en las Políticas, el Contratista de Sistemas notificará por escrito al Gerente y al Director Administrativo Financiero, informándoles el tipo y contenido de la falta, suspendiendo el servicio temporalmente al usuario responsable hasta que el encargado del área apruebe por escrito la restauración del servicio.

11.3. Reincidencia

En caso de presentarse un tercer incumplimiento en las Políticas por parte del mismo usuario, causará suspensión inmediata e indefinida del servicio y el caso se informará a la Gerencia para determinar si es necesario aplicar sanciones administrativas adicionales, si la seguridad se ve comprometida. El Contratista de Sistemas se reserva el derecho de suspender el acceso a la red y al equipo de cómputo al usuario de manera inmediata

ANEXO. Ninguno