

OFICINA DE ASESORÍA EN GESTIÓN (AUDITORÍA INTERNA)
METRO DE MEDELLIN
CUESTIONARIO USO LEGAL DE SOFTWARE
ÁREAS: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, SISTEMA OPERATIVO Y UNIDAD
ESTRATÉGICA DE NEGOCIOS (UEN Cívica)
MARZO DE 2025

Objetivo General

Dar cumplimiento a la Directiva Presidencial No 002 de 2002 y la Circular 04 de diciembre de 2006, conforme con el procedimiento determinado en la Circular 017 de 2011, modificada a través de la Circular Externa 027 de diciembre 29 de 2023, donde se solicita a las entidades u organismos públicos dar cumplimiento al compromiso de verificar el uso legal de software, se realiza el siguiente cuestionario:

Objetivos Específicos

- Recaudar los datos necesarios de la(s) dependencia(s) encargada(s) de la gestión y registro de datos del software en la Entidad para comprobar la razonabilidad de sus registros.
- Entregar a la Dirección Nacional de Derechos de Autor los datos solicitados por los medios previstos por dicho ente en los términos establecidos.
- Elaborar el informe que dé cuenta del cumplimiento a lo ordenado por la normatividad vigente y divulgarlo por los medios idóneos y autorizados.

Alcance

El informe tendrá como alcance el periodo comprendido entre enero y diciembre de 2024. Se referirá al software licenciado en uso y dado de baja y al hardware computacional del Metro de Medellín, así como los controles implementados para mitigar los riesgos asociados al uso de software no licenciado.

1. ¿Con cuántos equipos cuenta la entidad?

- ✓ Sistema Operativo: 276 (distribuidos así: 146 servidores + estaciones de trabajo 130)
- ✓ TI: 1.614 Equipos, entre PCs, portátiles, 180 Servidores
- ✓ UEN: 429 Equipos distribuidos de la siguiente forma (136 Máquinas de recarga (MRA), 123 Equipos de puntos de venta (PDV), 79 Lectores de saldo y recarga (LSR) y 91 servidores).

TOTAL EQUIPOS EMPRESA: 2.319

2. ¿El software instalado en estos equipos se encuentra debidamente licenciado?

- ✓ Sistema Operativo: Si, se encuentra licenciado, también se tiene software hecho a la medida y software libre.
- ✓ TI: Sí
- ✓ UEN: Sí

3. ¿Qué mecanismos de control se han implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?

Sistema Operativo

- Gestión y análisis de vulnerabilidades.
- Control de conexión y acceso a los equipos.
- Segregación de Roles y funciones en los sistemas.
- Protección de dispositivos con equipos UTM en HA y consola de antivirus.
- Revisión y monitoreo periódico a través del control y actualización del inventario.
- Instalación de software de inventarios ProactivaNet.
- Instalación de sensores HIPS en servidores para monitoreo.
- DR1571_Lineamientos de ciberseguridad, en el cual se especifica, quiénes son los autorizados para realizar la instalación y desinstalación de software y hardware en equipos de cómputo.

Tecnologías de la Información

- a) Se tiene publicado, dentro del Sistema de Gestión Integral de la Empresa los siguientes documentos:
- DR1571 Lineamientos de Ciberseguridad.
 - Lineamientos de seguridad de recursos informáticos:

➤ Equipos de cómputo y periféricos

Algunas áreas de la Empresa administran equipos y software especializado, el cual requiere personal con capacidades o formación técnica no disponible en la Mesa de servicios. Solo para estos casos la instalación, actualización o modificación del software y hardware en los equipos de cómputo podrá ser realizada por personal de cada área o a través de contratistas especializados, si se diera el caso. En caso de requerir apoyo técnico por parte de Gestión de Tecnologías de Información deberá ser solicitado a través del Portal de Servicios Integrados.

En caso de pérdida o robo de los equipos de cómputo, periféricos o dispositivos móviles asignados a empleados, practicantes, aprendices, y de los contratistas autorizados para conectarse a las redes de la Empresa, el responsable del equipo deberá realizar lo siguiente:

Reportar inmediatamente el incidente a su jefe inmediato o Supervisor de contrato y al área responsable de administrar el activo.

- Los empleados, practicantes y aprendices deben cumplir con lo descrito en el DH005 Procedimiento para la administración de bienes muebles devolutivos.

DR1387 Lineamientos para uso de servicios de tecnología de información

➤ Equipos de usuario final

El usuario del equipo de cómputo o dispositivo móvil adquirido por el área de Gestión de Tecnologías de la Información, es responsable de acatar las disposiciones del área de Gestión de Tecnologías de Información, en cuanto a los programas y aplicaciones que puede tener en el equipo asignado. Así mismo, no está autorizado para instalar software o aplicaciones no autorizadas o que no cuente con los licenciamientos legalmente adquiridos o que se considere como infractores de derechos de autor y que sean hallados en el equipo asignado. En tal caso, el usuario deberá responder integralmente ante La Empresa a través de los mecanismos definidos para ello.

El personal de la Mesa de Servicios Corporativa es el único autorizado en la Empresa para realizar modificaciones al software (instalación, desinstalación o actualización) e intervenciones al hardware de los equipos de cómputo y los dispositivos móviles. Para su solicitud, deberá utilizarse el Portal de Servicios Integrados.

➤ Dispositivos móviles

El área de Gestión Tecnología de Información es responsable del software para los sistemas de información, por lo que deberá validar que las aplicaciones que se proyecta instalar a los dispositivos móviles den cumplimiento estricto a las regulaciones y procedimientos vigentes a nivel de compra, licenciamiento, uso, mantenimiento y desincorporación de software en general.

Respecto a las aplicaciones que pueden ser utilizadas por parte de los usuarios del servicio al interior de la Empresa se deberá dar cumplimiento a las siguientes consideraciones:

- Cada uno de los dispositivos móviles cuenta con una tienda de aplicaciones que depende de su sistema operativo. Sin embargo, no está autorizada la instalación libre de aplicaciones que no hayan sido validadas por el equipo de ciberseguridad del área de Gestión Tecnología de Información.
- El área de Gestión Tecnología de Información cuenta con herramientas tecnológicas que protegen remotamente y permiten el control de aplicaciones y uso que sean instaladas en los dispositivos móviles.
- El área de Gestión Tecnología de Información es responsable del software para los sistemas de información, por lo que deberá validar que las aplicaciones que se proyecta instalar a los dispositivos móviles den cumplimiento estricto a las regulaciones y procedimientos vigentes a nivel de compra, licenciamiento, uso, mantenimiento y desincorporación de software en general.
- Dada la vocación de los procesos misionales y de soporte de la Empresa y como parte del modelo técnico operativo, no se permite el uso de aplicaciones que no estén directamente relacionadas con las actividades laborales definidas por la Empresa. Es responsabilidad del área usuaria garantizar que el requerimiento de instalación de aplicaciones cumpla rigurosamente esta condición.

- Si se identifica un uso de aplicaciones, indebido o por fuera de lo previsto, que exponga a cualquier riesgo a la Empresa, el área de Gestión Tecnología de Información implementará medidas de control y restricción de funcionamiento del dispositivo.

b) Controles técnicos y monitoreo de la seguridad de la información

- La Empresa cuenta con una aplicación que permite mantener un registro del software instalado y las características del hardware de los equipos de cómputo.
- Antes de asignar una licencia se valida la disponibilidad de esta en la respectiva consola.
- El área de Gestión de Tecnologías de Información realiza monitoreo periódico al software instalado en los equipos y desinstala el software que no es de uso corporativo, que haya sido instalado sin autorización, que no cuente con el debido licenciamiento a nombre de la Empresa, o que represente un riesgo para la seguridad de los activos de información.
- La Empresa cuenta con protocolos de descarga e instalación de actualizaciones y parches de seguridad para los sistemas operativos y aplicaciones de uso corporativo.
- No todos los usuarios tienen privilegios de administración local de su máquina y cada vez que un usuario requiere dicho privilegio, debe leer y aceptar los compromisos que se indican en el documento “Compromiso Administradores locales”, este mecanismo permite concientizar al usuario de la responsabilidad que adquiere sobre la instalación de software no autorizado en los equipos de la empresa.
- Se realiza control de los puertos USB de los computadores corporativos administrados por TI. Quien requiere un puerto desbloqueado, debe firmar un compromiso y el uso de este es monitoreado.
- El área de Gestión de Tecnologías de Información realiza monitoreo anual a los usuarios que son autorizados como administradores locales de los equipos; en caso de identificar un uso inadecuado de los privilegios o estos representan un riesgo para la seguridad de los activos de información, se realiza el correctivo.
- El área de Gestión de Tecnologías de Información a través del software antivirus corporativo realiza un control adicional, en caso de identificar equipos con software no autorizado, se hace la verificación y la desinstalación correspondiente.

UEN CIVICA

El único rol que puede instalar software en puntos de venta y servidores Cívica es el administrador local de los equipos de cómputo o administrador del sistema para el caso de infraestructura Cívica, el cual es utilizado por la mesa de servicios y administradores Cívicas respectivamente. Estas estaciones de trabajo son monitoreadas para verificar que el software instalado sea el autorizado.

Para los equipos asignados a los profesionales de la UEN Cívica, se corren las rutinas que se tienen dentro del Sistema de Gestión Integral de la empresa, en el procedimiento para la seguridad de los activos de información, en el ítem “Normas para la instalación y desinstalación de hardware y software en equipos de cómputo” donde se especifica quienes son las personas autorizadas para realizar la instalación y desinstalación de software y hardware en equipos de cómputo.

Las máquinas de recarga no cuentan con puertos USB externos, estos puertos se encuentran dentro de los cofres de estas, los cuales tienen accesos controlados.

4. ¿Cuál es el destino final que se le da al software dado de baja en su entidad?

Sistema Operativo

La disposición final del software se da de acuerdo con la finalidad de este con las políticas de derecho de autor y que la Empresa tiene para este fin.

Se cuenta con el TI012_Procedimiento para desincorporación de tecnología de información en el numeral 2.3.2 Desincorporación de componentes de software operación comercial, allí se describe que se desinstala de todos los equipos donde esté instalado. Si se trata de aplicativos, desarrollos a la medida se realiza respaldo de la información que se requiera y posteriormente se desinstala el sistema de todos los equipos donde esté instalado.

Tecnologías de la Información

El software que ya no se va a utilizar se desinstala de los equipos de cómputo en los que se encuentre instalado. Al momento dar de baja a un equipo de cómputo se realiza el formateo del computador.

UEN

En lo que respecta a los servidores y estaciones de trabajo (procedimiento de TI) las licencias OEM al dar de baja los equipos en los que vienen instaladas, se procede a formateos de bajo nivel donde se elimina toda la información del medio de almacenamiento y en caso de que este sea entregado en donación, se hace entrega con las licencias de software de sistema operativo OEM.