CODECHOCÓ
Corporación Autónoma Regional
Para el Desarrollo Sostenible del Chocó

CI- 110 - 47.10-2025-No.002

INFORME SOBRE LA GESTIÓN DE EQUIPOS Y SEGURIDAD INFORMÁTICA 2024

FECHA: 5 de marzo de 2025

OBJETIVO:

Analizar y argumentar la importancia de la implementación de medidas de seguridad en la gestión de equipos de cómputo dentro de la entidad, garantizando el uso eficiente de los recursos tecnológicos, la protección de la información y el cumplimiento de normativas sobre licenciamiento de software y control de uso de los mismos.

CRITERIOS:

Para evaluar la efectividad de las medidas implementadas, se consideran los siguientes criterios:

- ✓ Seguridad informática: Protección de los equipos y la información contra accesos no autorizados o software malicioso.
- ✓ Gestión eficiente de los recursos: Optimización del uso de equipos y software con licencias adecuadas.
- ✓ Control de acceso y administración: Regulación de los permisos de usuario para prevenir la instalación de programas no autorizados.
- ✓ Cumplimiento normativo: Asegurar que las prácticas implementadas estén alineadas con las políticas de seguridad y las normativas vigentes

ALCANCE:

Este informe abarca la evaluación de las acciones adoptadas por la entidad en cuanto a la administración de sus 107 equipos de cómputo, el licenciamiento del software instalado y la implementación de políticas de seguridad para evitar el uso indebido de los equipos. Además, se revisa la estrategia de almacenamiento y resguardo del software propio de la entidad en servidores locales.

1. Inventario de Equipos

Actualmente, la entidad cuenta con un total de 107 equipos de cómputo activos, distribuidos de la siguiente manera:

- ✓ 11 portátiles
- ✓ 84 equipos Todo en Uno
- ✓ 12 equipos de mesa

Esta información se encuentra registrada en el inventario administrado por la oficina de TI.

2. Licenciamiento del Software

Todos los equipos de cómputo de la entidad tienen instalado software debidamente licenciado, cumpliendo con las normativas y requerimientos legales.

3. Controles para el Uso de Software

Con el fin de evitar la instalación de software no autorizado en los equipos, se han implementado los siguientes controles:

- ✓ Se han creado usuarios sin permisos de administración, es decir, sin la posibilidad de instalar o desinstalar aplicaciones. Estos usuarios son los que se entregan a los encargados de los equipos, mientras que los usuarios administradores son manejados exclusivamente por el personal de la oficina de TI.
- ✓ Se han definido y difundido políticas de seguridad que establecen que los usuarios no tienen autorización para modificar la instalación de software en los equipos.
- ✓ Se han bloqueado páginas de descarga desde el firewall, reduciendo así el riesgo de instalación de software no autorizado.
- ✓ Se ha implementado un dominio para configurar políticas de seguridad en todos los equipos que forman parte de la red, facilitando su administración y control mediante configuraciones grupales.

4. Resguardo del Software Propio de la Entidad

El software desarrollado internamente por la entidad, que no está en uso actualmente, se encuentra almacenado en los servidores locales, junto con sus respectivos manuales y credenciales de acceso.

La gestión eficiente de los equipos de cómputo es un factor clave en la operatividad de una entidad, ya que permite optimizar los recursos tecnológicos y garantizar la seguridad de la información.

En este contexto, la entidad ha tomado medidas concretas para evitar la instalación de software no autorizado, lo que contribuye significativamente a la protección contra vulnerabilidades y amenazas cibernéticas.

Uno de los mecanismos fundamentales implementados es la restricción de permisos de usuario, evitando que los empleados puedan instalar o desinstalar aplicaciones sin la autorización del personal de TI. Esto no solo previene la instalación de software malicioso o incompatible, sino que también ayuda a mantener la estabilidad del sistema operativo y el correcto funcionamiento de los equipos.

Otro aspecto relevante es el bloqueo de páginas de descarga desde el firewall, lo que reduce la posibilidad de que los usuarios descarguen programas sin aprobación. Esta medida es esencial para evitar infecciones por malware y garantizar que todos los programas utilizados en la entidad sean seguros y legítimos.

Además, la implementación de un dominio para la configuración centralizada de políticas de seguridad permite una administración eficiente y homogénea de los equipos, facilitando el control de accesos y la aplicación de configuraciones grupales sin necesidad de intervenir manualmente en cada dispositivo.

Por último, el almacenamiento del software propio en servidores locales asegura que la entidad mantenga el control total sobre sus aplicaciones internas, minimizando riesgos de pérdida de datos o accesos no autorizados. Esta práctica es clave para la continuidad operativa y la protección de la propiedad intelectual de la organización.

En conclusión, la entidad ha adoptado un enfoque proactivo en la gestión de sus equipos de cómputo, promoviendo un ambiente tecnológico seguro y eficiente que garantiza la protección de la información y la continuidad operativa, además mantiene un control adecuado sobre sus equipos de cómputo mediante una gestión organizada del inventario, el cumplimiento de licenciamiento de software y la implementación de políticas de seguridad que previenen el uso indebido de los recursos tecnológicos.

Firma_____

YURISA ALEXANDRA TRUJILLO MOSQUERA
Jefe Oficina Control Interno

Proyecto/Elaboró	***Aprobó***	***Folios***	***Anexos***	***Folios de anexos***	***Fecha***
Yesenia Córdoba Quesada *Contratista OCI*	*Yurisa Alexandra Trujillo M* *Jefe Oficina de Control Interno*	*Tres (3)*	*( )*	*( )*	*05/03/2025*