

1. OBJETIVO

Garantizar el buen funcionamiento de los equipos de cómputo y dispositivos de comunicaciones, así mismo respaldar y salvaguardar la información sensible de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge CVS.

2. ALCANCE

Este documento aplica a:

- La oficina administrativa y financiera de la Corporación.
- A cada mantenimiento preventivo y copia de seguridad programada en los dispositivos de cómputo y comunicaciones.
- Usuarios que tengan a cargo recursos tecnológicos provistos por la Corporación
- Todos los procesos del SGI.

3. RESPONSABLES

- Profesional universitario código 2044 grado 9 con funciones de sistemas
- Ingeniero de soporte técnico (contratista)
- Técnico de sistemas (contratista)
- Estudiantes Pasantes de sistemas.

4. DEFINICIONES

- **Usuario:** Todo individuo ya sea funcionario, contratista o pasante, que hace uso de los recursos informáticos de la Corporación.
- **Información:** Conglomerado de datos escritos y gráficos consistentes y articulados que tratan sobre un tema o área del saber
- **Copia de Seguridad:** (Backup) Acción de copiar uno o varios archivos en una localización alternativa, de forma que una copia permanezca intacta si el original es destruido o dañado. Se puede guardar tanto un archivo como el contenido de todo un disco duro. Siempre que el soporte sobre el que se realice tenga la capacidad suficiente. Estas copias se suelen almacenar de forma comprimida.
- **Soporte:** Es el servicio o ayuda en temas informáticos que se presta a los usuarios de la Corporación para resolver un problema, falla o asesoría.
- **Plataforma tecnológica:** Es todo el conjunto de equipos y programas que integran la red de sistemas de la Corporación.
- **Red:** Conjunto de elementos activos y pasivos entrelazados que contribuyen al intercambio de información entre computadores o usuarios.

- **Comunicación:** Proceso de transmisión y recepción de ideas, información y mensajes.
- **Programa:** Conjunto de instrucciones de computación estructuradas y ordenadas de manera tal, que, cuando se ejecutan, hacen que un computador realice una función particular.
- **Hardware:** Los dispositivos o elementos físicos que comprenden un sistema de computación.
- **Periféricos:** dispositivo de comunicación que no hace parte integral del equipo de cómputo, pero se integra a su funcionalidad (impresoras, escáner, parlantes)
- **Plataforma de Backup "Nube":** Herramienta de tecnología que brinda espacio de almacenamiento virtual para el resguardo de información en la red de internet.
- **Equipos de Comunicación:** Dispositivos de red que conforman la plataforma tecnológica dentro de los que se encuentran:
 - Router
 - Switch
 - Access Point
 - Convertidor de fibra óptica.
- **Cableados Estructurados:** serie de componentes pasivos tales como:
 - Cable UTP
 - Tomas
 - Patch Panel
 - Gabinetes
 - Patch Cords

5. DESCRIPCIÓN DEL PROCEDIMIENTO

Mantenimiento preventivo:

- Se planifican los trabajos de mantenimiento de acuerdo a la programación de mantenimiento; para lo cual se utiliza el formato **GA-FO-29**, en Sistema Integrado de Gestión de Calidad/Proceso GA/GA-PR Soporte de Sistemas/GA-PR-02 Mantenimiento preventivo y copia de seguridad programada. Están estipulados dos (2) mantenimientos preventivos al año a todos los equipos de cómputo de la plataforma tecnológica.

- Se debe dejar registro mediante formato Control de Mantenimiento Preventivo **GA-FO-28**, de los mantenimientos de todos los equipos de cómputo de la CVS.
- Informar por medio de nota interna a los jefes de dependencias máximo con cinco (5) días de anticipación las fechas en las cuales se van a realizar los trabajos de mantenimiento a los equipos de cada área.
- Los trabajos de mantenimiento realizados, tienen que garantizar el buen funcionamiento de los equipos que conforman la plataforma tecnológica de la Corporación.
- Es obligación de los usuarios cumplir las reglas de las POLITICAS DE SEGURIDAD INFORMÁTICA para el manejo de los equipos de cómputo y la red informática de la Corporación.
- La solución a las fallas presentados en la plataforma tecnológica derivadas del mantenimiento preventivo que requieran reemplazo de piezas o repuesto, se tramitaran de acuerdo a las disponibilidades de inventario que tenga la Corporación.
- Para el mantenimiento de equipos y periféricos en las subsedes de la corporación, el usuario debe enviar el equipo hacia sede central al área administrativa y financiera para su posterior revisión, en caso del soporte sea de Software se hace de forma remota, solicitando conexión al equipo del usuario.

Descripción del Procedimiento Mantenimiento Preventivo de Equipos de Computo

1. Se verifica el funcionamiento general del equipo para determinar si este presenta algún fallo antes de realizar el mantenimiento.
2. Se revisa el equipo, se desensambla y se hace una limpieza general de todas las partes internas de Hardware, Memorias, Discos Duros, Procesadores, Disipadores unidades ópticas, tarjetas PCI, usando herramienta sopladora/aspiradora, se le aplica liquido limpia contactos, se ensambla y se aplica silicona al Chasis de la CPU, teclado y monitor.
3. Después de realizada la limpieza del equipo, se hace una prueba de funcionamiento de las partes del equipo. Si hay deficiencia en alguna parte se cambia según disponibilidad de inventarios de la Corporación.
4. Se realiza mantenimiento lógico, este se hace realizando análisis de virus, limpieza de Archivos Temporales, cache de internet, historial de navegación, cookies, historial de descargas, ejecuciones del explorador de Windows, documentos recientes, accesos directos del menú inicio y de la barra de tareas, vaciar papelera, volcados de memoria, informes de errores de Windows, cache DNS y limpiar errores de entrada del registro de Windows.

Descripción del Mantenimiento Lógico – Preventivo de los equipos de comunicación (RED LAN).

1. Se le comunica a cada área de la corporación, la fecha en la cual se va a realizar el mantenimiento.
2. Se verifica el funcionamiento de los equipos de comunicación y de los Patch Cords (cable que va de la toma de red al equipo) de la red por medio de probadores de red. Si presenta fallas se corrige enseguida.
3. Se verifica la integridad de las tomas de red y se les hace limpieza. Si hay fallas se corrige enseguida.
4. Se realiza una inspección física del Backbone (Cables principales entre Switch) para verificar la integridad y se le hace una prueba de continuidad. Si hay fallas se corrige enseguida.
5. Se desmonta el equipo de comunicación y se hace una limpieza general de las partes
6. Se instala el equipo nuevamente en su lugar, se hace una prueba de funcionalidad verificando los leds indicadores, si hay fallas se corrigen enseguida.
7. Se realiza verificación de las aplicaciones que tenga instalada el equipo para asegurar que no tenga instalado software sin licencias legalmente adquirida por la Corporación, así mismo se verifica la instalación de la aplicación de copias de seguridad en la nube.

Copias de seguridad.

- Las copias de seguridad se realizarán por medio de la plataforma en nube que la Corporación tenga contratada, cada usuario será responsable de resguardar únicamente la información institucional en la "Nube", la cual podrá ser accedida desde cualquier dispositivo con acceso a internet iniciando sesión en su cuenta de correo electrónico institucional en línea o en la aplicación de nube instalada en el equipo, igualmente se estipulará la salvaguarda de las bases de datos de los sistemas de información en la nube suministrada por el proveedor de servicios tecnológicos contratado, este procedimiento debe hacerse de forma constante por cada funcionario de la Corporación para garantizar la disponibilidad de la información.

Nota: Para el proceso de Gestión Administrativa y Financiera las copias de seguridad se realizarán diariamente, dos veces al día a las bases de datos de los sistemas de información y se guardarán automáticamente en la nube suministrada por el proveedor.

- La aplicación de la nube realizará copias de seguridad automáticamente a la información que se encuentre en la respectiva carpeta a sincronizar, información que se encuentre en otra ubicación no se le realiza copia de seguridad, por lo que el usuario deberá tener en cuenta cuáles son las carpetas sincronizadas y monitorear su sincronización.

- Los usuarios de la red Corporativa son los encargados y únicos responsables de realizar la copia de seguridad de su información, seleccionándola y guardándola en la respectiva carpeta en la "Nube" únicamente la información institucional excluyendo archivo personales, archivos de video y música, teniendo en cuenta que solo dispone de 1TB de almacenamiento, por lo que debe continuamente depurarla y conservar la información más relevante, si la información supera este tamaño debe solicitar a la oficina de almacén un medio magnético de almacenamiento sujeto a disponibilidad para su propio resguardo y control.
- La copia de seguridad de la información de los usuarios permanecerá en la plataforma de Backup en la nube que la Corporación tenga contratada, bajo la administración y responsabilidad de cada funcionario, los cuales pueden acceder a ella por medio de su correo electrónico institucional.
- Es obligación de los usuarios de la plataforma tecnológica cumplir las reglas de las POLITICAS DE SEGURIDAD INFORMÁTICA para el manejo de los equipos de cómputo y la red de sistemas de la Corporación.
- De acuerdo al cronograma, se fija la fecha y la hora para llevar a cabo el mantenimiento preventivo y las copias de seguridad se realizan en la nube automáticamente.

Descripción del procedimiento Copias de Seguridad Programadas

1. El usuario debe analizar y seleccionar la información que desea resguardar y copiarla en la respectiva carpeta en la nube que se encuentra claramente identificada en el explorador de Windows

NOTA: Solo se deben salvaguardar archivos de ofimática (PowerPoint, Excel, Word y bases de datos), no están admitidos los archivos de información personal (música y videos).

2. Cada usuario Dispone de 1TB de Almacenamiento, puesto que debe hacer selección de información relevante y efectuar continua depuración.
3. El Backup de los sistemas de información se resguardará en la nube suministrada por el proveedor de la plataforma informática administrativa y financiera, el cual suministrará las credenciales de acceso para hacer seguimiento a las Copias de seguridad generadas automáticamente de forma diaria, dos veces al día.
4. Se hace entrega del equipo al usuario una vez que el equipo ha sido probado y su funcionamiento se encuentra en óptimas condiciones de trabajo.

5. DOCUMENTOS DE REFERENCIA

Política de Seguridad Informática

6. REGISTROS Y ANEXOS

GA-FO-28 Control de Mantenimiento Preventivo

GA-FO-29 Programación Mantenimiento preventivo

7. CONTROL DE CAMBIOS

Versión:	Fecha:	Descripción de los Cambios:
01	25/10/2011	Reestructuración total de los procedimientos, acorde a los nuevos lineamientos del SIGCA; se utilizó versión 01 para este procedimiento Mantenimiento Preventivo y Copia de Seguridad Programada debido a que se fusionaron cuatro (4) procedimientos y todos tenían diferentes revisiones así: GS- P02 Copia de seguridad por solicitud de funcionarios v01; GS- P03 Copia de seguridad programada v03; GS-P05 Mantenimiento Preventivo v03; y GS-P06 Mantenimiento Lógico-preventivo v01.
02	09/07/2013	Actualización del ítem 5 "Descripción del Procedimiento" acorde a las actividades que se realizan en el proceso.
03	05/04/2019	Se realizan cambios a la metodología para realizar copias de seguridad y programación de copias de Seguridad.
04	11/09/2019	Actualización en el objetivo del procesamiento, responsable y descripción del procedimiento
05	20/02/2021	Actualización del objetivo, alcance, responsables y descripción del procedimiento.
06	05/03/2024	Actualización del objetivo, alcance, responsables y descripción del procedimiento.

CUADRO DE APROBACIÓN		
Elaboró: Álvaro Díaz Banda	Revisó: Jose L. Rodríguez	Aprobó: Adriana Negrete Cantillo
Cargo: Profesional Universitario	Cargo: Profesional Especializado	Cargo: Jefe Administrativa y Financiera
Firma: 	Firma: 	Firma: 