PLAN DE MANTENIMIENTO DEL PROYECTO

**Grupo C:** CASO 2: SINCOMPU S.A

1. Baldeón Silva Luis Fernando
2. Gudiño Estacio William Josué
3. Lara Jama Janis Odeth
4. Lozado Martinez Amanda Gabriela
5. Revelo Quintana José David
6. Yagual Villalva Hugo Alexis
7. Actualización del sistema operativo: Se recomienda mantener el sistema operativo actualizado a la última versión de su plataforma correspondiente para asegurar un rendimiento óptimo del sistema.
8. Actualización de controladores: Verifica que los controladores (drivers) de la computadora estén actualizados. Puedes encontrar las actualizaciones correspondientes en el sitio web del fabricante de tu dispositivo.
9. Actualización de software: Mantener al día todo el software utilizado es esencial para evitar problemas de compatibilidad. Asegúrate de instalar las últimas versiones disponibles.
10. Desinstalación de software innecesario: Realiza un análisis para identificar programas que realmente necesitas y elimina aquellos que no utilizas. Esto mejorará el rendimiento del sistema.
11. Mantenimiento del antivirus: Asegúrate de que tu antivirus esté siempre actualizado para garantizar la protección y seguridad de los datos.
12. Revisión de eventos programados: Verifica cada evento próximo en el calendario y asegúrate de que no afecte la integridad del sistema.
13. Limpieza física de la máquina: Mantén la máquina limpia para garantizar su funcionamiento adecuado y prevenir problemas relacionados con cortocircuitos.
14. Monitoreo del rendimiento: Implementa herramientas de monitoreo del sistema para detectar cuellos de botella, problemas de rendimiento o fallas.
15. Gestión de la configuración: Establece un proceso para controlar cambios en el sistema. Utiliza herramientas de control de versiones y registra las modificaciones para facilitar la identificación y resolución de problemas.
16. Pruebas y control de calidad: Realiza pruebas regulares para verificar el correcto funcionamiento del software. Esto incluye pruebas de integración, rendimiento, seguridad y funcionales. Implementa un proceso de control de calidad para garantizar que el software cumpla con los estándares y requisitos establecidos.
17. Respaldo regular de datos: Establece un plan de respaldo regular para asegurar la integridad de los datos. Utiliza soluciones de respaldo automáticas y verifica periódicamente la efectividad de la restauración de datos.
18. Optimización del inicio del sistema: Revisa y desactiva los programas que inician automáticamente con el sistema operativo. Esto puede mejorar significativamente el tiempo de arranque y el rendimiento general de la computadora.
19. Actualización de firmware: Verifica si hay actualizaciones de firmware disponibles para los componentes de hardware, como la BIOS. Mantener estos elementos actualizados puede resolver problemas de compatibilidad y mejorar la estabilidad del sistema.
20. Control de acceso y seguridad: Revisa y actualiza las políticas de acceso y las medidas de seguridad, como firewalls y configuraciones de permisos. Esto fortalecerá la protección contra amenazas externas y garantizará la privacidad de los datos.
21. Capacitación del personal: Proporciona capacitación regular al personal sobre las mejores prácticas de seguridad informática y el uso eficiente de las herramientas. Un equipo informado es fundamental para evitar errores y mejorar la seguridad global del sistema.
22. Respaldo regular de datos: Establece un plan de respaldo regular para asegurar la integridad de los datos. Utiliza soluciones de respaldo automáticas y verifica periódicamente la efectividad de la restauración de datos.
23. Optimización del inicio del sistema: Revisa y desactiva los programas que inician automáticamente con el sistema operativo. Esto puede mejorar significativamente el tiempo de arranque y el rendimiento general de la computadora.
24. Actualización de firmware: Verifica si hay actualizaciones de firmware disponibles para los componentes de hardware, como la BIOS. Mantener estos elementos actualizados puede resolver problemas de compatibilidad y mejorar la estabilidad del sistema.
25. Control de acceso y seguridad: Revisa y actualiza las políticas de acceso y las medidas de seguridad, como firewalls y configuraciones de permisos. Esto fortalecerá la protección contra amenazas externas y garantizará la privacidad de los datos.
26. Capacitación del personal: Proporciona capacitación regular al personal sobre las mejores prácticas de seguridad informática y el uso eficiente de las herramientas. Un equipo informado es fundamental para evitar errores y mejorar la seguridad global del sistema.