

PLAN DE MANTENIMIENTO TECNOLÓGICO 2024



Dirección Nacional de Bienes del Estado (DNBE)



*Dirección Nacional de
Bienes del Estado*




HONDURAS
GOBIERNO DE LA REPÚBLICA

	Dirección Nacional de Bienes del Estado	
	CONTENIDO DEL PLAN DE MANTENIMIENTOS TECNOLÓGICO.	

Responsables


Elaboración del Documento

Elaborado por	Cargo	Área de Trabajo	Fecha	Firma
Luis Enrique Mayorga Pineda	Jefe	Unidad de Informática	14/06/2024	


Revisión del Documento

Elaborado por	Cargo	Área de Trabajo	Fecha	Firma
Hector David Burgos Guzmán	Jefe	Unidad de Modernización	14/06/2024	

Verificación del Documento

Elaborado por	Cargo	Área de Trabajo	Fecha	Firma
Iris Natalia Brenes	Jefe	Gerencia Administrativa	14/06/2024	

Aprobación del Documento

Elaborado por	Cargo	Área de Trabajo	Fecha	Firma
Luis Alonso Sosa Salgado	Director Ejecutivo	Dirección Ejecutiva	14/06/2024	

Contenido

Introducción	4
Objetivos.....	4
Mantenimiento Preventivo	4
Mantenimiento Correctivo	5
Cronograma.....	5
Seguimiento y Monitoreo	6
Riesgos.....	7
Conclusión.....	7

Introducción

La Dirección Nacional de Bienes del Estado (DNBE) enfrenta el desafío de mantener la eficiencia y la continuidad operativa de sus sistemas y equipos tecnológicos. Este plan de mantenimiento tecnológico se ha desarrollado para asegurar que todos los recursos tecnológicos funcionen de manera óptima, minimizando tiempos de inactividad y prolongando la vida útil de los equipos. El plan abarca tanto el mantenimiento preventivo como el correctivo, y se estructura para atender las necesidades específicas de la DNBE.

Objetivos

1. **Garantizar la operatividad de los sistemas y equipos tecnológicos:** Asegurar que todos los sistemas y equipos funcionen de manera óptima.
2. **Reducir tiempos de inactividad:** Minimizar las interrupciones de servicios debido a fallos tecnológicos.
3. **Optimizar recursos:** Utilizar eficientemente los recursos destinados al mantenimiento.
4. **Prolongar la vida útil de los equipos:** Implementar prácticas que extiendan la durabilidad de los equipos y sistemas.
5. **Asegurar la seguridad de la información:** Proteger los datos contra fallos y vulnerabilidades tecnológicas.

Mantenimiento Preventivo

El mantenimiento preventivo se realiza de manera programada y regular para prevenir fallos antes de que ocurran. Incluye las siguientes actividades:

- **Inspección y limpieza de hardware:** Revisión y limpieza de equipos físicos para prevenir acumulación de polvo y suciedad. Esto incluye la limpieza de ventiladores, filtros y componentes internos de los dispositivos.

- **Actualización de software:** Instalación de parches y actualizaciones para mantener los sistemas operativos y aplicaciones al día, asegurando que los últimos arreglos de seguridad y mejoras de rendimiento estén implementados.
- **Verificación de sistemas de seguridad:** Revisión de antivirus, firewalls y otras medidas de seguridad para garantizar que estén funcionando correctamente y actualizados con las últimas definiciones de amenazas.
- **Copias de seguridad:** Realización regular de backups para asegurar la recuperación de datos en caso de fallos. Esto debe incluir pruebas periódicas de restauración para asegurar la integridad de las copias de seguridad.
- **Pruebas de funcionamiento:** Realización de pruebas periódicas de los sistemas para detectar posibles problemas antes de que se conviertan en fallos críticos. Esto puede incluir pruebas de carga, simulaciones de fallos y pruebas de redundancia.

Mantenimiento Correctivo

El mantenimiento correctivo se lleva a cabo cuando ya ha ocurrido un fallo. Incluye:

- **Diagnóstico de problemas:** Identificación y análisis de las causas de los fallos, utilizando herramientas de monitoreo y diagnóstico para determinar la raíz del problema.
- **Reparación de equipos y sistemas:** Solución de los problemas detectados, ya sea a través de reparaciones físicas o ajustes de software. Esto puede incluir la reinstalación de software, reemplazo de componentes defectuosos o ajustes en la configuración del sistema.
- **Reemplazo de componentes:** Sustitución de piezas o equipos que no puedan ser reparados. Se debe mantener un inventario actualizado de piezas de repuesto para asegurar una respuesta rápida.
- **Documentación de incidentes:** Registro detallado de los problemas y soluciones aplicadas para futuras referencias. Esta documentación debe incluir la descripción del problema, pasos tomados para la solución, tiempo de resolución y recomendaciones para evitar futuros incidentes similares.

Cronograma

Un cronograma bien definido es esencial para la ejecución efectiva del plan de mantenimiento. A continuación, se presenta una muestra del cronograma:

Actividad	Frecuencia	Responsable
Inspección y limpieza de hardware	Trimestral	Equipo de IT
Actualización de software	Mensual	Equipo de IT
Verificación de sistemas de seguridad	Mensual	Equipo de IT
Copias de seguridad	Diaria/Semanal	Equipo de IT
Pruebas de funcionamiento	Trimestral	Equipo de IT
Diagnóstico de problemas	Según necesidad	Equipo de IT
Reparación y reemplazo	Según necesidad	Equipo de IT
Documentación de incidentes	Continua	Equipo de IT

Seguimiento y Monitoreo

El seguimiento y monitoreo constante son cruciales para asegurar la eficacia del plan de mantenimiento. Incluye:

- **Sistemas de monitoreo en tiempo real:** Utilización de herramientas para vigilar el rendimiento y estado de los equipos y sistemas. Esto incluye el uso de software de monitoreo que alerta sobre posibles fallos antes de que ocurran.
- **Revisiones periódicas:** Evaluaciones regulares para asegurar que el plan de mantenimiento se está cumpliendo. Estas revisiones deben incluir auditorías

internas y externas para garantizar la adherencia a los procedimientos establecidos.

- **Informes de desempeño:** Generación de reportes para analizar la efectividad del mantenimiento y hacer ajustes si es necesario. Estos informes deben incluir métricas clave como tiempo de inactividad, número de incidentes, tiempo de respuesta y tiempo de resolución.

Riesgos

Los principales riesgos asociados con la implementación del plan de mantenimiento incluyen:

- **Falta de recursos:** Insuficiencia de personal o presupuesto para ejecutar el mantenimiento. Esto puede mitigarse mediante una planificación adecuada y la justificación de la necesidad de recursos adicionales.

- **Fallas no previstas:** Aparición de problemas inesperados que no pueden ser previstos por el mantenimiento preventivo. Para mitigar este riesgo, se debe contar con un equipo de respuesta rápida y procedimientos claros para la resolución de emergencias.

- **Obsolescencia tecnológica:** Equipos y sistemas que se vuelven obsoletos y necesitan ser reemplazados. Se debe realizar una evaluación periódica de la tecnología utilizada y planificar las actualizaciones o reemplazos necesarios.

- **Seguridad de datos:** Vulnerabilidades que podrían ser explotadas durante el proceso de mantenimiento. Es crucial mantener estrictos controles de seguridad durante todas las actividades de mantenimiento y capacitar al personal en prácticas de seguridad cibernética.

Conclusión

Un plan de mantenimiento tecnológico bien estructurado es esencial para la DNBE para asegurar la continuidad operativa y eficiencia de sus sistemas y equipos. A través de prácticas de mantenimiento preventivo y correctivo, seguimiento constante y un cronograma bien definido, se puede garantizar el funcionamiento óptimo y la seguridad de los recursos tecnológicos. Este plan no solo ayudará a minimizar los tiempos de inactividad y los costos de reparación, sino que también contribuirá a prolongar la vida útil de los equipos y sistemas, protegiendo al mismo tiempo la integridad de la información manejada por la DNBE.