



POLITÉCNICO COLOMBIANO
Jaime Isaza Cadavid

POLITECNICO COLOMBIANO JAIME ISAZA CADAVID

PLAN DE MANTENIMIENTO DE SERVICIOS
TECNOLÓGICOS

INFORMATICA CORPORATIVA

MEDELLIN

2025



Tabla de contenido

INTRODUCCIÓN.....	3
OBJETIVOS.....	4
Objetivo General.....	4
Objetivos específicos.....	4
Alcance del documento.....	4
Normatividad.....	4
Desarrollo del plan.....	6
Actividades de los responsables.....	6
Plan de mantenimiento.....	7
Actividades de mantenimiento preventivo.....	8
Seguimiento y Monitoreo.....	10
Riesgos.....	11
Glosario de términos.....	12
Anexos.....	14
Cibergrafía.....	15



INTRODUCCIÓN

El Politécnico Colombiano Jaime Isaza Cadavid, comprometido con el mejoramiento continuo, y en concordancia con el plan de desarrollo institucional, así como el modelo integrado de planeación y gestión (MIPG), establece un conjunto de actividades encaminadas a fortalecer y mantener los pilares de la seguridad de la información: Confidencialidad, Disponibilidad e integridad. En este sentido se establecen acciones de tipo preventivo y correctivo orientadas tanto al hardware como al software.

El soporte técnico en la institución es prestado en la actualidad por contratistas, quienes son los encargados de atender las solicitudes de primer nivel y en el caso de presentarse situaciones especiales en las que el primer nivel no pueda resolver, entrarían a revisar, apoyar y/o resolver los funcionarios o responsables de segundo nivel. Dependiendo del tipo de mantenimiento y su complejidad, sería ejecutado por unos u otros.

Como todo proceso o actividad se pueden presentar riesgos, sean positivos o negativos, razón por la cual se analizan y definen aquellos que puedan estar inmersos en el proceso. Además, como resultado del plan de mantenimiento, se establece el cronograma de actividades con los responsables respectivos y el seguimiento y monitoreo que permite controlar el proceso.



OBJETIVOS

Objetivo General

Definir el cronograma de actividades para prevenir y corregir los diferentes problemas técnicos que se presenten o puedan presentarse en la plataforma tecnológica del Politécnico Colombiano Jaime Isaza Cadavid, con el objetivo de asegurar su disponibilidad.

Objetivos específicos

1. Aportar al mejoramiento continuo institucional, por medio de la definición y estructuración del plan de mantenimiento tecnológico, para tener sistemas informáticos disponibles, confiables e íntegros.
2. Establecer mecanismos que permitan controlar posibles situaciones que afecten la continuidad del servicio, por medio de acciones preventivas, con el fin de mantener en un estado óptimo la infraestructura tecnológica y en consecuencia la calidad del servicio informático.
3. Definir fechas, actividades y responsables de acuerdo con funciones, roles y conocimiento específico, para de esta manera tener el control tanto sobre hardware y software, por medio de la ejecución del cronograma del plan de mantenimiento, así como de actividades de seguimiento y monitoreo definidas en este documento.

Alcance del documento

El plan de mantenimiento de infraestructura tecnológica, que es responsabilidad de la Coordinación de Informática Corporativa, inicia con la identificación de los tipos de activos tecnológicos a los que se les va a hacer el mantenimiento, la planeación de las actividades de mantenimiento preventivo y la identificación de la necesidad de mantenimiento correctivo, la ejecución del plan, el seguimiento y monitoreo de las actividades ejecutadas y finaliza con la evaluación del plan y el indicador de cumplimiento de este.

Los activos sobre los cuales se realiza el plan de mantenimiento está basado en el inventario de la dependencia de Bienes y Servicios y el inventario de servidores del Datacenter.

Normatividad

De acuerdo con lineamiento LI.ST.10: La dirección de tecnologías y sistemas de la información, o quien haga sus veces, debe implementar un plan de mantenimiento preventivo sobre toda la infraestructura y los Servicios Tecnológicos. (1)

G.ST.01 guía del dominio de servicios tecnológicos. (2)



POLITÉCNICO COLOMBIANO
Jaime Isaza Cadavid

En general Marco de referencia de arquitectura (3) y normatividad vigente y aplicable a este plan.



Desarrollo del plan

Actividades de los responsables

Identificar los activos tecnológicos: revisar el inventario de software y hardware de acuerdo con el número de inventario, y los servicios que se prestan. Este número de inventario es utilizado por la Coordinación de Informática Corporativa para la ejecución y control de los mantenimientos preventivos (según la periodicidad establecida) y correctivos (cuando presenten fallas o novedades en su funcionamiento) de los bienes tecnológicos de la Institución.

El mantenimiento preventivo permite disminuir el riesgo de daño o pérdida de los equipos. Consiste en revisar los servidores y equipos de informática periódicamente para evitar fallos o errores en el software como: sistema operativo, antivirus o programas ofimáticos.

El mantenimiento correctivo son las tareas que se llevan a cabo para dar solución a un fallo, una vez que éste se ha producido.

El mantenimiento preventivo y correctivo es realizado por el personal de la Coordinación y según el nivel tipo de mantenimiento o tipo de bien tecnológico por proveedores externos o fabricantes.

Los activos tecnológicos que estén en garantía, harán uso de ella según el acuerdo suscrito con el proveedor y el cronograma establecido por la Coordinación de Informática. Este será objeto de seguimiento y monitoreo por parte del personal de soporte técnico del área de Informática.

Niveles de mantenimiento:

- ✓ Primer nivel : Servidores y redes
- ✓ Segundo nivel : Software y aplicativos
- ✓ Tercer nivel : Equipos clientes

Niveles de prioridad:

- ✓ Alta
- ✓ Media
- ✓ Baja



ACTIVIDAD	RESPONSABLE
Mantenimiento de servidores	Profesional Universitario
Mantenimiento de la red	Profesional Universitario
Mantenimiento software antivirus	Profesional Universitario
Mantenimiento Directorio Activo	Auxiliar, Profesional Universitario
Mantenimiento Firewall	Profesional Universitario
Mantenimiento de las aplicaciones institucionales	Profesional Universitario
Equipos de escritorio y portátiles	Usuarios Mesa de ayuda Técnico

Plan de mantenimiento

Las interrupciones del servicio pueden ser causadas además por labores de mantenimiento y/o actualización. Estas interrupciones programadas afectan la disponibilidad del servicio y por lo tanto deben ser planificadas para minimizar el impacto. Se deben aprovechar franjas horarias de inactividad para realizar las tareas que implican la degradación o interrupción del servicio. (2)



Actividades de mantenimiento preventivo		
Actividad	Tarea	Periodicidad
<i>Mantenimiento de servidores:</i>	✓ Verificación estado de la virtualización: Memoria, almacenamiento, procesador.	✓ Mensual
	✓ Actualización de Firmware	✓ A necesidad
	✓ Revisión errores reportados en el log de la consola de virtualización.	✓ Semanal
	✓ Corrección y/o gestión de errores	✓ A necesidad
	✓ Inventario licencias vigentes	✓ Anual
	✓ Análisis y gestión de vulnerabilidades	✓ Semestral
	✓ Verificación de bases de datos de antivirus y actualizaciones del mismo.	✓ Mensual
	✓ Actualización del directorio activo en el servidor de dominio, usuarios vigentes y privilegios	✓ Diario
	✓ Verificación de estado de servidores físicos, lugar donde se encuentran (ambiente) y conexiones	✓ Semanal
<i>Mantenimiento de la red:</i>	✓ Revisión del estado físico de la red, Switches, puntos de acceso, WIFI	✓ Quincenal
	✓ Monitorización del estado de la red	✓ Diario
	✓ Control de acceso a la red	✓ Diario
	✓ Rotulación de cables	✓ Anual
	✓ Verificación estado de cableado tanto en servidores como oficinas	✓ Semestral
	✓ Pruebas de velocidad de red aleatorias	✓ Semestral
<i>Mantenimiento software antivirus:</i>	✓ Verificación cumplimiento de configuración de acuerdo con políticas definidas (actualización de Bases de datos y programa, ejecución en equipos)	✓ Semanal
	✓ Generar una copia completa del Estado del Sistema	✓ Semestral
	✓ Generar copia del DHCP	✓ Semestral



<i>Mantenimiento Directorio Activo:</i>	✓ Generar copia del DNS.	✓ Semestral
	✓ Restaurar copias de seguridad en el entorno de pruebas	✓ Semestral
	✓ Actualizar el software de seguridad y los paquetes instalados.	✓ A necesidad
	✓ Crear, modificar o mantener el sistema anti spam, antivirus y filtrado web.	✓ Mensual
	✓ Crear o modificar las políticas.	✓ A necesidad
	✓ Crear o modificar las cuentas de usuario.	✓ A necesidad
	✓ Solucionar incidencias.	✓ A necesidad
	✓ Actualizar las publicaciones hacia las diferentes zonas, sistema de antivirus perimetral, sistema de filtrado.	✓ A necesidad
<i>Mantenimiento de las aplicaciones institucionales:</i>	✓ Actualizar el sistema operativo	✓ A necesidad
	✓ Reconfigurar los respaldos	✓ A necesidad
	✓ Actualizar las aplicaciones	✓ A necesidad
	✓ Actualizar las extensiones (plugins), módulos o librerías.	✓ A necesidad
	✓ Instalar y configurar las nuevas extensiones (plugins), módulos o librerías.	✓ A necesidad
<i>Equipos de escritorio y portátiles</i>	✓ Verificación de estado de tarjetas de red	✓ Sujeto a solicitud de soporte técnico
	✓ Defragmentación de discos	✓ Sujeto a solicitud de soporte técnico
	✓ Limpieza del registro del Sistema	✓ Sujeto a solicitud de soporte técnico
	✓ Desinstalar aplicaciones que no se usan	✓ Sujeto a solicitud de soporte técnico
	✓ Borrar temporales y caché	✓ Sujeto a solicitud de soporte técnico
	✓ Revisar los programas de inicio	✓ Sujeto a solicitud de soporte técnico
	✓ Comprobación de actualizaciones	✓ A necesidad
	✓ Revisar el disco en busca de virus	✓ Semanal
	✓ Comprobación de errores del disco duro	✓ Sujeto a solicitud de soporte técnico



Seguimiento y Monitoreo

El seguimiento y monitoreo se realizará de acuerdo con la periodicidad del plan de mantenimiento y por medio de la herramienta de monitoreo definida por la dependencia.

Las ejecuciones que afecten la prestación del servicio de procesos institucionales, serán realizadas, previo acuerdo con el coordinador y el responsable de la dependencia en cuestión.

La periodicidad de todas y cada una de las actividades es de estricto cumplimiento, excepto en casos fortuitos que impidan la ejecución de estas.

Como resultado del plan de mantenimiento, el responsable de cada plan de mantenimiento deberá entregar el informe de la ejecución de este a la Coordinación de Informática Corporativa para su evaluación.

Indicador del plan

Fórmula:

(Número de tareas de mantenimiento ejecutadas / número de tareas de mantenimiento programadas) * 100

Medición: Anual

Techo: 85%



Riesgos

Riesgo	Efectos
Posibilidad de retraso en el desarrollo del plan mantenimiento por limitación de recursos (presupuestal, personal e insumos, imprevistos)	Se puede afectar la operatividad de los equipos y la prestación del servicio.
Posibilidad de cancelación del plan de mantenimiento por eventos fortuitos, ataques internos o externos	Se puede afectar en la disponibilidad de los servicios, la confidencialidad de los datos y la integridad de los mismos.



Glosario de términos

- Directorio Activo: es una estructura jerárquica que almacena información de objetos en la red. Un servicio de directorio activo, como Servicio de dominio del directorio activo (AD DS), proporciona los métodos para almacenar datos en un directorio, dejándolos disponibles a los usuarios de red y administradores. Por ejemplo, AD DS, almacena información de cuentas de usuario, tales como nombres, claves números de teléfono, etc..., y permite a otros usuarios autorizados en la misma red acceder esta información. (4)
- DHCP : (Dinamic Host configuration protocol), es un protocolo cliente – servidor utilizado en redes TCP/IP para proporcionar la configuración de los parámetros de red a un equipo, es decir, una dirección IP, una máscara de red, la dirección IP de la puerta de enlace, y la dirección IP de un servidor DNS. (5)
- DNS (Domain name Server); es un Sistema de nombres de dominio. Su función más común es la asignación de nombres de dominio a direcciones IP, la localización de los servidores de correo electrónico de cada dominio y la resolución inversa de direcciones IP. (6)
- DoS: (Denial of Service), « también conocido como ataque DoS (Denial-of-service attack)- es aquel que busca privar a los usuarios de acceso a su red o equipo. Una evolución de esta amenaza son los ataques de negación de servicio distribuido (DDoS) que se provocan al generar grandes cantidades de información desde varios puntos de forma voluntaria, para que el usuario o la organización se vean privados de un recurso ». (7)
- Firmware: « es un programa informático que permite que un dispositivo funcione tal y como el creador lo ha diseñado ». (8)
- IPS: « es un complemento a una configuración de IDS mediante la **inspección proactiva del tráfico entrante de un sistema** para eliminar las solicitudes maliciosas ». (9)
- « Mantenimiento correctivo Es el que se realiza de manera forzosa e imprevista, cuando ocurre un fallo, y que impone la necesidad de reparar el equipo antes de poder continuar haciendo uso de él ». (10)
- Mantenimiento preventivo: « es aquel que se hace con anticipación y de manera programada con el fin de evitar desperfectos, el mantenimiento preventivo consiste en dar limpieza general al equipo de cómputo y confirmar su correcto funcionamiento, en el caso de los computadores, el mantenimiento puede dividirse en dos, el que se le da al equipo (físico) o hardware y el que se le da a los programas instalados (lógicos) software ». (10)



- WSUS: « es un servicio que **permite la distribución de los parches y actualizaciones publicadas por Microsoft de forma centralizada** para todos los puestos cliente que corran con cualquier sistema operativo de Microsoft ». (11)
- VPN: « red privada virtual (virtual private network), es una herramienta digital que redirige tu tráfico de internet a través de un túnel seguro, ocultando tu dirección IP y encriptando tus datos. Así es como una VPN mantiene los datos privados y protege frente a ciberataques potenciales ». (12)



POLITÉCNICO COLOMBIANO
Jaime Isaza Cadavid

Anexos

Cronograma Plan de Mantenimiento Informática Corporativa.



**CronogramaPlanDe
Mantenimiento.pdf**



Cibergrafía

1. MINTIC. <https://mintic.gov.co/arquitecturati/630/w3-article-8842.html>. [En línea] [Citado el: 15 de Septiembre de 2021.] <https://mintic.gov.co/arquitecturati/630/w3-article-8842.html>.
2. MINTIC. *G.ST.01 Guía del dominio de servicios tecnológicos*. [En línea] 2019. [Citado el: 15 de Septiembre de 2021.] https://mintic.gov.co/arquitecturati/630/articles-9277_recurso_pdf.pdf.
3. MINTIC. *Marco de Referencia de Arquitectura*. [En línea] [Citado el: 15 de 09 de 2021.] <https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8118.html>.
4. Microsoft. *Active Directory Domain Services Overview*. [En línea] 31 de Marzo de 2017. <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>.
5. Moreno Pérez, Juan Carlos y Santos González, Manuel. *Sistemas Informáticos y Redes Locales*. Madrid : RA -MA, S.A. Editorial y Publicaciones, 2014.
6. Lederkremer, Miguel. *Redes Informáticas avanzado*. Autónoma de Buenos Aires : Six Ediciones, 2020.
7. pandasecurity.com. *Ataques DoS y DDoS*. [En línea] [Citado el: 28 de Septiembre de 2021.] <https://www.pandasecurity.com/es/security-info/network-attacks/>.
8. INTERNETPASOAPASO. *Firmware ¿Qué es, para qué sirve y cómo funciona este elemento de tus dispositivos?* [En línea] 2021. [Citado el: 28 de Septiembre de 2021.] <https://internetpasoapaso.com/firmware/>.
9. Industrial Cybersecurity. *IDS vs IPS ¿Cuál es la diferencia?* [En línea] 8 de Julio de 2020. [Citado el: 28 de Septiembre de 2021.] <https://www.ciberseguridadlogitek.com/ids-vs-ips-cual-es-la-diferencia/>.
10. bello.gov.co. *PLAN DE MANTENIMIENTO DE SERVICIOS TECNOLÓGICOS*. [En línea] 2019. [Citado el: 28 de Septiembre de 2021.] <https://bello.gov.co/images/archivos-mipg/TIC/PLAN-DE-MANTENIMIENTO-TICS-BELLO.doc#:~:text=Mantenimiento%20Preventivo%3A%20Es%20aquel%20que,puede%20dividir%20en%20dos%2C%20el>.
11. rootear. *Te explicamos qué es y para qué puedes usar WSUS en tu red Windows*. [En línea] 27 de Julio de 2014. [Citado el: 28 de Septiembre de 2021.] <https://rootear.com/windows/que-es-wsus>.
12. NordVPN. *¿Qué es una VPN y cómo funciona?* [En línea] 2021. [Citado el: 28 de Septiembre de 2021.] <https://nordvpn.com/es/download/#:~:text=Una%20VPN%20significa%20'red%20privada,pr otege%20frente%20a%20ciberataques%20potenciales..>