Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Estándar de TI: Políticas de Mantenimiento

18
CAPÍTULO

Estándar de TI:
Políticas de Mantenimiento

1.0 OBJETIVO

Garantizar que los recursos de tecnología de la información (TI) se mantengan de conformidad con las políticas, estándares y procedimientos de seguridad de TI.

2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

1. MANTENIMIENTO CONTROLADO

El Departamento de TI deberá:

a. Programar, realizar, documentar y revisar registros de mantenimiento y reparaciones de componentes del sistema de información de acuerdo con las especificaciones y/o requisitos del fabricante o proveedor realizados por entidades de TI locales y/o subcontratadas.
b. Aprobar y monitorear todas las actividades de mantenimiento, ya sea que se realicen en el sitio o de forma remota y si el equipo recibe servicio en el sitio o se traslada a otra ubicación.
c. Exigir que los propietarios del sistema aprueben explícitamente la eliminación del sistema de información o de los componentes del sistema de las instalaciones para mantenimiento o reparación fuera del sitio.
d. Desinfectar el equipo para eliminar toda la información de los medios asociados antes de retirarlo de las instalaciones de la Repartición para mantenimiento o reparaciones fuera del sitio.
e. Verificar todos los controles de seguridad potencialmente afectados para chequear que sigan funcionando correctamente después de las acciones de mantenimiento o reparación.
f. Incluir en los registros de mantenimiento la información relacionada con el mantenimiento definida por el propietario del sistema y de TI.
g. Para aquellos componentes que no están directamente asociados con el procesamiento de información, como escáneres, fotocopiadoras e impresoras, los registros de mantenimiento deben incluir la fecha y

hora del mantenimiento, la entidad que realiza el mantenimiento, el mantenimiento realizado, los componentes reemplazados o eliminados, incluidos los números de identificación/serie, según corresponda.

2. HERRAMIENTAS DE MANTENIMIENTO

El Departamento de TI deberá:

a. Asegurarse de que los propietarios del sistema y TI aprueben, controlen y supervisen las herramientas de mantenimiento del sistema de información.
b. Inspeccionar las herramientas de mantenimiento que el personal afín lleva a una instalación para detectar modificaciones inadecuadas o no autorizadas.
c. Verificar los medios que contienen programas de diagnóstico y prueba para detectar códigos maliciosos antes de utilizarlos en el sistema de información.

3. MANTENIMIENTO NO LOCAL

El Departamento de TI deberá:

a. Aprobar y monitorear las actividades de diagnóstico y mantenimiento no locales.
b. Permitir el uso de herramientas de diagnóstico y mantenimiento no locales solo según la política y documentados en el plan de seguridad del sistema de información.
c. Emplear autenticadores sólidos en el establecimiento de sesiones de diagnóstico y mantenimiento no locales.
d. Mantener registros de actividades de diagnóstico y mantenimiento no locales.
e. Finalizar las conexiones de red y de sesión cuando se complete el mantenimiento no local.
f. Documentar en el plan de seguridad del sistema de información, las políticas y procedimientos para el establecimiento y uso de conexiones no locales de mantenimiento y diagnóstico.

4. PERSONAL DE MANTENIMIENTO

El Departamento de TI deberá:

a. Establecer un proceso para la autorización del personal de mantenimiento y conservar una lista de organizaciones o personal autorizado.

b. Asegurar que el personal no acompañado que realiza el mantenimiento del sistema de información tenga las autorizaciones de acceso requeridas.
c. Designar personal con las autorizaciones de acceso requeridas y competencia técnica para supervisar las actividades de mantenimiento del personal que no posee las autorizaciones de acceso requeridas.

5. MANTENIMIENTO OPORTUNO

El Departamento de TI deberá:

a. Obtener soporte de mantenimiento y/o repuestos para sistemas de información según lo acordado dentro del acuerdo de nivel de servicio entre TI y el propietario del sistema.

3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC /SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

5.0 HISTORIAL DE REVISIONES

Fecha	Descripción de Cambio	Autores
18/07/24	Visado de documento	Pablo Zalazar, Alejandro Castro
30/07/24	Revisión de Documento, corrección de errores, ajuste de formato.	Alejandro Castro

6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53: mantenimiento del sistema (MA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-88, NIST SP 800-100; Estándares federales de procesamiento de información (FIPS) 140-2, FIPS 197, FIPS 201