Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Estándar de TI: Política de Protección de Medios

19
CAPÍTULO

Estándar de TI:
Política de Protección de Medios

1.0 OBJETIVO

Garantizar que la tecnología de la información (TI) controle el acceso y elimine los recursos multimedia 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. ACCESO A LOS MEDIOS:

TI, a través de la dirección de las reparticiones, deberá:

a. Restringir el acceso a tipos definidos de medios digitales y/o no digitales a personal identificado.
b. Marcar los medios del sistema de información indicando las limitaciones de distribución, las advertencias de manejo y las marcas de seguridad aplicables de los medios de información digitales y no digitales.

2. ALMACÉN DE DATOS

El Departamento de TI deberá:

a. Especificar el personal para controlar físicamente y almacenar de forma segura los medios dentro de áreas controladas definidas.
b. Proteger los medios del sistema de información hasta que los medios sean destruidos o desinfectados utilizando equipos, técnicas y procedimientos aprobados.

3. TRANSPORTE DE MEDIOS

El Departamento de TI deberá:

a. Proteger y controlar los medios durante el transporte fuera de áreas controladas.
b. Mantener la trazabilidad de los medios del sistema de información durante el transporte fuera de las áreas controladas.
c. Documentar las actividades asociadas al transporte de soportes de sistemas de información.
d. Restringir las actividades asociadas al transporte de soportes de sistemas de información al personal autorizado.

4. SANITIZACIÓN DE MEDIOS

El Departamento de TI deberá:

a. Desinfectar antes de desecharlo, liberarlo fuera del control de la organización o liberarlo para su reutilización utilizando un estándar especificado por la Repartición de acuerdo con las normas y políticas nacionales, provinciales y organizacionales aplicables.
b. Emplear mecanismos de sanitización con la solidez e integridad acorde a la categoría o clasificación de seguridad de la información.

5. USO DE MEDIOS

El Departamento de TI deberá:

Prohibir el uso de cualquier tipo de medio del sistema de información definidos por la Repartición en los equipos propios, utilizando medidas de seguridad no aprobadas.

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
19/07/24	Visado de documento.	Pablo Zalazar, Alejandro Castro
31/07/24	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: protección de medios (MP), NIST SP 800-12, NIST SP 800-56, NIST SP 800-57, NIST SP 800-60, NIST SP 800-88, NIST SP 800-100, NIST SP 800-111; NIST Estándares federales de procesamiento de información (FIPS)199.