



REGLAMENTO
DE
TECNOLOGÍA DE LA INFORMACIÓN,
DATOS Y CIBERSEGURIDAD

RI-REG-04

APROBADO POR RESOLUCIÓN
RUPMS N° 36/2025



ÍNDICE

REGLAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN, DATOS Y CIBERSEGURIDAD .	3
1. PRESENTACIÓN	3
2. OBJETIVOS	3
3. ÁMBITO DE APLICACIÓN	3
4. MARCOS NORMATIVOS	3
5. PRINCIPIOS.....	3
6. RESPONSABILIDADES	4
7. DISPOSICIONES GENERALES	4
8. SEGUIMIENTO	4
9. INCUMPLIMIENTOS.....	4



REGLAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN, DATOS Y CIBERSEGURIDAD

1. PRESENTACIÓN

Este reglamento establece las normas para el uso adecuado de los sistemas informáticos, gestión de datos institucionales, plataformas digitales y medidas de ciberseguridad en la UPMS.

2. OBJETIVOS

- ✓ Proteger sistemas, datos e infraestructura digital
- ✓ Regular uso de plataformas institucionales
- ✓ Establecer medidas de seguridad informática
- ✓ Garantizar privacidad y tratamiento adecuado de datos
- ✓ Prevenir riesgos digitales y vulneraciones

3. ÁMBITO DE APLICACIÓN

- ✓ Todo el personal administrativo, docente y estudiantes
- ✓ Todas las plataformas institucionales
- ✓ Equipos, redes, software, correo institucional
- ✓ Sedes y filiales

4. MARCOS NORMATIVOS

- ✓ Normas ISO 27001
- ✓ Ley de datos personales (si aplica según país)
- ✓ Estatuto UPMS
- ✓ Políticas institucionales de tecnología

5. PRINCIPIOS

- ✓ Confidencialidad
- ✓ Integridad
- ✓ Disponibilidad
- ✓ Seguridad
- ✓ Privacidad
- ✓ Uso responsable

6. RESPONSABILIDADES

Dirección de Administración y Finanzas – Unidad funcional dependiente

- ✦ Administra infraestructura digital
- ✦ Garantiza seguridad informática
- ✦ Gestiona accesos y permisos
- ✦ Mantiene respaldos institucionales

Usuarios (docentes, administrativos, estudiantes)

- ✦ Uso correcto de correo y plataformas
- ✦ Respetar políticas de contraseñas
- ✦ Reportar incidentes

7. DISPOSICIONES GENERALES

- ✦ El uso del correo institucional es obligatorio para comunicaciones oficiales.
- ✦ Las contraseñas deben ser personales y no compartirse.
- ✦ Prohibido instalar software no autorizado.
- ✦ Acceso a bases de datos según niveles de permiso autorizados.
- ✦ La UPMS mantendrá sistemas de respaldo y firewall.
- ✦ Incidentes de seguridad deben reportarse inmediatamente.

8. SEGUIMIENTO

- ✦ Auditorías de DTI
- ✦ Monitoreo de incidentes
- ✦ Indicadores de ciberseguridad

9. INCUMPLIMIENTOS

- ✦ Acceso no autorizado
- ✦ Violación de datos
- ✦ Instalación indebida
- ✦ Uso fraudulento de plataformas