



HEROICA
AGUA PRIETA

ADMINISTRACIÓN 2024-2027

**POLÍTICAS Y LINEAMIENTOS EN
MATERIA DE SEGURIDAD DE LA
INFORMACIÓN Y DE LOS SISTEMAS
INFORMÁTICOS DEL MUNICIPIO DE
AGUA PRIETA, SONORA**

Con fundamento en el Marco Integrado de Control Interno para la Administración Pública Estatal de Sonora, y con el propósito de fortalecer la protección de los activos de información, garantizar la continuidad de las operaciones y promover una adecuada administración de riesgos, se establecen las siguientes políticas y lineamientos:

I. OBJETIVO

Establecer las directrices y controles necesarios para proteger la confidencialidad, integridad, disponibilidad y trazabilidad de la información y de los sistemas informáticos del Municipio de Agua Prieta, Sonora, garantizando su uso adecuado y contribuyendo al cumplimiento de los objetivos institucionales.

II. ÁMBITO DE APLICACIÓN

Las presentes políticas son obligatorias para:

- Servidores públicos del Ayuntamiento.
 - Dependencias y entidades municipales.
 - Personal eventual o por honorarios.
 - Proveedores y terceros que tengan acceso a sistemas o información institucional.
-

III. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Toda la información y los sistemas informáticos deberán administrarse bajo los principios de:

1. **Confidencialidad**, garantizando que la información sólo sea accesible para las personas autorizadas.
 2. **Integridad**, asegurando que la información sea completa y no sea alterada indebidamente.
 3. **Disponibilidad**, garantizando que la información y los sistemas estén accesibles cuando se requieran.
 4. **Autenticidad**, verificando la identidad de los usuarios.
 5. **Trazabilidad**, permitiendo el registro y seguimiento de las operaciones realizadas.
-

IV. POLÍTICAS GENERALES

1. Administración de Usuarios y Contraseñas

- Cada usuario contará con credenciales individuales.
 - Las contraseñas deberán contener al menos ocho caracteres y combinar letras, números y símbolos.
 - Queda prohibido compartir contraseñas.
 - Los accesos deberán cancelarse cuando el servidor público concluya su relación laboral o cambie de funciones.
 - Anexo 1 Solicitud de alta, modificación o baja de usuarios
-

2. Uso de Equipos y Recursos Informáticos

- Los equipos de cómputo son para uso exclusivo de actividades institucionales.
 - Se prohíbe instalar programas no autorizados.
 - Los usuarios deberán mantener protegidos los equipos bajo su resguardo.
 - Los dispositivos institucionales deberán contar con antivirus actualizado y mecanismos de protección.
-

3. Protección de la Información

- La información generada por el Ayuntamiento constituye un activo institucional.
 - Deberá clasificarse conforme a su nivel de sensibilidad.
 - Los documentos que contengan datos personales deberán resguardarse de conformidad con la legislación aplicable.
 - Se limitará el acceso a la información únicamente al personal autorizado.
-

4. Respaldo y Recuperación de Información

- Se realizarán respaldos periódicos de las bases de datos y archivos críticos.
 - Los respaldos deberán almacenarse en medios seguros y, de ser posible, en una ubicación alterna.
 - Se efectuarán pruebas periódicas para verificar la recuperación de la información.
-

5. Seguridad en Redes y Comunicaciones

- El acceso a la red institucional deberá estar controlado.
 - Los equipos deberán contar con mecanismos de protección contra software malicioso.
 - Se restringirá el acceso a sitios o servicios que representen riesgos para la seguridad informática.
 - Anexo 2 Bitácora de control de acceso al área de servidores
-

6. Uso del Correo Electrónico Institucional

- El correo electrónico será utilizado exclusivamente para fines oficiales.
 - Se prohíbe abrir archivos o enlaces sospechosos.
 - Los usuarios deberán reportar mensajes fraudulentos o intentos de suplantación de identidad.
 - La información oficial deberá enviarse preferentemente mediante cuentas institucionales.
-

7. Gestión de Incidentes de Seguridad

- Todo incidente de seguridad deberá reportarse de manera inmediata al área responsable de tecnologías de la información.
 - Se documentarán los incidentes y las acciones correctivas implementadas.
 - Se promoverán medidas preventivas para evitar su recurrencia.
-

8. Continuidad de Operaciones

- Se establecerán procedimientos para garantizar la continuidad de los servicios informáticos esenciales.
 - Las áreas responsables deberán identificar los procesos críticos y los riesgos asociados.
 - Se implementarán medidas de recuperación ante contingencias.
-

9. Capacitación y Concientización

- Se promoverá la capacitación permanente del personal en materia de seguridad de la información.
 - Los servidores públicos deberán conocer las responsabilidades derivadas del manejo de la información institucional.
 - Se fomentará una cultura de prevención y administración de riesgos.
-

10. Supervisión y Evaluación

- El cumplimiento de estas políticas será supervisado por las áreas competentes.
 - Se realizarán revisiones periódicas para identificar áreas de mejora.
 - Las políticas podrán actualizarse cuando existan cambios normativos, tecnológicos o en los riesgos institucionales.
-

V. RESPONSABILIDADES

Unidad de Tecnologías de la Información

- Implementar controles de seguridad.
- Administrar usuarios y accesos.
- Mantener actualizados los sistemas y equipos.
- Realizar respaldos y monitoreo de la infraestructura tecnológica.

Titulares de las Dependencias Municipales

- Garantizar el cumplimiento de las presentes políticas.
- Identificar riesgos y reportar incidentes.
- Promover el uso adecuado de los recursos tecnológicos.

Servidores Públicos

- Salvaguardar la información bajo su responsabilidad.
 - Utilizar adecuadamente los sistemas informáticos.
 - Reportar cualquier vulnerabilidad o incidente detectado.
-

VI. CONTROL INTERNO Y ADMINISTRACIÓN DE RIESGOS

Las presentes políticas se alinean con los componentes del **Marco Integrado de Control Interno para la Administración Pública Estatal de Sonora**, particularmente con:

1. **Ambiente de Control.**
2. **Administración de Riesgos.**
3. **Actividades de Control.**
4. **Información y Comunicación.**
5. **Supervisión y Mejora Continua.**

VII. VIGENCIA

Las presentes **Políticas y Lineamientos en Materia de Seguridad de la Información y de los Sistemas Informáticos del Municipio de Agua Prieta, Sonora**, entrarán en vigor a partir de su aprobación por el Órgano de Control Gubernamental y Evaluación Gubernamental y permanecerán vigentes hasta en tanto sean modificadas o sustituidas por disposición expresa.

AUTORIZACIONES

FRANCISCO MONTOYA LEYVA	JESUS ALBERTO MORENO MORALES	MARIO FERNANDO SIERRA PALOMINO
  GOBIERNO MUNICIPAL ENCARGADO DE SISTEMAS AGUA PRIETA, SON. OFICIALIA MAYOR	  GOBIERNO MUNICIPAL HEROICA AGUA PRIETA, SON. OFICIALIA MAYOR	  H. AYUNTAMIENTO AGUA PRIETA, SONORA. ORGANO DE CONTROL Y EVALUACION GUBERNAMENTAL

FECHA DE ELABORACION: 12 DE JUNIO DEL 2026

FECHA DE APROBACION: 19-JUNIO-2026