Juárez Hidalgo
Gobierno Municipal
Honestidad, trabajo y progreso

HIDALGO
PRIMERO EL PUEBLO
2022-2028

POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD PARA LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIONES DEL MUNICIPIO DE JUÁREZ HIDALGO

ÍNDICE

1.Objetivo

Establecer las políticas y lineamientos que garanticen la seguridad, integridad, confidencialidad, disponibilidad y uso adecuado de los sistemas informáticos y de comunicaciones del Municipio de Juárez Hidalgo.

2. Alcance

Los presentes lineamientos aplican a todas las áreas del Municipio, así como a todo el personal que utilice, administre o tenga acceso a equipos de cómputo, redes, sistemas de información, dispositivos móviles, correo institucional y cualquier infraestructura tecnológica municipal.

3. Principios de Seguridad de la Información

- **Confidencialidad:** La información solo será accesible al personal autorizado.
- **Integridad:** La información debe mantenerse completa, precisa y sin alteraciones no autorizadas.
- **Disponibilidad:** Los sistemas deben permanecer accesibles y funcionales para las actividades oficiales.
- **Legalidad:** El uso de los sistemas deberá cumplir con la normatividad aplicable en materia administrativa y tecnológica.

4. Políticas y Lineamientos de Seguridad

4.1 Acceso a Sistemas y Equipos

- **Credenciales de acceso**
  - Todo usuario deberá contar con un nombre de usuario y una contraseña personal e intransferible para acceder a los sistemas y equipos institucionales.
  - Las contraseñas deberán ser **alfanuméricas**, con una longitud mínima de 8 a 12 caracteres, e incluir al menos una letra mayúscula, una letra minúscula y un carácter especial.
  - En casos especiales donde se requiera usar contraseñas **exclusivamente numéricas** (por compatibilidad con sistemas antiguos o dispositivos específicos), estas deberán ser **notificadas y registradas** por el área de Informática para su control y resguardo.
  - Las credenciales no deberán escribirse en papel, notas visibles o almacenarse sin protección en dispositivos personales.
- **Actualización y resguardo**
  - Las contraseñas deberán cambiarse **al menos cada 90 días** o cuando el sistema así lo solicite.

- En caso de sospecha de vulneración, pérdida o divulgación de la contraseña, el usuario deberá notificarlo inmediatamente al área de Informática para que se realice el reseteo y seguimiento correspondiente.
- Queda estrictamente prohibido compartir la contraseña con cualquier tercero, incluyendo compañeros de trabajo, directivos o personal externo.

- **Niveles de permisos y accesos privilegiados**
  - El acceso a sistemas sensibles, información clasificada o herramientas administrativas estará **limitado únicamente al personal autorizado**, de acuerdo con su función laboral y los niveles de permisos asignados.
  - El área de Informática será responsable de otorgar, modificar o revocar accesos, conforme a las solicitudes formales de cada área.
  - Los usuarios con permisos especiales (administradores, operadores o técnicos) deberán firmar un documento de responsabilidad y aceptar auditorías periódicas de uso.
- **Uso de equipos y sesiones**
  - Todo usuario deberá cerrar sesión al finalizar sus actividades, cambiar de área física o ausentarse del equipo por más de 5 minutos.
  - Los equipos deberán configurarse para activar el **bloqueo automático** después de un periodo máximo de 5 minutos de inactividad.
  - Queda prohibido dejar sesiones abiertas en equipos compartidos o de acceso público.
- **Acceso remoto y dispositivos externos**
  - Para acceder remotamente a sistemas institucionales, deberá utilizarse una conexión segura (VPN, portal seguro o doble autenticación) autorizada por el área de Informática.
  - El acceso desde dispositivos personales requerirá autorización previa y deberá cumplir con medidas mínimas de seguridad como antivirus actualizado y contraseña de bloqueo.
  - Está prohibido conectar dispositivos USB o discos externos no autorizados a equipos institucionales.
- **Supervisión y auditoría**
  - El área de Informática se reserva el derecho de supervisar el uso de credenciales, accesos, registros de actividad (logs) y comportamiento anómalo dentro de los sistemas.
  - Se podrán realizar auditorías periódicas para verificar el cumplimiento de esta política.
  - El incumplimiento de estas normas podrá derivar en suspensión de accesos, sanciones administrativas o medidas correctivas de acuerdo con la normatividad institucional.

4.2 Uso de los Recursos Informáticos

- Los recursos informáticos se utilizarán únicamente para actividades laborales.
- Queda prohibido instalar software sin autorización del área de Tecnologías de la Información (TI).
- No se permitirá el uso de dispositivos USB no autorizados por el área de TI.
- Se deberá evitar visitar sitios web no relacionados con actividades oficiales.

4.3 Seguridad en Redes y Comunicaciones

- Administración de la infraestructura:
  - Toda la infraestructura de red, incluyendo routers, switches, puntos de acceso, servidores y sistemas de comunicación, será administrada exclusivamente por el área de Tecnologías de la Información (TI). Ningún usuario o área podrá modificar configuraciones sin autorización expresa.
- Acceso seguro a la red interna:
  - El acceso a la red interna deberá contar con métodos de autenticación, segmentación por niveles de usuario y monitoreo continuo para garantizar la integridad del sistema.
  - Se implementarán redes separadas o de control estricto.
- Protección y filtrado de tráfico:
  - Se establecerán filtros, firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS) para evitar accesos no autorizados.
  - La red contará con herramientas contra malware, sitios maliciosos, descargas sospechosas y comportamiento anómalo.
- Correo institucional:
  - El correo electrónico institucional deberá utilizarse exclusivamente para fines laborales, siguiendo buenas prácticas de seguridad, tales como:
  - No abrir enlaces o archivos adjuntos de remitentes desconocidos.
  - Reportar intentos de phishing o correos sospechosos al área de TI.
  - No utilizar el correo institucional para registro en plataformas no autorizadas o con fines personales.
- Cifrado y comunicaciones seguras:
  - Toda transmisión de información sensible deberá realizarse mediante protocolos cifrados (HTTPS, SSL/TLS, VPN).
  - Las conexiones remotas solo podrán realizarse mediante canales seguros autorizados por TI.
- Uso de dispositivos conectados a la red:
  - Solo se permitirá conectar a la red institucional dispositivos autorizados y verificados por TI.

- Queda prohibido conectar equipos personales no autorizados, repetidores WiFi externos o internos y dispositivos no certificados sin autorización previa.
- Supervisión y registro de actividad:
- El área de TI mantendrá registros (logs) de acceso, actividad de red, intentos de intrusión y anomalías.

4.4 Protección de la Información

- La información institucional deberá respaldarse de forma periódica.
- Los respaldos deberán almacenarse en un sitio seguro y con acceso controlado.
- La información clasificada o sensible deberá manejarse conforme a protocolos establecidos.
- Queda prohibido divulgar información institucional sin autorización expresa.

4.5 Seguridad Física de Equipos y Servidores

- Los equipos de cómputo, servidores y dispositivos deberán ubicarse en áreas seguras y de acceso restringido.
- Se deberán implementar controles para evitar robo, daño o pérdida de equipos.
- El personal deberá reportar inmediatamente la pérdida o daño de cualquier dispositivo.

4.6 Gestión de Incidentes de Seguridad

- El personal deberá reportar inmediatamente virus, accesos no autorizados, fallas o cualquier incidente de seguridad.
- El área de TI deberá registrar, investigar y documentar todos los incidentes.
- En casos críticos, se podrán suspender temporalmente servicios o accesos para proteger la infraestructura.

4.7 Actualizaciones y Mantenimiento de Sistemas

- Todos los sistemas, redes y dispositivos deberán mantenerse actualizados.
- El área de TI será responsable de aplicar parches de seguridad, actualizaciones y mantenimiento preventivo.
- Se documentará todo cambio o actualización en los sistemas institucionales.

4.8 Uso de Dispositivos Móviles y Comunicación

- Los dispositivos móviles institucionales deberán usarse únicamente para tareas laborales.
- Todo acceso remoto deberá realizarse mediante protocolos seguros, con autorización previa.

- Las comunicaciones oficiales deberán realizarse preferentemente mediante los canales institucionales.

5. Responsabilidades

5.1 Área de Tecnologías de la Información

- Implementar, administrar y vigilar el cumplimiento de estos lineamientos.
- Mantener actualizados los sistemas y estructuras de seguridad.
- Brindar capacitación periódica al personal.

5.2 Titulares de Área

- Supervisar el uso adecuado de los recursos informáticos asignados a su personal.
- Reportar fallas, incidentes o irregularidades.

5.3 Servidores Públicos

- Cumplir con todas las políticas y lineamientos establecidos.
- Usar responsablemente los sistemas y equipos asignados.
- Reportar incidentes o vulneraciones.

Juárez Hidalgo
Gobierno Municipal
Honestidad trabajo y progreso

Aprobó
Ayuntamiento Municipal Constitucional
Administración 2024 - 2027

Prof. Luis Enrique Tapia Zapata
Presidente Municipal Constitucional

C. Ana Karen Tovar Muñoz
Síndico Propietaria

C. Elvira Ramos Bautista
Regidora

C. Karina Simón Ramos
Regidora

C. Sandra De La Cruz Lugo
Regidora

C. Víctor Iván Contreras Santiago
Regidor

C. Vianey Velázquez Ramos
Regidora

C. Prof. Edgar Ernesto Salcedo López
Regidor

Prof. Javier Salcedo Hernández
Regidor

C. Reyna Bautista Gómez
Regidora

Prof. Ezequiel Perusquia Muñoz
Regidor

Revisado y autorizado en sesión ordinaria de cabildo con fecha 03 de Diciembre del año 2025.