SAN FELIPE

# ORIZATLÁN

GOBIERNO MUNICIPAL **2024-2027**

## ¡UNA NUEVA ERA COMIENZA!

## H. AYUNTAMIENTO DE SAN FELIPE ORIZATLÁN, HIDALGO.

# PLAN DE LINEAMIENTOS Y POLÍTICAS DE SEGURIDAD INFORMÁTICAS

Elaboró:

Ing. Manuel Ulises Amaral Morales
Dir. De Informática y Sistemas.

Aprobó:

Dr. Carlos Cesar Pérez Escamilla
Presidente Municipal

Vo. Bo.

LAP. Sergio Flores Hernández
Contralor Municipal

## JUSTIFICACIÓN

La transformación digital en las administraciones públicas ha incrementado significativamente, por ende, la dependencia de los sistemas informáticos para la gestión de información, la prestación de servicios y la toma de decisiones estratégicas. En el caso del **H. Ayuntamiento de San Felipe Orizatlán**, el uso de herramientas tecnológicas es fundamental para el correcto funcionamiento de las distintas áreas administrativas, operativas y de atención ciudadana. Por ello, resulta indispensable establecer lineamientos y políticas de seguridad informática que garanticen el uso adecuado, responsable y seguro de los recursos tecnológicos institucionales.

La información que administra el Ayuntamiento —datos personales de ciudadanos, expedientes administrativos, información financiera, registros oficiales y comunicaciones internas— constituye un activo de alto valor. La ausencia de políticas claras puede derivar en riesgos como pérdida de información, accesos no autorizados, filtraciones de datos sensibles, ataques cibernéticos, uso indebido de los equipos o interrupciones en los servicios digitales. Estas situaciones no solo comprometen la integridad de los sistemas, sino también la confianza de la ciudadanía y la imagen institucional.

La implementación de lineamientos de seguridad permite establecer reglas claras sobre el uso de equipos de cómputo, redes, sistemas institucionales, contraseñas, correos electrónicos oficiales y dispositivos externos. Asimismo, define responsabilidades específicas para cada servidor público en el manejo de la información, promoviendo una cultura organizacional basada en la prevención, la confidencialidad y la protección de datos. Esto contribuye a reducir vulnerabilidades técnicas y humanas, que suelen ser una de las principales causas de incidentes de seguridad.

Además, contar con políticas formalmente establecidas fortalece los procesos internos de control y auditoría, facilita la estandarización de procedimientos y mejora la capacidad de respuesta ante incidentes tecnológicos. En un entorno donde las amenazas digitales evolucionan constantemente, resulta necesario que el Ayuntamiento adopte medidas preventivas que incluyan actualizaciones periódicas, respaldos de información, control de accesos y capacitación continua del personal.

La seguridad informática no debe considerarse únicamente como una medida técnica, sino como un elemento estratégico para garantizar la continuidad operativa, la transparencia administrativa y el cumplimiento de las disposiciones legales en materia de protección de datos. Implementar lineamientos claros permitirá optimizar recursos, minimizar riesgos y asegurar que los sistemas informáticos sean utilizados de manera eficiente y responsable.

En conclusión, la adopción de políticas y lineamientos de seguridad informática en el H. Ayuntamiento de San Felipe Orizatlán representa una acción necesaria y prioritaria para salvaguardar

la información institucional, fortalecer la confianza ciudadana y consolidar una administración pública moderna, segura y eficiente.

## PROBLEMÁTICA IDENTIFICADA

- Los equipos informáticos del Ayuntamiento se encuentran en estado comprometido, ya que estos presentan fallas y un estado físico de desgaste derivado de ser herencia de administraciones pasadas.
- Los equipos son obsoletos para desempeñar las actividades que la administración y atención ciudadana requieren hoy en día.
- Existen equipos que no cuentan con licenciamiento o software original.
- En muchos departamentos el personal no cuenta con las habilidades mínimas necesarias o capacitación suficiente para operar los equipos o software lo cual retrasa las actividades y atención ciudadana.
- No existe un plan de respaldo de información por área o generalizado, lo cual ocasiona que se reciba la administración con faltas de documentación, archivos o información entorpeciendo auditorias o actividades de entrega recepción.

## 1 POLÍTICAS DE SEGURIDAD PARA LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIONES.

### 1.1 Del uso aceptable de equipos y sistemas:

Los equipos de cómputo, redes, internet y sistemas institucionales deberán utilizarse exclusivamente para fines laborales y actividades oficiales del Ayuntamiento.

**Queda prohibido:**

- Instalar software no autorizado.
- Utilizar programas piratas.
- Acceder a sitios web de riesgo o contenido inapropiado.
- Usar los equipos para fines personales que comprometan la seguridad institucional.

### 1.2 Gestión de contraseñas

Todos los usuarios deberán:

- Utilizar contraseñas seguras (mínimo 8 caracteres con combinación de letras, números y símbolos).
- No compartir sus contraseñas con terceros.
- Cambiar periódicamente sus credenciales de acceso.
- No anotar contraseñas en lugares visibles.

El usuario es responsable del uso de su cuenta institucional.

### 1.3 Protección de la información

La información generada, almacenada o procesada en los sistemas municipales es confidencial y propiedad del Ayuntamiento.

Los usuarios deberán:

- Evitar copiar información en dispositivos USB sin autorización.
- No enviar información oficial desde correos personales.
- Proteger datos personales de ciudadanos conforme a la normativa aplicable.

### 1.4 Uso del correo institucional

El correo oficial deberá utilizarse exclusivamente para comunicaciones laborales.

Se prohíbe:

- Abrir enlaces o archivos sospechosos.
- Reenviar cadenas o información no relacionada con funciones institucionales.
- Compartir información sensible sin autorización.

El usuario deberá reportar correos sospechosos al área de Informática.

### 1.5 Respaldo y reporte de incidentes

Los usuarios deberán:

- Guardar su información en las ubicaciones designadas por el área de Informática.
- Permitir actualizaciones y mantenimientos programados.
- Reportar inmediatamente cualquier falla, virus, pérdida de información o acceso no autorizado.

No se deberán manipular configuraciones del sistema sin autorización técnica.

## 2 LINEAMIENTOS PARA LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.

### 2.1 Adquisiciones

Toda adquisición de equipo de cómputo, software, licencias o servicios tecnológicos deberá realizarse mediante solicitud formal y validación técnica del área de Informática, garantizando compatibilidad, estandarización, seguridad y eficiencia presupuestal.

### 2.2 Mantenimiento y Actualización

Los equipos y sistemas informáticos deberán someterse a mantenimiento preventivo y correctivo programado, así como a actualizaciones periódicas de seguridad, bajo la supervisión del área responsable de TIC.

### 2.3 Soporte Técnico

El soporte técnico deberá solicitarse a través de los canales oficiales establecidos, quedando prohibida la intervención no autorizada en equipos, redes o sistemas institucionales por parte de personal ajeno al área de Informática.

### 2.4 Desarrollo y Uso de Sistemas

El desarrollo, implementación o modificación de sistemas informáticos deberá cumplir con estándares de seguridad, protección de datos y normatividad vigente. El uso de las TIC deberá limitarse exclusivamente a fines institucionales.

### 2.5 Baja y Desecho Tecnológico

El desecho, reasignación o baja de equipos tecnológicos deberá realizarse mediante procedimiento administrativo formal, asegurando la eliminación segura de la información almacenada y el cumplimiento de normas ambientales y de protección de datos.

## 3 PLAN DE CONTINGENCIA CONTRA DESASTRES Y CONTINUIDAD DE OPERACIÓN.

**El presente plan aplica a:**

- Equipos de cómputo de todas las áreas municipales
- Servidores físicos o virtuales
- Redes y telecomunicaciones
- Sistemas institucionales y bases de datos
- Equipos de respaldo y almacenamiento

### 3.1 Identificación de riesgos

Se consideran como principales amenazas:

- Inundaciones
- Incendios
- Descargas eléctricas y variaciones de voltaje
- Sismos
- Fallas prolongadas de energía eléctrica

### 3.2 Medidas preventivas

#### 3.2.1 Respaldo de Información

- Realizar respaldos automáticos diarios de información crítica (Es responsabilidad de cada área generarlo y salva guardarlo).
- Mantener copias de seguridad en:
    - Dispositivo externo.
    - Nube institucional (cuando aplique).
    - Verificar periódicamente la integridad de los respaldos.

#### 3.2.2 Protección Eléctrica

- Instalar reguladores y UPS en equipos críticos.
- Implementar supresores de picos y tierras físicas adecuadas.

#### 3.2.3 Infraestructura Física

- Ubicar servidores en áreas elevadas y ventiladas. (Cuando aplique)
- Evitar instalación de equipos en zonas vulnerables a humedad o filtraciones.
- Señalizar y proteger cableado estructurado.

#### 3.2.4 Inventario y Documentación

- Mantener inventario actualizado de equipos.
- Registrar configuraciones críticas de red y sistemas.

### 3.3 Actuación durante desastre

1. Priorizar la seguridad del personal.
2. Desconectar equipos eléctricos si las condiciones lo permiten.

3. Resguardar dispositivos portátiles y respaldos físicos.
4. Notificar inmediatamente a la Dirección de Informática.
5. Activar protocolo de evaluación de daños.

### 3.4 Actuación posterior al evento

1. Evaluar daños físicos en equipos e infraestructura.
2. Verificar estado de servidores y sistemas críticos.
3. Restaurar información desde respaldos oficiales si fuera necesario.
4. Priorizar la recuperación de:
    - **Sistemas financieros (Tesorería, Recaudación).**
    - **Registro civil.**
    - **Catastro**
    - **Archivo Municipal**
    - **Plataformas de atención ciudadana**
5. Documentar incidencias y acciones correctivas.

### 3.5 Estrategia de Continuidad Operativa

Para evitar frenar la operación municipal:

- Habilitar equipos alternos de respaldo.
- Implementar trabajo remoto temporal si es viable.
- Utilizar respaldos en la nube para restablecer servicios prioritarios.
- Establecer un sitio alterno provisional para servicios críticos.

### 3.6 Responsables

- Dirección de Informática: Coordinación técnica y recuperación de sistemas.
- Dirección Administrativa: Gestión de recursos emergentes.
- Titulares de área: Resguardo de información bajo su responsabilidad.

### 3.7 Revisión y Actualización

El presente plan deberá revisarse anualmente o después de cualquier incidente significativo.