PROTOCOLO DE SEGURIDAD DE MANEJO DE LA INFORMACIÓN

CONCEJO DE SABANETA.

2024.

TABLA DE CONTENIDO.

Objetivos

El objetivo principal de estas políticas es asegurar la confidencialidad, integridad y disponibilidad de la información del Consejo Municipal, protegiendo sus activos digitales, recursos y operaciones, cumpliendo con las normativas vigentes y garantizando la continuidad de los servicios. Los objetivos específicos incluyen:

- Proteger la información sensible y confidencial del Consejo Municipal contra accesos no autorizados.
- Garantizar la integridad y exactitud de la información y los sistemas de información.
- Asegurar que los sistemas de información estén disponibles para el personal autorizado y los ciudadanos cuando sea necesario.
- Cumplir con todas las normativas y leyes aplicables relacionadas con la protección de la información.
- Fomentar una cultura de seguridad de la información entre el personal y los colaboradores.
- Establecer medidas de prevención, detección y respuesta a incidentes de seguridad.

Alcance

Estas políticas se aplican a todos los empleados, contratistas, proveedores y cualquier persona o entidad que maneje información del Consejo Municipal. Abarca el uso de sistemas, equipos de TI, información almacenada en cualquier medio y sistemas de comunicación que procesan información relacionada con el consejo.

Clasificación de la Información

Toda la información manejada por el Consejo Municipal se clasifica de la siguiente manera:

- **Pública**: Información accesible a cualquier ciudadano sin restricciones.
- **Confidencial**: Información cuyo acceso está limitado al personal autorizado debido a su sensibilidad.
- **Secreta**: Información de alta sensibilidad que podría afectar las operaciones o reputación del consejo si se divulga sin autorización.

Cada tipo de información debe manejarse con los niveles de seguridad adecuados para su clasificación

Control de Acceso

- El acceso a la información estará restringido según el rol y las responsabilidades de cada empleado.
- El personal solo tendrá acceso a la información que necesite para realizar sus funciones.
- El acceso a los sistemas de información estará protegido por contraseñas fuertes.

Uso Aceptable de los Sistemas de Información

- Los sistemas de información del Consejo Municipal deben utilizarse únicamente para fines laborales.
- Queda prohibido el uso de los recursos de TI para actividades ilegales o no autorizadas.
- Los usuarios no deben instalar software no autorizado ni modificar la configuración de seguridad de los sistemas.

Gestión de Contraseñas

- Las contraseñas deben cumplir con requisitos mínimos de complejidad: al menos 8 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.
- Las contraseñas deben cambiarse cada 90 días.
- Queda prohibido compartir contraseñas entre empleados o con terceros no autorizados.

Protección contra Amenazas

- Todos los sistemas de TI deben estar equipados con software antivirus y soluciones de detección y prevención de intrusiones.
- Se realizarán actualizaciones de seguridad y parches de software de forma periódica para proteger contra vulnerabilidades conocidas.
- Se implementarán cortafuegos para proteger la red interna de accesos no autorizados.

Gestión de Incidentes

- Se establecerá un protocolo de respuesta ante incidentes de seguridad para identificar, gestionar y resolver cualquier brecha de seguridad.
- Cualquier incidente o sospecha de incidente debe ser reportado inmediatamente al equipo de seguridad de la información.
- Se mantendrán registros detallados de todos los incidentes para su análisis y mejora continua.

Backup y Recuperación de Desastres

- Se implementará una política de copias de seguridad periódicas para asegurar la disponibilidad de la información crítica.
- Las copias de seguridad se almacenarán en ubicaciones seguras, tanto locales como externas (almacenamiento en la nube, centros de datos).
- Se realizarán pruebas periódicas de recuperación de datos para garantizar que las copias de seguridad sean funcionales.

Capacitación y Concientización

- Todo el personal debe recibir capacitación anual sobre seguridad de la información, riesgos cibernéticos y las políticas vigentes.
- Se fomentará una cultura de responsabilidad y concienciación en cuanto a la seguridad de la información a través de talleres, seminarios y campañas internas.

Cumplimiento Legal

- Las políticas de seguridad cumplirán con las normativas nacionales e internacionales aplicables, como la Ley de Protección de Datos Personales y las regulaciones locales sobre seguridad de la información.
- Se garantizará que el tratamiento de la información de los ciudadanos y empleados cumpla con los principios de licitud, consentimiento informado y protección adecuada.

Monitoreo y Auditoría

- Se realizará un monitoreo continuo de los sistemas de información para detectar comportamientos sospechosos o no autorizados.
- Se llevarán a cabo auditorías periódicas para asegurar el cumplimiento de estas políticas y evaluar posibles áreas de mejora.

Sanciones

El incumplimiento de las políticas de seguridad de la información por parte de los empleados o colaboradores externos podrá resultar en sanciones disciplinarias, incluyendo la terminación del contrato laboral o de servicios, y en casos graves, la notificación a las autoridades competentes.

Revisión y Actualización

Estas políticas serán revisadas y actualizadas anualmente o cuando sea necesario debido a cambios en las leyes, normativas o tecnología utilizada por el Consejo Municipal.

Esta política de seguridad proporciona una guía clara para proteger la información y los sistemas del Consejo Municipal, asegurando un entorno seguro y confiable para el manejo de datos.

Elaboro: **Anderson Adrian Niño Mora**
Analista de Infraestructura.
Fecha: 01/11/2024