Infraestructura y Seguridad

1) ¿La municipalidad cuenta con un departamento o equipo de TI dedicado a la ciberseguridad?

- Si
- No

2) Si la municipalidad cuenta con un equipo dedicado a la ciberseguridad, ¿cuántos funcionarios son parte de dicha unidad? (Indicar cargo y cantidad de personal)

---

3) ¿Dispone de un plan de seguridad de la información?

- Si
- No

4) ¿Cuántos funcionarios municipales tienen acceso a sistemas críticos de información? (Indicar cantidad)

---

5) ¿Qué tipo de autenticación utilizan para el acceso a sistemas municipales?

- Contraseña
- MFA
- Certificado Digital
- Otro (especificar): _____

6) ¿Se utilizan soluciones de monitoreo en tiempo real para detectar incidentes de ciberseguridad?

- Si
- No

7) ¿La municipalidad cuenta con software o herramientas SIEM? (Si cuenta indique cual o cuales)

---

8) ¿La municipalidad cuenta con software o herramientas SGSI? (Si cuenta indique cual o cuales)

---

9) ¿Cuáles son las herramientas que utilizan para las auditorías internas? (Si cuenta indicar cuáles)

---

10) ¿Se han realizado pruebas de penetración o análisis de vulnerabilidades en los sistemas municipales en los últimos 12 meses?

- Si
- No

11) ¿Se utilizan servicios en la nube para el almacenamiento de información municipal?

- Si
- No

Protocolos de Seguridad y Concienciación

12) ¿Se realizan capacitaciones en ciberseguridad para los funcionarios? (Si cuenta con capacitaciones indique frecuencia de ellas)

---

13) ¿Se han implementado políticas de contraseñas seguras?

- Si
- No

14) ¿Existe un protocolo de respuesta ante incidentes de ciberseguridad?

- Si
- No

15) ¿Se han realizado simulacros o auditorías de seguridad en los últimos 12 meses?

- Si
- No

Amenazas y Vulnerabilidades

16) ¿La municipalidad ha detectado ser víctima de algún ataque informático en los últimos dos años?

- Si
- No

17) ¿Cuántos ciberataques ha sufrido la municipalidad en 2023? (Número)

---

18) ¿Cuántos ciberataques ha sufrido la municipalidad en 2024? (Número)

---

19) ¿Cuál es la principal amenaza de ciberseguridad que enfrenta la municipalidad? (Phishing, Ransomware, Intrusiones, etc.)

---

20) ¿En caso de ataque, ha pagado alguna vez un rescate para recuperar la información?

- Si
- No

21) ¿Cuántos incidentes de ciberseguridad han sido reportados en el último año? (Número estimado)

---

22) ¿Se han registrado ataques de denegación de servicio (DDoS) contra los servicios en línea de la municipalidad?

- Si
- No

23) ¿Existe una política de respaldo y recuperación de datos?

- Si
- No

24) ¿Con qué frecuencia se realizan respaldos de la información municipal?
- Diarios
- Semanal
- Mensual
- Otra: _____
- Nunca

Cumplimiento Normativo y Estándares

25) ¿Ha implementado el marco NIST en la municipalidad?

- Si
- No

26) Si ha implementado el marco NIST, ¿qué versión del marco NIST tiene implementada? (Indicar versión)

- Si, Contamos con la version: _____
- No

27) ¿En qué nivel de implementación del marco NIST se encuentra la municipalidad? (Parcial, Intermedio, Completo), especificar avance por función.

_____

_____

28) ¿Cuáles han sido los principales desafíos en la implementación del marco NIST?

_____

_____

29) ¿Qué avances ha realizado la municipalidad en el cumplimiento de la Ley 21.663?

_____

_____

30) ¿Existen planes para mejorar el nivel de cumplimiento de la Ley 21.663 en los próximos años?

- Si
- No

31) ¿Cuáles son las principales dificultades para cumplir con la Ley 21.663? (Presupuesto, Falta de personal capacitado, Falta de normativas internas, etc.)

_____

_____

32) ¿Se cuenta con un equipo especializado en respuesta a incidentes de ciberseguridad (CSIRT interno o externo)?

- Si
- No

33) ¿Está certificada en algún estándar de seguridad, como ISO/IEC 27001?

- Si
- No

34) ¿Cuenta con un plan de continuidad operativa en caso de un ciberataque?

- Si
- No

35) ¿Dispone de un presupuesto asignado específicamente para ciberseguridad?

- Si
- No

36) ¿Existen procedimientos documentados para la gestión de accesos y permisos de usuarios?

- Si
- No

37) ¿Se ha realizado una evaluación formal de riesgos en ciberseguridad en los últimos dos años?

- Si
- No