ESPECIFICACIONES TÉCNICAS
PROPUESTA PÚBLICA
«MANTENCIÓN Y ADMINISTRACIÓN DE SERVICIOS INFORMÁTICOS»

La presente licitación demanda una gama de servicios, que tienen por objetivo incorporar una estructura que optimice la seguridad de la red de datos informática tanto interna como externa, contemplando mejoras e implementaciones de políticas de seguridad, control de tráficos, monitoreo continuo, establecer planes de trabajos y contingencias, respaldos de la información sensible y en general, cumplir con las exigencias que se describen a continuación:

1. **Mantención y mejoras para la red de comunicaciones de servidores y redes de datos municipales.**

   Se debe mejorar, mantener y auditar la estructura de la red municipal, implementando mejoras en las reglas, restricciones y permisos de tal forma que estas contribuyan a mejorar la fluidez de comunicación para los servidores, VPNs, equipos y conexiones LAN internas/externas de la Municipalidad de Lo Prado.

2. **Mantención y mejora de las políticas de comunicación desde exterior e interior de la red de datos municipal.**

   Mejorar el plan de mantención y creación de políticas de conexión del exterior y hacia el municipio de tal forma, que estas presenten un nivel óptimo de seguridad para los servidores y servicios relacionados con la red de datos municipal.

3. **Mantención, mejora y respaldo de los sistemas de correos.**

   Optimizar el funcionamiento del servicio de correos, respaldar las cuentas, realizar mantenciones a los servidores, servicios y restricciones, optimizando el plan de trabajo y contingencias ante eventuales fallos, ataques, vulnerabilidades, etc.

4. **Realizar mejoras y mantención a las políticas de seguridad y encriptación de datos en las comunicaciones de correo electrónico.**

   Auditar y mejorar el sistema de encriptado de correos para los usuarios del municipio por medio de certificados SSL por usuario o cuenta de correo electrónico. Esto en el marco de seguridad y privacidad de la información.

5. **Monitorear de forma continua, gráfica y estadística las comunicaciones de servidores y red de datos municipales.**

   Se debe monitorear de forma continua y estadística los respectivos flujos de comunicaciones, tanto de clientes finales, servidores y servicios de la Municipalidad, realizando entrega de informes a solicitud del departamento de informática frente a eventos u otros.

6. **Monitorear y reparar vulnerabilidades, mejorando la seguridad de las aplicaciones web y servicios municipales.**

   Monitorear periódicamente y realizar análisis de vulnerabilidades de seguridad para los aplicativos web del municipio, realizando las actualizaciones pertinentes y parches en caso de ser requeridos.

   Se deben realizar mantenciones preventivas y correctivas. En caso de existir anomalías en cuanto al funcionamiento de algún servicio, se debe informar a la ITS y proporcionar posibles soluciones y definir en conjunto los planes de acción.

7. **Detección, monitoreo y reparación de vulnerabilidades en servidores.**

   Analizar periódicamente las posibles vulnerabilidades a los servidores municipales considerando que la estructura actual, trabaja con distintas versiones en los sistemas operativos, se deben centrar en los servicios más críticos, como el servicio Web, Correo electrónico, la prioridad podrá ser informada por la ITS y en caso de que lo requiera, ser modificada en mutuo acuerdo.

   En caso de encontrar vulnerabilidades, se debe aplicar el plan de contingencia frente a eventuales problemas y soluciones a corto plazo. De no existir un plan de contingencia o no estar documentado, se deberá realizar, mejorar y documentar.

   Las actualizaciones de los diferentes servicios, se deben mantener al día y según los requerimientos actuales del municipio. Los planes de actualización, migración y trabajos sensibles que puedan afectar a la continuidad del servicio, deberán ser planificados en conjunto con la ITS.

8. **Diseño de parches de seguridad para sistemas, servidores, servicios y aplicaciones web.**

Se debe contar con un plan de diseño que permita desarrollar parches de seguridad que requieran los servicios, aplicaciones web y servidores, procurando no obstaculizar el flujo de información, comunicación y continuidad de los servidores y red municipal.

En caso de no existir el plan de contingencia o no estar documentado, se debe documentar según las necesidades del municipio.

9. **Mejora de los métodos de conexión al municipio.**

Se debe auditar y mejorar las actuales metodologías de conexión, asegurando que la información viaje por un canal completamente cifrado y seguro.

Se debe administrar un Firewall por cada dependencia municipal que lo requiera, realizando conexiones de las redes mediante una VPN en la cual garantice que la información viajará de forma segura, aplicando los respectivos métodos de cifrados y medidas de contingencias en caso de eventuales fallos.

En caso de implementar proyectos de conexiones con 3G, antenas punto a punto u otro similar que requieran de implementaciones u administración de firewalls, configuraciones de dispositivos, etc. El oferente deberá incorporar los nuevos dispositivos al servicio de configuración y administración sin costos adicionales.

10. **Servicios de Firewall intuitivo y autoadministrable.**

El servicio contempla incorporar un Firewall por dependencia municipal (actualmente 7) y en caso del edificio consistorial, dos máquinas Firewalls, estos deben ser configurados según las necesidades del municipio con el objetivo de controlar el tráfico de contenido, administrar el ancho de banda por host o segmentos de IP y/o MAC ADDR; deben ser capaces de administrar las restricciones de navegación, generar estadísticas, manejar información en línea y constante, poseer antivirus centralizado, anti-spam, contar con una interfaz gráfica de monitoreo y administración.

En la eventualidad de incorporar nuevas dependencias, estas deben ser incorporadas al servicio actual, con la configuración de Firewall respectivo y a demanda de la municipalidad.

En caso de no contar con las máquinas necesarias para la implementación de los Firewalls, el oferente debe recomendar la opción más viable para cada una de las dependencias que lo requiera.

11. Correo Corporativo Zimbra.

Actualmente el municipio cuenta con Zimbra V8.6, este servicio debe ser administrado, incorporando mejoras que ayuden a optimizar el flujo de correos, control de SPAM, propagación de virus, detección de cuentas posiblemente infectadas, bloqueo de ataques, detener infecciones y en general, tomar las medidas correspondientes para que el servicio opere de forma óptima.

En caso de ser necesario una actualización de versión del servicio, se debe coordinar con la ITS, el procedimiento y coordinaciones pertinentes, para ejecutar la actualización y proceso de migración.

12. Antivirus, sistema antispam y base de datos RBL municipal.

El servicio de correo y firewalls deberán contar con un antivirus y antispam, de los cuales se deben realizar mantención periódicas tanto en actualización de bases de datos de virus como en listas negras de clientes maliciosos, bloqueo de ataques que atenten con la integridad de la red y servicios del municipio, etc.

Las listas negras deben ser evaluadas en conjunto con la ITS y dependerán de las necesidades del municipio.

La base de datos RBL pertenecerá al municipio, se debe establecer un plan de mantención de listas negras, grises y blancas.

13. Mantención, mejora y monitoreo del servicio VPN con certificado.

Se deben realizar las mantenciones y mejoras al servicio VPN de tal forma que este sea estable, confiable y seguro.

El objetivo del servicio VPN es extender nuestra red interna a otros equipos o redes de otras dependencias que se encuentren físicamente ubicadas fuera del edificio consistorial y red interna del edificio consistorial.

Es imprescindible que la red VPN cuente con un cifrado y certificado acorde a las necesidades y que permita transmitir la información entre el cliente o redes externas de forma íntegra y por un canal seguro.

14. **Auditoría, estadística y respaldo de Navegación de red municipal y sus dependencias.**

Debe contar con una auditoría constante de las comunicaciones y tráficos de la red de datos municipales, realizando estadísticas de navegación por equipo o grupo de trabajo, mostrando de forma gráfica, intuitiva y en tiempo real, la interacción de los equipos.

Esta auditoría se debe extender y estar disponible para el caso de las dependencias externas del municipio, entendiéndose por estas, todas las dependencias que no se encuentren dentro del edificio consistorial de la municipalidad.

15. **Análisis y mejoras del plan de contingencia orientado a servidores, servicios y red de datos interna/externa municipal.**

Se debe mejorar el plan de contingencia para los eventuales fallos que puedan presentar los servidores, servicios y red de datos municipales, considerando tiempo de respuestas, solución y procedimientos a seguir.

En caso de no existir un plan de contingencia documentado, se debe realizar la documentación respectiva.

16. **Mantención y Restricciones de Páginas Web.**

Se deben realizar mantenciones a las reglas de navegación WEB y las restricciones pertinentes, éstas deben ser impartidas por instrucción de la ITS y se deben aplicar a todas las dependencias municipales que cuenten con el respectivo Firewall administrador por el oferente de la presente propuesta.

17. **Servicio de Respaldo/restauración programado y automatizado de cuentas de correo electrónico.**

Realizar respaldos de todas las cuentas de correos electrónicas mediante un sistema automatizado e incremental, en un repositorio que garantice la disponibilidad para cuando estos sean requeridos.

El sistema debe considerar configuraciones de servicios, carpetas y archivos críticos de los servidores para este fin.

En caso de requerir la restauración de alguna cuenta de correo, debe existir un medio automatizado, ya sea por script, sistema o servicio, que realice la restauración en el menor tiempo posible.

18. Mantención, análisis y mejoras para el sistema de respaldo de archivos municipal.

Se debe analizar el actual sistema de respaldos de archivos municipales, realizar las mantenciones pertinentes y proponer e implementar mejoras.

Este sistema debe ser accesible desde cualquier servidor que requiera los respaldos.

19. Mantención y mejoras del sistema de alerta de intrusos.

Se deben realizar las respectivas mantenciones preventivas/correctivas y mejoras de forma periódica al sistema de detección de intrusos o IDS de las redes municipales y sus servidores, teniendo como objetivo mantener en constante alerta frente a posibles detecciones de ataques informáticos, vulnerabilidades, problemas de servidores y/u otros.

20. Soporte telefónico 24/7, remoto y presencial.

Debe contar con soporte telefónico, remoto y presencial toda vez que estos sean requeridos, adicionalmente debe contar con una visita mensual, como mínimo, para efectos de presentar informes, mejoras, reuniones de planificación, proyectos, etc.

21. Diseño, implementación y mejoras de los manuales de procedimientos informáticos.

Se deben analizar los procedimientos y/o manual de procedimientos, realizando las mejoras respectivas de acuerdo a los estándares como por ejemplo, ITIL e ISO 27.001 orientados a la seguridad de sistemas y procedimientos informáticos.

En caso de no existir o no presentar documentación de dichos manuales, se deben diseñar e implementar.

22. Montaje de tecnologías de comunicación según demandas del municipio.

La empresa u oferente adjudicado, deberá presentar una carta de servicios que contemple proyectos de implementación, relacionados al área de informática. Estos servicios pueden ser desde el desarrollo de una plataforma web, módulos a demanda, proyectos de conexión, sites nuevos, alumbrado WiFi, etc.

Estos servicios se podrán contratar de forma anexa al contrato de licitación original y a demanda de la municipalidad de Lo Prado.

23. Monitoreo diario de detección de infecciones en equipos de planta conectados a la red municipal.

Se debe realizar un análisis periódico y continuo a equipos conectados a las redes LAN de la municipalidad y sus dependencias en caso de que se encuentren interconectadas, con el fin de detectar infecciones, hijacking, troyanos y accesos no autorizados.

24. Control de acceso remoto para la administración de servicios.

Se debe registrar la o las IPs autorizadas para realizar la administración remota de los servidores, máquinas, firewalls, servicios, etc. de tal modo que el oferente sea el que tenga acceso exclusivo a la administración y red interna de la municipalidad.

Todas las IPs externas que no se encuentren autorizadas para fines administrativos y acceso a la red de servidores, deben ser bloqueadas.

25. Respaldo de Site secundario en caso de contingencias.

Se debe implementar un Site de contingencia, ante eventuales fallos en condiciones de deterioro físico o lógicos del enlaces de datos principal.

Debe contar con un pool de al menos 3 IPs y un rack que permita un servicio de Housing a fin de mantener colas de correos, por ejemplo, o mantener de forma temporal el servicio web u otro de carácter indispensable.

26. Implementación de NOC y SOC.

El oferente debe realizar la implementación de un sistema NOC y SOC para monitorear la red y seguridad, otorgando informes de eventos fuera.

IMPORTANTE:

1. Los códigos fuentes, bases de datos, scripts, implementaciones, configuraciones y en general, cualquier producto desarrollado, configurado o implementado que no impliquen la compra de licenciamiento legal, serán de propiedad de la "Municipalidad de Lo Prado" y no del prestador del servicio.

2. La cantidad de máquinas a administrar, son cuantas sean necesarias para cumplir con una buena calidad de servicio, cumpliendo con las demandas de todos los puntos descritos en las presentes especificaciones técnicas.