**DICTAMEN TÉCNICO N° 11/2024**

*(Art 40 inc. a) Res DNCP N°4401 y Res DNCP N° 453 Art 12)*

**REFERENCIA:** RENOVACIÓN DE LICENCIA ANTIVIRUS

**Lugar y fecha:** Asunción, 2 de octubre de 2024
**UOC Convocante (*):** Dirección Operativa Contrataciones de la Auditoria General del Poder Ejecutivo
**Unidad o área requirente (*):** Dirección General de Tecnologías de la Información y Comunicación
**Funcionario o técnico responsable (*):** Lic. Carlos Montiel
**Dependencia y cargo que desempeña (*):** Director General de Tecnologías de la Información y Comunicación

- **Justificación técnica que respalda la objetividad, imparcialidad, regularidad y la razonabilidad o proporcionalidad de los requerimientos técnicos solicitados** (*).

La renovación de las licencias del software antivirus endpoint para la Auditoría General del Poder Ejecutivo (AGPE) responde a la necesidad imperiosa de asegurar la protección efectiva de los activos de información y garantizar el cumplimiento de las normativas nacionales e internacionales en materia de ciberseguridad. Los requerimientos técnicos que sustentan esta solicitud han sido formulados en base a los lineamientos del Ministerio de Tecnologías de la Información y Comunicación (MITIC), conforme a los estándares de software y los criterios mínimos de seguridad establecidos para el desarrollo y adquisición de software, de acuerdo a las resoluciones vigentes.

**Objetividad e Imparcialidad en la Renovación**

La renovación de las licencias antivirus endpoint es una medida objetiva e imparcial, fundamentada en los requerimientos técnicos y normativos establecidos por el MITIC, específicamente en el ***Estándar de Software****** y los ***Criterios Mínimos de Seguridad para el Desarrollo y Adquisición de Software***. Estos lineamientos se basan en estándares internacionales como ISO/IEC 27001 y 27002, que establecen requisitos precisos para la implementación y mantenimiento de controles de seguridad en los sistemas de información.

**Regularidad y Cumplimiento Normativo**

La AGPE tiene la obligación de cumplir con la normativa nacional en materia de seguridad de la información, especialmente en lo referido a la protección de datos sensibles y la preservación de la integridad de sus sistemas informáticos. El MITIC establece las directrices sobre seguridad de la información en instituciones del Estado, y dichas directrices obligan a que toda entidad pública disponga de soluciones de ciberseguridad actualizadas, como el antivirus endpoint, para mitigar riesgos de ciberataques, proteger la integridad de los datos y mantener la confidencialidad de la información gubernamental.

**Razonabilidad y Proporcionalidad de la Medida**

El volumen y la naturaleza de los datos que gestiona la AGPE justifican la proporcionalidad de la medida. La cantidad de dispositivos que requieren protección, así como la sensibilidad de la información auditada, exigen el uso de soluciones antivirus endpoint actualizadas, que respondan adecuadamente a la dinámica del ciberespacio, donde las amenazas evolucionan constantemente. Un software antivirus desactualizado o inexistente no sería capaz de enfrentar las nuevas variantes de malware, ransomware o ataques dirigidos, lo que aumentaría significativamente el riesgo de comprometer los sistemas de la AGPE.

**Consecuencias de No Contar con Protección Antivirus Endpoint**

La falta de protección antivirus en los equipos y sistemas de la AGPE puede generar consecuencias catastróficas:

Exposición a Amenazas Cibernéticas: Sin una solución de antivirus endpoint actualizada, los sistemas de la AGPE serían vulnerables a infecciones por malware, ransomware, spyware y otras amenazas cibernéticas, lo que podría resultar en la pérdida de datos críticos o en el acceso no autorizado a información confidencial.

Incumplimiento Normativo: No contar con una solución de seguridad eficiente podría implicar el incumplimiento de las normativas nacionales de seguridad de la información y las políticas emitidas por el MITIC, lo que derivaría en sanciones administrativas y posibles responsabilidades legales.

Interrupción Operativa: Un ciberataque que comprometa los sistemas de la AGPE podría paralizar sus operaciones, afectando el proceso de auditoría y revisión gubernamental, lo que comprometería el funcionamiento de todo el aparato estatal.

Pérdida de Confianza: La falta de protección adecuada podría afectar negativamente la imagen de la AGPE y del Gobierno en general, generando desconfianza en los ciudadanos y entidades que dependen de la información precisa y segura manejada por la institución.

**Referencias a Estándares Internacionales**

ISO/IEC 27001: Proporciona los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), alineándose con la necesidad de la AGPE de proteger la confidencialidad, integridad y disponibilidad de sus datos.

NIST SP 800-53: Directrices para la protección de los sistemas de información de las organizaciones públicas mediante controles técnicos y operativos que garantizan la seguridad continua.

**En conclusión**, la renovación de las licencias de antivirus endpoint para la AGPE es una medida necesaria, objetiva y proporcional, basada en parámetros técnicos y normativos que buscan garantizar la seguridad de la información y el cumplimiento con los estándares nacionales e internacionales de ciberseguridad. La no renovación de estas licencias expondría a la institución a riesgos graves que podrían afectar su funcionamiento y la confianza pública en sus servicios.

- **Identificar y justificar de forma expresa si algún requerimiento podría limitar la participación de potenciales oferentes**.

  **NO APLICA.**

- **Si en las bases licitatorias se indica una marca específica u otro derecho intelectual exclusivo, mencionar la justificación que respalda lo solicitado o que no existe otro modo de identificarlo. Se aclara que, en caso de incluirlos, los mismos tendrán carácter referencial**.

Considerando que es la renovación de licencias existentes, se especifica la marca Panda, que es derecho intelectual exclusivo de Panda Security, una empresa fundada en 1990 en Bilbao, España.

La renovación de las licencias del antivirus endpoint actualmente en uso en la Auditoría General del Poder Ejecutivo (AGPE) es una opción técnica y operativamente superior a la instalación de una nueva solución de seguridad. Esta decisión se fundamenta en la eficacia demostrada del sistema actual, el costo-beneficio de su continuidad y el cumplimiento de los requisitos de ciberseguridad establecidos por el Ministerio de Tecnologías de la Información y Comunicación (MITIC). A continuación, se detallan las razones clave que respaldan la renovación de las licencias existentes:

**Eficacia Comprobada y Confiabilidad**

El hecho de que con la solución antivirus endpoint actual no se hayan registrado casos de equipos infectados ni ciberataques exitosos es una evidencia contundente de su eficacia. Cambiar a una nueva solución podría introducir riesgos desconocidos y no probados en el entorno actual, donde la protección está asegurada por una solución que ha sido eficiente y confiable. Este historial favorable indica que la solución vigente está alineada con las amenazas cibernéticas presentes y que su arquitectura de seguridad ha brindado la protección necesaria.

Renovar las licencias del antivirus existente garantiza la continuidad de un sistema probado, sin la necesidad de enfrentar la curva de aprendizaje o los desafíos operacionales que conlleva una nueva implementación.

**Costos de Implementación y Adaptación Reducidos**

La instalación de una nueva solución antivirus implicaría costos adicionales y un uso considerable de recursos, tanto en términos financieros como de tiempo. Estos costos incluyen:

Adquisición de Nuevas Licencias: Dependiendo de la solución seleccionada, los costos iniciales de adquisición podrían ser significativamente mayores que los de la renovación de licencias actuales.

Capacitación del Personal: La adopción de un nuevo sistema implicaría la necesidad de capacitar al personal de la AGPE, tanto en su administración como en su uso, generando posibles interrupciones y un impacto temporal en la productividad.

Migración de Sistemas: El cambio a una nueva solución requeriría la migración de los sistemas actuales, lo que podría generar incompatibilidades técnicas o incluso ventanas de vulnerabilidad durante el proceso de instalación y configuración.

Optar por la renovación de las licencias actuales reduce estos costos a un mínimo, manteniendo la infraestructura de seguridad intacta y sin interrupciones.

**Compatibilidad con la Infraestructura Existente**

La solución antivirus actual ha sido configurada y optimizada para trabajar eficazmente con la infraestructura tecnológica de la AGPE. Implementar una nueva solución podría presentar desafíos de compatibilidad con los sistemas operativos, aplicaciones críticas y otros elementos de la red. Este riesgo es especialmente relevante en entornos gubernamentales, donde las interrupciones en los sistemas de seguridad podrían tener consecuencias serias para la continuidad de las operaciones.

La renovación garantiza la continuidad sin necesidad de ajustes adicionales o riesgos de incompatibilidad que podrían surgir con una nueva solución.

**Cumplimiento Normativo y Estándares de Seguridad**

El sistema antivirus en uso cumple con los lineamientos técnicos establecidos por el MITIC y con las normativas nacionales e internacionales en materia de ciberseguridad. No existe una necesidad normativa que obligue a cambiar la solución actual, y su continuidad permitirá mantener el cumplimiento con

estándares como ISO/IEC 27001, que exige soluciones de seguridad eficientes, continuas y actualizadas.

Cambiar a una nueva solución sin una razón técnica o normativa justificada podría generar retrasos o complicaciones en la auditoría del cumplimiento de seguridad de la información.

**Minimización de Riesgos de Transición**

Uno de los riesgos más grandes al cambiar a una nueva solución de seguridad es el período de transición. Durante este período, pueden surgir vulnerabilidades inesperadas, lo que aumenta las probabilidades de sufrir un ciberataque. Además, es posible que una nueva solución necesite un tiempo de ajuste para adaptarse a las necesidades específicas de la AGPE, lo que podría afectar temporalmente la eficiencia del sistema de protección.

Al renovar las licencias actuales, se elimina completamente este riesgo, ya que la solución en uso ha demostrado su eficacia en la protección contra amenazas sin necesidad de ajustes o periodos de transición.

**Optimización de Recursos y Planificación a Largo Plazo**

La renovación de las licencias garantiza una mejor optimización de los recursos al permitir que la AGPE continúe utilizando una solución que ha sido ajustada y adaptada a sus necesidades a lo largo del tiempo. Esta continuidad también facilita una planificación financiera y técnica más estable a largo plazo, evitando los gastos imprevistos y las dificultades operacionales asociadas con una implementación nueva.

**Conclusión**

Renovar las licencias de la solución antivirus endpoint actualmente implementada en la AGPE es la decisión más racional desde el punto de vista técnico, económico y de ciberseguridad. La solución ha demostrado ser efectiva al prevenir infecciones y

ataques cibernéticos, es completamente compatible con la infraestructura actual, y su continuidad garantiza el cumplimiento normativo sin incurrir en los riesgos y costos asociados con la adopción de una nueva herramienta.

**Obs.:**

-En caso de citar o remitirse al análisis o argumentos contenidos en otra documentación, se debe adjuntar la misma al presente dictamen.

-Podrán formar parte de los argumentos técnicos de este dictamen, el análisis previo citado en el artículo 25 de la Ley N° 7021/22, los resultados de dicho análisis o los documentos que lo integran.

**Firma del técnico o responsable del área requirente (*):**

**Aclaración (*):**

CARLOS RAUL MONTIEL FLORES

Firmado digitalmente por CARLOS RAUL MONTIEL FLORES
Fecha: 2024.10.02 13:32:32 -04'00'

**Firma del responsable UOC(*):**

**Aclaración (*):**

MARCOS DANIEL SOSA GONZALEZ

Firmado digitalmente por MARCOS DANIEL SOSA GONZALEZ
Fecha: 2024.10.03 08:23:11 -04'00'