DICTAMEN TÉCNICO DTIC

RECTIFICACIÓN DEL DICTAMEN TÉCNICO DTIC de fecha 10 de setiembre de 2025 (ampliación dela justificación)

REFERENCIA: En atención a las Observaciones por parte del MITIC sobre la Ampliación de la Justificación de las Especificaciones Técnicas.

LLAMADO PARA LA "ADQUISICION DE LICENCIAS DE CIBERSEGURIDAD CON INCORPORACIÓN DE TECNOLOGÍA EDR, EQUIPOS FIREWALL Y SWITCHES"

La Resolución DNCP N° 230/2025 "Por la cual se reglamentan los procedimientos de Contratación regidos por la Ley N° 7021/2022 "DE SUMINISTRO Y CONTRATACIONES PÚBLICAS", establece que para la realización de la comunicación que realice la convocante a la DNCP a través del SICP, a los efectos de la verificación y la difusión de los procedimientos de Contratación, además del PBC particular, deberá remitir mínimamente la siguiente documentación; Artículo 40° inc. *a) Dictamen técnico en el cual se sustenten las especificaciones técnicas requeridas en el procedimiento de contratación, suscrito por el responsable del área requirente o del técnico que las recomendó. En caso de que los mismos sugieran criterios de evaluación y/o condiciones de ejecución contractual, la fundamentación de tales sugerencias deberá formar parte del dictamen técnico.*

Lugar y Fecha: Asunción, 03 de octubre de 2025
UOC Convocante: Secretaría de Repatriados
Unidad o área requirente: Dirección de Tecnología de la Información y Comunicación
Funcionario o técnico responsable: Lic. Emilce Micaela Rojas
Dependencia y cargo que desempeña: Directora

Justificación Técnica para la Adquisición de Equipos y Software de Ciberseguridad

La presente justificación tiene como objetivo fundamentar la necesidad de adquirir nueva infraestructura de seguridad de la red de nuestra institución. La inversión en firewalls, switches de red y licencias de ciberseguridad con tecnología EDR es crítica para proteger los activos digitales, la información sensible de la ciudadanía y los sistemas internos, garantizando así la continuidad operativa y el cumplimiento de las normativas vigentes.

---

1. Adquisición de Firewalls

Los firewalls actúan como la primera línea de defensa, controlando y filtrando el tráfico de red entrante y saliente. La adquisición de un firewall moderno es fundamental por varias razones:

Protección contra amenazas externas: Bloquea ataques de malware, intentos de intrusión, denegación de servicio (DDoS) y otras amenazas que provienen de internet. Un firewall de próxima generación (NGFW) ofrece inspección profunda de paquetes (DPI) y prevención de intrusiones (IPS), lo que permite identificar y neutralizar amenazas sofisticadas que los firewalls tradicionales no pueden detectar.
Segmentación de la red: Permite dividir la red en zonas lógicas (por ejemplo, red de servidores, red de usuarios, red de invitados), aplicando políticas de seguridad específicas a cada segmento. Esto limita el movimiento de un atacante dentro de la red en caso de una brecha, una práctica conocida como segmentación de red.
Control de acceso y uso de aplicaciones: Permite a la institución controlar el acceso a aplicaciones web y servicios en la nube, optimizando el ancho de banda y garantizando que el uso de la red se alinee con las políticas de la organización.

2. Adquisición de Switches de Red

Los switches son componentes esenciales para la conectividad y el rendimiento de la red. Los switches gestionables de alta gama son necesarios para:

Rendimiento y escalabilidad: Un switch de alto rendimiento facilita la transferencia de datos a velocidades adecuadas para la carga de trabajo de la institución, reduciendo la latencia y mejorando la experiencia del usuario. Además, un switch escalable permite la incorporación de nuevos dispositivos y servicios en el futuro sin comprometer el rendimiento.

Segmentación y seguridad a nivel de red: Permiten la creación de redes virtuales (VLANs), una técnica que segmenta la red a nivel de capa 2. Esto aísla el tráfico entre diferentes grupos de usuarios o departamentos, previniendo el acceso no autorizado y conteniendo los efectos de un posible ataque.

Resiliencia y redundancia: La capacidad de configuración de los switches modernos permite implementar arquitecturas redundantes que garantizan la alta disponibilidad de la red. Si un switch falla, el tráfico puede ser automáticamente redirigido por otro, minimizando el tiempo de inactividad.

3. Adquisición de Licencias con Tecnología EDR

La tecnología EDR (Endpoint Detection and Response) representa un pilar crucial en la estrategia de ciberseguridad moderna, complementando la protección perimetral del firewall. Su función principal es la monitorización, detección y respuesta a amenazas que logran sortear las defensas iniciales.

Detección y respuesta proactiva: A diferencia de los antivirus tradicionales, que se basan en firmas para detectar amenazas conocidas, un EDR analiza el comportamiento de los procesos en los puntos finales (computadoras, servidores) para identificar actividades sospechosas que podrían indicar un ataque avanzado o desconocido (amenazas de día cero).
Visibilidad completa: Proporciona una visión centralizada de todo lo que ocurre en los dispositivos finales. Esto incluye el historial de procesos ejecutados, conexiones de red establecidas y cambios en el sistema, permitiendo a los equipos de TI investigar incidentes de seguridad de forma rápida y eficaz.
Capacidad de respuesta automatizada: Permite una respuesta inmediata ante una amenaza detectada. El EDR puede aislar automáticamente un dispositivo infectado de la red para evitar la propagación de un malware, o revertir los cambios maliciosos en el sistema.

4. Conclusión

La obsolescencia de los equipos de red y la creciente sofisticación de los ciberataques representan un riesgo significativo para la integridad y confidencialidad de la información de nuestra institución. La adquisición de firewalls de última generación, switches gestionables y licencias de ciberseguridad con tecnología EDR no es un gasto, sino una inversión estratégica. Esta medida fortalecerá nuestra postura de seguridad, protegerá los datos críticos y asegurará el cumplimiento de nuestras responsabilidades como entidad pública, garantizando la confianza de los ciudadanos y la operatividad de nuestros servicios.

Argumento sobre la Capacidad Técnica – Lote 2, Ítem 1 y 2

La infraestructura de seguridad a ser implementada requiere un plantel técnico robusto y certificado, que asegure tanto el diseño correcto como la ejecución y operación sin interrupciones. Por este motivo, se plantea la necesidad

de contar con perfiles en distintos niveles de certificación, cuya distribución garantiza la alta disponibilidad de personal especializado en cada etapa del proyecto.

1. Técnico certificado con nivel Experto y/o Arquitecto en Seguridad

Este perfil asegura la visión estratégica y de arquitectura de la solución, validando que el diseño cumpla con las mejores prácticas del fabricante y se integre de manera adecuada a la infraestructura existente. La presencia de un profesional de este nivel es esencial para anticipar riesgos, definir redundancias y establecer lineamientos de seguridad consistentes. Al contar con un recurso de tan alto nivel, se asegura la alta disponibilidad en la toma de decisiones críticas, evitando puntos únicos de falla en el diseño de la red y garantizando continuidad operativa.

2. Técnicos certificados con nivel Profesional y/o Especialista (2 recursos)

Los técnicos de nivel profesional son responsables de la implementación avanzada y configuración de políticas de seguridad en los dispositivos, siguiendo la arquitectura definida por el experto. La exigencia de contar con dos profesionales garantiza redundancia de personal para cubrir eventuales contingencias, y permite atender de manera simultánea múltiples frentes de configuración. De esta forma, se asegura la alta disponibilidad operativa durante la ejecución del proyecto y en el soporte posterior, evitando retrasos por dependencia de un único especialista.

3. Técnicos certificados con nivel Asociado (4 recursos)

El equipo de técnicos asociados respalda las tareas de despliegue, pruebas, documentación y soporte de primera línea. Su mayor número responde a la necesidad de contar con capacidad operativa suficiente para cubrir varios dispositivos y sitios de forma paralela, evitando cuellos de botella en las actividades de campo. La participación de cuatro recursos asociados garantiza que siempre exista disponibilidad inmediata de personal para atender incidentes, documentar cambios o realizar ajustes operativos, contribuyendo así a la estabilidad de la solución.

De esta manera, la combinación de 1 experto/arquitecto, 2 profesionales/especialistas y 4 asociados no solo asegura un diseño sólido y una implementación confiable, sino que además establece un esquema de alta disponibilidad de técnicos en todos los niveles, minimizando riesgos y garantizando la continuidad del servicio durante y después de la implementación.

4. Técnico certificado en ITIL v4 y/o Project Management Professional (PMP) (1 recurso)

Este perfil asegura la gestión integral del proyecto, aportando metodologías reconocidas internacionalmente para planificar, coordinar y supervisar cada una de las etapas de la consultoría e implementación. La certificación ITIL v4 garantiza la alineación con las mejores prácticas en gestión de servicios de TI, mientras que PMP avala la capacidad de administrar cronogramas, recursos y riesgos de manera eficiente. Contar con este recurso certificado permite asegurar la alta disponibilidad en la gestión y coordinación técnica, ya que actúa como punto de enlace entre el equipo técnico y el cliente, mitigando riesgos de descoordinación y asegurando que las actividades críticas se ejecuten en tiempo y forma.

Directora
Dirección de TIC

DICTAMEN TÉCNICO DTIC

LLAMADO PARA LA "ADQUISICION DE LICENCIAS DE CIBERSEGURIDAD CON INCORPORACIÓN DE TECNOLOGÍA EDR, EQUIPOS FIREWALL Y SWITCHES"

La Resolución DNCP N° 230/2025 "Por la cual se reglamentan los procedimientos de Contratación regidos por la Ley N° 7021/2022 "DE SUMINISTRO Y CONTRATACIONES PÚBLICAS", establece que para la realización de la comunicación que realice la convocante a la DNCP a través del SICP, a los efectos de la verificación y la difusión de los procedimientos de Contratación, además del PBC particular, deberá remitir mínimamente la siguiente documentación; Artículo 40° inc. *a) Dictamen técnico en el cual se sustenten las especificaciones técnicas requeridas en el procedimiento de contratación, suscrito por el responsable del área requirente o del técnico que las recomendó. En caso de que los mismos sugieran criterios de evaluación y/o condiciones de ejecución contractual, la fundamentación de tales sugerencias deberá formar parte del dictamen técnico.*

Lugar y Fecha: Asunción, 10 de setiembre de 2025
UOC Convocante: Secretaría de Repatriados
Unidad o área requirente: Dirección de Tecnología de la Información y Comunicación
Funcionario o técnico responsable: Lic. Emilce Micaela Rojas
Dependencia y cargo que desempeña: Directora

Justificación Técnica para la Adquisición de Equipos y Software de Ciberseguridad

La presente justificación tiene como objetivo fundamentar la necesidad de adquirir nueva infraestructura de seguridad de la red de nuestra institución. La inversión en firewalls, switches de red y licencias de ciberseguridad con tecnología EDR es crítica para proteger los activos digitales, la información sensible de la ciudadanía y los sistemas internos, garantizando así la continuidad operativa y el cumplimiento de las normativas vigentes.

1. Adquisición de Firewalls

Los firewalls actúan como la primera línea de defensa, controlando y filtrando el tráfico de red entrante y saliente. La adquisición de un firewall moderno es fundamental por varias razones:

Protección contra amenazas externas: Bloquea ataques de malware, intentos de intrusión, denegación de servicio (DDoS) y otras amenazas que provienen de internet. Un firewall de próxima generación (NGFW) ofrece inspección profunda de paquetes (DPI) y prevención de intrusiones (IPS), lo que permite identificar y neutralizar amenazas sofisticadas que los firewalls tradicionales no pueden detectar.
Segmentación de la red: Permite dividir la red en zonas lógicas (por ejemplo, red de servidores, red de usuarios, red de invitados), aplicando políticas de seguridad específicas a cada segmento. Esto limita el movimiento de un atacante dentro de la red en caso de una brecha, una práctica conocida como segmentación de red.
Control de acceso y uso de aplicaciones: Permite a la institución controlar el acceso a aplicaciones web y servicios en la nube, optimizando el ancho de banda y garantizando que el uso de la red se alinee con las políticas de la organización.

2. Adquisición de Switches de Red

Los switches son componentes esenciales para la conectividad y el rendimiento de la red. Los switches gestionables de alta gama son necesarios para:

Rendimiento y escalabilidad: Un switch de alto rendimiento facilita la transferencia de datos a velocidades adecuadas para la carga de trabajo de la institución, reduciendo la latencia y mejorando la experiencia del usuario. Además, un switch escalable permite la incorporación de nuevos dispositivos y servicios en el futuro sin comprometer el rendimiento.

Segmentación y seguridad a nivel de red: Permiten la creación de redes virtuales (VLANs), una técnica que segmenta la red a nivel de capa 2. Esto aísla el tráfico entre diferentes grupos de usuarios o departamentos, previniendo el acceso no autorizado y conteniendo los efectos de un posible ataque.

Resiliencia y redundancia: La capacidad de configuración de los switches modernos permite implementar arquitecturas redundantes que garantizan la alta disponibilidad de la red. Si un switch falla, el tráfico puede ser automáticamente redirigido por otro, minimizando el tiempo de inactividad.

3. Adquisición de Licencias con Tecnología EDR

La tecnología EDR (Endpoint Detection and Response) representa un pilar crucial en la estrategia de ciberseguridad moderna, complementando la protección perimetral del firewall. Su función principal es la monitorización, detección y respuesta a amenazas que logran sortear las defensas iniciales.

Detección y respuesta proactiva: A diferencia de los antivirus tradicionales, que se basan en firmas para detectar amenazas conocidas, un EDR analiza el comportamiento de los procesos en los puntos finales (computadoras, servidores) para identificar actividades sospechosas que podrían indicar un ataque avanzado o desconocido (amenazas de día cero).
Visibilidad completa: Proporciona una visión centralizada de todo lo que ocurre en los dispositivos finales. Esto incluye el historial de procesos ejecutados, conexiones de red establecidas y cambios en el sistema, permitiendo a los equipos de TI investigar incidentes de seguridad de forma rápida y eficaz.
Capacidad de respuesta automatizada: Permite una respuesta inmediata ante una amenaza detectada. El EDR puede aislar automáticamente un dispositivo infectado de la red para evitar la propagación de un malware, o revertir los cambios maliciosos en el sistema.

4. Conclusión

La obsolescencia de los equipos de red y la creciente sofisticación de los ciberataques representan un riesgo significativo para la integridad y confidencialidad de la información de nuestra institución. La adquisición de firewalls de última generación, switches gestionables y licencias de ciberseguridad con tecnología EDR no es un gasto, sino una inversión estratégica. Esta medida fortalecerá nuestra postura de seguridad, protegerá los datos críticos y asegurará el cumplimiento de nuestras responsabilidades como entidad pública, garantizando la confianza de los ciudadanos y la operatividad de nuestros servicios.

Directora