Consultas Realizadas

Licitación 487252 - Licencias de Correo y Plataforma Endpoint de proteccion para PC y Servidores

Consulta 1 - Fuentes de red, identidad y SIEM

Consulta	Fecha de Consulta	11-09-2026

Considerando que las EETT requieren correlación nativa entre eventos provenientes de endpoint, servidores, red, autenticación e inteligencia de amenazas, solicitamos indicar las soluciones actualmente utilizadas por la institución para seguridad de red/perimetral, autenticación/gestión de identidades y SIEM, detallando fabricante y producto, a efectos de dimensionar las integraciones requeridas por la solución XDR.

Respuesta	Fecha de Respuesta	24-09-2026

Señores potenciales oferentes: El requerimiento establecido para la plataforma XDR no fue concebido como una integración dependiente de una marca determinada, sino como una capacidad funcional y arquitectónica. El PBC exige correlación nativa entre eventos de endpoint, servidores, red, autenticación e inteligencia de amenazas, además de la posibilidad de remitir eventos de forma continua y automatizada hacia sistemas externos de correlación mediante mecanismos estandarizados como syslog/CEF y/o API REST documentada. Técnicamente, esto permite que la solución ofertada sea evaluada por su capacidad real de interoperabilidad, correlación y automatización, evitando que el cumplimiento quede condicionado a un único fabricante.
La identificación de las soluciones actualmente utilizadas por la Institución constituye información de contexto operativo y no modifica la obligación principal del oferente: la plataforma propuesta deberá disponer de los conectores, interfaces y capacidades necesarias para integrarse con las fuentes institucionales que correspondan durante la implementación, manteniendo la correlación exigida y sin degradar las funcionalidades solicitadas. A efectos de completar la aclaración con la información institucional disponible, podrán consignarse los siguientes datos:
Como seguridad de red Perimetral tenemos un equipo Palo Alto, Cloud Sophos Email Security y Cloud Forti EDR
Los agentes deberán ser instalados en servidores Linux Server y Windows Server, además en PC de escritorio con Windows.
Por lo tanto, remitirse a lo establecido en el PBC.

Consulta 2 - ¿Se requiere monitoreo/MDR o solamente la plataforma?

Consulta	Fecha de Consulta	11-09-2026

Respecto al requisito que establece que el proveedor deberá notificar todo incidente de seguridad crítico o de alta severidad dentro de las cuatro horas de su confirmación, solicitamos aclarar si la contratación incluye un servicio de monitoreo continuo, MDR/SOC o análisis administrado de incidentes por parte del proveedor, o si dicha obligación corresponde únicamente a incidentes identificados y escalados durante la prestación del soporte técnico de la solución.

Respuesta	Fecha de Respuesta	24-09-2026

Señores potenciales oferentes: La obligación de notificar incidentes críticos o de alta severidad dentro de las cuatro (4) horas de su confirmación se mantiene como un control de seguridad obligatorio asociado a la operación de la plataforma y al soporte técnico contratado. El PBC exige capacidades de detección, correlación, investigación y respuesta, por lo que el adjudicatario debe contar con un procedimiento operativo que permita identificar, confirmar, escalar y comunicar oportunamente los incidentes que se encuentren dentro del alcance de la solución.
El PBC no incorpora como prestación independiente un servicio MDR/SOC 24x7 distinto del objeto contratado. En consecuencia, la cláusula no debe interpretarse como la creación de un servicio administrado adicional no previsto, sino como una obligación de gestión y comunicación para todo incidente que sea confirmado por la solución y/o por el proveedor durante la prestación del soporte, manteniéndose además la obligación de emitir el informe post-incidente dentro del plazo establecido. La finalidad técnica es evitar que un evento de severidad crítica o alta permanezca sin escalamiento institucional una vez confirmado.
Por lo tanto, remitirse a lo establecido en el PBC.

Consulta 3 - Código fuente / Escrow

Consulta	Fecha de Consulta	11-09-2026

Considerando que la solución requerida corresponde a software comercial estándar bajo modalidad SaaS, solicitamos confirmar que el requisito relativo a entrega de código fuente o depósito mediante Escrow será aplicable únicamente en caso de desarrollos de software a medida, no resultando exigible para plataformas comerciales propietarias licenciadas bajo modalidad de suscripción.

Respuesta	Fecha de Respuesta	24-09-2026

Señores potenciales oferentes: Se mantiene la redacción prevista en el PBC. El requisito establece expresamente la entrega de documentación técnica y, “en caso de resultar necesario”, la entrega del código fuente con sus manuales o su depósito a cargo de un tercero mediante un mecanismo de Escrow. La expresión utilizada configura una previsión de continuidad y resguardo técnico que debe permanecer disponible para los supuestos en que, por la naturaleza de la solución, su arquitectura, las condiciones de licenciamiento o un evento de discontinuidad, resulte necesario asegurar la continuidad operativa y la capacidad de recuperación institucional.
Técnicamente, la figura de Escrow constituye una salvaguarda frente a escenarios de discontinuidad del fabricante, imposibilidad sobreviniente de soporte, cese del proveedor o situaciones en las que la Institución necesite preservar elementos indispensables para mantener el servicio. La cláusula no implica que toda plataforma SaaS propietaria deba transferir automáticamente su código fuente en condiciones incompatibles con su modelo de licenciamiento; su aplicación debe realizarse conforme a la literalidad del PBC y a la condición de necesidad allí prevista. Por ello, no corresponde su eliminación ni su sustitución.
Por lo tanto, remitirse a lo establecido en el PBC.

Consulta 4 - Garantía de 8 años/perpetuidad vs suscripción de 2 años

Consulta	Fecha de Consulta	11-09-2026

Considerando que el objeto corresponde a una solución comercial bajo modalidad SaaS y licenciamiento por suscripción por un periodo de dos años, solicitamos confirmar que las disposiciones relativas a funcionamiento perpetuo y garantía posterior por ocho años, incluidas en la sección de garantía general de software, no resultan aplicables al licenciamiento SaaS objeto de la presente contratación, siendo aplicable la garantía de buen funcionamiento establecida específicamente para el ítem durante el periodo contractual de dos años.

Respuesta	Fecha de Respuesta	24-09-2026

Señores potenciales oferentes: El PBC diferencia dos conceptos técnicos distintos: por una parte, la vigencia del derecho de uso o suscripción de la solución, fijada para el ítem correspondiente en dos (2) años; y, por otra, las obligaciones de garantía y responsabilidad vinculadas a vicios ocultos, fallas o defectos atribuibles al software. La vigencia de una suscripción determina durante cuánto tiempo se encuentra habilitado el servicio y sus funcionalidades licenciadas, mientras que la garantía regula la responsabilidad del proveedor respecto de defectos que tengan origen en el software suministrado o implementado.
En consecuencia, la previsión general de garantía no debe interpretarse como una conversión automática de una suscripción temporal en una licencia perpetua ni como una extensión gratuita del derecho de uso más allá de su vigencia contractual. Sin embargo, tampoco corresponde excluir en forma general las obligaciones de garantía previstas en el PBC, las cuales se aplicarán en el alcance que resulte técnicamente compatible con la naturaleza de cada componente y, especialmente, respecto de vicios ocultos o defectos originados en el código fuente y/o código objeto. Para el ítem SaaS se mantiene asimismo la garantía específica de buen funcionamiento durante el periodo de suscripción de dos (2) años.
Por lo tanto, remitirse a lo establecido en el PBC.

Consulta 5 - Distribución de los 70 servidores y CentOS Stream

Consulta	Fecha de Consulta	11-09-2026

A efectos de validar compatibilidad y dimensionamiento, favor indicar, si se encuentra disponible, la cantidad aproximada de servidores por sistema operativo y versión, especialmente los equipos que utilizan CentOS Stream, incluyendo la versión actualmente desplegada.

Respuesta	Fecha de Respuesta	24-09-2026

Señores potenciales oferentes: El dimensionamiento mínimo exigido en el PBC se encuentra definido por la cobertura de setenta (70) servidores y por la compatibilidad obligatoria con los sistemas operativos expresamente enumerados. La distribución interna de los servidores por sistema operativo puede variar durante la vigencia contractual por actualizaciones, migraciones, altas, bajas o cambios de plataforma; por esta razón, el requisito fue definido en términos de cobertura total y matriz de compatibilidad, y no mediante una cantidad rígida por sistema operativo.
En consecuencia, la solución ofertada deberá acreditar soporte para los sistemas operativos indicados en el PBC, incluido CentOS Stream, independientemente de la distribución puntual existente al momento de la oferta. La información que sigue puede ser consignada únicamente como dato operativo de referencia, sin alterar el alcance ni reducir la obligación de compatibilidad:
Distribución aproximada actual de los 70 de los cuales 60 son servidores Linux (Ubuntu Server, Debian) y Windows Server 2019 y 2022
Por lo tanto, remitirse a lo establecido en el PBC.

Consulta 6 - Alcance de los 90 días de retención

Consulta	Fecha de Consulta	11-09-2026

Favor aclarar si el requisito de conservación de telemetría y eventos de seguridad por un periodo mínimo de 90 días en línea aplica exclusivamente a la telemetría generada por los agentes instalados en estaciones de trabajo y servidores, o también a la totalidad de eventos provenientes de fuentes externas integradas a la plataforma XDR.

Respuesta	Fecha de Respuesta	24-09-2026

Señores potenciales oferentes: El requisito de conservación mínima de noventa (90) días en línea tiene como finalidad garantizar capacidad efectiva de investigación retrospectiva, threat hunting, reconstrucción de la línea de tiempo de incidentes y correlación histórica. Por tanto, debe comprender la telemetría y los eventos de seguridad que sean recolectados, procesados, correlacionados y almacenados por la plataforma XDR dentro del alcance de la solución, incluidos los eventos provenientes de fuentes externas que efectivamente sean integrados e ingeridos por la plataforma.
La exigencia de retención es independiente de la obligación adicional de exportar eventos hacia sistemas externos de correlación. El envío a un SIEM externo no sustituye ni reduce la capacidad de búsqueda y exportación que debe permanecer disponible en la propia plataforma durante el periodo mínimo establecido. Este criterio es técnicamente necesario para que la investigación no dependa exclusivamente de sistemas de terceros y para preservar la trazabilidad de los eventos gestionados por la solución contratada.
Por lo tanto, remitirse a lo establecido en el PBC.

Consulta 7 - Volumen de logs para dimensionamiento

Consulta	Fecha de Consulta	11-09-2026

En caso de requerirse la ingestión de eventos provenientes de soluciones de terceros (firewall, sistemas de autenticación, SIEM u otras fuentes), favor indicar el volumen aproximado de eventos o datos generado diariamente, expresado preferentemente en GB/día, o facilitar la información disponible para su dimensionamiento.

Respuesta	Fecha de Respuesta	24-09-2026

Señores potenciales oferentes: El PBC no establece una contratación basada en una cuota específica de ingestión expresada en GB/día ni define un servicio separado de almacenamiento de logs de terceros. El dimensionamiento funcional se encuentra determinado por la cobertura de 480 estaciones de trabajo y 70 servidores, la correlación de múltiples fuentes, la retención mínima de 90 días para la telemetría y eventos gestionados por la plataforma, y la interoperabilidad requerida mediante interfaces y protocolos documentados.
En consecuencia, el oferente deberá dimensionar su arquitectura y licenciamiento para cumplir integralmente dichas capacidades sin trasladar a la Institución limitaciones técnicas que impidan alcanzar los requisitos del PBC. Si la Institución dispone de una métrica consolidada de generación de eventos, podrá informarse como dato de referencia, sin que ello constituya un máximo contractual ni reduzca las obligaciones técnicas:
No se cuenta con medición consolidada
Por lo tanto, remitirse a lo establecido en el PBC.

Consulta 8 - Capacidad Técnica — Lote N° 2, Ítems 1, 2 y 3, numeral 4, subnumeral 4.4 (Certificación PMP)

Consulta	Fecha de Consulta	15-09-2026

Texto/Exigencia Actual: "Se deberá Contar con al menos 1 (un) Profesional con certificación PMP (Project Management Professional) del PMI (Project Management Institute)."
Consulta/Observación/Petición Concreta: La certificación PMP acredita competencias generales de gestión de proyectos y no guarda relación técnica directa con el objeto específico de la contratación —licencias de correo y plataforma de protección de endpoint—, lo cual constituye una exigencia de Capacidad Técnica desproporcionada y desvinculada del objeto contractual, en contravención de los principios de Economía, Igualdad y Libre Concurrencia que rigen las contrataciones públicas. En virtud de ello, solicitamos a la Convocante se sirva fundamentar técnicamente la relación de causalidad entre dicha certificación y la naturaleza del servicio requerido, o bien proceda a eliminar esta exigencia, admitiendo como alternativa no excluyente la acreditación de experiencia comprobable en gestión de proyectos de implementación de soluciones tecnológicas de similar naturaleza.

Respuesta	Fecha de Respuesta	24-09-2026

Señores potenciales oferentes: Se mantiene la exigencia de contar con al menos un (1) profesional con certificación PMP. El objeto del Lote N° 2 no se limita a la mera provisión de licencias: comprende una implementación tecnológica con arquitectura híbrida, coexistencia e integración de Microsoft 365, Exchange Server, licencias de acceso de usuario, plataforma de protección perimetral de correo existente, certificados digitales, migración de cuentas, configuración, puesta en producción, transferencia de conocimiento y soporte posterior. Estas actividades presentan dependencias técnicas, ventanas de intervención, riesgos de continuidad y coordinación simultánea de múltiples perfiles especializados.
La certificación PMP aporta una metodología verificable para la gestión de alcance, cronograma, riesgos, recursos, comunicaciones, cambios, dependencias y criterios de aceptación. En un servicio de correo institucional, una deficiente coordinación puede generar indisponibilidad, pérdida de mensajes, fallas de coexistencia, inconsistencias de autenticación o afectación de la continuidad operativa. Por ello, la experiencia genérica en proyectos similares no sustituye la finalidad del requisito, que consiste en asegurar que el oferente disponga de una capacidad formal de dirección y control del proyecto, adicional a la competencia técnica de los especialistas.
Por lo tanto, remitirse a lo establecido en el PBC.

Consulta 9 - Capacidad Técnica — Lote N° 2, Ítems 1, 2 y 3, numeral 5 (Certificación en plataforma "Existente")

Consulta	Fecha de Consulta	15-09-2026

Texto/Exigencia Actual: "El oferente deberá presentar 3 técnicos certificados en la plataforma de Email Security y/o tres técnicos certificados en la plataforma de Protección Perimetral Email Gateway (Existente)..."
Consulta/Observación/Petición Concreta: El Pliego exige, dentro de la Capacidad Técnica, certificación del personal sobre la plataforma de Protección Perimetral Email Gateway actualmente instalada, sin identificar en ningún apartado su fabricante, marca o modelo, circunstancia que coloca a los potenciales oferentes en absoluta indefensión respecto del cumplimiento de este requisito, al resultar materialmente imposible certificarse sobre una solución cuya identidad no ha sido revelada. Esta omisión vulnera los principios de Transparencia e Igualdad de condiciones, toda vez que únicamente el proveedor que instaló o mantiene actualmente dicha plataforma se encontraría en condiciones reales de acreditar el cumplimiento. Solicitamos a la Convocante se sirva indicar expresamente la marca, fabricante y modelo de la plataforma existente, a fin de que los oferentes puedan verificar la disponibilidad de certificaciones vigentes en el mercado; y en caso de no proporcionarse dicha información con la debida antelación al cierre de presentación de ofertas, solicitamos se admita como equivalente la certificación de los técnicos en la plataforma de Email Security/Gateway que cada oferente proponga como parte de su solución, siempre que cumpla la misma función y estándar de desempeño.

Respuesta	Fecha de Respuesta	24-09-2026

Señores potenciales oferentes: Se mantiene el requisito de tres (3) técnicos certificados en la plataforma de Email Security y/o en la plataforma de Protección Perimetral Email Gateway existente. La exigencia responde a una necesidad técnica concreta: la nueva plataforma de correo debe coexistir e integrarse de manera transparente y automatizada con el servicio actual de protección perimetral, y el adjudicatario deberá acompañar la migración sin interrumpir los flujos de correo entrante y saliente, las políticas de seguridad, los mecanismos de filtrado y las configuraciones de protección ya operativas.
La certificación en la plataforma que el oferente eventualmente proponga no resulta técnicamente equivalente, porque el riesgo operativo se encuentra precisamente en la interacción con la solución actualmente instalada. El personal debe acreditar conocimiento de la plataforma existente para realizar diagnóstico, integración, ajustes, escalamiento y soporte durante la transición. A fin de que el requisito pueda ser verificado objetivamente por todos los potenciales oferentes, deberán completarse los datos de identificación de la solución existente:
La plataforma actual de la institución Sophos Email Security/ Forti EDR
Por lo tanto, remitirse a lo establecido en el PBC.

Consulta 10 - Capacidad Técnica — Cláusula transversal, Lote N° 2 (Antigüedad de 1 año del plantel técnico)

Consulta	Fecha de Consulta	15-09-2026

Texto/Exigencia Actual: "...los profesionales deberán acreditar su pertenencia a la firma oferente con una antigüedad de al menos 1 (un) año."
Consulta/Observación/Petición Concreta: La exigencia de antigüedad laboral interna de un año para la totalidad del plantel técnico certificado, como parte de la acreditación de Capacidad Técnica, sin admitir vinculación contractual reciente o compromiso formal de disponibilidad para el proyecto, restringe injustificadamente la conformación de consorcios/UTE y la incorporación de personal recientemente certificado, sin relación de causalidad directa con la calidad de ejecución del servicio contratado. Solicitamos a la Convocante se sirva aclarar si será admitida la acreditación de disponibilidad y vinculación contractual —aunque reciente— del personal técnico para el proyecto, en sustitución de la exigencia de antigüedad interna de un año, por resultar esta última desproporcionada respecto del objeto contractual y contraria a los principios de Igualdad y Libre Concurrencia.

Respuesta	Fecha de Respuesta	24-09-2026

Señores potenciales oferentes: Se mantiene la exigencia de que los profesionales acrediten una antigüedad mínima de un (1) año de pertenencia a la firma oferente. El requisito no busca medir únicamente la experiencia individual del técnico, sino la capacidad organizacional real del oferente para ejecutar y sostener el servicio con un equipo estable, integrado a sus procesos internos de soporte, escalamiento, documentación, seguridad y gestión de cambios.
En una implementación que involucra múltiples especialidades y componentes críticos, la mera disponibilidad reciente de un profesional no acredita el mismo nivel de integración operativa, conocimiento de procedimientos internos ni continuidad del recurso durante la ejecución. La antigüedad mínima reduce el riesgo de conformar equipos exclusivamente para la presentación de la oferta, limita la dependencia de recursos circunstanciales y fortalece la trazabilidad de responsabilidades durante la migración y el soporte posterior. Se trata, por tanto, de una medida de estabilidad del plantel técnico vinculado al oferente y de continuidad del servicio.
Por lo tanto, remitirse a lo establecido en el PBC.

Consulta 11 - Capacidad Técnica — Lote N° 2, Ítems 1, 2 y 3, numeral 4, subnumeral 4.5 (MAICPP)

Consulta	Fecha de Consulta	15-09-2026

Texto/Exigencia Actual: "El oferente deberá pertenecer al Programa de Microsoft AI Cloud Partner y poseer como mínimo las competencias de Solutions Partner for Infrastructure y Solutions Partner for Modern Work."
Consulta/Observación/Petición Concreta: La exigencia referida constituye una designación de partnership comercial otorgada a nivel corporativo, cuya obtención depende de umbrales de facturación y volumen de licenciamiento con el fabricante, y no una certificación técnica individual del personal que preste el servicio. Ello resulta ajeno a la capacidad técnica real exigible para la prestación del servicio de correo/endpoint y favorece indebidamente a un grupo reducido de grandes distribuidores, en desmedro de empresas especializadas en ciberseguridad que acreditan idéntica competencia funcional mediante certificaciones técnicas de producto, vulnerando así los principios de Igualdad y Libre Concurrencia.
Solicitamos a la Convocante se sirva aclarar si serán admitidas como equivalentes las certificaciones técnicas individuales del fabricante de la solución ofertada que acrediten la misma competencia funcional, sin exigir la designación corporativa de "Solutions Partner", o en su defecto, fundamente la necesidad técnica ineludible de dicho nivel de partnership para la correcta ejecución contractual.

Respuesta	Fecha de Respuesta	24-09-2026

Señores potenciales oferentes: Se mantiene el requisito de pertenencia al Programa Microsoft AI Cloud Partner y de contar, como mínimo, con las competencias Solutions Partner for Infrastructure y Solutions Partner for Modern Work. El alcance del Lote N° 2 se encuentra directamente relacionado con una arquitectura Microsoft híbrida que combina servicios de productividad, correo, infraestructura de servidor, licenciamiento, integración, migración y soporte, por lo que la capacidad requerida no se limita al conocimiento de un técnico individual sobre un producto aislado.
La designación a nivel corporativo acredita que la empresa dispone de una estructura técnica y organizacional reconocida por el fabricante para trabajar con soluciones de infraestructura y de Modern Work, además de mecanismos de soporte, escalamiento, acceso a recursos técnicos y capacidad de acompañamiento durante la implementación. Las certificaciones individuales son necesarias para demostrar conocimientos personales, pero no sustituyen la capacidad corporativa exigida al oferente, quien será el responsable contractual de la provisión, integración, migración y soporte de la solución. Por esta razón, no corresponde admitirlas como equivalentes al requisito empresarial establecido.
Por lo tanto, remitirse a lo establecido en el PBC.