Pliego Técnico

CPP

Adquisición de Licencias de solución de seguridad de Trend Micro

Licenciamiento para endpoints y servidores incluyendo consolas de gestión y horas de consultoría y soporte

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

Gerencia Operaciones

Índice de contenido

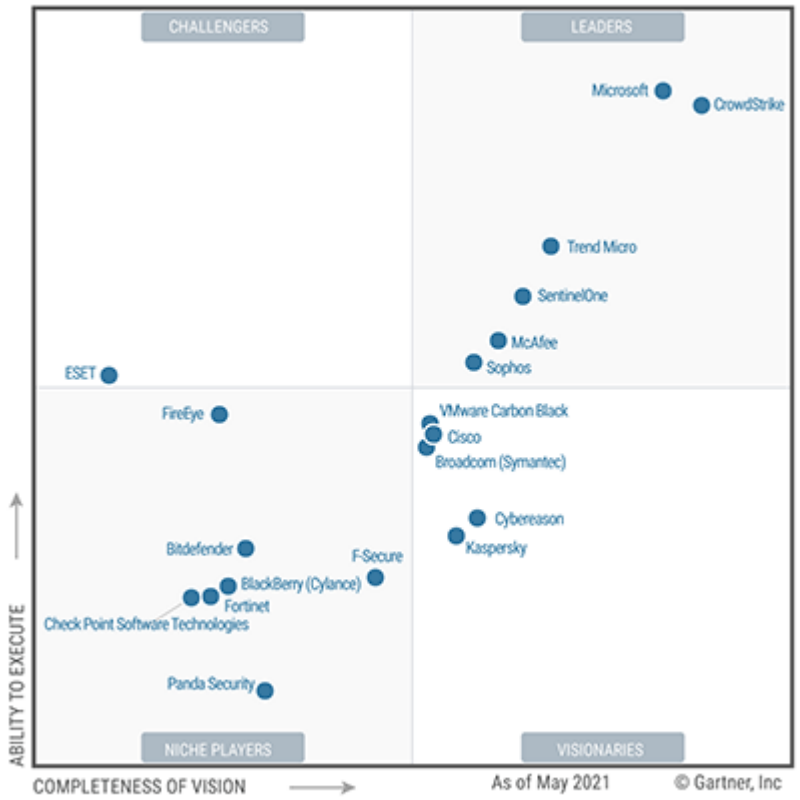
+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

1. INTRODUCCIÓN

En el marco de la protección integral de la infraestructura de Centro Ceibal, se busca renovar y adquirir licencias de software de la suite de solución de protección de la empresa Trend Micro, que permitan proteger los dispositivos de los usuarios finales (laptops y PCs) así como la infraestructura de servidores (tanto onpremise como en la nube) que se ubican en los datacenters de Centro Ceibal ya sea físicos o virtualizados.La solución debe permitir la instalación de agentes compatibles con las distintas tecnologías usadas en Ceibal, la gestión y monitoreo centralizados, la gestión de alertas y logs y la conexión con otros componentes que conforman el entorno de seguridad de Centro Ceibal. La solución de Trend Micro es la usada por Centro Ceibal desde hace varios años de manera exitosa, siendo un líder del cuadrante de gartner en protección antimalware para endpoints de manera sostenida en el tiempo.

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)

2. OBJETO DEL LLAMADO Y PRODUCTOS A COTIZAR

El objeto del llamado es la adquisición del licenciamiento de la suite de protección de Trend Micro necesaria para proteger la infraestructura actual y futura del Centro Ceibal. El sistema a adquirir debe cumplir con:

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

1) Ser compatible con la infraestructura desplegada en los datacenters de Centro Ceibal entre los que se incluyen sistemas operativos como Windows 10 y 11, Windows Server, CentOS, Debian, Ubuntu, MS SQL Server, My SQL entre otros.
2) Permitir la gestión y monitoreo centralizados a través de consolas en la nube que soporten las siguientes funciones entre otras:
    - Aplicación de políticas personalizadas y parametrizables que puedas ser desplegadas masivamente mediante scripts
    - Monitoreo en tiempo real de la infraestructura desplegada
    - Gestión de alertas configurable, que incluya grado de criticidad y sugerencias sobre las acciones correctivas a tomar
    - Trazabilidad y auditoría mediante logs parametrizables que permitan el análisis forense de incidentes y que sea compatible con el SIEM desplegado en Centro Ceibal (IBM Qradar)
    - Protección superior al promedio de la industria (99,7% según el instituto AV-TEST GmbH) sobre malwares y ataques de día cero.

Se solicitan cotizaciones de licencias de 3 productos (Categoría 1 y 2), donde se podrán adquirir distintas cantidades de cada uno de los productos. En la Categoría 3 se solicita cotización de horas de consultoría para instalación, migración, configuración y soporte. El oferente deberá ofertar obligatoriamente todos los productos solicitados.

3. ESPECIFICACIONES TÉCNICAS

En la presente sección se listan los requerimientos técnicos y de licenciamiento correspondiente a las licencias a adquirir y las horas de soporte necesarias para un correcto funcionamiento de la solución.

En todos los casos el producto ofertado deberá cumplir con la totalidad de las especificaciones obligatorias.

En caso de que un producto ofertado no cumpla con una o más especificaciones obligatorias la oferta será descartada.

Categoría 1 - Solución de protección para PCs y laptops

1.1 - Trend Micro APEX ONE SaaS

Debe incluir:

- Apex central cloud
- Apex para PCs y Mac
- Protection para servidores windows
- Vulnerability Protection
- Application Control
- Integración de Vulnerability Protection & Application Control en un mismo agente
- Data Loss Prevention (DLP)

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

Categoría 2 - Solución de protección para servidores

2.1 - Trend Micro Cloud One Endpoint Security with XDR

Debe incluir:

- Antimalware
- XDR Detección y Respuesta Extendida

2.2 - Trend Micro Cloud One Workload Security with XDR

Debe incluir:

- Antimalware,
- Web reputation,
- Behavioral analysis,
- Machine learning,
- Application control,
- Log inspection,
- File integrity monitoring,
- Host-based intrusion prevention,
- Firewall,
- Vulnerability scanning,
- Device control,
- EDR/XDR.

Categoría 3 - Instalación / Migración, configuración y soporte

3.1 - Migración de la consola actual a la nueva consola en la nube

Debe incluir:

- Configuración de las credenciales en el portal de licencias de Trend Micro.
- Configuración de la consola central y migración de políticas y settings.
- Migración de los agentes agentes On-premises a SaaS (aproximadamente 500).
- Configuración de políticas de buenas prácticas y optimización de la consola.

3.2 - Instalación y configuración de la solución Trend Micro Cloud One

Debe incluir:

- Activación de la consola en la nube con licencia
- Preparación de políticas y configuración de la consola
- Capacitación de uso básico del sistema
- Verificación de que el sistema queda funcionando correctamente

3.3 - Horas de soporte y consultoría (hasta 200 horas anuales para uso a demanda de Centro Ceibal)

A modo de ejemplo, las horas de soporte podrán incluir tareas de

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

- Configuración de las consolas, agentes y demás componentes de las soluciones de Trend Micro.
- Aplicación y mantenimiento de políticas y buenas prácticas.
- Capacitación en el uso de la herramienta.
- Migración y actualización de los sistemas.
- Servicio de soporte para asegurar el óptimo funcionamiento de la solución.
- Colaboración en la resolución de problemas e incidentes de ciberseguridad.

4. REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación se establecen los requisitos de seguridad de la información para la compra de soluciones informáticas.

Requisitos obligatorios Estos requisitos son obligatorios para todas las soluciones informáticas, así como herramientas de hardware, a ser adquiridas por Centro Ceibal. Podrá haber excepciones que deberán estar justificadas y aprobadas por quien corresponda.

Requisitos deseados Estos requisitos no son obligatorios, pero serán valorados al momento de adjudicar la compra.

Descripción de requisitos:

4.1 Diseño y arquitectura

La solución deberá tener incorporada la seguridad en su diseño mediante el uso de buenas prácticas y la incorporación de la seguridad desde el diseño como parte de todo el proceso del ciclo de desarrollo de la solución.

Deberá cumplir los siguientes requisitos:

- Desarrollo por capas (presentación, lógica de negocio y datos).
- Solución modular con separación y agrupación de funcionalidades por categorías o módulos que permita la escalabilidad de la solución y facilite la integración y compatibilidad con otras soluciones.
- Arquitectura confiable que incorpore una visión de la seguridad integral cubriendo los aspectos de confidencialidad, disponibilidad, integridad, no repudio y privacidad a través de métricas e indicadores cualitativos como cuantitativos.

4.2 Autenticación

La solución deberá cumplir con métodos de autenticación seguros que permitan verificar la identidad de los usuarios y protejan la confidencialidad de la información.

Deberá incorporar los siguientes requisitos:

- Autenticación con usuario y contraseña que cumpla las políticas de contraseñas del Centro Ceibal.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

- Compatibilidad con los sistemas de autenticación centralizados (SSO) usados por Centro Ceibal según corresponda:
- Sistema de Login único para beneficiarios. (protocolo CAS)
- Compatibilidad para autenticación con alguno de los siguientes proveedores de identidades (Google, Active Directory) detallando protocolos y configuraciones usados.
- Posibilidad de autenticación con múltiples factores (MFA) para cuentas privilegiadas.

4.3 Gestión de sesiones

La solución deberá proveer una adecuada gestión de sesiones de usuarios permitiendo conocer el estado actual del usuario o el dispositivo conectado.

Para esto deberá:

- Mantener sesiones únicas para cada usuario que no podrán ser adivinadas o compartidas.
- Las sesiones serán desconectadas cuando ya no sean necesarias o durante un período de inactividad (en lo posible parametrizable).

4.4 Control de acceso

La solución deberá proveer una adecuada gestión del control de acceso de manera de autorizar el acceso a las funcionalidades y datos en concordancia con los perfiles y roles que se definan.

Para esto deberá cumplir que::

- Los usuarios que quieren acceder a determinados recursos posean las credenciales correctas.
- Los usuarios estén asociados a un conjunto adecuado de roles y privilegios de acuerdo a las funcionalidades brindadas por la solución y a los recursos accesibles.
- Los metadatos de los roles y permisos deberán estar protegidos de manipulaciones y reutilizaciones.
- La asignación del control de acceso sigue el principio de menor privilegio.

4.5 Codificación y validación

Las debilidades más comunes en aplicaciones web modernas, son los fallos en validar correctamente las entradas de datos que provienen de los usuarios y el entorno, previo al uso de esta información. Estas debilidades generan la mayoría de las vulnerabilidades y ataques conocidos como por ejemplo Cross-Site Scripting (XSS), Inyección SQL, ataques al sistema de archivos, ataques Unicode y desbordamiento de buffers.

La solución deberá cumplir con:

- Asegurar la validación de entradas y salidas mediante una arquitectura de codificación y flujos seguros de la información que prevengan la inyección.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

- Los datos de entrada sean robustamente ingresados y validados o en el peor de los casos filtrados y depurados.
- Asegurar una codificación de salida robusta que tome en cuenta el contexto de la información y sea lo más cercana al intérprete externo.

4.6 Manejo de errores y verificación de logs

La solución deberá generar información de calidad en los logs y gestionar adecuadamente los mensajes de error, evitando en lo posible la publicación de información sensible.

Para lograr esto la solución deberá:

- No recolectar información sensible en los logs a menos que sea necesario o específicamente requerido.
- Asegurar que la información contenida en los logs es gestionada de acuerdo al nivel de clasificación de la misma (por ej. tomar en cuenta el ciclo de vida de la información y la caducidad de la misma).
- Incluir información útil para la auditoría y la solución de problemas que incluya como mínimo fecha, hora y detalle de los eventos, cambios en las configuraciones, intentos de acceso al sistema (exitosos y rechazados),

4.7 Confidencialidad y Protección de datos

La solución deberá asegurar la confidencialidad, integridad y disponibilidad de la información y datos personales. Para implementar una adecuada protección de datos, la solución deberá asegurar la: legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva, y responsabilidad. Para esto la solución deberá:

- Cumplir con la normativa vigente uruguaya en materia de datos personales (Ley Nº 18.331, de 11 de agosto de 2008 y Decreto Nº 414/2009, de 31 de agosto de 2009). Se considera dato personal la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, a modo enunciativo, cualquier información numérica, alfabética, gráfica, fotográfica, registro de voz e imagen, acústica o de cualquier otro tipo que refiera a ellas directa o indirectamente, conforme con lo dispuesto en el artículo 4 de la Ley Nº 18.331 y artículos 1 y 4 del Decreto Nº 414/009.
- Adoptar las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de los datos y evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información.
- Proteger la información y datos creada, editada, borrada o accedida sin las autorizaciones correspondientes, en particular en cantidades masivas de datos.
- Tomar las precauciones y controles necesarios para que la información y los datos personales no queden disponibles en navegadores, balanceadores de carga, copias temporales, cookies y otras estructuras donde no sea necesario.
- Asegurar la confidencialidad de toda la información que se procese o utilice. La Información Confidencial comprende, entre otros y a vía de ejemplo, la siguiente

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

información: toda estrategia, plan y procedimiento comercial, información propietaria, software, herramienta, proceso, imágenes, datos personales, metodología, información y secreto comercial, y demás información y material de Ceibal, así como de los alumnos, beneficiarios, docentes, centros de estudios, que pudiera ser obtenida de cualquier fuente o pudiera ser desarrollada. .

- Alojar los datos en territorio uruguayo, o en caso de transferencia internacional asegurar que el servidor se encuentre en países considerados con niveles adecuados de acuerdo con la Directiva 95/46/CE. En caso contrario, contar con el consentimiento del titular del dato para la transferencia a un territorio no adecuado, o a que el importador haya suscripto cláusulas contractuales tipo con el exportador o posea un Código de Conducta inscripto, con la consecuente autorización de transferencia internacional de datos tramitada ante la Unidad Reguladora y de Control de Datos Personales, en los dos últimos supuestos.
- No utilizar la información / datos para una finalidad distinta a la contratada, ni en beneficio propio ya sea gratuito u oneroso, ni cederlos, comunicarlos o transferirlos a terceros.
- Centro Ceibal será el responsable de la base de datos y del tratamiento, siendo la Empresa adjudicada y sus empresas sub contratadas, encargados de tratamiento, de acuerdo con lo dispuesto en los literales H) y K) del artículo 4 de la Ley Nº 18.331.
- Permitir la publicación de las políticas de privacidad y términos y condiciones de uso de Centro Ceibal en el desarrollo.
- Permitir el derecho de acceso, rectificación, actualización, inclusión o supresión de los datos personales.
- Devolver o suprimir de todos sus sistemas y archivos físicos y lógicos, sean propios o contratados a terceros, los datos personales accedidos, obtenidos o tratados, así como los metadatos asociados, a requerimiento de Ceibal.

4.8 Comunicaciones

La solución deberá proveer una comunicación segura de la información gestionada de manera de asegurar la confidencialidad de la misma.

Para esto deberá:

- Publicar servicios a través de protocolos seguros (TLS o encriptación robusta) para todos los usuarios y sin importar la sensibilidad de la información transmitida.
- Se utilizarán protocolos y algoritmos considerados seguros por la industria y las buenas prácticas, dejando como último recurso o por temas de compatibilidad que sean expresamente autorizados por Centro Ceibal el uso de otros protocolos menos seguros.
- La solución deberá ser enteramente compatible con los certificados usados por Centro Ceibal y en caso de usar certificados generados internamente deberán ser validados por las autoridades de certificación que Centro Ceibal establezca.
- Todas las comunicaciones por fuera del protocolo HTTP, como por ej. accesos remotos, comunicación entre capas de la solución, middleware, bases de datos,

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

fuentes externas de datos, monitoreo, herramientas de comunicación, etc. deberán ser comunicaciones seguras y en lo posible encriptadas.

4.9 Uso de archivos y recursos

La solución deberá proveer controles sobre la gestión de archivos de manera de garantizar la seguridad de la información.

Para esto debe cumplir con:

- Los archivos inseguros deben ser gestionados adecuadamente de manera de garantizar la confidencialidad, integridad y disponibilidad de la información.
- Se deberán implementar controles para la subida, ejecución, bajada y alojamiento de los archivos que blinden la solución de ataques maliciosos y configuraciones inadecuadas como por ej.: bombas zip, tipos de archivos incorrectos, ataque pass traversal, alojamiento con permisos o en directorios incorrectos, ataque SSRF.

4.10 API y Web services

La solución que haga uso de APIs (comúnmente a través del uso de JSON, XML, GraphQL u otros formatos) deberá cumplir con:

- Mantener una adecuada autenticación, gestión de sesiones y autorizaciones para todos los web services.
- Validación de entrada para todos los parámetros que son ingresados.
- Controles efectivos de seguridad sobre todo tipo de APIs, incluidas las nubes y las APIs sin servidores.

4.11 Respaldos y contingencia

La solución deberá ser compatible con una adecuada política de respaldos y recuperación de datos de manera de asegurar la integridad y disponibilidad de la información frente a incidentes.

En caso de brindar la solución en modalidad de software como servicio (SaaS) la solución deberá:

- Cumplir con un plan de continuidad del negocio, que ofrezca la contingencia necesaria para asegurar la disponibilidad, integridad y confidencialidad de la información frente a distintos tipos de incidentes.
- Brindar las soluciones tecnológicas necesarias (por ej. respaldos y plan de recuperación ante desastres) de manera de asegurar los niveles de disponibilidad e integridad estipulados en el acuerdo de nivel de servicio correspondiente (SLA).

4.12 Criptografía

La solución deberá cumplir con los siguientes requisitos a nivel de controles criptográficos:

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

- Permitir el uso de módulos criptográficos para proteger la información sensible de la solución como ser información financiera, datos personales y datos de roles y permisos, ya sea en reposo, en uso y en tránsito.
- Usar algoritmos de cifrado robustos (como por ej AES y RSA) con claves de longitud adecuadas para protegerse contra ataques.
- Generar números aleatorios adecuados.
- El acceso a las claves de cifrado es gestionado de manera segura.

4.13 Código malicioso

La solución no deberá contener código malicioso de ningún tipo. Para cumplir con esto la solución deberá entre otras características:

- Utilizar herramientas de detección del código malicioso en el proceso de desarrollo.
- No incluir bombas de tiempo u otros tipos de ataque similares.
- No realizar transmisiones de información o contacto a destinos maliciosos o no autorizados.
- No contener puertas traseras, rootkits, ataques "salami", huevos de pascua y otros tipos de códigos maliciosos o que no siguen las buenas prácticas.
- Tomar las medidas necesarias para que la solución no incorpore código malicioso a través de controles como ser firma de código, uso de bibliotecas y frameworks seguros, control de caducidad sobre DNS, etc.

4.14 Lógica de negocio

La solución deberá proveer una capa de negocio desarrollada de manera segura y que permita evitar los ciberataques más frecuentes. Para esto debe cumplir que:

- El flujo de la lógica de negocio debe ser secuencial, coherente y no puede ser alterado.
- La lógica de negocio incluye controles y límites que permiten detectar y prevenir ataques automatizados.
- La lógica de negocio debe tomar en cuenta casos de uso que incluyen actores maliciosos, casos de abuso y además debe contener protecciones contra ataques de spoofing, manipulación, repudio, divulgación de información y elevación de privilegios entre otros.

4.15 Configuración

La solución deberá cumplir con los requerimientos y controles de configuración que garanticen una aplicación segura.

Los mismos deberán incluir:

- Un entorno lo más seguro, repetitivo y automatizable posible a través de la incorporación de buenas prácticas (ej. modelo DevSecOps) con herramientas,

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

procesos y tecnologías que la * implementen adecuadamente (ej. contenedores, despliegues automatizados, etc.).
- Herramientas y entornos de desarrollo actualizados y correctamente mantenidos.
- Herramientas y entornos de desarrollo correctamente configurados y verificados en su seguridad (hardening) como por ej. deshabilitar el modo debug en entornos de producción.
- Seguridad por defecto en las configuraciones de los usuarios y los permisos.

4.16 Certificaciones

Se valorarán las certificaciones y el cumplimiento con estándares relacionados al desarrollo seguro, la seguridad de la información y la privacidad como ser:

- Common criteria certification (ISO IEC 15408)
- CPA Build Standard
- OWASP ASVS
- ISO 27001
- FIPS 140
- SCAMP
- CIS Benchmarks
- AICPA SOC2-3
- NIST CSF / 800
- ISACA Cobit
- PCI DSS
- GDPR

4.17 Metodología

Se valorarán las propuestas que incorporen metodologías de diseño y desarrollo del software con una visión integral de la seguridad en el proceso de desarrollo.

4.18 Análisis de vulnerabilidades

Se valorarán las soluciones que hayan sido sometidas a chequeos estandarizados de vulnerabilidades y/o tests de penetración. Se deberá proveer constancia de las mismas mediante un informe resumen o certificado correspondiente.

Se valorará informe detallando cobertura de amenazas sobre el último OWASP Top Ten vigente.

.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

Adicionalmente se deberán cumplir con las siguientes condiciones:

4.19 Cumplimiento de políticas

Todo proveedor debe conocer el Manual de Políticas de Seguridad de la Información y cumplir con lo que le resulte aplicable. Estás políticas se encuentran publicadas a disposición de los proveedores en el portal de Centro Ceibal en:

https://www.ceibal.edu.uy/storage/app/media/manual-de-politicas-de-seguridad-de-la-informacion-wiki-ceibal.pdf

4.20 Acuerdo de confidencialidad

Se deberá incluir una cláusula de confidencialidad con el proveedor adjudicado que garantice la protección de la información de Centro Ceibal.

4.21 Trazabilidad y auditoría

Centro Ceibal se reserva el derecho de auditar los procesos relacionados a la seguridad de la información y a la privacidad con el objetivo de verificar que se cumpla lo estipulado entre las partes. Para ello podrá solicitar al proveedor la documentación respaldante que corresponda en cada caso. A estos efectos deberá preverse tal facultad en el contrato.

4.22 Uso de la infraestructura de Centro Ceibal

En el caso que el servicio a contratar incluya el uso, instalación, configuración y/o mantenimiento de infraestructura de Centro Ceibal tanto lógica como física, se deberán estipular claramente las condiciones, responsabilidades y usos adecuados de la información afectada de manera de asegurar su confidencialidad, integridad y disponibilidad.

Se deberán completar las matrices de cumplimiento establecidas en el Anexo II.

5. ANTECEDENTES

5.1 Antecedentes de las empresas oferentes

Es requisito obligatorio ser partner oficial de Trend Micro (deberá incluirse certificado que lo acredite). Se analizarán los proyectos de implementación y migración de equipamiento Trend Micro similares a los que se están adquiriendo, en empresas de mediano y gran porte. Se deberá completar el Anexo III detallando los 3 proyectos más relevantes.

5.2 Requisitos de consultores y capacitadores

Es requisito obligatorio que el proveedor provea al menos dos técnicos (titular y suplente) con experiencia en implementaciones similares a las del presente llamado en empresas de mediano y gran porte.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

6. PRESENTACIÓN DE OFERTAS

6.1 Documentación técnica

Junto con la oferta se deberán incluir hojas de datos con las especificaciones técnicas de los productos ofertados. Las hojas de datos deberán ser las provistas por el fabricante del producto y coincidir con los productos ofertados. Centro Ceibal se reserva el derecho de descartar aquellas ofertas que no presenten hojas de datos o que presenten hojas de datos que no se correspondan con el productos ofertados.

6.2 Formato

La oferta deberá ser presentada completando las tablas incluídas en los Anexos I a IV.

El oferente completará todos los campos bajo el título A COMPLETAR POR EL OFERENTE de las tablas correspondientes.

Si un campo no fuese completado se considerará que el producto no cumple con la especificación correspondiente .

Centro Ceibal se reserva el derecho de descartar aquellas ofertas que no sean presentadas en el formato solicitado y/o indiquen el cumplimiento de una especificación que no pueda ser acreditada mediante las hojas de datos.

6.3 Plazo de entrega

El oferente deberá especificar el plazo de entrega de los productos a partir de la fecha de notificación de adjudicación. Es deseable un plazo de hasta 3 días corridos a partir de dicha fecha.

7. CRITERIOS DE EVALUACIÓN

La evaluación de las ofertas para cada uno de los productos solicitados en la sección 3 se realizará en 2 etapas. En la primera se verifica que la oferta cumple con los requisitos solicitados. Todas las ofertas que cumplan con lo estipulado en la etapa 1 pasan a la etapa 2 para ser evaluadas económicamente.

Etapa 1

1) Se verifica que la información presentada sea completa, coherente con el producto cotizado y que cumpla con el formato pedido.
2) Se verifica si el producto ofertado cumple con las especificaciones obligatorias.
3) Se verifica que los oferentes cumplen con los antecedentes estipulados.

Etapa 2

1) Se comparan todas las ofertas económicas recibidas para cada ítem. **Se adjudicará a un único oferente por todos los ítems solicitados.** Centro Ceibal se reserva el derecho

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

de elegir cuál de las 2 modalidades (1 año o 2 años) así como la cantidad de licencias y horas en cada una de las categorías se adjudicará.

La no verificación de una o más condiciones mencionadas en la etapa 1 habilita a Centro Ceibal a no incluir la oferta en la siguiente etapa de evaluación.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

ANEXO I - TABLA DE COTIZACIONES

Categoría 1 - Trend Micro APEX ONE SaaS

TABLA DE COTIZACIONES	Cantidad de licencias a adquirir	A COMPLETAR POR EL OFERENTE Se podrá cotizar en USD o $UYU, ambas modalidades con impuestos incluídos de acuerdo a la cantidad de licencias a adquirir			
Producto	Rangos	por 1 año de servicio		por 2 año de servicios	
		$UYU	USD	$UYU	USD
Trend Micro APEX ONE SaaS	De 1 a 250 licencias				
Trend Micro APEX ONE SaaS	De 251 a 500 licencias				
Trend Micro APEX ONE SaaS	Más de 500 licencias				

Categoría 2.1 - Trend Micro Cloud One Endpoint Security with XDR

TABLA DE COTIZACIONES	Cantidad de licencias a adquirir	A COMPLETAR POR EL OFERENTE Se podrá cotizar en USD o $UYU, ambas modalidades con impuestos incluídos de acuerdo a la cantidad de licencias a adquirir			
Producto	Rangos	por 1 año de servicio		por 2 año de servicios	
		$UYU	USD	$UYU	USD
Trend Micro Cloud One Endpoint Security with XDR	De 1 a 250 licencias				
Trend Micro Cloud One Endpoint Security with XDR	De 251 a 500 licencias				
Trend Micro Cloud One Endpoint Security with XDR	Más de 500 licencias				

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

Categoría 2.2 - Trend Micro Cloud One Workload Security with XDR

TABLA DE COTIZACIONES	Cantidad de licencias a adquirir	A COMPLETAR POR EL OFERENTE Se podrá cotizar en USD o $UYU, ambas modalidades con impuestos incluídos de acuerdo a la cantidad de licencias a adquirir			
Producto	Rangos	por 1 año de servicio		por 2 año de servicios	
		$UYU	USD	$UYU	USD
Trend Micro Cloud One Workload Security with XDR	De 1 a 250 licencias				
Trend Micro Cloud One Workload Security with XDR	De 251 a 500 licencias				
Trend Micro Cloud One Workload Security with XDR	Más de 500 licencias				

Categoría 3.1 - Migración de la consola actual a la nueva consola en la nube

TABLA DE COTIZACIONES	A COMPLETAR POR EL OFERENTE	
Descripción	precio total del servicio en USD o $UYU (impuestos incluidos)	
	$UYU	USD
Migración de la consola actual a la nueva consola en la nube		

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

Categoría 3.2 - Instalación y configuración de la solución Trend Micro Cloud One

TABLA DE COTIZACIONES	A COMPLETAR POR EL OFERENTE	
Descripción	precio total del servicio en USD o $UYU (impuestos incluidos)	
	$UYU	USD
Instalación y configuración de la solución Trend Micro Cloud One		

Categoría 3.3 - *Horas de soporte y consultoría (hasta 200 horas anuales para uso a demanda de Centro Ceibal)*

TABLA DE COTIZACIONES	A COMPLETAR POR EL OFERENTE	
Descripción	precio por hora del servicio en USD o $UYU (impuestos incluidos)	
	$UYU	USD
Horas de soporte y consultoría (*)		
Horas de soporte y consultoría (**)=		

(*Horario de oficina: lunes a viernes de 9 a 18hs.

(**) Fuera de los días y horarios de oficina.

Todos los costos necesarios para brindar el servicio (conexión a internet, computadoras, teléfono, equipamiento necesario para desarrollar), viáticos y horas de transferencia deberán ser asumidos por el proveedor.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

ANEXO II - TABLA DE CUMPLIMIENTO DE SEGURIDAD DE LA INFORMACIÓN

Matriz de cumplimiento de requerimientos de Seguridad de la Información para soluciones de software				
A completar por Ceibal			A completar por oferente	
Nº Req.	Requerimiento	Tipo	¿Acepto lo requerido? [SI/NO]	Observaciones (si corresponde)
4.1	Diseño y Arquitectura	Obligatorio		
4.2	Autenticación	Obligatorio		
4.3	Gestión de sesiones	Obligatorio		
4.4	Control de acceso	Obligatorio		
4.5	Codificación y validación	Obligatorio		
4.6	Manejo de errores y logs	Obligatorio		
4.7	Confidencialidad y protección de datos	Obligatorio		
4.8	Comunicaciones	Obligatorio		
4.9	Uso de archivos y recursos	Obligatorio		
4.10	API y Web Services	Obligatorio		
4.11	Respaldos y contingencia	Obligatorio		
4.12	Criptografía	Obligatorio		
4.13	Código malicioso	Obligatorio		
4.14	Lógica de negocio	Obligatorio		
4.15	Configuración	Obligatorio		
4.16	Certificaciones	Deseado		
4.17	Metodologías	Deseado		
4.18	Análisis de vulnerabilidades	Obligatorio		

El campo Cumplimiento deberá completarse con “Cumple totalmente”, “Cumple parcialmente” o “No cumple”, con la observación que consideren pertinente añadir.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

MATRIZ DE CUMPLIMIENTO DE SEGURIDAD DE LA INFORMACIÓN Horas de servicio (consultoría y soporte)		A COMPLETAR POR EL OFERENTE (en cada especificación marcar con una cruz (X) la opción que corresponda)	
		CUMPLE	
Nº Req.	Requerimiento	SI	NO
4.19	Cumplimiento de políticas https://www.ceibal.edu.uy/storage/app/media/manual-de-politicas-de-seguridad-de-la-informacion-wiki-ceibal.pdf		
4.20	Acuerdo de confidencialidad		
4.21	Trazabilidad y auditoría		
4.22	Uso de la infraestructura de Ceibal		

ANEXO III - ANTECEDENTES DE LAS EMPRESAS OFERENTES Y EL EQUIPO DE TRABAJO

Proyectos de instalación y configuración de productos Trend Micro

TABLA DE ANTECEDENTES	A COMPLETAR POR EL OFERENTE				
Proyecto	Datos del proyecto				
	Año	Empresa o cliente	Cantidad de horas aproximada del proyecto	Descripción del proyecto	Contacto para verificar datos o carta de clientes
1					
2					
3					

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

Antecedentes del personal que participará en las horas de consultoría y soporte

TABLA DE ANTECEDENTES	A COMPLETAR POR EL OFERENTE				
Técnico / Profesional	Datos del equipo de consultoría /soporte				
	Nombre	Experiencia en años	Título de grado	Certificaciones	Proyectos en los que participó
Titular					
Suplente					

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

ANEXO IV - SLA - NIVEL DE SERVICIO

TIEMPO DE RESPUESTA

En la columna de la siguiente tabla "Cumple con lo requerido" es donde el oferente deberá expresamente indicar "SI" o "No" con lo solicitado. En caso de que no se indique explícitamente el cumplimiento por parte del oferente, la oferta será rechazada.

Incidentes en Producción

Urgencia del incidente	SLA (en horas)	Observaciones	¿Cumple? [SI/NO]
Urgente			
Alta			
Media /Baja			

Atención a pedido de servicio

Prioridad De la Solicitud	SLA (días hábiles)	Observaciones	¿Cumple? [SI/NO]

[1] Incidencias: corresponden a cualquier evento que cause una interrupción del servicio o una reducción de la calidad del mismo

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

Alta			
Media			
Baja			

TIEMPO DE RESOLUCIÓN

Las partes acordarán para cada incidente/solicitud el tiempo de solución del mismo.

El oferente puede añadir información que le parezca relevante en su propuesta de SLA.

El oferente deberá enviar mensualmente el informe con los indicadores definidos del SLA, de acuerdo al formato que otorgue Ceibal.

Fin del documento

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy