Documento de Alcance Técnico

Renovación Solución de Protección de Punto Final

Tabla de contenidos

Introducción

Como parte de su estrategia de gestión de la seguridad, que tiene como objetivo la mejora sistemática y continua de su postura de ciberseguridad, el Poder Judicial de San Juan, en adelante el CLIENTE, gestiona este proyecto que tiene como alcance el renovar su solución actual de Protección de Punto Final.

Esta transición tiene como objetivo reforzar la capacidad de la organización para detectar, responder y mitigar de manera proactiva a amenazas avanzadas dirigidas a los puntos finales.

Este documento de alcance técnico describe los objetivos, el alcance, las características (básicas y extendidas), así como los entregables del proyecto.

Objetivos

El objetivo principal de este proyecto es renovar la solución actual de Protección de Punto Final por una que mejore significativamente la capacidad de la organización para detectar, investigar y responder a incidentes de ciberseguridad dirigidos a sus puntos finales.

Estos objetivos incluyen:

1. *Mejorar la Detección y Respuesta a Amenazas*: Incrementar significativamente la capacidad de la organización para detectar, investigar y responder a incidentes de ciberseguridad, con un enfoque especial en amenazas avanzadas y de día cero.
2. *Aumentar la Visibilidad de Actividades de Seguridad*: Proporcionar mayor visibilidad de las actividades de los endpoints y los eventos de seguridad para identificar y mitigar rápidamente comportamientos sospechosos.
3. *Automatización y Agilización de Procesos de Respuesta*: Implementar procesos automatizados y ágiles para la respuesta a incidentes, reduciendo el tiempo de reacción y mejorando la eficiencia operativa.
4. *Integración con Infraestructura de Seguridad Existente*: Asegurar una integración fluida con la infraestructura de seguridad actual, incluyendo Active Directory, Firewalls Fortinet y Wazuh SIEM, para un manejo centralizado y eficaz de la seguridad.

Este proyecto se alinea con el compromiso de la organización de mantener una postura de seguridad proactiva y resiliente.

Supuestos

Cualquier producto de software ofrecido deberá permanecer activo (soporte mainstream) durante toda la vida útil del contrato. Si así no lo fuera, el OFERENTE deberá proveer, sin costo adicional, un reemplazo que provea funcionalidades iguales o superiores.

Por defecto el OFERENTE realizará todas las tareas de manera remota con soporte y logística local (“manos remotas”) provisto por el CLIENTE. El CLIENTE proveerá un acceso remoto nombrado usando su plataforma VPN durante la vida útil del proyecto. Este acceso podrá ser monitorizado y solo podrá usarse a los efectos de este proyecto.

La provisión de hardware, software de base, almacenamiento, conectividad y demás elementos de infraestructura son responsabilidad del CLIENTE a petición del OFERENTE.

Si el OFERENTE necesitara apersonarse en dependencias del CLIENTE, todos los costos asociados correrán por cuenta del primero y deben ser especificados en la propuesta.

La propuesta se considera “llave en mano”, todos los costos, directos o indirectos, se consideran parte de alcance.

Las propuestas deberán seguir una estructura similar a este documento para facilitar la evaluación y comparación de propuestas.

Si la propuesta incluyese la renovación de la actual solución, *Kaspersky Endpoint Detection and Response Optimum*, los servicios profesionales no serán parte de la contratación. Para este caso particular sólo se deberá incluir dentro del apartado una revisión del estado de salud (“*healthcheck*”) de la consola de gestión y del sistema en general.

Funcionalidades

La siguiente es una lista de funcionalidades a proveer por el/los producto/s ofertados, se identifican con “**B”** aquellas básicas y con “**E**” aquellas extendidas. Las primeras son consideradas mandatorias.

En la oferta se deberá declarar si el producto cumple total (**T**), parcialmente (**P**) o no cumple (**NC**) con la funcionalidad e incluir una referencia (página en la descripción de producto, URL, etc.) siguiendo la lista a continuación.

Funcionalidad	Tipo	Soporte (T/P/NC)
Análisis forense de amenazas procesables para permitir a los administradores aislar rápidamente las infecciones	B	
Aprendizaje automático y análisis de comportamiento para la detección avanzada de amenazas	B	
Automatización y orquestación de respuesta a incidentes	B	
Bloqueo de almacenamiento removible USB	B	
Capacidad para identificar y bloquear secuencias de comandos (scripting) maliciosas	B	

Capacidades avanzadas de detección de amenazas, incluido malware sin archivos y exploits de día cero	B	
Capacidades de aislamiento y contención de endpoints	B	
Capacidades forenses para respaldar el análisis y la investigación posteriores al incidente	B	
Control de aplicaciones a través de listas blancas o negras, que permita bloquear automáticamente las aplicaciones no deseadas en cada punto final a través de una política	B	
Cortafuegos integrado para bloquear ataques de red hostiles	B	
Cumplimiento de los requisitos y estándares reglamentarios pertinentes incluyendo MITRE Framework, ISO/IEC 27001, NIST Cybersecurity Framework y NIST Special Publication 800-53	B	
Gestión de Activos	B	
Gestión granular de políticas a nivel de usuario/dispositivo, grupo, sitio/ubicación/VLAN, sistema operativo, aplicaciones, etc	B	
Instalación y desinstalación desatendida	B	
Integración con Active Directory, incluyendo autenticación y gestión de ABM (Altas, Bajas y Modificaciones)	B	
Integración con fuentes de inteligencia sobre amenazas para una búsqueda proactiva de amenazas	B	
Integración con Wazuh SIEM	B	
Monitoreo y análisis en tiempo real de las actividades de los endpoints	B	
Plataforma de Gestión de Terminales centralizada, on-premise, en alta disponibilidad	B	
Protección contra Ransomware	B	
Reportes y alertas programados	B	
Seguridad web proactiva para garantizar una navegación segura en la web	B	
Soporte para Sistemas Operativos Windows y Linux, server y escritorio, incluyendo: Windows 7, 10 y 11 Windows Server 2008R2, 2012R2, 2016, 2019 y 2022 CentOS (7 y superiores), Oracle Unbreakable Linux (8 y superiores), Ubuntu LTS (18.04 y superiores) y Debian (8 y superiores)	B	
Análisis de reputación de archivos basado en inteligencia artificial	E	
Cifrado de terminales, correo electrónico y disco para evitar la filtración de datos (claves de cifrado deben ser almacenadas y gestionadas en Active Directory)	E	
Integración con Firewalls Fortinet	E	

Alcances

El alcance incluye:

- Provisión de licencias;
- Servicios profesionales:
    - Implementación y configuración de una *consola de gestión centralizada* en alta disponibilidad, incluyendo políticas, actualizaciones de firmas, reportes, alertas, etc.;
    - Ingeniería y paquetes de software para la *desinstalación* desatendida (incluyendo opciones de scripting, GPO, login script, batch, etc.) de la solución actual (***Kaspersky Endpoint Detection and Response Optimum***);
    - *Instalación* desatendida (incluyendo paquetes de instalación personalizados) de la solución propuesta para una muestra significativa (mínimo 10%) de todos los sistemas operativos dentro del alcance;
    - Pruebas, validación y ajustes;
    - Procedimientos de Operación Estándar (soporte y mantenimiento de clientes, backup y recuperación de la consola, ransomware playbook, etc.);
    - Integraciones
- Transferencia de Conocimiento y Capacitación;
- Documentación;
- Software assurance durante toda la vida del contrato;
- Soporte experto 5x2, NBD durante toda la vida del contrato.

Entregables

La siguiente es una lista de entregables sujetos a recepción y certificación por parte del CLIENTE como paso previo a la aceptación y facturación del proyecto.

1. *Plan de Implementación*;
2. *Plan de Migración*;
3. *Licencias* de acuerdo con el inventario de equipos:
    a. Un mínimo de 90 licencias para cubrir distintas versiones de Windows Server, incluyendo 2008R2, 2012R2, 2016, 2019 y 2022.
    b. Un mínimo de 110 licencias para cubrir distintas versiones de Linux incluyendo CentOS (7 y superiores), Oracle (8 y superiores), Ubuntu LTS (18.04 y superiores) y Debian (8 y superiores).
    c. Un mínimo de 2300 licencias para cubrir clientes de escritorio con diferentes versiones de Windows (7, 10 y 11)
4. *Servicios profesionales, incluyendo:*
    a. *Implementación y configuración de una Consola de Gestión centralizada;*
    b. *Paquete de Desinstalación Desatendida* por cada versión de SO;
    c. *Paquete de Instalación Desatendida* por cada versión de SO;
    d. *Kit de Procedimientos de Operación Estándar* (SOP): respaldo, recuperación,

monitoreo y gestión de performance, mantenimiento y actualización y respuesta ante incidentes;

e. "*Ransomware Playbook*", este manual deberá incluir secciones relacionadas con:
    i. Preparación y Prevención,
    ii. Detección y Análisis,
    iii. Contención y Erradicación,
    iv. Recuperación,
    v. Análisis Post-Incidente.
f. *Configuración de Políticas*;
g. *Integración con Wazuh SIEM*;
h. *Integración con firewalls Fortinet (*)*;
i. *Protocolo de Pruebas y Aceptación;*
j. *Documentación* Conforme a Obra (CAO) de la implementación, incluida la integración con Active Directory y Wazuh SIEM;
k. Transferencia de Conocimientos;
l. Modelo de Soporte y Escalamiento, incluyendo datos de contacto.

(*) de acuerdo con la funcionalidad ofrecida y adjudicada.

Nota:

De acuerdo con el apartado "*Supuestos*" si la propuesta incluyese la renovación de la actual solución, *Kaspersky Endpoint Detection and Response Optimum*, los servicios profesionales no serán parte de la contratación. Para este caso particular sólo se deberá incluir dentro del apartado una revisión del estado de salud ("*healthcheck*") de la consola de gestión.

Soporte

Como parte de alcance se deberá proveer soporte 5x2, NBD en orden a asegurar:

1. Que la solución funcione de manera eficiente en condiciones de carga normales y máximas.
2. Que la solución sea accesible y funcional cuando sea requerido.
3. Que la solución funcione consistentemente como se espera a lo largo del tiempo sin fallas.

Severidad

Para gestionar eficazmente incidentes y problemas se propone un sistema estructurado de evaluación y clasificación del impacto, en términos de severidad, que ayude a priorizar las respuestas y asignar recursos.

A continuación se define un sistema de clasificación de tres niveles, cada uno con tiempos de resolución recomendados según el impacto en la disponibilidad, el rendimiento y la seguridad.

Crítico

Este nivel se asigna cuando *hay un impacto severo en las operaciones o la seguridad*, incluidas violaciones de datos importantes, interrupciones del sistema, pérdida de funcionalidades “core” o cualquier otro evento que podría causar daños a largo plazo a la reputación o la capacidad operativa de la organización.

Ejemplos:

- Interrupción total de la consola de administración.
- Imposibilidad de obtener y distribuir actualizaciones.
- Pérdida de protección para un número importante de endpoints.
- Explotación activa de una vulnerabilidad dentro del sistema.

Objetivo de tiempo de resolución: respuesta inmediata con el objetivo de comenzar la corrección dentro de 1 hora de la detección. Los esfuerzos deben continuar las 24 horas del día hasta que se implemente una resolución. El tiempo de resolución objetivo debe ser dentro de las 4 horas posteriores al momento en que se identificó y reportó el incidente.

Alto

Este nivel involucra incidentes y problemas que degradan el rendimiento o la funcionalidad del sistema pero que no resultan directamente en una interrupción completa o un riesgo inmediato para los sistemas críticos para el negocio.

Ejemplos:

- Degradación parcial del rendimiento del sistema que afecta a algunos, pero no a todos, los puntos finales.
- Vulnerabilidades de seguridad no críticas que podrían aumentar si no se abordan.
- incidentes y problemas intermitentes con los componentes del sistema que afectan la estabilidad o el rendimiento del sistema.

Objetivo de tiempo de resolución: se requiere respuesta dentro de las 4 horas posteriores a la identificación del problema, con un tiempo de resolución objetivo de 12 horas. Esto permite disponer de tiempo suficiente para evaluar el problema en profundidad e implementar soluciones sin prisas inmediatas, lo que reduce el riesgo de errores.

Moderado

Este nivel incluye incidentes y problemas que causan una interrupción mínima en el sistema y tienen un impacto reducido inmediato en las operaciones. Suelen ser problemas cosméticos, errores no urgentes o incidentes y problemas de rendimiento que no afectan las funcionalidades principales.

Ejemplos:

- Incidentes y problemas menores de rendimiento que no afectan significativamente las operaciones del sistema.
- Fallos en la interfaz de usuario o informes inexactos.

- Solicitudes de información o consultas operativas estándar que no requieren acción inmediata.

Objetivo de tiempo de resolución: la respuesta debe iniciarse dentro de las 12 horas, con un plan de resolución o mitigación previsto dentro de las 48 horas. Este marco de tiempo permite una programación y asignación de recursos adecuada sin desviar recursos críticos de incidentes y problemas de mayor gravedad.

Métricas

Severidad, Tiempos de Respuesta y Tiempos de Resolución:

Severidad	Descripción	Tiempo de Respuesta	Tiempo de Resolución
Crítico	Hay un impacto severo en las operaciones o la seguridad	1 hora	4 horas
Alto	Degradan el rendimiento o la funcionalidad pero no resultan directamente en una interrupción completa o un riesgo inmediato para los sistemas críticos para el negocio	4 horas	12 horas
Moderado		12 horas	48 horas

En adición a las métricas propuestas asociadas a la severidad, las siguientes son aplicables:

- Disponibilidad promedio de la consola > 99,9% (medida trimestralmente) - cuando la consola se provista en modalidad cloud -;
- Frecuencia de actualización mínima de firmas no mayor a 2 horas;
- AV-Test scoring > 12.

Plan de Pruebas y Aceptación

El objetivo del *Plan de Pruebas y Aceptación* es el de certificar que la nueva solución de protección de punto final cumple con los requisitos especificados, funciona correctamente en el entorno del CLIENTE y es aceptada formalmente tras la implementación.

Alcance

Pruebas Iniciales

- Pruebas de Instalación
    - Verificación de la correcta instalación en una muestra representativa de endpoints (mínimo 10% del total).
- Pruebas de Configuración
    - Validación de la configuración de políticas de seguridad y perfiles de usuarios.

Pruebas Funcionales

- Detección de Amenazas
    - Simulación de amenazas comunes y avanzadas para verificar la eficacia de detección.
- Respuestas a Incidentes
    - Ejecución de escenarios de incidentes para probar la capacidad de respuesta automatizada y manual.
- Monitoreo y Reportes
    - Validación del monitoreo en tiempo real y la generación de reportes de seguridad.

Pruebas de Integración

- Integración con Sistemas Existentes
    - Pruebas de integración con Active Directory, Fortinet y Wazuh SIEM.
- Interoperabilidad
    - Verificación de la interoperabilidad con otras soluciones de seguridad y TI.

Pruebas de Rendimiento

- Carga y Escalabilidad
    - Pruebas bajo diferentes niveles de carga para asegurar el rendimiento y la escalabilidad de la solución.
- Resiliencia y Recuperación
    - Simulación de fallos y verificación de los procedimientos de recuperación.

Aceptación Formal

- Informe de Pruebas
    - Documentación detallada de los resultados de las pruebas.
- Criterios de Aceptación
    - Se definirán en conjunto con el CLIENTE criterios claros para la aceptación final de la solución.
- Revisión y Aprobación
    - Revisión conjunta de los resultados por el CLIENTE y el proveedor.
- Firma de un documento de aceptación formal.

Provisión y Ejecución

Plazo

El Plazo de Provisión y Ejecución máximo será de 60 días hábiles corridos, contados a partir de la firma del contrato. Esta es una condición de cumplimiento obligatorio y causal de rechazo.

Ejecución

El OFERENTE deberá proveer un "*Gestor de Proyectos*" como líder de la ejecución del mismo.

Se deberá proveer reportes de avances con periodicidad semanal.

Licenciamiento

Los productos dentro del alcance deben estar licenciados para su uso por un plazo de 36 meses -plazo principal- a contar desde la recepción definitiva en producción.

Adicionalmente se podrán cotizar alternativas de contratación a 48 y 60 meses.

Deberán presentarse propuestas separadas para cada caso -ver apartado "*Ofertas*".

Renovación

A petición del CLIENTE la suscripción a los productos dentro del alcance podrá renovarse, de manera automática y mediando la aprobación expresa de ambas partes en los términos y precios de la contratación original, por períodos sucesivos 12 meses adicionales al plazo de licenciamiento originalmente contratado (36, 48 ó 60 meses).

Evaluación

La siguiente es la matriz de evaluación a aplicar en la selección de las propuestas:

Técnico		**60%**
Criterio	Peso	Incidencia
Aspectos funcionales	25.00%	15%
Antecedentes en casos similares	15.00%	9%
Plan de Implementación	15.00%	9%
Plan de Migración	10.00%	6%
Plazo de Implementación	15.00%	9%
Plan de Capacitación y Transferencia de Conocimiento	10.00%	6%
Soporte y Garantía Post-implementación	10.00%	6%
Económico		**40%**

Ofertas

Renglón 1 - Licencias por suscripción

Un mínimo de 2500 licencias de acuerdo con el detalle a continuación:

1. Un mínimo de 90 licencias para cubrir distintas versiones de Windows Server, incluyendo 2008R2, 2012R2, 2016, 2019 y 2022.
2. Un mínimo de 110 licencias para cubrir distintas versiones de Linux incluyendo CentOS (7 y superiores), Oracle (8 y superiores), Ubuntu LTS (18.04 y superiores) y Debian (8 y superiores).
3. Un mínimo de 2300 licencias para cubrir clientes de escritorio con diferentes versiones de Windows (7, 10 y 11)

Propuesta	Nombre y Descripción del producto	Plazo de suscripción (mes)	Cantidad	Costo Unitario	Costo total (IVA incluido)
Base		36			
Opcional		48			
Opcional		60			

Renglón 2 - Servicios Profesionales

De acuerdo con el ítem “*Servicios Profesionales*” del apartado de entregables y el formato a continuación.

Descripción	**Cantidad (horas/hombre)**	**Costo Unitario**	**Costo total (IVA incluido)**
(Ejemplo "Soporte experto, ingeniero de implementación")			

Si la propuesta incluyese la renovación de la actual solución, *Kaspersky Endpoint Detection and Response Optimum*, los servicios profesionales no serán parte de la contratación. Para este caso particular sólo se deberá incluir dentro del apartado una revisión del estado de salud (“healthcheck”) de la consola de gestión.

Los Servicios Profesionales deberán cotizarse en AR$.

Precios

De acuerdo con el Acuerdo General N° 132 de 2018 los servicios deben ser cotizados en pesos argentinos y los bienes pueden ser cotizados en dólares estadounidenses, es decir, **las licencias por suscripción pueden cotizarse en US$ y los servicios profesionales deben cotizarse en AR$.**

Garantías

Los servicios y bienes adjudicados deben estar garantizados durante toda la vida del contrato y en los términos de este documento.

Confidencialidad

El OFERENTE queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer en ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en los presentes documento, ni tampoco ceder a otros ni siquiera a efectos de conservación.

El OFERENTE debe asegurar confidencialidad, integridad y privacidad de los datos que puedan quedar expuestos al cumplir el objeto del contrato, explicitando las normas y procedimientos que respaldan el mismo.

El CLIENTE se reserva el derecho de controlar y auditar, por sí o por terceros, el cumplimiento de dichas normas en el momento que considere oportuno, incluyendo la auditoría de cada bien y/o servicio involucrado en el alcance de los servicios prestados por

el presente documento.

La pérdida de datos así como la difusión de estos a personas no autorizadas expresamente, como consecuencia del contrato, dará lugar a la rescisión automática y las acciones penales y civiles que correspondan.

Acuerdo de No Divulgación

El OFERENTE deberá firmar de manera previa al inicio de actividades un Acuerdo de No Divulgación en los términos del CLIENTE.

RODRIGUEZ Raul Cesar

Digitally signed by RODRIGUEZ Raul Cesar
Date: 2024.07.25 09:38:00 -03'00'