BANCO DE TIERRA DEL FUEGO | Tenés un banco

LICITACIÓN PÚBLICA DE PRECIOS NRO. 01-2023

"ADQUISICIÓN DE UNA SOLUCIÓN INFORMÁTICA DEL TIPO EDR (ENDPOINT DETECTION AND RESPONSE)"

Pliego de Bases y Condiciones Particulares

PLIEGO DE BASES Y CONDICIONES PARTICULARES

1) Objeto

El Banco de Tierra del Fuego llama a Licitación Pública de Precios 01/2023 para la "Adquisición de una solución informática del tipo EDR (Endpoint Detection and Response)", que permita mantener la operatividad de la red, protegiendo adecuadamente a los dispositivos informáticos finales (endpoint) de la Entidad de ataques informáticos.

2) Requerimientos

A continuación, se detalla el alcance y los requerimientos técnicos, y de soporte que deberá cumplir el Oferente, en el marco de la implementación de una solución de protección de Endpoints.

3) Alcance

El Banco de Tierra del Fuego requiere de un servicio centralizado de protección de puntos finales (Equipos de escritorio, laptops y servidores) que deberá ser gestionado mediante una sola consola de administración accesible desde cualquier equipo de cómputo a través de un navegador web como Microsoft Edge.
La solución deberá dar soporte a 700 endpoint (estaciones de trabajo, servidores, VDI y contar con al menos las siguientes características:

3.1) Consola central de administración / Agente:

a. La consola de administración deberá de ser accesible por los puntos finales en cualquier red de la "dependencia/institución/empresa" e incluso cuando se encuentren conectados a redes públicas sin necesidad de conexión VPN.
b. La solución deberá tener un agente único conectado a la consola central para todas las características descritas en este documento.
c. Deberá tener la capacidad de crear grupos con la finalidad de ser utilizados en la definición de políticas al menos por dominio, Sistema Operativo, Unidad Organizacional, versión del agente, tipo de equipo.
d. Se requiere el uso de un doble factor de autenticación para acceder a la consola de administración con el fin de incrementar la postura de seguridad.
e. La comunicación entre los agentes y el servidor deberá utilizar un túnel de seguridad SSL/TLS encriptado.
f. La consola de administración deberá centralizar la administración de los sistemas operativos Windows, Mac OS y Linux, además que el mismo agente podrá ser instalado en equipos físicos, virtuales, VDI y Cloud, dando la misma funcionalidad en cualquiera de ellos.
g. Es mandatorio que la consola de administración se encuentre alineada al MITRE ATT&CK FRAMEWORK.

h. La solución debe soportar la posibilidad de escalar, asegurando que independientemente del número de nodos de la instalación la plataforma funcione con el mismo nivel de eficiencia.
i. El agente desplegado permitirá la comunicación y gestión de tanto la protección de antivirus tradicional, así como de la protección de procesos desconocidos.

3.2) Antivirus de próxima generación:

La solución deberá contar como mínimo los siguientes elementos de análisis y características:
a. Aprendizaje máquina (machine learning en inglés) de forma local en cada punto final con Sistema operativo Microsoft Windows, Mac OS y Linux
b. Aprendizaje máquina configurable de forma independiente para detectar y para prevenir ataques, de tal forma que pueda tener visibilidad agresiva pero los parámetros de bloqueo moderados.
c. Integración con Virus total.
d. Detección y prevención de explotaciones de tipo Force DEP, Heap Spray pre-allocation, Force ASLR, SEH Overwrite protection, NULL Page Allocation, Remote Library Loading, Untrusted Font Loading.
e. Definir listas negras por hash.
f. Definir listas blancas por hash.
g. Definir listas blancas por archivos y/o carpetas.
h. Detección y prevención de scripts o comandos maliciosos vía powershell o CMD.
i. Detección y prevención de intentos de borrado de respaldos del sistema (volume shadow copy por sus siglas en inglés) comúnmente realizado por ataques de ransomware.
j. Detección y prevención de los procesos de cifrado de archivos relacionados a extensiones usadas por ransomware.
k. Detección y prevención de procesos asociados a accesos indiscriminados al sistema de archivos asociados a ransomware.
l. Detección y prevención de movimientos laterales.
m. Detección y prevención de intentos de elevación de privilegios.
n. Detección y prevención de intentos de uso de “sticky keys”
o. Detección y prevención de intentos de ejecución de rutinas de javascript por línea de comandos vía rundll32.exe
p. Bloqueo de todos los dispositivos o dispositivos específicos (unidades de almacenamiento extraíbles, dispositivos de captura de imágenes, unidades de CD/DVD, módems USB, Bluetooth, etc.), impidiendo la entrada de malware y fugas de información. Permitiendo la definición de diferentes acciones para cada tipo de dispositivo (bloqueo, acceso, lectura/escritura).
q. Los agentes deberán instalarse y funcionar de forma inmediata sin la necesidad de reinicio.

r. Se requiere que la solución no esté basada en firmas, de tal forma que los equipos no tengan que recibir diariamente actualizaciones de definiciones de virus o ataques.
s. Deberá contar con un tablero ejecutivo de detecciones de malware y de ataques informáticos
t. El agente podrá ser actualizado de forma automática desde la consola de administración.
u. Se deberá contar con un gerente técnico de cuenta para temas de soporte.

3.3) Sistema de detección y respuesta de puntos finales (EDR por sus siglas en inglés):

Las características mínimas del sistema de detección y respuesta de puntos finales son:
a. Deberá crear un árbol de procesos para que en una sola pantalla fácil de leer se indiquen todos los detalles y el contexto del ataque, a fin de realizar investigaciones más rápidas y sencillas.
b. Capacidad de contener el punto final o ponerlo en una cuarentena de red solo con una acción.
c. El agente deberá trabajar en modo kernel para poder visualizar y capturar la información para investigaciones forenses
d. El agente deberá contar un password de protección para desinstalación.
e. Los detalles de una detección deberán estar disponibles al menos noventa días
f. El agente deberá ser el mismo para todas las funcionalidades descritas en este anexo y no deberá exceder 30 MB.
g. Deberá mostrar un reporte de sensores inactivos por un determinado número de días.
h. Deberá contar con una conexión segura vía powershell a los equipos para realizar respuesta a incidentes, lo anterior si necesidad de permisos adicionales, es decir usando la misma conexión cliente servidor, y con al menos las siguientes funcionalidades: Listado de procesos, capacidad de detener procesos (Kill proccess), dump de procesos, dump de memoria, obtención de muestras, modificación de registros, eliminación de archivos.

4) Implementación y Configuración

El adjudicatario deberá de realizar la implementación del sistema. El personal que realizará la implementación debe ser certificado por el fabricante del sistema.
La instalación comprende como mínimo:

a. Creación y configuración de políticas de protección para el endpoint
b. Creación de grupos
c. Afinamiento de políticas de seguridad.

El adjudicatario deberá realizar todo lo necesario para el traslado, entrega e instalación del sistema en la Sucursal.
El Banco facilitará la infraestructura requerida para la instalación del sistema. El horario de trabajo debe ser de lunes a viernes de 08:00 a.m. a 05:45 p.m.

La instalación de la solución deberá ser realizada por un (01) persona certificada por el fabricante de la solución ofertada y debe tener una experiencia mínima de dos (02) años en labores relacionadas a seguridad de información / ciberseguridad.
La acreditación del perfil del personal se presentará para la suscripción del contrato, cuyo cumplimiento será verificado por el área usuaria.

De ser necesarios trabajos presenciales en las sucursales del Banco, el personal del adjudicatario deberá de contar con los Seguros Complementarios de Trabajos de Riesgo.

4.1) Capacitación

Se debe incluir, sin costo para el personal del Banco, capacitación con un mínimo de ocho (8 horas) entregando material referencial.
La capacitación se realizará en fundamentos, configuración, solución de problemas y gestión de la solución implementada.
La capacitación deberá ser virtual, dentro de los primeros 30 días calendario, luego de firmado el contrato.

4.2) Soporte Técnico

Se solicita un soporte técnico de 24x7 por el período que dure el contrato, con un tiempo de respuesta de tres (03) horas para restablecer el servicio. Deberá de incluirse un soporte por el fabricante 24x7, por el mismo periodo.

4.3) Garantía Comercial

Se requiere que se brinde una garantía comercial de doce (12) meses de la solución adquirida. La garantía debe ser otorgada por el adjudicatario y confirmada por el fabricante.
Las características de la garantía solicitada son:

- Las garantías y soporte iniciarán su vigencia desde el momento que se otorgue la conformidad de la puesta en marcha del sistema integral, contados a partir del día siguiente de la firma del Acta de Conformidad de la Instalación (entregar documento de garantía a la suscripción del acta de conformidad de instalación).

5) Periodo de contratación

El Contrato por el presente Servicio tendrá una duración de 36 meses, a partir del 01 de abril de 2023, solo si los indicadores de gestión tienen resultados positivos durante la duración del contrato.
Durante la vigencia del contrato el Banco tendrá acceso a la descarga e instalación de las actualizaciones del producto que libere el fabricante.
El Banco se reserva el derecho de reducir o cancelar el contrato, total o parcialmente, con una notificación previa de 30 días, debiendo abonar solo los servicios efectivamente prestados hasta la fecha de cancelación efectiva.

6) Plazo y lugar de entrega

El plazo de entrega de la solución informática deberá ser establecido juntamente con la oferta económica. El mismo será contado en días hábiles a partir de la emisión de la Orden de Compra respectiva.

7) Fecha, lugar y hora de los Eventos

Fecha límite para recepción de consultas: 20 de marzo de 2023 a la hora 13:00.

Fecha límite para la presentación de las ofertas: 23 de marzo de 2023

- ✓ Casa Central: Maipú Nº 897 – Ushuaia – TDF a la hora 13:00.
- ✓ Sucursal Buenos Aires: Sarmiento Nº 741 - CABA a la hora 15:00.

Fecha de apertura de las ofertas: 31 de marzo de 2023 a la hora 13:00.

La fecha de apertura quedará sujeta a la recepción en Casa Central de las ofertas enviadas por correspondencia interna desde la Sucursal Buenos Aires. En caso de que las mismas no sean recibidas en la fecha estipulada para la apertura, se notificará a los oferentes una nueva fecha para realizar la misma.

8) Identificación de la Licitación

Las propuestas deberán ser presentadas en un sobre debidamente cerrado, sin individualizar el oferente y consignar en su exterior la leyenda

BANCO PROVINCIA TIERRA DEL FUEGO

LICITACIÓN PÚBLICA DE PRECIOS - N° 01/2023

"Adquisición de una solución informática del tipo EDR"

9) Elegibilidad y calificación del Oferente

La elegibilidad y calificación del Oferente serán definidas con base en los siguientes requisitos:

El Oferente deberá operar en el país con una antigüedad mínima de 3 (tres) años, a considerar como referencia la fecha de apertura del presente llamado.

El Oferente deberá adjuntar en su oferta información o declaración jurada que certifique experiencia en la prestación de servicios de similares características y dimensiones al solicitado en la presente Licitación, en los últimos 3 años.

A tal fin, para aceptar el servicio se evaluarán los siguientes indicadores, que, en caso de no cumplirse, darán derecho a Banco de Tierra del Fuego para rescindir del acuerdo por

considerar que el oferente adjudicado no está en condiciones de desempeñar bien los servicios objeto de la contratación:

Casos de soporte tratados y resueltos	95%
Servicios acordados en el alcance detallado correctamente configurados	80%
Casos de uso acordados implementados	80%
Documentación de proyecto entregada	75%
SLAs de servicios cumplidos	80%

10) Condiciones

El Oferente sólo podrá usar o permitir el uso de la Información Confidencial a fin de efectuar los trabajos adjudicados. Como única excepción el Banco de Tierra del Fuego podrá autorizar - mediante solicitud escrita - al Oferente para el uso de la información obtenida como consecuencia de los trabajos realizados para abastecer su base de datos, con la cual se construyen normas para benchmark por categoría/Industria, sin identificación o mención sobre el cliente o marca utilizados.

El Oferente será responsable de asegurar que todas las personas bajo su dependencia a quienes sea divulgada la Información Confidencial según este acuerdo mantengan la confidencialidad de la misma y que no la divulguen a ninguna persona no autorizada.

La Información Confidencial seguirá siendo, en todo momento, propiedad del Banco y/o del tercero que le otorga el derecho de poseerla, y el Banco podrá reclamar al Oferente la devolución de cualquier instrumento en que se encontrare plasmada. Dentro de los treinta (30) días a partir de la fecha de recepción del requerimiento mencionado anteriormente, el Oferente deberá devolver la documentación original recibida y deberá destruir todas las copias y reproducciones (tanto escritas como electrónicas) que estuvieren en su posesión y/o en posesión de las personas a quienes se le hubiere suministrado en virtud de lo dispuesto en este acuerdo.

La obligación de confidencialidad establecida en el presente acuerdo terminará a los diez (10) años a partir de su fecha de celebración.

El Banco no garantiza la calidad, certeza o veracidad de la Información Confidencial. La recepción de Información Confidencial será interpretada en el sentido de que el Oferente ha reconocido y aceptado la posibilidad de error en el procesamiento e interpretación de

la Información Confidencial. El Banco, sus sociedades vinculadas y sus respectivos empleados, agentes, representantes y directores no tendrán responsabilidad alguna con respecto al uso que el Oferente haga de la Información Confidencial.

Las partes se comprometen a dar estricto cumplimiento con lo dispuesto por la ley 25.326 en materia de Protección de los Datos Personales, obligándose a mantener a la otra parte indemne de cualquier reclamo de un tercero derivado de las disposiciones de esta materia.

11) Garantía de Funcionamiento y Servicio Técnico

El Adjudicatario deberá garantizar el correcto desempeño del servicio provistos, por un lapso de 1 (un) año a contar desde la respectiva fecha de aceptación de contrato. Durante dicho período el Adjudicatario deberá cumplir con los SLAs establecidos.

12) Multas (de corresponder)

Adicionalmente a los SLA establecidos, Banco podrá aplicar penalidades por incumplimiento de los SLA.

Ambas partes acordarán que: en caso de no alcanzarse los indicadores de Niveles de Servicio, será responsabilidad del Adjudicatario:

Identificar la causa raíz de las fallas;

Corregir aquellos problemas atribuibles al Adjudicatario;

- Hacer recomendaciones al Banco para las mejoras pertinentes en los procedimientos.
- Informar al Banco los cambios realizados para alcanzar los Niveles de Servicio.
- Reportar al Banco todos los problemas de los cuales el Adjudicatario no es responsable y que pueden tener efecto adverso sobre los Niveles de Servicio incluyendo cambios de arquitectura o de procedimientos.

13) Confidencialidad

El oferente se obliga a mantener en la más estricta confidencialidad todos los datos, así como cualquier información que hubiere llegado o llegase a su conocimiento con motivo de o en ocasión de este llamado a licitación o durante el cumplimiento del objeto de la presente Licitación. Por otra parte, el Adjudicatario no utilizará para provecho propio, ni facilitará a terceros, ni divulgará ninguna información, datos y know how a los que pudiera tener acceso con motivo de la prestación de servicios, sin contar con el previo consentimiento expreso del Banco, asumiendo plena responsabilidad por cualquier trasgresión a esta obligación.

14) Cotización

La cotización también podrá efectuarse en dólares estadounidenses.

Al momento de la apertura de ofertas, se considerará el tipo de cambio vendedor del Banco de la Nación Argentina del día previo a la misma.

En cuanto al pago, se considerará el tipo de cambio vendedor del Banco de la Nación Argentina del día previo a la erogación.

ANEXO III

DECLARACION JURADA

.....de.....de 2023

La firma.....que suscribe, con domicilio real en la calle..... Nº..... de la ciudad de....., Provincia
de……..……,
domicilio especial en la calle..... N°……..... de la ciudad de..... de la Provincia de Tierra del Fuego A e I. A. S./C.A.B.A., y domicilio electrónico……, manifiesta que:

1. No se encuentra contemplado en los términos del Art. 2.5 del PLIEGO DE BASES Y CONDICIONES GENERALES.

2. Conoce y acepta la totalidad de la documentación que rige el llamado a LICITACION PUBLICA DE PRECIOS N° 01-2023 para la Adquisición de una solución informática del tipo EDR".

3. Acepta todas las condiciones locales, los precios de materiales y mano de obra de la localidad y todos los otros datos que puedan influir sobre el costo de los trabajos.

4. Renuncia a cualquier reclamación o indemnización originada por error en la interpretación de la documentación del llamado a Licitación.

5. Conoce la normativa que se aplica a la presente Licitación.

6. Se compromete al estricto cumplimiento de las obligaciones asumidas en su presentación a esta Licitación.

7. Conviene en mantener su oferta para la prestación del servicio del soporte, que integran la LICITACION PUBLICA DE PRECIOS N° 01-2023, durante un plazo de TREINTA DÍAS (30), PRORROGABLES POR CUARENTA Y CINCO (45) DÍAS ADICIONALES POR DECISIÓN DEL BANCO.

8. Reconoce expresamente que el domicilio electrónico indicado tiene carácter de especial en los términos del artículo 75 del Código Civil y Comercial de la Nación en el que se tendrán por eficaces todas las notificaciones, comunicaciones y emplazamientos que allí se dirijan.

Firma y sello