UNIDAD OPERATIVA DE CONTRATACIÓN
ADENDA N° 2 – LPN N° 3/2021

Asunción, 5 de febrero de 2021

Señores
PRESENTE

De nuestra consideración:

En atención a lo establecido en el punto 3 de la sección Datos de la Licitación (DDL) del Pliego de Bases y Condiciones para la **LICITACIÓN PÚBLICA NACIONAL N° 3/2021 – CONTRATACIÓN DE SERVICIOS DE GESTIÓN DE CIBERSEGURIDAD– AD REFERENDUM**, cumplimos en informar la modificación al PBC para el presente llamado:

Punto 1

El "**LOTE N° 3 SOLUCIÓN DE SEGURIDAD PERIMETRAL DEFINIDA POR SOFTWARE"** de la sección **ESPECIFICACIONES TÉCNICAS Y SUMINISTROS REQUERIDOS** del PBC, quedan redactados como sigue:

LOTE N° 3 - SOLUCIÓN DE SEGURIDAD PERIMETRAL DEFINIDA POR SOFTWARE		
LOTE N° 3 - ITEM N° 1 - Solución de Seguridad Perimetral Definida por Software		
3.1.1 Características de la Solución		
Marca y modelo de la solución ofertada:		
Se debe proveer una solución de seguridad perimetral definida por software, de manera a asegurar los accesos de los usuarios a las plataformas tecnológicas, gestionando los accesos dependiendo del contexto de la conexión utilizado por el usuario, para por lo menos 800 usuarios, y con protección para 1 (un) sitio o centro de datos, con soporte y mantenimiento del fabricante por 24 meses, en modalidad de suscripción, computados a partir de la emisión de la orden de inicio emitida por el área administradora del contrato.		
Debe brindar protección a los recursos sin que sean requeridos cambios obligatorios de configuración en la infraestructura de red, tales como switches, firewalls o routers.		
Debe soportar los protocolos TCP, UDP, GRE, HTTP, ICMP, ICMP v6, IPv6, AH, ESP,		
Debe ser capaz de re-enrutar el tráfico TCP entre el cliente y el recurso que requiere utilizar.		
Debe contar con soporte para ser administrada vía REST API, así como con un portal web de administración propietario.		
Debe tener software cliente para sistemas operativos como Windows 7 o superior, Android 6 o superior, IOS 11 o superior, Ubuntu 16.04 o posterior, RedHat y CentOS 7.7.		
Debe contar con modos de instalación de agentes para equipos desatendidos, la instalación deberá ejecutarse desde la línea de comandos.		
Debe tener soporte para implementarse en ambientes virtuales		
Debe tener soporte para implementarse tanto en servicios cloud como on-permise.		
Debe contar con las características para que el appliance que autentica a los usuarios no responda a tráfico de red hasta que el host de origen envíe un requerimiento de autorización de conexión mediante protocolo SPA (Single Packet Authorization)		
El proceso de autorización de conexión de usuario debe poder ser validado mediante un método de autenticación multifactor como un one-time password (OTP).		
El proceso de autenticación de los usuarios hacia los recursos protegidos y entre los diferentes componentes que controlen el acceso a los recursos de red debe realizarse de manera independiente y previo al establecimiento de cualquier canal de comunicación hacia los recursos privilegiados.		
El sistema se debe poder integrar a proveedores de identidad que utilicen los protocolos SAML, Radius o LDAP/LDAPS.		
El proceso de onboarding de nuevos usuarios y dispositivos debe ser compatible con autenticación multifactor.		
Los usuarios solo deben poder establecer canales de comunicación con los sitios protegidos que fueron autorizados para cada usuario tras el proceso de autenticación.		

Debe tener la capacidad de conectar a diferentes sitios (diferentes nubes, diferentes Centros de datos, oficinas, etc.) con una sola autenticación, no se admiten autenticaciones por sitio		
Todas las comunicaciones (tanto en el proceso de autenticación/autorización como el intercambio de datos con los recursos protegidos) deben estar cifrados.		
Debe funcionar como una entidad certificadora independiente para la validación de los usuarios y dispositivos.		
La comunicación entre servicios cloud, datacenter públicos y datacenter privados debe estar cifrada en todo momento.		
Debe contar con la opción de revocar en tiempo real los permisos de acceso a un usuario en particular o a todos los usuarios de Sistema.		
Debe ser capaz de revocar los permisos de conexión a cualquier dispositivo de red conectado.		
Debe ser posible establecer el tiempo de inactividad de la sesión de usuario de manera configurable por cada recurso o grupo de recursos de red.		
Debe ser posible establecer reglas de acceso de manera individual por cada recurso o grupo de recursos de red.		
Debe ser capaz de combinar múltiples reglas de acceso por cada usuario para establecer los permisos de acceso a través de microsegmentación.		
Debe ser posible configurar reglas de acceso que exijan la validación de autenticación multifactor de manera individual.		
Debe validar el contexto del usuario al momento de acceder a los recursos. Se deben verificar tanto los parámetros estáticos (tales como: nombre de usuario, versión del sistema operativo, dirección MAC) y dinámicos (tales como horario permitido de la conexión, cambios en dirección IP de origen, preguntas de control).		
La solución debe registrar toda información conocida sobre un usuario a medida que se otorga o deniega el acceso.		
Debe poder ser configurada en alta disponibilidad.		
Debe permitir aplicar estrategias de recuperación de desastres.		
Debe permitir agregar nuevos recursos o usuarios sin provocar indisponibilidad en los servicios		
Todos los componentes de la solución deben poder enviar los registros del sistema a un servidor centralizado de logs		
Debe ser escalable.		
La solución propuesta debe poder desplegarse en hipervisores como: VMware ESX, Microsoft Hyper-V, Citrix Hypervisor, Nutanix AHV, Amazon Web Services (AWS) y Microsoft Azure.		
Debe soportar al menos cifrado 256 bits AES de todas las comunicaciones entre todos los componentes		
Debe admitir el nivel de cifrado FIPS 140-2		
Debe estar basada en un appliance central y agentes		
Los agentes de la solución deben permitir diferentes tipos de instalación, incluyendo silenciosa y para equipos desatendidos		
Debe soportar la verificación de la postura del usuario final funciona sin la inclusión de software adicional de terceros		
Debe proveer mecanismos de protección que permitan ocultar recursos en un mismo segmento de red		
Debe contar con la flexibilidad para crear diferentes reglas de protección para ocultar recursos		
Debe contar con la opción de bloquear todo el tráfico de entrada o salida desde y hacia cualquier destino		
La opción de ocultar recursos debe ser aplicable a usuarios y servidores		
La solución debe proveer control de tráfico entre servidores en un mismo segmento de red		
Debe proporcionar túneles de red seguros y micro firewalls de forma individual para cada Cliente conectado		
Debe registrar todos los accesos de usuarios, incluyendo el trafico permitido y denegado.		
Debe permitir exportar el syslog a herramientas de correlación tipo SIEM		
Debe admitir el control de acceso basado en roles para la consola de administración		
Los usuarios solo deben poder establecer canales de comunicación con los sitios protegidos que fueron autorizados para cada usuario tras el proceso de autenticación.		
Debe ser capaz de supervisar TODOS los flujos de tráfico del centro de datos: tanto Este-Oeste (servidor-servidor) como Norte-Sur (cliente-servidor o red externa de servidor		

Debe contar con la capacidad para hacer respaldos de configuración que no impliquen reinicio del appliance		
Debe contar con la capacidad para hacer actualización de sistema operativo en línea o de forma local		
El oferente debe incluir todo el hardware y software de base (licencias de sistemas operativos y/o virtualización) que sea necesario para el funcionamiento óptimo de la solución, mientras sea ofrecido el servicio.		
Se debe incluir una plataforma en la nube para alojar los componentes que se requieran, para que se pueda realizar las conexiones directamente desde la nube cuando el usuario se encuentre fuera de la red del BCP.		

Punto 2

El "**LOTE N°4 ÍTEM 2 SOLUCIÓN DE SEGURIDAD ANTIMALWARE Y EDR"** de la sección **ESPECIFICACIONES TÉCNICAS Y SUMINISTROS REQUERIDOS** del PBC, quedan redactados como sigue:

LOTE N° 4 - ITEM N° 2 - Solución de Seguridad Antimalware y EDR			
4.2.1 Características principales de la Solución			
4.2.1.1	La solución ofertada debe estar basada en cloud, es decir, todo el procesamiento de datos se debe realizar en la nube.		
4.2.1.2	Debe permitir la búsqueda de información en tiempo real de distintos elementos dentro del endpoint.		
4.2.1.3	Debe permitir la creación de procesos de investigación, carga de información y análisis directamente desde la consola de monitoreo.		
4.2.1.4	Debe monitorear posibles anomalías en tiempo real y reportarlas a la plataforma para que sean analizadas.		
4.2.1.5	Debe permitir aplicar mecanismos de contención directamente de la consola y sin la necesidad de contar con herramientas de terceros para estos efectos.		
4.2.1.6	La solución debe utilizar distintos mecanismos de análisis los cuales deben incluir el uso de playbooks, información de terceros para detectar posibles incidentes dentro del ecosistema.		
4.2.1.7	La solución debe utilizar The MITRE Attack Framework para el análisis de posibles incidentes dentro de la organización.		
4.2.1.8	En el proceso de análisis de un posible incidente, la herramienta debe permitir asignar distintos estados al proceso de evaluación para determinar la etapa en que se encuentra un incidente.		
4.2.1.9	Debe permitir poner en cuarentena a los hosts comprometidos con el objetivo evitar movimientos laterales de códigos maliciosos.		
4.2.1.10	Debe permitir detener y/o eliminar un proceso en ejecución o persistente en las estaciones de trabajo.		
4.2.1.11	Debe permitir la segmentación de políticas para la operación de la plataforma, es decir, la herramienta debe permitir aplicar distintos tipos de políticas para un mismo ecosistema cliente.		
4.2.1.12	Debe permitir mecanismo de contención remotos en el endpoint.		
4.2.1.13	Debe permitir mecanismos de remediación remotos en el endpoint.		
4.2.1.14	Debe recolectar información de procesos en ejecución.		
4.2.1.15	Debe recolectar información de conexiones activas de red.		
4.2.1.16	Debe recolectar información de servicios que se ejecutan en el endpoint.		
4.2.1.17	Debe recolectar información de las tareas programadas en el endpoint.		
4.2.1.18	Debe recolectar información histórica de navegación web y descargas.		
4.2.1.19	Debe recolectar información del filesystem.		
4.2.1.20	Debe recolectar logs de eventos.		
4.2.1.21	Debe permitir eliminar/modificar llaves de registro.		
4.2.1.22	Debe permitir eliminar archivos remotamente.		
4.2.1.23	Debe permitir ejecutar scritp de manera arbitraria.		
4.2.1.24	Debe permitir desinstalar programas de manera remota.		
4.2.1.25	Debe permitir alertar un incidente en un tiempo cercano a tiempo real.		
4.2.1.26	La solución debe llevar el proceso de investigación a minutos.		
4.2.1.27	La solución debe tener cobertura sobre TTPs descritos en Mitre Attack Framework.		
4.2.1.28	La solución debe poseer un proceso de investigación guiada, el cual permita realizar una investigación profunda a un hallazgo clave. La investigación a ser realizada se basa en la hipótesis de la existencia de algún comportamiento anómalo, guiando al analista en las posibles acciones de contención. Esta investigación se centra en la capacidad de poder identificar esto hallazgos siempre basados en el MITRE ATT&CK Framework.		

4.2.1.29	Debe prevenir los ataques que aún no han afectado a la organización, poder priorizar qué amenazas son más importantes y urgentes en función de la eficacia de detección de las contramedidas de otros.		
4.2.1.30	Debe predecir como probablemente funcionarían mis contramedidas al observar la eficacia de detección comparativa de las contramedidas de otros.		
4.2.1.31	Ofrecer una solución que incluya información sobre amenazas + priorización + recomendaciones + automatización.		
4.2.1.32	Debe incluir una solución que brinda Análisis de seguridad proactiva y procesable, inteligencia activa integral, análisis distintivo de amenazas globales, protección proactiva.		
4.2.1.33	La solución de análisis de seguridad proactiva debe integrarse en forma nativa con la solución EDR, de tal manera a poder contar con toda la facilidad de información para investigación de IOC que se manifiestan en el entorno.		
4.2.1.34	Solución de filtrado de contenido Web, que incluye funcionalidades nativas integradas de: filtrado URL, control de aplicaciones Web, antimalware y prevención de fuga de información (DLP).		
4.2.1.35	La solución debe contar con un servicio web Proxy para la utilización de filtrado web de los usuarios móviles de la organización con el fin de contar con seguridad en todos los sitios físicos a través de la nube.		
4.2.1.36	La solución debe orientarse a un despliegue de protección web hibrida, es decir utilizar una gestión central para la navegación local como para el filtrado en nube sin importar donde se encuentre el usuario.		
4.2.1.37	La solución debe contar con la opción de que el tráfico web de usuarios pueda enrutarse de forma automática hacia la nube para su análisis fuera de sitio		
4.2.1.38	La solución debe brindar un mecanismo para que los usuarios no manipulen el proxy de navegación, sea independiente del navegador y aplicaciones que utilicen internet para que sean filtrados de forma transparente.		
4.2.1.39	Solución de filtrado de contenido Web debe estar basado en sistemas virtuales y servicio SaaS en nube de tipo Gateway.		
4.2.1.40	La solución deberá permitir la inspección del tráfico SSL, HTTPS de forma que pueda analizar sobre este protocolo para la identificación de malware.		
4.2.1.41	La solución debe permitir descifrar el tráfico SSL para escanearlos y luego volver a cifrarlo antes de enviar al usuario.		
4.2.1.42	La solución debe soportar terminación SSL para pedidos HTTPS.		
4.2.1.43	La solución debe soportar hasta 5 dispositivos por usuarios, entre ellos Android e IOS.		
4.2.1.44	Debe contar con un panel de visualización de métricas de uso de la plataforma.		
4.2.1.45	Debe permitir la creación de distintos roles de usuarios dentro de la consola de gestión para el perfilamiento de usuarios.		
4.2.1.46	Debe permitir la vinculación de procesos mediante mecanismos de trace.		
4.2.1.47	Debe permitir la visualización de información en distintos modelos, desde vistas graficas de los hallazgos hasta el detalle de la información recolectada.		
4.2.1.48	Debe permitir la visualización de los hallazgos mediante vistas gráficas.		
4.2.1.49	Debe permitir visualizar eventos históricos.		
4.2.1.50	Debe poseer integración con una herramienta para la gestión de políticas y despliegue ya sea en la nube o desplegada onpremise.		
4.2.1.51	La solución ofertada, debe permitir la integración nativa y sencilla con Windows defender y sus módulos de exploit Guard y Firewall		
4.2.1.52	Se debe poder realizar la instalación y gestión de la plataforma de EDR sin tener dependencias de la solución de defensa instalada en el Endpoint.		
4.2.1.53	Debe detectar comportamiento anómalo post-infección y permita remediar un incidente mediante acciones particulares o generales.		
4.2.1.54	Debe contar con una consola de administración donde se aprecie las amenazas o riesgos presentes en el equipo.		
4.2.1.55	Debe ser capaz de colectar información en las estaciones y servidores tales como flujos de red, creación/modificación de archivos, ejecución de procesos, copia de documentos para evaluar comportamiento anómalo.		
4.2.1.56	Debe ser capaz de almacenar de forma local la información de actividad de red		
4.2.1.57	Debe contar con un asistente que ayude al usuario a generar la instrucción de forma adecuada en la configuración de búsqueda.		
4.2.1.58	Las búsquedas y acciones deben poder ser configuradas por el administrador de la solución.		
4.2.1.59	Se deben poder configurar las búsquedas y acciones como instrucciones en la línea de comandos de los sistemas windows, el shell en linux, utilizando cmdlet de powershell o a través de instrucciones programadas en VB.		
4.2.1.60	Debe permitir ejecutar búsquedas masivas de todo dato colectado desde una consola central.		
4.2.1.61	Debe permitir generar acciones de respuesta automáticas a las búsquedas.		
4.2.4.62	Debe permitir ejecutar acciones precisas de remediación o contención en las estaciones de trabajo, como resultado de la respuesta a búsquedas de solución.		

4.2.4.63	Debe permitir visualizar la totalidad de las amenazas		
4.2.4.64	Debe permitir visualizar la edad y prevalencia de las amenazas		
4.2.4.65	Debe permitir visualizar la línea de tiempo de las amenazas		
4.2.4.66	Debe permitir visualizar los equipos afectados por cada amenaza		
4.2.4.67	Debe permitir visualizar la trazabilidad detallada de las acciones realizadas por la amenaza en cada equipo.		
4.2.4.68	Debe permitir visualizar la reputación del ejecutable responsable de cada amenaza.		
4.2.4.69	Debe realizar acciones de remediación sobre cada uno de los equipos afectados y los elementos involucrados en cada una de las trazas, desde la consola de detección.		
4.2.4.70	Debe contar con un panel de trazabilidad de las acciones realizadas por las amenazas en cada endpoint.		
4.2.4.71	Debe permitir visualizar la línea de tiempo en donde se evidencia inicio y fin de cada proceso.		
4.2.4.72	Debe permitir visualizar información acerca de la creación, eliminación o modificación de llaves de registro.		
4.2.4.73	Debe permitir visualizar información acerca de la creación, eliminación o modificación de archivos.		
4.2.4.74	Debe permitir visualizar información acerca de las conexiones de red realizadas		
4.2.4.75	Debe permitir visualizar información acerca del inicio y fin de subprocesos		
4.2.4.76	Debe permitir al administrador determinar por extensión los tipos de archivos a los que se desea dar seguimiento.		
4.2.4.77	Debe permitir dar seguimiento a la creación, modificación y borrado de cualquier tipo de archivo.		
4.2.4.78	Se debe entregar todos los módulos de software necesarios para la correcta implementación de lo requerido en este lote. Se deben incluir todas las licencias necesarias para al menos 1200 usuarios, con soporte y mantenimiento del fabricante por 24 meses, en modalidad de suscripción, computados a partir de la emisión de la orden de inicio emitida por el área administradora del contrato.		
4.2.4.79	El oferente debe incluir todo el hardware y software de base (licencias de sistemas operativos y/o virtualización) que sea necesario para el funcionamiento óptimo de la solución, mientras sea ofrecido el servicio. De manera opcional, el BCP ha reservado la siguiente infraestructura de su propiedad, la cual podrá ser utilizada por el oferente para la instalación de las soluciones ofertadas en este lote (en caso de que sean compatibles): 1 (un) Servidor Cisco UCS C220-M3S, 12 CPU físicos y 24 vCPU (2 sockets) 2Ghz, 128 GB RAM y 1,5 TB de almacenamiento; 1 (un) Servidor Cisco UCS C220-M4S, 12 CPU físicos y 24 vCPU (2 sockets) a 2Ghz, 128 GB RAM y 1,5 TB de almacenamiento; y 1 (un) Servidor DELL T710, 8 CPU físicos y 16 vCPU (2 sockets) a 3Ghz, 64 GB RAM y 1,5 TB de almacenamiento.		

Punto 3

Se modifican en el SICP las fechas establecidas en el SICP.

Atentamente,

VICTOR ENRIQUE CIPRIANO CARUGATI IBAÑEZ
Firmado digitalmente por VICTOR ENRIQUE CIPRIANO CARUGATI IBAÑEZ
Fecha: 2021.02.05 11:56:01 -03'00'

Encargado de Despacho
Unidad Operativa de Contratación

SILVIA PATRICIA NUÑEZ MAZACOTTE
Firmado digitalmente por SILVIA PATRICIA NUÑEZ MAZACOTTE
Fecha: 2021.02.05 12:25:13 -03'00'

Gerente
Gerencia de Patrimonio y Logística

SONIA ISABEL GOMEZ GONZALEZ
Firmado digitalmente por SONIA ISABEL GOMEZ GONZALEZ
Fecha: 2021.02.05 12:33:11 -03'00'

Encargada de Despacho
Sub Gcia. Gral. de Administración y Finanzas

WALTER ANTONIO ZARATE ALMIRON
Firmado digitalmente por WALTER ANTONIO ZARATE ALMIRON
Fecha: 2021.02.05 13:23:14 -03'00'

Encargado de Despacho
Gerencia General
Banco Central del Paraguay