METODOLOGÍA DE OBTENCIÓN DE LOS PRECIOS DE REFERENCIA - RES. DNCP N° 1890/2020 DEL 07/05/2020.

LCO N° 54/2023 - CONTRATACIÓN DE SOLUCIÓN DE AUTOEVALUACIÓN DE CONTROLES DE CIBERSEGURIDAD - ID Nº 428680

							RESPONSABLE: Área Técnica Requirente (Departamento de Ciberseguridad)										
ÍTEM	DESCRIPCIÓN	CONTRATACIÓN ANTERIOR				FUENTES DE REFERENCIA			PROMEDIO	PRESENTE LLAMADO					VARIACIÓN ENTRE LA ADJUDICACIÓN ANTERIOR Y EL PRECIO REFERENCIAL CONSIDERADO	DIFERENCIAS A SER CONSIDERADAS ENTRE EL PRECIO REFERENCIAL Y POTENCIALES OFERTAS	
		Duración/ Tipo	Precio Unitario	Cantidad Adjudicada	Total	FUENTE 1: Presupuesto presentado por la firma Grupo Welltech MAYO 2023	FUENTE 2: Presupuesto presentado por la firma Information Security Services S.A. JUNIO 2023	FUENTE 3: Presupuesto presentado por la firma Knowledge Consulting S.A. JUNIO 2023		Duración del contrato/ tipo	Procedimiento/ Método (Precio referencial final)	Precio referencial considerado	CANTIDAD	PRECIO TOTAL			
	CONTRATACIÓN DE SOLUCIÓN DE AUTOEVALUACIÓN DE CONTROLES DE CIBERSEGURIDAD	N/A				Precio Unitario	Precio Unitario	Precio Unitario								15% POR ENCIMA DEL PRECIO REFERENCIAL	25% POR DEBAJO DEL PRECIO REFERENCIAL
	Contrato Abierto: NUEVAS / AMPLIACIÓN / RENOVACIÓN																
	X																
1	CONTRATACIÓN DE SOLUCIÓN DE AUTOEVALUACIÓN DE CONTROLES DE CIBERSEGURIDAD	N/A				455.000.000	450.000.000	463.808.000	456.269.333	Duración: 24 meses. Tipo: Contrato Cerrado	Se optó por el precio más bajo de las fuentes obtenidas	450.000.000	1	450.000.000	N/A	**517.500.000**	**337.500.000**

MIGUEL MARIA TOFFOLETTI CAÑETE
Firmado digitalmente por MIGUEL MARIA TOFFOLETTI CAÑETE
Fecha: 2023.07.27 10:22:17 -04'00'

DICTAMEN UOC:

Con base en los datos proporcionados por el área técnica requirente, Departamento de Ciberseguridad, incluidos en la presente planilla, los documentos respaldatorios adjuntos y el método indicado por la misma, esta Unidad Operativa de Contratación señala que la metodología utilizada a fin de determinar el precio referencial ha sido el especificado en la columna "Procedimiento/Método (Precio referencial final)" de las fuentes obtenidas. Se menciona que debido a la especialidad de la solución objeto de la suscripción a ser contratada y por ser una nueva contratación, no se cuenta con antecedentes de llamados anteriores, tampoco se ha podido obtener precios de contrataciones de otras instuciones, páginas web, publicaciones, catálogos u otros; por lo que se obtiene el precio referencial en virtud de lo establecido en el Anexo de la Res. DNCP N° 1890/2020 que dice: *"Excepcionalmente, si por la complejidad, especialidad o particularidad de la contratación no resultare posible alcanzar la cantidad de 3 (tres) fuentes requeridas para la obtención de los precios, la convocante podrá adoptar el mecanismo que considere apropiado para obtener los Precios de Referencia, en cuyo caso tal situación deberá ser suficientemente fundada en el Dictamen firmado por el Encargado de la UOC en el que se detalle la metodología utilizada para la obtención de los Precios de Referencia".-*

VICTOR ENRIQUE CIPRIANO CARUGATI IBAÑEZ
Firmado digitalmente por VICTOR ENRIQUE CIPRIANO CARUGATI IBAÑEZ
Fecha: 2023.07.27 11:07:04 -04'00'

MARIA EMILIA ACHA PALACIOS
Firmado digitalmente por MARIA EMILIA ACHA PALACIOS
Fecha: 2023.07.25 11:30:50 -04'00'

Freddy Barreto Villar

De: Ariel Emilio Caceres Ramirez
Enviado el: miércoles, 14 de junio de 2023 17:18
Para: Freddy Barreto Villar
Asunto: Fwd: Solicitud de cotización KC-Latam
Datos adjuntos: Propuesta Monitoreo de Amenazas BCP.pdf

FYI

Enviado desde Outlook para Android

From: Raul Monges <raul@kc-latam.com>
Sent: Tuesday, June 13, 2023 12:55:10 PM
To: Ariel Emilio Caceres Ramirez <acaceres@bcp.gov.py>
Subject: RE: Solicitud de cotización KC-Latam

Buenos días,
Envío el presupuesto solicitado.
Ante cualquier consulta no duden en contactarse.

Saludos cordiales

KC LATAM

Raul Monges Luces
Country Manager-Paraguay
Cel: +595 991 925047
Web: www.kc-latam.com

De: Ariel Emilio Caceres Ramirez <acaceres@bcp.gov.py>
Enviado: martes, 6 de junio de 2023 13:48
Para: Raul Monges <raul@kc-latam.com>
Cc: Freddy Barreto Villar <fbarreto@bcp.gov.py>
Asunto: RE: Solicitud de cotización KC-Latam

Buenas tardes, estimado Raúl:
Reiteramos una vez más la solicitud enviada en fecha 24/05/2023, atendiendo a que nos encontramos con plazos vencidos para obtener la información solicitada.
Agradeceríamos favor nos puedas indicar, a más tardar el día de mañana, **miércoles 07/06/2023,** si ofrecen este software (con su respectivo presupuesto) o si es que no.
Saludos,

ANIVERSARIO DEL GUARANÍ 80 1943 - 2023

ARIEL EMILIO
CÁCERES RAMIREZ
Director – Departamento de Ciberseguridad

BANCO CENTRAL DEL PARAGUAY
Federación Rusa y Augusto Roa Bastos
4to. Piso Asunción, Paraguay
Tel. (595 21) 619 2696
E-mail: acaceres@bcp.gov.py
dcs@bcp.gov.py

De: Freddy Barreto Villar <fbarreto@bcp.gov.py>
Enviado el: jueves, 1 de junio de 2023 14:49
Para: raul@kc-latam.com
CC: Ariel Emilio Caceres Ramirez <acaceres@bcp.gov.py>
Asunto: RV: Solicitud de cotización KC-Latam

Buenas tardes! Espero se encuentre muy bien.
¿Podríamos tener una respuesta a la solicitud de cotización del correo precedente?
Si requieren alguna información adicional, por favor, no duden en consultar.

Saludos,
F. Barreto

De: Freddy Barreto Villar
Enviado el: miércoles, 24 de mayo de 2023 13:45
Para: raul@kc-latam.com
Asunto: Solicitud de cotización KC-Latam

Buenas tardes, estimados:

Quisiéramos consultarles primeramente si ofrecen un Software con las siguientes características:

1. Solución que permita recopilar, calificar y monitorear la salud general de la ciberseguridad de al menos 10 (diez) entidades (postura de seguridad).
2. La postura de seguridad o monitoreo de riesgo debe estar basado en el score/puntaje, y debe estar integrado en la plataforma.
3. La plataforma debe brindar una visión holística de la postura de seguridad de la organización y de terceros, que permita evaluar dicha postura de manera general y con posibilidad de indagar la causa raíz de las señales de riesgo.
4. La solución debe permitir crear cuestionarios que puedan ser editables en cuanto a la forma y opciones de respuesta.
5. Estos cuestionarios podrán ser completados por otras entidades a modo de autoevaluación de controles técnicos de ciberseguridad.
6. La solución debe permitir tipificar a las entidades participantes de los cuestionarios según los criterios que el BCP defina.
7. Debe incluir soporte y mantenimiento local (proveedor) y del fabricante por 24 meses desde la puesta en funcionamiento de la herramienta, en modalidad de licenciamiento SaaS (Software as a Service).

En caso de que así sea, agradeceríamos nos puedan remitir un presupuesto aproximado de la solución correspondiente.

Si requieren mayores detalles acerca de lo solicitado, favor consultar.

Gracias y saludos,

FREDDY BARRETO V.
Departamento de Ciberseguridad

BANCO CENTRAL DEL PARAGUAY
Federación Rusa y Augusto Roa Bastos
4to. Piso Asunción, Paraguay
Tel. (595 21) 619 2722

Propuesta

Monitoreo de Amenazas

para

Banco Central del Paraguay

Por

Versión 2.0

28/2/2023

Asunción, 13 de junio de 2023

Sr.

Ariel Caceres

Presente

Ref.: Monitoreo de Amenazas Inteligentes

Estimado:

Por medio de la presente, nos es grato presentarles a Uds. nuestra propuesta de Servicio Gestionado de Amenazas Inteligentes por **KC Latam (Knowledge Consulting)** usando tecnología de nuestro partner Blueliv.

El ***Servicio Gestionado de Amenazas Inteligentes*** basado en Threat Compass de BlueLiv es una solución en línea que monitoriza y recolecta información de más de 10.000 fuentes de información, de forma continua (24x7), entregando automáticamente al cliente sólo lo que se denomina como "Targeted Cyber Threat Intelligence". Es decir, entregando únicamente información e inteligencia acerca de las amenazas dirigidas al propio cliente

Seguros que nuestra propuesta satisface sus requerimientos, quedamos a su total disposición en lo que considere necesario.

Saluda Atentamente a Ud.

Raul Monges Luces

Country Manager

Cel +54 991-925047

Email: raul@kc-latam.com

Aviso de Confidencialidad

Este documento es confidencial y propiedad de **Knowledge Consulting sa (KC LATAM)**, y no puede ser utilizado para propósitos distintos de la evaluación de la propuesta de Knowledge Consulting que en él se incluye.

En ningún caso el documento, o cualquiera de sus partes, deberán ser distribuidos a terceros sin el consentimiento explícito y por escrito por parte de **Knowledge Consulting**.

Asimismo, ninguna de las partes del documento puede ser copiada, fotografiada, fotocopiada, transmitida electrónicamente, almacenada en un sistema de gestión documental o reproducida mediante cualquier otro mecanismo sin la autorización previa y por escrito por parte de **Knowledge Consulting.**

KC LATAM

KNOWLEDGE CONSULTING LATAM

Índice

KC LATAM **5**
Partners 5
Clientes 6
Propuesta Técnica **7**
Introducción 7
Descripción y alcance 7
Diferencias Claves 8
Algunos Clientes 9
Potencia y Flexibilidad 10
Arquitectura Modular de la Plataforma 11
Eficiencia 13
Reducción de falsos positivos con filtros avanzados 14
Modelo de Servicio 16
Horario de Cobertura de los Servicios 16
Punto Único de Contacto 16
Reportes/Reporting 17
Módulos incluidos en el servicio 18
Propuesta Comercial **18**
Cargos del servicio 18
Condiciones Comerciales 18

KC LATAM

Empresa fundada en 2012, líder en soluciones de IT y Ciberseguridad. Ofrece Servicios de Consultoría, Implementación de Software y Outsourcing, entregando soluciones “end-to-end” y de valor agregado a sus clientes del sector público y privado.

Durante toda su trayectoria, KC LATAM ha acompañado el crecimiento de diversas organizaciones con un enfoque claramente orientado al concepto de “empresa adaptable”, brindando una amplia gama de soluciones de tecnología que permiten alinear la optimización de los recursos de IT con los objetivos del negocio.

La compañía cuenta con un equipo de profesionales en el área de preventas, gestión comercial, servicios profesionales y administración financiera que posee el conocimiento y la experiencia para el diseño e implementación de soluciones que se ajustan a la medida de cada cliente, según sus objetivos, procesos de negocios, entornos de sistema y necesidades específicas.

Desde hace varios años, KC LATAM exporta sus servicios al mundo, desarrollando proyectos en Paraguay, Estados Unidos, Uruguay, Chile, Reino Unido y España.

Finalmente, **KC LATAM** busca ofrecer soluciones orientadas a simplificar los entornos de tecnología de las empresas con soluciones altamente integradas; y con capacidad para realizar una planificación de los proyectos a través de un control exhaustivo del proceso de Ciclo de Vida de los Sistemas.

Partners

Clientes

falabella.
Santander
Claro
Bci
somosdiferentes
PRISMA
medios de pago
Banco de Chile
TELECOM
un mundo próximo
transbank
Macro
SANCOR SEGUROS
LINK
DIRECTV
Hewlett Packard Enterprise
CaixaBank
Redbanc
Medifé
Itaú
BancoEstado
BOLDT
bancor
Mercantil andina
BPN
NUESTRO BANCO
FiberCorp
PROSEGUR
CCA
nexus
ADEXUS
First Data.
BancoCiudad
BANCO COMAFI
Si te va bien, nos va bien.
BANCOPIANO
BT
Nuevo
Banco de Santa Fe
BANCO
Hipotecario
Banco Falabella
FRESENIUS
BANCOBICE
Telefónica
DXC.technology
Nación Servicios
UADE

Propuesta Técnica

Introducción

Knowledge Consulting sa (**KC LATAM)** se complace en poner a consideración de BCP la presente propuesta de Servicio de Monitoreo de Amenazas basado en la herramienta BlueLiv.

Descripción y alcance

Creemos que nuestras soluciones y servicios destacan en el mercado por su **arquitectura modular** y la **tecnología de automatización** en la detección de la Inteligencia de Amenazas.

En primer lugar, trabajamos con nuestros clientes para entregar ciberinteligencia adaptada y dirigida a las necesidades de su negocio. Al fin y al cabo, el modularidad de ***la solución de Amenazas Inteligentes con la solución de Threat Compass de BlueLiv*** nos permite ofrecer un servicio optimizado y de calidad que se adapta al presupuesto de nuestros clientes, aportando además la inteligencia que realmente es de interés. De la misma forma que no hay dos clientes con las mismas necesidades, KC LATAM tampoco entiende que una única solución puede dar respuesta a dichas necesidades dispares, por eso, nuestras soluciones y servicios ofrecen respuestas efectivas a las particulares necesidades de Seguridad de cada uno de nuestros clientes.

En segundo lugar, nuestro partner BlueLiv cuenta con una tecnología desarrollada y afinada durante casi una década, lo que nos permite además disponer de una de las más extensas colecciones de amenazas identificadas del mercado.

Somos capaces de encontrar y entregar Inteligencia de Amenazas actualizada, en la mayoría de los casos es crítico. Por ejemplo, la detección temprana de credenciales (no superior a un par de días desde el momento en que se vieron comprometidas) puede reducir dramáticamente el impacto negativo de su perdida ya que los cibercriminales no tendrán tiempo para usarlas y conseguir sus objetivos (en muchos casos financieros).

Otro factor diferenciador es la “usabilidad”, Blue Liv con Threat Compass ha sido desarrollado pensando en nuestros clientes y en los usuarios que lo van a utilizar. La interfaz de trabajo es un entorno verdaderamente amigable y lo que es aún más importante, la información se presenta en un formato fácilmente entendible por cualquier tipo de usuario. Pero si lo que desea es profundizar en el análisis, Threat Compass cuenta con un nivel de detalle tal que será fácil para sus analistas realizar sus investigaciones. Por ejemplo, tras un incidente, distintas personas y equipos demandan distinta información: los analistas quieren saber cómo paso mientras que los CISOs quieren saber que no volverá a pasar. Threat Compass puede satisfacer ambas necesidades.

Adicionalmente, nuestra API permite la integración sencilla y directa con soluciones e infraestructuras de seguridad ya existentes. La sencilla configuración y puesta en marcha del servicio de CIBERVIGILANCIA utilizando Threat Compass permite a nuestros clientes ver el valor del servicio en minutos, no en meses.

©2023 Knowledge Consulting sa

Diferencias Claves

La tecnología y los servicios de Blueliv son únicos en múltiples aspectos y aportan valor a la seguridad de nuestros clientes desde el primer día. De entre las múltiples diferencias de nuestra oferta, nos permitimos destacar estas cuatro diferencias clave:

1. **Tecnología patentada y dilatada experiencia en análisis de malware**. En el núcleo de las tareas de investigación que desarrolla Blueliv están las relacionadas con la identificación y análisis de los ecosistemas de malware que afectan a nuestros clientes. Blueliv, con su tecnología propietaria y patentada, es líder global en la recolección y procesamiento de muestras de malware lo que nos permite identificar y extraer información de gran calidad y relevancia sobre dicho malware y su modus operandi. El cliente tendrá acceso a este conocimiento a través de la plataforma Threat-Compass.

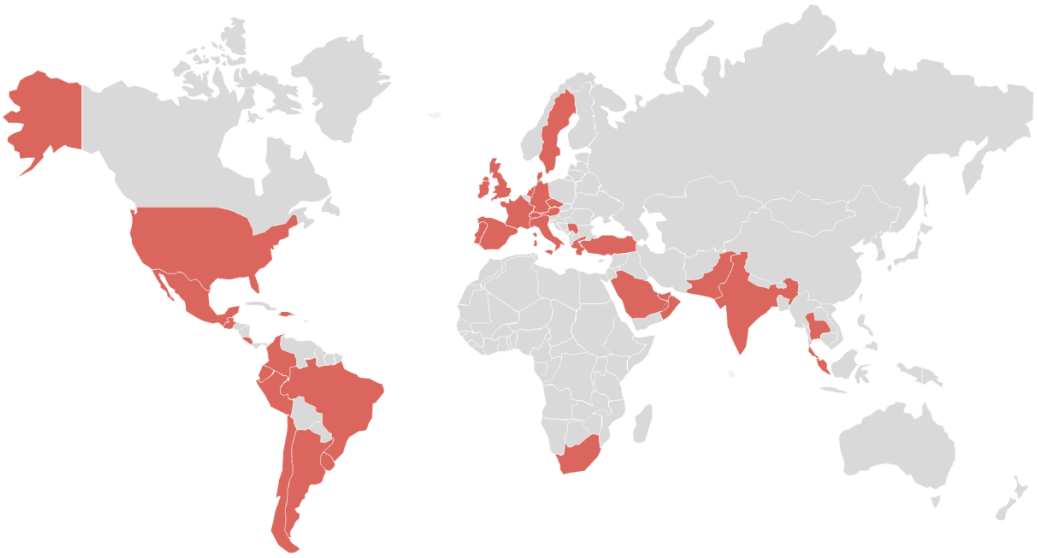
2. **La más rápida detección y respuesta de incidentes gracias a la automatización**. La plataforma Threat-Compass está en servicio 24x7 para detectar, en miles de fuentes, información de amenazas relevantes para nuestros clientes. En muchos casos únicamente relevantes para una empresa en concreto. La información se obtiene de forma automatizada y se entrega en una plataforma fácil de utilizar, en un formato fácil de entender y accionable. Con ello se reducen los tiempos de detección y también los de respuesta y remediación y/o mitigación.

3. **Ser el Desarrollador Líder Europeo en Threat Intelligence**. Blueliv desarrolla su propia Inteligencia de Amenazas (Threat Intelligence). Uno de nuestros principios básicos es ser flexibles. Flexibles para adaptarnos y buscar soluciones a las necesidades de nuestros clientes. Flexibles en el modo en el que desarrollamos nuestros productos y servicios. Flexibilidad que se demuestra en la arquitectura modular de nuestra plataforma THREAT COMPASS.

4. **Un equipo profesional de dilatada y contrastada experiencia**, El equipo humano es uno de nuestros valores más destacados, apreciados y valorados. Destacados, por la gran experiencia que hemos ido acumulando a lo largo de los años, desde que en 2009 empezamos a ofrecer nuestros servicios de seguridad: apreciados por nuestros clientes a nivel nacional e internacional, cuya satisfacción se confirma con su renovada confianza en Blueliv; y valorados por las empresas del sector a nivel global en dónde son invitados a participar en foros y charlas para presentar nuestros informes.

©2023 Knowledge Consulting sa

Algunos Clientes



Presencia de clientes y usuarios de Blueliv en el mundo.

Potencia y Flexibilidad

Blueliv recupera, filtra, clasifica e indexa de forma automática y en tiempo real información relativa a amenazas dirigidas al cliente, facilitando la labor de los analistas y reduciendo la ventana de oportunidad de un ataque.

El ***Servicio Gestionado de Amenazas Inteligentes*** de KC LATAM basado en Threat Compass de BlueLiv es una solución en línea que monitoriza y recolecta información de más de 10.000 fuentes de información, de forma continua (24x7), entregando automáticamente al cliente sólo lo que se denomina como “Targeted Cyber Threat Intelligence”. Es decir, entregando únicamente información e inteligencia acerca de las amenazas dirigidas al propio cliente.

Threat Compass consulta estas miles de fuentes de forma automática a través de diversas tecnologías propias que se ejecutan de forma programada y periódica. La información obtenida de las fuentes es indexada en tiempo real y queda disponible en Threat Compass para su revisión y/o gestión.

Toda la información recuperada puede clasificarse utilizando etiquetas y/o filtros, que arrojan inteligencia sobre la monitorización. Por ejemplo, si se configura la herramienta para etiquetar los resultados dependiendo del producto mencionado, podríamos generar automáticamente una gráfica que muestre el número de menciones a cada uno de nuestros productos, identificando fácilmente cual es más popular en las redes sociales.

Los resultados recuperados pueden clasificarse en base a diferentes criterios dependiendo del módulo, por ejemplo, nivel de confidencialidad, fuente de información, región, etc. Pudiendo crearse también criterios personalizados, por ejemplo, clasificar los resultados por ministerio u organismo afectado.

©2023 Knowledge Consulting sa

Arquitectura Modular de la Plataforma

Las 10.000 fuentes de información mencionadas anteriormente se dividen en varios módulos que se detallan en la siguiente tabla:

Modulo	Descripción de la utilidad del módulo
Credenciales	Este módulo entrega al cliente credenciales comprometidas relacionadas con los dominios o IPs del cliente. Detectándose credenciales comprometidas a través de una *botnet* y también credenciales filtradas a *sites* públicos (pastebin, foros, etc.) y/o leaks.
Credit Card	Se entregan tarjetas de crédito comprometidas que hayan sido utilizadas en un POS infectado, así como tarjetas disponibles a la venta en *markets underground*. Pueden monitorizarse *bincodes* completos, o tarjetas de crédito corporativas individualmente.
Malware	El módulo indexará muestras de malware que afecten a los dominios e IPs de la compañía. Miles de muestra son ejecutadas en las *sandboxes* de Blueliv al día, obteniendo un fichero que describe el comportamiento del malware, permitiéndonos saber si una muestra afecta, o no, a una organización. También cubre malware tipo web-inject.
Hacktivism	Blueliv utiliza indicadores de *hacktivismo* para detectar ítems *hacktivistas* (posts en blogs, tweets, chats IRC, pastebins) los cuales son cotejados con los parámetros del cliente. De esta forma cualquier ítem *hacktivista* que contenga un parámetro relacionado con el cliente se entregará de forma automática para ser revisado por el analista.
Domain Protection	El módulo recupera casos de *Phishing* (un dominio con interfaz que suplante la identidad de la original con el objetivo de robar credenciales) y *Cybersquatting* (dominios sin interfaz muy similares a los originales y que pueden ser utilizados para futuros casos de Phishing).
Mobile App	Detecta aplicaciones móviles utilizando de forma no autorizada la imagen corporativa del cliente, así como la distribución ilegítima de *apps* oficiales en *markets* de aplicaciones alternativos.
Social Media	El módulo entregará todo tipo de menciones en redes sociales, con la intención de detectar comentarios negativos y perfiles falsos en redes sociales que cometan abuso de marca.
Data Leakage	El módulo busca de forma automática más de 30 *sites* de hospedaje de documentos, presentaciones y archivos en general. Todos los documentos conteniendo las palabras clave que indique el cliente serán recuperados automáticamente.
Dark Web	El módulo indexa menciones en la Dark Web y Deep web de forma automática y permite además realizar investigaciones con un potente buscador. Ejemplos de amenazas que pueden localizarse en la Dark Web son fugas de información, ítems no legítimos a la venta, menciones negativas, planificación de ataques en el contexto de operaciones *hacktivistas* etc. Entendemos por Dark Web todo aquel contenido en redes Onion, i2P y similares. Entendemos por Deep web diversos foros y sites que requieren de autenticación para poder

©2023 Knowledge Consulting sa

Modulo	Descripción de la utilidad del módulo
	ser accedidos y que no son indexados por defecto por los buscadores comerciales.
Threat Context	Módulo que permite a analistas y a grupos de respuesta de incidentes acceder a una gran base de datos con más de 100 millones de entradas sobre IoCs, actores, técnicas, procedimientos, herramientas y CVEs

La configuración de los módulos se realiza fácilmente en una única pantalla de configuración. Esto permite reducir el tiempo de formación necesario para analistas, así como acelerar el proceso de puesta en marcha y con él el de obtención de los primeros resultados.

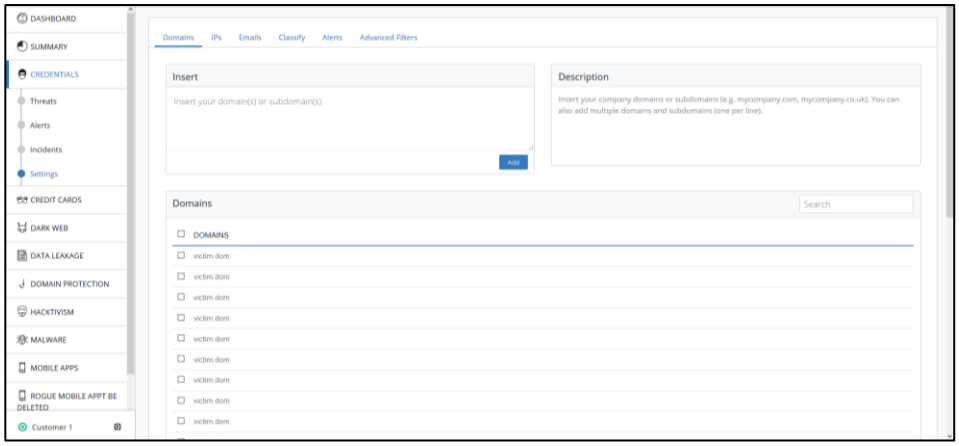


Figura 1. Ejemplo de Pantalla de Configuración

Por otra parte, los resultados son presentados en una interfaz amigable, que permite analizar, filtrar y priorizar las amenazas desde la propia herramienta con funcionalidades cómo el FollowUp (ser avisado automáticamente si un resultado varía), los incidentes (carpetas de resultados escalados), alertas en tiempo real por correo electrónico, etc.

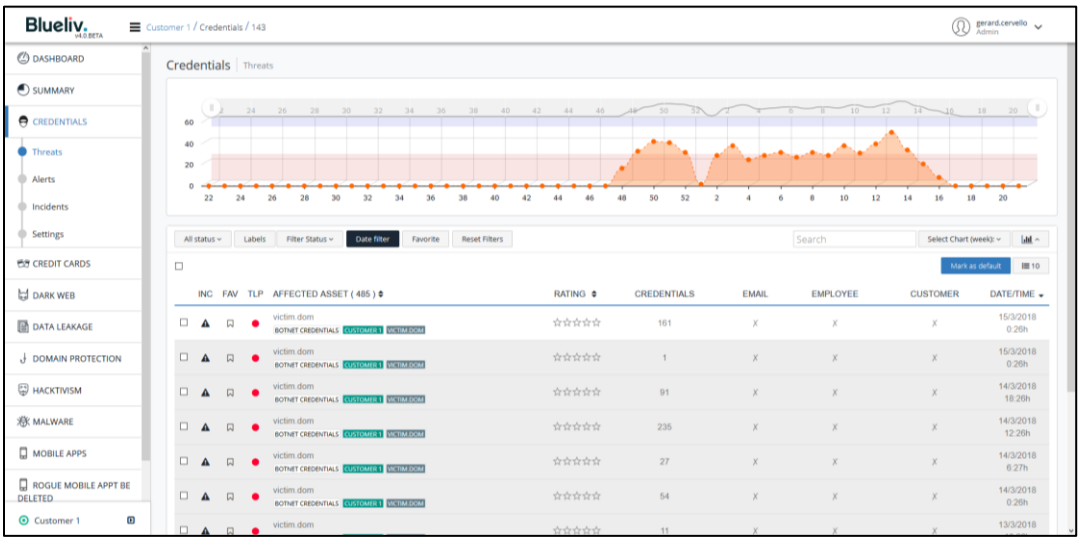


Figura 2. Pantalla de resultados. Un interfaz limpio y lleno de información

También merece la pena destacar que todos los resultados pueden ser recuperados vía API, exportándose en respuesta JSON, permitiendo así integrar los resultados recuperados por Blueliv en otra plataforma o sistema.

Eficiencia

Utilizando Blueliv puede iniciarse una monitorización en minutos si previamente se conocen los parámetros a monitorizar.

Los tipos de parámetros necesarios para una correcta detección de amenazas son:

- Palabras clave relativas al cliente (compañía, productos, servicios, directivos, etc.)
- IPs públicas del cliente
- Dominios
- BIN-Codes para la monitorización de Tarjetas de Crédito y Débito.

Una vez introducidos los parámetros, se ejecuta la tecnología de recolección de información asociada a cada módulo de forma automática, periódica y ordenada automáticamente.

En otras palabras, Blueliv automatiza el proceso de búsqueda e indexación de información en más de 10.000 fuentes, entregando sólo aquellos ítems relevantes para el cliente. Esto resultaría imposible de realizar manualmente o con APIs separadas para cada fuente o canal. Esta búsqueda y recogida se realiza 24x7, entregando las amenazas en tiempo real, tan pronto como han sido detectadas.

©2023 Knowledge Consulting sa

Reducción de falsos positivos con filtros avanzados

Blueliv cuenta con la funcionalidad “Advanced Filters” que permite filtrar la información recuperada de acuerdo con los criterios de cada cliente.

Estos filtros avanzados permiten borrar resultados no relevantes de forma automática. Por ejemplo, si nuestro cliente fuera la marca de estilográficas Montblanc, podríamos realizar un filtro que borrar automáticamente resultados con palabras como “hiking”, “mountain”, “escalada”, etc.

Esta frase de filtrado puede ser tan compleja como se desee, incluyendo la posibilidad de utilizar expresiones regulares, booleanos, grupos, algoritmos de proximidad y wildcards.

A parte de la frase de filtrado, en la siguiente figura se muestran las distintas opciones dentro de un filtro avanzado.

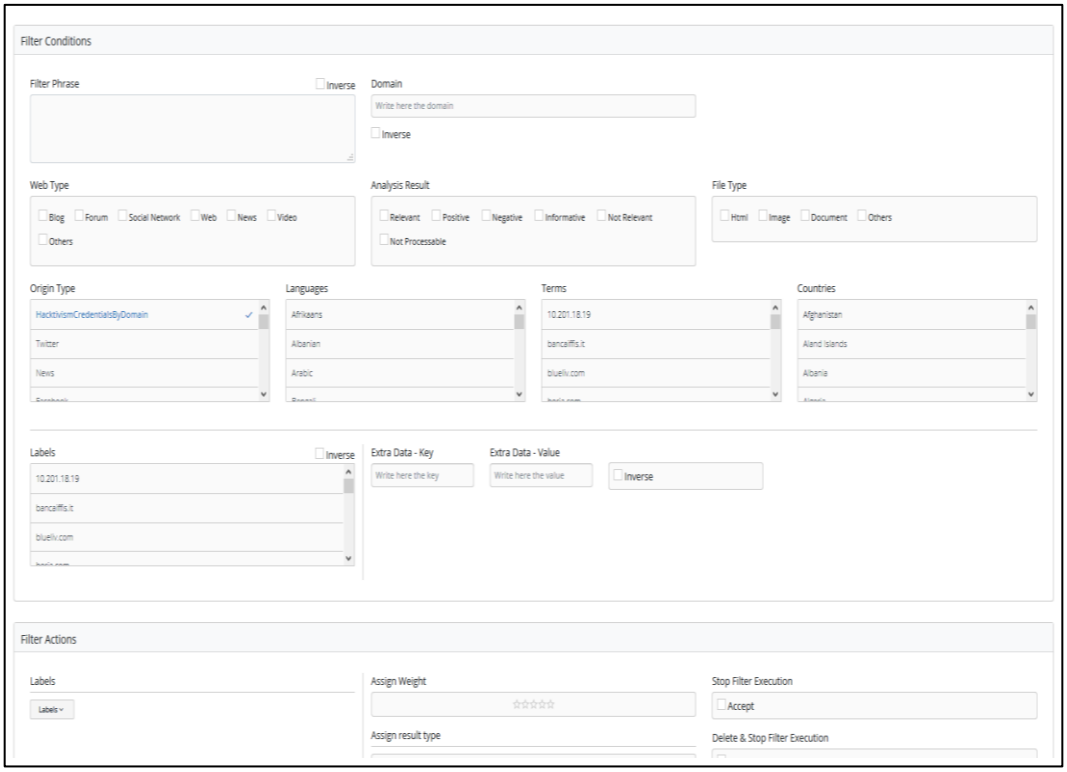


Figura 3. Filtros Avanzados

Entre las condiciones por la que filtrar resultados están: frase de filtrado, dominio, idioma, país, frase de búsqueda, etiqueta, tipo de recurso, entre otros.

Las acciones aplicables son: asignar una etiqueta, aumentar el peso del resultado, asignar un estatus, borrar, parar la ejecución de filtros, enviar alertas o cambiar el TLP.

©2023 Knowledge Consulting sa

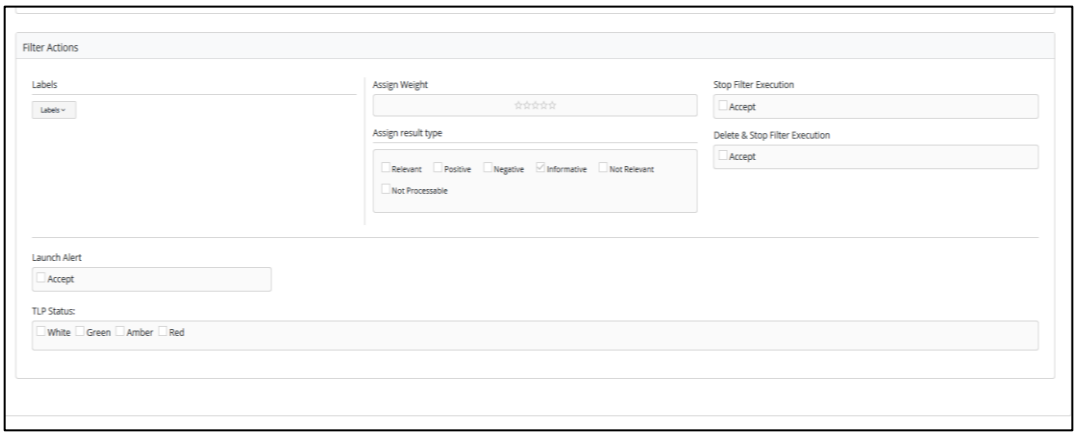


Figura 4.

Acciones ejecutables mediante filtros avanzados

Todas estas condiciones y acciones permiten al usuario personalizar el comportamiento de Threat Compass, teniendo especial relevancia a la hora de eliminar falsos positivos o resultados no relevantes.

Por ejemplo, en un supuesto, podríamos llegar a eliminar resultados en danés, provenientes de un dominio en concreto y conteniendo “x” palabras clave, entre otras condiciones.

Esta granularidad al indexar las propiedades de un ítem permite que puedan borrarse los resultados no deseados automáticamente al identificar, por ejemplo, una palabra clave que recupera resultados no relevantes.

©2023 Knowledge Consulting sa

Modelo de Servicio

El ***Servicio Gestionado de Amenazas Inteligentes*** se basa en el Centro de Operaciones de Ciberseguridad (CSOC) de KC LATAM ubicado en la ciudad de Buenos Aires, Argentina.

Toda la gestión de la plataforma, KC LATAM, basado en la metodología mejora continua, esta permanentemente realizando optimización del servicio a través de procesos de automatización y orquestación.

En el caso de la propuesta y alcance, **BCP** podrá disponer de Dashboard ejecutivo del servicio.

Horario de Cobertura de los Servicios.

El horario de cobertura de los servicios es el siguiente:

Servicio	Cobertura horaria	Tipo
Servicio Gestionado de Amenazas Inteligentes	7x24	Incidentes
Servicio Gestionado de Amenazas Inteligentes	5x8	Requerimientos Problemas

Punto Único de Contacto

El cliente tendrá asignado un único canal que centraliza y regularizará la recepción de los requerimientos, incidentes y problemas reportados.

La atención podrá ser realizada mediante contacto telefónico (llamada local del país), correo electrónico o a definir entre las partes.

Cabe destacar que los procesos utilizados por el punto único de contacto corresponden a procesos actualmente modelados según las buenas prácticas impulsadas por el Framework de Trabajo ITIL.

Las principales actividades del Punto Único de Contacto corresponden a:

©2023 Knowledge Consulting sa

- Recepción y registro de solicitudes
- Control y seguimiento de incidentes o solicitudes
- Escalamientos entre las diversas áreas especialistas.

El Servicio tendrá asignado un **Service *Delivery Manger*** (SDM) a cargo de la gestión y contraparte del cliente

- Análisis de los Incidentes para evitar que se conviertan en problemas.
- Reuniones mensuales con el Cliente.
- Informe de gestión mensual con datos estadísticos, riesgos detectados, planificaciones, actividades realizadas en el periodo y control de las actividades por realizar.

Reportes/Reporting

El reporting de la información relacionada con amenazas dirigidas puede realizarse de forma automática exportando la información de varias formas, a convenir con el cliente:

- Alertas por correo electrónico, personalizables y integrables con una herramienta de ticketing del cliente (fuera del alcance la integración)
- Exportación de resultados en Excel, Word.
- Exportación cuantitativa de analíticas mediante Dashboard en tiempo real.
- API: Para la integración del Threat Compass con sistemas de terceros. (fuera del alcance)

©2023 Knowledge Consulting sa

Módulos incluidos en el servicio

El cliente ha definido el servicio con los siguientes módulos:

1. PHISHING

Incluye los siguientes parámetros máximos:

Parámetros	# Cantidad
Cantidad de dominios	10

Nota. No se incluye la administración y gestión del servicio.

Propuesta Comercial

Cargos del servicio

Descripción	Duración contrato	Valor total USD + IVA
Implementación y Configuración Inicial		
Servicio de Protección de Dominio de acuerdo con alcance de la propuesta	24 meses	USD 64.000

Nota 1: Forma de Pago: Trimestral adelantado.

Nota 2: Hitos de Facturación: Al inicio de cada tres meses.

Nota 3: La Implementación y Configuración inicial es un cargo por única vez.

Condiciones Comerciales

Precios

Todos los precios que figuran en la presente propuesta no incluyen el IVA, y están expresados en Dólares Estadounidenses.

Estos precios cotizados están calculados en función de los impuestos, tasas, aranceles y contribuciones vigentes a la fecha, según las correspondientes disposiciones legales, cualquier cambio en las mismas anterior al momento en que KC LATAM hubiera recibido el pago total de lo cotizado, dará derecho a KC LATAM a modificar los precios indicados en la presente.

Forma de Pago

30 (treinta) días fecha de factura.

©2023 Knowledge Consulting sa

Facturación

Se facturará trimestralmente por adelantado. La primera factura se realizará contra aceptación de la Orden de Compra o Firma del contrato.

Lugar y Fecha de Entrega

En Asunción, 30 días recibida Orden de Compra

Validez de la Propuesta

30 (treinta) días a partir de la fecha de la propuesta.

Aceptación de la Propuesta

La aceptación de la presente Propuesta tendrá lugar con la emisión de una Orden de Compra que haga referencia al número de Propuesta o con la firma de una carta y/o notificación de aceptación por el Cliente con referencia a la presente Propuesta.

Confidencialidad

Toda información técnica y comercial intercambiada en virtud de la presente, será tratada en forma confidencial, incluyendo, sin que ello implique una limitación, la referida a los sistemas, ingeniería o datos técnicos, correspondencia y toda otra información que por su naturaleza debe ser considerada como tal, debiendo mantenerse y guardarse de manera apropiada atento a su carácter de reservado. La confidencialidad prevista en la presente subsistirá 2 años posteriores a la finalización por cualquier causa de la presente propuesta.

©2023 Knowledge Consulting sa

Firma

Mediante la firma del presente documento las Partes aceptan la presente propuesta, así como todos los términos y condiciones establecidos en ella, constituyendo la presente un total acuerdo entre ambas Partes con relación al objeto de la misma.

Los abajo firmantes declaran que cuentan con las facultades suficientes y necesarias para obligar a sus representantes para este tipo de actos jurídicos, las que se encuentran en plena vigencia.

Por BCP	Por Knowledge Consulting sa
_____	_____
Firma	Firma
_____	_____
Nombre	Nombre
_____	_____
Fecha de Firma	Fecha de Firma
_____	_____
CI	CI
_____	_____
Cargo	Cargo

©2023 Knowledge Consulting sa

Freddy Barreto Villar

De: Victoria Aguilera <victoriaaguilera@grupowelltech.com>
Enviado el: jueves, 25 de mayo de 2023 16:04
Para: Freddy Barreto Villar
Asunto: Re: Solicitud de cotización WellTech Next Generation Partner
Datos adjuntos: Presupuesto Solucion BCP 2023.pdf

Estimado Freddy,

Adjunta se encuentra la cotizacion solicitada, espero que les sirva!

Saludos cordiales,

Victoria Aguilera

De: Victoria Aguilera <victoriaaguilera@grupowelltech.com>
Fecha: miércoles, 24 de mayo de 2023, 15:40
Para: Freddy Barreto Villar <fbarreto@bcp.gov.py>
Asunto: Re: Solicitud de cotización WellTech Next Generation Partner

Estimado Freddy

Como estas? Recepciono el mail, analizamos las caracteristicas y te doy retorno

Saludos cordiales,

WellTech Next Generation Partner
Maria Victoria Aguilera
Sales Territory Manager
(+595) 971 218 274
www.grupowelltech.com

Por favor piense en el medio ambiente antes de imprimir este mensaje.

Este mensaje está dirigido exclusivamente al destinatario y puede contener información confidencial de Welltech SRL. Si lo recibió por error, por favor bórrelo y avise de inmediato al emisor. Difundirlo, copiarlo y/o distribuirlo está prohibido y puede ser sancionado conforme a la legislación aplicable, pudiendo generar responsabilidad civil y penal, de conformidad con lo normado en el Capítulo "Violación de secretos", del Código Penal.
This message is exclusively meant for the addressee and may contain confidential information related to Welltech SRL. If you received it by mistake, please delete it and give immediate notice to the sender. The dissemination, duplication or distribution of the information herein is prohibited and may result in penalties according to applicable regulations, including civil and criminal liability according to the provision of the Title "Violation of Secrets" of the Criminal Code

De: Freddy Barreto Villar <fbarreto@bcp.gov.py>
Fecha: miércoles, 24 de mayo de 2023, 13:41
Para: victoriaaguilera@grupowelltech.com <victoriaaguilera@grupowelltech.com>
Asunto: Solicitud de cotización WellTech Next Generation Partner

Buenas tardes, estimados:

Quisiéramos consultarles primeramente si ofrecen un Software con las siguientes características:

1. Solución que permita recopilar, calificar y monitorear la salud general de la ciberseguridad de al menos 10 (diez) entidades (postura de seguridad).
2. La postura de seguridad o monitoreo de riesgo debe estar basado en el score/puntaje, y debe estar integrado en la plataforma.
3. La plataforma debe brindar una visión holística de la postura de seguridad de la organización y de terceros, que permita evaluar dicha postura de manera general y con posibilidad de indagar la causa raíz de las señales de riesgo.
4. La solución debe permitir crear cuestionarios que puedan ser editables en cuanto a la forma y opciones de respuesta.
5. Estos cuestionarios podrán ser completados por otras entidades a modo de autoevaluación de controles técnicos de ciberseguridad.
6. La solución debe permitir tipificar a las entidades participantes de los cuestionarios según los criterios que el BCP defina.
7. Debe incluir soporte y mantenimiento local (proveedor) y del fabricante por 24 meses desde la puesta en funcionamiento de la herramienta, en modalidad de licenciamiento SaaS (Software as a Service).

En caso de que así sea, agradeceríamos nos puedan remitir un presupuesto aproximado de la solución correspondiente.

Si requieren mayores detalles acerca de lo solicitado, favor consultar.

Gracias y saludos,

FREDDY BARRETO V.
Departamento de Ciberseguridad

BANCO CENTRAL DEL PARAGUAY
Federación Rusa y Augusto Roa Bastos
4to. Piso Asunción, Paraguay
Tel. (595 21) 619 2722

WellTech
Next generation partner

Asunción, 25 de Mayo del 2023

Señores: Banco Central del Paraguay.

Es un privilegio para WellTech, presentar esta propuesta

No duden en contactarme con cualquier pregunta sobre nuestras soluciones y esta propuesta.

Cordialmente,

Victoria Aguilera

Sales Territory Manager

Propuesta Económica

2 años de Software as a Service y soporte

Item	Nro De Parte	Descripción	Cantidad	Precio Unitario	Sub Total
1	WT1	Solucion de monitoreo de riesgo - 24 months	1	455.000.000	455.000.000
	Total				Gs. 455.000.000

Condiciones Comerciales

Entrega de licencias: 15 Días hábiles a partir de la OC.
Precio: Los precios cotizados están valorados en Guaraníes e incluyen IVA.
Forma de Pago: A convenir
Validez de la propuesta: 30 días

Razón Social: IRSA – RUC 80099454-0.

Freddy Barreto Villar

De: Ricardo Vera Falcón <ricardo@iss.com.py>
Enviado el: jueves, 1 de junio de 2023 11:57
Para: Freddy Barreto Villar
CC: Betania Balmaceda; Osvaldo Casagrande
Asunto: RE: Solicitud de cotización Information Security Services S.A.

Hola Freddy:

Cómo estás?, espero que te encuentres bien.

Te detallo una breve descripción y la inversion requerida, para contratar la herramienta y los servicios profesionales para cubrir tus requerientos basicos.

Item	Descripción	Vigencia
1	SSC Platform SaaS, incluye monitoreo la empresa y 10 entidades adicionales.	24 meses
2	ATLAS Module, provee 100 cuestionarios por año, con procesamiento del lenguaje natural (NLP) para permitir a los proveedores completarlos en segundos y comparar con Datos de calificación de seguridad.	24 meses
3	Soporte básico de ISS SA	24 months

Precio Total U$s. 450.000.000

Referencias:

- **Moneda:** el valor se encuentra expresado en guaraníes e incluye el IVA.
- **Forma de pago:** 30 días para la cancelación total, una vez habilitada la plataforma.
- **Plazo de entrega:** de 3 a 5 días para habilitar la plataforma, de 10 a 21 días, para la configuración.

Información técnica en:

- Solución para calificar la postura de ciberseguridad – https://securityscorecard.com/product/security-ratings/
- Solución para la Evaluación de seguridad - https://securityscorecard.com/product/security-assessments/

Quedo atento a tus comentarios.

Saludos cordiales.

Lic. Ricardo Vera Falcón
Director

Information Security Services S.A.

Dirección: Av. España casi San Rafael – Complejo La Torre – Piso 4
Teléfonos: 595.21.607.777 al 9
Correo: ricardo@iss.com.py
Página WEB: www.iss.com.py
Facebook: ISS.Paraguay
LinkedIn: Information Security Services S.A.

"Su estrategia de Ciberseguridad de hoy, permitirá que su negocio funcione mañana", es un eslogan que aplica para todo tipo de empresas, independiente de su tamaño o rubro.

De: Freddy Barreto Villar <fbarreto@bcp.gov.py>
Enviado el: miércoles, 24 de mayo de 2023 13:43
Para: Ricardo Vera Falcón <ricardo@iss.com.py>
Asunto: Solicitud de cotización Information Security Services S.A.

Buenas tardes, estimados:

Quisiéramos consultarles primeramente si ofrecen un Software con las siguientes características:

1. Solución que permita recopilar, calificar y monitorear la salud general de la ciberseguridad de al menos 10 (diez) entidades (postura de seguridad).
2. La postura de seguridad o monitoreo de riesgo debe estar basado en el score/puntaje, y debe estar integrado en la plataforma.
3. La plataforma debe brindar una visión holística de la postura de seguridad de la organización y de terceros, que permita evaluar dicha postura de manera general y con posibilidad de indagar la causa raíz de las señales de riesgo.
4. La solución debe permitir crear cuestionarios que puedan ser editables en cuanto a la forma y opciones de respuesta.
5. Estos cuestionarios podrán ser completados por otras entidades a modo de autoevaluación de controles técnicos de ciberseguridad.
6. La solución debe permitir tipificar a las entidades participantes de los cuestionarios según los criterios que el BCP defina.
7. Debe incluir soporte y mantenimiento local (proveedor) y del fabricante por 24 meses desde la puesta en funcionamiento de la herramienta, en modalidad de licenciamiento SaaS (Software as a Service).

En caso de que así sea, agradeceríamos nos puedan remitir un presupuesto aproximado de la solución correspondiente.

Si requieren mayores detalles acerca de lo solicitado, favor consultar.

Gracias y saludos,

FREDDY BARRETO V.
Departamento de Ciberseguridad

BANCO CENTRAL DEL PARAGUAY
Federación Rusa y Augusto Roa Bastos
4to. Piso Asunción, Paraguay
Tel. (595 21) 619 2722

[Mensaje procesado por lista blanca]

PLANILLA DE COTIZACIONES AL MARTES 13 DE JUNIO DEL 2023

MONEDA	ME/USD.	₲ / ME
DÓLAR ESTADOUNIDENSE	1,0000	7.247,22
YEN JAPONÉS	139,9300	51,79
LIBRA ESTERLINA *	1,2618	9.144,54
FRANCO SUIZO	0,9044	8.013,29
CORONA SUECA	10,7080	676,80
CORONA DANESA	6,9028	1.049,90
CORONA NORUEGA	10,6436	680,90
REAL BRASILEÑO	4,8514	1.493,84
PESO ARGENTINO	247,3065	29,30
DÓLAR CANADIENSE	1,3296	5.450,68
RAND SUDAFRICANO	18,5421	390,85
DERECHOS ESPECIALES DE GIRO (FMI)	1,3333	9.662,72
ONZA DE ORO *	1.945,6600	14.100.626,07
PESO CHILENO	804,0000	9,01
EURO *	1,0797	7.824,82
PESO URUGUAYO	38,3350	189,05
DÓLAR AUSTRALIANO *	0,6781	4.914,34
YUAN RENMINBI DE CHINA	7,1585	1.012,39
DÓLAR DE SINGAPUR	1,3412	5.403,53
BOLIVIANO	6,8531	1.057,51
SOL PERUANO	3,6380	1.992,09
DÓLAR NEOZELANDÉS	0,6154	4.459,94
PESO MEXICANO	17,2058	421,21
PESO COLOMBIANO	4.193,8500	1,73
DÓLAR TAIWANÉS	30,6960	236,10
DIRHAM DE LOS EMIRATOS ÁRABES UNIDOS	3,6728	1.973,21

(*) USD x GBP, DEG, EUR, XAU, AUD.

(**) Moneda Extranjera (ME) | Dólar Americano (USD) | Guaraní (₲)