AFD - Agencia Financiera de Desarrollo

REVISIÓN DE EVALUACIÓN DE OFERTAS

Llamado de Suscripción de Licencias Varias

ID: 48730 - Lote 6

Fecha: 22/10/2026

Item	Descrición	TEISA
1	FortiSASE para 170 usuarios - FC2-10-EMS05-547-02-DD x 170 POR 24 MESES SERIAL FCTEMS8824000313 VTO. 12/01/2027, según especificaciones técnicas.	**Cumple**
2	FortiCASB - SSPM, 50- 499 users SKU. SaaS Protection. FortiCare Premium Support included. FC1-10-FCSSM-1278-02-24 POR 24 MESES SERIAL FCASBR0000001182 VTO. 12/01/2027, según especificaciones técnicas.	
3	Fortimail Workspace Mail Security para 170 usuarios Serial FC2-10-PVMCL-1195-02-24 por 24 meses soporte 24x7, con instalación e implementación según especificaciones técnicas.	
4	FortiDeceptor por 12 meses soporte 24x7 el cual deberá incluir cuanto sigue Windows License Expands FortiDeceptor Licensed Windows VM capacity by 2. (1) Win7 and (1) Win10 license added (CODIGO DE PRODUCTO LIC-FDC-WIN) VM Subscription License 1 Year VM model FortiCare Premium, Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (ARAE, AV, IPS, and Web Filtering). 1 network VLAN unit price, minimum order of 2 VLANs. Supports up to 20 Deception VMs and up to 128 network VLANS (CODIGO DE PRODUCTO FC1-10-DCVMS-496-02-12) VM Support License 1 Year FortiCare premium support Contract for FortiDeceptor-Edge virtual appliance supports on-premises FortiDeceptor Central Management and FortiDeceptor-as-a-Service and can extend up to 128 VLANs (CODIGO DE PRODUCTO FC-10-DCVME-248-02-12) SERIAL LIC-FDC-WIN, FC1-10-DCVMS-496-02-12, FC-10-DCVME-248-02-12, con instalación e implementación según especificaciones técnicas.	
5	El oferente deberá contar con personal certificado con experiencia en la instalación y configuración de lo ofertado, que de forma individual o en conjunto cuente con las siguientes certificaciones del fabricante: Al menos 1 (un) Fortinet Certified Professional Network; y, Al menos 2 (dos) Fortinet Certified Associate in Cybersecurity, vigente al momento de la presentación de la propuesta.	**Cumple,** Federico Benegas - certificación FCPNS, Alejandro Ozuna y Daniel Peña - certificación FCAC.
6	a. Copia de certificado solicitado b. Currículum Vitae (CV) del/os técnico/s propuesto/s. c. Certificados de capacitación, entrenamientos o certificaciones relacionadas con el objeto de la contratación. d. Declaración jurada del oferente indicando que los técnicos forman parte de su plantel.	**Cumple**, Presenta copia de certificados que avalen la experiencia, Presenta Curriculum Vitae de los técnicos, Presenta copia de certificados.Presenta declaración jurada
7	Todas las licencias deberán estar a nombre de la Agencia Financiera de Desarrollo. Todas las licencias de software deberán incluir las actualizaciones a nuevas versiones del producto ofertado, soporte de funcionamiento, en caso de necesidad las licencias deberán ofrecer la posibilidad de escalar el problema al fabricante. Durante la vigencia de la suscripción, la AFD podrá solicitar estos servicios en cualquier momento, sin que esto implique costos adicionales para la misma.	Se comprobará al momento de la adjudicación
8	PARA TODOS LOS ÍTEMS DE LOS SIGUIENTES LOTES: 01, 02, 03, 04, 05, 06, 08 y 09. El Oferente deberá acreditar estar autorizado para la comercialización de la solución de la marca ofertada en el territorio paraguayo mediante documento emitido por la Marca y/o los canales autorizados correspondientes La nota de autorización deberá: Indicar que el Oferente posee capacidad para proveer la cantidad ofertada en el tiempo solicitado, así como para realizar la instalación, configuración y soporte del software, en caso de resultar adjudicado. Estar firmada por una autoridad con injerencia comercial sobre la región o país. Ser original, estar dirigida a la Agencia Financiera de Desarrollo (AFD) y hacer referencia específica al presente llamado de contratación. En caso de que el Oferente sea distribuidor, deberá adjuntar además la documentación que demuestre el vínculo entre el fabricante, el representante y el Oferente, acreditando la cadena de autorizaciones correspondiente.	**Cumple**

ALBERTO SILVANO AMARILLA CACERES

Firmado digitalmente por ALBERTO SILVANO AMARILLA CACERES
Fecha: 2026.10.22 09:31:07 -03'00'

AFD - Agencia Financiera de Desarrollo

REVISIÓN DE EVALUACIÓN DE OFERTAS

Llamado de Suscripción de Licencias Varias

ID: 48730 - Lote 7

Fecha: 22/10/2026

Item	Descrición	OLAM
1	Suscripción a Mindmanager para Microsoft Teams 5 usuarios por 12 meses con soporte y actualización, según especificaciones técnicas.	**Cumple**
2	Las licencias deberán estar a nombre de la Agencia Financiera de Desarrollo.	Se comprobará al momento de la adjudicación

AFD - Agencia Financiera de Desarrollo

REVISIÓN DE EVALUACIÓN DE OFERTAS

Llamado de Suscripción de Licencias Varias

ID: 48730 - Lote 8 y Lote 9

Fecha: 22/10/2026

Item	Descrición	ONE
1	1 Solución tecnológica para identificar, evaluar y priorizar indicadores de compromiso y actividades maliciosas en tiempo cercano al real por 12 meses, según especificaciones técnicas.	**Cumple**
2	2 Solución tecnológica para evaluación externa de superficie de ataque por 12 meses en forma continua, modalidad SAAS, según especificaciones técnicas.	
3	Lo ofertado deberá poder integrarse con las soluciones que posee actualmente la AFD: Directorio Activo y Splunk, a fin de la identificación de patrones, configuración de reportes, programación de alertas e incorporar a los dashboards utilizados para el monitoreo utilizados por las áreas técnicas de la AFD.	
4	El Oferente deberá prestar servicio de Soporte técnico, el cual deberá contemplar: instalación, actualizaciones de software, soporte, servicios de activación, configuración, capacitación en el uso, gestión y mantenimiento de la solución ofertado en caso de que la AFD lo requiera	Se comprobará al momento de la adjudicación
5	Todas las licencias deberán estar a nombre de la Agencia Financiera de Desarrollo, todas las licencias de software/suscripción deberán incluir las actualizaciones a nuevas versiones del producto ofertado, soporte de funcionamiento, en caso de necesidad las licencias deberán ofrecer la posibilidad de escalar el problema al fabricante.	Se comprobará una vez entregada la licencia
6	El Oferente adjudicado deberá ejecutar toda actividad de activación, configuración, soporte, integración, capacitación, actualización y mantenimiento sobre la plataforma objeto del presente llamado bajo controles mínimos de ciberseguridad operativa. Como mínimo deberá garantizar: uso de protocolos seguros; autenticación robusta y MFA para accesos administrativos cuando la plataforma lo permita; cuentas nominales; control de acceso basado en roles; mínimo privilegio; trazabilidad de accesos y cambios; protección de credenciales, tokens y claves API; gestión documentada de incidentes; control de cambios; respaldo y restauración de configuraciones cuando aplique; y generación de evidencias verificables para la AFD. Se tomarán como referencia ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27035, NIST SP 800-61, NIST SP 800-40, NIST Cybersecurity Framework, CIS Controls v8 y CIS Benchmarks aplicables.	Se comprobará una vex realizada la solicitud
7	PARA TODOS LOS ÍTEMS DE LOS SIGUIENTES LOTES: 01, 02, 03, 04, 05, 06, 08 y 09. El Oferente deberá acreditar estar autorizado para la comercialización de la solución de la marca ofertada en el territorio paraguayo mediante documento emitido por la Marca y/o los canales autorizados correspondientes La nota de autorización deberá: Indicar que el Oferente posee capacidad para proveer la cantidad ofertada en el tiempo solicitado, así como para realizar la instalación, configuración y soporte del software, en caso de resultar adjudicado. Estar firmada por una autoridad con injerencia comercial sobre la región o país. Ser original, estar dirigida a la Agencia Financiera de Desarrollo (AFD) y hacer referencia específica al presente llamado de contratación. En caso de que el Oferente sea distribuidor, deberá adjuntar además la documentación que demuestre el vínculo entre el fabricante, el representante y el Oferente, acreditando la cadena de autorizaciones correspondiente.	**Cumple**
1.Solución tecnológica para identificar, evaluar y priorizar indicadores de compromiso y actividades maliciosas en tiempo cercano al real por 12 meses, según especificaciones técnicas.		
1	Nombre del fabricante	**Lumu Technologies Inc.**
2	Nombre del producto	**Lumu Defender**
3	Versión	**SaaS - versión vigente durante la suscrpción (actualización continua del fabricante)**
4	Ficha de lo ofertado	**DOC-01 Ficha Técnica Lumu Defender (lumu-Datasheet-ES.pdf)**
5	La solución debe proporcionar, en modo SAAS, la capacidad de medir el compromiso de los activos informáticos en tiempo cercano al real. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
6	La solución no requiere de la instalación de agentes en ningún elemento del ecosistema tecnológico de la AFD on premise para la realización de las actividades de detección, reportaje y atención la red. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
7	La solución debe proveer la capacidad de recolectar la información a través de la instalación de un agente dentro de la red de la organización y hacia el cual se haga reenvío (forward) de los logs detección de compromisos. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
8	La solución debe permitir la implantación mediante la instalación de un colector pasivo dentro de la AFD que no implique la utilización de hardware específico. EXIGIDO El recolector o su equivalente como mínimo con el hipervisor VMware. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.

AFD - Agencia Financiera de Desarrollo

REVISIÓN DE EVALUACIÓN DE OFERTAS

Llamado de Suscripción de Licencias Varias

ID: 48730 - Lote 8 y Lote 9

Fecha: 22/10/2026

Item	Descrición	ONE
9	El producto ofertado deberá poseer una certificación SOC2 Tipo 2 para confirmar que el servicio SaaS cumple con las mejores prácticas de seguridad. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
10	La telemetría utilizada por la solución debe basarse en metadata de red y la misma debe ser colectada exclusivamente sobre los siguientes elementos de la red: DNS, netflow, firewall, proxy, email. La solución deberá operar mediante el análisis de metadatos de red y registros de seguridad provenientes de diversas fuentes, sin requerir obligatoriamente captura completa de paquetes, siempre capacidades de detección.	Cumple, conforme la documentación presentada por el oferente.
11	Para el proceso de recolección, la solución debe tener la capacidad de realizarlo sin necesidad de hardware especial y sin necesidad de utilización puertos espejo en los dispositivos de red. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
12	La solución debe ser capaz de recopilar, procesar y analizar los datos de los buzones de spam de Office 365 para identificar quién y cómo intenta atacar a la organización. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
13	La solución debe tener la capacidad de recopilar, procesar y analizar metadatos de red en dispositivos Windows y macOS remotos Integración obligatoria de la recopilación de datos con Windows 10.15 o superior. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
14	La solución debe tener la capacidad de recopilar, procesar y analizar metadatos de red en dispositivos Linux operando con las siguientes distribuciones: Ubuntu, Debian, Red Hat Enterprise, Fedora, La solución debe tener la capacidad de recopilar, procesar y analizar metadatos de red de protocolo DNS en servidores Windows que ejecuten el sistema operativo Windows Server 2019 o superior. El proceso de recolección de datos para medir el compromiso debe basarse en metadatos, es decir, no debe incluir los paquetes de datos completos (logs, pcaps, taps). EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
15	La solución debe ser capaz de recopilar metadatos de nubes, como AWS, Azure como mínimo a través de integraciones API. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
16	La solución debe permitir la ingestión de metadatos de plataformas VPN para medir la participación de dispositivos remotos en modo de full tunel y split tunnel. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
17	La solución debe permitir la ingesta de metadatos mediante un agente para la medición remota del compromiso del dispositivo. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
18	La solución debe proporcionar una API de ingestión de metadatos abierta, de modo que la organización pueda utilizarla para fines específicos. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
19	La solución debe tener la capacidad de integrarse con soluciones de respuesta a incidentes y/o SIEMs para la gestión de incidentes que posee la AFD. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
20	La evaluación del compromiso debe tener una visión de toda la red y no sólo a nivel de las máquinas de los usuarios finales. EXIGIDO La solución debe analizar en tiempo cercano al real el estado de compromiso de los activos informáticos de la AFD (incluyendo estaciones de trabajo, servidores físicos/virtuales, ambientes legacy, conectados a la red IP). EXIGIDO La solución debe tener la capacidad de clasificar el resultado de los compromisos detectados como mínimo: Malware, Phishing. EXIGIDO La solución debe proveer la capacidad de almacenar datos manteniendo la información en línea para poder ser consultada. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
21	El proceso de análisis de metadatos de la AFD debe basarse en: Capacidad para consumir e integrar múltiples fuentes de inteligencia de amenazas, tanto comerciales como de código abierto, mediante documentadas, Analizadores supervisados de Aprendizaje Automático e Inteligencia Artificial, Analizadores no supervisados de Machine Learning e Inteligencia Artificial. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
22	La solución debe proporcionar los indicadores de compromiso y hashes de archivos maliciosos para cada incidente detectado y debe ofrecer la capacidad de poder descargarlos directamente de La solución debe proporcionar contexto para cada compromiso con referencias internas y externas para comprender la naturaleza del compromiso. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
23	La solución debe tener la capacidad y flexibilidad de permitir asignar relevancia a los activos de información de la AFD con al menos 3 categorías como ser alto, medio y bajo. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
24	La solución debe proporcionar un portal web accesible a través de Chrome, Firefox, Microsoft Edge o Safari. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
25	La solución debe contar con un portal web que proporcione estadísticas sobre los indicadores de compromiso. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
26	La solución debe tener la opción de filtros de fecha predefinidos o por un periodo de tiempo personalizado. La solución debe tener la opción de filtros de datos relacionados con incidentes basado número de endpoints, número de contactos, fecha de creación, entre otros. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.

AFD - Agencia Financiera de Desarrollo

REVISIÓN DE EVALUACIÓN DE OFERTAS

Llamado de Suscripción de Licencias Varias

ID: 48730 - Lote 8 y Lote 9

Fecha: 22/10/2026

Item	Descrición	ONE
27	La solución debe incluir la frecuencia de compromiso por día de la semana y hora del día. También debe mostrar la distribución de los ataques en función de los grupos configurados previamente remoto, oficina central, IOT), así como las características relacionadas con el compromiso y los playbooks para cada tipo de ataque detectado. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
28	La solución debe disponer de una vista de incidentes para gestionar los incidentes abiertos, los cerrados y los silenciados, y para llevar un registro de las acciones realizadas para cada incidente. El portal web debe permitir la creación de nuevos usuarios de la organización con los siguientes roles como mínimo: Administrador y otro de sólo lectura. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
29	El portal debe permitir la supervisión de los colectores desplegados en la red de al menos estado de los colectores, entre otros, gráficas que muestren en el tiempo la cantidad de información recolectada colector de metadatos. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
30	El portal debe permitir la monitorización de los agentes desplegados en la red de al menos: Nombre de host, sistema operativo (SO), versión, versión del agente, vista analítica que permita entregar comportamiento de la red, así como de anomalías evidenciadas en el tráfico analizado. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
31	La solución debe entregar capacidades que permitan gestionar un incidente dentro de la propia solución tecnológica y realizar el cierre automatizado de los incidentes reportados. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
32	La solución debe contar con capacidades de incorporación de forma modular de componentes que permitan a través del uso de la inteligencia artificial, una vez que se ha generado la respuesta desde la propia plataforma, iterar igualmente de forma automatizada sobre la incidencia tantas veces como sea necesario hasta poder llegar a la conclusión que no existe presencia de comunicación vinculado al incidente y en consecuencia proceder de forma automática con el cierre del incidente. Si por el contrario no puede llegarse a esta conclusión, escalar el incidente de vuelta a un operador, contexto necesario que justifique el escalamiento. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
33	Una vez que existe un incidente, la solución enviará una notificación al correo electrónico del administrador de la solución tecnológicao a los usuarios involucrados según se determine. EXIGIDO capacidad de reportar para cada incidente de forma automática cual fué el primer dispositivo de la red que se vió afectado por el adversario vinculado en la incidencia. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
34	La solución de proveer información que evidencie la eficiencia operativa que está alcanzando la organización en el procesamiento de IOCs a través del ahorro operacional expresado en horas de seguridad. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
35	La solución debe tener la capacidad de mostrar el tiempo promedio de respuesta de la organización un incidente, así como también la cantidad de incidentes en promedio que se registran diariamente. La solución debe enviar informes por correo electrónico con información sobre los resultados de la evaluación del compromiso. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
36	La solución debe permitir exportar la información de los agentes instalados en la red en formato CSV. EXIGIDO La solución debe permitir la exportación del detalle de los incidentes reportados en La solución debe tener la capacidad de descargar información sobre amenazas. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
37	La solución debe incluir el análisis de cada incidente a partir de una matriz de conocimiento de las tácticas y técnicas adversarias basada en observaciones del mundo real (MITRE ATT&CK). EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
38	La solución debería incluir un análisis global de las tácticas y técnicas adversarias utilizadas por los atacantes en la organización basado en la matriz ATT&CK MITRE basado en las incidencias reportadas Esta función debería permitir ver a través de un mapa de calor, cómo los atacantes intentan acceder a la red, proporcionando la visibilidad necesaria para ajustar el stack de ciberseguridad con eficiencia y eficacia de las ciberdefensas. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
39	Tras la detección de un compromiso, la solución debe ser capaz de responder automáticamente mediante la conexión a través de API a la infraestructura de defensa para ajustar las políticas de EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
40	La solución debe incorporar integración nativa para funciones de bloqueo automático con los proveedores más reconocidos del sector utilizados por la AFD como ser Fortinet, además Palo Alto Cisco, entre otros. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
41	Las capacidades de detección y respuesta automatizadas ofrecidas por la solución no pueden estar basadas en la creación de playbooks, casos de uso o reglas. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
42	La tecnología debe tener la capacidad de mostrar cuales elementos del stack de seguridad a través de procesos de integración, recibieron la información de IOCs vinculados con un incidente y en respondieron de forma automática para mitigar la amenaza en base a la información entregada por la solución. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
43	La solución debe estar en capacidad de mostrar en tiempo cercano al real información que permita conocer la cantidad de IOCs que están activos clasificados en Dominios, URLs, hashes y direcciones La solución debe estar en capacidad de mostrar en tiempo cercano al real y sin ninguna configuración, información que permita conocer la cantidad de IOCs incluidos en los últimos 30 días. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.

AFD - Agencia Financiera de Desarrollo

REVISIÓN DE EVALUACIÓN DE OFERTAS

Llamado de Suscripción de Licencias Varias

ID: 48730 - Lote 8 y Lote 9

Fecha: 22/10/2026

Item	Descrición	ONE
44	La solución debe estar en capacidad de mostrar en tiempo cercano al real y sin ninguna configuración, información que permita conocer la cantidad de horas hombre (ahorro operacional) que Las capacidades de la solución deben proporcionar una API abierta para que la AFD construya la integración necesaria con fines de defensa o gestión de incidentes. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
45	La mitigación automática no debería requerir la instalación de un componente en los endpoints de la organización. La mitigación deberá realizarse a través de los componentes ya existentes en organización. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
46	La solución deberá soportar mecanismos modernos de respuesta automatizada mediante APIs, integración con herramientas de seguridad o controles de red, sin limitarse a un único método de La solución debe proveer información que permita verificar en todo momento el comportamiento del tráfico de la red dirigido hacia Internet, con capacidades de filtrado por fecha o por grupo organización. Este perfilamiento de comunicación hacia el exterior, debe mostrar de forma gráfica el destino geográfico del tráfico de la AFD dirigido hacia internet, la distribución de actividad por la distribución porcentual del tráfico en base a la popularidad del dominio en Internet con el que se intenta la comunicación, el top 50 de dominios/subdominios con los que contacta la AFD, mostrando porcentual de los top 5 destinos y categorías. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
47	Lo solución debe proveer en base al uso de la inteligencia artificial, capacidades de identificación de actividad anómala de tipo DGA (Domain Generation Algorithms) dentro de la red corporativa. mostrada, se debe incluir el nombre o IP del dispositivo identificado, la cantidad de dominios contactados, el número de contactos realizados, el nivel de precisión de la identificación (alto, medio, dominios con el número de contactos el patrón de las comunicaciones por día/hora de la semana, para cada contacto, se debe indicar la fecha/hora, el dominio y la respuesta que generó la resolución De igual forma esta información de ser posible mostrarla en forma de grafos que permitan gráficamente visibilizar los nodos involucrados en las comunicaciones. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
48	Lo solución debe proveer en base al uso de la inteligencia artificial, capacidades de identificación de actividad anómala relacionada con tunneling DNS dentro de la red corporativa. Entre la información incluir los destinos sospechosos, fechas de identificación, cantidad de sesiones, servidor autorizado de la resolución, data transferida (entrante/saliente), cantidad de equipos involucrados, nivel detección (al menos alto,medio,bajo) y total de registros identificados. Esta información debe igualmente mostrarse de forma gráfica y se de tener la posibilidad de exportarla en formato CSV. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
49	La solución debe proveer información sobre el número promedio de incidentes reportados en un período de tiempo determinado. EXIGIDO La solución debe proveer información sobre el tiempo ante incidentes reportados en un período de tiempo determinado. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
50	Para un incidente específico, la solución debe proveer información sobre el tiempo promedio de respuesta. EXIGIDO La solución debe proveer información sobre el tiempo promedio de resolución reportados en un período de tiempo determinado. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
51	La solución debe permitir configurar la periodicidad de los informes: Diario, Semanal, Quincenal y Mensual. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
52	La solución debe tener la opción de configurar la periodicidad de las notificaciones por correo electrónico. EXIGIDO.	Cumple, conforme la documentación presentada por el oferente.
53	Acreditación de madurez técnica, seguridad y adopción de la solución	Cumple, conforme la documentación presentada por el oferente.
54	El oferente deberá acreditar la madurez técnica, seguridad, adopción y respaldo de mercado de la solución ofertada mediante al menos dos (2) medios verificables, a elección del oferente, pertenecientes distintas de las siguientes:	Cumple, conforme la documentación presentada por el oferente.
55	a) Evaluaciones independientes de analistas de mercado reconocidos internacionalmente, relacionadas con detección y respuesta de red, análisis y visibilidad de red, medición continua de compromiso, externa, gestión de superficie de ataque, inteligencia de amenazas o categorías funcionalmente equivalentes. Se admitirán informes de Gartner, Forrester, IDC, GigaOM, Frost & Sullivan u otros posicionamiento específico, categoría de liderazgo, cuadrante, ranking o calificación editorial determinada.	Cumple, conforme la documentación presentada por el oferente.
56	b) Certificaciones, auditorías o reportes independientes de seguridad y privacidad aplicables al servicio o plataforma ofertada, tales como ISO/IEC 27001:2022, ISO/IEC 27017, ISO/IEC 27018, ISO/CSA STAR o equivalentes vigentes.	Cumple, conforme la documentación presentada por el oferente.
57	c) Casos de implementación verificables en entidades financieras, organismos públicos, entidades reguladas, infraestructuras críticas o instituciones de complejidad equivalente, preferentemente que permitan comprobar alcance, cantidad aproximada de activos, tipo de integración, modalidad del servicio y resultado satisfactorio.	Cumple, conforme la documentación presentada por el oferente.
58	d) Evidencia técnica de interoperabilidad y operación, incluyendo documentación oficial, guías de integración, APIs, conectores, referencias de integración con SIEM/SOAR/firewalls/EDR/DNS/proxy, arquitectura, pruebas de concepto, reportes de desempeño o informes técnicos emitidos por terceros independientes.	Cumple, conforme la documentación presentada por el oferente.

AFD - Agencia Financiera de Desarrollo

REVISIÓN DE EVALUACIÓN DE OFERTAS

Llamado de Suscripción de Licencias Varias

ID: 48730 - Lote 8 y Lote 9

Fecha: 22/10/2026

Item	Descrición	ONE
59	La AFD evaluará la idoneidad técnica de la solución principalmente en función del cumplimiento funcional, seguridad, interoperabilidad, protección de datos, pruebas de aceptación y adecuación no en función del posicionamiento editorial de terceros.	Cumple, conforme la documentación presentada por el oferente.
60	Transferencia internacional, privacidad y tratamiento de datos	Cumple, conforme la documentación presentada por el oferente.
61	Cuando la solución, sus servicios SaaS, motores de análisis, repositorios, soporte técnico, subprocesadores o componentes asociados impliquen tratamiento o transferencia internacional de datos, indicadores, evidencias, credenciales expuestas, telemetría o información de usuarios, el oferente deberá acreditar mecanismos jurídicos, técnicos y organizativos conformes al marco normativo A tal efecto, podrá presentar, según corresponda, certificación vigente bajo el EU-U.S. Data Privacy Framework u otro mecanismo de adecuación reconocido internacionalmente, cláusulas contractuales procesamiento de datos, certificaciones ISO/IEC 27001:2022, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, SOC 2 Tipo II, CSA STAR o evidencia equivalente que demuestre controles adecuados confidencialidad, subprocesamiento, retención, eliminación y portabilidad de datos.	Cumple, conforme la documentación presentada por el oferente.
62	La solución no deberá capturar, revelar, almacenar ni exportar contraseñas en texto claro. Cuando identifique credenciales comprometidas, cookies, tokens u otros secretos, deberá aplicar mecanismos enmascaramiento, acceso restringido, trazabilidad y finalidad exclusiva de remediación	Cumple, conforme la documentación presentada por el oferente.
63	A futuro con la incorporación de otro producto del mismo fabricante la solución podrá automatizar la respuesta por medio de ejecución de acciones automáticas sin intervención humana como de inteligencia artificial, entre otros. EXIGIDO	No aplica, conforme a la documentación presentada por el oferente.
2. Solución tecnológica para evaluación externa de Superficie de Ataque por 12 meses, modalidad SAAS, según especificaciones técnicas.		
1	Nombre del fabricante	**Lumu Technologies Inc.**
2	Nombre del producto	**Lumu Discover**
3	Version	**SaaS - versión vigente durante la suscrpción (actualización continua del fabricante)**
4	Ficha de lo ofertado	**DOC-02 Ficha Técnica Lumu Discover (lumu-Datasheet-ES.pdf)**
5	La solución debe ofrecer durante el período de licenciamiento de forma ilimitada, utilizando como insumo los dominios de la AFD y FOGAPY, funcionalidades que permitan realizar una evaluación ataque corporativa (vista externa) y generar un reporte asociado sobre las capacidades de parte de un atacante sobre los recursos disponibles de la organización para poder concretar algun tipo Esta vista debe contemplar dominios similares (detallando nombre del dominio, registro A de DNS asociado, nombre de servidor de correo si es el caso, identificación del servidor de nombres la organización desde el exterior, puertos abiertos identificados y posibles vulnerabilidades con posibilidad de explotación desde el exterior a través de dichos puertos. La solución ofertada para de ataque externo deberá permitir su integración, mediante API documentada o exportación estructurada de datos (CSV, JSON, STIX/TAXII), con la solución adjudicada en el Ítem 1, a fin de exposición externa con actividad de compromiso interno detectada. No se exigirá que ambas soluciones provengan de un mismo fabricante; la interoperabilidad podrá acreditarse mediante integración desarrollo de integración a cargo del Oferente sin costo adicional para la AFD. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
6	Para la evaluación de superficie de ataque se debe entregar un dashboard que de forma resumida la cantidad de dominios similares identificados, direcciones de email expuestas, gráficas de información tiempo, cantidad de usuarios de la organización comprometidos así como el número de credenciales comprometidas con gráficas que muestren este	Cumple, conforme la documentación presentada por el oferente.
7	La solución debe ofrecer capacidades que permitan consultar de forma ilimitada durante el período de licenciamiento información relacionada con los usuarios de la AFD cuya información haya disponible en la dark web. Esta información debe incluir: email, password, teléfono, data leak, última fecha de exposición; entregando la posibilidad de exportar esta información en formato CSV. 26/42	Cumple, conforme la documentación presentada por el oferente.

AFD - Agencia Financiera de Desarrollo

REVISIÓN DE EVALUACIÓN DE OFERTAS

Llamado de Suscripción de Licencias Varias

ID: 48730 - Lote 8 y Lote 9

Fecha: 22/10/2026

Item	Descrición	ONE
8	La solución debe ofrecer capacidades que permitan consultar de forma ilimitada durante el período de licenciamiento información relacionada con fuga de información (data leak) existente en presente información de la organización. Esta información debe incluir cantidad de data existente en el data leak, cantidad de registros existentes en el data leak y que estén relacionados con la identificación del tipo de data exfiltrada (passwords, email, hash cuentas de usuario, nombres de usuario) y evidencia de la data exfiltrada. Adicionalmente, se poder extraer en formato CSV esta La solución debe ofrecer capacidades que permitan consultar de forma ilimitada durante el período de licenciamiento información relacionada con infostealers existente en la dark web donde la organización. Esta información debe incluir nombre del computador, familia de infostealer, credenciales, cookies, fecha de compromiso y última fecha de detección. Adicionalmente, se debe información en formato CSV. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
9	PARA TODOS LOS ÍTEMS DE LOS SIGUIENTES LOTES: 01, 02, 03, 04, 05, 06, 08 y 09. El Oferente deberá acreditar estar autorizado para la comercialización de la solución de la marca ofertada en el territorio paraguayo mediante documento emitido por la Marca y/o los canales autorizados correspondientes La nota de autorización deberá: Indicar que el Oferente posee capacidad para proveer la cantidad ofertada en el tiempo solicitado, así como para realizar la instalación, configuración y soporte del software, en caso de resultar adjudicado. Estar firmada por una autoridad con injerencia comercial sobre la región o país. Ser original, estar dirigida a la Agencia Financiera de Desarrollo (AFD) y hacer referencia específica al presente llamado de contratación. En caso de que el Oferente sea distribuidor, deberá adjuntar además la documentación que demuestre el vínculo entre el fabricante, el representante y el Oferente, acreditando la cadena de autorizaciones correspondiente.	Cumple, conforme la documentación presentada por el oferente.
Lote 9 Item 1 Software concientización de usuarios		
1	El Oferente deberá brindar servicios y soporte de instalación, configuración y capacitación de la solución ofertada en caso de que la AFD lo requiera durante la vigencia de la suscripción.	Se comprobará una vez adjudicado
2	Todas las licencias deberán estar a nombre de la Agencia Financiera de Desarrollo, todas las licencias de software deberán incluir las actualizaciones a nuevas versiones del producto ofertado, soporte de funcionamiento, en caso de necesidad las licencias deberán ofrecer la posibilidad de escalar el problema al fabricante. Durante la vigencia de la suscripción de uso del software, la AFD podrá solicitar estos servicios en cualquier momento, sin que esto implique costos adicionales para la misma.	Se comprobará una vez adjudicado
3	Ciberseguridad operativa: El Oferente adjudicado deberá ejecutar toda actividad de activación, configuración, soporte, integración, capacitación, actualización y mantenimiento sobre la plataforma objeto del presente llamado bajo controles mínimos de ciberseguridad operativa.	Se comprobará una vez adjudicado
4	Como mínimo deberá garantizar: uso de protocolos seguros; autenticación robusta y MFA para accesos administrativos cuando la plataforma lo permita; cuentas nominales; control de acceso basado en roles; mínimo privilegio; trazabilidad de accesos y cambios; protección de credenciales, tokens y claves API; gestión documentada de incidentes; control de cambios; respaldo y restauración de configuraciones cuando aplique; y generación de evidencias verificables para la AFD.	Se comprobará una vez adjudicado
5	Se tomarán como referencia ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27035, NIST SP 800-61, NIST SP 800-40, NIST Cybersecurity Framework, CIS Controls v8 y CIS Benchmarks aplicables	Se comprobará una vez adjudicado
6	Nombre del fabricante	**WhaleMate**
7	Nombre del producto	**Plataforma Whalemate de gestión de riesgo humano y concientización en ciberseguridad**
8	Version	**Solución SaaS en versión vigente y actualizada por el fabricante**
9	Ficha de lo ofertado El Oferente deberá proveer ficha técnica o link d acceso al sitio del fabricante para la verificación del cumplimiento	**Especificaciones Técnicas Plataforma Whalemate.pdf**
10	El acceso a las plataformas será remoto y deberá ser único, y cada licencia estará vinculada a un usuario registrado. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
11	La solución tecnológica deberá estar basada en la nube y no deberá requerir ningún servidor adicional, ni una IP dedicada para el envío de correo electrónico	Cumple, conforme la documentación presentada por el oferente.
12	La solución tecnológica deberá admitir la integración con Azure Active Directory (AD) y/o LDAP Active Directory o equivalente de la AFD. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.

AFD - Agencia Financiera de Desarrollo

REVISIÓN DE EVALUACIÓN DE OFERTAS

Llamado de Suscripción de Licencias Varias

ID: 48730 - Lote 8 y Lote 9

Fecha: 22/10/2026

Item	Descrición	ONE
13	La solución tecnológica debe proporcionar, en una única consola integrada, los siguientes módulos y funcionalidades:	Cumple, conforme la documentación presentada por el oferente.
14	Parametrización/personalización de la simulación de phishing para el envío de correos electrónicos; Exámenes y pruebas; Informes e indicadores; y Material educativo en diversos formatos digitales, como folletos, fondos de pantalla, vídeos, etc. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
15	La solución tecnológica debe permitir la parametrización de la identidad visual del cliente en el entorno, incluyendo los mensajes dirigidos a los usuarios	Cumple, conforme la documentación presentada por el oferente.
16	La solución tecnológica debe contar con modelos o formatos de texto o imágenes un repositorio para su uso en simulaciones de phishing y acciones de sensibilización	Cumple, conforme la documentación presentada por el oferente.
17	La solución tecnológica debe permitir la parametrización de alertas para la interacción con usuarios internos cuando: se asigne una nueva acción de sensibilización al usuario, se asigne una nueva capacitación al usuario, se complete con éxito o esté pendiente una sensibilización. y un informe de seguimiento del usuario con acciones pendientes. EXIGIDO acción de	Cumple, conforme la documentación presentada por el oferente.
18	La solución tecnológica debe proporcionar una evaluación del riesgo humano de cada usuario. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
19	La solución tecnológica también debe ser accesible mediante una interfaz web adaptable, compatible con los principales navegadores modernos (Google Chrome y Microsoft Edge), sin necesidad de instalación local. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
20	La solución tecnológica debe contar con un canal o botón formal para reportar correos electrónicos sospechosos de phishing. Este requisito tiene como objetivo garantizar la integridad del proceso de concienciación y la evolución iterativa de la postura de seguridad de la información de la organización. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
Simulación de phishing enviada por correo electrónico:		
1	La solución tecnológica no debe imponer restricciones al volumen de correos electrónicos de phishing enviados durante la vigencia del contrato	Cumple, conforme la documentación presentada por el oferente.
2	La solución tecnológica debe permitir la creación de campañas de phishing personalizadas con las siguientes características mínimas: Permitir campañas en formato de texto y HTML; Adjuntar archivos en los siguientes formatos digitales: PDF, Word, Excel y HTML; y Adjuntar archivos comprimidos en formato .ZIP con y sin contraseña. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
3	La solución tecnológica debe proporcionar un mínimo de 20 plantillas estándar de correo electrónico de phishing, listas para usar con distintos niveles de complejidad. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
4	La solución tecnológica debe permitir la creación de nuevas plantillas de correo electrónico de phishing según las necesidades de la AFD, sin restricciones en el número de plantillas. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
5	La solución tecnológica debe permitir la parametrización de nuevas plantillas de correo electrónico de phishing.	Cumple, conforme la documentación presentada por el oferente.
6	La solución tecnológica debe realizar pruebas controladas del correo electrónico de phishing antes de su uso en campañas de concienciación o en simulaciones/pruebas. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
7	La solución tecnológica debe permitir programar el envío de campañas de phishing. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
8	La solución tecnológica debe permitir la parametrización del periodo de disponibilidad del acceso a la URL (enlace y dirección) utilizada en la campaña de phishing. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
9	La solución tecnológica debe proporcionar el número de infracciones repetidas por usuario en las campañas de phishing. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
10	Las simulaciones de phishing deben ser compatibles con los principales sistemas operativos del mercado, como Windows, Mac OS, Linux, Android e iOS. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
11	La solución tecnológica debe registrar y generar resultados de las simulaciones de phishing con, como mínimo, la siguiente información: Dirección IP desde la que el usuario final abrió el correo electrónico de phishing; Dirección IP del dispositivo o computadora desde la cual el usuario final abrió el correo electrónico de phishing. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
12	La solución tecnológica debe permitir exportar los resultados en formato digital CSV y/o PDF. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.

AFD - Agencia Financiera de Desarrollo

REVISIÓN DE EVALUACIÓN DE OFERTAS

Llamado de Suscripción de Licencias Varias

ID: 48730 - Lote 8 y Lote 9

Fecha: 22/10/2026

Item	Descrición	ONE
13	La solución tecnológica debe permitir monitorear el progreso de la campaña a través de su portal/interfaz. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
14	La solución tecnológica debe proporcionar un botón para reportar la identificación de la campaña de phishing, integrable con el sistema de correo electrónico de la institución (Microsoft o Google). EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
Módulo de Acciones para Usuarios		
1	La solución tecnológica debe permitir el acceso tanto desde computadoras institucionales como desde dispositivos móviles (teléfonos	Cumple, conforme la documentación presentada por el oferente.
2	celulares y tabletas). EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
3	Los materiales de sensibilización deben incluir, como mínimo, los siguientes recursos: Videos; Juegos o elementos gamificados; Módulos con recursos interactivos; Cuestionarios de evaluación; Pruebas (cuestionarios rápidos); Simulaciones de incidentes cibernéticos (ejercicio de mesa o equivalente). EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
4	Debe contar con al menos 50 piezas de contenido de sensibilización, que abarquen: ○ Identificación de enlaces fraudulentos EXIGIDO:	Cumple, conforme la documentación presentada por el oferente.
5	Identificación de correos electrónicos de phishing, Contraseñas seguras y política de contraseñas, Información y requisitos de LGPD,	Cumple, conforme la documentación presentada por el oferente.
6	Protección de datos y confidencialidad, Seguridad en redes sociales, Seguridad física, Ataques de compromiso de correo electrónico empresarial (BEC), Ingeniería social; Ataques de ransomware, Uso seguro de la inteligencia artificial, Desarrollo seguro de sistemas.	Cumple, conforme la documentación presentada por el oferente.
7	La solución tecnológica debe permitir la parametrización del contenido de las acciones según las necesidades del AFD. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
8	La solución tecnológica debe permitir programar las fechas de inicio y finalización de la ejecución de las acciones de concienciación. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
9	La solución tecnológica debe permitir la aplicación de más de un módulo de acción de concienciación por grupo de usuarios y sin restricciones en el número de módulos vinculados a usuarios o grupos de usuarios. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
10	La solución tecnológica debe proporcionar al administrador de la solución tecnológica y al usuario final una vista del tiempo de cada módulo asignado y del tiempo total de las acciones de concienciación vinculadas. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
11	La solución tecnológica debe permitir a la AFD crear y configurar un certificado virtual que se entregará al usuario de las acciones de concienciación una vez que estas se completen con éxito. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
12	La solución tecnológica debe entregar este certificado virtual al usuario que complete con éxito la acción de concienciación. EXIGIDO	Cumple, conforme la documentación presentada por el oferente.
Simulaciones de concientización seguras		
1	Toda campaña de simulación deberá ser previamente aprobada por la AFD, indicando alcance, usuarios o grupos incluidos, fechas, contenidos, indicadores a medir y responsables. Las simulaciones no deberán recolectar, almacenar ni exponer contraseñas reales, datos financieros, información sensible o credenciales válidas. Los adjuntos, enlaces y formularios utilizados deberán ser inocuos, controlados y diseñados exclusivamente para fines de capacitación y medición de conducta segura.	Cumple, conforme la documentación presentada por el oferente.
2	Los resultados deberán tratarse bajo criterios de minimización, confidencialidad y uso exclusivo para mejora de la cultura de seguridad, evitando fines disciplinarios salvo disposición institucional expresa y conforme a la normativa aplicable.	Cumple, conforme la documentación presentada por el oferente.
3	PARA TODOS LOS ÍTEMS DE LOS SIGUIENTES LOTES: 01, 02, 03, 04, 05, 06, 08 y 09. El Oferente deberá acreditar estar autorizado para la comercialización de la solución de la marca ofertada en el territorio paraguayo mediante documento emitido por la Marca y/o los canales autorizados correspondientes La nota de autorización deberá: Indicar que el Oferente posee capacidad para proveer la cantidad ofertada en el tiempo solicitado, así como para realizar la instalación, configuración y soporte del software, en caso de resultar adjudicado. Estar firmada por una autoridad con injerencia comercial sobre la región o país. Ser original, estar dirigida a la Agencia Financiera de Desarrollo (AFD) y hacer referencia específica al presente llamado de contratación. En caso de que el Oferente sea distribuidor, deberá adjuntar además la documentación que demuestre el vínculo entre el fabricante, el representante y el Oferente, acreditando la cadena de autorizaciones correspondiente.	Cumple, conforme la documentación presentada por el oferente.