

ACTA DEL COMITÉ DESELECCIÓN
ADMISION DE OFERTAS, EVALUACIÓN, CALIFICACIÓN Y OTORGAMIENTO DE LA BUENA
PRO
PROCEDIMIENTO ELECTRÓNICO

ADJUDICACIÓN SIMPLIFICADA N° 06-2023-SIMA - SEGUNDA CONVOCATORIA
ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL Y
FILTRO DE CONTENIDO EN ALTA DISPONIBILIDAD

En la Provincia Constitucional del Callao, siendo las 09:30 horas del día 10 de noviembre del 2023, se reunieron los integrantes del Comité de Selección nombrado para el presente procedimiento de selección a efectos de llevar a cabo la admisión, evaluación, calificación y el otorgamiento de la buena pro, de la Adjudicación Simplificada N° AS-06-2023-SIMA-SEGUNDA CONVOCATORIA.

El Comité de Selección para el presente acto se encontró integrado por los siguientes miembros designados mediante Formato N° AS-06-2023-SIMA aprobado el 22 de septiembre del 2023.

NOMBRES Y APELLIDOS	DEPENDENCIA	DNI	CARGO
RICARDO CONDEMARIN MONTEALEGRE	AREA USUARIA	18099233	PRESIDENTE
MANUEL MEREGILDO ALTAMIRANO	AREA USUARIA	43435601	PRIMER INTEGRANTE
ADELAIDA ALBURQUEQUE TORRES	OEC	25604583	SEGUNDO INTEGRANTE

1. DETALLE DE LOS PARTICIPANTES:

De acuerdo con el listado de actividades establecido en el SEACE, se registraron los siguientes participantes:

Entidad convocante
Nomenclatura
Nro. de convocatoria
Objeto de contratación
Descripción del objeto
Número de Contratación

SERVICIO INDUSTRIAL DE LA MARINA S.A.
AS-SIM-6-2023-SIMA PERU-2
2
Bien
ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL CON FILTRO DE CONTENIDO EN ALTA DISPONIBILIDAD
SIMA PERU SA-2023-495

Búsqueda de participante

Estado de registro

[Selecciona]

Participante

[Selecciona]

Buscar

Limpiar

Regresar

Nro	Tipo proveedor	RUC/Código	Nombre o Razón Social	Fecha de registro en el procedimiento	Estado	Adscripción	Fecha de registro	Usuario de Registro	Acciones
1	Proveedor con RUC	20475805101	INNOVARE E-BUSINESS S.A.C.	28/10/2023	Válido		28/10/2023	20475805101	0 0 1
2	Proveedor con RUC	20519286794	FRAVATEL EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA	30/10/2023	Válido		30/10/2023	20519286794	0 0 1
3	Proveedor con RUC	20552075341	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	30/10/2023	Válido		30/10/2023	20552075341	0 0 1
4	Proveedor con RUC	20604021813	INSPIRA SECURE TECHNOLOGY S.A.C.	31/10/2023	Válido		31/10/2023	20604021813	0 0 1
5	Proveedor con RUC	20605361901	INVERSIONES MARHIL S.R.L.	29/10/2023	Válido		29/10/2023	20605361901	0 0 1
6	Proveedor con RUC	20606100273	L & F PROYECTOS Y SOLUCIONES SOCIEDAD COMERCIAL DE RESPONSABILIDAD LIMITADA	29/10/2023	Válido		29/10/2023	20606100273	0 0 1
7	Proveedor con RUC	20608993909	IT ONE S.A.C.	07/11/2023	Válido		07/11/2023	20608993909	0 0 1

7 registros encontrados, mostrando 7 registro(s), de 1 a 7. Página 1 / 1.

2. DETALLE DE LOS POSTORES:

Dentro de la fecha prevista en el listado de actividades, para la evaluación y calificación de ofertas presentadas, el comité de selección realiza la apertura de ofertas de manera electrónica a través del SEACE (descarga de las ofertas).

Presentación de ofertas/expresión de interés

Entidad convocante: SERVICIO INDUSTRIAL DE LA MARINA S.A.
Nomenclatura: AS-SM-S-2023-SIMA PERU-2
Nro. de convocatoria: 2
Objeto de contratación: Bien
Descripción del objeto: ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL CON FILTRO DE CONTENIDO EN ALTA DISPONIBILIDAD

Nro. ítem	Descripción del ítem			
RUC / Código	Nombre o Razón Social		Fecha Presentación	Forma de presentación
1	ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL CON FILTRO DE CONTENIDO EN ALTA DISPONIBILIDAD			
20552075341	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.		08/11/2023	Electronico

Acto seguido, se procede a la apertura electrónica de las ofertas a fin de verificar la presentación de lo requerido en la sección específica de las bases, de conformidad con el numeral 73.2 del artículo 73 del Reglamento de la Ley de Contrataciones del Estado (RLCE), y determina si las ofertas responden a las características y/o requisitos funcionales y condiciones de las Especificaciones Técnicas, detallados en las bases integradas.

3. DETALLE DE LA PRESENTACIÓN DE OFERTAS:

De acuerdo al artículo 73 del RLCE, la presentación de ofertas, se realiza de manera electrónica a través del SEACE, durante el periodo establecido en la convocatoria;

Artículo 52 del RLCE.- Contenido mínimo de las ofertas: Los documentos del procedimiento establecen el contenido de las ofertas;

CAPITULO II Numeral 2.2.1 Documentación de presentación obligatoria:

CUADRO COMPARATIVO										
ADJUDICACIÓN SIMPLIFICADA N°04-2023-SIMA PERÚ-SEGUNDA CONVOCATORIA										
ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL Y FILTRO DE CONTENIDO EN ALTA DISPONIBILIDAD										
PAC- 15										
EVALUACION DE OFERTAS										
A.- VERIFICACIÓN DE DOCUMENTOS OBLIGATORIOS										
EMPRESAS POSTORAS	a	b	c	d	e	f	g	h	ADMISIBILIDAD	OBSERVACIONES
	Declaración Jurada de datos del postor	Documento de Acreditación de la representación de quien suscribe la oferta	Declaración Jurada Artículo 52 del Reglamento	Declaración Jurada de cumplimiento de las Especificaciones Técnicas contenidas en el numeral 3.1 del Cap. II de la Sección REQUERIMIENTO	Indicar marca y modelo de los equipos propuestos, presentar documento oficial (fabricante / hoja técnica, brochure, datasheet) indicar número de folio que sustente las características técnicas numeral 5.4 de las EE.TT., de acuerdo Anexo N° 12 de las Bases	Declaración Jurada plazo de prestación del servicio	Promesa de Consorcio (Sólo para el caso en que un consorcio se presente como postor), con firmas legalizadas, de ser el caso	Precio de la Oferta en soles		
	anexo 1		anexo 2	anexo 3		anexo 4	anexo 5	anexo 6		
IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	PRESENTA	PRESENTA	PRESENTA	PRESENTA	PRESENTA	PRESENTA	NO APLICA	PRESENTA	ADMITIDO	NINGUNA

DETALLE EVALUACIÓN FICHA TÉCNICA (ENTE TÉCNICO)

PROCESO: ADJUDICACIÓN SIMPLIFICADA N° 06-2023 - SIMA PERÚ-SEGUNDA CONVOCATORIA			
Descripción del Bien:	EVALUACIÓN TÉCNICA PARA LA "ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL Y FILTRO DE CONTENIDO EN ALTA DISPONIBILIDAD"		
Plazo:	35 días calendarlos		
Presupuesto:	S/ 170,000.00 sin IGV		
Forma de pago:	Único pago posterior a la firma del acta de conformidad respectiva.		
Detalle de las ofertas		IMPERIA SOLUCIONES TECNOLOGICAS S.A.C. PROVEEDOR 1	
1. CARACTERÍSTICAS Y/O CONDICIONES DEL BIEN			
5.2 CARACTERÍSTICAS GENERALES.			
	5.2.1NEXT GENERATION FIREWALL PARA LA SEDE PRINCIPAL EN ALTA DISPONIBILIDAD.		
	La solución tiene que ser ofrecida en Alta Disponibilidad (HA), es decir por lo menos DOS (02) equipos appliances con las mismas características mínimas mencionadas en estas especificaciones.		CUMPLE
5.3 CARACTERÍSTICAS TÉCNICAS DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL			
	5.3.1 CARACTERÍSTICAS DE RENDIMIENTO PARA FIREWALL.		
	a. Throughput de Next Generation Firewall de 4.3 Gbps (mínimo) medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.		CUMPLE
	b. Throughput de Prevención de Amenazas de 2 Gbps (mínimo) medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: control de aplicaciones, sistema de prevención de intrusos (IPS), seguridad del tráfico DNS, antivirus/antimalware de red, antispymware/antibot, sandboxing, filtro de archivos y logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido al habilitar los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242.		CUMPLE
	c. El equipo debe soportar como mínimo 390.000 sesiones simultaneas y 70.000 sesiones por segundo, medidos con paquetes HTTP de 1 byte.		CUMPLE
	d. Debe contar con fuente de poder redundante.		CUMPLE
	e. Disco interno de 120 GB o superior.		CUMPLE
	f. Mínimo OCHO (08) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red.		CUMPLE

	g. La plataforma deberá contar con al menos UN (01) puerto de gestión fuera de banda dedicada para la gestión del equipo.	CUMPLE
	h. Deberá tener CPU dedicado para tareas de gestión del equipo, de manera independiente a los recursos de CPU para el procesamiento del tráfico. Esta arquitectura podrá estar integrada dentro del NGFW, o en caso no lo soporte, se podrán incluir consolas de gestión externas al NGFW.	CUMPLE
	i. El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicasi, jumpo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.	CUMPLE
	j. Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).	CUMPLE
	k. Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VLAN e IPsec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.	CUMPLE
	l. Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de ruteo y NAT), capa 2, transparente y sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.	CUMPLE
	m. Soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based forwarding, ECMP, dual-stack, QoS, DSCP, NPTv6, NAT64, LLDP, BFD, DHCPv6 relay, SLAAC, SNMP.	CUMPLE
	n. La plataforma propuesta por el fabricante debe contar con certificación USGV6-1 para las pruebas de firewall, IDS e IPS.	CUMPLE
	o. Soporte a configuración de alta disponibilidad Activo/Activo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).	CUMPLE
	p. La configuración en alta disponibilidad debe sincronizar sesiones, certificados de descifrado, configuraciones, incluyendo, más no limitada a políticas de seguridad, NAT, QoS y objetos de red.	CUMPLE
	q. Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.	CUMPLE
	r. Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.	CUMPLE
	5.3.2 FUNCIONALIDADES DE FIREWALL.	
	a. Control de políticas puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos).	CUMPLE
	b. Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.	CUMPLE
	c. Debe realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).	CUMPLE
	d. Debe mostrar la primera y última vez que se utilizó una regla de seguridad.	CUMPLE
	e. Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.	CUMPLE
	f. Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.	CUMPLE

	g. Debe permitir tener un registro de auditoría en cada política que permita conocer que cambios se realizó con anterioridad.	CUMPLE
	h. Debe permitir la definición de grupos dinámicos de direcciones IP, que permita colocar de manera automática direcciones IP en grupos de cuarentena si éstos realizan acciones maliciosas o restringidas. Estas acciones, deberán poder ser personalizadas en la consola del equipo.	CUMPLE
	5.3.3 DESCIFRADO DE TRÁFICO SSL/TLS.	
	a. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.	CUMPLE
	b. Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.	CUMPLE
	c. Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.	CUMPLE
	d. Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.	CUMPLE
	e. Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS.	CUMPLE
	f. Debe soportar certificados que utilice subject alternative name (SAN) y Server Name Indication (SNI).	CUMPLE
	g. Debe permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar el no descifrado de páginas con contenido sensible, mientras forzar el descifrado de páginas de clasificación de riesgo alto o medio.	CUMPLE
	h. Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.	CUMPLE
	i. Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores.	CUMPLE
	j. Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).	CUMPLE
	5.3.4 CONTROL DE APLICACIONES.	
	a. Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, video, proxy, mensajería instantánea, email.	CUMPLE
	b. Las aplicaciones deberán estar clasificadas en al menos 30 tipos, de tal manera que se puedan configurar políticas en base al tipo de aplicación.	CUMPLE
	c. Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.	CUMPLE

	d. Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. Debe ser capaz de determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.	CUMPLE
	e. Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.	CUMPLE
	f. Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación. Es decir, si 2 aplicaciones utilizan el mismo puerto y protocolo, se debe poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.	CUMPLE
	g. Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión.	CUMPLE
	h. Deberá contar con un módulo de aprendizaje que permita migrar las políticas basadas en puertos específicos y políticas con puertos ALL/ANY, a políticas basadas en aplicaciones.	CUMPLE
	i. El módulo de aprendizaje deberá ser específico por cada política de seguridad.	CUMPLE
	j. El módulo de aprendizaje deberá mostrar el nombre de la(s) aplicación(es) que han pasado por una política de seguridad, fecha de primera y última ocurrencia y volumen de datos transferido por cada aplicación.	CUMPLE
	k. Deberá contar con un wizard que permita convertir una política basada en puertos (capa 4) a una política basada en aplicaciones (capa 7) en base al aprendizaje realizado. En caso la solución propuesta no tenga este módulo de aprendizaje el postor deberá incluir en su oferta técnica el servicio de migración de todas las políticas de seguridad basadas en puertos a políticas basadas en aplicaciones.	CUMPLE
	5.3.5 PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS).	
	a. Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood.	CUMPLE
	b. Debe ser posible utilizar SYN Cookies como medida de defensa.	CUMPLE
	c. La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor).	CUMPLE
	d. Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo.	CUMPLE
	e. Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route.	CUMPLE
	f. Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino con la finalidad de evitar la saturación de sesiones hacia dicho equipo.	CUMPLE
	5.3.6 PREVENCIÓN DE AMENAZAS.	
	a. La solución propuesta deberá contar con capacidades de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.	CUMPLE
	b. Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar de forma permanente, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.	CUMPLE


	c. El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.	CUMPLE
	d. La solución deberá identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que se pueda bloquear dichas consultas DNS.	CUMPLE
	e. Deberá contar con un mecanismo que permita identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, inclusive si el tráfico entre la potencial víctima y su servidor DNS utilizado no pasa por el NGFW.	CUMPLE
	f. Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado sobre HTTPS (DNS over HTTPS - DoH), y también DNS sobre TLS.	CUMPLE
	g. El módulo de IPS debe ser capaz de bloquear ataques en base a firmas, heurística y anomalías en el protocolo.	CUMPLE
	h. El módulo de IPS debe permitir personalizar firmas directamente desde la consola gráfica.	CUMPLE
	i. Deberá ser capaz de identificar y bloquear amenazas avanzadas indetectables por firmas o heurística, incluyendo ataques de inyección y command and control realizados con herramientas de Cobalt Strike, Brute Ratel C4.	CUMPLE
	j. La protección contra amenazas avanzadas indetectables por firmas, heurística o reputación del dominio o contenido deberá estar basado en mecanismos de inteligencia artificial, tales como deep learning y/o machine learning.	CUMPLE
	k. Respecto a ataques de malware, las firmas deberán estar basadas en patrones y no únicamente en hashes, con el objetivo de identificar y bloquear el malware polimórfico que pertenezca a una misma familia.	CUMPLE
	l. Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SFTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención	CUMPLE
	5.3.7 ANALISIS DE MALWARE DE DÍA CERO.	
	a. La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.	CUMPLE
	b. La plataforma de Sandboxing debe ser ofrecido en Nube (Cloud). Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac.	CUMPLE
	c. También se aceptará soluciones sandbox terceras de otro fabricante distinto al NGFW.	CUMPLE
	d. Con la finalidad de contar con una protección robusta contra amenazas emergentes a nivel mundial, la solución deberá ser capaz de actualizar su base de firmas de malware en tiempo real sin afectar el performance del equipo.	CUMPLE
	e. El análisis dinámico deberá realizarse de forma paralela para todos los archivos enviados y no deberá tomar más de 10 minutos en dar un veredicto.	CUMPLE
	f. Deberá emular los archivos sospechosos en entornos Windows, Linux, Android y Mac sin estar limitado a una capacidad de hardware ni VMs (Virtual Machines).	CUMPLE
	g. Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.	CUMPLE

	h. El Next Generation Firewall deberá ser capaz de actualizar las firmas de malware en tiempo real, con el objetivo de tener información de malware detectado a nivel global por el fabricante.	CUMPLE
	i. Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II Plus de AICPA, ISO 27001, ISO 27017 e ISO 27018.	CUMPLE
	j. El malware de día cero deberá poder ser identificado dentro de la infraestructura de la Entidad, sin necesidad de enviar el archivo a ser analizado fuera de la red.	CUMPLE
	k. Debe proveer información forense sobre las acciones realizadas por el malware, tales como resumen del comportamiento visto, actividad sobre los archivos, peticiones DNS, conexiones de red, actividad de los archivos, procesos y registros. Esta información deberá poder ser extraída en un reporte PDF.	CUMPLE
	l. Deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.	CUMPLE
	m. Debe permitir al administrador la descarga del archivo original analizado por el sandbox.	CUMPLE
	n. Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.	CUMPLE
	o. Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico.	CUMPLE
	p. Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.	CUMPLE
	q. La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.	CUMPLE
	5.3.8 PROTECCION AVANZADA DE DNS.	CUMPLE
	a. La plataforma deberá ser alimentada por un servicio de inteligencia global de amenazas capaz de identificar millones de dominios maliciosos con análisis en tiempo real.	CUMPLE
	b. La protección del tráfico DNS deberá contar con mecanismos avanzados de protección, para identificar ataques imposibles de mitigar con firmas y/o reputación del dominio. Para lo cual se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial.	CUMPLE
	c. Deberá ser capaz de prevenir ataques como DGA (Domain Generation Algorithm) Random y de Diccionario, DNS Tunneling, Fast Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS.	CUMPLE
	d. Deberá soportar el manejo excepciones para poder mitigar los falsos positivos.	CUMPLE
	e. Deberá contar con dashboards y estadísticas sobre la cantidad, tipo de peticiones DNS, clasificación de la amenaza, generadas por los dispositivos internos de la Empresa/Institución.	CUMPLE
	f. El análisis del tráfico DNS podrá ser realizar de manera local en el mismo equipo, una solución externa (en nube u onpremise) del mismo u otro fabricante.	CUMPLE
	g. En caso de ser una plataforma en nube deberá estar certificado en SOC2 Tipo II de AICPA.	CUMPLE
	5.3.9 IDENTIFICACION DE USUARIOS.	CUMPLE

	a. Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell Directory, Exchange y base de datos local.	CUMPLE
	b. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.	CUMPLE
	c. Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI.	CUMPLE
	d. Debe disponer de un servicio en nube o onpremise que extraiga automáticamente la información del usuario grupos de usuario de varios IDPs y proveedores de SSO como Azure AD, okta, Google Identity y PingID y la ponga a disposición de los NGFW para ser incluidos en la política de seguridad.	CUMPLE
	e. Debe disponer de un servicio en nube o onpremise que simplifique la autenticación SAML de usuarios, que actúe como Service Provider único frente a IDPs o proveedores de SSO.	CUMPLE
	f. Debe disponer de un servicio en nube o onpremise que almacene todos los grupos disponibles del Active Directory, los filtre y ponga a disposición únicamente los grupos necesarios que el NGFW utilice en la política de seguridad.	CUMPLE
	g. Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.	CUMPLE
	h. Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.	CUMPLE
	i. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a Internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.	CUMPLE
	j. Debe permitir la definición de grupos dinámicos de usuarios.	CUMPLE
	5.3.10 FILTRO DE CONTENIDO WEB.	
	a. Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.	CUMPLE
	b. Debe soportar un cache local de URLs en el dispositivo, evitando el delay de comunicación/validación de las URLs.	CUMPLE
	c. Debido a que diariamente se crean decenas de miles de nuevas páginas web, la solución deberá ser capaz de analizar en tiempo real si la página web tiene contenido malicioso cuando un usuario intenta acceder.	CUMPLE
	d. El análisis en tiempo real deberá determinar si la página web desconocida (no categorizada en la base de datos del fabricante), tiene contenido javascript malicioso, phishing, actividad de command and control y otros tipos de contenido malicioso.	CUMPLE
	e. Debe contar con medidas de anulación como Cloaking, Captcha falsos, codificación de caracteres HTML, entre otros.	CUMPLE
	f. Debe permitir la creación de categorías personalizadas.	CUMPLE
	g. Debe permitir la personalización de la página de bloqueo.	CUMPLE
	h. Debe permitir notificar al usuario, mostrándole solo una página de alerta personalizable, pero permitiéndole continuar la navegación al site.	CUMPLE
	i. Debe ser capaz de registrar el User-agent, Referer, XFF de cada sesión hacia Internet.	CUMPLE

j.	Debe ser capaz de forzar la navegación de los usuarios en el modo Safe Search Enforcement.	CUMPLE
k.	Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de robo de credenciales	CUMPLE
5.3.11 FUNCIONALIDADES DE OPTIMIZACIÓN.		
a.	Se debe proporcionar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de configuración en el Firewall implementado.	CUMPLE
b.	Esta herramienta debe funcionar en línea y de manera automática. Es decir, luego de cada configuración realizada en el Firewall, debe mostrar los cambios realizados.	CUMPLE
c.	Debe contar con gráficos ejecutivos que permitan mostrar el nivel de adopción de los módulos de seguridad del NGFW en las políticas de seguridad.	CUMPLE
d.	Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red.	CUMPLE
e.	Debe identificar automáticamente las políticas abiertas que no tengan restricciones de puertos y/o aplicaciones (ANY o ALL), con el objetivo de corregirlas y hacer cumplir el principio de mínimo privilegio.	CUMPLE
f.	La herramienta de evaluación de buenas prácticas debe mostrar al menos lo siguiente: nivel de adopción del control de aplicaciones, visibilidad de usuarios, configuraciones correctas de los perfiles de seguridad (antivirus, IPS, sandboxing), hardening de la plataforma.	CUMPLE
g.	La herramienta de evaluación de buenas prácticas debe ser específica para la configuración de firewall implementado, no se aceptarán guías de usuarios genéricas.	CUMPLE
h.	Debe contar con un dashboard que muestre la salud del equipo. Asimismo, si apareciera una falla debe enviar un correo de manera automática.	CUMPLE
5.3.12 CONSOLA DE ADMINISTRACIÓN Y MONITOREO.		
a.	Con la finalidad de no degradar el performance de procesamiento de red y seguridad del NGFW, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante.	CUMPLE
b.	Permitir exportar las reglas de seguridad en formato CSV y PDF.	CUMPLE
c.	Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.	CUMPLE
d.	Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.	CUMPLE
e.	Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino).	CUMPLE
f.	Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de sólo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.	CUMPLE


	g. Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.	CUMPLE
	h. Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).	CUMPLE
	i. Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).	CUMPLE
	j. Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.	CUMPLE
	k. Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).	CUMPLE
	l. Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, su IP y el horario de la alteración.	CUMPLE
	m. Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.	CUMPLE
	n. Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a Internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.	CUMPLE
	o. Debe permitir configurar reportes para ver el tiempo de navegación de los usuarios en Internet, clasificado por tipo de página web y URL.	CUMPLE
	p. Debe contar con reportes predeterminados que muestren información y diversas estadísticas sobre el uso de aplicaciones SaaS.	CUMPLE
	q. La gestión de NGFW debe permitir realizar tareas de gestión a través del API basado en XML.	CUMPLE
2. REQUERIMIENTOS DEL POSTOR Y/O PERSONAL		
7.1. REQUISITOS DEL POSTOR.		
1. El proveedor deberá de demostrar mediante carta de fabricante o enlace de página web oficial del fabricante, que es partner autorizado de la solución ofertada.		
2. El proveedor deberá de enviar una copia de la certificación, el cual valida que su SOC (Security Operations Center) está de acuerdo con la norma ISO 27001.		

<p>3. PLAZO DE ENTREGA DEL BIEN</p> <p>8.2.1.1. Plazo de entrega de los bienes. Los bienes y/o licenciamiento serán entregados en un plazo no mayor a TREINTA (30) días calendario, contados a partir del día siguiente del perfeccionamiento del contrato.</p> <p>8.2.1.2. Plazo de instalación, configuración y puesta en producción. La instalación, configuración y puesta en producción será en un plazo no mayor a CINCO (05) días calendario, contados a partir de la entrega de los bienes y/o licencias.</p>	<p>CUMPLE</p>
<p>4. FECHA DE VALIDACIÓN: 09/11/2023</p>	
<p>5. RESPONSABLE DE VALIDACIÓN (NOMBRE Y FIRMA)</p> <p><i>RODRIGO MANUEL MEREZUELO ALVARADO</i></p> 	

RESULTADO:

Proveedor N°1
CUMPLE

OBSERVACIONES:


 Ing. Luis Villa Mostacero
 Experto en Infraestructura y
 Servicios Informáticos (e) OTIC
 SIMA - PERÚ S.A.

EVALUACIÓN DE OFERTAS:

Artículo 74 RLCE. - Evaluación de Ofertas

La evaluación de ofertas consiste en la aplicación de los factores de evaluación a las ofertas que cumplen con lo señalado en el numeral 73.2 del artículo 73;

Párrafo 1.8 Sección General de las Bases Administrativas. -

La evaluación de las ofertas que cumplan con lo señalado en el numeral anterior tiene por objeto determinar la oferta con el mejor puntaje y el orden de prelación de la oferta, según los factores y el procedimiento de evaluación enunciados en la sección específica de las Bases:

B.- FACTORES DE EVALUACIÓN						
EMPRESAS POSTORAS	Precio Ofertado (100 pts)		Bonificación 5%			OBSERVACIONES
	$P_i = \frac{Q_m \times PMPE}{Q_i}$		ANEXO N° 10 SOLICITUD ASIGNACIÓN DE BONIFICACIÓN DEL CINCO POR CIENTO (5%) SOBRE EL PUNTAJE TOTAL OBTENIDO, POR TENER LA CONDICIÓN DE MICRO Y PEQUEÑA EMPRESA		PUNTAJE TOTAL	
	Oferta	Puntaje	Oferta	Puntaje	Puntaje	ORDEN DE PRELACIÓN
IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	200,590.00	100.00	Presento Anexo 10 solicitud bonificación	5.00	105.00	†

RESULTADO DE LOS FACTORES DE EVALUACIÓN A LAS OFERTAS QUE CUMPLEN			
N°	POSTOR	RESULTADO	PUNTAJE TOTAL
1	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	CUMPLE	105.00

CALIFICACIÓN DE OFERTAS:

Artículo 75 RLCE. - Calificación

Luego de culminada la evaluación, el comité de selección califica a los postores que obtuvieron el primer y segundo lugar, según el orden de prelación, verificando que cumplan con los requisitos de calificación especificados en las bases. La oferta del postor que no cumpla con los requisitos de calificación es descalificada;

Párrafo 2.2.1.2 Sección Específica de las Bases Administrativas

Documentos para acreditar los requisitos de calificación;

Si algunos de los postores cumplen con los requisitos de calificación su oferta se CALIFICA:

C.- VERIFICACIÓN DE DOCUMENTOS DE CALIFICACIÓN

	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD	CAPACIDAD TÉCNICA Y PROFESIONAL		EXPERIENCIA DEL PERSONAL CLAVE
		CALIFICACIONES DEL PERSONAL CLAVE		
		FORMACIÓN ACADÉMICA		
EMPRESAS POSTORAS	<p>Requisitos:</p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/. 220,000.00 (DOSCIENTOS VEINTE MIL CON 00/100 SOLES), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acreditará una experiencia de S/. 24,180.00 (VEINTICUATRO MIL CIENTO OCHENTA CON 00/100 SOLES), por la venta de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p>Se consideran ventas similares a los siguientes: venta de equipos de seguridad firewall y/o venta de equipos de seguridad anti spam y/o venta de equipos de seguridad ips y/o venta de servidores de datos y/o venta de sistema de almacenamiento y/o venta de soluciones de infraestructura.</p> <p>Acreditación:</p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta; cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago(1); correspondientes a un máximo de veinte (20) contrataciones:</p>	<p>DEL JEFE DE PROYECTO</p> <p>Requisitos:</p> <p>UN (01) profesional titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas. Deberá estar colegiado y habilitado al momento de la presentación de la oferta.</p> <p>Deberá contar con certificación PMP vigente y/o especialización o diplomado en gestión de proyectos con base en el enfoque del Project Management Institute - PMI, con una duración mínima de 160 horas.</p> <p>Acreditación:</p> <p>Copia simple de título en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.</p> <p>El título profesional podrá ser verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe, o según corresponda.</p> <p>Deberá demostrar estar colegiado y estar habilitado en el CIP.</p> <p>Copia simple de certificado oficial PMP</p> <p>DEL SUPERVISOR DE PROYECTO</p> <p>Requisitos:</p> <p>UN (01) profesional titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas. Deberá estar colegiado y habilitado al momento de la presentación de la oferta.</p> <p>Deberá contar con certificación services desk leader o IT service management (ITSM).</p> <p>Deberá contar con certificación ITIL y Lead Cybersecurity Professional Certificate (LCSPC).</p> <p>Acreditación:</p> <p>Copia simple de título en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.</p> <p>El título profesional podrá ser verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe, o según corresponda.</p> <p>Deberá demostrar estar colegiado y estar habilitado en el CIP.</p> <p>Copia simple de certificado oficial services desk leader o IT service management (ITSM).</p> <p>Copia simple de certificado oficial ITIL y Lead Cybersecurity Professional Certificate (LCSPC).</p> <p>DEL ESPECIALISTA DE SEGURIDAD PERIMETRAL</p> <p>Requisitos:</p> <p>UN (01) técnico titulado, profesional, bachiller o titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.</p> <p>Certificado en la marca ofertada.</p> <p>Acreditación:</p> <p>Copia simple de, profesional, bachiller o titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.</p> <p>El título profesional podrá ser verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe, o según corresponda.</p> <p>Copia simple de certificado en la marca ofertada.</p>	<p>DEL JEFE DE PROYECTO</p> <p>Requisitos:</p> <p>Deberá contar con experiencia mínima de DOS (02) años en Gestión de Proyectos de TI y/o proyectos de seguridad de la información.</p> <p>DEL SUPERVISOR DE PROYECTO</p> <p>Requisitos:</p> <p>Deberá contar con experiencia mínima de DOS (02) años en supervisión de proyectos de seguridad informática y/o soluciones de seguridad y/o soluciones de seguridad de la información.</p> <p>DEL ESPECIALISTA DE SEGURIDAD PERIMETRAL</p> <p>Requisitos:</p> <p>Deberá contar con experiencia mínima de DOS (02) años en implementaciones, soporte técnico y mantenimiento de soluciones de firewall de seguridad perimetral e interno.</p> <p>Acreditación:</p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto</p>	
	IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.	Cumple	Cumple	Cumple

Nota: Este Cuadro de Verificación de Documentos de Calificación, se Anexa a la presente Acta, el cuadro original, para mejor visualización.

Culminada la verificación de documentos de calificación con el siguiente resultado:

Nº	POSTOR	RESULTADO
1	IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	CALIFICA

OTORGAMIENTO DE LA BUENA PRO:

Artículo 76 del RLC. - Otorgamiento de la buena pro

Definida la oferta ganadora, el comité de selección otorga la buena pro, mediante su publicación en el SEACE;

Párrafo 1.12 Sección General de las Bases Administrativas, Luego de la calificación de la oferta, el comité de selección otorga la buena pro en la fecha señalada en el calendario de las bases mediante su publicación en el SEACE.

D. BUENA PRO			
EMPRESA POSTORA	PLAZO DE ENTREGA	MONTO ADJUDICADO EN SOLES	MONTO ADJUDICADO EN LETRAS
IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.	SEGÚN LAS ESPECIFICACIONES TÉCNICAS SU OFERTA EN (PLAZO DE EJECUCIÓN TRENTA Y CINCO (35) DÍAS CALENDARIO)	S/ 200,590.00	DOSCIENTOS MIL QUINIENTOS NOVENTA CON 00/100 SOLES

4. ACUERDOS

El Comité de Selección del procedimiento de selección electrónico Adjudicación Simplificada N° AS-06-2023-SIMA - SEGUNDA CONVOCATORIA, luego de efectuar la admisión, evaluación y calificación de ofertas por unanimidad, procede a otorgar la BUENA PRO para la Adquisición de Solución de Seguridad perimetral Next Generation firewall y filtro de contenido en alta disponibilidad, de acuerdo a las Bases integradas del debido procedimiento de selección, al postor IMPERIA SOLUCIONES TECNOLOGICAS S.A.C., por un monto total de DOSCIENTOS MIL QUINIENTOS NOVENTA CON 00/100 SOLES (S/ 200,590.00).

Al haber cumplido con los requisitos técnicos mínimos y su oferta económica al estar dentro del marco presupuestal asignado.

Siendo las 10:30 horas del día 10 de noviembre del 2023, se culmina el acto, firmando los presentes en señal de conformidad.

Ing. Manuel MEREGILDO Altamirano
Primer Integrante del
Comité de Selección
AS-06-2023-2

Esp. Adelaida ALBURQUEQUE Torres
Segundo Integrante del
Comité de Selección
AS-06-2023-2

Ing. Ricardo CONDEMARIN Montealegre
Presidente del Comité de Selección
AS-06-2023-2

ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL Y FILTRO DE CONTENIDO EN ALTA DISPONIBILIDAD

EVALUACION DE OFERTAS

EVALUACION DE OFERTAS

EVALUACION DE OFERTAS

Don Williams Esq.

Don Williams Esq.

CAPACIDAD TECNICA Y PROFESIONAL

CAPACIDAD TECNICA Y PROFESIONAL

