

FORMATO								
RESUMEN EJECUTIVO DE LAS ACTUACIONES PREPARATORIAS (SERVICIOS)								
1.	DATOS GENERALES							
1.1	FECHA DE EMISIÓN DEL FORMATO	16/04/2025						
1.2	ÁREA USUARIA	OFICINA GENERAL DE TECNOLOGÍAS DE INFORMACIÓN						
1.3	DENOMINACIÓN DE LA CONTRATACIÓN	SERVICIO DE GESTIÓN DE CIBERSEGURIDAD PERIMETRAL PARA EL MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS						
1.4	ACTIVIDAD DEL POI VINCULADA A LA CONTRATACIÓN	C0043 CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL MINJUSDH						
1.5	Nº DE REFERENCIA DEL PAC	21						
1.6	PROYECTO DE INVERSIÓN PÚBLICA	Código	----					
		Documento que declaró la viabilidad	----					
2.	INFORMACIÓN SOBRE EL REQUERIMIENTO							
2.1	DATOS DEL REQUERIMIENTO	Documento de requerimiento	Memorando N°557-2025-JUS/OGTI	Fecha de recepción	25/03/2025			
2.2	MODIFICACIONES EFECTUADAS AL REQUERIMIENTO POR PARTE DEL ÁREA USUARIA	Fecha de la segunda versión	3/04/2025	De oficio		Con motivo de observaciones	X	
Fecha de la tercera versión		8/04/2025	De oficio		Con motivo de observaciones	X		
Fecha de la cuarta versión		11/04/2025	De oficio	X	Con motivo de observaciones			
2.3	SEÑALAR SI LA CONTRATACIÓN INCLUIRÁ PAQUETE(S)	SI			NO	X		
		De ser afirmativa la respuesta, detallar el sustento técnico del área usuaria o el órgano encargado de las contrataciones, según el caso.						
2.4	SEÑALAR SI LA CONTRATACIÓN SE EFECTUARÁ POR ITEMS	SI		NO	X			
2.5	SEÑALAR SI SE HA LLEVADO A CABO UN PROCESO DE ESTANDARIZACIÓN	SI		NO	X			
		Documento de aprobación de la estandarización		Fecha de aprobación				
2.6	SEÑALAR SI EL SERVICIO OBJETO DE LA CONTRATACIÓN HA SIDO HOMOLOGADO	SI		NO	X			
		N° de Resolución que aprobó la Ficha de Homologación		Fecha de inicio de vigencia				
2.7	REQUERIMIENTO	Lo indicado se visulaiza en el Capítulo III de la Sección Específica de las Bases.						
2.8	OBSERVACIONES AL REQUERIMIENTO							
	Nº Item	Cantidad total de observaciones	Cantidad de observaciones formuladas por el OEC	Comunicación con la cual se remitió al área usuaria las observaciones al requerimiento	Fecha de remisión de la comunicación	Cantidad de observaciones formuladas por los proveedores	Comunicación con la cual se remitió al área usuaria las observaciones al requerimiento	Fecha de remisión de la comunicación
	Único	158				158	Memorando N°1648-2025-JUS/OGA-OAB	1/04/2025

FORMATO							
RESUMEN EJECUTIVO DE LAS ACTUACIONES PREPARATORIAS (SERVICIOS)							
<p>Observaciones referente a:</p> <p>5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO.</p> <p>A. SERVICIO DE SEGURIDAD PERIMETRAL: Consideraciones generales; 3. Capacidad de rendimiento; 6. Funcionalidades de Firewall; 9. Prevención de amenazas; 10. Sandboxing; 11. Filtro de contenido web; 13. QOS; 15. VPN; 16. Detección y respuesta extendida; 18. Administración y monitoreo.</p> <p>B. SERVICIO DE PROTECCIÓN CONTRA ATAQUES A LAS APLICACIONES Y SERVICIOS WEB: Consideraciones específicas; requerimientos de seguridad web; requerimientos de seguridad de aplicaciones.</p> <p>C. ETHICAL HACKING; Consideraciones generales; Consideraciones específicas.</p> <p>D. PROTECCIÓN ANTIDDS PERIMETRAL NO VOLUMÉTRICO</p> <p>E. SERVICIO DE PROTECCIÓN DE CORREO ELECTRÓNICO (ANTISPAM); características generales; Uso de mecanismos de TLS; Gestión y reporte.</p> <p>F. SERVICIO DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD (CYBERSOC); Consideraciones generales; Consideraciones específicas de los servicios especializados requeridos del CYBERSOC;.</p> <p>Plazo del plan de trabajo.</p> <p>5.3 RECURSOS A SER PROVISTOS POR EL CONTRATISTA</p> <p>5.5 PRESTACIONES ACCESORIAS A LA PRINCIPAL</p> <p>5.6 REQUERIMIENTOS DEL PROVEEDOR Y DE SU PERSONAL; Ingenieros de implementación; Profesional asignado al proyecto.</p> <p>5.13 OTRAS PENALIDADES</p>							
Único	9	9	Memorando N°1775-2025-JUS/OGA-OAB	7/04/2025			
<p>Observaciones referente a:</p> <p>A. SERVICIO DE SEGURIDAD PERIMETRAL / Consideraciones generales</p> <p>18. ADMINISTRACIÓN Y MONITOREO / Para las consolas de administración de las soluciones perimetrales</p> <p>D. PROTECCIÓN ANTIDDS PERIMETRAL NO VOLUMÉTRICO</p> <p>F. SERVICIO DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD (CYBERSOC) / Gestión de las soluciones implementadas para brindar el servicio.</p> <p>5.2.1 Planteamiento del proyecto / penalidad.</p> <p>5.8 ENTREGABLES DEL SERVICIO</p> <p>6. REQUISITOS DE CALIFICACIÓN / C. Experiencia del postor en la especialidad / Anexos.</p>							
<b>2.9 RESPUESTA DEL ÁREA USUARIA</b>							
Nº Item	Cantidad total de respuestas a las observaciones	Cantidad de respuestas a las observaciones formuladas por el OEC	Comunicación de respuesta del área usuaria	Fecha de remisión de la comunicación	Cantidad de respuestas a las observaciones formuladas por los proveedores	Comunicación de respuesta del área usuaria	Fecha de remisión de la comunicación
Único	157				157	Memorando N°636-2025-JUS/OGTI	3/04/2025
<p>Absoluciones referente a:</p> <p>5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO.</p> <p>A. SERVICIO DE SEGURIDAD PERIMETRAL: Consideraciones generales; 3. Capacidad de rendimiento; 6. Funcionalidades de Firewall; 9. Prevención de amenazas; 10. Sandboxing; 11. Filtro de contenido web; 13. QOS; 15. VPN; 16. Detección y respuesta extendida; 18. Administración y monitoreo.</p> <p>B. SERVICIO DE PROTECCIÓN CONTRA ATAQUES A LAS APLICACIONES Y SERVICIOS WEB: Consideraciones específicas; requerimientos de seguridad web; requerimientos de seguridad de aplicaciones.</p> <p>C. ETHICAL HACKING; Consideraciones generales; Consideraciones específicas.</p> <p>D. PROTECCIÓN ANTIDDS PERIMETRAL NO VOLUMÉTRICO</p> <p>E. SERVICIO DE PROTECCIÓN DE CORREO ELECTRÓNICO (ANTISPAM); características generales; Uso de mecanismos de TLS; Gestión y reporte.</p> <p>F. SERVICIO DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD (CYBERSOC); Consideraciones generales; Consideraciones específicas de los servicios especializados requeridos del CYBERSOC.</p> <p>Plazo del plan de trabajo.</p> <p>5.3 RECURSOS A SER PROVISTOS POR EL CONTRATISTA</p> <p>5.5 PRESTACIONES ACCESORIAS A LA PRINCIPAL</p> <p>5.6 REQUERIMIENTOS DEL PROVEEDOR Y DE SU PERSONAL; Ingenieros de implementación; Profesional asignado al proyecto.</p> <p>5.13 OTRAS PENALIDADES</p>							
Único	9	9	Memorando N°666-2025-JUS/OGTI	8/04/2025			
<p>Absoluciones referente a:</p> <p>A. SERVICIO DE SEGURIDAD PERIMETRAL / Consideraciones generales</p> <p>18. ADMINISTRACIÓN Y MONITOREO / Para las consolas de administración de las soluciones perimetrales</p> <p>D. PROTECCIÓN ANTIDDS PERIMETRAL NO VOLUMÉTRICO</p> <p>F. SERVICIO DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD (CYBERSOC) / Gestión de las soluciones implementadas para brindar el servicio.</p> <p>5.2.1 Planteamiento del proyecto / penalidad.</p> <p>5.8 ENTREGABLES DEL SERVICIO</p> <p>6. REQUISITOS DE CALIFICACIÓN / C. Experiencia del postor en la especialidad / Anexos.</p>							
<b>2.10 AJUSTES QUE SE REALIZARON AL REQUERIMIENTO</b>							

FORMATO		
RESUMEN EJECUTIVO DE LAS ACTUACIONES PREPARATORIAS (SERVICIOS)		
Nº Item	Ajustes realizados al requerimiento	
Único	<p><u>5. ALCANCES Y DESCRIPCION DEL SERVICIO</u>  A la presentación de ofertas, el postor debe entregar la siguiente información técnica: La acreditación del cumplimiento de las características técnicas o funcionalidades requeridas por los componentes o soluciones del "Servicio de Ciberseguridad para el MINJUSDH" (...).</p> <p><u>A. SERVICIO DE SEGURIDAD PERIMETRAL</u>  3. CAPACIDAD DE RENDIMIENTO  *La plataforma de hardware debe soportar como mínimo 3 millones sesiones/conexiones concurrentes y 260 mil nuevas sesiones/conexiones por segundo como mínimo,...).</p> <p>*Debe contar con fuente de poder redundante intercambiable en caliente (HOT SWAP) o fuentes intercambiables (...)</p> <p>6. FUNCIONALIDADES DE FIREWALL  La solución debe permitir identificar las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall, (...).</p> <p>9. PREVENCIÓN Y AMENAZAS  *Con la finalidad de contar con pluralidad de marcas se acepta lo solicitado quedando de la siguiente manera: Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), y/o también DNS sobre TLS.</p> <p>10. SANDBOXING  *Deberá ser capaz de emular o analizar el potencial malware en entornos: Windows, Linux y/o MacOS.</p> <p>11. FILTRO DE CONTENIDO WEB  Debe contar con medidas de antievasión como Cloaking y/o Captcha falsos y/o codificación de caracteres HTML; o mecanismos similares que dificulten técnicas de evasión automatizadas por bots o scripts maliciosos.</p> <p>15. VPN: Autenticación MD5, SHA-1, SHA-2 y/o SHA-256; como mínimo.</p>	
	<p>16. DETECCIÓN Y RESPUESTA EXTENDIDA  *Asimismo, deberá contar con un módulo anti exploit el cual deberá identificar y bloquear técnicas de explotación sin necesidad de utilizar firmas y/o heurísticas (...).</p> <p>*Análisis Forense (entiéndase a investigaciones detalladas después de un incidente de seguridad, incluyendo el análisis de logs, tráfico de red, eventos de endpoints esto puede ser recopilado por telemetría o similar).</p> <p>*Asimismo deberá de incluir una secuencia grafica de incidentes de seguridad.</p> <p>*Cada incidente de seguridad asociado a un analista debe tener la siguiente información: Acciones de prevención realizadas y/o acciones de prevención recomendadas.</p> <p>*Las capacidades de análisis de cada incidente deben permitir tener una vista detallada de: Información y análisis forense para ver procesos (...).</p> <p>*Debe contar con un módulo de Inteligencia de Amenazas, que permita brindar contexto a través de la fuente del propio fabricante, así como de una fuente tercera o soportar integrarse con una fuente de terceros como mínimo, (...).</p> <p>*Debe poder crear y editar indicadores de compromiso (IoC) que se aplican a todos los productos (estaciones finales y servidores) integrados con la solución de XDR.</p> <p>*La consola de administración deberá estar alojada en nube provista por el fabricante a través de Internet. opcionalmente la consola de administración podría mostrar una secuencia gráfica del incidente de seguridad, (...).</p> <p>18. ADMINISTRACIÓN Y MONITOREO  *La solución debe permitir exportar las reglas de seguridad del NGFW al menos en formato CSV y PDF desde su consola de administración o mediante herramientas integradas del fabricante.</p> <p>*La gestión de NGFW debe permitir realizar tareas de gestión a través del API basado en XML y/o JSON.</p> <p>*Para las consolas de administración de las soluciones perimetrales:</p> <ul style="list-style-type: none"> <li>- "O en su defecto brindar soluciones que sean capaces de limitar la ejecución(compilar) de cambios efectuados por usuarios de menor jerarquía".</li> <li>- "O en su defecto brindar soluciones que sean capaces de limitar la ejecución(compilar) de cambios efectuados por usuarios de menor jerarquía".</li> <li>- "O en su defecto brindar soluciones que sean capaces de limitar la ejecución(compilar) de cambios efectuados por usuarios de menor jerarquía".</li> </ul> <p>*Deberá soportar la ingesta de 14 000 eventos por segundo para garantizar la recepción de los registros de todas las políticas configuradas, (...).</p> <p>*Debe contar con una capacidad de 16 TB utilizables después de realizado el RAID, en caso que Next Generation Firewall no cuente con recursos dedicados para la gestión, (...).</p>	

FORMATO	
RESUMEN EJECUTIVO DE LAS ACTUACIONES PREPARATORIAS (SERVICIOS)	
	<p><b>B. SERVICIO DE PROTECCIÓN CONTRA ATAQUES A LAS APLICACIONES Y SERVICIOS WEB</b></p> <p>*La solución debe incluir capacidades de protección contra vulnerabilidades descritas en OWASP Top 10, así como funcionalidades de WAF, Bot Manager, API Protection, Client Side Protection y mitigación DDoS para las aplicaciones web expuestas al entorno público (...).</p> <p>*El servicio debe cubrir la protección de subdominios/hosts/aplicaciones/servicios web en protocolos HTTP y HTTPS. Las 25 aplicaciones con capacidades de protección contra vulnerabilidades descritas en OWASP Top 10, (...).</p> <p>*El contratista deberá considerar un volumen estimado de llamadas API, tomando como base el tráfico actual de 4 millones de solicitudes HTTP/S por día (...).</p> <p>*El servicio de protección de BOT debe permitir integración nativa con ambientes Android e iPhone, mediante un SDK provisto por el fabricante (...).</p> <p><b>D. PROTECCIÓN ANTIDDS PERIMETRAL NO VOLUMETRICO</b></p> <p>*La solución deberá brindar protección para un volumen total de tráfico de 9Gb como mínimo.</p> <p><b>E. SERVICIO DE PROTECCIÓN DE CORREO ELECTRÓNICO (ANTISPAM)</b></p> <p>*La solución debe tener la capacidad de analizar el correo entrante y saliente hacia los servicios de Google Workspace u Office 365 tanto de manera en línea como a través de API, de manera que pueda ser aplicado el control de antispam y/o antivirus y detectar dichas amenazas.</p> <p>*Debe incluir el filtrado de contenido para el control de datos salientes y el cifrado de correo electrónico mediante cifrado de canal de comunicación tanto entrante como saliente.</p> <p>*La solución debe proteger todo el correo electrónico entrante y saliente al dominio incluso antes de que sea entregado en la bandeja del usuario final, de manera que se pueda proteger al usuarios final que accede incluso desde dispositivos móviles.</p> <p>*Debe soportar SPF, DMARC y DKIM tanto para la validación de la entrada de correos como para la salida a través de llaves de infraestructura pública o certificados digitales.</p> <p>*Deberá permitir verificar la versión de TLS, mínimo 1.2 y/o 1.3</p> <p>*Debe permitir la programación de informes o emisión de informes con determinada frecuencia en diversos formatos PDF o HTML y/o XML y/o CSV.</p>
	<p><b>F. SERVICIO DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD (CYBERSOC)</b></p> <p>*El CyberSOC debe brindar información de eventos e incidentes de seguridad, a través de consolas de visualización, que seguidos por los lineamientos especificados en el procedimiento de respuestas a incidentes faciliten la toma de decisiones a fin de mitigar los riesgos que pueden afectar notoriamente a los activos informáticos del MINJUSDH (...).</p> <p>*De los servicios especializados requeridos del CyberSOC. El CyberSOC debe brindar información de eventos e incidentes de seguridad, a través de consolas de visualización unificadas o consolas individuales de cada solución, (...).</p> <p><b>5.6 REQUERIMIENTOS DEL PROVEEDOR Y SU PERSONAL</b></p> <p>a) Profesional asignado al proyecto (01) - Dedicado</p> <p>*Se podrá asignar a los ingenieros de implementación para la ejecución del servicio (personal dedicado) brindando la documentación y experiencia solicitada según el perfil o para periodo de ejecución del servicio.</p> <p><b>5.7 LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO</b></p> <p>El plazo de entrega del Plan de Trabajo del servicio, es de hasta veinte (20) días calendario contados a partir del día siguiente de la suscripción del contrato. Por el incumplimiento en los plazos, se aplicará la penalidad establecida en el numeral 5.12 de los Términos de Referencia.</p>
Único	<p><b>A. SERVICIO DE SEGURIDAD PERIMETRAL / Consideraciones generales</b></p> <p>*El fabricante puede pertenecer al cuadrante de Líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 8 reportes. (Opcional).</p> <p><b>18. ADMINISTRACIÓN Y MONITOREO.</b> Se juntó el cuadro de "Acuerdo de niveles de servicio (ANS)</p> <p><b>D. PROTECCIÓN ANTIDDS PERIMETRAL NO VOLUMETRICO</b></p> <p>*La solución deberá brindar protección para un volumen total de tráfico de 9Gb como mínimo.</p> <p><b>F. SERVICIO DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD (CYBERSOC) / Gestión de las soluciones implementadas para brindar el servicio.</b></p> <p>*El Contratista debe acreditar mediante documentos y/o certificados oficiales lo requerido para la conformidad de la implementación e inicio del servicio.</p> <p><b>5.2.1 Planteamiento del proyecto</b></p> <p>*Dentro de los veinte (20) días calendarios (...), de no cumplir con dicho plazo se aplicará al contratista la penalidad mencionada en el numeral 5.13. de los Términos de Referencia, (...).</p> <p><b>5.8 ENTREGABLES DEL SERVICIO</b></p> <p>*De acuerdo a lo definido en el numeral 5.2.1 Planteamiento del Proyecto</p> <p>*De acuerdo a lo definido en el numeral 5.2.2. Inicio del Servicio</p> <p><b>6. REQUISITOS DE CALIFICACIÓN / C. Experiencia del postor en la especialidad.</b></p> <p>*Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo correspondiente.</p> <p>*Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo referido a la Experiencia del Postor en la Especialidad</p>
3.	<b>INFORMACIÓN SOBRE LA DETERMINACIÓN DEL VALOR REFERENCIAL</b>
3.1	<b>SOBRE EL VALOR REFERENCIAL EN CASO DE CONSULTORÍA DE OBRAS</b>
3.1.1	<b>ESTRUCTURA DE COMPONENTES O RUBROS</b>
	<b>DEL PROVEEDOR</b>
Nº Item	Detalle de la Estructura de Componentes o Rubros
	<b>DE LA ENTIDAD</b>

FORMATO									
RESUMEN EJECUTIVO DE LAS ACTUACIONES PREPARATORIAS (SERVICIOS)									
Nº Item		Detalle de la Estructura de Componentes o Rubros							
3.1.2	VALOR REFERENCIAL DE LA CONSULTORÍA DE OBRA	MONEDA	Nuevos Soles		Dólares		Otro:	Señalar otra moneda	
		MONTO							
	En el caso de consultoría de obras, además, detallar los costos directos, los gastos generales, fijos y variables, y la utilidad de acuerdo a las características, plazos y demás condiciones definidas en el requerimiento.								
4. INFORMACIÓN RELEVANTE ADICIONAL COMO RESULTADO DE LAS INDAGACIONES DE MERCADO									
4.1		FECHA DE INICIO DE LAS INDAGACIONES EN EL MERCADO			26/03/2025		FECHA DE CULMINACIÓN DE LAS INDAGACIONES EN EL MERCADO		15/04/2025
4.2	PLURALIDAD DE PROVEEDORES QUE CUMPLEN CON EL REQUERIMIENTO				SI	X	NO		
	De ser negativa la respuesta, indicar la evaluación de la Entidad respecto de la falta de pluralidad de proveedores que cumplen con el requerimiento.								
4.3	POSIBILIDAD DE DISTRIBUIR LA BUENA PRO (EN CASO DE SERVICIOS EN GENERAL, DE CORRESPONDER)				SI		NO	X	
	De ser afirmativa la respuesta, sustentar la posibilidad de distribuir la buena pro.								
4.4	SOBRE LA INFORMACIÓN QUE PUEDA UTILIZARSE PARA LA DETERMINACIÓN DE LOS FACTORES DE EVALUACIÓN				SI		NO	X	
	De ser afirmativa la respuesta, detallar la información que pueda utilizarse para la determinación de los factores de evaluación.								
4.5	SOBRE OTROS ASPECTOS NECESARIOS QUE TENGAN INCIDENCIA EN LA EFICIENCIA DE LA CONTRATACIÓN				SI		NO	X	
	De ser afirmativa la respuesta, detallar.								
5.									
NOMBRE, FIRMA Y SELLO DEL FUNCIONARIO COMPETENTE DEL ÓRGANO ENCARGADO DE LAS CONTRATACIONES									
<b>NOTA:</b> El presente formato se utilizará en servicios en general, servicios de consultoría en general y en consultoría de obras.									