Proyecto	Especialidad	Pregunta	Respuesta
	Técnica	¿Es excluyente para esta RFP, pertenecer al team FIRST?	No, siempre que se respete el acuerdo de confidencialidad
	Técnica	¿Respecto de las certificaciones ISO, es excluyente contar con ellas?	En capitulo 5.5.1 se indica los requisitos obligatorio y opcionales en cuanto a las certificaciones.
	Técnica	¿AVO ya cuenta con una solución de escaneo de vulnerabilidades que se deba explotar o se debe incorporar una por parte del oferente?	No se cuenta con solución de escaneo de vulnerabilidad, esto es parte de lo que se debe ofertar.
	Técnica	En caso de que la respuesta anterior sea positiva, por favor indicar el nombre de la solución de escaneo de vulnerabilidades.	No aplica.
	Técnica	¿AVO ya cuenta con una solución de correlación de eventos SIEM que se deba explotar o se debe incorporar una por parte del oferente?	No se cuenta con solución de correlación de eventos SIEM, esto es parte de lo que se debe ofertar.
	Técnica	En caso de que la respuesta anterior sea positiva, por favor indicar el nombre de la solución SIEM.	No aplica.
	Técnica	Para dimensionar los servicios de monitoreo de seguridad necesitamos el detalle de la suma total Eventos por segundos ¿Avo cuenta con esta información?	No.
	Técnica	¿Qué tipos de recursos se desea incluir en el monitoreo de correlación de eventos? Indicar, tipo, marca, modelo y sistema operativo o Firmware.	Sistemas Operativos: Windows y Linux Switches: Cisco y FS Access Point: Meraki Firewall: Fortinet Notebooks: HP, Lenovo, Dell PC: Dell, HP Telefonos: Avaya
	Técnica	En base a la consulta anterior ¿Cuál es la cantidad total de recursos a incluir en el monitoreo de seguridad?	Firewall = 2 Server = 89 Storage = 4 Switch = 30 Unidad de Respaldo = 2 WorkStation = 80
	Técnica	¿En qué modalidad se requiere la atención de requerimientos e incidentes? ¿5x8? ¿7x24?	En el Capitulo 5.5.4 se detalla la modalidad del servicio de Registro de Requerimientos e Incidentes
	Técnica	¿Todos los recursos de seguridad a incluir en el servicio cuentan con licencia y soporte del fabricante?	Si
	Técnica	En caso de que la respuesta sea negativa, por favor indicar cuáles no cuentan con licencia ni el soporte del fabricante.	No aplica.
	Técnica	¿Cuál es la cantidad de incidentes promedio durante los últimos 12 meses?	No se cuenta con esa información, la operación lleva menos de 1 mes.
	Técnica	¿Cuál es la cantidad de requerimientos promedio durante los últimos 12 meses?	No se cuenta con esa información, la operación lleva menos de 1 mes.
	Técnica	Para efectos del punto 6.2.1.1 por favor proveer un diagrama de red con ubicaciones de DC y oficinas a cubrir en el levantamiento inicial.	El data center esta en Av Los Turistas 0300, nivel -1 en los niveles 1 y en edificio contiguo se encuentran las oficinas que deben cubrirse, ademas considerar oficinas ubicadas en Av Ossa 2253.
	Técnica	Para efectos del punto 6.2.1.2 por favor indicar cantidad de servidores y ubicaciones de estos.	89 Servidores entre fisicos y virtuales, todos ubicados en el data center de Av los Turistas 0300 y Av Ossa 2253.

Técnica	Para efectos del punto 6.2.1.4 ¿qué cantidad aproximada de vulnerabilidades están mitigando mensualmente?	No se cuenta con esa información, la operación lleva menos de 1 mes.
Técnica	Para efectos del punto 6.2.1.6 ¿qué cantidad aproximada de servivios web desean incluir en las pruebas de penetración?	Aproximadamente 10 servicios Web, desde redes publicas y privadas.
Técnica	Para efectos del punto 6.2.1.6 ¿qué modalidad de pruebas se espera del servicio White box, black box, grey box?	Deben ser acordadas en conjunto, como referencia para caso de Black Box utilizar casos de usos (Input/Output), para efectos de White Box referenciar el componente APM,etc.
Técnica	Para efectos del punto 6.2.1.6 ¿esto se requiere como un servicio puntual cada cierto tiempo o de forma continua dentro del proceso de desarrollo?	Cada cierto tiempo, en función del despliegue de aplicaciones.
Técnica	Para efectos del punto 6.2.1.7 Por favor indicar si cuentan con un sistema de orquestación de configuración, seguridad y compliance de la red.	No se cuenta con un sistema de orquestación de Configuración, seguridad y compliance de la red.
Técnica	Para efectos del punto 6.2.1.7 Por favor proveer un diagrama de red detallado para dimensionar el servicio.	Firewall = 2 Server = 89 Storage = 4 Switch = 30 Unidad de Respaldo = 2 WorkStation = 80
Técnica	Por favor indicar qué marcas de Firewall posee AVO en la actualidad	2 FortiGate 101F en Stack en modo HA
Técnica	Por favor indicar cantidad de dominios del AD, usuarios y OU.	3 dominios AD, Aprox 80 usuarios y 8 OU
Técnica	¿Se requiere personal in-situ?	No
Técnica	En caso de que la respuesta a la consulta anterior sea positiva, por favor indicar: Cantidad de horas a la semana, modalidad ¿5X8? ¿7x24?	No aplica.
Técnica	5.5 REQUERIMIENTOS GENERALES MÍNIMOS,	No aplica.
Técnica	7 SERVICIOS, 6.3 SERVICIOS DE SOCPara el caso de monitorización de seguridad, nosotros podemos ocupar Sentinel de MSFT/Splunk Cloud, valdría la pena conocer si la Sociedad cuenta con licenciamiento Microsoft y que tipo en específico (E5, A5, P2 EMS5) Favor de especificar, si la respuesta anterior fue afirmativa, cantidad por tipo de licencias	No se cuenta con Licenciamiento Microsoft, las licencias son fisicas tipo OEM.
Técnica	8 SERVICIOS, 6.3 SERVICIOS DE SOC. Favor de especificar su arquitectura actual de AD (debe cubrir si este se encuentra OnPrem, Cloud o Híbrido).	hay tres AD un Principal avo1.cl y dos subdominios its.avo1.cl y bo.avo1.cl, todo OnPrem
Técnica	9 SERVICIOS, 6.3 SERVICIOS DE SOC. Actualmente, ¿Cuenta con un servicio gestionado de seguridad?¿Cuál?	No
Técnica	10 SERVICIOS, 6.3 SERVICIOS DE SOC. Actualmente, ¿Está utilizando un SIEM? ¿Cuál? ¿Cuántos GBPD/EPS esta utilizando?	No
Técnica	11 SERVICIOS, 6.3 SERVICIOS DE SOC. Si la pregunta anterior fue afirmativa, ¿Estarían dispuestos a reemplazarlo?, ó desean que se realice un trabajo en paralelo con la otra solución?	No aplica.
Técnica	12 SERVICIOS, 6.3 SERVICIOS DE SOC. Aunque se habla de un descubrimiento de los activos, aplicaciones, IPs, etc. para el servicio de monitoreo de seguridad se requiere del inventario con detalle de las fuentes a ingestar (cantidad de EndPoints [especificar cantidad por Windows y MacOS si aplica], Servidores [especificar por Windows y Linux si aplica, de igual manera si son onprem o en nube especificando la nube], FWs DMZ y Thrust, IPS/IDS, Switches, Routers, Email Security, etc)	Firewall = 2 Server = 89 Storage = 4 Switch = 30 Unidad de Respaldo = 2 WorkStation = 80
Técnica	13 SERVICIOS, 6.3 SERVICIOS DE SOCDe igual manera necesitamos un inventario de las aplicaciones, software, plataformas a evaluar en el vulnerability assessment. ¿Nos lo pueden proporcionar.	Sistemas Operativos: Windows y Linux Switches: Cisco y FS Access Point: Meraki Firewall: Fortinet Notebooks: HP, Lenovo, Dell PC: Dell, HP Telefonos: Avaya

SERVICIOS DE OPERACIONES DE MONITOREO Y CIBERSEGURIDAD	Técnica	14 SERVICIOS, 6.3 SERVICIOS DE SOC. En el caso de las estaciones de trabajo, ¿cómo las gestiona actualmente (INTUNE, Conf Manager)?	Todavia no se aplica ningun producto de gestión.
	Técnica	15 SERVICIOS, 6.3 SERVICIOS DE SOC¿Qué Antivirus están utilizando?, favor de especificar nombre y nivel de licenciamiento	Antivirus Karspersky.
	Técnica	16 SERVICIOS, 6.3 SERVICIOS DE SOC. El AntiVirus utilizado actualmente, ¿se encuentra totalmente desplegados en puestos de trabajo y Servidores? Favor de brindar detalles.	si, esta desplegado en las estaciones instaladas.
	Técnica	17 SERVICIOS, 6.3 SERVICIOS DE SOC, ¿Estarían dispuestos a reemplazarlo por otro NGAV?	No, esta recien renovado el licnciamiento.
	Técnica	18 SERVICIOS, 6.3 SERVICIOS DE SOC ¿Están buscando Treat Hunting adicional al escaneo de las vulnerabilidades?	seria de interes como un valor agregado aplicarlo como una campaña programada.
	Técnica	19 SERVICIOS, 6.3 SERVICIOS DE SOC, ¿Cuentan con algún requerimiento adicional de las certificaciones como el cumplimiento de un estándar o regulación/auditoría?, favor de especificar con detalle	En capitulo 5.5.1 se indica los requisitos obligatorio y opcionales en cuanto a las certificaciones.
	Técnica	20 SERVICIOS, 6.3 SERVICIOS DE SOC, ¿Cuenta con casos de uso específico a implementar?, Nos podría proporcionar una lista	No se tienen casos de uso.
	Técnica	Actualmente cuentan con alguna solución de correlación de eventos o el proveedor deberá proveer una?	No, es parte de la oferta que se debe realizar.
	Técnica	Dentro de las responsabilidades del Responsable de Operación, El proveedor deberá tomar acciones correctivas sobre la plataforma monitoreada?	Si, en caso de ser de riesgo inmediato para la continuidad operacional, de lo contrario se debera proponer las acciones para ser evaluadas por los proveedores de los sistemas impactados.
	Técnica	Dentro de las responsabilidades del Consultor Sistemas y Ciberseguridad, este deberá tener los accesos a los sistemas monitoreados para su revisión, o esto será realizado por el cliente, y solo se tendrán responsabilidades de supervisión?	sera actividades compartidas en equipo.
	Técnica	Favor entregar información de componentes de la plataforma TI, seguridad y comunicaciones, diagrama de red que incluya lo anterior y los activos internos.	Sistemas Operativos: Windows y Linux Switches: Cisco y FS Access Point: Meraki Firewall: Fortinet Notebooks: HP, Lenovo, Dell PC: Dell, HP Telefonos: Avaya
	Técnica	Indicar cantidad de URLs externas	Aproximadamente 10 URL, desde redes publicas y privadas.
	Técnica	Cantidad de EPS	No se cuenta con esa información, la operación lleva menos de 1 mes.
	Técnica	¿A qué cantidad de usuarios se desea realizar las pruebas de phishing'	Se debe acordar una muestra representativa de al menos el 20% en cada proceso.
	Técnica	Cantidad de Servidores Críticos	32 Servers
	Técnica	¿Qué solución de antivirus poseen actualmente, para cuántos usuarios y si ésta cuenta con una herramienta de administración centralizada y si ella es Cloud u onpremise?	Antivirus Karspersky.
	Técnica	Proyección de crecimiento en cuanto a usuarios y equipamiento anual.	Aprox 5%
	Técnica	Favor describir si cuentan con plataforma de virtualización y sus características	Si, es sobre la solución Vmware.
	Técnica	Favor indicar si cuentan con la disponibilidad de desplegar un colector de eventos con al menos 16GB de Ram en su infraestructura.	No, se espera un servicio llave en mano.
	Técnica	Favor especificar el medio y donde se deben entregar los documentos, es decir, propuestas y boleta, ya que en las bases dan una información y la página indica otra.	La fecha límite para la entrega de las propuestas será el día 5 de septiembre de 2022. Las propuestas deben entregarse antes de las 18:00 horas en la oficina de la Sociedad Concesionaria ubicada en Avenida Américo Vespucio Sur N°100, piso 16, Comuna de Las Condes, Ciudad de Santiago.
	Técnica	Favor si pueden disponibilizar los anexos en formato editable.	Se disponibilizaran los anexo en formato editable
	Técnica	Respecto a las certificaciones indicadas como obligatorias 27001, y 9000, en el caso de la segunda, si estuviera en proceso, la propuesta sería aceptada?	En capitulo 5.5.1 se indica los requisitos obligatorio y opcionales en cuanto a las certificaciones.

Técnica	No se ve dentro de la documentación en su sitio que se incluya la información de la actual infraestructura a cubrir, cantidad de usuarios, para hacer dimensionamiento, se puede enviar?	Esto se disponibilizara como parte del proceso de habilitación. En grandes numeros el detalle de los usuario y dispositivo de la red son: Sistemas Operativos: Windows y Linux Switches: Cisco y FS Access Point: Meraki Firewall: Fortinet Notebooks: HP, Lenovo, Dell PC: Dell, HP Telefonos: Avaya Firewall = 2 Server = 89 Storage = 4 Switch = 30 Unidad de Respaldo = 2 WorkStation = 80 Telefonos= 80
Técnica	Según indicacion en su propuesta, dice que los servicios deben ser cotizados sin IVA, sin embargo se conoce que habrán algunos cambios tributarios a partir del 01/01/2023. ¿Se puede indicar en la propuesta una nota que haga referencia al respecto? Y/o se puede revisar este punto con su equipo financiero a su debido momento.	Si
Técnica	¿Cuáles son los SLA asociados a tiempos de respuesta una vez levantado un ticket por AVO hacia nuestra mesa de ayuda?	Deberan ser acordados como parte del proyecto de implementación del servicio.
Técnica	Dentro del servicio solicitado, se espera tiempos de solución de los componentes bajo contrato? ¿Si es así, se exige un SLA de solución o los debe proponer la empresa adjudicada?	Deberan ser acordados como parte del proyecto de implementación del servicio.
Técnica	Cuantos, que marca, donde se encuentran los equipos y que sistema operativo/versión de software base tienen los equipos que estarán bajo contrato?	Sistemas Operativos: Windows y Linux Switches: Cisco y FS Access Point: Meraki Firewall: Fortinet Notebooks: HP, Lenovo, Dell PC: Dell, HP Telefonos: Avaya Firewall = 2 Server = 89 Storage = 4 Switch = 30 Unidad de Respaldo = 2 WorkStation = 80 Telefonos= 80
Técnica	Para la disponibilidad de la página web, ¿se debe incluir ingenieros de sistema/networking e infraestructura en general o solamente se debe considerar el servicio de medición de tiempo de disponibilidad del sitio?	en capitulo 6.2.1.6 se indica los requisitos de Analisis de los entornos webs y en capítulo 6.3 los servicios de SOC asociado a la infraestructura de TI relacionada a la prestación de los servicios.
Técnica	Para el punto 6.2.3 de Auditoria del AD, solamente se espera un informe de recomendaciones o el servicio contratado espera también la ejecución de dichas recomendaciones?	Referirse a lo que se indica en el capítulo 6.2.3
Técnica	Para el punto 6.3.1.8 de Gestión de incidentes de seguridad, solamente se espera un informe de recomendaciones y revisiones o el servicio contratado espera también la ejecución de las actividades sugeridas?	Referirse a lo que se indica en el capítulo 6.3.1.8

Técnica	Para la conectividad hacia cada uno de los componentes, ¿qué servicio de conectividad facilitará el cliente? (VPN, enlace directo)	Las conexiones se realizaran a traves de VPN
Técnica	Para el punto 6.3.2 "Definición y ejecución de políticas de exploraciones manuales periódicas en grupos de equipos.", AVO considera que se deberá tener acceso a cada uno de los equipos de trabajo y servidores?Si es así, AVO facilitará el software para dicha conexión (Ej. teamviewer, VPN, ¿conexión directa)?	Las conexiones se realizaran a traves de VPN
Técnica	Se debe usar el sistema propio de AVO, SIC-NS, ¿para la ejecución del servicio? ¿Si es así, AVO contempla una capacitación a la empresa adjudicada sobre el uso de esta herramienta?	No, el sistema SIC-NS es de uso interno de AVO y solo debe ser parte del monitoreo.
Técnica	Se debe incorporar en la oferta, la ejecución de las actualizaciones preventivas en cada uno de los equipos bajo el servicio NOC/SOC?	Solo a modo de sugerencia, las actualizaciones las gestionara AVO con quien mantiene los sistemas.
Técnica	Favor, entregar más antecedentes del sistema SIC-NS, ¿debe estar bajo la administración del contrato o este sistema lo tendrá AVO directamente y se debe medir solamente su disponibilidad?	Lo tiene AVO y solo se debe monitorear y medir la disponibilidad
Técnica	A qué se refiere el sistema SIC-NS?, no se entiende el ROL dentro de la licitación. Favor, aclarar	Es el Sistema Informatico de Control del Nivel de Servicio y debe ser monitoreado como cualquier sistema web. Ademas de integrarse para registrar el resultado de su disponibilidad.
Técnica	Favor, necesitamos los siguientes datos para poder dimensionar el servicio: a) Lista de servidores (fisico/virtuales) - Marca - Sistema operativo - Nivel de parches b) Lista de equipos de comunicaciones (fisico/virtuales) - Marca - Sistema operativo- Nivel de parches c) Lista de equipos de seguridad (fisico/virtuales) - Marca - Sistema operativo- Nivel de parches d) Lista de End Point (fisico/virtuales) - Marca - Sistema operativo- Nivel de parches e) Lista de dipositivos móviles (fisico/virtuales) - Marca - Sistema operativo- Nivel de parches f) Antivirus instalados en los equipos y versión del mismo	Sistemas Operativos: Windows y Linux Switches: Cisco y FS Access Point: Meraki Firewall: Fortinet Notebooks: HP, Lenovo, Dell PC: Dell, HP Telefonos: Avaya Firewall = 2 Server = 89 Storage = 4 Switch = 30 Unidad de Respaldo = 2 WorkStation = 80 Telefonos= 80
Técnica	AVO espera que se propongan equipos de seguridad que ayuden a fortalecer el servicio NOC/SOC?	Si
Técnica	la lista de KPI los facilitará el cliente o los debe proponer el proveedor?	Se trabajaran en Conjunto
Técnica	¿Hay algún inconveniente que el servicio SOC/NOC se entregue por personal que esté ubicado fuera de Chile?	No
Técnica	Para el punto 7.4.1, se indica que el SLA de la página web debe ser de 99,5%...para esto, AVO espera que se el proveedor administre la infraestructura donde estará alojada la página web o solamente, el rol del servicio será informar el SLA que tendrá el sitio?	Monitoreo e informar el SLA acompañando la evidencia.
Técnica	Nuestra compañía está en proceso de certificación ISO 27001 e ISO 9001...Se puede adjuntar este certificado?	Si
Técnica	En el punto 5.2.2, las eventuales interrupciones no planificadas podrían no ser imputables al servicio propuesto (Ej. caída de equipos de comunicaciones de AVO)... ¿En este caso, se entenderá que es responsabilidad del proveedor actual de AVO y no nuestra?	Si
Técnica	En el punto 5.5.3, ¿cuál es el alcance, plan y sobre qué productos se espera que se realice la capacitación?	Sobre las herramientas utilizadas en el servicio.
Técnica	Por acuerdos confidenciales con nuestros clientes, no podemos facilitar información detallada sobre nuestros proyectos, no obstante, sí podemos entregar información de las empresas. En caso de ser adjudicado, podremos entregar información más detallada... ¿Esto es viable para AVO?	Si

	Técnica	Para el punto de "Experiencia", ¿AVO tomará en cuenta solamente la experiencia en el rubro de "Concesiones" o se puede considerar cualquier rubro?	Se refiere a experiencia en el Rubro de la Ciberseguridad
	Técnica	Los SLA de los componentes que estarán dentro del servicio NOC/SOC, ¿los deberá proponer el proveedor adjudicado, AVO o se desarrollarán en conjunto?	Se desarrollaran en conjunto.
	Técnica	en el punto 6.2.1.1. Análisis de la red, AVO espera que se realice un levantamiento de todos los equipos que estarán bajo el servicio NOC/SOC?	Si
	Técnica	En virtud de la complejidad del servicio solicitado, ¿es posible extender la entrega del plazo de la propuesta?	No
	Técnica	¿Según lo expresado se seguirán los SLA que nosotros entreguemos por apartado?	seran acordados en conjunto durante el proceso de implementación del servicio.
	Técnica	¿Cuantos usuarios internos hay que monitorear en la red?	al menos 100 usuarios
	Técnica	¿Cuantos dispositivos hay externos a la red que hay que monitorear y se conectan fueras de las dependencias?	pueden llegar a ser al menos 100 dispositivos.
	Técnica	¿Que dispositivos y sistema operativo tienen en actualmente en la red?	Dispositivos: Switches, Firewall, Notebooks, PC, Telefonos, Access Point Sistemas Operativos: Windows y Linux
	Técnica	¿Cuáles son sus dispositivos endpoint y Sistema operativo y marca (Switches, routers , firewalls , notebooks , pc, teléfonos (sistema operativo)?	Sistemas Operativos: Windows y Linux Switches: Cisco y FS Access Point: Meraki Firewall: Fortinet Notebooks: HP, Lenovo, Dell PC: Dell, HP Telefonos: Avaya
	Técnica	¿Tienen integración hibrida ? (equipos Onsite y cloud)	Si
	Técnica	¿Tienen Active Directory?	Si
	Técnica	¿Qué sistema de Correo tiene?	Office 365
	Técnica	¿Tienen alguna restricción para dar acceso por VPN para el monitoreo Proactivo? O tiene que ser por máquina virtual.	Las conexiones se realizaran a traves de VPN
	Técnica	¿Qué pasaría si tengo solamente algunas certificaciones en Tramites?	En capitulo 5.5.1 se indica los requisitos obligatorio y opcionales en cuanto a las certificaciones.