	Sociedad Concesionaria Vespucio Oriente S.A.
	Términos de Referencia para la Licitación Pública de los Servicios de Operaciones de Monitoreo y Ciberseguridad **Versión C**
Nombre Proyecto:	***Servicios de Operaciones de Monitoreo y Ciberseguridad***
Fecha Autorización:	
Fecha Inicio:	
Fecha Termino:	

versiones

ver	autores	aprobador	fecha	observaciones
1	Alvaro Urbina			

distribución

destinatario	contacto	e-mail

información

archivo: RFP Servicios de Operaciones de Monitoreo y Ciberseguridad

páginas 39 **estado:** Borrador

Tabla de contenido

1. DESCRIPCIÓN DEL CLIENTE

La **Sociedad Concesionaria Vespucio Oriente S.A**, surge de su constitución por las empresas ALEATICA S.A.U. (ex OHL Concesiones S.A.) junto con SACYR Concesiones Chile SpA (ex Sacyr Concesiones Chile S.A.), con el fin de dar ejecución al contrato de concesión de la obra pública fiscal denominada “Concesión Américo Vespucio Oriente, Tramo Av. El Salto - Príncipe de Gales”.

La concesión Américo Vespucio Oriente se extenderá 9,1 kilómetros, desde Avda. El Salto hasta el sector de Av. Príncipe de Gales. El proyecto se inserta en el programa de mejoramiento del Sistema de Transporte Urbano de Santiago que impulsa el Gobierno de Chile, a través del Ministerio de Obras Públicas.

El proyecto tiene prevista su puesta en servicio en junio de 2022 y consta de dos sectores: el Sector 1, que va desde Avda. El Salto a Puente Centenario, y el Sector 2, que va desde el Puente Centenario hasta Avda. Príncipe de Gales.

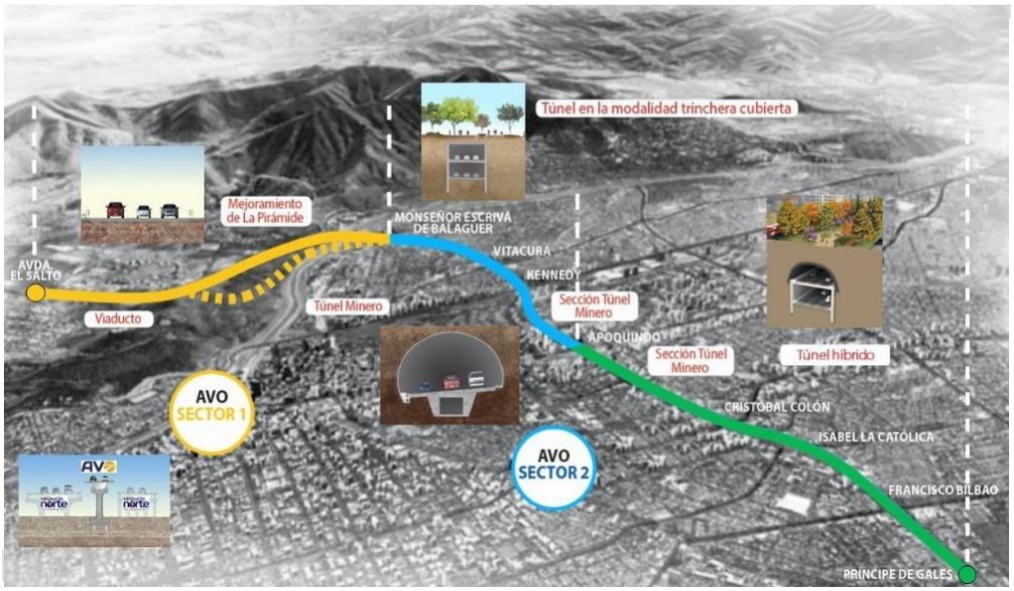

Ilustración 1. Tramos AVO.

El Sistema de Cobro está formado a nivel de campo por diferentes Puntos de Cobro, distribuidos a lo largo de la autopista de modo que se permita la captura de todos los vehículos de los usuarios, tanto en el ingreso como en el egreso de los diferentes sectores. Por otro lado, el entorno de nivel central, hacia el que confluyen todas las transacciones generadas en los Puntos de Cobro para su análisis y validación, estará formado por el Centro de Operaciones de Peaje (COP) el cual centraliza la información de los pasos de vehículos, generando viajes y enviando estos viajes al nivel de gestión compuesto por el Centro de Atención de Clientes (CAC) el cual se encargará del proceso de facturación, recaudación y cobro del peaje, en conjunto con los servicios de la Plataforma de Atención a Clientes en general. Complementando lo anterior, se dispone de un Portal Web de Servicio de Atención a los Usuarios que permite la atención virtual de los clientes.

En tal sentido, el Concesionario, como parte clave de la gestión de su plataforma tecnológica y adicionalmente dando cumplimiento al Art. 2.4.5.3.1 letra f) de las Bases de Licitación, ha iniciado un proceso de licitación y contratación de un Proveedor para Servicios de Operaciones de Monitoreo y Ciberseguridad, incluido el Sistema SIC-NS, en adelante los "Servicios", con el objetivo de incrementar la capacidad de monitoreo de disponibilidad, vigilancia y detección de amenazas en las actividades diarias de los sistemas de información y comunicaciones.

2. ABREVIACIONES

Término	Descripción
AVO	Autopista Vespucio Oriente
SCAVO	Sociedad Concesionaria Vespucio Oriente S.A.
COP	Centro de Operación de Peaje
CAC	Centro de Atención de Clientes
ISO	International Organization for Standardization.
ITIL	Information Technology Infrastructure Library.
MOP	Ministerio de Obras Públicas
TDR	Términos de Referencia
SIC-NS	Sistema Informático para la Constatación de Niveles de Servicio.
QA	Acrónimo del inglés “Quality Assurance”, relacionado a los ambientes de calidad para realización de pruebas.

3. GLOSARIO

Concepto	Descripción
BALI	Bases de Licitación de la "Concesión Américo Vespucio Oriente, Tramo Av. El Salto - Príncipe de Gales".
Centro de Operación de Peaje	Conocido con la abreviatura COP, es el sistema informático que rescata del punto de cobro la información básica para establecer los viajes realizados por la autopista y tarificarlos.
Centro de Atención a Clientes	Conocido con la abreviatura CAC, es el sistema informático que procesa los viajes enviados por el COP para su posterior gestión comercial, desde la facturación hasta su recaudación. Este sistema se integra con varios otros sistemas externos de AVO que complementan las labores comerciales, como, por ejemplo, empresas externas de recaudación y cobranzas, empresas de envíos de mailing, impresores físicos, empresas de correos.
Punto de Cobro	Lugar físico en la autopista donde existe infraestructura tecnológica que permite la captura de un tránsito para el cobro del peaje (pórtico de peaje).

4. ANTECEDENTES PARA EL SERVICIO

4.1. Alcance.

El presente documento, denominado **Términos de Referencia Técnica** detalla los requerimientos que **la Concesionaria** plantea a los oferentes, para que éstos presenten sus propuestas de un Servicio de Operaciones de Monitoreo y Ciberseguridad, incluido el Sistema SIC-NS que permita disponer de una adecuada operación y seguridad de las plataformas tecnológicas de la Concesionaria, lo que da adicionalmente cumplimiento a lo requerido en el Articulo 2.4.5.3.1 (Estándares del Servicio de Atención de Usuarios) letra f) de las BALI y Artículo 2.2.1 del Anexo N° 4 de las BALI.

4.2. Objetivo Principal

Disponer de un Servicio de Operaciones de Monitoreo y Ciberseguridad incluido el Sistema SIC-NS desde el cual se realicen todas las actividades encaminadas a garantizar la disponibilidad y seguridad de las infraestructuras y servicios. Para ello, el Servicio de Operaciones de Monitoreo y Ciberseguridad, incluido el Sistema SIC-NS, deberá contar con la información más actualizada sobre las vulnerabilidades de seguridad y las últimas tendencias en ciberataques. Los servicios ofrecidos en modalidad 24x7 engloban los relacionados con el monitoreo de las plataformas, operación y gestión técnica de la seguridad, incluyendo la ejecución de todas las actuaciones preventivas, respuesta ante incidentes, identificación de puntos de mejora en la seguridad de la información, análisis y evaluación de riesgos para ofrecer la mejor respuesta ante posibles amenazas, todo lo anterior, a través de un registro automático y en tiempo real de la disponibilidad y los tiempos de interacción.

4.3. Objetivos Secundarios

Establecer SLA por cada uno de los servicios asociados a la disponibilidad y del servicio de monitoreo de la infraestructura y plataformas y los tiempos de interacción.

Establecer claramente las responsabilidades asociadas al **Proveedor** respecto del servicio entregado.

Establecer Servicios de Soporte o Comunicación que estén de acuerdo a las necesidades de **la Concesionaria y/o del MOP**.

Establecer formalmente los flujos de interacción entre el **Proveedor** seleccionado y **la Concesionaria** para brindar el servicio licitado.

Contar con mecanismos de control que permitan tener la certeza del correcto cumplimiento por parte del Proveedor en relación al monitoreo de la infraestructura y de las plataformas, con especial énfasis en aspectos de seguridad de la información.

Sobre la metodología de trabajo: El oferente deberá poner en conocimiento de **la Concesionaria**, previo al comienzo de la contratación del servicio, sobre su metodología de trabajo, experiencia en el rubro y organización, tanto para la fase de implementación como de operación del servicio.

4.4. Entrega y contenido de las Ofertas

Los Oferentes deberán presentar sus ofertas vía correo electrónico, en la forma definida a continuación.

La OFERTA COMPLETA se compone de 4 carpetas comprimidas más 1 (un) sobre con la Boleta de Garantía de Seriedad de la Oferta.

Carpeta Comprimida N°1: Antecedentes Generales, Legales y Financieros.
Carpeta Comprimida N°2: Oferta Técnica.
Carpeta Comprimida N°3: Oferta Económica.
Carpeta Comprimida N°4: Boleta de Garantía de Seriedad de la Oferta en PDF.
Sobre: Boleta de Garantía de Seriedad de la Oferta (original).

El sobre con la Boleta de Garantía debe venir debidamente identificado y deberá agregarse el siguiente texto:

SOCIEDAD CONCESIONARIA VESPUCIO ORIENTE S.A.
GERENCIA COMERCIAL
AV. AMERICO VESPUCIO SUR N°100, PISO 16
“DOCUMENTACION CONFIDENCIAL”
PARA: ALVARO URBINA C.
EMPRESA: [***]

En el remitente se debe especificar, el nombre y domicilio del Oferente.

Los documentos entregados en formato papel, estarán todos en tamaño DIN A4 a doble cara y perfectamente legibles, estando a color si el oferente así lo estima. Estarán encuadernados de manera sencilla, usando índices y separadores.

Los sobres deben ser presentados de la siguiente forma:

Sobres	Presentación
Carpeta Comprimida N°1: Antecedentes Generales, Legales y Financieros.	En formato PDF los antecedentes generales, legales y declaraciones firmadas. En formato Excel y PDF los antecedentes financieros del Oferente.
Carpeta Comprimida N°2: Oferta Técnica.	En formato PDF y Excel para los datos numéricos.
Carpeta Comprimida N°3: Oferta Económica.	En formato PDF y Excel para los datos numéricos.
Carpeta Comprimida N°4: Boleta de Garantía de Seriedad de la Oferta.	En formato PDF.

Sobre N°1: Boleta de Garantía de Seriedad de la Oferta.	Documento Original extendido como se indica en las Bases de Licitación.

En la medida que los sobres, antes individualizados, no contengan toda la documentación solicitada, o ella se entregue con formatos distintos a los solicitados o con enmiendas o ralladuras, estos se entenderán como no presentados y en consecuencia se entenderá que los antecedentes son incompletos, desechándose la Oferta presentada.

4.4.1. Documentos que deben incluirse en la Carpeta Comprimida N°1

Antecedentes Generales, Legales y Financieros

Se deberán acompañar los antecedentes individualizados en el Anexo N°5.

4.4.2. Documentos que se deben incluir en el Carpeta Comprimida N°2

Oferta Técnica

A ser incluida por el Oferente en esta carpeta.

4.4.3. Documentos que se deben incluir en el Carpeta Comprimida N°3

Oferta Económica

La oferta económica se entregará según se especifica en el Anexo N°6.

4.4.4. Documentos que deben incluirse en el Carpeta Comprimida N°4

Boleta de Garantía Bancaria de Seriedad de la Oferta

La Boleta de Garantía de Seriedad de la Oferta en formato PDF.

4.4.5. Documentos que se deben incluir en el Sobre N°1

Boleta de Garantía Bancaria de Seriedad de la Oferta.

Los Oferentes deberán incluir una boleta emitida a la vista, irrevocable de cobro unilateral a su sola presentación para garantizar la seriedad de sus ofertas. Dicha boleta de garantía deberá cumplir además con las siguientes características:

- Emitida en Santiago de Chile por un Banco con oficina en Santiago.
- Las Boletas serán pagaderas a la vista.
- El monto total de la boleta de garantía será de UF 200.
- El tomador debe ser el Proponente.
- La boleta de garantía debe ser tomada a la orden de Sociedad Concesionaria Vespucio Oriente S.A., RUT 76.376.061-8.
- La glosa de dicha boleta será: “Para garantizar la seriedad de la oferta de la licitación, “Servicios de Operaciones de Monitoreo y Ciberseguridad” y firma del contrato en los plazos estipulados”.
- El plazo de vigencia de la boleta de garantía será de 4 meses contados desde la presentación de la Oferta.
- El Adjudicatario deberá mantener siempre vigente la garantía de seriedad de la Oferta hasta que sea sustituida por la Garantía de Fiel Cumplimiento del Contrato a entera satisfacción de AVO.

En caso que se extiendan los plazos de la licitación, dicha boleta deberá ser renovada en los mismos términos antes descritos, y con vigencia hasta la nueva fecha que AVO señale.

AVO podrá hacer efectiva esta garantía sin derecho a reclamo alguno en los siguientes casos:

1. Si los antecedentes entregados en la oferta hubiesen sido alterados o hubiesen inducido a AVO a error en la adjudicación de la licitación.

2. Si el Oferente se desiste de su oferta, o no suscribe el Contrato, en caso de serle adjudicado en el plazo establecido para su firma, o no presenta oportunamente la boleta de garantía de fiel cumplimiento del Contrato.

La Boleta de Garantía de Seriedad de la oferta será devuelta a los Oferentes no favorecidos, dentro de los 30 días posteriores a su notificación de la suscripción del contrato por parte del Adjudicatario. Será obligación de los Oferentes retirar esa garantía dentro del plazo establecido.

5. DESCRIPCIÓN DE LA SOLUCIÓN REQUERIDA

5.1. Descripción General.

Se requiere implementar un Servicio de Operaciones de Monitoreo y Ciberseguridad, incluido el Sistema SIC-NS, para la infraestructura y plataformas de **la Concesionaria**, de forma tal que se garantice una operación segura y de alta disponibilidad.

5.2. Modalidad de Servicio

La modalidad del servicio será de monitoreo remoto 24x7 con sesiones de seguimiento e informes periódicos y se citará expresamente al Proveedor cuando sea necesaria su asistencia a las oficinas.

El **Proveedor** debe considerar en la arquitectura de su solución todos los requisitos de comunicación y seguridad para permitir el monitoreo de las plataformas, con los sistemas y redes de **la Concesionaria** (internos y externos), los sistemas pueden ser transaccionales, de registros de auditoría y niveles de servicio, de estados financieros y de inteligencia de negocios según corresponda a lo que tenga implementado **la Concesionaria**.

5.3. Duración del Servicio

El servicio de monitoreo será contratado por un periodo inicial de 2 años con renovaciones automáticas por periodos anuales sujeto a que el Concesionario y el Inspector Fiscal no manifiesten opinión en contrario con una anticipación mayor a 6 meses de la fecha de término o renovación aplicables.

5.4. Definición de Roles del Servicio

A continuación, se describen los roles tanto de **la Concesionaria**, como del **Proveedor** que participarán en la provisión del servicio.

La Concesionaria será responsable de:

Administrador de Contrato

- Encargado del cumplimiento de los servicios contenidos en el contrato.
- Analiza el cumplimiento de los SLA.
- Determina la aplicación de multas, en caso de producirse los eventos definidos para ello.
- Establece las condiciones comerciales de los servicios.

Soporte de Operación

- Gestiona el cumplimiento de la continuidad operacional.
- Mide y controla en forma interna el cumplimiento de SLA.
- Levanta tickets operacionales al Soporte del **Proveedor**.
- Coordina soluciones a las incidencias levantadas.
- Genera informes uptime de los Servicios.

Dado que **la Concesionaria** se encuentra en fase de implementación de sus sistemas de redes y aplicaciones, será sólo el rol de Administrador del Contrato el cual se encontrará operativo en esta fase, dejando los demás roles declarados para la fase de inicio de operaciones y explotación de la concesión.

Proveedor adjudicado será responsable de:

Gerente de Operaciones.

- Gestiona la solución de incidencias, escaladas de acuerdo a procedimiento.
- Gestiona la entrega del servicio de acuerdo a los estándares definidos en el contrato y sus documentos integrantes.
- Gestiona nuevas solicitudes, reclamos y cualquier otra actividad que no pueda ser resuelta por los operadores de soporte.

Responsable de Operación.

- Administra la Mesa de Soporte, gestión de incidentes y seguimiento de soluciones.
- Responde a consultas de operación.
- Mantiene la continuidad operacional del servicio.
- Gestiona incidentes que requieren escalamiento.
- Genera reporte de solución en caso de fallas.
- Genera informes periódicos de operación.

Consultor Sistemas y Ciberseguridad.

- Responde a consultas de **la Concesionaria** generadas en la operación de la plataforma.
- Revisa el estado de la plataforma, analiza casos reportados y detecta posibles problemas.
- Propone mejoras proactivas del servicio.
- Identifica, evalúa y gestiona en forma anticipada las soluciones a las brechas de seguridad detectadas.
- Apoya en la confección de informes de operación.

5.5. REQUERIMIENTOS GENERALES MÍNIMOS.

5.5.1. Certificaciones del Oferente.

Los Oferentes deben proporcionar información que permita a la Concesionaria asegurar que están capacitados para implementar el servicio requerido, soportar la implementación desde la situación existente y cumplir con los requerimientos de continuidad operacional del servicio, durante el periodo de vigencia del contrato.

Se solicita como requisito obligatorio que los oferentes cuenten a lo menos con las siguientes certificaciones vigentes:

- Certificación de Sistema de Gestión de la Seguridad de la Información (ISO 27001).
- Certificaciones de Calidad (ISO 9001).

Siendo además deseable la:

- Certificación de Sistema de Gestión de la Servicios de Tecnologías de la Información (ISO 20000).
- Certificaciones de Medioambiente (ISO 14001).

Asimismo, y como un indicador más de las capacidades de la compañía en el ámbito de la Ciberseguridad, es deseable que el Oferente acredite ser miembro de las principales organizaciones relacionadas con la seguridad informática y respuesta ante incidentes de seguridad, por ejemplo:

- FIRST: Forum of Incident Response and Security Teams.
- CSIRT: Equipos de Ciberseguridad y Gestión de Incidentes.

5.5.2. Soporte y Niveles de Servicios

Las soluciones tecnológicas propuestas deberán funcionar en base a estándares que deberán ser definidos en común acuerdo para cada uno de los servicios requeridos.

A su vez, cualquier interrupción justificada y programada del servicio, por ejemplo, por mantenimiento, deberá ser informada a **la Concesionaria** con al menos una semana de anticipación y autorizada por **la Concesionaria** para su ejecución. Dichas interrupciones programadas del servicio deberán ser efectuadas en horario de baja demanda correspondiente al período comprendido entre las 00:00 hrs. y las 08:00 hrs. del día Domingo, sin superar un máximo de 3 horas de indisponibilidad del Servicio de Operaciones de Monitoreo y Ciberseguridad.

Del mismo modo, las eventuales interrupciones no planificadas, tampoco podrán superar 3 horas continuas sin Servicio de Operaciones de Monitoreo y Ciberseguridad. Por lo tanto, los oferentes deberán incorporar en su solución todas las medidas de contingencia orientadas a satisfacer estos requerimientos.

Con la finalidad de velar por el correcto funcionamiento de los servicios contratados, el **Proveedor** adjudicado deberá informar mensualmente el grado de cumplimiento de

los niveles de disponibilidad del servicio y de los estándares exigidos. Sin perjuicio de la facultad de **la Concesionaria** de requerir en cualquier momento información respecto de las prestaciones estipuladas en el Contrato.

Para ello el sistema deberá contar con medios electrónicos y automáticos de monitoreo y registro en tiempo real de la disponibilidad y los tiempos de interacción, que permitirá recabar estadísticas del comportamiento de los niveles de servicio y estándares exigidos.

5.5.3. Capacitación

Junto con la propuesta, los oferentes deberán presentar y posteriormente ejecutar un plan de capacitación que incorpore al personal interno responsable de la administración TI. Dicho plan deberá además establecer la forma en que se realizará cada actividad (presencial o remota) de capacitación, así como su duración, relatores, tutores, etc.

5.5.4. Soporte

El **Proveedor** deberá contar con al menos una mesa de ayuda que le permita registrar tickets y realizar el seguimiento de ellos, en horario de 08:30 a 18:30:00 horas en días hábiles de lunes a viernes. El servicio de Monitoreo debe ser realizado en modalidad 24x7.

El Proveedor deberá disponer de números telefónicos (fijo y móvil), nombre y correo del encargado del soporte (primer contacto), números telefónicos (fijo y móvil), nombre y correo del Jefe de Servicio (escalamiento). Ver ANEXO N° 1: ESCALAMIENTO DEL SERVICIO DE SOPORTE.

Las solicitudes pueden provenir de cualquiera de los usuarios encargados del sistema.

5.5.5. Plazos a Cumplir en el Proyecto de Setup Inicial.

Junto con la propuesta, los oferentes deberán presentar la planificación detallada de su proyecto, considerando el tiempo y esfuerzo necesario para la implementación del servicio correspondiente, así como el tiempo y esfuerzo asociados a cualquier otra actividad que consideren relevante y necesaria para el éxito del proyecto. Todo lo cual deberá ser presentado en una Carta Gantt con el detalle de cada actividad.

5.5.6. Experiencia en Servicios Similares.

Los oferentes deberán contar con experiencia en el rubro, mínima y comprobable, de al menos 5 años entregando servicios o implementando soluciones similares, la cual deberá acreditarse mediante la entrega de una carpeta por cada uno de sus proyectos anteriores, adjuntando en cada caso información del cliente, URL, breve descripción del trabajo desarrollado y tecnología utilizada.

5.5.7. Equipo de Proyecto.

Los profesionales que formarán parte del equipo del proyecto por parte de los Oferentes, deberán contar con experiencias similares, mínimas y comprobables, de al menos 3 años en las funciones que desarrollarán en el marco de la presente licitación, lo que deberá ser acreditado a su vez mediante la entrega de tantas fichas como profesionales formen parte del equipo de trabajo propuesto para el proyecto. Se deberá especificar en cada caso el rol desempeñado, así como las capacidades y calificaciones del profesional en relación con el rol y las actividades que desempeñará.

5.5.8. Gestión de Calidad.

Junto con la propuesta, los oferentes deberán presentar, y posteriormente, el **Proveedor** adjudicado ejecutar, un plan de gestión de calidad que considere al menos las metodologías que utilizará para administrar la gestión de requerimientos durante el desarrollo del proyecto y en la fase de operación. A su vez, deberá presentar los elementos que la metodología a utilizar ofrece para facilitar la auditoría de la ejecución del plan de calidad por parte de terceros. **La Concesionaria** podrá acceder en cualquier momento a dicha información de auditoría.

5.5.9. Aseguramiento de Calidad.

Junto con la propuesta, los oferentes deberán presentar, y posteriormente el adjudicado ejecutar, un plan de pruebas para la totalidad de los elementos asociados al proyecto, que considere al menos la existencia de un equipo de certificación.

Una vez finalizada conforme la implementación de la solución, y previo a su puesta en marcha, se procederá a certificar si la misma cumple con el plan de pruebas presentado por el adjudicado. Sin perjuicio de dicho plan, se deberá considerar y ejecutar como necesarias las siguientes:

- Pruebas de interfaces utilizadas en monitoreo.
- Pruebas de operación.
- Pruebas de seguridad.

Las adecuaciones de hardware, software base y configuraciones que sean realizadas en forma posterior al inicio de la operación de la solución propuesta, deberán pasar por el mismo proceso de certificación, para lo cual el **Proveedor** asignado deberá aplicar la metodología de certificación en cada cambio.

5.5.10. Gestión de Riesgos.

Junto con la propuesta, los oferentes y posteriormente el adjudicado deberá demostrar que cuenta con un plan de riesgos y los planes de contingencia necesarios. Asimismo, deberá facilitar las eventuales auditorías a ambos planes por parte de terceros.

6. DESCRIPCIÓN DE SERVICIOS

La oferta de servicio debe considerar al menos las siguientes actividades:

1. Monitoreo de disponibilidad de plataformas y equipos.
2. Diagnóstico de Control de Seguridad Semestral.
3. Diagnóstico de Control del Estado de Sistemas y Comunicaciones Anual.
4. Auditoría de Software Anual.
5. Servicios de SOC.
   - Seguridad de red e infraestructuras.
   - Seguridad del puesto de trabajo.
   - Reporting.
   - Gestión del proyecto.

6.1. Monitoreo de disponibilidad de plataformas

Se requiere realizar monitoreos permanentes de disponibilidad (uptime en minutos) de los servidores asociados a las plataformas de la Concesionaria, en especial se deberá monitorear la disponibilidad de la página web corporativa (ver anexo 7.4.1) y del sistema SIC-NS (ver anexo 7.4.2). Estas mediciones se deberán alertar inmediatamente si se encuentran bajo un umbral definido y consolidar mensualmente como reporte en el formato que la Concesionaria defina para integrar automáticamente dicha información en el Sistema Informático para la Constatación del Nivel de Servicio (SIC-NS) de la Concesionaria.

6.2. Diagnóstico de Control de Seguridad.

Se requiere realizar diagnósticos de control de sistemas de información periódicos, con el fin de estudiar el estado general de las infraestructuras, detectar las debilidades y proponer un plan de acción para corregirlas que sirva como apoyo a la correcta gestión de la seguridad de cada una de las redes. La periodicidad mínima requerida es la siguiente:

- Diagnóstico de seguridad: Semestral
- Diagnóstico del estado de sistemas y comunicaciones: Anual
- Auditoria de AD: Anual
- Auditoría de software instalado: Anual

6.2.1. Diagnóstico de Seguridad.

Se requiere realizar diagnósticos sobre las aplicaciones con el objetivo de detectar el máximo número de vulnerabilidades y analizar su posible explotación, adoptando el personal técnico el mismo papel que desempeñaría un eventual hacker para descubrir y explotar vulnerabilidades.

Cada diagnóstico se deberá ejecutar en fases diferenciadas. Una, correspondiente a la fase externa, desde las instalaciones del Proveedor simulando la actividad de un usuario externo. La segunda, correspondiente a la fase interna, desde una red conectada a **la Concesionaria** simulando la actividad de un usuario interno sin permisos de acceso, solo con una conexión a la red interna.

Se debe llegar a descubrir los siguientes tipos de vulnerabilidades:

- **Vulnerabilidades de los Sistemas Operativos y Aplicaciones Comerciales**.
  Se debe encontrar aquellas vulnerabilidades que puedan existir en los sistemas operativos y en las aplicaciones comerciales de los servicios encontrados y que puedan ser explotadas para conseguir accesos no autorizados.
- **Vulnerabilidades en Aplicaciones Propietarias**.
  Se debe verificar el nivel de seguridad que posee el desarrollo de los servicios web analizados, comprobando si existen deficiencias en la programación que pudieran ser aprovechadas por un atacante.
- **Riesgo en el acceso a la Red Corporativa**.
  Se debe estudiar las posibilidades de que un atacante se adentrase en la LAN de la arquitectura de red de **la Concesionaria** y la posibilidad de escalar privilegios.
- **Explotación de vulnerabilidades**.
  Las vulnerabilidades detectadas se intentarán explotar, demostrando los resultados obtenidos para justificar las consecuencias de un acceso no autorizado.

Para descubrir los puntos débiles del sistema se deben considerar al menos la realización de tres tipos de ataques:

- **Pasivos**: recogiendo toda la información posible de los sistemas. Este tipo de ataque facilitará el tener un mejor conocimiento del objetivo para lanzar posteriormente ataques activos.
- **Activos**: aplicación de los conocimientos recogidos para intentar violar la seguridad existente.
- **Intrusivo**: si se ha logrado violar la seguridad existente, se intentará obtener un mayor nivel de acceso. En ningún caso se realizará actividades potencialmente peligrosas para la integridad del sistema o servicio, este tipo de ataque será únicamente para recoger evidencias.

El alcance de los trabajos para cada uno de los sistemas auditados deberá incluir, entre otros, las siguientes actividades:

6.2.1.1. Análisis de la red:

Se debe considerar como actividad a realizar un análisis de la red como primer paso para conocer la magnitud y complejidad del sistema que se tratará.

Deberá encontrar el número de máquinas implicadas en el sistema de información que puedan convertirse en objetivos, siempre sin exceder los límites legales. Los resultados esperados son:

- Nombres de Dominio.

- Nombres de Servidores.
- Direcciones IP.
- Mapas de Red.
- Información del ISP.
- Dueños de Sistemas y Servicios.

6.2.1.2. Análisis e identificación de servicios.

El objetivo es detectar los servicios que las máquinas tienen activos, así como los programas que los soportan. Para ello se deberán realizar test de visibilidad que permitan obtener un inventario de los servicios accesibles desde las direcciones IP públicas con el fin de determinar cuáles serían las principales puertas de entrada que valoraría un intruso a la hora de intentar un ataque contra los recursos de **la Concesionaria**. Dentro del alcance propuesto se deberán tener los siguientes resultados:

- Puertos abiertos, cerrados o filtrados.
- Direcciones IP de los sistemas vivos.
- Direcciones IP de la red interior.
- Topología de la red.
- Tipos de servicios.
- Servicios activos.
- Tipo de aplicación y nivel de actualización.

6.2.1.3. Identificación de sistema.

El objetivo es identificar el sistema operativo. Se espera el siguiente resultado:

- Sistemas operativos y versiones.
- Nivel de actualización.
- Direcciones IP internas.

6.2.1.4. Búsqueda de vulnerabilidades.

En esta actividad se requiere buscar la existencia de vulnerabilidades en todos los sistemas informáticos de la entidad (servidores, estaciones de trabajo, dispositivos móviles, firewalls, routers, etc.). Se deberán realizar test automáticos y manuales con las últimas versiones de software de detección de vulnerabilidades. Los resultados esperados son:

- Tipo de aplicación o servicio por vulnerabilidad.
- Nivel de actualización de sistemas y aplicaciones.
- Vulnerabilidades en los puestos de trabajo y dispositivos móviles.
- Vulnerabilidades por denegación de servicio.
- Áreas securizadas por ocultación o visibles.
- Vulnerabilidades reales (sin contar las falsas alarmas).
- Topología de red.

6.2.1.5. Análisis de firewalls, routers y VPN.

El objetivo es comprobar que ambos sistemas cumplen su función de una manera efectiva, es decir, bloquean las conexiones indebidas y proporcionan acceso seguro a los sistemas pertenecientes a su lista de accesos permitidos.

Se deberá comprobar además si el firewall ofrece algún sistema de conexión para la creación de VPN, comprobando su nivel de acceso. Los resultados esperados son:

- Política de entrada y salida a la red.
- Lista de posibles protocolos y paquetes que pueden entrar en la red.
- Listado de sistemas vivos encontrados.
- Listado de caminos no monitorizados con acceso a la red.

6.2.1.6. Análisis de los entornos webs

Se debe contemplar al menos los siguientes análisis de entorno en ambientes web.

- Recopilación de Información utilizando motores de búsqueda, peticiones http, firma digital, análisis sobre códigos de error, nombres del dominio, nombre de servidores, etc.
- Identificación de los posibles puntos débiles desde el punto de vista de la seguridad:
  - Pruebas de los mecanismos de autenticación.
  - Pruebas de los mecanismos de sesión.
  - Pruebas del sistema de permisos y autorización.
  - Pruebas de la lógica de negocio.
  - Pruebas de la validación de datos.
  - Pruebas de denegación de servicio.
  - Pruebas sobre los servicios web.
  - Pruebas sobre AJAX.
  - Explotación de fallos de programación (SQL injection, XSS, inyección de ficheros, escalado de privilegios, etc.).
- Vulnerabilidades en la autenticación:
  - Enumeración de usuarios.
  - Pruebas de diccionario sobre cuentas de usuario o cuentas predeterminadas.
  - Pruebas de fuerza bruta.
  - Pruebas para saltarse el sistema de autenticación.
  - Pruebas de gestión del caché de navegación y de salida de sesión.
  - Comprobar sistemas de recordatorio/restauración de contraseñas vulnerables.
  - Pruebas de CAPTCHA.

6.2.1.7. Diagnóstico de seguridad de red.

El objetivo de esta actividad es comprobar que los dispositivos de comunicaciones están configurados de forma robusta e identificar los posibles puntos débiles. Para ellos se realizarán, entre otras, las siguientes actividades:

- Test de seguridad en VLAN.
  Se comprobará si es posible conectar cualquier equipo en un puerto y obtener acceso a la VLAN a la que esté conectado ese puerto.

- Descubrimiento de activos internos con técnicas ICMP y ARP. Descubrimientos de VLAN.
  El objetivo es obtener las VLAN utilizadas mediante la observación de los paquetes CDP y la realización de ataques DTP trunk, para intentar convertir el puerto conectado al dispositivo de test en un puerto trunk. Así el equipo de test podría tener acceso a las tramas etiquetadas y obtener los identificadores de VLAN. A partir de aquí se puede hacer un barrido arp o icmp para encontrar los equipos conectados a la red.

- Test de ARP Poisoning / ARP Spoofing.
  Se realizarán pruebas de ataques de envenenamiento de cache de dos equipos seleccionados, enviando múltiples tramas ARP. A cada equipo se le enviarán tramas indicando que la MAC del otro equipo es la del equipo de test hasta que se consiga que la comunicación entre los dos equipos pase por el equipo de test y lograr así un ataque MITM (Man-In-The-Middle)

- Test de captura de tráfico en VLAN active.
  Se realizarán pruebas para tratar de lograr un desbordamiento de la tabla de MACs del switch, de forma que el switch se vea obligado a propagar el tráfico por todos sus puertos y así poder capturar el tráfico de la VLAN.

- Test de seguridad de VLAN / Técnicas de VLAN hopping.
  Se realizarán tests de salto de VLAN mediante técnicas de simulación de router trunk y de doble etiquetado de tramas.

6.2.1.8. Pruebas de Ingeniería Social.

Se requiere la realización de pruebas de ingeniería social mediante phishing. Se debe considerar al menos estudiar la posibilidad de que un atacante consiga suplantar la identidad de un tercero de confianza para conseguir información confidencial como usuarios y contraseñas válidas dentro de la red. Para ello, se debe contemplar la creación de un correo electrónico que aparente ser una comunicación interna, invitando a los destinarios a realizar unas pruebas en la red, intentando que el destinatario no sospeche del fraude ni al recibir el correo ni al realizar la operación que se demanda.

Estas pruebas se podrán ver reforzadas, si **la Concesionaria** y el Proveedor así lo acuerdan, mediante otro tipo de pruebas de Ingeniería Social, llamadas encubiertas, dispositivos infectados por malware, etc.

6.2.2. Diagnóstico del Estado de Sistemas y Comunicaciones.

Se deberán llevar a cabo una serie de pruebas y análisis de forma interna sobre los sistemas, no solo evaluando sus vulnerabilidades, si no estudiando en profundidad su arquitectura, con el objetivo de revisar cada uno de los aspectos de la seguridad. El alcance de los trabajos para cada uno de los sistemas y servicios auditados deberá incluir, entre otras, las siguientes actividades:

- Análisis de firewalls y routers.
  Se debe estudiar la **ubicación** de los elementos en la arquitectura física y lógica de la red, además de su configuración.

- Revisión de la arquitectura de sistemas.
  Se debe estudiar el **diseño** y conjunto de relaciones entre las partes que constituyen el sistema.

- Revisiones políticas de AD.
  Se debe revisar las políticas de seguridad configuradas en los servidores de Active Directory.

- Seguridad en los accesos remotos.
  Se debe realizar un estudio de los protocolos y políticas de acceso remoto, así como los sistemas de protección para usuarios remotos (firewalls, routers, etc.) tanto su configuración como su ubicación dentro de la red.

- Hardening y la configuración de los sistemas.
  Se debe revisar si se están siguiendo las buenas prácticas de configuración en los sistemas en cuanto a hardening y configuración. En concreto, se debe evaluar sobre la aplicación de las siguientes configuraciones de seguridad específicas, tanto para prevenir ataques como para contener la elevación de privilegios en caso de que un ataque se materialice:
  - Establecimiento de Permisos.
  - Uso de usuarios por defecto.
  - Configuración de los arranques.
  - Revisión de seguridad del sistema de archivos.
  - Desactivación de servicios y usuarios no imprescindibles.
  - Políticas de acceso y contraseñas.
  - Activación de servicios de auditoría.
  - Revisión de tareas periódicas.
  - Configuración, generación, rotación, y notificación de logs.
  - Conectividad con sistemas externos.
  - Seguridad de las configuraciones aplicadas a los servicios: web, BBDD, servidor de aplicaciones, etc.
  - Políticas de antivirus.
- Gestión y Mantenimiento de la seguridad.
  Se debe revisar los distintos aspectos de administración y gestión de seguridad de los sistemas, entre ellos:
  - Monitorización de los sistemas.
  - Mantenimiento preventivo.
  - Seguimiento de incidentes de seguridad.

6.2.3. Auditoria del AD.

Se debe contemplar revisar los usuarios, grupos y permisos dados de alta en los servidores de Active Directory, y como resultado realizar las recomendaciones para mejorar el nivel de seguridad actual.

6.2.4. Documentación Esperada.

Una vez realizadas las actividades de diagnóstico se debe contemplar emitir a **la Concesionaria** un informe con los resultados y las acciones correctoras a realizar. Tanto para los diagnósticos internos como para los externos se debe redactar por parte del **Proveedor** como parte del servicio un informe detallado que refleje los resultados de las actividades y que recopile los hallazgos y un plan de acción para solventar los fallos de seguridad encontrados y proteger eficazmente los sistemas de información y aplicaciones.

El informe deberá contener, al menos, la siguiente información:

Alcance: Clara identificación de los activos analizados (nombres de los equipos e IPs analizadas).

Aspectos revisados: Para cada uno de los activos analizados se indicará qué aspectos se han revisado (protocolos, puertos, vulnerabilidades conocidas, etc.).

Método para reproducir las vulnerabilidades encontradas. En el caso de que se encuentren vulnerabilidades críticas, se indicará qué pasos se han dado para demostrar la presencia de la vulnerabilidad en cuestión.

Método para subsanar las vulnerabilidades encontradas. Se indicará qué acciones hay que adoptar para la subsanación de las vulnerabilidades encontradas.

Estado de actualización de las máquinas: Se indicará la información sobre el estado actualización de las máquinas, esto es, aplicación de parches y actualizaciones en los principales componentes (Sistema Operativo, Bases de Datos, etc.).

Deficiencias detectadas en sistemas y comunicaciones.

Plan de acción recomendado: Se definirá un plan de acción que incluirá todas las acciones necesarias para subsanar las deficiencias detectadas y llegar a la línea base de seguridad definida por **la Concesionaria**.

6.2.5. Auditoria de Software Instalado.

Se deberá considerar la recopilación de la información del software instalado, versión, e identificación del dispositivo físico o virtual que lo contiene con el objetivo de analizar la información para verificar los siguientes puntos:

- Software que precisa licenciamiento.
- Software que tiene condiciones específicas de uso.
- Software que pueda suponer un riesgo para la seguridad.

Una vez recopilado el software se debe analizar el detalle de los posibles problemas de seguridad encontrados en el software inventariado, y en ese caso establecer el siguiente plan de acción, donde se detalle las acciones a llevar a cabo, principalmente:

- Propuestas de actualización de software vulnerable.
- Eliminación de software obsoleto o fuera de soporte, propuestas de migración.
- Propuestas de mitigación en caso de software que no se puede eliminar.

6.3. Servicios de SOC.

Un servicio de SOC (Security Operations Center) es un servicio de ciberseguridad para la infraestructura TI de las empresas en modalidad 7/24. Su función principal es

proteger, detectar y responder frente a amenazas de seguridad que afecten al negocio y los incidentes que estas puedan causar a la empresa.

6.3.1. Seguridad de Red e Infraestructuras.

El objetivo de los servicios preventivos es auditar y certificar de manera permanente el nivel de seguridad de los servicios que ofrece **la Concesionaria**, tanto externa como internamente. Para ello se proponen varios tipos de acciones que se describen en los siguientes apartados.

6.3.1.1. Monitorización Permanente de Seguridad.

Este servicio debe estar orientado principalmente a la detección continúa de vulnerabilidades y de incidentes de seguridad. Para la correcta monitorización de la infraestructura, el Proveedor deberá proponer la configuración de una herramienta de monitorización automática y de renombre en la industria. El Proveedor deberá entregar un apartado con la evaluación y la descripción de la herramienta seleccionada, como el proceso de implantación.

Las funciones mínimas que debe contemplar este servicio son:

- Escaneos de vulnerabilidades continuos de elementos de seguridad perimetral, redes y servidores, permitiendo conocer los puntos débiles de los sistemas de manera permanente y enviar avisos ante las debilidades encontradas.
- Análisis de los eventos reportados por los sistemas de seguridad perimetral. Para aquellos eventos que se consideren signo de peligro real.
- Monitorización permanente de los parámetros de seguridad en tiempo real con objeto de detectar las anomalías de la manera más inmediata posible.
- Establecimiento de filtros en los sistemas de seguridad perimetral para optimizar la detección de actividades potencialmente peligrosas.
- Seguimiento de actividades sospechosas. Ante la detección de una actividad de este tipo se cruzarán las informaciones obtenidas de las trazas de los distintos sistemas para determinar el alcance de la actividad de un usuario.

6.3.1.2. Monitorización Permanente de Disponibilidad.

Los servicios de monitorización de disponibilidad deberán permitir al servicio eSOC conocer la indisponibilidad de un servicio en el mismo momento que se produce con el objetivo de valorar si la indisponibilidad viene derivada de un problema de seguridad o por cualquier otro tipo de problema técnico.

El Proveedor deberá incluir en la propuesta una herramienta de monitorización que le permita mantener una monitorización de todos los servicios utilizados por los sistemas de **la Concesionaria** 24x7 y evaluar la disponibilidad de manera externa.

Esta monitorización debe permitir saber de forma prácticamente inmediata cuándo se producen fallos o retrasos en los tiempos de respuesta de los servicios públicos o internos, de forma tal que permita tratar la incidencia rápidamente. Lo anterior debe garantizar un tiempo de disponibilidad y una calidad de servicio máxima a la vez que

le ayude al Proveedor a detectar cualquier incidente de seguridad que pueda afectar a la disponibilidad de los sistemas, incluso antes de que este se materialice.

Los eventos detectados serán notificados por los grupos que designe el **Proveedor** para que procedan a aplicar el correspondiente procedimiento de gestión de la incidencia.

6.3.1.3. Apoyo a las Labores de Corrección de Vulnerabilidades

Durante la aplicación de los planes de acción para la corrección de vulnerabilidades, el equipo de expertos en sistemas y comunicaciones del **Proveedor** deberá ofrecer el soporte necesario para la aplicación de las medidas necesarias para la solución de las vulnerabilidades, en caso de que **la Concesionaria** deba participar.

6.3.1.4. Evaluación de Seguridad de Nuevos Servicios.

Antes de la puesta en producción de un nuevo servicio por parte de **la Concesionaria**, el **Proveedor** deberá considerar realizar todos los trabajos necesarios para asegurar que el servicio se ofrecerá con las garantías de seguridad que **la Concesionaria** determine. Entre las actividades de revisión que se realizarán se destacan, al menos, las siguientes:

- Hardening del sistema operativo y del software base.
- Estado de actualizaciones y parches.
- Antivirus.
- Políticas de acceso y usuarios permitidos.
- Permisos establecidos en los elementos de seguridad perimetral.
- Posibilidad de acceso a la red interna desde el sistema.
- Análisis de vulnerabilidades completo.

6.3.1.5. Servicios de Hardening.

Se deberá contempla un servicio de Hardening con el objetivo de mejorar la seguridad de los sistemas mediante la aplicación de configuraciones de seguridad específicas, tanto para prevenir ataques informáticos como para contener la elevación de privilegios en caso de que un ataque se materialice. Entre las labores del servicio de hardening, se debe al menos considerar:

- Establecimiento de permisos.
- Configuración de los arranques.
- Revisión de seguridad del sistema de archivos.
- Desactivación de servicios y usuario no imprescindibles.
- Revisión de políticas de acceso y contraseñas.
- Activación de servicios de auditoría.
- Revisión de tareas periódicas.
- Configuración, generación, rotación y notificación de logs.

6.3.1.6. Guías de Hardening.

El Proveedor deberá redactar las guías detalladas de hardening de varios sistemas operativos, servidores web y bases de datos. Cada una de las guías debe seguir un esquema similar para facilitar su uso, y contendrá al menos los siguientes apartados:

- **Descripción de las características a asegurar**: Se deben explicar las implicaciones de la implantación de las medidas sugeridas.
- **Implantación**: Incluye las instrucciones concretas para la aplicación de cada medida.
- **Comprobación**: Se deben incluir las instrucciones para verificar que las medidas se han implantado correctamente.

Al menos se debe considerar inicialmente las siguientes guías:

- **Procedimientos generales de hardening.**
- **Hardening de S.O.** (Windows, Linux).

6.3.1.7. Apoyo al Hardening en Implantación de Nuevos Proyectos

En la puesta en producción de nuevos servicios el Proveedor debe considerar actualizar las guías ya redactadas, o elaborar nuevas guías en caso de no disponer de información para el software base del nuevo servicio. De esta manera, a lo largo del tiempo de ejecución del proyecto **la Concesionaria** recopilará guías actualizadas de todo el software base en uso en sus infraestructuras TI.

Además, durante la puesta en producción, el equipo de expertos en sistemas y comunicaciones del **Proveedor** debe ofrecer el soporte necesario para la aplicación del hardening antes de la puesta en producción.

6.3.1.8. Gestión de incidentes de seguridad

El **Proveedor** deberá comprometer el apoyo con las acciones reactivas necesarias para dar respuesta a los ataques y/o incidentes de seguridad que pudiera requerir **la Concesionaria**, estas acciones se realizarán siempre de acuerdo con la Política de Seguridad de **la Concesionaria** ante los eventos contemplados en ella. Se desatacan al menos en estas acciones:

- Identificación de sistemas y servicios afectados.
- Identificación del origen: acceso no autorizado, vulnerabilidad explotada, malware, etc.
- Revisión de los registros de los elementos de seguridad perimetral: IDS, proxy, firewall, etc.
- Revisión y análisis de trazas de los sistemas afectados.
- Determinación del alcance del incidente.
- Determinación de medidas correctivas.
- Emisión de un análisis forense.

El **Proveedor** deberá contemplar al término de la revisión de todos los datos adquiridos en fase de gestión del incidente de seguridad, la emisión de un informe

técnico que lo describa detalladamente. El informe constará de al menos los siguientes puntos.

- **Objeto del informe**, donde se describe el objeto principal del informe y se detallan todos los puntos tratados.
- **Descripción**, donde se describe de manera clara el incidente analizado y sus consecuencias.
- **Evidencias**, donde se describe y muestran de forma detallada los datos y evidencias obtenidas del estudio de los diferentes sistemas.
- **Conclusiones y recomendaciones**, donde se describen de manera detallada las conclusiones del estudio y se proponen las medidas necesarias para evitar que el incidente se repita.

6.3.2. Seguridad del Puesto de Trabajo

El Proveedor deberá realizar una monitorización activa de los puestos de trabajo y de los servidores con el objeto de prevenir, detectar y contener cualquier incidente relacionado con malware. Para ello desde el servicio se debe contemplar la realización, al menos, de los siguientes trabajos:

- Comprobación del estado de actualización del antivirus en los diferentes puestos e implementación de antivirus en nuevos puestos de usuario y/o servidores.
- Definición y seguimiento de configuraciones de exploración antivirus y antispyware.
- Definición y ejecución de políticas de exploraciones manuales periódicas en grupos de equipos.
- Configuración de notificaciones de la consola del antivirus.
- Configuración y explotación de informes de registro e informes para las actividades relacionadas con las amenazas
- Elaboración de avisos generales de alerta a la organización, o específicos a usuarios, ante amenazas de infecciones por malware.
- Elaboración de informes periódicos sobre el servicio y actualización de las métricas e indicadores definidos.
- Análisis, tratamiento, seguimiento y resolución de los incidentes relacionados por infecciones de malware.
- Análisis de malware.

6.4. Reporting.

Durante la ejecución del contrato el **Proveedor** deberá generar, a lo menos, los siguientes entregables:

6.4.1. Informe Semestral de Seguridad.

Como resultado del diagnóstico de control de sistemas de la información que realiza el **Proveedor** como parte del servicio, deberá emitir un “Informe técnico y ejecutivo

del estado de seguridad y recomendaciones", el cual incluirá al menos los siguientes apartados:

- Detalles de resultados de análisis de vulnerabilidades de la red corporativa de **la Concesionaria** que contendrá una visión del grado actual de calidad de la seguridad, incluyendo indicadores de:
  - Porcentaje de vulnerabilidades detectadas por tipo.
  - Total de equipos examinados.
  - Total de vulnerabilidades leves, medias y altas.
  - Dificultad de explotación de problemas.
  - Deficiencias en las configuraciones aplicadas.
  - Descripción de los problemas de seguridad relevantes, puertos abiertos, servicios habilitados, etc.
- Informe de detalle de vulnerabilidades destacadas. En este apartado se deberá aportar información de aquellas vulnerabilidades más relevantes, sobre los potenciales problemas que implican y recomendaciones.
- Conclusiones. Conclusiones del estado de seguridad a la vista de los resultados del análisis de seguridad y propuesta de objetivos de mejora.
- Recomendaciones de acciones para alcanzar el nivel de seguridad superior. El Proveedor deberá presentar recomendaciones de líneas de acción propuestas para alcanzar las mejoras indicadas en el apartado de conclusiones.

6.4.2. Informe del Estado de los Sistemas

Se deberá considerar con una periodicidad anual, la emisión de un informe de estado de seguridad de los sistemas y comunicaciones que a lo menos incluirá lo siguiente:

- Resumen ejecutivo con las principales debilidades encontradas en sistemas y comunicaciones.
- Para cada uno de los siguientes puntos se debe describir el estado actual, las conclusiones o análisis del estado desde el punto de vista de la seguridad, y las acciones a llevar a cabo para mejorar la seguridad:
  - Infraestructuras y comunicaciones.
  - Dispositivos de seguridad: cortafuegos.
  - Mantenimiento de servidores:
    - Copias de seguridad. Sistemas de respaldo.
    - Inventarios.
    - Gestión de incidentes.
    - Monitorización.
    - Mantenimientos preventivos (parcheados, logs, gestión de usuarios, revisiones periódicas, etc.).
    - Informes.
  - Políticas de seguridad del Directorio Activo.
  - Bastionado.

6.4.3. Informe de Estado del Software

El **Proveedor** deberá emitir un informe con periodicidad anual en donde se incluirán los resultados de la auditoría de software instalado. En el informe a lo menos se incluirá, lo siguiente:

- Resumen ejecutivo, con una evaluación global del estado de seguridad según el software instalado.
- Estado actual del software instalado, con un resumen de los distintos paquetes de software detectados.
- Análisis de las debilidades de seguridad encontradas según el software instalado.
- Plan de acción recomendado para corregir las debilidades encontradas.

6.4.4. Informe de Auditoría de AD

Se deberá emitir un informe con periodicidad anual que contendrá al menos la siguiente información:

- Usuarios activos en el AD y grupos.
- Políticas configuradas.
- Permisos sobre recursos y sobre la gestión de la red.
- Conclusiones.
- Acciones recomendadas.

6.4.5. Informes Mensuales

Se deberá realizar un informe mensual con el resumen de actividades del periodo, elaborado por la jefatura de proyecto del **Proveedor**, que recogerá todas y cada una de las actuaciones realizadas durante el periodo y el estado de las tareas pendientes. Se incluirá, además, un apartado resumen de los incidentes de seguridad detectados durante el periodo y apartado exclusivo de vulnerabilidades, con el contenido detallado de las vulnerabilidades encontradas y las soluciones propuestas para eliminar dichas vulnerabilidades.

Este informe contendrá un apartado de cumplimiento de SLA y KPI.

6.4.6. Informe Específico de Vulnerabilidades Significativas

En el caso de la aparición de una vulnerabilidad significativa, bien por su gravedad o por el impacto que pueda tener en la infraestructura de **la Concesionaria**, el **Proveedor** deberá avisar inmediatamente a **la Concesionaria**, por los cauces establecidos y elaborará un informe específico con todos los datos necesarios para la identificación y corrección de la vulnerabilidad.

6.4.7. Informe de Disponibilidad del SIC-NS.

El primer día hábil de cada mes se deberá entregar un informe mensual denominado "***Informe de Disponibilidad del SIC-NS***", que deberá contener los aspectos relevantes de la explotación del Sistema SIC-NS del mes anterior. Este informe deberá detallar los eventos que hayan afectado el registro oportuno de la información del período y se entregará acompañado del certificado original emitido por la empresa externa de monitoreo en que se acredite la disponibilidad medida del Sistema SIC-NS durante el mes informado.

7. ANEXOS

7.1. ANEXO N° 1: ESCALAMIENTO DEL SERVICIO DE SOPORTE

El Proveedor deberá definir en su propuesta cómo abordará las comunicaciones con **AVO** para brindar un servicio de acuerdo a los estándares definidos por esta última.

En particular el Proveedor deberá definir la contraparte en las siguientes áreas:

Consultor Sistemas y Ciberseguridad

Permitirá a **AVO** resolver dudas respecto a la operación de las plataformas y su estado, análisis de casos y detección de posibles problemas.

Dentro de las actividades importantes de este Rol, estará la de identificar, evaluar y gestionar en forma anticipada las soluciones a brechas de seguridad detectadas y el cumplimiento de normativas sobre el tratamiento de información.

Responsable Centro de Operaciones

Será el responsable de la explotación y continuidad operacional del servicio. Su disponibilidad deberá estar de acuerdo con la modalidad de horarios en que se brinda el servicio. Para este efecto se deberá conocer los siguientes datos y niveles de escalamientos:

- Correo genérico de soporte. Ejemplo: soporte@Proveedor.cl
- Tel. Fijo: XXXXXXXX
- Tel. Móvil: XXXXXXXX

Gerente de Operaciones

El Gerente de Operaciones debe ser el último nivel de escalamiento al cual AVO deberá derivar los problemas no resueltos por las áreas encargadas de operación del servicio, nuevas solicitudes, reclamos y cualquier otra actividad que no pueda ser resuelta por los operadores de soporte.

Administrador del Contrato

El Administrador del Contrato deberá gestionar nuevos servicios a contratar, cambio en las condiciones de servicio, renovación de servicios, término de servicios, negociación de valores de servicios y cualquier otra actividad que no pueda ser resuelta por los niveles de contacto operativos.

7.2. ANEXO N° 2: SOLUCIONES Y/O SERVICIOS SIMILARES

(Completar tantas fichas como experiencias demostrables se presenten)

N° Ficha	*(Correlativo de experiencia demostrable)*
Nombre del cliente o Mandante	
Tipo de empresa	
Nombre Contacto	
Fono contacto	
Cargo Contacto	
Fecha de inicio	
Fecha de Término	
Estado de fecha	
Descripción del proyecto	

7.3. ANEXO N° 3: CURRÍCULUM VITAE DE LOS PROFESIONALES

(Completar tantas fichas como profesionales se incorporen)

N° Ficha	*(Correlativo de experiencia demostrable)*
Nombre del profesional	
Cargo	
Fecha de nacimiento	
Nombre del proyecto	
% Participación en el proyecto	
Estudios medios o técnicos	
Estudios universitarios	• *Profesión* • *Universidad* • *Año de ingreso* • *Año Egreso* • *Profesión* • *Universidad* • *Año de ingreso* • *Año Egreso* • *Profesión* • *Universidad* • *Año de ingreso* • *Año Egreso*
Otros Estudios	• *Diplomado/Curso/MBA/Otros* • *Institución* • *Duración* • *Diplomado/Curso/MBA/Otros* • *Institución* • *Duración* • *Diplomado/Curso/MBA/Otros* • *Institución* • *Duración*

Experiencia profesional			
Fecha (Desde - Hasta)	Empresa	Función	Cargo
Proyectos relevantes			
Fecha (Desde - Hasta)	Empresa	Función	Cargo

7.4. ANEXO N° 4: ESTRUCTURA INTEGRACION BITACORAS DEL SIC-NS

7.4.1. Indicador DPW.

Indicador 7 [I7]: porcentaje mensual de disponibilidad de la página web [DPW].

Estándar de servicio [ES7]: que la página web se encuentre disponible, a lo menos en un 99,5% de los minutos del mes.

Datos de Entrada – Registro de Bitacora.		
Indicador	DPW	Varchar (4)
código	I7	Varchar (4)
exigencia	E0	Varchar (4)
Fecha_informada	YYYY-MM-DD THH:MM:SS	Datetime
fecha_medicion	YYYY-MM-DD	Date
minutos_disponibilidad	1380	int
minutos_mes	1440	int

Método de Constatación [MC7]: corresponde a los registros efectuados en la Bitácora que está definida como parte del SIC-NS según lo señalado en el anexo 4 de las presentes Bases de Licitación. Para este caso se utilizará los informes de Hosting del servicio de monitoreo.

7.4.2. Disponibilidad SIC-NS.

Medición de la disponibilidad efectiva del SIC-NS correspondiente al mes "m" sera determinada a partir de la ecuación (1) que corresponde l menor valor de los factores de disponibilidades descritos en las ecuaciones (2) y (3).

$$DE = Min[FD_1; FD_2] \qquad (1)$$

$$FD_1 = \frac{MRI}{TMM} x100 \qquad (2); \qquad FD_2 = \frac{MDU}{TMM} x100 \qquad (3)$$

donde:

DE : **Disponibilidad efectiva**

FD_1 : **Factor de disponibilidad 1**

MRI : **Minutos mensuales en que el SIC-NS registró en tiempo real la información de los sistemas que debe estar integrado**

TMM : **Total de minutos del mes**

FD_2 : **Factor de disponibilidad 2**

MDU : **Minutos mensuales en que el SIC-NS desplegó su funcionalidad a sus usuarios en sus respectivos puestos de trabajo.**

El servicio de monitoreo, debe registrar en forma automática y en tiempo real la disponibilidad y los tiempos de interacción del Sistema SIC-NS.

7.5. ANEXO N° 5: ANTECEDENTES LEGALES Y FINANCIEROS

7.5.1. Antecedentes Legales

1	Razón Social.	
2	RUT.	
3	Dirección Comercial.	
4	Teléfono.	
5	Nombre del representante legal.	
6	Rut del representante legal.	
7	Nombre del responsable de la Oferta.	
8	Teléfono DEL responsable de la Oferta (fijo y móvil).	
9	Correo electrónico del responsable de la Oferta.	
10	Copia de la escritura pública en donde conste la personería de los representantes legales y certificado de vigencia de dichos poderes, ambos con una vigencia no superior a 30 días contados desde la presentación de la Oferta.	
11	Copia de la escritura pública de constitución de la Sociedad (Fotocopia no legalizada o CD), su extracto publicado en el D.O. e inscripción, con anotaciones marginales en CBR con vigencia menor a 30 días desde la presentación de la Oferta. Copia de todas las modificaciones	

7.5.2. Socios

RUT	Nombres	Participación (%)

7.5.3. Antecedentes Financieros

a) Estados Financieros:

- Balance General de los últimos dos años (2019 y 2020).
- Estado de Resultado de los últimos dos años (2019 y 2020).
- Flujo de Efectivo de los últimos dos años (2019 y 2020).

Se debe incluir el informe de Auditorías Externas del último año si procede, con una estructura financiera similar a la normada por la Superintendencia de Valores y Seguros, debidamente autorizados por el contador y representante legal de la Empresa.

b) Certificado de Endeudamiento en el sistema financiero, otorgado por la Superintendencia de Bancos e Instituciones Financieras, de no más de 10 días de antigüedad.

c) Certificado de situación al día de deudas laborales y previsionales emitido por la Inspección del trabajo, de no más de 10 días de antigüedad.

d) Certificado de Tesorería General de la República que acredite que no tiene deuda fiscal morosa a la fecha de presentación de los estados financieros, de no más de 10 días de antigüedad.

e) Certificado de pago de Renta de los 3 últimos años.

f) Certificado de Liquidez Disponible, libre de prendas y gravámenes, emitido por institución bancaria, de no más de 10 días de antigüedad.

7.6. ANEXO N° 6: FORMULARIO OFERTA ECONÓMICA

El Oferente que suscribe el presente formulario; declara haber estudiado con detalle todos los documentos del proceso de Licitación para el denominado ***CONTRATO DE PRESTACIÓN SERVICIOS DE OPERACIONES DE MONITOREO Y CIBERSEGURIDAD PARA LA "CONCESIÓN AMÉRICO VESPUCIO ORIENTE, TRAMO AV. EL SALTO – PRÍNCIPE DE GALES",*** *oferta los siguientes precios unitarios según lo establecido en las Bases de Licitación:*

Cuadro de Precios Unitarios (*)

ITEM	DESCRIPCIÓN	UNIDAD	*PRECIO UNITARIO EN UF*
1	*Servicios de Operaciones de Monitoreo y Ciberseguridad*	Mes	

(*) Notas al Cuadro de Precios Unitarios:

(i).- Precios en UF.-

(ii).- Valores sin IVA.-

(iii).- Se entienden incluidos todos los servicios y responsabilidades de los Documentos del Contrato, aunque no tengan ítem o descripción especifica en el Cuadro de Precios Unitarios.-

(iv).- Los precios del Contrato únicamente se reajustarán, si corresponde, según lo establecido al respecto en los documentos del proceso de Licitación.–

CUADRO DE FIRMA(S) COTIZANTE:	
Nombre o Razón Social:	
RUT:	
Nombre de Representante(s) Legal(s):	
RUT de Represente(s) Legal(es):	
Firma(s):	

7.7. ANEXO N° 7: MATRIZ DE EVALUACIÓN DE OFERTAS

Se incluye archivo “Anexo N° 7 – Matriz de Evaluación de Ofertas.xls”