



ASOCIACIÓN CHILENA DE SEGURIDAD

LICITACIÓN

PROYECTO RENOVACIÓN TECNOLÓGICA DE FIREWALLS

(SUMINISTRO, IMPLEMENTACIÓN Y SOPORTE)

Marzo 2022

CONTENIDO

1	INTRODUCCIÓN	4
2	OBJETIVO DE LA LICITACIÓN	5
3	PROVEEDOR	6
3.1	Consideraciones Generales	7
4	DESCRIPCIÓN DE LA GERENCIA DE SERVICIOS TECNOLÓGICOS.....	9
4.1	Situación Actual.....	9
5	REQUERIMIENTOS DEL PROYECTO.....	12
5.1	COMPONENTE 1: INFRAESTRUCTURA TECNOLÓGICA PARA SEGURIDAD PERIMETRAL.....	12
5.1.1	Base de Diseño.	12
5.1.2	Firewall Perimetrales.....	14
5.1.3	Protección Web Application, DNS y Load Balancing (CDN).....	15
5.1.4	Balanceo de Servicios	16
5.1.5	Web Application Firewalls (WAF).....	17
5.1.6	Consolas de Administración	18
5.2	COMPONENTE 2: SOC	18
5.2.1	Administración de Infraestructura	19
5.2.1.1	Monitoreo de la Infraestructura	19
5.2.1.2	Mantenimiento Preventiva	20
5.2.1.3	Mantenimiento Correctiva.....	20
5.2.1.4	Requerimientos que debe Gestionar del SOC.....	22
5.2.1.5	Reportes de Gestión de Servicios.....	22
5.2.2	Analizador de Logs	23
5.2.3	Gestión de Eventos de Seguridad.....	23
5.2.3.1	Gestión del Servicio.....	23
5.2.3.2	Análisis de Eventos	24
5.2.4	Equipo de Respuesta ante Incidentes (IRM)	25
5.2.4.1	Documentación	25
5.2.4.2	Control y Gestión.....	27
5.2.4.3	Gestión sobre incidentes.....	27
5.2.4.4	Análisis Forense.....	28
5.3	IMPLEMENTACIÓN DE SERVICIOS	28
5.3.1	Gerenciamiento.....	29

5.3.2	Instalación y Configuración	29
5.3.2.1	Carta Gantt	30
5.3.2.2	Plan de Implementación y de Migración.....	30
5.3.2.3	Ambiente Pre-Productivo.....	31
5.3.2.4	Instalación de Componentes.....	31
5.3.2.5	Pruebas de Contingencia.....	32
5.3.3	Capacitación Técnica	32
5.3.4	Entregables.....	33
5.3.5	Garantía de Implementación del Proyecto	33
5.4	OPERACIÓN DE LOS SERVICIOS	33
5.4.1	Gobierno de Servicios.....	33
5.4.2	Supervisor de Servicio	34
5.4.3	Estructura de Gestión y Supervisión de Servicios	34
5.4.4	Esquema de Escalamiento.....	35
5.4.5	Reuniones de Trabajo y Revisiones	35
5.5	MANTENIMIENTO DE COMPONENTES.....	35
5.5.1	Upgrades y Updates	35
5.5.2	Plan de Continuidad y Contingencia	36
5.5.3	Gestión de Capacidad de Servicio	37
5.5.4	Garantías y Mantenimiento	38
5.5.5	Plan de Devolución.....	38
5.6	EXPERIENCIA DEL PROVEEDOR	39
5.6.1	Experiencia de la Empresa	39
5.6.2	Experiencia del Equipo	39
5.7	NIVELES DE SERVICIOS	40
5.7.1	Definiciones.....	40
5.7.2	Calidad de Servicio	41
5.7.3	SLA de Monitoreo de Seguridad.....	42
5.7.4	SLA de Administración.....	42
5.7.5	SLA de Monitoreo de Disponibilidad.....	43
5.7.6	SLA Disponibilidad del Servicio.....	43
5.7.7	SLA de Eventos Almacenados de Monitoreo	44
5.7.8	SLA de Gestión de Fallas.....	44
5.7.9	SLA de Mantenimiento Preventivo	45

5.7.10	Consideraciones de Niveles de Servicio	46
5.7.11	Cálculo de la Disponibilidad de los Servicios.....	46
5.7.12	Penalidades	47
6	MULTAS.....	47
6.1	Multas por Atrasos en la Entrega de los Servicios	47
6.2	Multas por Indisponibilidad Mensual	48
6.3	Multas por Facturación No Oportuna	49
7	PROPUESTA ECONÓMICA.....	49
7.1	Pautas de Evaluación.....	50
7.1.1	Pautas de Evaluación General	50
7.1.2	Pautas de Evaluación Técnica.....	50
8	CRONOGRAMA DE IMPLEMENTACIÓN	51
9	APORTES DEL PROVEEDOR.....	51
10	APORTES DE ACHS.....	51
11	CONFIDENCIALIDAD	51
11.1	ANEXOS TÉCNICOS	53
11.1.1	Anexo 1: Experiencia del Oferente.....	54
11.1.2	Anexo 2: Experiencia de los Ingenieros.....	55
11.1.3	Anexo 3: Plazos de Entrega	56
11.1.4	Anexo 4: Niveles de Servicio y Penalidades	57
11.1.5	Anexo 5: Cronograma de Implementación	58
11.1.6	Anexo 6: Formulario Propuesta Económica.....	59
11.1.7	Anexo 7: Formulario Preguntas y Respuesta	61
11.1.8	Anexo 8: Entregables Compromiso Proyecto.....	62

1 INTRODUCCIÓN

La Gerencia de Servicios Tecnológicos de la Asociación Chilena de la Seguridad, en adelante ACHS, requiere contar con plataformas tecnológicas que permitan proveer una capa de seguridad perimetral en el acceso a Internet, además de los servicios profesionales para la habilitación y operación de los componentes asociados.

Estas bases técnicas describen el equipamiento, configuraciones necesarias, instalación y el servicio de mantención a adquirir por la Asociación Chilena de Seguridad (ACHS en adelante) en el presente llamado a licitación. El documento se ha estructurado en su primera parte señalando el objetivo de la licitación, las características generales del proveedor buscado para la entrega de los equipos y servicios, la organización de Gerencia de Servicios Tecnológicos y el modelo de servicios buscado por ACHS.

Si bien ACHS ha preparado esta solicitud para especificar en forma clara y precisa los requerimientos mínimos que debe contener la solución, es el oferente en calidad de experto quien tiene que plantear una propuesta bien fundamentada que cumpla con lo estipulado, definiendo los detalles de la solución ofertada.

Se requiere contar con la correcta infraestructura tecnológica y servicios profesionales para la prestación de servicios de Seguridad TI en la red de ACHS. Específicamente, los equipos y servicios requeridos son:

- Equipamiento para controlar el acceso desde y hacia redes externas.
- Plataformas de balanceo de Servicios.
- Instalación, Configuración, Operación y Mantención de los Servicios.
- Centro de Operaciones de Seguridad (SOC).

Los componentes de la Licitación deben cumplir con las especificaciones declaradas en el formato de entregables. Ver Anexo 8.

La información de servicios, funcionalidades y cantidades se presentan en este documento y sus anexos.

Por otra parte, se indica descripción, alcance, requerimientos del equipamiento y servicios a contratar. De existir en este documento alguna alusión a marcas, íconos, modelos de equipos o

protocolos propietarios, deben ser tomadas como referenciales para establecer prestaciones o niveles de desempeño mínimos y, en ningún caso, obliga al Oferente a ofrecer una marca o modelo en particular.

Esta licitación busca la selección de una empresa con la experiencia, tecnología, procedimientos y personal certificado, necesarios para asegurar un óptimo suministro y operación de los servicios que se le encomienden.

Esta integración de procesos, tecnologías y personal, serán evaluados en conjunto por ACHS de forma de asegurar un servicio que disponga de un grado de madurez integral y cohesionado.

2 OBJETIVO DE LA LICITACIÓN

La ACHS ha decidido convocar a empresas nacionales o Internacionales instaladas en Chile, que dispongan de comprobada experiencia y capacidad para proveer servicios tecnológicos en ciberseguridad y seguridad perimetral de última generación, bajo normativas y estándares internacionales y otros servicios asociados.

La Gerencia de Servicios Tecnológicos requiere la renovación por medio de adquisición y migración de equipamiento necesario para robustecer el perímetro de seguridad en la red ACHS, al mismo tiempo la contratación de los trabajos referentes al diseño, análisis, configuración, homologación, implementación y mantención de una nueva plataforma de firewalls.

La solución propuesta debe ser robusta, confiable y segura, para brindar un servicio de seguridad con una mejor calidad técnica que aumente la experiencia del usuario, enmarcado en las siguientes consideraciones:

- Establecer las definiciones necesarias para mantener una relación estable y duradera con un socio estratégico que preste servicios a ACHS, proponiendo innovación y mejoras continuas acordes a las nuevas tendencias digitales.
- Disponer de infraestructura de última generación para garantizar la seguridad perimetral y Acceso a Internet de alta disponibilidad y velocidad de ACHS.
- Capacidad para gestionar la distribución de los recursos para un óptimo servicio de las distintas categorías de clientes de ACHS
- Contar con personal experto para la administración, soporte técnico y atención de incidentes, de acuerdo con niveles de servicio que aseguren la continuidad de las operaciones de ACHS.

- Disponer de ciclos de mejora continua para mantener la calidad esperada en los servicios, a fin de garantizar la calidad y su capacidad de afrontar los retos crecientes que nos plantean nuestros clientes y así disminuir el número de incidentes de seguridad, su impacto y el tiempo de gestión de estos.

En este contexto la necesidad se basa en el reemplazo de la plataforma de firewall, balanceadores, homologación de los sistemas VPN y la adquisición de un software de análisis y gestión de eventos (logs). Todo esto debe estar diseñado en una arquitectura de alta disponibilidad (HA) distribuyendo el equipamiento entre los dos data center que posee ACHS, que tenga un dashboard de monitoreo y se integre con Active Directory para la administración.

La nueva plataforma de seguridad perimetral debe cubrir la operación en Casa Central, Hospital y las diferentes agencias ACHS, así como el proceso de crecimiento y transformación tecnológica con el fin de proporcionar las facilidades y herramientas necesarias para cumplir con las metas operacionales y de negocios.

El desafío mayor de la Gerencia de Servicios Tecnológicos es entregar el nivel de servicio prometido a sus usuarios, potenciarnos como una organización de excelencia operacional y satisfacer los intereses de ACHS en orden a proveer una plataforma de seguridad perimetral de nueva generación.

3 PROVEEDOR

La ACHS busca un partner estratégico, con experiencia en equipamiento y los servicios que son materia de la presente licitación y con experiencia certificada, normas de calidad en la prestación de sus servicios y con un nivel de madurez comprobable.

Debe tener la capacidad de proveer el equipamiento necesario en tiempos acordes a la planificación del proyecto a adjudicar y brindar garantía, soporte y mantención bajo los acuerdos de servicios contratados.

Todo trabajo debe cumplir con los estándares tecnológicos de acuerdo con el equipamiento a licitar. Si existiera una limitante en su aplicación, deben seguirse aquellas especificaciones que sean más adecuadas tecnológicamente. Además, debe contar con personal capacitado y certificado en la instalación de sistemas de seguridad, ciberseguridad y afines.

3.1 Consideraciones Generales

El oferente deberá tener en cuenta las siguientes consideraciones para la definición de la solución técnica:

Aspectos Administrativos

- ACHS se reserva el derecho a declarar el Proceso desierto en su totalidad o de parte de él (adjudicando solo algunos de los ítems), sin que ello implique para los Participantes el pago de indemnización ni reembolso de posibles gastos.
- La adjudicación podrá ser total o parcial a uno o más Oferentes, por lo tanto, los valores solicitados deben ser independientes para los ítems de la licitación.
- Serán propiedad de ACHS tanto los equipos, software, artefactos, accesorios y gabinetes, como el mobiliario que ponga en servicio el Oferente y que formen parte de su oferta para cualquiera de los servicios requeridos.
- El Oferente deberá cumplir con el 100% de los requerimientos citados en las Bases de la licitación. En caso contrario la Oferta será declarada inadmisibile.
- En el caso de contradicción en la propuesta entregada, la Oferta será declarada inadmisibile.
- El Oferente deberá aclarar todas las dudas en el proceso de preguntas y respuestas. Cualquier diferencia de interpretación de las Bases Técnicas por parte del Adjudicado será resuelta por lo que defina ACHS.
- En la propuesta se deberá informar claramente que aspectos técnicos NO están considerados en la solución propuesta.
- El plazo máximo de implementación de los servicios será de 6 meses y el contrato tendrá una duración de 3 o 5 años.

Aspectos Técnicos

- El equipamiento propuesto para cada uno de los servicios requeridos en esta solicitud deberá ser nuevo y sin uso, con el objeto de disponer de la última tecnología y versiones disponibles en el mercado y asegurar su integración entre ellos.
- Todas las actualizaciones (por nuevas funcionalidades, por vulnerabilidades, otros.) deben estar contempladas durante todo el período de contrato.
- Los servicios prestados no estarán limitados solo a requerimientos de configuración básica de equipos señalados en estas bases. El proveedor deberá configurar los dispositivos involucrados en el contrato a solicitud de ACHS, si la funcionalidad está disponible en el licenciamiento considerado, sin costo adicional durante la vigencia del

contrato. Además, ACHS podrá solicitar la adición y eliminación de configuraciones de manera ilimitada en cualquier equipo de la solución, sin costo adicional durante la vigencia del contrato.

- ACHS tendrá acceso a todos los equipos instalados con privilegios de administrador. El proveedor deberá implementar sistemas de auditoría (ejemplo syslog) para cada equipo. En caso de incidentes atribuibles a la intervención de ingenieros, una comisión integrada por personal de ACHS y del Oferente revisarán los registros para identificar las responsabilidades.
- Todos los dispositivos de la solución deberán ser hardenizados de acuerdo con las recomendaciones del fabricante.
- El Oferente deberá contemplar que, actualmente, la red se encuentra en producción con servicios críticos de comunicaciones, que operan las 24 horas del día y los 365 días del año en forma continua e ininterrumpida. Razón por la cual toda intervención en la red debe contemplar el mínimo impacto en los servicios, en consecuencia, se deberá efectuar en horarios de bajo o nulo tráfico, los que más adelante serán informados al Adjudicado.
- Todos los equipos deben tener la capacidad de ser integrados a la plataforma SIEM de ACHS y el Oferente deberá hacer las configuraciones asociadas en los equipos de su solución cuando sea solicitado, sin costo adicional.
- La administración remota deberá ser realizada vía VPN a través del sistema y credenciales suministrado por ACHS.
- Todos los productos deben cumplir con los requisitos listados en las especificaciones técnicas.
- Se exigirá que todas las ofertas presentadas vengán acompañadas de una carta emitida por el fabricante en donde se avale el respaldo de este a la empresa oferente y se asuma un compromiso por la garantía.
- Se exigirá la presencia del fabricante en varias etapas del proceso de instalación, a fin de garantizar que la empresa seleccionada cumpla con todos los requerimientos exigidos por el mismo para la entrega de la garantía sin inconvenientes algunos, y en el caso de que fuese necesario, se hagan las correcciones pertinentes a su debido momento.
- Todo hardware de conexión y cable de telecomunicaciones debe estar manufacturado por certificado ISO 9001.

El proveedor está obligado a ejercer las más estrictas normas de cuidado en el desempeño de sus obligaciones tal como se definen en esta propuesta.

4 DESCRIPCIÓN DE LA GERENCIA DE SERVICIOS TECNOLÓGICOS

La Gerencia de Servicios Tecnológicos de ACHS, es responsable de proveer servicio de seguridad perimetral y conexiones remotas a sus usuarios, clientes internos, externos e invitados, los cuales están en las sedes de Casa Matriz, Hospital, ESACHS, red de Agencias y sedes distribuidas en el país.

La seguridad perimetral ha controlado tradicionalmente esta frontera, vigilando las comunicaciones para evitar accesos no autorizados, salida de datos desde el interior y ataques desde el exterior. Se podría decir que, con la evolución de las TIC, el perímetro ha cambiado.

Hoy en día la evolución tecnológica permite que el acceso desde el exterior de la red se realice con elementos con mayor capacidad de proceso, distantes (remotos), de forma inalámbrica y/o mediante dispositivos móviles. Igualmente, con la difusión de Internet cada vez resulta más complejo controlar las comunicaciones, en ocasiones cifradas, que establecen las aplicaciones web, mensajería instantánea, conferencias Web, entre otros.

Por otra parte, en la medida en que aumenta el uso de las arquitecturas orientadas al servicio o SaaS (del inglés Software As A Service, además de la virtualización y la computación en la nube o Cloud Computing) y en la medida en que se hace más común el uso de herramientas dirigidas a la web, las políticas basadas en puertos y protocolos, tradicionalmente utilizadas para el control del perímetro, son cada vez menos efectivas.

Por eso son necesarias nuevas herramientas para hacer frente a la evolución del comportamiento de los usuarios, a las nuevas formas en que los procesos de negocio utilizan las TIC y a los cambios en los mecanismos de los ataques que comprometen los sistemas de información.

4.1 Situación Actual

ACHS cuenta con una plataforma de seguridad perimetral basada en equipos marca Cisco que proveen el control de acceso para las conexiones desde y hacia la red privada. El acceso a las redes no seguras (Internet, proveedores, otros.) está dividida en tres zonas:

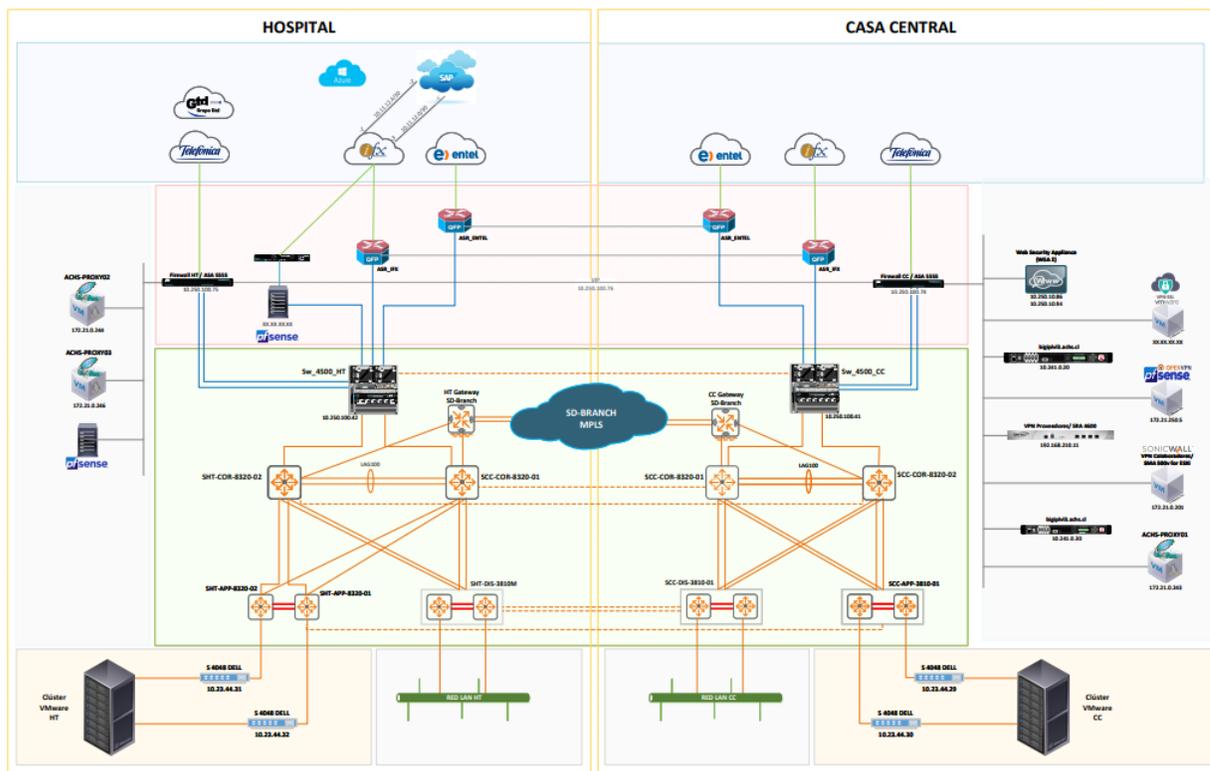
- Seguridad Zona Navegación.
 - Se refiere al bloque de seguridad para la navegación en Internet de los usuarios de la red institucional de ACHS.
- Seguridad Zona Publicación de Servicios.

- Se refiere a la seguridad de los servicios TI que publica ACHS y que quedan disponibles en Internet.
- Seguridad Zona Terceros.
 - Bloque de Seguridad para el acceso a la red de ACHS de personal externo a la empresa.

Para cada zona se cuenta con Firewalls, filtro de contenidos, Concentradores VPN, otros. que deben ser reemplazados por el adjudicado en este proceso.

La arquitectura actual de a la red se presenta en el siguiente diagrama.

Topología Actual Seguridad Perimetral ACHS



La red de ACHS actualmente utiliza a nivel Core tecnología Cisco Catalyst 4500 extendiendo Vlans en capa2 entre los sitios Hospital (Ramón Carnicer 185, Providencia) y Central (Ramón Carnicer 163, Providencia).

A nivel de seguridad perimetral se utilizan diferentes tecnologías que deberán ser provistas por la solución de seguridad perimetral propuesta, fundamentalmente haciendo uso de Firewall de nueva generación (NGFW).

Se enumeran las soluciones actuales

- Firewall Cisco ASA serie 5500 (Para la conectividad a internet se utilizan múltiples ISP, GTD y Entel).
- Firewall para conexión a SAP Cloud.
- Cisco Web Security Appliance (WSA2).
- VPN SSL VMware.
- Firewall para conexión de usuarios ACHS por VPN.
- Firewall VPN Proveedores.
- Squid Proxy para navegación usuarios y filtro de contenido.
- A nivel de balanceadores de carga se utiliza F5® BIG-IP appliance en modo clúster.

. El escenario de seguridad de hoy día se enmarca en las siguientes definiciones:

- La ACHS posee una plataforma de seguridad perimetral compuesta por equipamiento marca Cisco, en firewalls, filtros de contenidos y dispositivos de control de acceso.
- En cada uno de los sitios (Casa Central y Hospital) se encuentra implementado un cluster de firewalls perimetrales a los cuales se conectan los servicios de Internet de GTD
- Los firewalls operan en conjunto con los routers (ASR) que nos conectan con Internet para proporcionar redundancia en caso de caída de enlaces, routers o firewalls
- Los mismos firewalls ASA ya mencionados realizan funciones de terminador VPN Site to Site para consumir los servicios Azure desde la nube
- Actualmente sobre en el acceso desde la red MPLS de Telefónica existe control de tráfico básico
- La navegación Internet de los usuarios pasa por filtros de Proxy. Esto implica que se aplican diferentes controles respecto del contenido y los sitios a los cuales pueden navegar basados en grupos Full, Medio y Bajo.
- El perímetro de seguridad es distribuido, depende de varios componentes aislados que no se administran en forma unificada.
- Este esquema está replicado tanto en HT como en CC
- Cisco ASR 1004: Router Internet
- Cisco ASA 5555: Firewall Internet
- Cisco WSA: Filtro contenidos (proxy)
- La solución de seguridad actual solo considera el perímetro externo
 - No considera la seguridad interna de la red
 - Tampoco la seguridad del acceso desde y hacia la red WAN.

- El equipamiento de seguridad, aun siendo del mismo fabricante, no permite tener controles unificados.
 - Esto dificulta la visión integrada de los usuarios y su comportamiento de tráfico
- La solución actual no permite tener visibilidad y control del tráfico en tiempo real
- La administración la gestiona con un tercero
- El contrato actual no incluye retención de logs

5 REQUERIMIENTOS DEL PROYECTO

En esta sección se describen las especificaciones técnicas asociadas al suministro, instalación, configuración y migración del equipamiento de firewall, servicios VPN y demás componentes requeridos por ACHS, los cuales deben estar contemplados en la propuesta realizada por el Oferente.

Para este proyecto se requiere un análisis previo de las soluciones de seguridad actual, rediseño de la arquitectura y topología de seguridad, implementación y configuración del equipamiento, implementación de definiciones, políticas y reglas de seguridad, documentación y transferencia de conocimientos, garantía y soportes exigida por ACHS.

5.1 COMPONENTE 1: INFRAESTRUCTURA TECNOLÓGICA PARA SEGURIDAD PERIMETRAL

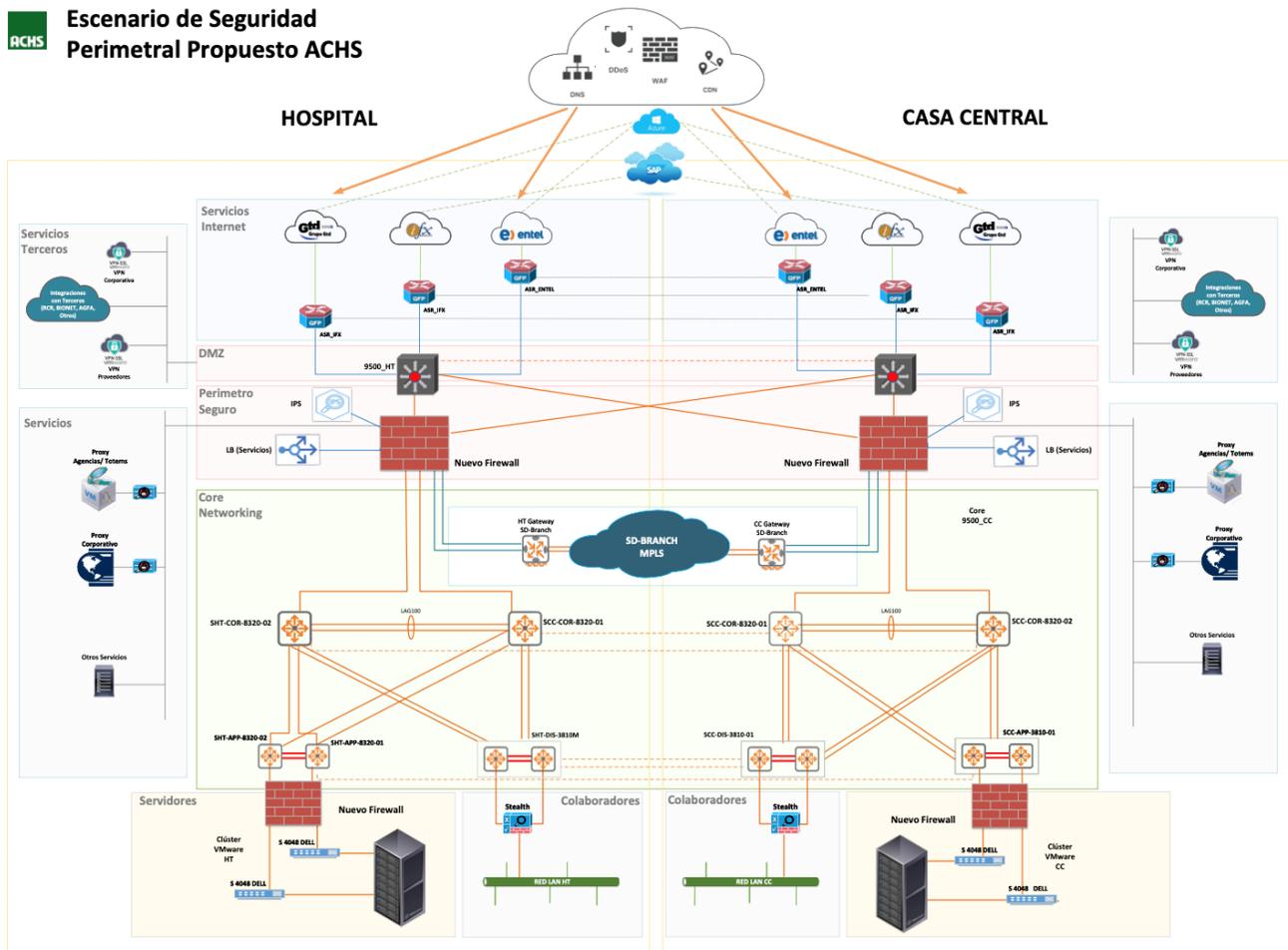
5.1.1 Base de Diseño.

El Oferente deberá diseñar una solución que considere:

- Todas las plataformas deben contar con Alta Disponibilidad.
- Los servicios TI (aplicaciones) estarán disponibles en ambos data centers y operarán en modalidad **Activo-Activo**.
- ACHS proveerá las conexiones Layer 2 y 3 entre los data centers en las zonas que el Oferente indique en su propuesta.
- Proponer equipos de fabricantes que estén citados en el cuadrante de líderes de Gartner del año 2021 en su respectivo nicho de mercado
 - Este punto es obligatorio, la ACHS solo aceptará ofertas que cumplan a cabalidad con este aspecto.

- Todos los equipos deben de poseer fuente de poder redundante.

El siguiente diagrama presenta la arquitectura definida por ACHS:



Se considera disponer de una protección externa mediante un CDN y que debe considerar además DDoS, DDNS, GSLB, WAF. En red interna se considera la actualización tecnológica de los firewalls perimetrales y de los balanceadores de carga.

El proveedor deberá validar el diseño o proponer cambios a este con las justificaciones correspondientes.

5.1.2 Firewall Perimetrales

ACHS requiere contar con dispositivos virtualizables en cada data center, y a través de ellos segmentar los accesos a Internet y terceros. En cada data center se debe contar con al menos un equipo, que será virtualizado en múltiples contextos que cumplirán distintas funciones. La alta disponibilidad de los contextos será local en cada data center y se ha considerado, hasta ahora, la construcción de los siguientes sistemas virtuales:

- Firewall Navegación.
- Firewall Publicación de Servicios.
- Servicio VPN ACHS (usuarios y empresas).
- Firewall de Terceros.
- Firewall de Visitas.
- Firewall DMZ interna.

Las características de cada equipo se presenta a continuación:

- Next Generation Firewall.
- Disponibilidad para crear al menos 10 firewalls virtuales y asignación de recursos por firewall virtual.
- Capacidad Deep packet inspection (DPI) en hardware.
- Debe soportar IPv4 e IPv6.
- Administración segura por SSH y HTTPS.
- Administración fuera de banda. ACHS proveerá la arquitectura de red para el acceso a los Firewalls.
- Compatibilidad con active Directory LDAP.
- Disponer de funcionalidad de prevención de ataques (IPS).
- Capacidad de análisis de malware o código malicioso.
- Debe identificar aplicaciones que utilizan puertos aleatorios mediante el análisis de tráfico.
- Capacidad de detección de anomalías y vulnerabilidades de aplicaciones.
- Capacidad de balanceo de tráfico de salida con múltiples proveedores WAN.
- Capacidad de realizar capturas de tráfico en formatos estándar.
- Capacidad para generar el perfil de tráfico y monitoreo de conexión mediante reglas.
- Categoría de las reglas File-Executables, DoS, DDoS, Exploit, P2P, Web-IIS, SQL, Indicator-Obfuscation, RPC y Botnet.
- Reconocimiento y control de aplicaciones:

- Debe disponer de un sistema de reconocimiento y clasificación de aplicaciones en categorías, tales como tipo de aplicación, nivel de riesgo de seguridad, implicaciones de productividad, uso de recursos, otros.
- Debe permitir crear políticas granulares basadas en usuarios, IP, o grupos, para bloquear o limitar el uso de aplicaciones y basado en horario, día de la semana, riesgo, categoría
- Filtros URL por grupos, tipos, sitios, otros.
- Se requiere que solución de seguridad tenga la capacidad de integrarse con organizaciones gubernamentales que emitan informes de seguridad de la información.
- FW (Deep packet Inspection) multiprotocol de 10Gbps.
- Capacidad para soportar, al menos, 3.000.000 conexiones concurrentes.
- Disponer de, al menos, 8 interfaces de 10Gbps, 8 interfaces de 1Gbps, por cada equipo y de forma concurrente, con estimación de crecimiento de 25%.
- Discos de estado sólido.
- Soporte hardware y software del respectivo fabricante a nombre de la ACHS por la duración del contrato en modalidad 24x7x4 con reemplazo de hardware siguiente día hábil

El Firewall de Next Generation debe ser capaz de soportar todos sus módulos activos con el Decrypt SSL del FW activado. Dado esto, se debe hacer el dimensionamiento del equipamiento considerando 50 segmentos internos a descifrar y soportando un crecimiento anual aproximado del 10%.

Además, se debe incluir en la propuesta los siguientes elementos para la conectividad adyacente de los firewalls

- 8 módulos 10G SFP+ Multimodo para firewalls a utilizar.
- 8 módulos 10G SFP+ LR Monomodo para firewalls a utilizar.
- 6 módulos 10G SFP+ Multimodo Aruba. Número de Parte J9150D.
- 4 módulos 10G SFP+ LR Monomodo Aruba. Número de Parte J9151E.
- 2 módulos 10G SFP+ Multimodo Cisco para los equipos directamente conectados a la plataforma. Número de Parte SFP-10G-SR.

5.1.3 Protección Web Application, DNS y Load Balancing (CDN)

Se requiere implementar una solución del tipo CDN para proteger la infraestructura Web. Se planea implementar los siguientes módulos:

- DDoS Protection.

- Web Application Firewall (WAF).
- DNS Global Load Balancing.
- Distribución de contenido (CDN).

La solución debe considerar:

- Solución de Balanceo Global. Soportar enrutamiento avanzado, como OSPF y BGP.
- Protección con ataques DNS.
- Debe incorporar georeferencia.
- Debe soportar DNS Autoritativo.
- Soporte DNSSEC.
- Distintos métodos de balanceo inteligente; es decir, que tenga capacidad de distribuir el tráfico de red por igual entre varios servidores de manera autónoma.
- Manejo del estado de la conexión.
- Debe bloquear los ataques en la capa de aplicación con protección basada reputación y firmas.
- Debe identificar y reportar comportamientos anómalos.
- Debe integrar una base de datos de amenazas en línea.
- Debe considerar protección contra ataques de robot o ataques automatizados.
- Debe considerar protección para APIs.
- Protección de ataques de fuerza bruta y enumeración.
- Protección de Web Scraping.
- Debe soportar al menos 1 millón requerimientos L7 por segundo.
- Debe proporcionar redundancia de sitio.
- Debe entregar protección por DDoS o ataque volumétrico.
- Debe disponer integración con herramientas de automatización.
- Debe considerar bloqueo geolocalizado.
- Integración con SIEM y Gestor de Log de ACHS.
- Correlación de eventos.
- Soporte hardware y software del respectivo fabricante a nombre de ACHS de acuerdo a lo establecido en el Anexo 4. (SLA).

5.1.4 Balanceo de Servicios

Se requiere de una solución de balanceo de carga de servicios en alta disponibilidad virtualizable sobre plataforma VMware que cumpla con las siguientes características:

- Debe ser capaz de balancear una carga de a lo menos 1 millón de requerimientos por segundos en L7.
- Debe soportar al menos 4.000 transacciones SSL/TPS.
- Administración segura por SSH y HTTPS.
- Se debe considerar una capacidad de crecimiento de tráfico del 10% anual.
- Distintos métodos de balanceo inteligente
- Manejo del estado de la conexión.
- Debe tener integración con herramientas de automatización.
- Capacidad de integración con SIEM y Gestor de Log de ACHS.
- Soporte software del respectivo fabricante a nombre de la ACHS de acuerdo con lo establecido en el Anexo 4. (SLA).

El Oferente debe informar las características de los servidores que requiere para la implementación de la solución de balanceo de servicios.

5.1.5 Web Application Firewalls (WAF)

Se requiere de una solución de Web Application Firewall para la protección de los sitios y aplicaciones publicadas por ACHS a Internet y que cumpla con las siguientes características:

- La solución debe ser On-Premise.
- Debe bloquear los ataques en la capa de aplicación con protección basada reputación y firmas.
- Debe identificar y reportar comportamientos anómalos.
- Debe integrar una base de datos de amenazas en línea.
- Debe considerar protección contra ataques de robot o ataques automatizados.
- Debe considerar protección para APIs.
- Protección de ataques de fuerza bruta y enumeración.
- Protección de Web Scraping.
- Debe soportar al menos 1 millón de requerimientos por segundos en L7.
- Debe dar redundancia de sitio.
- Debe entregar protección por DDoS o ataque volumétrico.
- Debe tener integración con herramientas de automatización.
- Debe considerar bloqueo geolocalizado.
- Integración con SIEM y Gestor de Log de ACHS.
- Correlación de eventos.

- Disponer como mínimo de 2 interfaces de 10 Gigabit Ethernet, 6 interfaces Gigabit Ethernet cobre 100/1000, por cada equipo y de forma concurrente.
- Se requieren discos de estado sólido.
- Administración fuera de banda.
- Considerar módulos 10G SFP+ Multimodo a utilizar por la plataforma.
- Considerar módulos 10G SFP+ Multimodo Aruba para los equipos directamente conectados a la plataforma.
- Soporte hardware y software del respectivo fabricante a nombre de la ACHS por la duración del contrato de acuerdo a lo establecido en el Anexo 4 (SLA).

5.1.6 Consolas de Administración

Se debe considerar el software o herramientas para la gestión y configuración de los Firewalls y Balanceadores de manera centralizada.

La compra de Software, sistema operativo, licencias, implementación y soporte necesarias para instalación de las consolas son responsabilidad del Oferente.

El hardware para la habilitación de las consolas será provisto por ACHS en ambientes virtuales VMware y el Oferente deberá informar las características de los servidores requeridos completando el anexo correspondiente.

5.2 COMPONENTE 2: SOC

En este proceso se requiere la contratación de un Centro de Operaciones de Seguridad llamado SOC, el que deberá interactuar tanto con ACHS como con los proveedores de los servicios asociados a las herramientas corporativas.

Las principales actividades por desarrollar son:

- Administración de la infraestructura.
- Monitoreo continuo de las alertas de seguridad.
- Análisis de vulnerabilidades informadas por organismos externos, además del estudio de su impacto en las plataformas de ACHS
- Análisis y Seguimiento de Eventos e Incidentes reportados por las herramientas de seguridad y/u otro canal de información.

El SOC será responsable de las actividades solicitadas en los siguientes puntos.

5.2.1 Administración de Infraestructura

5.2.1.1 Monitoreo de la Infraestructura

El Oferente deberá contemplar como parte de su servicio el monitoreo, alertas tempranas y alertas de SIEM, así como tomar las medidas necesarias para gestionar o corregir de manera proactiva aquellas situaciones en que se detecten comportamientos irregulares.

Es importante precisar que el servicio de Monitoreo deberá operar en régimen 7x24, donde cada día a las 8:00 am se enviará un informe con el estado de los servicios en operación. El contenido y formato del informe será entregado por ACHS al adjudicado.

El hardware requerido para la instalación de las herramientas de Monitoreo será provisto por ACHS. Será de responsabilidad del Oferente la configuración, administración, soporte y mantención de todas las herramientas requeridas para el monitoreo de la infraestructura objeto de esta licitación.

El Oferente deberá realizar el monitoreo de las Plataformas propuestas en su solución y deberá entregar credenciales de acceso al personal de ACHS, así como también, considerar un dashboard con al menos, los siguientes aspectos:

- Chequeo periódico del comportamiento de la plataforma 7x24.
- Detección de fallas en el flujo normal de los casos de uso.
- Detección, seguimiento y escalamiento de eventos.
- Recolección de Estadísticas.
- Generación de informes de uso de recursos.
- Informe a personal de ACHS de los eventos detectados.
- Responder consultas asociadas al estado de los servicios.
- Validación de servicios tras incidentes.

Se debe considerar el siguiente SLA:

Prioridad	Inicio de Análisis	Notificación a ACHS	Tiempo de Contacto a ACHS*
Alerta Crítica	15 Minutos	15 Minutos	30 Minutos
Alerta Alta	15 Minutos	15 Minutos	30 Minutos
Alerta Media	90 Minutos		
Alerta Baja	120 Minutos		

5.2.1.2 Mantenimiento Preventiva

La oferta debe contemplar los programas de mantenimiento preventivo para dar cumplimiento a los niveles de servicios definidos y detallados en las presentes bases técnicas (ver Anexo 4). La oferta debe indicar la periodicidad y las condiciones de las mantenciones preventivas, no siendo este inferior a una mantención anual de cada equipo.

Por otra parte, cada seis meses deberá realizar pruebas de la correcta operación de los sistemas que estén en modo activo-pasivo, tales como la característica de alta disponibilidad de los elementos con esta facilidad. Para esto, se entregará durante la etapa de implantación el calendario con las fechas de ejecución de dichas pruebas.

Durante esta etapa el Oferente deberá realizar una revisión de las configuraciones de los equipos y proponer su optimización. En particular, se espera que, durante el primer período de Mantenimiento Preventiva, las reglas de Firewalls sean analizadas para aplicación de mejoras.

Todas las actividades preventivas requieren de la respectiva coordinación previa con ACHS, y cada solicitud de mantención deberá ser informada con 48 horas de anticipación y siguiendo los procedimientos de control de cambios establecidos por ACHS.

Tras cada mantención preventiva, el Oferente deberá entregar un informe con los resultados de las actividades e informar las mejoras a implementar en las redes de ACHS.

5.2.1.3 Mantenimiento Correctiva

El servicio que se licita requiere atención ante incidentes que afecten su disponibilidad o desempeño. Los problemas detectados que requieran trabajos en sitio para su solución deberán ser coordinados con ACHS de forma previa, de acuerdo con los siguientes SLAs:

Prioridad	Tiempo de Respuesta	Tiempo de Conexión Remota	Tiempo de Visita Terreno
Crítico	30 Minutos	2 Horas	8 Horas
Alta	1 Hora	4 Horas	16 Horas
Media	8 Horas	10 Horas	N/A
Baja	16 Horas	NBD	N/A

Además, el Oferente deberá considerar:

- Poner a disposición de ACHS una plataforma de comunicación central (Mesa de Soporte) dedicada al control y gestión de todas los componentes de la solución. Esta plataforma cumplirá funciones de:
 - Capacidad de atención a problemas de primer y segundo nivel.
 - Punto único de entrada de los requerimientos escalados hacia los procesos del Oferente por parte del personal del ACHS.
 - Capacidad de abrir y cerrar tickets de manera automática y proactiva desde la mesa de soporte.
 - Atención inmediata de incidentes que afecten la disponibilidad o desempeño de los servicios.
- Ante un evento Urgente que afecte los servicios en operación, ACHS podrá solicitar una visita a terreno de personal técnico del Oferente. En el caso que el Oferente no envíe el personal, será considerado un incumplimiento.
- Control y seguimiento de los eventos escalados al Oferente y de aquellos de gestión propia y particular de la Mesa.
- Administración y gestión de los eventos generados por las distintas herramientas de apoyo y gestión de la plataforma, incluyendo monitoreo y sistema de correlación de eventos.
- Redacción y entrega de Procedimientos Técnicos de la revisión de servicios para el personal de la Mesa de Ayuda de ACHS.
- El Oferente deberá considerar un sistema de Tickets para el registro de casos que sean abiertos a la mesa.
- El Oferente deberá comprometer un procedimiento e informe destinado a la detección de eventos recurrentes. Sobre este aspecto, deberá realizar mensualmente un análisis de toda la información de eventos disponible en los sistemas, de modo que permita la detección de fallas reiterativas y así efectuar acciones correctivas. Deberá, para cada caso, proponer un procedimiento que permita realizar las mejoras necesarias que mantengan el nivel de servicio comprometido.
- Junto con la documentación de procedimientos de operación, el Oferente deberá contemplar una tabla de tiempos comprometidos para cada uno de ellos. Estos tiempos deberán ser auditables para el análisis de los cumplimientos.
- Los informes de fallas tendrán que ser entregados 24 horas corridas después del fin del incidente, haciendo un análisis de causa raíz. ACHS podrá solicitar un nuevo informe asociado a un incidente cuando lo estime necesario.

5.2.1.4 Requerimientos que debe Gestionar del SOC

Además de las mantenciones citadas en los párrafos precedentes, el Oferente deberá dar respuesta a los requerimientos solicitados por ACHS. Se deberá considerar:

- Realizar las configuraciones que ACHS solicite en los equipos de la solución. El Oferente deberá considerar que no existirá un límite en la cantidad de configuraciones a realizar en los equipos materia de esta licitación.
- El Oferente tendrá la responsabilidad de supervisar los procesos técnicos de implementación de nuevas facilidades o de crecimiento vegetativo de la plataforma, por lo tanto, deberá:
 - Mantener control del equipamiento que sea incorporado o remplazado en la plataforma.
 - Apoyar el proceso de instalación y actuar como interlocutor entre los responsables de ACHS.
 - Validar que nuevos elementos cumplan a cabalidad con los estándares comprometidos con ACHS.
- Labores de coordinación de las actividades habituales de operación y explotación de la plataforma.

El Oferente deberá considerar que cualquier cambio a realizar, en cualquier etapa del contrato, debe ser aprobado por ACHS a través del proceso de Control de Cambios establecido en la Gerencia de TI y cuyos detalles serán entregados al Adjudicado.

5.2.1.5 Reportes de Gestión de Servicios

El Oferente deberá entregar por escrito un completo Informe de Gestión de Servicios, de manera semanal y mensual, acompañado de las correspondientes estadísticas de servicio. Debe contener, a lo menos:

- Volumen de requerimientos e incidentes tanto abiertos y cerrados, como de solucionados y pendientes, de acuerdo con la clasificación de ACHS.
- Estadísticas de cumplimiento de “Niveles de Servicio”.
- Modificaciones de mejoras aplicadas al servicio entregado.
- Alertas informadas por el fabricante tales como: Cambio de estado (End-of-Sale, End-of-Support, otros.), vulnerabilidades que afecten a los equipos en operación, otros.
- Gestión de Capacidad (puertas disponibles, holgura de recursos, otros.).

- Otros que ACHS especifique.

Cada Informe de Gestión de Servicios deberá ser suscrito por el Gerente o el equivalente jerárquico que esté a cargo del Servicio por parte del Proveedor.

5.2.2 Analizador de Logs

Se requiere que el servicio de SOC contemple una herramienta tipo SIEM para el apoyo de la gestión de incidentes de seguridad en los equipos de la solución propuesta.

El servicio debe considerar:

- Administración por perfil de usuario.
- Almacenamiento centralizado de eventos.
- Almacenamiento de Bitácoras (log), manteniendo en línea al menos los últimos 6 meses e histórico por 5 años.
- Se deberá configurar la recolección de datos y eventos de los múltiples dispositivos que conforman las plataformas de seguridad de ACHS, con capacidad de detectar, mostrar tendencias y patrones. Las plataformas para soportar son las consideradas en este proceso.
- Generar procedimientos de creación, identificación, soporte de casos de uso y otros que aparezcan durante la vigencia del contrato.
- Análisis de seguridad en tiempo real por defecto (reglas, firmas, comportamientos, otros.) y análisis personalizados, en caso de que sea necesario.
- Despliegue de información de seguridad en vistas, en línea para ACHS.
- Generación de Informes y alertas personalizadas.
- Afinamiento y optimización continua de la analítica del sistema.

El Oferente debe entregar los detalles de las herramientas consideradas para la entrega del servicio.

5.2.3 Gestión de Eventos de Seguridad

ACHS requiere contar con un servicio especializado para la gestión de eventos de seguridad. Este servicio (basado en personal experto) debe considerar lo citado en los siguientes puntos.

5.2.3.1 Gestión del Servicio

La Gestión del Servicio debe considerar:

- Disponer de personal especializado para gestión de incidentes de Seguridad.
- Registrar toda acción relacionada con los eventos atendidos en un sistema de tickets.
- Escalamiento de eventos, incidentes y/o requerimientos hacia áreas y/o proveedores. Se espera que el proveedor de SOC realice la gestión sobre la mayoría de los casos que deben ser atendidos, lo que no debe superar el 20% de escalamiento.
- Coordinación permanente con las áreas y/o proveedores de ACHS.
- Definición de Plan de Mitigación de Incidentes de acuerdo a los RPO y RTO definidos por ACHS.
- Ejecución de Plan de Mitigación de Incidentes.
- Apoyo a la Coordinación de equipos de seguridad y redes para atender incidentes.
- Definir y aplicar un Protocolo de escalamiento de alertas para aprobación de ACHS.
- Construir y mantener el inventario de equipos y sistemas relacionados.
- Mantener la documentación relativa a cada implementación de los servicios materia de esta contratación.
- Generación de informes formales ante alertas críticas que posteriormente podrán ser enviados a quien ACHS determine.

El SOC será el encargado de monitorear la plataforma de seguridad y por lo tanto podrá recibir requerimientos de ACHS. Por otro lado, el SOC enviará constantemente información a ACHS asociada a la operación de las plataformas de seguridad y gestión de contratos con proveedores.

5.2.3.2 Análisis de Eventos

Para el análisis de eventos se debe considerar:

- Analizar cada evento recibido en el centro de operación y entregar el resultado del análisis a personal de ACHS.
- Proveer un servicio de inteligencia ante amenazas con conocimiento de la realidad mundial en materia de ciberseguridad, de modo de ser asesor en la materia para ACHS.
- Comprobación de vulnerabilidades.
- Detección y seguimiento de incidentes de Seguridad.
- Gestión del SIEM para análisis, priorización, correlación, reporte y alerta de los eventos que puedan poner en riesgo los activos de ACHS en modalidad 7x24.
- Estudio de vulnerabilidades procedentes de soluciones/productos en operación en la red de ACHS.
- Gestión de alertas informadas por fabricantes: recibir información y coordinar medidas correctivas o paliativas recomendadas.

- Debe cumplir con los siguientes SLAs:

Prioridad	Inicio de Análisis	Notificación a ACHS	Tiempo de Contacto a ACHS*
Alerta Crítica	15 Minutos	15 Minutos	30 Minutos
Alerta Alta	15 Minutos	15 Minutos	30 Minutos
Alerta Media	90 Minutos		
Alerta Baja	120 Minutos		

5.2.4 Equipo de Respuesta ante Incidentes (IRM)

Se requiere contratar servicios profesionales para implementar y operar un Servicio de Respuesta ante Incidentes de Ciber Seguridad en la infraestructura tecnológica según las políticas de ACHS, en las cuales se toma como referencia <https://www.csirt.gob.cl> . Específicamente, los servicios requeridos son:

- Definición del Plan de Respuesta ante Incidentes.
- Definición de Procesos y Procedimientos de respuesta para cada tipo de incidente.
- Gestión y control de los Procesos y Procedimientos de respuesta. Incluye análisis forense de incidentes de Ciberseguridad, en los casos que sea necesario.

Los Servicios deben estar basados en un equipo de profesionales tanto para generar la documentación, como ejecutar el control y gestión del Plan de Respuesta ante incidentes.

Será altamente valorado por ACHS si el Oferente considera en su propuesta una herramienta de Orquestación de Respuesta a Incidentes SOAR.

5.2.4.1 Documentación

El equipo a cargo del Servicio IRM deberá generar la documentación presentada a continuación:

- Plan de Seguridad y Respuesta ante Incidentes. Documento general basado en NIST 800-61 que establece las bases para la implementación del plan de respuesta ante incidentes.
- Procesos y Procedimientos de respuesta para cada tipo de incidente. Documentos específicos para cada tipo de incidentes, por ejemplo, Malware, Acceso No autorizado, Phishing, otros. Se debe considerar:
 - Categorización de los incidentes.

- ACHS definirá el orden en que deben ser abordados los tipos de incidentes según criticidad.
- Estos documentos deben considerar, al menos, lo descrito en la siguiente tabla donde, además, se presentan algunos ejemplos para cada etapa.

Etapa	Descripción
Preparación	<p>Definir pautas de comunicación: se debe contar con pautas de comunicación para permitir una comunicación fluida durante y después del incidente. Plan y caso de uso en cada tipo de incidente.</p> <p>Evaluar la capacidad de detección de amenazas: evaluar la capacidad actual de detección de amenazas y actualizar los programas de evaluación y mejora de riesgos.</p> <p>Coordinación de múltiples proveedores.</p>
Detección	<p>Supervisar: los eventos de seguridad deben ser supervisados en su entorno utilizando firewalls, sistemas de prevención de intrusiones y prevención de pérdida de datos.</p> <p>Detectar: prever posibles incidentes de seguridad correlacionando alertas dentro de la solución SIEM.</p> <p>Alertar: los analistas deben generar tickets de incidentes documentando los hallazgos iniciales y asignando una clasificación del incidente inicial.</p> <p>Informar: el proceso de informe debe realizarse según las políticas definidas por la organización.</p>
Identificación	<p>Determinar qué huellas puede haber dejado el actor de la intrusión.</p> <p>Reunir las evidencias necesarias para construir una línea de tiempo de actividades.</p> <p>Analizar una copia bit a bit de los sistemas, desde una perspectiva forense, para determinar qué ocurrió en un dispositivo.</p> <p>Analizar los sistemas existentes y las tecnologías de registro de eventos para determinar el alcance del compromiso.</p> <p>Documentar todas las cuentas, máquinas, otros. comprometidas para que se pueda realizar una contención y neutralización efectivas.</p>
Contención	<p>Se deben buscar los mecanismos para controlar el incidente considerando, al menos:</p> <p>Aplicar reglas en los componentes.</p> <p>Desconexión de equipos.</p>
Remediación	<p>Apagado coordinado: una vez que haya identificado todos los sistemas que han sido comprometidos dentro del entorno por un actor de amenazas, realizar un apagado coordinado de estos dispositivos. Se debe enviar una notificación a todas las áreas involucradas para garantizar el momento adecuado.</p>

	<p>Limpiar y reconstruir: limpiar los dispositivos intervenidos y reconstruir el sistema operativo desde cero. Cambiar las contraseñas de todas las cuentas comprometidas.</p> <p>Solicitudes de mitigación de amenazas: si se han identificado dominios o direcciones IP que los actores de amenazas aprovechan para el comando y el control, se deben realizar solicitudes de mitigación de amenazas para bloquear la comunicación de todos los canales de salida conectados a estos dominios.</p>
Recuperación	<p>Cambiar todas las contraseñas del sistema y cuentas. Luego, hacer que los usuarios lo hagan de manera segura según la política de cambio de contraseñas de la organización.</p> <p>Comprobar la integridad de todos los datos almacenados en el sistema.</p> <p>Restaurar todos los archivos que podrían haber sido modificados.</p>

Los procedimientos definidos deben ser “chequeados”. Esto es, simular la existencia del incidente y validar que todos los involucrados ejecuten las tareas que se han establecido. Las pruebas se realizarán una vez al año por tipo de incidente.

5.2.4.2 Control y Gestión

La documentación generada será distribuida entre los responsables al interior de ACHS, y el Oferente estará encargado de hacer el control de la ejecución de los procesos y procedimientos definidos para la gestión de Incidentes.

El Oferente deberá desarrollar, al menos, las siguientes actividades:

- Hacer seguimiento a la ejecución de los procesos y procedimientos de respuesta ante incidentes.
- Realizar el escalamiento en caso de no ejecución de los procesos y procedimientos.
- Apoyar a los responsables de la ejecución en los procesos y procedimientos.
- El servicio debe operar 24x7.

5.2.4.3 Gestión sobre incidentes

Ante un incidente, el SOC deberá informar a los involucrados en el proceso (unidades internas, proveedores, otros.) y el Oferente deberá analizar, validar y categorizar o re-categorizar el caso reportado (“Triage”).

Para los incidentes categorizados como “Críticos” en la etapa de documentación, el Oferente deberá liderar la gestión del incidente desde el inicio hasta su término. Esto considera:

- Convocar al comité de crisis.
- Informar al inicio y periódicamente sobre el estado del incidente.
- Establecer mesas de trabajo con las áreas que deban ser involucradas.
- Hacer seguimiento a la ejecución de los Procedimientos establecidos.
- Definir las actividades necesarias para dar respuesta al Incidente.
- Generar informes técnicos y ejecutivos.

Para los incidentes categorizados como No Críticos, el Oferente deberá realizar el seguimiento y controlar cada hito en los procedimientos establecidos. En caso de que los responsables no cumplan con lo establecido en los procedimientos, el Oferente deberá informar a las áreas que ACHS indicará oportunamente.

Se debe considerar los siguientes SLAs:

Prioridad	Inicio de Evaluación	Notificación a ACHS	Tiempo de Contacto a ACHS*
Alerta Crítica	15 Minutos	45 Minutos	45 Minutos
Alerta Alta	15 Minutos	45 Minutos	45 Minutos
Alerta Media	90 Minutos		
Alerta Baja	120 Minutos		

5.2.4.4 Análisis Forense

Desarrollar un Análisis Forense para los incidentes que ACHS indique, donde se redactará un informe del incidente que será distribuido entre todos los responsables que ACHS designe. Deben de describirse, al menos, los siguientes temas:

- Causa inicial.
- Acciones y líneas de tiempo de cada evento.
- Tareas exitosas y fallidas.
- Acciones para mejorar los procesos.

5.3 IMPLEMENTACIÓN DE SERVICIOS

En esta sección se definen los Servicios Profesionales asociados a la implementación de los servicios requeridos en esta licitación. Es importante hacer notar que en esta etapa de Implantación se adhiera a las mejores prácticas definidas en ITIL.

5.3.1 Gerenciamiento

Se requiere disponer de una estructura organizacional a cargo del gerenciamiento del proceso desde la implementación hasta la puesta en marcha de todos los servicios y componentes que forman parte del proyecto.

Se requiere conocer la estructura para la provisión de los servicios, considerando al menos los siguientes puntos:

- Diagrama jerárquico de la estructura Organizacional que provee los servicios.
- Roles en la organización y descripción de sus principales actividades asociadas al proyecto.
- Contactos y flujo de escalamientos Técnicos y Comerciales.

El Oferente entregará el nombre del Jefe de Proyecto con dedicación exclusiva, con su certificación PMI (Project Management Institute) o equivalente vigente y experiencia en proyectos similares, quien será la contraparte válida frente a ACHS durante todo el proceso de implementación del proyecto. Para ello, el oferente deberá entregar toda documentación que avale la experiencia del Jefe de Proyecto en la administración de proyectos de similar magnitud y características.

ACHS entiende que los roles técnicos considerados en el proyecto deben ser:

Roles del Proyecto
Jefe de Proyectos
Ingeniero PMO
Arquitecto de Ciberseguridad
Ingeniero de Proyecto Ciberseguridad

El Oferente en su calidad de experto podría modificar el listado detallando las funciones desarrolladas por cada rol.

5.3.2 Instalación y Configuración

El Oferente deberá generar un plan de implementación en el cual deberá detallar las actividades que realizará, acorde a los tiempos planificados por ACHS y recursos que requerirá para la puesta en funcionamiento al 100% los servicios a entregar.

5.3.2.1 Carta Gantt

El oferente deberá entregar una carta Gantt general y proponer un **Plan de Implementación y un plan de Migración** que contemple desde la situación actual hasta la futura, detallando las etapas y tiempos para la ejecución de cada una de ellas.

Si la propuesta llegara a ser seleccionada, se deberá actualizar de acuerdo con lineamientos ACHS la Gantt definitiva.

5.3.2.2 Plan de Implementación y de Migración

La presentación del proyecto debe considerar un Plan de Implementación y de Migración que contemple todos los servicios ofertados para la habilitación de cada servicio requerido mediante una carta Gantt.

El Oferente considerará:

- ACHS se reserva el derecho a observar y/o modificar el plan de implementación en consideración a atender sus prioridades.
- Durante el período de implementación y con periodicidad semanal, el Jefe de Proyecto del oferente deberá entregar información descriptiva al personal técnico de ACHS respecto de las actividades que se están llevando a cabo y del estado de avance del proyecto, indicando el grado de cumplimiento de cada una de las etapas planificadas.
- El Plan de Implementación deberá contemplar al menos las siguientes etapas (hitos) en su cuerpo: Importación y Distribución de Equipos, Instalación de servicios, Pruebas y Puesta en Operación.
- En caso de atraso en la llegada de equipos propuestos, el Oferente podrá justificar la situación con una carta de respaldo del fabricante y deberá instalar uno o más dispositivos que proveen las mismas funcionalidades y capacidades del equipo propuesto en la solución. Una vez que el equipo propuesto llegue tendrá un plazo de 30 días para su instalación.
- La etapa de implementación se dará por concluida una vez que el Oferente haga entrega formal de o los informes finales de implementación, de manera formal-corporativo y ACHS lo acepte sin observaciones.

El Oferente debe informar el plazo de habilitación de todos los servicios citados en estas Bases Técnicas completando en Anexo 3.

5.3.2.3 Ambiente Pre-Productivo

El Oferente deberá considerar la habilitación de un Ambiente de Pre-Producción donde todos los componentes de la solución sean probados. El ambiente será definido por ACHS y deberá considerar, al menos, lo siguiente:

- Utilizar los equipos que posteriormente se instalarán en la red de ACHS.
- La habilitación de las plataformas centrales consideradas en la solución.
- La generación de la Configuración Base de los equipos.

Durante esta etapa, el Oferente deberá desarrollar y entregar a ACHS documento de Ingeniería de Detalles, donde describa cada paso para la instalación y configuración de los componentes considerados en la solución.

Este documento deberá ser aprobado por ACHS y se convertirá en el procedimiento base para la habilitación de los servicios de conectividad solicitados.

5.3.2.4 Instalación de Componentes

El Oferente deberá realizar la instalación física de los equipos solicitados y deberá considerar todos los suministros para la puesta en marcha de los servicios. Así mismo, deberá considerar el retiro de los actuales equipos que están en operación en ACHS y entregarlos al responsable de su baja, el que será debidamente informado.

Dado que el período de habilitación de servicios puede ser extenso, las plataformas de servicios existentes y nuevos deberán coexistir. En consecuencia, se deben considerar los recursos necesarios (equipos, enlaces, ingeniería, otros.) para que ambas plataformas interoperen y permitan la operación normal de los servicios TI de ACHS.

Al final del proceso de instalación de servicios y durante todo el período de contrato, se debe contemplar la entrega de toda la información de los servicios provisionados considerando, al menos, un inventario de componentes (servidores, equipos, racks, cableado, otros.), diagramas topológicos y configuraciones, esquemas de flujos de tráfico esperado.

Se requiere que todos los equipos considerados en la solución sean instalados y configurados para la óptima operación de los servicios. Además, el Oferente debe considerar agregar

configuraciones a los equipos a solicitud de ACHS de manera ilimitada durante esta etapa y la de Operación de Servicios.

El Oferente deberá realizar la migración y optimización de configuraciones (reglas, listas de acceso, otros.) desde las actuales plataformas en operación a las nuevas propuestas en su solución. Además, deberá entregar en su oferta el método que utilizará para el proceso de migración.

5.3.2.5 Pruebas de Contingencia

Antes del inicio de los servicios en operación, el Oferente deberá desarrollar pruebas de contingencia con el objetivo de validar el correcto funcionamiento de todos los sistemas adjudicados, poniendo especial énfasis en características de alta disponibilidad y continuidad de la operación de los elementos considerados.

El plan de pruebas deberá ser presentado a ACHS con 30 días de anticipación y tras su aprobación podrá ser ejecutado en la fecha y hora que ACHS indique.

Así mismo, cada vez que un componente pase a producción, el Oferente deberá realizar las pruebas que correspondan e informar a la ACHS del resultado de estas para su aprobación.

5.3.3 Capacitación Técnica

Se requiere que el proceso de implantación y operación de proyecto incluya un programa de capacitación para el personal de la Gerencia de TI, en las distintas tecnologías que se habilitan.

El oferente deberá entregar el programa de capacitación que permita lograr el mejor nivel de especialización para todo el personal que ACHS designe.

El oferente deberá considerar:

- La capacitación debe estar estructurada a Personal Técnico (4 personas) designados por ACHS.
- La capacitación necesaria para que personal de ACHS pueda ejercer sus funciones de operación y ser contraparte técnica del adjudicado.
- Estas capacitaciones deberán ser desarrolladas por personal experto del oferente y serán ejecutadas en forma presencial o remota.
- Debe considerar 3 días (24 horas) abordando tópicos asociados a los componentes de la solución.
- Las sesiones podrán ser grabadas por ACHS para su posterior reproducción.
- Debe considerar la entrega de manuales de operación y soporte de los dispositivos.

Así mismo, el Oferente deberá considerar todo lo necesario (cursos y pruebas) para un mínimo de 2 ingenieros de ACHS puedan optar a certificaciones en la solución de seguridad propuesta.

5.3.4 Entregables

Al finalizar la etapa de implantación de Servicios, el Oferente deberá entregar los siguientes documentos:

- Memoria Técnica con los detalles del proyecto.
- Evidencia de cumplimiento de todas las solicitudes indicadas en estas Bases.
- Material de Capacitación Técnica.
- Informe de mejoras a realizar en los sistemas de Firewalls.

5.3.5 Garantía de Implementación del Proyecto

Se establece un período de garantía de tres (3) meses, a partir de la recepción conforme de la implementación del último de los servicios. Esta garantía cubre los defectos de instalación de acuerdo con la evaluación y calificación que realizará cada una de ACHS.

En caso de que se detecte un defecto de instalación el proveedor contará con un plazo máximo de tres días hábiles para darle solución a partir de la fecha de la notificación formal a ACHS, quedando extendido la garantía por igual período, a contar de la fecha de solución del inconveniente que motivó el reclamo. El periodo de garantía de implementación deberá ser incorporado en la Carta Gantt y de Cumplimiento de Hitos que formará parte integrante del Contrato.

5.4 OPERACIÓN DE LOS SERVICIOS

A continuación, se describen los servicios profesionales que sostienen la continuidad operativa de la solución durante el régimen normal de servicios. Al respecto, se requiere contar con soporte para todo el hardware, software y todo elemento que forme parte de la solución de servicios.

5.4.1 Gobierno de Servicios

Se requiere disponer de la estructura organizacional a cargo del gerenciamiento del proceso de Operación Continua de todos los servicios y componentes que forman parte del proyecto.

Se requiere conocer la estructura para la Operación de los servicios, considerando al menos los siguientes puntos:

- Modelo de Servicios.
- Diagrama jerárquico de la estructura Organizacional.
- Roles en la organización y descripción de sus principales actividades.

El Proveedor deberá definir en su oferta un Protocolo de Coordinación y Control Permanente de los equipos y servicios contratados con ACHS, que redunde en una administración eficiente y eficaz de estos mismos. Dicho Protocolo de Coordinación y Control de Servicios deberá incluir entre otros aspectos:

- Entrega periódica y regular de Informes de Gestión de Servicio a definir con ACHS, incluyendo el control de cumplimiento de los niveles de servicio.
- Esquema de coordinación regular y permanente de los servicios otorgados, incluyendo requerimientos especiales o actividades específicas no cubiertas dentro del presente proceso, pero vinculadas a la configuración de equipos, partes y piezas.
- Esquema de escalamiento de problemas en casos del incumplimiento parcial o total de los servicios contratados, así como de casos conflictivos.
- Definición y descripción de los flujos de trabajo desde ACHS hacia el Proveedor y viceversa para el traspaso regular y permanente de los requerimientos de servicio.

5.4.2 Supervisor de Servicio

El Proveedor debe designar un Supervisor del Contrato con las competencias y experiencia necesarias para la supervisión de un contrato de provisión de equipamiento y garantías. Esto incluye la supervisión tanto del personal del proveedor encargado de las actividades de logística, configuración, servicio técnico y programación de entregas como de la supervisión del contrato de aprovisionamiento de equipamiento y gestión de garantías.

Como parte de la oferta del proveedor, debe hacer llegar los antecedentes profesionales de la persona designada para el cargo, los que serán visados por la ACHS. En caso de cambio del profesional su reemplazo debe ser visado por la ACHS previa revisión de sus antecedentes profesionales.

5.4.3 Estructura de Gestión y Supervisión de Servicios

Respecto de condiciones contractuales de coordinación entre las partes, tanto el proveedor como ACHS designarán sus respectivos Administradores de Contrato de Servicio.

En las labores de supervisión y coordinación de los servicios contratados, el Administrador de Contrato de ACHS podrá instruir al Oferente, en caso de que sea necesario, para que adopte acciones correctivas tendientes al cumplimiento de los requerimientos y niveles de servicio contratados.

Respecto a las coordinaciones funcionales, el Supervisor del Servicio del Oferente interactuará con la contraparte válida definida por ACHS para tratar los temas específicos de las presentes Bases, con los niveles de autoridad que permitan asegurar la entrega de los servicios comprometidos.

5.4.4 Esquema de Escalamiento

El Proveedor deberá indicar en su propuesta de operación, la información de escalamientos funcionales, indicando desde los niveles de soporte hasta los niveles gerenciales del proveedor.

Dicha propuesta de acciones deberá contemplar los pasos a seguir desde el reporte o reclamo a nivel del Supervisor del Servicio, los Administradores del Contrato designados por las partes (el Proveedor y ACHS) y los niveles gerenciales en caso de ser requerido. Además, debe incluir indicación de las responsabilidades.

Cambios temporales y/o permanentes de las personas en la cadena de escalamiento deben ser informados por escrito a la ACHS con un máximo de 48 horas corridas luego de definido el mismo.

5.4.5 Reuniones de Trabajo y Revisiones

Durante la vigencia del contrato, los Administradores del Contrato de Servicio efectuarán reuniones periódicas para revisar la marcha de la prestación de servicios del Proveedor a ACHS.

Estas reuniones se efectuarán normalmente en oficinas de ACHS, se llevará un acta de los puntos y acuerdos tratados y se analizarán los informes de gestión de servicio presentados por el Proveedor contratado, como también los temas planteados por las partes.

La periodicidad de las reuniones regulares se ajustará de acuerdo con la marcha del contrato provisión y servicios. Sin perjuicio de lo anterior y, a requerimiento de una de las partes, se podrán efectuar reuniones extraordinarias en la medida que las circunstancias lo ameriten y ACHS lo acepte.

5.5 MANTENIMIENTO DE COMPONENTES

5.5.1 Upgrades y Updates

Durante la operación de los servicios requeridos, se debe contemplar que todo el equipamiento siempre debe operar con la última y más estable versión de componentes firmware, software y/o sistema operativo, de acuerdo con las recomendaciones del respectivo fabricante.

Al respecto, se debe disponer inmediatamente de personal experto designado por el proveedor en un plazo máximo de 72 horas corridas, desde la fecha de publicación en boletín/web del fabricante, para su atención y ejecución de un protocolo que considere, al menos:

- Descripción del problema (bug o vulnerabilidad y codificación).
- Reporte del fabricante (URL).
- Identificación de elementos afectados (HW, Firmware, SW, OS).
- Identificación del parche que se aplicará (si existe).
- Procedimiento para la aplicación del parche.
- Tiempo requerido para aplicación de parche.
- Forma de solución parcial o alternativa (workaround).
- Procedimiento vuelta atrás (rollback).

Además, el Oferente deberá enviar un reporte trimestral con la información del estado del firmware, software y/o sistema operativo de los equipos de la solución.

5.5.2 Plan de Continuidad y Contingencia

El adjudicado es responsable de evaluar el nivel de seguridad de los servicios entregados, dar garantía necesaria para proteger los recursos asignados a la prestación de los servicios contratados y proponer los procedimientos para recuperación de los servicios prestados a ACHS ante desastres.

ACHS, se reserva el derecho de auditar, por cuenta propia o de terceros, contratación de personal para estos fines, los cuales deberán ser pagados por el adjudicado.

ACHS, en tanto, requiere que el Oferente presente un plan de continuidad que responda a todos los aspectos de la prestación y operación de los servicios requeridos en el presente contrato. También es necesario establecer cómo dichos servicios se restaurarían en caso de una falla mayor del servicio, brechas de seguridad con acceso indebido a aplicaciones y datos, en caso de desastre en las instalaciones del Oferente o por indisponibilidad de personal del Oferente asignado al servicio.

Un borrador inicial de dicho plan debe ser entregado como parte de la Propuesta del Oferente en respuesta a esta invitación a postular por los Servicios.

Será responsabilidad del Oferente implementar dicho Plan de Contingencia tras la aprobación de ACHS, así como de tomar todas las medidas necesarias para asegurar el cumplimiento de la continuidad operacional del servicio de acuerdo con los lineamientos generales que se indican a continuación.

El objetivo del Plan de Contingencia es definir y regular las acciones que permitan mantener la continuidad operacional de los servicios ante una contingencia en el Servicio adjudicado por ACHS respecto a la provisión de equipos y servicios asociados.

El alcance del Plan de Contingencia es administrar de forma eficiente las acciones que permitan recuperar, en el plazo definido en los SLAs, todos los recursos destinados a la provisión de equipos y entrega de los servicios para los tipos de riesgos definidos en la presente cláusula. Todo cambio de alcance deberá ser evaluado dentro de los requisitos establecidos en las presentes Bases y de los documentos que forman parte del proceso de invitación a presentar ofertas.

El Administrador de Contrato del Oferente deberá liderar el Equipo de Trabajo del Plan de Contingencia, particularmente por su rol de administrador y responsable de rendir cuentas por las operaciones del servicio global.

El Plan de Contingencia se aplica bajo las siguientes condiciones:

- **Desastres Ambientales:** Incendio, Terremoto, Inundaciones u otros que afecten las instalaciones del Oferente o de las instalaciones de sus servicios técnicos.
- **Interrupción Organizada o Deliberada:** Huelga del personal del Oferente, Quiebra o Huelga de las Empresas Sub-Contratistas del Oferente prestadoras de servicios u otros.
- **Interrupción en el Suministro de Servicios Públicos:** Cortes de Energía, transporte u otros.
- **Ausencia de stock de repuestos:** Falta de repuestos para efectuar las reparaciones a los equipos por un tiempo mayor a dos semanas.

Estas condiciones afectan a la operación de los servicios y en caso de incumplimiento de los niveles de servicios definidos se aplicarán las penalidades establecidas en el Anexo 4.

5.5.3 Gestión de Capacidad de Servicio

El Oferente será responsable de generar un informe sobre la Capacidad del Servicio, de tal forma que se vea respaldado por una capacidad de proceso y atención suficientemente dimensionada. La correcta Gestión de la Capacidad de los recursos permitirá cumplir con los niveles de servicio y procedimientos establecidos para la entrega de servicio establecidos entre ACHS y el Oferente.

Esto asegurará la provisión adecuada de recursos y las inversiones en recursos humanos, infraestructura de hardware y software necesarios, junto a los enlaces de comunicación que deberá suministrar el Oferente para conectarse con los sistemas de ACHS.

Además, considerará su mantenimiento y administración, evitando la degradación en la atención e incumplimiento de los niveles de servicio. Entre las responsabilidades de la Gestión de la Capacidad de servicio se encuentran:

- Ha de asegurarse que se cubren las necesidades de capacidad requeridas.
- Controlar el rendimiento de los recursos asociados al servicio.
- Desarrollar planes de capacidad para anticipar demandas futuras específicas o permanentes asociadas a los niveles de servicio acordados.
- Gestionar y racionalizar la demanda sobre la utilización de los recursos.
- Este informe deberá ser entregado cada seis (6) meses.

5.5.4 Garantías y Mantenimiento

Se debe considerar que todo el equipamiento ofertado cuente con las debidas garantías contra defectos, fallas de fabricación o fallas de funcionalidad por el período de duración del contrato.

Se establece un período de garantía de tres (3) meses, a partir de la recepción conforme de la implementación del último de los servicios. Esta garantía cubre los defectos de instalación y equipamiento de acuerdo con la evaluación y calificación que realizará cada una de ACHS.

En caso de que se detecte un defecto de instalación el proveedor contará con un plazo máximo de tres (3) días hábiles para darle solución a partir de la fecha de la notificación formal a ACHS, quedando extendido la garantía por igual período, a contar de la fecha de solución del inconveniente que motivó el reclamo.

El período de garantía de implementación deberá ser incorporado en la Carta Gantt y de Cumplimiento de Hitos que formará parte integrante del Contrato.

En su defecto, que existan procedimientos que permitan la reposición del Hardware, Software o servicio en caso de falla, de acuerdo con SLA que se defina. Para estos efectos, se requiere de los servicios de gestión de garantías y mantenimiento.

5.5.5 Plan de Devolución

Antes de finalizar el contrato, el Oferente estará sujeto a las exigencias siguientes:

- Actualizar toda la documentación técnica, específicamente 120 días antes de la fecha de término, en especial los diagramas de las redes, inventario de servicios detallando equipos y sus características relevantes, como capacidades y estadísticas de su desempeño, entre otros. Esta información debe ser de la granularidad que permita ser procesada por ACHS a nivel de red y de servicio individual y en formatos editables (planillas Excel, gráficos editables, planos, diagramas). Toda esta documentación deberá ser nuevamente actualizada al momento de traspasar los servicios a un nuevo proponente, si corresponde.
- Finalizar a entera satisfacción de ACHS todos los requerimientos que se encuentren vigentes, específicamente 90 días antes de la fecha de término.

Por último, el prestador actual del servicio deberá coordinarse y facilitar las actividades con ACHS y con el eventual nuevo prestador, para la migración de los servicios.

5.6 EXPERIENCIA DEL PROVEEDOR

5.6.1 Experiencia de la Empresa

Es requisito esencial que ACHS pueda comprobar la experiencia del Oferente en proyectos de similar o mayor envergadura utilizando la misma tecnología ofrecida para cada servicio.

Al respecto, se solicita que los Oferentes acrediten su experiencia señalando explícitamente la cantidad de servicios que cumplen con lo relacionado en estas bases, efectuando una breve descripción de sus alcances e identificando la empresa o institución. A esto se le debe adjuntar uno o más contactos decisivos que tengan o hayan tenido participación directa sobre el servicio en cualquiera de sus fases.

ACHS se reservará el derecho de efectuar las comunicaciones necesarias con estos clientes y el o los contactos informados por el Oferente, con el objetivo de obtener una evaluación del servicio y cumplimiento de compromisos.

Se contabilizará el número de proyectos de este tipo terminados en los últimos tres (3) años y aquellos vigentes que hayan sido adjudicados en el período mencionado. La información deberá ser entregada conforme a la tabla contenida en los Anexo Técnicos.

Así mismo, el Oferente deberá informar en su propuesta Técnica las certificaciones de Ciberseguridad del tipo ISO27002 o similar vigente con las que cuenta la empresa al 1 de febrero de 2022.

El Oferente deberá completar todos los campos solicitados en los Anexos y ACHS podrá contactar a los responsables en cada cliente citado en el Anexo.

5.6.2 Experiencia del Equipo

El oferente debe garantizar la idoneidad del personal que efectuará los servicios requeridos por ACHS. El personal deberá acreditar experiencia y casos de éxitos previa en plataformas de Firewalls y Balanceadores, CDN y WAF presentadas en su solución completando la tabla contenida en los Anexos Técnicos.

5.7 NIVELES DE SERVICIOS

5.7.1 Definiciones

Los Niveles de Servicio corresponden al acuerdo formal entre el Oferente del servicio y ACHS en donde se definen los métodos de cálculo para el cumplimiento de los Indicadores Clave de Servicio. Estos se basan en los datos registrados en los Tickets que se generan en el sistema Administración de Servicios que utiliza ACHS para el manejo de servicios y equipos.

Cada Indicador de Servicio tiene una meta única establecida, en la cual se indica el porcentaje mínimo de cumplimiento o cantidad máxima que se debe considerar.

El indicador de cumplimiento es comparado contra esta meta única, con lo que se logra establecer si el servicio está cumpliendo con la meta definida y su incumplimiento corresponde aplicar la multa establecida.

Las ofertas deben aceptar las exigencias de Niveles de Servicio que se definen y que tienen el propósito de asegurar la continuidad de operaciones de ACHS.

Los Niveles de Servicio han sido clasificados de la siguiente manera: Disponibilidad, Reposición, Atraso e Incumplimiento.

Definiciones generales:

- La disponibilidad se refiere a la circunstancia de estar operativo un servicio. Se mide en porcentaje de operación mensual.
- La Reposición se refiere a los tiempos para el reemplazo o reparación de equipos, enlaces o servicios. Se miden en horas.
- Atraso se refiere a los días de atraso en entrega de servicios.
- Incumplimiento se refiere a la falta en algún compromiso del Oferente, por ejemplo, la entrega fuera de plazo de algún informe, no aplicación de upgrade de acuerdo con el plan, otros.

Las referidas situaciones comenzarán a contarse desde el momento en que se detecta la falla o situación particular.

5.7.2 Calidad de Servicio

El oferente, adicionalmente a garantizar los niveles de servicios indicados anteriormente, deberá considerar en su propuesta las herramientas o medidas necesarias para garantizar que las perturbaciones que puedan ocurrir en el tiempo no sean perceptibles por los usuarios de negocio.

Cabe destacar, que es posible que existan perturbaciones en el tiempo, pero ACHS espera que estas sean imperceptibles por los usuarios ACHS.

Para ello se espera que el oferente tome medidas preventivas y proactivas, y que además este midiendo constantemente el estado de la infraestructura, buscando que esté en una condición óptima de funcionamiento. Se espera que todas estas mediciones preventivas y proactivas le permitan al oferente tomar las acciones necesarias para mitigar las eventuales perturbaciones a un nivel que no sean perceptibles por los usuarios.

Dichas perturbaciones, deberán catalogarse de la siguiente forma:

N°	Categoría	Tiempos	Multas
1	Insignificante	Menor de 15 Segundos	Constancia
2	Menor	menor a 30 segundos	Constancia
3	Moderado	Entre 1 a 3 minutos	Constancia
4	Mayor	Entre 5 a 9 minutos	Constancia
5	Catastrófico	Mayor a 10 minutos	10 UF por cada 10 minutos

ACHS podrá realizar encuestas de satisfacción de calidad de servicio a sus usuarios de negocio, y en el caso de contar con resultados insatisfactorios, espera que el oferente pueda participar y proponer mejoras ya sea en la medición, como también en la solución de problemáticas que puedan ser declaradas.

5.7.3 SLA de Monitoreo de Seguridad

Los SLAs definidos para el servicio de Monitoreo de Seguridad se indican a continuación:

Actividad	Horario	SLA
Monitoreo de alertas de Seguridad en pantalla	7X24	Monitoreo permanente
Inicio de evaluación de alerta en pantalla	7X24	15 minutos después de aparición de alerta en pantalla
Notificación de alerta a cliente	7X24	30 minutos máximo después de inicio de evaluación de alerta en pantalla
Inicio de contacto a cliente frente a alerta	7X24	30 minutos máximo después de inicio de evaluación de alerta pantalla
Cierre de casos abiertos	5x10	2 días hábiles después de reportado el incidente si no ha habido actividad adicional o el cliente no ha dado información adicional

5.7.4 SLA de Administración

Se define como tiempo de respuesta para atención a solicitudes, al transcurrido entre el contacto por parte del equipo de ACHS vía email o teléfono y el primer contacto por parte del Proveedor para catalogar el requerimiento o para solicitar más información que permita ejecutar el requerimiento en forma remota.

A continuación, se indican los SLAs según la clasificación del requerimiento:

Actividad	Horario	SLA
Atención de requerimiento de cambio de configuración	5 x 10	30 minutos máximo desde la recepción del requerimiento para coordinación de actividades
Atención de requerimiento de cambio de configuración	Horario extraordinario	45 minutos máximo desde la recepción el requerimiento para coordinación de actividades
Respaldos de configuración	5 x 8	Una vez a la semana (Semanal)
Reporte Nativo	5x10	24 hh hábiles es el plazo de entrega.

Reporte Procesado	5x10	Cliente contará con 24 hh anuales, no acumulables, para la configuración de estos reportes.
--------------------------	------	---

5.7.5 SLA de Monitoreo de Disponibilidad

Para los dispositivos administrados por el Proveedor, las variables mínimas que serán monitoreadas (según la plataforma) son:

Variable	Umbral
Uso de CPU	>90% durante más de 4 minutos
Memoria RAM	>90% utilizado
Espacio en Disco	>90% utilizado
Disponibilidad de red (ICMP)	Pérdida de ICMP (ping) por 4 minutos continuos
Disponibilidad de Servicios (ej: HTTP / FTP / DNS)	Pérdida de servicio en el port tcp por más de 4 minutos

Nota: Las variables dependerán del dispositivo y sus capacidades.

El sistema debe generar alertas cuando se sobrepasan los umbrales definidos para cada una de estas variables.

Se definirá como tiempo de respuesta para atención a incidentes de disponibilidad, al transcurrido entre la detección del incidente de disponibilidad y el contacto por parte del Proveedor con los contactos informados por ACHS.

Los tiempos de respuesta dependerán del SLA que hace parte del servicio según SLAs definidos para el servicio.

Características	Horario	SLA	Actividades Involucradas
Notificación de caída de dispositivo	7x24	Notificación hasta 45 min una vez caído	Notificación de alertas: 15 min: Recolección agente 15 min: Evaluación y pruebas manuales. 15 min: Notificación a ACHS

5.7.6 SLA Disponibilidad del Servicio

El servicio tendrá la siguiente disponibilidad comprometida:

Servicio	Horario	SLA
Servicio de monitoreo	7x24	99,9% uptime en base mensual
Servicio SOC	7x24	99,9% mensual de disponibilidad

5.7.7 SLA de Eventos Almacenados de Monitoreo

El Proveedor deberá almacenar los eventos recibidos como parte del servicio Gestión de Logs y los eventos correlacionados generados por la plataforma.

ACHS podrá solicitar evidencia de eventos de un período específico y por una ventana de tiempo, origen, destino y usuario, según sea el caso. El tiempo de respuesta para estas solicitudes queda directamente relacionado con la ventana de tiempo solicitada, lo que se detalla en la siguiente tabla:

Aspecto del servicio	SLA
Días de almacenamiento de eventos	30 días corridos
Entrega de logs en ventana < a 1 hora	3 horas
Entrega de logs en ventana 1 y 4 horas	6 horas
Entrega de logs en ventana >a 4 horas	24 horas
Máxima ventana de tiempo a solicitar	24 horas

5.7.8 SLA de Gestión de Fallas

Se define las siguientes situaciones:

Requerimientos o incidentes de Nivel 1: el servicio primario está detenido o fue gravemente perjudicado

Requerimientos o incidentes de Nivel 2: se puede seguir operando con tiempos de respuesta disminuidos para los servicios configurados

Actividad	Cobertura	Horario	SLA
Inicio de atención de requerimientos de soporte Nivel 1 y Nivel 2	Cualquier zona	7x24	Máximo 30 minutos después de recibido el incidente
Diagnóstico remoto requerimientos Nivel y Nivel 2	Cualquier zona	7x24	Máximo 1 hora después de atendido el requerimiento
Vista a terreno requerimiento soporte Nivel 1	Zona Urbana Santiago	5x10	Máximo 2 horas después de realizado el diagnóstico
Vista a terreno requerimiento soporte Nivel 1	Zona Urbana Santiago	Horario extraordinario	Máximo 3 horas después de realizado el diagnóstico

Actividad	Cobertura	Horario	SLA
Vista a terreno requerimiento soporte Nivel 1	Zona Urbana Santiago	5x10	Máximo 1 horas más tiempo de traslado hasta locación del cliente después de realizado el diagnóstico
Vista a terreno requerimiento soporte Nivel 1	Zona Urbana Santiago	Horario extraordinario	Máximo 3 horas más tiempo de traslado hasta locación del cliente después de realizado el diagnóstico
Vista a terreno requerimiento soporte Nivel 2	Zona Urbana Santiago	5x10	Máximo 4 horas después de realizado el diagnóstico
Vista a terreno requerimiento soporte Nivel 2	Zona Urbana Santiago	Horario extraordinario	Vista en terreno, máximo 6 horas después de realizado el diagnóstico
Vista a terreno requerimiento soporte Nivel 2	Zona Urbana Santiago	5x10	Máximo 4 horas más tiempo de traslado a locación del cliente, después de realizado el diagnóstico
Vista a terreno requerimiento soporte Nivel 2	Zona Urbana Santiago	Horario extraordinario	Máximo 6 horas más tiempo de traslado a locación del cliente, después de realizado el diagnóstico
Recambio de HW (aplica si hay soporte de HW como servicio)	Zona Urbana Santiago	5x10	Máximo 4 horas después de iniciada la atención del requerimiento
Recambio de HW (aplica si hay soporte de HW como servicio)	Zona Urbana Santiago	Horario extraordinario	Máximo 5 horas después de iniciada la atención del requerimiento
Recambio de HW (aplica si hay soporte de HW como servicio)	Zona Urbana Santiago	5x10	Máximo 5 horas más tiempo de traslado a locación del cliente después de iniciada la atención del requerimiento
Recambio de HW (aplica si hay soporte de HW como servicio)	Zona Urbana Santiago	Horario extraordinario	Máximo 6 horas más tiempo de traslado a locación del cliente después de iniciada la atención del requerimiento

5.7.9 SLA de Mantenimiento Preventivo

La instalación de parches, updates y mantenencias preventivas se podrán realizar en forma remota. Se debe entregar reportes o evidencias, con los siguientes SLAs:

Actividad	Descripción	Entregable	SLA
Mantenencias preventivas	Mantenición física y lógica de las plataformas del cliente descritas en la presente propuesta	REPORTE. Incluye: Cliente final, quién recibió la mantención, ingeniero a cargo, fecha, hora, equipos revisados y tareas realizadas.	1 vez por año
Instalación hotfix o update crítico	Update requerido para la estabilidad del sistema o para parche de vulnerabilidad crítica	REPORTE. Incluye: Fecha, hora, ingeniero a cargo, quien recibió, detalle de las	Dentro de los tres días su aparición

Actividad	Descripción	Entregable	SLA
		actividades realizadas y nombre de quién recibió la conformidad.	
Instalación hotfix o update no crítico			Hotfix no crítico: en mantenencias preventivas
Upgrade	Sujeto a disponibilidad de una nueva versión desde el fabricante, capacidad y compatibilidad en la plataforma del cliente para soportarlo.	REPORTE. Incluye: Cliente final, quién recibió la mantención, ingeniero a cargo, fecha, hora, equipos revisados y tareas realizadas.	Una vez al año durante mantenencias preventivas

5.7.10 Consideraciones de Niveles de Servicio

El oferente debe considerar los siguientes aspectos:

- No se considerará indisponibilidad cuando la interrupción sea atribuible a ACHS.
- El servicio esta indisponible cuando no están operativos los componentes primarios ni secundarios.
- El Oferente deberá disponibilizar vía web, un dashboard con la información acumulada detallando las fallas por condición de Indisponibilidad, Reposición, Atraso o Incumplimiento para cada evento y con capacidad de hacer drill down.
- El oferente debe disponibilizará vía web un dashboard indicando el problema y la solución para cada uno de los eventos.

5.7.11 Cálculo de la Disponibilidad de los Servicios

Para el cálculo del porcentaje de disponibilidad del servicio adjudicado, se considera el total de minutos sin servicio respecto del total de minutos que contiene el mes a evaluar, tal y como se indica a continuación:

$$Dm (\%) = (1 - (Ti/Tm)) * 100$$

Donde:

- “Dm” es el porcentaje de la disponibilidad mensual.
- “Ti” es el total de minutos de indisponibilidad del servicio para el mes evaluado.
- “Tm” es el total de minutos del mes evaluado.

La disponibilidad de los servicios se medirá mensualmente con un máximo de 720 horas.

5.7.12 Penalidades

El no cumplimiento de las condiciones indicadas, facultarán a ACHS a las sanciones administrativas que se establecen en estas Bases. Cabe señalar que gran parte de las condiciones indicadas tienen por objetivo minimizar las situaciones de falla e indisponibilidad de los servicios.

En caso de que el Oferente no cumpla con los Niveles de Servicio establecidos, se aplicarán las penalidades indicadas en la sección de multas y del Anexo 4. En el caso de duplicidad de multa para una misma variable, se aplicará la de mayor valor.

6 MULTAS

ACHS podrá aplicar multas que se indican en los siguientes numerales. En todo caso su aplicación estará sujeta a las siguientes normas:

- Las multas que corresponda aplicar se establecerán como resultado del incumplimiento de los plazos de puesta en operación, **por lo tanto, para la fecha comprometida en la carta Gantt final, el adjudicado deberá tener para cada uno de los servicios, completamente instalados, operativos y aprobados formalmente por ACHS.**
- La aplicación de multas al proveedor será notificada por escrito y/o vía correo electrónico.
- El proveedor tendrá un plazo único de máximo 10 días corridos desde que se le notifique la aplicación de la multa, para formular por escrito sus descargos y acompañar todos los antecedentes en que ellos se funden.
- ACHS analizará los descargos formulados por el proveedor y en el plazo de máximo de 15 días hábiles de recibidos le notificará por escrito y/o vía correo electrónico, su decisión de mantener las multas impuestas, reducirlas o dejarlas sin efecto.
- Si ACHS resolviere la aplicación de la multa, estas se harán efectivas mediante vale vista, retenciones de pagos pendientes o mediante el cobro de las garantías que se contemplan en el contrato; todo ello a criterio exclusivo de ACHS.

6.1 Multas por Atrasos en la Entrega de los Servicios

El proveedor de servicios deberá dar cumplimiento a los plazos establecidos en el contrato para la entrega de los servicios operando en óptimas condiciones de funcionamiento. Se aplicarán las siguientes multas en caso de que se produzcan atrasos atribuibles al proveedor:

Días corridos de atraso de puesta en servicio	% de la multa asociado a la renta mes del servicio
1-3	15%
4-15	50%
16-30	100%
Mayor a 30	130%

Superado el plazo de 45 días corridos de la fecha comprometida de puesta en servicio, ACHS podrá a su criterio y elección poner término unilateralmente a la totalidad de los servicios contratados o a aquellos que no hayan sido entregados en correctas condiciones de funcionamiento, los que podrán ser asignados a otro proveedor de servicios sin ningún costo para ACHS.

6.2 Multas por Indisponibilidad Mensual

En caso de excederse los índices mensuales de indisponibilidad máximos especificados en estas Bases, se aplicará una multa equivalente a 3 UF por hora o fracción por cada sitio afectado cuyo SLA no se cumpla.

Es decir, si un sitio tiene como límite un tiempo de indisponibilidad máximo de 2 horas y es afectado durante 2,5 horas, la multa será 3 UF.

Asimismo, en caso de fallas masivas de servicios, es decir, que dos o más servicios fallan en forma simultánea por una causa común, se aplicará una multa si la sumatoria del tiempo de indisponibilidad de cada uno de los servicios fallados es mayor a 2 horas y 10 minutos, siendo la multa equivalente a 3 UF por cada servicio que fue parte de la falla masiva.

Con todo, si durante 2 meses consecutivos o 3 meses no consecutivos en un período de 12 meses: (i) un mismo servicio contratado registrare una indisponibilidad mensual igual o superior al doble del nivel máximo convenido; o, (ii) un 5% o más de los servicios contratados excediese el nivel máximo de indisponibilidad mensual permitido, cualquiera sea la magnitud del exceso; dará derecho a ACHS para poner inmediato término al Contrato o a uno o más de los servicios contratados, sin perjuicio de la aplicación de las multas correspondientes con arreglo a esta cláusula.

Las multas y/o penalidades establecidas no serán aplicables cuando el Proveedor acredite suficientemente que el incumplimiento que las ha originado ha provenido de caso fortuito o fuerza mayor, en los términos previstos en el artículo 45 del Código Civil.

6.3 Multas por Facturación No Oportuna

La facturación no oportuna dentro de los primeros 5 días de cada mes, sin notificación formal por parte del proveedor que justifique tal atraso, será causa de una multa del 5% del monto total de la factura.

7 PROPUESTA ECONÓMICA

Las propuestas deberán indicar el MONTO DETALLADO y TOTAL por cada uno de los ítems y servicios correspondientes solicitados por ACHS. El monto de la propuesta deberá estar expresado en **UF incluyendo el IVA**.

Cabe señalar que la ACHS podrá solicitar al Proveedor seleccionado, servicios adicionales o extraordinarios a los requerimientos contratados, lo cual deberá ser realizado a través de la Contraparte en la Gerencia de Servicios Tecnológicos de ACHS, para proceder con la generación de la Orden de Compra respectiva.

El Proveedor participante financiará todos los costos relacionados con la preparación y presentación de su propuesta, por lo que ACHS, no será responsable en caso alguno de ellos.

La propuesta deberá incluir contrato tipo con sus cláusulas de salida anticipada para ser analizado con nuestra área legal.

Para efectos de estandarizar los formatos de propuestas se solicita que los proveedores resuman los precios de su Oferta de Servicio, tomando como referencia el Anexo 6, en base a lo siguiente:

- 1- Suministro, instalación y configuración de **Infraestructura de Firewalls, CDN y Balanceadores de Carga**. Valor detallado en UF incluyendo IVA. ***Se tomará en cuenta la totalidad de todos los servicios asociados a los ítems contenidos en estas bases técnicas.***
- 2- Suministro, instalación y configuración de **Web Application Firewalls (WAF)**. Valor detallado en UF incluyendo IVA. ***Se tomará en cuenta la totalidad de todos los servicios asociados a los ítems contenidos en estas bases técnicas.***

- 3- Servicio y Soporte por 3 y 5 años de **Security Operation Center (SOC) – Administración y Gestión**. Valor detallado en UF incluyendo IVA. ***Se tomará en cuenta la totalidad de todos los servicios asociados a los ítems contenidos en estas bases técnicas.***
- 4- Servicio y Soporte por 3 y 5 años de **Security Operation Center (SOC) – Analizador de Logs y Gestión de Eventos**. Valor detallado en UF incluyendo IVA. ***Se tomará en cuenta la totalidad de todos los servicios asociados a los ítems contenidos en estas bases técnicas.***
- 5- Servicio y Soporte por 3 y 5 años de **Security Operation Center (SOC) – IRM**. Valor detallado en UF incluyendo IVA. ***Se tomará en cuenta la totalidad de todos los servicios asociados a los ítems contenidos en estas bases técnicas.***

En los valores se deben incluir todos los servicios especificados en las presentes bases técnicas, en el caso que el proveedor incluya servicios adicionales, mejoras tecnológicas, elementos de innovación y otros, estos deben quedar especificados en el formulario correspondiente, (ver Anexo 6).

7.1 Pautas de Evaluación

La pauta de evaluación para esta licitación se realizará en base a la siguiente tabla, la cual se hace toma como referencia del Anexo Nro. 6 del documento de Bases Administrativas:

7.1.1 Pautas de Evaluación General

Ítem	Item a Evaluar	Ponderación
1	Propuesta Económica	50%
3	Propuesta Técnica	4%
4	Aspectos Administrativos	10%
5	Plazos de Entrega y puesta en Marcha	5%

7.1.2 Pautas de Evaluación Técnica

Ítem	Aspectos a Evaluar	Ponderación
1	Experiencia del Proveedor	10%
2	Experiencia del Equipo	10%
3	Propuesta Técnica	40%
4	Experiencia en ACHS	10%
5	Certificaciones obtenidas por la Empresa	10%
6	Evaluación en la Industria	20%

8 CRONOGRAMA DE IMPLEMENTACIÓN

El Proveedor deberá generar un cronograma de implementación en el cual deberá detallar las actividades que realizará, acorde a los tiempos planificados por ACHS (Ver Anexo 5) y recursos que requerirá para la puesta en funcionamiento al 100% los servicios a entregar.

9 APORTES DEL PROVEEDOR

El proponente deberá disponer de toda la infraestructura necesaria para la entrega cabal y oportuna de los equipos y servicios requeridos.

Deberá disponer de oficinas, mobiliario, infraestructura computacional, correo electrónico, redes de comunicación, equipos de video conferencia, telefonía, sistemas de grabación, licencias de software y todo aquello que considere necesario para cumplir con los requerimientos.

10 APORTES DE ACHS

ACHS para la ejecución de los servicios encomendados al Proveedor, proveerá la información requerida para la instalación y configuración de los requerimientos solicitados.

El Proveedor deberá en su propuesta indicar todos los elementos que requiere de ACHS para una correcta ejecución de sus servicios. Adicionalmente, proveerá las contrapartes necesarias requeridas por el Proveedor para la ejecución del servicio.

11 CONFIDENCIALIDAD

El Proveedor y sus empleados que presten servicios en el marco de la presente licitación, asume el compromiso de mantener la confidencialidad de la información que en el cumplimiento del servicio para el que fue contratado, le corresponda conocer, procesar, almacenar, recuperar, imprimir o transmitir.

Con el propósito de no arriesgar innecesariamente la seguridad de la información (confidencialidad, integridad y disponibilidad), el Proveedor ejecutará, de las acciones precedentes, sólo aquellas que sean necesarias para la ejecución del servicio, absteniéndose de realizar las acciones restantes y absteniéndose de acceder, por cualquier medio, a otra información de ACHS, que no es necesaria para el cumplimiento de sus funciones. El Proveedor deberá abstenerse de introducir y conectar equipos TI y software sin la autorización correspondiente, otorgada por los Jefes de Áreas designados por ACHS.

ACHS se reserva el derecho a auditar el fiel cumplimiento de esta cláusula, sin previo aviso, siendo obligación del Proveedor colaborar en las actividades correspondientes.

En caso de detectarse incumplimiento, ACHS podrá aplicar sanciones que dependerán de la gravedad de la falta:

- Carta-amonestación a la empresa que otorga el servicio.
- Reemplazo inmediato del empleado sorprendido en incumplimiento

Sin perjuicio de lo anterior, ACHS se reserva el derecho de ejercer todas las acciones legales que correspondan, si el incumplimiento de la presente cláusula deriva en perjuicio a los intereses de ACHS.



11.1 ANEXOS TÉCNICOS

11.1.1 Anexo 1: Experiencia del Oferente

ANEXO 1: EXPERIENCIA DEL OFERENTE: Firewalls				
NOMBRE DEL PROYECTO	DESCRIPCIÓN DEL PROYECTO	RAZÓN SOCIAL DE EMPRESA O INSTITUCIÓN	NOMBRE, E-MAIL, TELÉFONO DE CONTACTO	TIEMPO DURANTE EL CUAL PRESTÓ EL SERVICIO
				Desde - Hasta
ANEXO 1: EXPERIENCIA DEL OFERENTE: CDN				
NOMBRE DEL PROYECTO	DESCRIPCIÓN DEL PROYECTO	RAZÓN SOCIAL DE EMPRESA O INSTITUCIÓN	NOMBRE, E-MAIL, TELÉFONO DE CONTACTO	TIEMPO DURANTE EL CUAL PRESTÓ EL SERVICIO
				Desde - Hasta
ANEXO 1: EXPERIENCIA DEL OFERENTE: Balanceadores				
NOMBRE DEL PROYECTO	DESCRIPCIÓN DEL PROYECTO	RAZÓN SOCIAL DE EMPRESA O INSTITUCIÓN	NOMBRE, E-MAIL, TELÉFONO DE CONTACTO	TIEMPO DURANTE EL CUAL PRESTÓ EL SERVICIO
				Desde - Hasta
ANEXO 1: EXPERIENCIA DEL OFERENTE: WAF				
NOMBRE DEL PROYECTO	DESCRIPCIÓN DEL PROYECTO	RAZÓN SOCIAL DE EMPRESA O INSTITUCIÓN	NOMBRE, E-MAIL, TELÉFONO DE CONTACTO	TIEMPO DURANTE EL CUAL PRESTÓ EL SERVICIO
				Desde - Hasta
ANEXO 1: EXPERIENCIA DEL OFERENTE: SOC				
NOMBRE DEL PROYECTO	DESCRIPCIÓN DEL PROYECTO	RAZÓN SOCIAL DE EMPRESA O INSTITUCIÓN	NOMBRE, E-MAIL, TELÉFONO DE CONTACTO	TIEMPO DURANTE EL CUAL PRESTÓ EL SERVICIO
				Desde - Hasta

Ver documento anexo “Anexos BT- Renovación Tecnológica de Firewall.xlsx”

11.1.2 Anexo 2: Experiencia de los Ingenieros

ANEXO 2: EXPERIENCIA DE INGENIEROS: FIREWALL				
NOMBRE DEL PROFESIONAL	TITULO PROFESIONAL Y/O CERTIFICACIÓN	DESCRIPCIÓN DEL PROYECTO Y TECNOLOGÍA UTILIZADA	RAZÓN SOCIAL DE EMPRESA O INSTITUCIÓN	NOMBRE, E-MAIL, TELÉFONO DE CONTACTO EN EMPRESA
ANEXO 2: EXPERIENCIA DE INGENIEROS: CDN				
NOMBRE DEL PROFESIONAL	TITULO PROFESIONAL Y/O CERTIFICACIÓN	DESCRIPCIÓN DEL PROYECTO Y TECNOLOGÍA UTILIZADA	RAZÓN SOCIAL DE EMPRESA O INSTITUCIÓN	NOMBRE, E-MAIL, TELÉFONO DE CONTACTO EN EMPRESA
ANEXO 2: EXPERIENCIA DE INGENIEROS: BALANCEADORES				
NOMBRE DEL PROFESIONAL	TITULO PROFESIONAL Y/O CERTIFICACIÓN	DESCRIPCIÓN DEL PROYECTO Y TECNOLOGÍA UTILIZADA	RAZÓN SOCIAL DE EMPRESA O INSTITUCIÓN	NOMBRE, E-MAIL, TELÉFONO DE CONTACTO EN EMPRESA
ANEXO 2: EXPERIENCIA DE INGENIEROS: WAF				
NOMBRE DEL PROFESIONAL	TITULO PROFESIONAL Y/O CERTIFICACIÓN	DESCRIPCIÓN DEL PROYECTO Y TECNOLOGÍA UTILIZADA	RAZÓN SOCIAL DE EMPRESA O INSTITUCIÓN	NOMBRE, E-MAIL, TELÉFONO DE CONTACTO EN EMPRESA
ANEXO 2: EXPERIENCIA DE INGENIEROS: SOC				
NOMBRE DEL PROFESIONAL	TITULO PROFESIONAL Y/O CERTIFICACIÓN	DESCRIPCIÓN DEL PROYECTO Y TECNOLOGÍA UTILIZADA	RAZÓN SOCIAL DE EMPRESA O INSTITUCIÓN	NOMBRE, E-MAIL, TELÉFONO DE CONTACTO EN EMPRESA

Ver documento anexo “Anexos BT- Renovación Tecnológica de Firewall.xlsx”

11.1.3 Anexo 3: Plazos de Entrega

	Días corridos
Plazo de Entrega Total de Productos y Servicios	

Ver documento anexo “Anexos BT- Renovación Tecnológica de Firewall.xlsx”

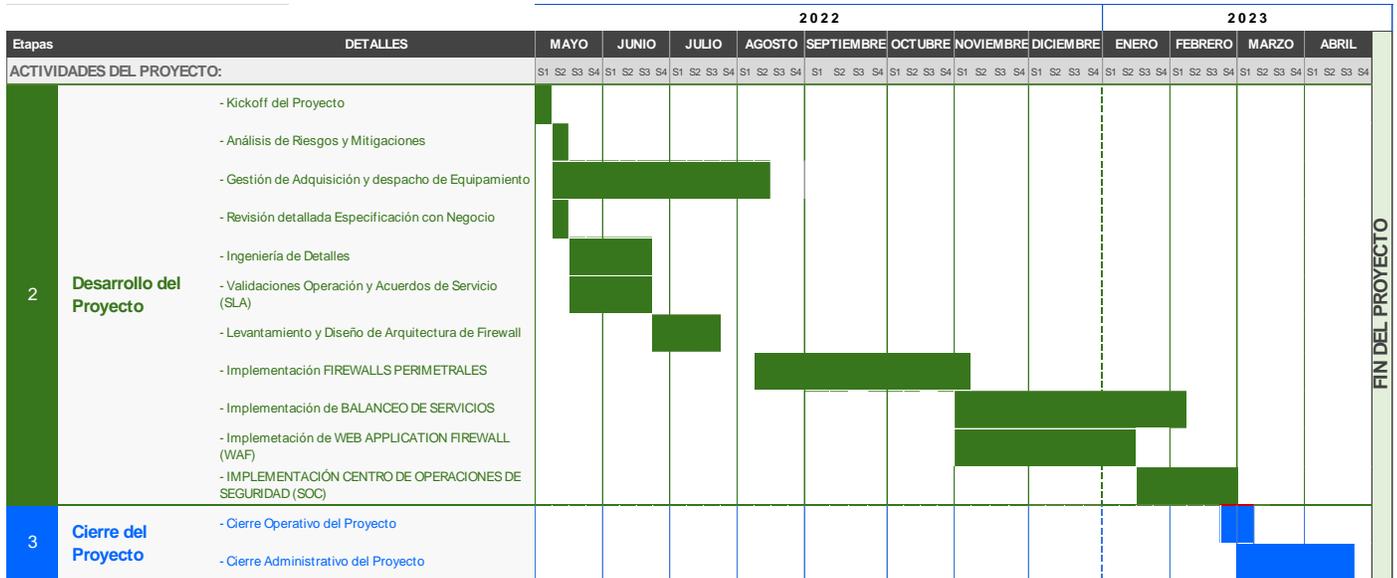
11.1.4 Anexo 4: Niveles de Servicio y Penalidades

Item	Variable	Descripción	Umbral	Penalidad	Observación
Implementación	Atraso Ambiente de Pre-Producción	Días de atraso máximo del Término de Tareas en Ambiente de PreProducción	0	UF 10	Por día de atraso
	Atraso en el cumplimiento de las tareas definidas en los entregables comprometidos en el proyecto	Días de atraso máximo por hito (excepto para el último hito)	5	UF 10	Por día de atraso
	Atraso de proyecto	Días de atraso máximo del proyecto	0	0,1% del total del contrato	por día de atraso
Infraestructura	Reposición de Firewalls	Tiempo máximo de reposición de equipos con fallas.	6 horas	UF 1	Por cada hora sobre el umbral
	Reposición Balanceadores de Carga	Tiempo máximo de reposición de equipos con fallas.	6 horas	UF 1	Por cada hora sobre el umbral
	Plataformas Centrales	Porcentaje de disponibilidad mensual	99,90%	UF 10	Por cada 0,1% bajo el umbral
Operación	Documentación	Reporte Diario de Servicios	Informe electrónico de las 8:00hrs	UF 1	Por hora de atraso
		Entrega de Informes de Gestión de Servicios	Sexto día de cada mes	UF 10	Por día de atraso
		Entrega de Reporte de Incidentes	24 horas	UF 1	Por hora de atraso
		Tiempo de confección de procesos y procedimientos para IRM	10 días	UF 10	Por día de atraso
		Tiempo de entrega de informe de análisis forense de un incidente	2 días	UF 10	Por día de atraso
	Soporte	Resolución de incidentes	2 horas	UF 1	Por hora de atraso
		Resolución de incidentes por fallas en configuración	1 horas	UF 1	Por hora de atraso
		Tiempo de Análisis de eventos de seguridad	1 hora	UF 1	Por hora de atraso
		Tiempo de Respuesta de la Mesa de Ayuda a llamadas	Respuesta en 3 minutos	UF 1	Por cada 10 minutos de atraso
		Cumplimiento del tiempo desde que es informada una amenaza por el servicio de inteligencia hasta que ACHS recibe el informe de impacto y plan de mitigación.	24 horas	UF 1	Por hora de atraso
		Tiempo de análisis de vulnerabilidades reportadas por fabricantes	7 días	UF 1	Por día de atraso
	Mantenimiento	Aplicación upgrade y updates a equipos que prestan servicios, según recomendación del fabricante	7 días	UF 1	Por día de atraso
		Cumplimiento del Plan de Mantención del equipamiento	Según calendarios acordados	UF 10	Por hora de atraso
	Requerimientos	Ejecución de Requerimientos en equipos	4 horas	UF 1	Por hora de atraso

Ver documento anexo “Anexos BT- Renovación Tecnológica de Firewall.xlsx”

11.1.5 Anexo 5: Cronograma de Implementación

Gerencia: GST



11.1.6 Anexo 6: Formulario Propuesta Económica

FORMULARIO DE VALORES DE EQUIPOS (CAPEX)					
Ítem	Descripción	Bienes y/o Equipamiento			
		Cantidad (Unidad)	Valor Neto (UF)	Subtotal (UF)	IVA 19% (UF)
1	Suministro, Instalación y Configuración de Infraestructura de Firewalls, CDN y Balanceadores de Carga.				
	Detalle				
	Detalle				
2	Suministro, Instalación y Configuración de Web Application Firewalls (WAF).				
	Detalle				
	Detalle				
Observaciones:					

FORMULARIO DE VALORES DE SERVICIOS (OPEX)					
Ítem	Descripción	Bienes y/o Servicio a 3 Años			
		Afecto a IVA?	Costo Total Año 1 (UF)	Costo Total Año 2 (UF)	Costo Total Año 3 (UF)
3	Servicio y Soporte por 5 años de Security Operation Center (SOC) – Administración y Gestión (Firewall, CDN, Balanceadores, WAF)	<i>Nota: Sí afecta IVA, se debe incluir en el costo total por año</i>			
	Detalle				
	Detalle				
4	Servicio y Soporte por 5 años de Security Operation Center (SOC) – Analizador de Logs y Gestión de Eventos.	<i>Nota: Sí afecta IVA, se debe incluir en el costo total por año</i>			
	Detalle				
	Detalle				
5	Servicio y Soporte por 5 años de Security Operation Center (SOC) – IRM	<i>Nota: Sí afecta IVA, se debe incluir en el costo total por año</i>			
	Detalle				
	Detalle				
Observaciones:					

FORMULARIO DE VALORES DE SERVICIOS (OPEX)							
Ítem	Descripción	Bienes y/o Servicio a 5 Años					
		Afecto a IVA?	Costo Total Año 1 (UF)	Costo Total Año 2 (UF)	Costo Total Año 3 (UF)	Costo Total Año 4 (UF)	Costo Total Año 5 (UF)
3	Servicio y Soporte por 5 años de Security Operation Center (SOC) – Administración y Gestión (Firewall, CDN, Balanceadores, WAF)	<i>Nota: Si afecta IVA, se debe incluir en el costo total por año</i>					
	Detalle						
	Detalle						
4	Servicio y Soporte por 5 años de Security Operation Center (SOC) – Analizador de Logs y Gestión de Eventos.	<i>Nota: Si afecta IVA, se debe incluir en el costo total por año</i>					
	Detalle						
	Detalle						
5	Servicio y Soporte por 5 años de Security Operation Center (SOC) – IRM	<i>Nota: Si afecta IVA, se debe incluir en el costo total por año</i>					
	Detalle						
	Detalle						
Observaciones:							

Ver documento anexo “Servicios Licitados por Items Proy. Renov. Tec. Firewall.xlsx”

11.1.8 Anexo 8: Entregables Compromiso Proyecto

ACHS Cumplimientos de Entregables del Proyecto				
EDT	ENTREGABLE	Tipo	Carácter	Fecha
5	REQUERIMIENTOS DEL PROYECTO	Definición	Mandatorio	
COMPONENTE 1: INFRAESTRUCTURA TECNOLÓGICA PARA SEGURIDAD PERIMETRAL				
5.1.1	Base de Diseño.	Digital	Mandatorio	
5.1.2	Firewall Perimetrales	Equipamiento	Mandatorio	
5.1.3	Protección Web Application, DNS y Load Balancing (CDN)	Licenciamiento	Mandatorio	
5.1.4	Balaceo de Servicios	Requerimiento	Mandatorio	
5.1.5	Web Application Firewalls (WAF)	Requerimiento	Mandatorio	
5.1.6	Consolas de Administración	Requerimiento	Mandatorio	
COMPONENTE 2: SOC				
5.2.1	Administración de Infraestructura	Requerimiento	Mandatorio	
5.2.1.1	Monitoreo de la Infraestructura	Requerimiento	Mandatorio	
5.2.1.2	Mantenimiento Preventiva	Requerimiento	Mandatorio	
5.2.1.3	Mantenimiento Correctiva	Requerimiento	Mandatorio	
5.2.1.4	Requerimientos que debe Gestionar del SOC	Requerimiento	Mandatorio	
5.2.1.5	Reportes de Gestión de Servicios	Requerimiento	Mandatorio	
5.2.2	Analizador de Logs	Requerimiento	Mandatorio	
5.2.3	Gestión de Eventos de Seguridad	Requerimiento	Mandatorio	
5.2.3.1	Gestión del Servicio	Requerimiento	Mandatorio	
5.2.3.2	Análisis de Eventos	Requerimiento	Mandatorio	
5.2.4	Equipo de Respuesta ante Incidentes (IRM)	Requerimiento	Mandatorio	
5.2.4.1	Documentación	Requerimiento	Mandatorio	
5.2.4.2	Control y Gestión	Requerimiento	Mandatorio	
5.2.4.3	Gestión sobre incidentes	Requerimiento	Mandatorio	
5.2.4.4	Análisis Forense	Requerimiento	Mandatorio	
IMPLEMENTACIÓN DE SERVICIOS				
5.3.1	Gerenciamiento	Gestión de Proyectos	Mandatorio	
5.3.2	Instalación y Configuración	Gestión de Proyectos	Mandatorio	
5.3.2.1	Carta Gantt	Gestión de Proyectos	Mandatorio	
5.3.2.2	Plan de Implementación	Gestión de Proyectos	Mandatorio	
5.3.2.3	Ambiente Pre-Productivo	Gestión de Proyectos	Mandatorio	
5.3.2.4	Instalación de Componentes	Gestión de Proyectos	Mandatorio	
5.3.2.5	Pruebas de Contingencia	Gestión de Proyectos	Mandatorio	
5.3.3	Capacitación Técnica	Gestión de Proyectos	Mandatorio	
5.3.4	Entregables	Gestión de Proyectos	Mandatorio	
5.3.5	Garantía de Implementación del Proyecto	Gestión de Proyectos	Mandatorio	
OPERACIÓN DE LOS SERVICIOS				
5.4.1	Gobierno de Servicios	Servicio	Mandatorio	
5.4.2	Supervisor de Servicio	Servicio	Mandatorio	
5.4.3	Estructura de Gestión y Supervisión de Servicios	Servicio	Mandatorio	
5.4.4	Esquema de Escalamiento	Servicio	Mandatorio	
5.4.5	Reuniones de Trabajo y Revisiones	Servicio	Mandatorio	
MANTENIMIENTO DE COMPONENTES				
5.5.1	Upgrades y Updates	Servicio	Mandatorio	
5.5.2	Plan de Continuidad y Contingencia	Servicio	Mandatorio	
5.5.3	Gestión de Capacidad de Servicio	Servicio	Mandatorio	
5.5.4	Garantías y Mantenimiento	Servicio	Mandatorio	
5.5.5	Plan de Devolución	Servicio	Mandatorio	
EXPERIENCIA DEL PROVEEDOR				
5.6.1	Experiencia de la Empresa	Requerimiento	Mandatorio	
5.6.2	Experiencia del Equipo	Requerimiento	Mandatorio	
NIVELES DE SERVICIOS				
5.7.1	Definiciones	Servicio	Mandatorio	
5.7.2	SLA de Monitoreo de Seguridad	Servicio	Mandatorio	
5.7.3	SLA de Administración	Servicio	Mandatorio	
5.7.4	SLA de Monitoreo de Disponibilidad	Servicio	Mandatorio	
5.7.5	SLA Disponibilidad del Servicio	Servicio	Mandatorio	
5.7.6	SLA de Eventos Almacenados de Monitoreo	Servicio	Mandatorio	
5.7.7	SLA de Gestión de Fallas	Servicio	Mandatorio	
5.7.8	SLA de Mantenimiento Preventivo	Servicio	Mandatorio	
5.7.9	Consideraciones de Niveles de Servicio	Servicio	Mandatorio	
5.7.10	Cálculo de la Disponibilidad de los Servicios	Servicio	Mandatorio	
5.7.11	Penalizaciones	Servicio	Mandatorio	
MULTAS				
6.1	Multas por Atrasos en la Entrega de los Servicios	Servicio	Mandatorio	
6.2	Multas por Indisponibilidad Mensual	Servicio	Mandatorio	
6.3	Multas por Facturación No Oportuna	Servicio	Mandatorio	
7	PROPUESTA ECONÓMICA	Requerimiento	Mandatorio	
8	CRONOGRAMA DE IMPLEMENTACIÓN	Requerimiento	Mandatorio	
11	CONFIDENCIALIDAD	Requerimiento	Mandatorio	
	Acta de Aceptación Firmada por el Proveedor	Requerimiento	Mandatorio	
Firma JP Proveedor				

Ver documento anexo "Entregables Compromiso Proyecto.xlsx"