EANA | NAVEGACIÓN AÉREA ARGENTINA

Ministerio de Transporte
Presidencia de la Nación

ADQUISICIÓN DE EQUIPAMIENTO PARA NUEVA RED CORE

ESPECIFICACIÓN TÉCNICA

CONTENIDO

ING. MALENA REINOSO
Gerenta de Ingeniería CNS
Empresa Argentina de Navegación Aérea
Sociedad de Estado

1. DENOMINACIÓN DE LA ADQUISICIÓN

Adquisición de hardware, software y servicios profesionales para la actualización de la red de EANA y su migración a SDN.

2. OBJETO DE LA ADQUISICIÓN

EANA como empresa encargada de la prestación de servicios a la Navegación Aérea y Seguridad del vuelo en el país, planificó en su plan de servicios 2020-2024 la migración de la actual red ATN – red de telecomunicaciones aeronáuticas – (red híbrida con tecnología cercana a su obsolescencia) y su red corporativa, a una red definida por software (SDN) integrada en su totalidad por enlaces digitales de diferentes tecnologías con interfaces IP.

La contratación de la solución detallada en la presente especificación técnica será bajo la modalidad llave en mano.

3. REQUERIMIENTOS TÉCNICOS

La red actual de EANA desplegada a lo largo de todo el país se encuentra implementada con equipamiento Cisco. Esto incluye equipos obsoletos y equipos de nueva generación. El porcentaje de equipamiento de red que se encuentra obsoleto es el 60%. EANA adquiere en el año 2018 routers Cisco de nueva generación que no fueron implementados y se encuentran en depósitos, más el que ya se encuentra instalado de nueva generación suma un total de equipos del 40%

Ante esta situación y luego de un análisis técnico y económico EANA ha decidido utilizar todo el equipamiento de nueva generación tanto productivo como en stock, agregando las licencias requeridas para la migración a SDN, de forma tal de reducir costos y minimizar el impacto operativo durante la implementación. En el título 4 de este documento se describe todo el equipamiento de EANA.

Por tal motivo es requisito que la red SDN sea compatible con el equipamiento de nueva generación Cisco que EANA dispone actualmente. Cabe mencionar que dicho equipamiento tiene fecha de EOS en 2026.

La solución deberá incluir la totalidad del hardware, licencias y software solicitado, no aceptando propuestas parciales, para implementar una red SDN que cubra con las necesidades tecnológicas especificadas de forma general a continuación:

- Creación de una red de nueva generación que integre los servicios operativos y corporativos de EANA
- Incorporar máximo nivel de seguridad de los activos lógicos y físicos de la red
- Asegurar la disponibilidad de la red para dar calidad, previsibilidad y seguridad a los servicios esenciales
- Priorizar los servicios críticos
- Proveer redundancia de los vínculos que soportan la red

- Optimizar el uso de los recursos disponibles

4. EQUIPAMIENTO DE EANA

A continuación, se detalla el equipamiento Cisco en producción actualmente:

#	Sitio	Detalle del Equipo (Modelo)	Puertos
1	Bahía Blanca	ISR4221/K9	2GE, 2NIM/NIM ES2-4
2	Chacharramendi	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
3	Choele Choel	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
4	Junín	ISR4221/K9	2GE, 2NIM/NIM ES2-4
5	Mar del Plata	ISR4221/K9	2GE, 2NIM/NIM ES2-4
6	Neuquén	ISR4221/K9	2GE, 2NIM/NIM ES2-4
7	Pehuajó	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
8	Piedra del Águila	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
9	Santa Rosa	ISR4221/K9	2GE, 2NIM/NIM ES2-4
10	Tandil	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
11	El Calafate	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
12	Esquel	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
13	Puerto Madryn	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
14	Rio Gallegos	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
15	Rio Grande	ISR4221/K9	2GE, 2NIM/NIM ES2-4
16	Puerto San Julian	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
17	Viedma	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
18	Rio Mayo	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
19	Ingeniero Jacobacci	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
20	San Juan	ISR4221/K9	2GE, 2NIM/NIM ES2-4
21	Villa Reynolds	ISR4221/K9	2GE, 2NIM/NIM ES2-4/G703
22	Malargüe	ISR4221/K9	2GE, 2NIM/NIM ES2-4
23	Rincón de los Sauces	ISR4221/k9	2GE, 2NIM/NIM ES2-4
24	Rincón de los Sauces	ISR4221/k9	2GE, 2NIM/NIM ES2-4

Equipos adquiridos y en stock en EANA:

Tipo	*Detalle del Equipo (Modelo)*	*Cantidad*	*EOS (End of Support)*
Router	CISCO4431/K9	8	No
Router	CISCO4321/K9	48	No
Router	C1601	1	Si
Router	C1760	2	Si
Router	C1841	1	Si
Router	C2611XM	3	Si
Router	C2691	3	Si
Router	C2801	23	Si
Router	C2851	2	Si
Router	C3845	2	Si
Router	C805	1	Si
Router	CISCO 2900	1	Si
Router	CISCO 871 (MPC8272)	1	Si
Router	CISCO1921/K9	6	Si
Router	CISCO2901/K9	38	Si
Router	CISCO2911/K9	4	Si
Router	CISCO2921/K9	7	Si
Router	CISCO3945	2	Si
Router	CISCO887VA-K9	1	No
Router	ISR4221/K9	24	No
Router	ISR4331/K9	4	No
Switch	C1-WS3850-1248UL	10	No
Switch	Cisco 200E 24-Port 10/100 Smart Switch	1	Si
Switch	Linksys SRW224	9	Si
Switch	SG300-20	1	Si
Switch	SG300-28P	4	Si
Switch	WS-C2950-24	8	Si
Switch	WS-C2950C-24	1	Si
Switch	WS-C2950G-12-EI	2	Si
Switch	WS-C2950G-24-EI	3	Si
Switch	WS-C2950T-24	2	Si
Switch	WS-C2960+24LC-L	5	Si
Switch	WS-C2960-24PC-L	4	Si
Switch	WS-C2960-24PC-S	2	Si
Switch	WS-C2960-8TC-L	2	Si
Switch	WS-C2960G-8TC-L	1	Si
Switch	WS-C2960L-8TS-LL	19	Si
Switch	WS-C3560CX-12PC-S	18	Si
Switch	WS-C3650-24TS	20	Si
Switch	WS-CE500-24TT	5	Si

AP	Cisco AIR AP 1200	1	Si
AP	Cisco AIR Bridge 1300	1	Si
TOTAL		287	

5. ETAPAS DEL PROYECTO

Debido a la magnitud e importancia de las dos redes de datos de EANA (red ATN y red corporativa) el proyecto se dividirá en 9 fases agrupadas en 2 etapas, que determinará la actualización de ambas redes en tiempos diferentes. A continuación, se describen las etapas.

5.1 Etapa 1

Se adquirirá hardware, software y servicios profesionales para actualizar la **red corporativa** a una red SDN, tanto para WAN, LAN y Seguridad. Esto implicará realizar el despliegue del hardware en todos los aeropuertos en donde EANA posee la red corporativa.

La implementación será realizada en 4 fases:

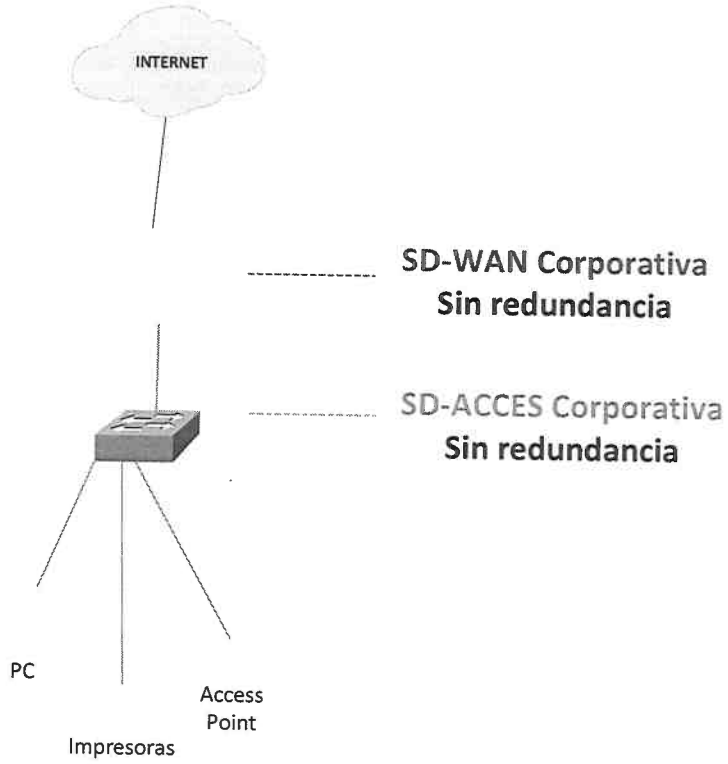
a. Fase 1 = 6 nodos (FIRS + AEP)

b. Fase 2 = 23 nodos (Sitios EAVAS + aeropuertos)

c. Fase 3 = 8 nodos (Sitios RADAR + aeropuertos)

d. Fase 4 = 20 nodos (Aeropuertos)

A continuación, se muestra un ejemplo del diagrama genérico de la red corporativa.



La solución de SDN para WAN será a través de Internet a través del enlace existente de cada aeropuerto.

5.2 Etapa 2

Se adquirirá hardware, software y servicios profesionales para actualizar la **red operativa** a una red SDN, tanto para WAN, LAN y Seguridad. Esto implicará realizar el despliegue del hardware en todos los aeropuertos en donde EANA posee la red operativa.

De esta manera, ambas redes de EANA quedarán actualizadas con tecnología SDN. Se logrará la integración de la plataforma SDN de WAN y se contará con redundancia a nivel equipamiento WAN, pudiendo utilizar los enlaces de datos WAN e Internet.

Dada la criticidad de esta red es requisito excluyente para iniciar la etapa 2 que la totalidad de los sitios de la etapa 1 se encuentren 100% operativos y funcionando en forma estable por 3 meses.

La etapa 2 será realizada manteniendo la red legacy 100% operativa. Luego de la implementación de la red SDN los servicios se migrarán en forma progresiva manteniendo la red legacy como backup por un periodo de 24 meses.

Se deberá documentar el proceso de contingencia y rollback hacia la red legacy, incluyendo el proceso en la capacitación que dictará el proveedor al personal de EANA.

La implementación será realizada en 5 fases:

a. Fase 5 = 10 nodos (EAVAS terceros)

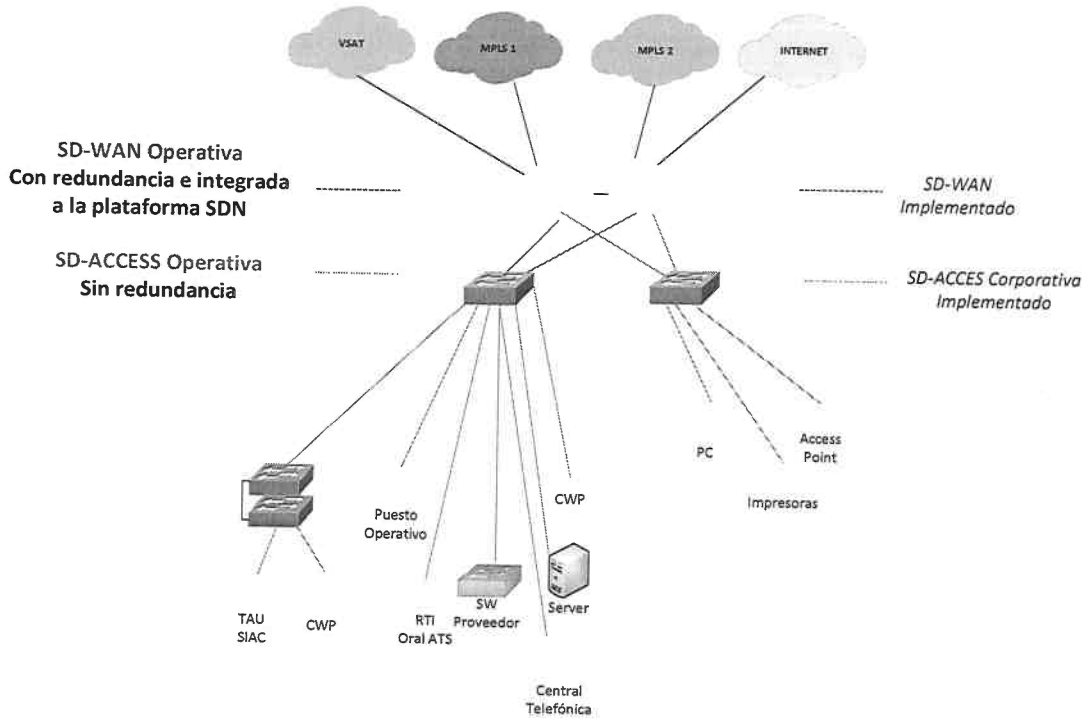
b. Fase 6 = 20 nodos (Aeropuertos)

c. Fase 7 = 11 nodos (Sitios RADAR)

d. Fase 8 = 31 nodos (Sitios EAVAS)

e. Fase 9 = 6 nodos (FIRS + AEP)

A continuación, se muestra un ejemplo del diagrama genérico de la red operativa.



6. ALCANCE DE LA CONTRATACIÓN

Comprende la provisión de hardware, software y servicios profesionales, teniendo que ser lo cotizado de características iguales o superiores a lo indicado en el presente Pliego de Especificaciones Técnicas. Los mismos han sido diseñados, dimensionados y documentados luego de haber realizado una consultoría profesional de la totalidad de los nodos (OC 101/2020 -

Contratación Directa por Excepción N° 29/2020 - "Adquisición de servicios profesionales de consultoría - Nueva Red CORE").

Para la oferta técnica, los oferentes deberán cumplir con las especificaciones técnicas requeridas en este documento, y además deberán anexar el documento ANEXO III – PLANILLA DE DATOS GARANTIZADOS, debidamente completado y respondido por los oferentes, para que EANA realice la evaluación técnica correspondiente.

Renglón	*Ítem*	*Medida*	*Cantidad*
1	SFP 1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM	Unidad	194
2	SFP 1000BASE-T SFP transceiver module for Category 5 copper wire	Unidad	234
3	Router C1111-8P-DNA	Unidad	19
4	Router C8300-1N1S-6T	Unidad	2
5	Access point C9105AXI-A	Unidad	117
6	Switch C9300-48P-A	Unidad	11
7	Switch C9300L-24P-4X-A	Unidad	126
8	Switch C9300L-48P-4X-A	Unidad	8
9	Máquina Virtual FPR2110-NGFW-K9	Unidad	1
10	Máquina Virtual R-ISE-VMM-K9=	Unidad	4
11	Máquina Virtual R-ISE-VMS-K9=	Unidad	9
12	Máquina Virtual SF-FMC-VMW-2-K9	Unidad	1
13	Extensor LAN WS-C3560CX-12PC-S	Unidad	83
14	Servicios: Licencias de software por única vez	Unidad	1
15	Servicios: Licencias de software por 3 años	Unidad	3
16	Servicios: Servicios Profesionales	Unidad	1

7. CARACTERISTICAS Y EXPERIENCIA DE LA FIRMA ADJUDICADA

Los oferentes deberán presentar una Carta del Fabricante, demostrando estar certificado por la marca para la provisión, implementación y soporte de software y hardware solicitado en la presente.
Los oferentes deberán presentar máxima certificación del fabricante (Cisco Gold Partner Integrator o equivalente).
Los oferentes deberán cumplir con las siguientes especializaciones para poder participar en la provisión e implementación del presente pedido:

- Cisco Advanced Enterprise Networks Architecture Specialization
- Cisco Advanced SP Architecture Specialization
- Cisco Advanced Security Architecture Specialization
- Cisco Customer Experience Specialization

Deberá acreditar experiencia brindando soluciones de similar envergadura de redes SDN.
Dentro del equipo de trabajo de implementación, los oferentes deberán contar dentro de su nómina de empleados con al menos 2 (dos) recursos certificados por el fabricante en la especialización de Cisco customer experience (CCSM), con el objetivo de acompañar al organismo en el on-boarding de las soluciones implementadas, acelerar la adopción de estas tecnologías, e integrar estas nuevas capacidades en los procesos de negocios de EANA.
Dentro del equipo de trabajo, los oferentes deberán manejar sus procedimientos bajo las normas ITIL. Para ello deberá presentar un recurso responsable de posventa con certificación ITILv3 o ITILv4.
Se deberá asignar un recurso Líder del Proyecto que deberá ser PM. El mismo será quien lleve adelante el proyecto y será punto focal entre EANA y el adjudicatario. La información de este recurso deberá estar contemplado en la propuesta técnico económica para la evaluación.
Los oferentes deberán asignar 4 recursos CCIE (Cisco Certified Internetwork Expert) dentro del equipo de ingeniería con los roles de Arquitectos Especialistas certificados por el fabricante, quienes participarán en todas las etapas del Proyecto.
Las especialidades deberán ser las siguientes:

- CCIE ENT (Cisco Certified Internetwork Expert Enterprise Infraestructure)
- CCIE SP (Cisco Certified Internetwork Expert Service Provider)
- CCIE WIFI (Cisco Certified Internetwork Expert WIFI)

8. GENERALIDADES

8.1 Terminología utilizada

Donde dice "poseer capacidad", deberá interpretarse: instalada, funcionando y respondiendo a las facilidades requeridas en el presente Pliego.

Donde dice "soportar", interpretarse: preparado para poseer la capacidad a través de una actualización de HW y/o SW futura.

Toda otra terminología se ajustará a las definiciones expresadas por los principales Organismos Internacionales de Estandarización.

8.2 Cumplimientos generales

Se requiere el cumplimiento de los siguientes puntos para todo el hardware y software a adquirir:

- Entrega de documentación y manuales de configuración de hardware y software. Los manuales podrán ser entregados como original en papel, en medios digitales o mediante descarga web.
- Garantía por 36 meses, aclarado en el título 12.
- Actualización de software a la última versión disponible a la fecha de la recepción definitiva.

- Ciclo de vida de los equipos ofertados: la fecha mínima de EOL (end of life) dichos equipos no deben ser inferior a 5 años.

Los equipos ofertados deben ser nuevos sin uso y de solución definitiva. Deberá estar en producción efectiva a la fecha de apertura del concurso, es decir, no pueden haber sido discontinuados ni estar anunciado su fin de venta del producto.

9. MINIMO DE CUMPLIMIENTO OBLIGADO

9.1 SD-WAN

La arquitectura propuesta debe permitir aprovechar todos los beneficios de una red WAN definida por software. Los requerimientos primordiales son:

1. **WAN híbrida:** que permite el acomodamiento de múltiples conexiones de red subyacentes de diferente naturaleza.
2. **Conexión a la nube pública en servicios IaaS y SaaS:** la solución de SD WAN debe permitir la conexión hacia un VPC tanto de AWS como de AZURE como si fuesen un DC interno y para el caso de aplicaciones SaaS, debe permitir identificar los servicios SaaS y enrutarlos por el camino deseado de Internet. También, deberá poseer capacidad de conectar con servicios de nube de otros proveedores, como por ejemplo la nube de ARSAT.
3. **Enrutamiento basado en aplicaciones:** que proporciona la capacidad de reconocer el tráfico de aplicaciones hasta la Capa 7 con un control muy granular de la selección de la ruta.
4. **Overlay asegurado mediante IPSec:** Se debe garantizar que el overlay se proteja vía IPSec al menos AES-256. Las distintas redes virtuales deberán viajar segmentadas dentro de este túnel IPSEC.
5. **Soporte de enrutamiento dinámico en la LAN:** la solución debe garantizar que sobre las VPN de servicios se puedan habilitar protocolos de enrutamiento como VRRP, BGP/OSPF.
6. **Descubrimiento automático de aplicaciones vía DPI:** la solución debe permitir el descubrimiento de al menos 1000 aplicaciones vía firmas dentro de los mismos CPEs de la plataforma para poder categorizar el enrutamiento dinámico.
7. **Segmentación de red:** La segmentación se proporciona como una capacidad inherente de los planos de control y de datos y permite la construcción de un entorno de red donde dicha segmentación abarca intrínsecamente una rama subdividida con varios segmentos para extenderse a través de la WAN.
8. **Zero Touch Provisioning:** La solución debe contar con un proceso del tipo Zero Touch Provisioning.

9. **Arquitectura con escalabilidad horizontal (scale-out architecture) con redundancia**: La arquitectura de SDWAN debe proporcionar redundancia en elementos del plano de control, soportando múltiples fallas en cualquier capa. Adicional debe permitir crecer de forma horizontal en la capa de orquestación para hacer un "scale-out".
10. La solución debe soportar tanto IPv4 como IPv6.
11. El plano de control debe responder a una arquitectura Zero Trust. Se deberá realizar una autenticación bidireccional entre dispositivos y controladores usando certificados PKI. Con el uso de certificados emitidos por el CA de la empresa.
12. Frente a una pérdida de la sesión de control, los routers deberán seguir manteniendo activa su sesión del plano de datos, hasta al menos 4 días desde el incidente.
13. Se deberá proveer en el sitio es esquemas de alta disponibilidad, con dos routers funcionando en esquema activo/activo.
14. La solución deberá permitir configurar los servicios de telefonía directamente desde el controlador. Este requisito es deseable, no excluyente.
15. Deberá integrarse con el dominio SDN en Data Center, permitiendo extender la segmentación a este último. Este requisito es deseable, no excluyente.
16. Deberá integrarse con el dominio SDN en red de Acceso, permitiendo extender la segmentación a este último. Este requisito es deseable, no excluyente.

Las características mínimas de los equipos a suministrar y herramienta de gestión y monitoreo se detalla en los siguientes subtítulos:

a. Underlay
f. Overlay
g. Seguridad
h. Descubrimiento de aplicaciones
i. Conexión a la nube pública IaaS, SaaS
j. Segmentación VPN
k. Gestión y orquestación
l. Hardware
m. Funcionalidades varias

9.1.1 Underlay

La solución ofertada debe soportar los siguientes requerimientos:

1. Tipo de conexiones:
    a. Conexiones privadas vía MPLS.
    b. Conexiones privadas vía MetroEthernet.
    c. Conexiones Públicas de Internet Residencial.
    d. Conexiones Públicas de Internet Empresarial.
    e. Conexiones Públicas de Internet 3G/4G.
    f. Otros (usando puertos ethernet).
2. Los túneles deben poder establecerse de forma automática entre sitios, a través de enlaces MPLS, internet público, LTE o satelitales.
3. El controlador debe poder integrarse con soluciones Single Sign On (SSO).

9.1.2 Overlay

La solución debe soportar la creación de múltiples redes virtuales (overlays). Estas redes virtules deben estar aisladas entre sí. La solución deberá soportar al menos 20 redes virtuales.

La solución ofertada debe soportar los siguientes requerimientos:

1. Cada CPE establecerá conexiones del plano de datos con los demás CPEs de manera subyacente por defecto.
2. El orquestador debe poder restringir la conectividad de modo que los CPEs solo formen conexiones entre los nodos que se encuentran en la misma red de transporte.
3. Se deben poder crear topologías: Hub-and-Spoke, Full Mesh o Partial Mesh desde las políticas definidas en el orquestador.
4. Se deben poder definir políticas desde el orquestador para usar el overlay de la siguiente manera:
    a. Balance de carga (ECMP)
    b. Conexión Principal y Backup
    c. Enrutamiento por aplicaciones
    d. Encadenamiento de servicios (forzar que un flujo de tráfico pase primero por alguna plataforma de inspección)

5. Cada red virtual deberá poder tener una topología independiente de la seleccionada para las demás redes virtuales. Este requisito es deseable, no es excluyente.
6. Se deberá poder insertar un servicio que resida en otro sitio (como por ejemplo un firewall) en el camino del tráfico entre dos sucursales. Este requisito es deseable, no es excluyente.
7. Crear SLA por aplicaciones que permitan definir los parámetros de óptimo comportamiento en la WAN por aplicación como: Jitter, Delay y Packet Loss.
8. Debe contar con la capacidad de considerar factores en la selección de rutas distintas a las utilizadas por los protocolos de enrutamiento estándares, como los prefijos de rutas, métricas, información del estado del enlace.
9. Las políticas de enrutamiento deben permitir granularidad basado en:
    a. Aplicaciones
    b. Direcciones IP
    c. Puertos UDP/TCP
    d. Marcación DSCP
10. Se debe poder definir una preferencia de enlace, y una contingencia en caso de que dicho enlace no cumpla con los SLA de la política.
11. Identificación:

a. Define la aplicación de interés y luego crea una política de datos centralizada que mapea la aplicación a los requisitos específicos de SLA. Destaca el tráfico de datos de interés al hacer coincidir los encabezados de la Capa 3 y la Capa 4 en los paquetes, incluidos los prefijos fuente y de destino y los puertos, el protocolo y el campo DSCP.

b. Las políticas deben ser definidas desde el gestor de políticas centralizado, y desde allí indicar a que CPEs se deben aplicar.

12. Monitoreo y medición:

a. El software de SDWAN debe monitorear continuamente el tráfico de datos en los túneles del plano de datos entre CPEs y medir periódicamente las características de rendimiento del túnel. Recopilar latencia, pérdida y otras estadísticas de paquetes para su uso en un enrutamiento basado en aplicaciones.

b. Se deben soportar 8 colas de QoS en las interfaces para poder tratar el tráfico saliente del sitio.

13. Software de reportes y monitoreo avanzado:

    a. Se debe proveer un software para monitorear continuamente el tráfico de datos de los túneles SD WAN del plano de datos entre CPEs, proporcionar visualización de los cambios de topología en las rutas de la red, cambios en la ruta PfR por motivos fuera de la política, registro del cambio de tráfico asociado.

    b. Reportes y gráficos avanzados del tráfico en la red WAN, informes basados en dashboards y por sitio, filtros y búsquedas selectivas, vista de informes de 360 grados y flujos de trabajo altamente correlacionados para resolver rápidamente problemas de rendimiento críticos.

14. Debe existir un nodo de autenticación inicial que en el bring-up use un mecanismo de seguridad como DTLS.

15. El proceso de autenticación para un nuevo nodo debe verificar una base de datos de seriales en el Sistema de Gestión.

9.1.3 Seguridad

1. La solución debe soportar de encriptación simétrica de AES256.
2. Cada CPE debe contar con la capacidad de mantener decenas de pares de encriptación.
3. El tráfico entre CPEs se debe firmar utilizando el encabezado de autenticación estándar de IPsec (IPsec AH) preservando la integridad de los paquetes para evitar ataques de intermediarios (man-in-the-middle attacks).
4. Se deben soportar funcionalidades de, DNS Security y L7 Firewall embebidos en la caja y gestionables desde el mismo orquestador de SDWAN protegiendo las VPN de servicio usando DI (Direct Internet Access).
5. Soporte de IPS/IDS en la misma plataforma (opcional) con granularidad a nivel de VPN de servicio.
6. Soporte de URL-Filtering en la misma plataforma con granularidad a nivel de VPN de servicio.
7. Debe soportar Forward Error Correction (FEC) y Packet Duplication.
8. Debe soportar optimización TCP, para utilizarse en enlaces de muy alta latencia (por ejemplo, satelitales).

9.1.4 Descubrimiento de aplicaciones

1. La solución debe reconocer aplicaciones en categorías, como por ejemplo: antivirus, transferencia de archivos, correo, Microsoft-office, Middleware, peer-to-peer, telefonía, web y webmail, entre otras.
2. Los mecanismos de descubrimiento de aplicaciones se deben basar en firmas.
3. El motor de DPI debe poder permitir la creación de aplicaciones personalizadas.
4. La medición de la calidad del enlace deberá realizarse dentro del túnel IPSEC usando BFD. Este requisito es deseable, no es excluyente.
5. Debe permitir desplegar VNFs a los routers de borde que lo soporten. Este requisito es deseable, no es excluyente.

9.1.5 Conexión a la nube pública IASS, SAAS

1. La solución debe tener la capacidad de realizar off load de internet directamente en el CPE de cada Branch (Local Internet Breakout).
2. La solución debe tener la capacidad de realizar off load de internet en un CPE centralizado.
3. Se debe poder orquestar desde la solución de SD WAN el VPC al cual se debe desplegar el vCPE para interconectar todo el fabric SDWAN hacia la nube pública en modelo IaaS.
4. La solución debe tener soporte de DIA (Direct Internet Access) y conmutación a internet centralizado en caso de fallo en la interfaz de DIA.
5. Para aplicaciones SaaS (al menos Office 365 y Google Suite) se debe poder medir la calidad de la experiencia al acceder directamente desde un sitio. La medición debe realizarse en Capa 7 y directamente contra la aplicación sin necesidad de gateways multitenats.
6. Para aplicaciones SaaS se debe proveer un mecanismo que permita comparar la experiencia de un usuario accediendo a estas aplicaciones directamente desde el enlace de Internet disponible en el sitio contra la experiencia saliendo vía uno de los Data Centers. En base a esta comparación se debe elegir el mejor camino. Esto debe ofrecerse al menos para Office 365 y Google Suite.
7. Contar con un puerto predefinido en el CPE que reciba DHCP por defecto, para asignar una IP con acceso a la nube pública.
8. Debe contar con un certificado digital precargado en el CPE generado por una root CA pública reconocida.
9. Se debe contar con una instancia en la nube pública que permita determinar si el CPE que se está conectando pertenece a la organización que lo ha adquirido.

10. Solo después de pasar el proceso de autenticación basado en el certificado digital, el CPE podrá recibir las direcciones IP de los orquestadores del fabric de SD WAN correspondiente.

9.1.6 Segmentación VPN

La solución debe soportar:

1. La capacidad de segmentar por VPN de servicios en cada branch.
2. Se debe poder extender cada VPN sobre el overlay de SD WAN.
3. Se deben poder extender los segmentos más allá de los CPEs usando 802.1Q.
4. Indicar la cantidad máxima de VPN por CPEs (mínimo se deben soportar 4).

9.1.7 Gestión y orquestación

La solución debe soportar:

1. controladoras en el sitio y en la nube.
2. Monitoreo de los SLA de cada uno de los transportes SD WAN.
3. Creación de Templates de configuración de todos los CPEs.
4. Updates de software de forma masiva.
5. Creación de políticas de enrutamiento basado en la aplicación.
6. Creación de políticas de QoS.
7. Monitoreo de desempeño de los enlaces de overlay.
8. Monitoreo de desempeño de los CPEs.
9. Monitoreo del plano de control de todos los CPEs.
10. Control de inventario de los CPEs.
11. Geolocalización de los CPEs.
12. Gestión de alarmas.
13. Debe permitir crear usuarios de:
    a. Administrador
    b. Operador
14. Auditoría del acceso al NMS.

15. La solución debe debe contar con el monitoreo del desempeño de la conexión a la nube pública en las aplicaciones de SaaS.
16. Se debe poder gestionar vía SSH cada uno de los CPE o vCPE del fabric de SD WAN.
17. La solución debe contar tanto con interfaz gráfica GUI con acceso vía HTTPS, como así también con acceso a CLI vía consola o SSH.
18. El controlador de la solución debe poder aprovisionar de forma centralizada las configuraciones y actualizaciones de software de todos los equipos de red.
19. La solución deberá proveer herramientas gráficas de troubleshooting que permitan por lo menos lo siguiente:
    a. Ejecutar pings y traceroutes.
    b. Simular el flujo de alguna aplicación para validar las políticas de enrutamiento de tráfico.
    c. Verificar los pasos necesarios para que el equipo esté completamente operativo.
20. La solución deberá tener APIs REST para poder extraer información del inventario de la red, extraer y generar configuraciones, o extraer datos históricos de monitoreo.

9.1.8 Funcionalidades varias

La solución debe soportar:

1. AAA: TACACS+, RADIUS, local, Role Based Access Control
2. Routing:
    a. IPv4: OSPFv2 y BGP. una instancia por red virtual.
    b. IPv6: OSPFv3 y BGP.
    c. NAT para IPv4 e IPv6 en las interfaces hacia los proveedores de servicio.
3. Bridging: 802.1Q, native VLAN
4. Security: Zero-trust, whitelisting, Tamper Anchor Module, DTLS/TLS, IPSec, ESP-256-CBC, AH, HMAC-SHA1, DDOS protection, control plane protection, NAT traversal, RADIUS, TACACS, funcionalidad de IPS (intrusion Prevention Systems) soportado en hardware sin necesidad de agregar equipamiento adicional.
5. Forwarding and QoS: Classification, prioritization, low latency queuing, remarking, shaping, scheduling, policing, mirroring, NAT/PAT

6. Policy: Route policies, App Aware Routing, control policy, data policy, ACL policy, VPN membership policy, service advertisement and insertion policy
7. Location Services: Geo-location
8. Soporte de redes celulares: Integrated or module 4G/LTE modem, circuit of last resort (no es excluyente).
9. System and Network Services: IPv4, SNMP, NTP, DNS client, DHCP client, DHCP server, DHCP relay, config archival, Syslog, SSH, SCP, NAT/PAT, Cflowd, VRRP o similar en IPv4 e IPv6.
10. Configuration and Monitoring: Netconf over SSH, CLI, REST, Linux shell, Netflow o similar.
11. Multicast: PIM-SM, PIM-SSM, Auto-RP IGMP V1 V2 Y V3.

9.1.9 Hardware

Las características que deben cumplir los routers SD WAN a proveer son las siguientes:

ROUTERS con 6 puertos utilizables, modelo Cisco C8300 o superior:

Características Routers SD WAN a proveer:

1. Memory (DRAM) default 8 GB
2. Storage (M.2 SSD) default 16 GB
3. Puertos de tráfico para conectarse a los ISPs y la red SD Access interna, por router mínimo 2x1G SFP, más 4x1G Ethernet, 6 puertos en total utilizables al unísono.
1. Hardware embebido para aceleración de cifrado.
2. Soporte de 4G LTE SIM (no es excluyente).
3. Puerto de Management Ethernet. Cantidad1, Tipo: RJ-45 10/100/1000
4. Opciones de fuentes de poder: 1+1 PSU Hot Swappable.
5. Máximo ancho de banda agregado hacia la red WAN: 1.75 Gbps con IPSec en SD WAN.
6. Funcionalidad activa/activo. Alta disponibilidad, en caso de que existan dos equipos en sitio.
7. Apto para rack estándar de 19"
8. Debe soporta VoIP y tráfico de telefonía
9. Deberá contar con módulos de expansión para agregar más interfaces de red.
10. Cada equipo deberá poder levantar al menos 5000 túneles SD WAN entre dispositivos.

1. La solución deberá ser definida por Software, basada en controlador, donde se separe el plano de control del plano de datos.
2. La solución deberá poseer la capacidad de configurar políticas desde un controlador central.
3. La solución deberá ser capaz de reducir los tiempos de aprovisionamiento u orquestación de servicios mediante automatización y administración simplificada.
4. La solución deberá poseer la capacidad de ser administrada de manera centralizada desde una plataforma, provista en la solución, que permita configuraciones globales.
5. La solución deberá poseer la capacidad de ser programada vía REST API.
6. La solución deberá poseer la capacidad de obtener visibilidad a través de módulos de analítica provistos en la solución.
7. La solución deberá poseer la capacidad de desplegar nuevos switches sin intervención de los administradores (Zero touch provisioning).
8. La solución deberá poseer capacidad de configurar automáticamente las interfaces según el tipo de dispositivo conectado.
9. La solución deberá poseer la capacidad de implementar múltiples redes de servicio o tenants en la misma red física, utilizando VRFs y las mismas deberán estar aisladas entre sí.
10. Deberá poseer capacidad de asegurar usuarios, dispositivos y aplicaciones basados en políticas de identidad y no en la ubicación de acceso a la red.
11. Deberá soportar la integración y el monitoreo tanto de la red cableada como inalámbrica desde una única plataforma de gestión centralizada.
12. Deberá poseer la capacidad de monitorear dispositivos y usuarios desde la misma plataforma de gestión centralizada de equipos de red, para poder correlacionar problemas en la red con usuarios afectados.
13. Deberá brindar visibilidad de dispositivos conectados: quién / qué / cuándo / dónde / cómo.

9.2.2 Switches de acceso

9.2.2.1 Características generales

1. La solución deberá poseer capacidad de ofrecer servicios de red de capa 2 y 3.

2. Deberá poseer capacidad de manejar Bit rate 100/1000 Mbps auto negociable con posibilidad de configuración manual en los puertos de entrada. Asimismo, en los puertos de entrada deberá poseer la característica MDI/MDIX.

3. Deberá poseer capacidad de operación Half y Full Duplex, con modo de selección automática y manual.

4. Deberá poseer capacidad de controlar el flujo en los puertos configurados como Full Duplex según la norma IEEE 802.3x.

5. Deberá poseer la capacidad de manejar puertos Ethernet IEEE 802.3 / Fast Ethernet IEEE 802.3u / Gigabit Ethernet IEEE 802.3z / Gigabit Ethernet IEEE 802.3ab.

6. Deberá soportar al menos 4 (cuatro) puertos 10 Gigabit Ethernet IEEE 802.3ae, IEEE 802.3z, para uplinks. Las cantidades de puertos para el equipamiento solicitado se detalla en el título 9.5

7. Deberá contar con almacenamiento de sistema operativo en memoria tipo Flash reescribible. Se valorará que el sistema permita actualizaciones de software en línea y parches en caliente sin necesidad de interrumpir su funcionamiento.

8. Deberá poseer soporte para la ejecución de aplicaciones (ej. Wireshark) dentro del Switch; las mismas deberán ser empaquetadas en algún tipo de plataforma de container (por ejemplo, Docker).

9. Deberá poseer puerto USB 2.0 o 3.0 o mini-USB para backups y recuperación del archivo de configuración y backups y recuperación de la imagen de software.

10. Deberá poseer la capacidad de realizar copias de imágenes y configuraciones vía SCP (Secure Copy Protocol) o SFTP.

11. Cada equipo deberá poseer la capacidad de realizar una pila mediante un anillo cerrado (tolerante a fallas con camino redundante) con puertos o módulos de stacking especiales dedicados a tal fin, los cuales deberán ser independientes de los puertos Gigabit solicitados para el uplink. Deben incluirse todos los elementos requeridos para el funcionamiento en stack. No se admitirá el apilado mediante equipos externos o conexiones tipo "cascada".

12. Los equipos deberán poseer capacidad de conformar pilas de stack de al menos 8 (ocho) equipos.

13. Cualquier equipo integrante de una pila de stack deberá poseer la capacidad de ser reemplazado, insertado o removido, sin interrupción del servicio en los restantes equipos.

14. La pila de stack deberá poseer la capacidad de comportarse como una única entidad lógica desde el punto de vista administrativo, de gestión y monitoreo.
15. Deberá poseer capacidad de manejar los siguientes estándares de PoE: IEEE 802.3af y IEEE802.3at.
16. Deberá poseer la capacidad de implementar protocolos de encapsulación (tunelizado) para redes overlay, como ser VXLAN, que permitan el despliegue de redes virtuales escalables.
17. La potencia de POE+ disponible en el chasis debe ser de 400W o superior.
18. Deberá ser apto e incluir los accesorios necesarios para montaje en racks estándar de 19".
19. Los equipos deben operar en el rango mínimo de temperaturas de 0 a 40 grados centígrados y humedad relativa de 10% a 90% no condensante.
20. Alimentación de potencia: voltaje de entrada entre 200-240V, Frecuencia 50 Hz
21. El equipo debe contar con las siguientes certificaciones relacionadas con seguridad ambiental, inmunidad y control de emisiones: IEC 60950-1, UL 60950, FCC CRF Title Sub B Class y/o Part 15 Class A.

9.2.2.2 Configuración solicitada (mínima)

1. Deberá ser posible de insertar fuente de alimentación redundantes internas extraíbles en caliente (hot-swappable). Solo se solicita una unidad por Switch en esta etapa.
2. La solución deber tener ventiladores redundantes extraíbles en caliente.
3. La solución deberá contar con 24 (veinticuatro) o 48 (cuarenta y ocho) interfaces 10/100/1000 Base T en RJ45. Las cantidades de puertos para el equipamiento solicitado se detalla en el título 9.5
4. La solución deberá contar con al menos 4 (cuatro) slots libres para la inserción de módulos SFP, uplinks 1/10Gbps SFP/SFP+. De necesitarse más interfaces, se solicitará expresamente en el apartado de hardware.

9.2.2.3 Rendimiento

1. Deberá poseer la capacidad de manejar tramas Jumbo de 9.000 Bytes en todos sus puertos.
2. Deberá poseer la capacidad de realizar el manejo de 30.000 direcciones MAC como mínimo.
3. Los Switches deberán ser wirespeed. Los Switches de 24 puertos deberán poseer la capacidad de reenviar trafico al menos por 90 Mpps, y los switches de 48 puertos de reenviar tráfico por 130 Mpps.

4. Cada puerto deberá soportar velocidad "wired speed" / "line rate".
5. Deberá poseer la capacidad de soportar al menos 4095 VLANs.
6. Soporte de PBR (Policy Based Routing).

9.2.2.4 Funcionalidades de capa 2

1. Deberá poseer compatibilidad con todos y cada uno de los siguientes estándares: Spanning Tree IEEE 802.1D (STP), IEEE 802.1p (CoS), IEEE 802.1Q (VLANs), IEEE 802.1w (RSTP), IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1X (Security), IEEE 802.3u: 100BASE-T, IEEE 802.3ab: 1000BASE-T, IEEE 802.3z: 1000BASE-X, IEEE 802.3ad (Link Aggregation Control Protocol), IEEE 802.3x (Flow Control).
2. Deberá poseer capacidad de realizar SPAN y RSPAN.
3. Deberá poseer capacidad de definir dominios de broadcast (VLANs) en cualquiera de los puertos, por reglas de asignación por puerto, como mínimo.
4. Deberá poseer la capacidad de configurar puertos en la modalidad link aggregation para troncalización y balanceo de carga entre equipos, según estándar IEEE 802.3ad.
5. Deberá poseer la capacidad de realizar asignación dinámica de VLANs con 802.1x o MAC Address Bypass Authentication (MAB), con integración con la Solución de Autenticación y Control de Acceso a la Red especificado en la sección 8.3.1 de Seguridad.
6. Deberá poseer la capacidad de manejar 802.1AB (LLDP) o equivalente CDP.

9.2.2.5 Funcionalidades de capa 3

1. Deberá poseer capacidad de ruteo estático en IPv4 e IPv6.
2. Deberá soportar ruteo dinámico en RIP, OSPFv2, OSPFv3, IS-IS y BGP.
3. Deberá tener soporte para BFD en función de detectar caídas de enlaces.
4. Deberá poseer soporte para segmentación con VRFs como mínimo 255.
5. Deberá poder contar con soporte para etiquetado de tráfico en MPLS.
6. Deberá poseer la capacidad de efectuar ruteo entre las VLANs / servicios de redes.
7. Deberá poseer la capacidad de utilizar el protocolo de redundancia VRRP.
8. Deberá poseer la capacidad de implementar DHCP Relay.
9. Deberá poseer la capacidad de soportar PIM.

2. Deberá poseer la capacidad de notificar al administrador del sistema, por traps SNMP a la consola central de monitoreo, cuando este se aparte de los limites operativos, como asíí también mensajes de syslog que deberán ser registrados en forma local y transferidos a un servidor de logs.
3. Deberá contar con un puerto serial para administración.
4. Deberá poseer la capacidad de ser administrado mediante CLI (Command Line Interface) y SNMP (v2 y v3).
5. Deberá poseer la capacidad de ser administrado mediante SSH (Secure Shell) versión 2 y a través de interfaz gráfica por medio de una conexión segura del tipo SSL o SNMP v3.
6. Deberá poseer una GUI local como configuración alternativa.
7. Deberá poseer la capacidad de implementar filtros de acceso para la gestión del switch.
8. Deberá soportar autenticación de usuarios administrativos vía RADIUS.
9. Deberá poseer la capacidad de manejar alguno de los estándares Netflow / SFLOW / IPFIX / NETSTREAM en cualquiera de los puertos según los estándares RFC vigentes.
10. Deberá poseer interfaces programables NETCONF/RESTCONF o YANG.
11. Deberá contar con la capacidad de ejecución de scripts en el mismo switch con algún lenguaje de programación.

9.2.3 Extensores

En los aeropuertos en donde EANA posea dependencias separadas a una distancia superior de 100 metros, se deberá proporcionar extensores de red LAN. En cada sala técnica principal habrá al menos un switch, al cual se conectarán dichos extensores directamente por medio de dos fibras SM. Los extensores heredan las características del switch, y la conmutación de paquetes se realiza en el switch. Las cantidades del equipamiento solicitado se detalla en el título 9.5

Características Generales:

1. Se solicitan 12 puertos de 10/100/1000 Gigabit Ethernet, más dos uplinks combo, tanto de 2 x 1G copper como de 2 x 1G SFP.
2. Deberá soportar la configuración de SD Access junto con el switch al que se conecta.
3. Debe poseer fuente de alimentación para conectar a la línea de 220V AC, capaz de suministrar al menos 240W de PoE+
4. Licenciamiento SD Access capaz de soportar las políticas de seguridad definidas para los switches en este pliego.

9.2.4 Sistema de administración, monitoreo y análisis de la red

El sistema de administración deberá ser capaz de monitorear todos los elementos que componen la red, siendo parte de la solución la provisión del licenciamiento necesario para cubrir la funcionalidad solicitada en los siguientes puntos. Las cantidades del equipamiento solicitado se detalla en el título 9.5

1. proveer una interfaz gráfica (GUI) de gestión.
2. Se deberá proveer, instalar, configurar y poner en funcionamiento un Sistema de Administración, Monitoreo y Análisis de Red para la totalidad del equipamiento especificado, incluyendo software, hardware y licencias necesarias para su instalación y puesta en marcha. Dicho sistema debe ser unificado.
3. Deberá contar con el inventario de todo el equipamiento de electrónica de red ofrecido en esta contratación.
4. Deberá permitir el descubrimiento de dispositivos en la red, a través de un barrido IP o protocolos de descubrimiento como LLDP o equivalente.
5. Deberá poder mostrar topologías de red descubiertas de forma automática de toda la electrónica de red motivo de esta contratación.
6. Deberá soportar la implementación de redes tipo SDN (overlay) en distintos sitios/segmentos de la red. El despliegue de este tipo de redes deberá poder especificarse de forma jerárquica por sitio.
7. Para las redes SDN, deberá soportar la automatización de todas las configuraciones de los equipos involucrados en esta contratación.
8. El sistema de Administración, Monitoreo y Análisis de Red deberá funcionar como un todo junto a la solución de Autenticación y Control de Acceso a la Red.
9. En líneas generales, el Sistema de Administración, monitoreo y Análisis de Red deberá contemplar lo siguiente:
   a. Administración de los dispositivos de red.
   b. Escaneo de red de manera de actualizar en forma automática el inventario de equipamiento. El inventario deberá estar agrupado en estructuras jerárquicas.
   c. Identificar niveles de severidad de alarma como falla critica, falla mayor, falla menor y advertencia, utilizando diferentes colores o palabras. Notificar a los administradores en el panel y mediante alertas sonoras, e-mail, etc., a fin de resolver fallas de manera rápida y precisa.

d. Deberá poseer capacidad de identificar problemas de hardware en todas las interfaces físicas de los componentes de electrónica de red de esta contratación.

e. La solución deberá recomendar imágenes de software ideales para cada dispositivo, según lo determinado por el fabricante y las vulnerabilidades conocidas.

f. La solución debe alertar la presencia de dispositivos en el inventario corriendo imágenes de software con vulnerabilidades detectadas y publicadas por el fabricante.

g. Monitoreo de los indicadores de performance de todos los dispositivos de red que forman parte de esta contratación, como ser el uso de la CPU, uso de memoria, conectividad del dispositivo, tiempo de respuesta del dispositivo, tráfico de puertos, velocidad de conectividad de la red y nivel de utilización.

h. Obtención de un registro histórico detallado de eventos de red e información de los usuarios y los dispositivos finales conectados de manera de identificar de manera temprana de problemas que afecten la experiencia de los usuarios.

i. Actualización de software de los equipos de electrónica de red, chequeando los prerrequisitos para el correcto funcionamiento de la nueva versión a desplegar.

j. Colección de estadísticas históricas para poder realizar un análisis de tendencias en la red.

k. Configuración de parámetros/políticas iguales simultáneamente en múltiples dispositivos tanto cableado como inalámbrico, con una única acción.

10. Deberá poseer la capacidad de detectar tempranamente los problemas por medio de motor de analítica sin necesidad de contar con software o soluciones de terceras partes, permitiendo realizar tareas de aseguramiento de la calidad de red

11. Deberá poseer capacidad de identificar automáticamente problemas de red y predecir proactivamente los mismos utilizando herramientas de Inteligencia Artificial.

12. Deberá poseer la capacidad de revisar fallas o problemas ocurridos en el pasado, permitiendo visualizar hasta 10 días de antigüedad.

13. Deberá poseer capacidad de colectar variedad de datos de telemetría y correlacionar la información proveniente de múltiples fuentes, incluidos switches, NAC, topología, entre otros.

14. Debe permitir visibilidad de salud de red y dispositivos de clientes.

15. Deberá poseer capacidad de ser consultados por otras aplicaciones por medio de APIs abiertas.
16. Deberá poseer la capacidad de desplegar nuevos switches sin intervención de los administradores (Zero touch provisioning).
17. Deberá contar con un wizard y templates de configuración para múltiples dispositivos.
18. La consola de administración deberá poseer la capacidad de definir cuentas de administrador basadas en roles.
19. Deberá generar reportes.
20. La GUI deberá permitir ejecutar comandos (CLI) en equipos de red, desde la misma consola, con el objetivo de simplificar la resolución de problemas (troubleshooting).
21. Deberá proporcionar la capacidad de administrar eventos detectados y reportados, indicando si ya fueron resueltos, si aún se encuentran abiertos o si se los prefiere ignorar.
22. Deberá proporcionar visibilidad sobre las licencias adquiridas relativas a esta plataforma de administración desde la misma GUI, para facilitar su administración, sin necesidad de ir a sitios del fabricante o terceras páginas.
23. Se deberán permitir capacidades de microsegmentación y macrosegmentación de la red en un entorno que involucre una combinación de tecnologías de VRF, vlan (virtual LAN) y etiquetado de paquetes inteligentes adicionalmente a QoS, de manera de ofrecer una mayor granularidad en el control de la información de determinadas aplicaciones.

9.3 WIFI

Las características mínimas de los equipos a suministrar y herramienta de gestión y monitoreo se detalla en los siguientes subtítulos:

a. WIRELESS LAN CONTROLLER
b. ACCESS POINT

Se aclara que, el adjudicatario deberá realizar los estudios de radiofrecuencia e interferencia electromagnética necesarios, de modo de asegurar que la ubicación y características de los Access points a proveer, sea acorde a la concurrencia y ancho de banda que se desea garantizar a los usuarios de cada área de cobertura de la red inalámbrica.

9.3.1 Wireless controller

Software Controlador Wifi

1. La cantidad mínima total, físicos o virtuales será de 2. En caso de que sea físico debe contar con dos interfaces de 10G por caja.
2. Deberá soportar una cantidad mínima de 50 Access point
3. Debe soportar la cantidad mínima de 1000 clientes
4. Deberá proveer control centralizado y administración de los Access points.
5. Protocolos de Redes Cableadas a Soportar, en la opción de dispositivo físico:
   a. IEEE 802.3u 100BASE-TX specification, 1000BASE-T. 1000BASE-SX, 1000-BASE-LH
   b. IEEE 802.1Q VLAN tagging
6. Protocolos de Redes Inalámbricas a Soportar:
   a. IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave1 and Wave2, 802.11ax
7. Compatibilidad con Protocolos y Estándares
   a. RFC 768 UDP
   b. RFC 791 IP
   c. RFC 2460 IPv6
   d. RFC 792 ICMP
   e. RFC 793 TCP
   f. RFC 826 ARP
   g. RFC 1122 Requerimientos para hosts de Internet
   h. RFC 1519 CIDR
   i. RFC 1542 BOOTP
   j. RFC 2131 DHCP
   k. RFC 5415 CAPWAP Protocol Specification

Seguridad:

1. Compatibilidad con Estándares de Seguridad. Debe cumplir con los siguientes estándares de seguridad:
   a. WPA

b. IEEE 802.11i (WPA2, RSN)

c. RFC 1321 MD5 Message-Digest Algorithm

d. RFC 1851 The ESP Triple DES Transform

e. RFC 3280 Internet X.509 PKI Certificate and CRL Profile

f. RFC 4347 Datagram Transport Layer Security

g. RFC 5246 TLS Protocol Versión 1.2

h. Advanced Encryption Standard (AES), Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

i. Data Encryption Standard (DES): DES-CBC, 3DES

j. Secure Sockets Layer (SSL) y Transport Layer Security (TLS): RC4 128-bit y RSA 1024- y 2048-bit

k. IEEE 802.1X

l. RFC 2865 RADIUS Authentication

m. RFC 2866 RADIUS Accounting

n. RFC 2867 RADIUS Tunnel Accounting

o. RFC 2869 RADIUS Extensions

p. RFC 3576 Dynamic Authorization Extensions to RADIUS

q. RFC 5176 Dynamic Authorization Extensions to RADIUS

r. RFC 3579 RADIUS Support for EAP

s. RFC 3580 IEEE 802.1X RADIUS Guidelines

t. RFC 3748 Extensible Authentication Protocol (EAP)

u. Web-based authentication

v. IPsec: DES-CBC, 3DES, AES-CBC

2. La solución deberá poseer capacidad de bloquear el acceso a los usuarios a partir de una hora prefijada.

3. Deberá poseer la capacidad de acceder vía portal cautivo (splash page) vía HTTPS con los siguientes métodos de autenticación, conforme se requiera:

- Portal cautivo directo, donde no se requieren credenciales de usuario, pero permite desplegar un mensaje de bienvenida previo al acceso a Internet del usuario.
- Portal "Click-through", donde el usuario debe ver un portal de bienvenida (que incluya términos y condiciones) y dar "click" a un botón para continuar su acceso.
- Portal cautivo tipo "sign-on", donde se le requiera al usuario sus credenciales de usuario y contraseña para su autenticación.

4. Deberá contar con la funcionalidad de Walled Garden, que permita el acceso a direcciones públicas y/o dominios de Internet específicos, previos a la autenticación del cliente.
5. La solución deberá poseer capacidad de generar distintas redes de usuarios o servicios (Guest/Clientes) y solo tendrá conexión a Internet y no estará vinculada a la red de EANA.

ADMINISTRACION

1. Debe soportar los siguientes protocolos:
   a. SNMP v1, v2c, v3
   b. RFC 854 Telnet
   c. RFC 2616 HTTP
   d. RFC 1350 Trivial File Transfer Protocol (TFTP)
   e. RFC 2030 Simple Network Time Protocol (SNTP)
   f. RFC 3414 User-Based Security Model (USM) for SNMPv3
   g. RFC 4741 Base NETCONF protocol
   h. RFC 4742 NETCONF over SSH
   i. RFC 6241 NETCONF
   j. RFC 6020 YANG
   k. RFC 3164 Syslog
2. Portal de administración web vía http o https
3. Administración vía CLI: Telnet, Secure Shell (SSH) Protocol, serial port

Características Avanzadas

1. Debe permitir la portabilidad (roaming) de dispositivos entre distintas sedes a Nivel 2

2. Mediante la consola de administración, y sin necesidad de agregar un equipo externo adicional, se debe poseer la capacidad de limitar o garantizar el ancho de banda por usuario y por SSID de manera simétrica (mismo ancho de banda de bajada y de subida) o asimétricamente (diferente ancho de banda de bajada y subida), y desde cada Access Point.
3. La asignación de ancho de banda deberá poderse definir mediante dos mecanismos:
   a. Manual: Rangos CIDR/IP, hostname (URL), Puertos UDP/TCP, Combinación de Red, Subnet y puerto, Red local (subredes y redes de clase completa en la LAN)
   b. Mediante categorías de tráfico: Blogging, Email, Compartición de archivos, Juegos, Noticias, Respaldo en línea, Peer-to-Peer, redes sociales, actualizaciones de programas y antivirus, Deportes, VoIP y videoconferencia, compartir archivos vía web
4. Deberá poseer capacidad de, mediante reglas de capa 3 y 4, definir políticas de acceso por:
   a. Protocolo (UDP o TCP)
   b. Host, subred o red origen
   c. Puerto TCP o UDP origen
   d. Host, subred o red destino
   e. Puerto TCP o UDP destino
5. Deberá poseer capacidad de restringir tráfico mediante reglas de capa 7 a partir de categorías predefinidas. Al menos deberá identificar las siguientes categorías:
   a. Blogging
   b. Email
   c. Compartición de archivos
   d. Juegos
   e. Noticias
   f. Respaldo en línea
   g. Peer-to-peer
   h. Redes sociales
   i. Actualizaciones de programas y antivirus
   j. Deportes

k. VoIP y videoconferencia

l. Compartir de archivos vía web

m. Streaming

6. La solución deberá contar con la funcionalidad de selección de la banda de operación por cada SSID:

   a. Modo dual, publicando el SSID en ambas bandas, 2.4 y 5 GHz.

   b. 5 GHz únicamente.

   c. Ambas bandas, pero con la capacidad de detectar dispositivos que soporten ambas bandas, direccionándolos a la de 5 GHz por estar menos congestionada.

9.3.2 Access point

Características Generales

Dispositivo del Tipo Access Point

1. Deberán poseer capacidad de crear al menos 8 SSID por Access Point.
2. Cada Access Point deberá soportar los siguientes esquemas de direccionamiento IP:

   a. Modo NAT, donde los usuarios pueden recibir una dirección directamente desde el Access Point, a fin de ahorrar direcciones IP privadas de la red local, o prescindir de un servidor DHCP.

   b. Roaming de capa 3 (L3), que permita al usuario mantener la misma dirección IP en caso de cambio de segmento de red, manteniendo la sesión activa todo el tiempo.

3. Los Access Points deberán disponer de un radio de Bluetooth Low Energy (BLE) (beacons bluetooth). Éste permitirá actividades de interacción con una aplicación móvil, mandando notificaciones. También permitirá actividades de monitoreo de entrada y salida de dispositivos que emitan beacons, mandando alertas de estos eventos. El radio de BLE deberá ser dedicado e independiente a los radios de usuarios.
4. Deberá contar con "dual stack" IPV4/IPV6

Características de Antena

1. Debe estar incluida teniendo la capacidad de funcionar en los rangos de frecuencia de 2.4 GHz y 5 GHz.
2. Deberán disponer de antenas integradas al interior del equipo del tipo omnidireccional

3. La ganancia de las antenas de los AP deberá ser de 3 dBi en la banda de 2.4 GHz y de 4 dBi en la banda de 5 GHz.
4. Soporte de calibración automática del radio transmisor.
5. Deberá soportar dos flujos espaciales, MU-MIMO que permita que los puntos de acceso dividan flujos espaciales entre dispositivos cliente.
6. Debe soportar un mínimo de 2x2 spatial streams (2 flujos emisores y 2 receptores) por radio

Estándares de Seguridad Soportado

1. Debe soportar IEEE 802.11i para Acceso WiFi Protegido WPA, WPA2 y WPA3.
2. Debe soportar protocolos de autenticación extensibles (EAP) IEEE 802.1X para autenticación basada en el usuario, como mínimo: PEAP, MSCHAPv2, EAP-TLS, EAP-TTLS.
3. Los usuarios conectados a un SSID, estén validados o no, no deberán poder tener visibilidad del tráfico de los otros usuarios, incluso dentro de la misma red.
4. La solución de red inalámbrica deberá contar con un sistema de defensa y análisis de interferencia que tenga por funcionalidad el escaneo en tiempo real de interferencia en los canales de las bandas de 2.4 y 5 GHz.

Estándares de Calidad de Servicio

1. Debe soportar WiFi Multimedia (WMM) y calidad de servicio (QoS) compatible con IEEE 802.11e
2. Deberá poseer capacidad de manejar DSCP y 802.1p.

Puertos LAN

1. Deberán disponer al menos una interfaz gigabit.

Administración

1. Deberá contar con la capacidad de gestión centralizada de los APs.
2. El sistema de gestión centralizado deberá dar la opción de enviar nuevo firmware a los APs, para habilitar nuevas funcionalidades sin costos adicionales y entregar parches de seguridad.
3. Deberá contar con un puerto de administración local del tipo RJ45

Alimentación y Entorno

1. Los equipos deberán soportar alimentación PoE/PoE+, compatible con IEEE 802.3af/at, así como también por medio de un transformador a corriente continua.

2. Deberá funcionar en un rango de temperatura ambiente entre mínimo 0°C y máximo 50°C

Compatibilidad

Deberán ser compatibles con los estándares IEEE 801.11ax (Wifi 6) IEEE 801.11ac, IEEE 801.11ac Wave 2, IEEE 802.11n, definidos por WiFi Alliance.

9.4 Seguridad

Las características mínimas de los equipos a suministrar y herramientas de gestión y monitoreo relacionados a Seguridad se detallan en los siguientes subtítulos:

- NAC-Seguridad
- Firewall
- Licencias Malware Protection
- DNS Security
- Licencias Solución para Multi-Factor Authentication (MFA)

9.4.1 NAC-SEGURIDAD

La propuesta debe contemplar todo lo necesario para:

- Identificar y brindar acceso seguro de usuario Guest.
- Identificar y brindar acceso seguro de Empleados vía WIFI.
- Identificar distintos tipos de dispositivos para generar distintos accesos según sus características.
- Identificar y brindar acceso seguro de la red cableada.
- La solución deberá ser capaz de realizar segmentación de la red.
- Deberá brindar la posibilidad de hacer el "Onboarding" de los dispositivos propios de usuarios que quieran utilizar dichos equipos para realizar sus tareas.
- Deberá ser capaz de identificar los dispositivos y darle acceso a los lugares de la red que los administradores considere.

La solución debe cumplir con las siguientes características:

Autenticación de usuarios y dispositivos a la red.

1. La solución deberá implementar autenticación de dispositivos y usuarios a la red utilizando el protocolo IEEE 802.1X, soportando por lo menos los siguientes métodos EAP: EAP-MD5, EAP-TLS, PEAP, EAP-FAST y EAP-GTC.

2. Debe permitir la autenticación de usuarios/dispositivos usando las siguientes fuentes de información de identidad:
   a. Interna, de usuario
   b. Interna, de dispositivo
   c. Con Autoridad Certificadora interna
   d. Externa vía RADIUS
   e. Externa vía LDAP
   f. Externa vía IdPs de SAMLv2
   g. Interna/Externa vía Windows Active Directory
   h. Externa vía Autoridad Certificadora de terceros.
   i. Externa vía ODBC
   j. Externa con servidores de Tokens
3. La solución deberá ofrecer autenticación de usuarios a través de un portal web seguro HTTPS con redireccionamiento automático, tanto en red inalámbrica como en red alámbrica.
4. La solución deberá implementar autenticación específica para dispositivos basada en MAC Address.
5. La solución deberá contar con una base de datos interna para registro de dispositivos basada en MAC Address, pudiendo esta base ser cargada automáticamente mediante un mecanismo de detección automática de perfil de los dispositivos.
6. La solución deberá implementar validación de certificados digitales con las siguientes características:
   a. Soportar integración a una CA (Certificate Authority) externa.
   b. Soportar la consulta periódica de lista de revocación CRL (Certificate Revocation List) vía HTTP
   c. Soportar el protocolo OCSP para verificación de estado de certificados.
   d. Soportar una CA interna para dispositivos tipo BYOD (Bring Your Own Device).
7. La solución deberá implementar un mecanismo flexible de reglas que permita seleccionar la base de datos donde será autenticado un usuario y/o dispositivo en base a atributos

RADIUS existentes en la solicitud enviada por el equipo de red y tipo de protocolo, permitiendo al menos las siguientes combinaciones de reglas:

a. Alámbrico 802.1x

b. Inalámbrico 802.1x

c. Autenticación sin 802.1x

8. El sistema deberá poder obtener información de otros sistemas para realizar identificación pasiva de usuarios, a través de protocolos/especificaciones como syslog y API REST.

9. El sistema deberá poder brindar información para identificación pasiva de usuarios hacia otros sistemas a través de un API.

Autorización

1. Debe implementar asignación de VLAN asignada por el servidor de control de acceso.

2. Debe implementar asignación de ACL descargable automáticamente por el Sistema de Control de Acceso.

3. Debe implementar asignación de ACL de tipo "filter-id"

4. Debe implementar asignación de ACL tipo "nombradas" compatible con controladoras wireless que posee actualmente la organización.

5. Debe implementar asignación de ACL de tipo Redireccionamento Web compatible con Switches y controladoras Wireless Cisco.

6. Debe implementar gestión centralizada de ACLs basadas en etiquetas de grupo de seguridad y el monitoreo en tipo real del tráfico etiquetado.

7. Debe implementar asignación de política MacSec conforme al estándar IEEE802.1AE

8. Debe implementar asignación de dominio de voz para teléfonos IP (Voice Domain).

9. Debe implementar asignación de parámetro de re-autenticación 802.1X

10. Debe contar con la funcionalidad de configurar dinámicamente los puertos de acuerdo al tipo de dispositivo detectado en el puerto

11. Debe permitir la personalización de atributos de autorización

12. Debe permitir el agrupamiento de atributos de autorización

13. Debe permitir la creación de perfiles de usuarios.

14. Debe permitir autorización de acceso condicional en base a los siguientes factores:

a. Atributos LDAP del usuario autenticado
b. Grupo de Active Directory del usuario autenticado
c. Contenido del certificado digital (CN, OU)
d. Horario de conexión
e. Medio de acceso
f. Ubicación
g. Tipo de dispositivo (ejemplo: IPad, IPhone, Android, Windows, Mac OS)
h. Cumplimiento de políticas de postura en sistemas Windows, MAC OS y móviles vía integración a MDM
i. Posicionamiento físico de un dispositivo inalámbrico en base a un área definida, vía integración a algún Sistema de Ubicación.

15. Debe permitir la libre combinación de los factores descritos en el ítem anterior.

16. Implementar el estándar RADIUS Change of Authorization (CoA).

Gestión de cuentas temporales – Visitantes/Consultores

1. Debe implementar un portal web seguro SSL para la creación de cuentas temporales de tipo "visitante, consultor" con autenticación de autorizadores en base externa do tipo Active Directory, LDAP y asignación de privilegio al autorizador según su perfil.

2. Debe permitir la creación de perfiles de cuentas temporales pudiendo asignar distintos privilegios de acceso a la red, contando con al menos los siguientes privilegios (no limitativo):

a. Perfil Visitante – Solamente acceso HTTP a Internet
b. Perfil Consultor – Solamente acceso HTTP a Internet e Intranet

3. Deberá permitir a los visitantes hacer login con cuentas de redes sociales

4. Debe permitir la creación de "Perfiles de Tiempo" estipulando, por ejemplo, las siguientes opciones de duración:

a. La cuenta temporal tiene validez de 1 día a partir de su creación.
b. La cuenta temporal tiene validez de 7 días a partir de su creación.
c. La cuenta temporal tiene validez de 1 día a partir del primer login.

d. La cuenta temporal tiene validez de 7 días a partir del primer login.

e. El autorizador determinará el inicio y fin de cada cuenta en función de su privilegio de autorizador

5. Debe permitir la creación de grupos de autorizadores con privilegios distintos de creación de cuentas temporales, especificando los siguientes privilegios por grupo:

a. Crear cuenta individual

b. Crear cuentas aleatorias

c. Importar cuentas desde un archivo .csv

d. Enviar credenciales vía Email

e. Enviar credenciales vía SMS

f. Ver la contraseña de la cuenta de visitante

g. Imprimir los detalles de la cuenta de visitante

h. Ver y editar las cuentas creadas por todos los grupos de autorizadores

i. Ver y editar las cuentas creadas por el mismo grupo de autorizadores

j. Ver y editar las cuentas creadas por el propio autorizador

k. Suspender cuentas creadas por todos los grupos de autorizadores

l. Suspender cuentas creadas por el mismo grupo de autorizadores

m. Suspender cuentas creadas por el propio autorizador

n. Duración máxima de la cuenta de visitante

o. Especificar el Perfil de acceso a la red que será asignado a la cuenta visitante

p. Especificar el Perfil de Tiempo que será asignado al visitante

6. Debe permitir la personalización del formulario de creación de cuentas temporales que será completado por el autorizador, especificando cuáles campos son obligatorios y cuáles son opcionales. Se debe permitir además la creación de nuevos campos customizados. Con todo, el formulario a ser completado deberá permitir especificar como mínimo los siguientes campos:

a. Nombre

b. Apellido

c. Email

d. Empresa

e. Teléfono

f. Campos personalizados

7. Debe permitir la customización del nivel de seguridad de la contraseña temporal que será asignada al visitante, especificando la cantidad mínima de caracteres, cantidad de caracteres especiales y cuántos números serán utilizados para componer la contraseña temporal.

8. Debe implementar un portal web seguro (HTTPS) que se presentará automáticamente a los usuarios temporales (visitante/consultor) durante su conexión a la red (hotspot).

9. Debe permitir la customización de las páginas de portal captivo (visitante/consultor) deberán poder ser personalizadas, y la solución deberá integrarse a un editor gráfico exclusivo para este propósito, mismo que permitirá agregar contenido imágenes, texto, botones y modificar temática del portal (columnas, colores, etc.)

10. El layout de los portales deberán ser adaptables al tipo de dispositivo de usuario final, ya sea móvil o de escritorio.

11. Debe poseer soporte nativo de idiomas Inglés y Español.

12. Debe poder implementar la opción de "self-service" que permita al usuario visitante crear su propia cuenta temporal directamente a través del portal seguro hotspot sin necesidad de un autorizador.

13. Debe implementar las siguientes funciones en el Portal Web (hotspot):

    a. Permitir el cambio de contraseña del usuario visitante directamente en el portal seguro

    b. Determinar el número máximo de días antes de exigir un cambio de contraseña

    c. Determinar el número máximo de errores de login antes de bloquear la cuenta

    d. Exigir en cada login en la red la aceptación de "Términos de uso aceptable de red"

    e. Exigir solamente en el primer login la aceptación de "Términos de uso aceptable de red"

    f. Customización de la página de "Términos de uso aceptable de red"

14. Deberá contar con un REST API para poder efectuar altas, cambios y bajas a cuentas de invitados desde sistemas externos a la solución (p. ej. un sistema de control de acceso físico)

Clasificación automática de dispositivos (Perfilamiento)

1. Debe poder implementar un mecanismo de perfilamiento automático y transparente de dispositivos que se conecten a la red inalámbrica y cableada, clasificándolos en alguna de las siguientes categorías:
   a. Apple Device – Iphone, Ipad, Ipod, MAC
   b. Android Devices
   c. Impresora – Lexmark, HP, Xerox
   d. Teléfono IP – Cisco, Avaya
   e. Workstation/Notebook – Windows, MAC OS, Linux
   f. Dispositivos tipo IoT como televisores, cámaras IP, proyectores, sensores de edificios inteligentes
2. Debe poder implementar los siguientes mecanismos para recolectar información de dispositivos, para ser utilizada en la construcción de reglas de perfilamiento.
   a. Recolección de tráfico DHCP y HTTP enviado por el dispositivo
   b. Recolección de tráfico Netflow
   c. Recolección de atributos RADIUS relacionados con la sesión de 802.1X del dispositivo.
   d. Consulta SNMP al switch de acceso o controladora wireless
   e. Consulta DNS para resolución de nombre
   f. Iniciar validación de puertos abiertos TCP contra el dispositivo.
   g. Recolección de tráfico LLDP

Recolección de información de dispositivo desde el Directorio Activo

1. Debe contar con una interfaz para la construcción de reglas customizadas de clasificación de dispositivos, adicional a poder asignar pesos y nivel de certeza.
2. Debe permitir la creación de reglas y categorías customizadas
3. Debe contar con una base de reglas y categorías pre-configuradas
4. Debe soportar un mecanismo de actualización de reglas y categorías pre-configuradas.
5. Debe permitir que la clasificación del dispositivo perfilado sea utilizada como parámetro de autorización en las reglas de acceso de dispositivos.

6. Debe permitir que el administrador registre manualmente un determinado dispositivo en una categoría

7. El sistema debe poder suscribirse y descargar automáticamente nuevas categorías y reglas desde el sitio del fabricante.

Postura de Admisión (Verificación)

1. La solución deberá permitir la verificación de postura de estaciones de usuario en las siguientes formas:

   a. **Agente Instalado**: Agente que se instala en la estación del usuario, encargado de la recolección de información referente a postura. El agente deberá encargarse sólo de la verificación de postura de la estación. Todo el control de nivel de acceso a la red, control de tiempo concedido y control de ancho de banda deberán ser efectuados a través del Sistema de Control de Acceso

   b. **Agente Temporal** (en formato .exe ó .dmg): Agente que se carga en la estación al momento de la verificación de postura para la recolección de información referente a postura. El agente deberá encargarse sólo de la verificación de postura de la estación. Todo el control de nivel de acceso a la red, control de tiempo concedido y control de ancho de banda deberán ser efectuados a través del Sistema de Control de Acceso.

2. El Agente (Instalado o Temporal) deberá permitir la verificación de los siguientes ítems:

   a. Sistema Operativo Instalado

   b. Verificación del Service Pack Instalado

   c. Llaves de Registro de Windows

   d. Archivos existentes en la estación del usuario

   e. Estatus de los servicios en ejecución en la máquina

   f. Existencia de Software Antivirus y AntiSpyware Instalado

   g. Fecha de la última actualización del Antivirus

   h. Estatus del software Antivirus (Habilitado o Deshabilitado)

   i. Verificación de Hotfixes de Windows Instalados

   j. Inventario de Aplicaciones instaladas

   k. Estado de cifrado de disco duro

   l. Puertos USB

3. La solución deberá permitir la verificación de la última versión de antivirus provista. La solución deberá ser capaz de verificar cuál es la última firma disponible y su fecha respectiva. Deberán ser soportados los siguientes fabricantes de Antivirus:

   a. Symantec

   b. Trend Micro

   c. McAfee

   d. AVG

   e. Kaspersky

   f. Panda

   g. Sophos

   h. ClamAV

   i. Avira

4. La solución deberá contar con una base de datos actualizada periódicamente con la información de firmas de antivirus, Antispyware y Hotfixes Microsoft.

5. El proceso de verificación de postura, aislamiento y remediación deberá soportar un ambiente de telefonía IP, donde el equipo de cómputo se conecta en el puerto de red del teléfono IP y no directamente al switch. Se requiere que el fabricante aclare el diseño y componentes necesarios para lograr esto.

Control de dispositivos personales y "BYOD (Bring Your Own Device)"

1. La solución deberá permitir la creación de reglas para diferenciación de dispositivos corporativos y personales, haciendo posible la adopción de políticas de "BYOD (Bring Your Own Device)"

2. Deberá proveer un portal para que los usuarios registren y administren sus propios dispositivos para su uso en la red.

3. Deberá permitir la integración con sistemas MDM (Mobile Device Management)

4. Se deberá soportar una Autoridad Certificadora interna para el aprovisionamiento y gestión de certificados digitales a los dispositivos de BYOD.

5. El auto-registro de dispositivos de los usuarios deberá soportar el aprovisionamiento de un certificado digital que identifique al dispositivo BYOD y sirva como método de autenticación para la red alámbrica e inalámbrica.

6. El administrador tendrá capacidad de suspender/reactivar dispositivos y de revocar certificados desde la interfaz dentro de la misma solución.

Gestión de equipos de red

1. La solución debe poder gestionar la autenticación, autorización y contabilidad en dispositivos de red como switches, routers, firewalls, equipos de red inalámbrica y adicionales por medio del protocolo estándar TACACS+.
2. La gestión de AAA por medio de TACACS+ deberá permitir la autorización granular de los comandos que un administrador de red puede ejecutar en un equipo de red configurado con este protocolo.
3. Se deberán tener perfiles de autorización de comandos predefinidos (out-of-the-box) para la gestión de controladores inalámbricos, ruteadores y switches, de tal manera que no se tengan que construir listas de comandos desde cero.
4. Se deberán poder generar bitácoras para auditorías de autenticaciones, autorizaciones y comandos ejecutados en los dispositivos de red configurados con TACACS+.
5. Se deberá soportar la función de proxy de protocolo TACACS+
6. Se requiere soporte de TACACS+ sobre IPv6

Gestión y Administración

1. La solución deberá ser capaz de administrar, configurar e modificar reglas y políticas a través de una interfaz gráfica web, accesible por HTTPS.
2. Debe contar con un Dashboard para la rápida visualización de la siguiente información sumarizadas:
   a. Métricas de las últimas 24 horas
      - Número de dispositivos activos
      - Número de visitantes activos
      - Tiempo promedio para la remediación de dispositivos
      - Porcentaje de dispositivos que cumplen la postura
      - Número de dispositivos perfilados
      - Numero de dispositivos rechazados que intentaron acceso
   b. Información de desempeño, CPU, Memoria de cada componente de la solución.

c. Cantidad total de fallas de autenticación en las últimas 24 horas y el motivo principal.

3. Debe contar con una pantalla de monitoreo continuo de autenticaciones en tiempo real con visualización inmediata de la siguiente información:

   a. Fecha y hora

   b. Capacidad de hacer drill-down hacia los detalles avanzados de autenticación y autorización

   c. Estatus de la autenticación

   d. Nombre de usuario/dispositivo

   e. Dirección MAC

   f. Dirección IP

   g. Equipo de red donde se conectó

   h. Interfaz de red donde se conectó

   i. Perfil de Autorización asignado

   j. Resultado de perfilamiento del dispositivo – Categoría

   k. Estatus de Postura (cumplimiento)

   l. Motivo en caso de falla

   m. Método de autenticación

   n. Protocolo de autenticación

4. Deberá ser capaz de generar reportes con información referente al resultado de la verificación de postura de la máquina.

Capacidad e Integración

1. Deberá soportar un mecanismo de alta disponibilidad para las todas las funciones del Sistema de Control de Acceso.

2. En caso de falla de algún appliance (físico o virtual) no se necesitará de intervención manual para recuperar o realizar fail-over.

3. La solución deberá soportar una arquitectura totalmente centralizada de sus servicios, es decir, sin necesidad de implementar appliances fuera del Centro de Cómputo Central y soportando todas las funcionalidades indicadas en las secciones anteriores.

4. La solución deberá soportar la operación en appliances de hardware de propósito específico.
5. En caso de hacerse una implementación de appliances de hardware de propósito específico, deberá contar con capacidad de hacer bonding de interfaces de red.
6. La solución deberá soportar instalarse como una máquina virtual (Vmware o KVM)
7. La API para integración con terceros deberá ser basada en estándares y en arquitectura cliente-servidor descentralizada, de tal manera que las integraciones no serán de 1-a-1 por cada sistema nuevo que se agregue.
8. Con la finalidad de proteger la inversión y evitar costos posteriores que no hayan sido contemplados dentro de este proyecto, se dará preferencia a los sistemas que NO requieran licenciamiento adicional por cada integración hacia terceros.

9.4.2 FIREWALL

La propuesta debe contemplar todo lo necesario para la adquisición, instalación, y puesta en marcha de una solución integral de NGFW. Se necesita incorporar una solución para el control y visibilidad de la seguridad y mitigar los riesgos modernos. La visibilidad y el control son cruciales para una defensa eficaz contra amenazas, no solo para prevenir ataques, sino también para detectar, contener y corregir amenazas rápidamente.

Esta solución de Firewall de nueva generación se deberá poder integrar a una única herramienta que consolide los eventos detectados y/o mitigados tanto en este NGFW como en las soluciones de AntiMalware y de protección de DNS.

La propuesta debe incluir un equipo FW de Nueva generación que cumpla con las siguientes características:

1. Cantidad de FW de nueva generación: 1 en fase 1, lugar de instalación Ezeiza.
2. La solución ofertada debe ser del tipo Next-Generation Firewall.
3. El firmware de la solución propuesta, debe estar firmado digitalmente por el fabricante, de tal manera que se pueda garantizar que el mismo no sea alterado. La secuencia de inicio del dispositivo propuesto debe validar dichas firmas y comprobar su integridad.
4. El sistema debe contar con un proceso de inicio seguro, que identifique y evite las amenazas contra el estado funcional del sistema y firmware utilizando en el mismo. En caso de una modificación ilícita que comprometa el estado de seguridad del sistema el proceso de arranque del mismo debe poder identificar dicha situación.
5. Capacidad de failover activo/pasivo sin necesidad de licencia adicional.

6. El equipamiento ofertado debe ser del tipo para rack de 19".
7. Todo el equipamiento deberá aceptar alimentación eléctrica 220V 50Hz monofásica, sin el uso de transformadores externos.
8. Cantidad de Interfaces mínimas:

n. 12 (doce) interfaces GE RJ45

o. 4 (cuatro) interfaces GE SPF slot

p. 1 (una) interfaz de gestión GE RJ45

q. 1 (uno) puerto de consola o puerto USB en su defecto.

9. La solución propuesta debe tener posibilidad de limitar el ancho de banda utilizado por determinada aplicación, usuario o contenido.

Control de aplicaciones:

1. Capacidad para identificar aplicaciones activas en el mercado (incluyendo aplicaciones Web 2.0).
2. Entendiéndose "Aplicación" no el puerto (TCP/UDP) sino la identificación como tal mediante firmas, como base para todas sus decisiones de políticas de habilitación segura como permitir, denegar, programar, inspeccionar y aplicar control de tráfico.
3. La solución debe clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con estas categorías / subcategorías (control granular dentro de la aplicación)
4. Aplicar técnicas de identificación de aplicaciones a todos los puertos TCP / UDP y no sólo en los más comunes.
5. Utilizar la identificación de la aplicación como base para las decisiones a la hora de establecer políticas de uso, permitiendo un control granular sobre el tráfico de la red.
6. Capacidad para identificar las aplicaciones bajo túneles HTTPS.

Identificación de usuarios:

1. Identificar usuarios integrándose con Microsoft Active Directory
2. Posibilidad de identificar tráfico a través de tags para aplicar políticas de restricción de accesos (SGT)
3. Funcionalidad de consolidación de logs y diferentes niveles de agrupación (origen, destino, aplicación, amenaza, websites y aplicaciones cloud) para su visualización.

Filtrado de contenidos:

1. Monitorizar y controlar la navegación web sin penalizar el tiempo de respuesta ni la satisfacción del usuario.
2. Tomar decisiones en tiempo real como permitir / denegar una URL basándose en políticas y en una base de datos de URLs mundiales que permita establecer controles para un filtrado granular de las URLs.
3. Ha de permitir crear categorías personalizables como listas blancas/negras.
4. Además, la plataforma tiene que tener la capacidad de hacer filtrado basado en las peticiones DNS y las categorías URL, así como poder hacer un sinkhole engañando así a la amenaza.

Características:

1. La solución ofertada debe incluir en la cotización el licenciamiento necesario para tener activas las siguientes características: Antimalware, IPS, Control de aplicaciones, Control de usuarios, Control de contenido, filtro de sitios web, Inspección de SSL, prevención de amenazas.
2. El Antimalware debe ser capaz de identificar archivos y hacer seguimiento al tránsito de los archivos a través de la red.
3. Debe poder identificar amenazas avanzadas, incluyendo varios métodos para la identificación de payload sospechoso, permitiendo que este tráfico pueda ser enviado a un dispositivo local o servicio en la nube para identificar archivos potencialmente maliciosos (Day Zero)
4. El acceso a la administración del equipamiento (plano de control) debe ser procesado independiente al manejo del tráfico, permitiendo una disponibilidad dedicada para situaciones de saturación.
5. La solución ofertada que debe soportar un mínimo de Throughput de 2,3 Gbps Dicho valor debe ser obtenido como el resultado de que el equipo posea activadas las características:
   a. IPS
   b. Antivirus
   c. Antimalware
   d. Threat protection/prevention
   e. URL Filtering

f. Identificación de contenido y usuarios

g. Identificación de aplicaciones

h. SSL decryption

i. Geolocation (con actualizaciones periódicas)

6. El equipamiento debe soportar mínimamente:

a. Sesiones concurrentes: 1 Millón

b. Cantidad de nuevas sesiones por segundo: 12.000

Reportes:

1. La nueva plataforma de seguridad Firewall debe incluir un sistema de dashboard centralizado que, mediante informes fácilmente personalizables, permita a los usuarios filtrar y revisar, analizar y visualizar rápidamente las amenazas de red, ineficiencias y su uso.

2. Debe tratarse de una plataforma gráfica que entre otras características disponga de:

a. Gráficos predefinidos y personalizables.

b. Identificación de patrones de ataque y cumplimiento de políticas.

c. Funciones de gestión de seguridad avanzadas:

i. Correlación de eventos.

ii. Evaluaciones de vulnerabilidad.

iii. Análisis de tráfico.

Administración:

1. La solución debe contemplar una herramienta de administración del tipo GUI desde la cual se pueda administrar el firewall de nueva generación.

2. Esta solución puede ser del tipo appliance o Virtual.

3. Manejo del dispositivo vía API

4. El equipo deberá tener la capacidad de enviar eventos a una consola de análisis e investigación indicadores de compromiso tipo hash, direcciones ip, dominios, etc. Brindar información acerca de esos loc y además relacionarlos con eventos generados en el equipo.

5. La propuesta debe cubrir los costos de licenciamiento y arquitectura para los reportes solicitados, con la disponibilidad de la información online, como mínimo por 3 años y sin costo adicional.

6. La solución propuesta debe poseer la capacidad de reenviar los logs de todo el equipamiento y conexión a un equipo remoto de tipo Syslog o SIEM y debe soportar diferentes formatos de log estándar en el mercado.

Licencias de cliente VPN

1. Se requerirán los clientes VPN necesarios para establecer 200 conexiones de usuarios finales durante la ETAPA 1 – Fase 1 (Red Corporativa).

9.4.3 Licencias de Malware Protection

A continuación, se detallan las especificaciones para adquirir, instalar y poner en marcha licencias de Malware Protection para contar con protección en Servers (Windows y Linux) y también en endpoints (Desktops, laptops, etc). Para eso requiere de una solución que se extienda más allá de las capacidades de prevención y que aborde el ciclo de vida completo del malware avanzado, antes, durante y después de un ataque.

- **Prevención:** la solución debe utilizar inteligencia de amenazas global para fortalecer las defensas y bloquear el malware conocido con antivirus, así como análisis de archivos estáticos y dinámicos para detectar malware emergente.
- **Detección:** la solución deberá supervisar continuamente la actividad de los archivos y del sistema en busca de amenazas emergentes. Cuando se detecta algo nuevo, esta solución proporcionara una alerta retrospectiva con el historial completo registrado del archivo de regreso al punto de entrada.
- **Respuesta**: La solución proporcionará información contextual necesaria durante una posible investigación de incumplimiento para priorizar la remediación y crear planes de respuesta.

La solución debe ofrecer una visibilidad, un contexto y un control profundos para detectar, contener y remediar rápidamente las amenazas avanzadas si evaden las defensas de primera línea.

Para la implementación, se deberán configurar las políticas específicas para los servers, pudiendo dividirse en primer lugar entre Servers Linux y Servers Windows y luego se deberán configurar políticas particulares según se crea necesario por funcionalidad de los equipos.

En cuanto a las políticas para los clientes finales (Desktops, Notebooks, etc) se deberán definir reglas generales que se puedan aplicar a toda la microinformática de la Empresa Argentina de Navegación Aérea, aunque se deberán tener en cuenta casos particulares que requieran alguna configuración especial.

Características que debe cumplir el software:

1. Debe poder administrar por lo menos 10.000 agentes de protección para endpoints desde un único sistema de administración.
2. Debe ser capaz de usar, crear y editar IoC's (indicative of compromise) para actividades de respuesta a incidentes.
3. Debe soportar OpenIOC.
4. Debe automáticamente correlacionar eventos de seguridad, actividades sospechosas y condiciones de tráfico para crear y administrar indicativos de comprometimiento en tiempo-real.
5. Debe permitir automáticamente poner en cuarentena amenazas en tiempo-real sin la necesidad de estar integrados con sistemas de monitoreo de redes sean estos del mismo fabricante o terceros.
6. Permitir de forma automática la detección y envió de archivos para análisis dinámico (sandbox) o estático con prevalencia baja en el ambiente monitoreado.
7. No depender de un proceso de escaneo o calendarización para identificar software vulnerable.
8. No debe depender de una política de análisis de vulnerabilidades para identificación.
9. Debe permitir informar la fecha, hora y listar cuales dispositivos tienen el software vulnerable.
10. Informar el CVE (Common Vulnerabilties and Exposures) asociado al software vulnerable detectado.
11. Debe permitir la protección de activos cuando no estén en la red interna.
12. Debe permite crear automáticamente y mantener un historial o flujo de trabajo forense para:
    a. Identificar Causa raíz del malware, por sí mismo aun cuando no sea detectado como malware la causa original.
    b. Identificar y seguir en tiempo-real actividades de creación, movimiento, ejecución de archivos y procesos, aun cuando no sean detectados o conocidos como malware.

c. Permitir las condiciones anteriores de forma automática y simultánea en todos los activos monitoreados en el ambiente.

d. Permite identificar cambios en la clasificación de seguridad de archivos, aplicaciones y procesos de forma automática y sin necesidad de una acción del administrador como escaneo o ejecución.

13. Debe hacer uso de recursos de inteligencia global en tiempo-real sin necesidad de calendarizar e identificar cambios en la postura de amenazas en el ambiente monitoreado.

14. Integrarse con soluciones de monitoreo y prevención de amenazas avanzadas de red nativamente.

15. Tener una API programable, documentada para personalizar e integrar acciones de prevención, respuesta y reporteo.

16. Permitir cuarentena y alerta de amenazas no detectadas durante análisis inicial sea esta por escaneo o en tiempo-real.

17. Usa diversos mecanismos de análisis, determinación y control de amenazas avanzadas en software único en el endpoint que incluye sin costo adicional recursos antivirus tradicionales.

18. Usa mecanismos de detección y prevención de exploración de vulnerabilidades en aplicaciones y/o procesos en el endpoint.

19. Permite la detección y prevención de amenazas de forma automática al obtener y evaluar en tiempo real metadatos de la estructura de archivos.

20. Usa mecanismo de detección basado en machine learning.

21. usa mecanismo de detección basado en reputación global en tiempo real

22. usa mecanismo de detección anti-virus

23. usa mecanismos de detección que implementa lógica fuzzy.

24. usa mecanismo de detección de heurística

25. usa mecanismo de detección comportamientos para identificar ataques ransomware

26. usa mecanismo para identificar rootkits

27. debe incluir sin costo adicional la posibilidad de activar de forma centralizada en la solución (a criterio del administrador) el recurso nativo de anti-virus tradicional que incluye un mecanismo (motor) de detección y escaneo presente localmente en el endpoint.

28. permite de forma nativa y opcional la integración con la tecnología de análisis cognitiva en larga escala para automatizar la identificación de amenazas e incidentes en el ambiente con la ayuda de soluciones proxy del mismo fabricante o de terceros.
29. permite operar en ambientes que usan direcciones IP vía DHCP.
30. permite rescatar archivos (en cuarentena) de sistemas remotos vía interface gráfica.
31. tiene una interface para hacer búsquedas de eventos en todo el ambiente monitoreado por condiciones como nombre, extensión, dirección IP , dominios, acciones, resultados sandbox, vulnerabilidades e historial de uso.
32. identifica mutexes, strings, acceso a archivos, cambios del registro, archivos creados, comportamientos que indican maliciosidad.
33. Permite remediación y contención como:
    a. control de aplicaciones
    b. cuarentena de archivos
    c. Terminar procesos
    d. Bloqueo de trafico de red
    e. Crear detección personalizada automáticamente.
    f. Crear detección personalizada en distintos formatos soportados.
    g. Identificar amenazas personalizadas por uso de hash sha-256, MD5, datos y anomalías de sección de archivos.
34. Permite uso de operaciones lógicas para datos de detección customizada.
35. permite identificar, hacer el bloqueo y contención de amenazas en condición de día-cero o personalizadas.
36. Soportar:
    a. Microsoft Windows 7, Microsoft Windows 8, 8.1, windows 10
    b. Microsoft Windows Server 2008 R2
    c. Microsoft Windows Server 2012
    d. Mac OS X 10.11, 10.12, 10.13
    e. CentOS 6.8/6.9/7.3/7.4

f. redHat Enterprise Linux 6.5/6.6/6.7/6.8/7.2/7.3

g. Android 2.1 hasta 6.0 en plataforma ARM y Intel Atom

h. Soporte y solución para plataforma Apple IOS.

37. Ejecución en modo auditoria o modo bloqueo.

38. implementa comunicación para administración por protocolos de seguridad.

39. permite su uso en ambientes con proxy.

40. Permite modelo de uso SaaS (software-as-a-Service).

41. permite modelo de implementación local en ambiente del cliente (on-premise).

42. Permite whitelists, blacklists para archivos, direcciones IP, CIDR.

43. Permite definir exclusiones de forma personalizada por política, por grupo de activos protegidos y tipo de plataforma monitoreada.

44. Permite operación en paralelo con antivirus de terceros en el endpoint

45. Permite protección en tiempo-real por reputación global de amenazas.

46. Permite correlación generadas por recursos de análisis dinámico tipo sandbox de forma integrada y nativa (locales o en nube) con mecanismos globales de reputación y determinación automatizada.

47. Debe nativamente implementar de forma automática y constante una re-evaluación de postura de detección y debido a cambios de inteligencia de amenazas en escala global, de esta forma se promueve una postura proactiva en la respuesta a amenazas avanzadas y sus variantes, condiciones día-cero y actividades de respuesta a incidentes.

48. Permite definir password de protección para el agente en el endpoint.

49. Permite automatizar la generación de reportes y notificaciones a los administradores.

50. Permite crear exclusiones de detección para: archivos/rutas (path), extensión de archivos, procesos (incluyendo rutas/path, hash y procesos hijos), wildcards y especificando amenazas (nombres).

51. Permite la correlación y consolidación automática de elementos conocidos como causa raíz de infecciones y propagación de malware en tiempo real.

52. Debe permitir realizar el análisis de causa-raíz de forma automática para todo el ambiente monitoreado de la siguiente forma:

a. Debe permitir establecer un intervalo de tiempo deseado para evaluación
b. Debe Informar la cantidad de sistemas afectados
c. Debe informa la cantidad de amenazas detectadas por cada una de las causas raíz identificadas
d. Debe informar el tipo de actividad identificada
e. Debe informar el tipo de amenaza identificada

53. Soporta la visualización gráfica de un contexto en tiempo-real e historial de uso y detecciones en endpoints monitoreados, creando un soporte preciso para respuesta a incidentes y actividades de evaluación forense de incidentes de seguridad.

54. Permite determinar la realización de análisis dinámico para archivos o artefactos observados en las estaciones monitoreadas en el contexto de la solución, de forma que permite establecer nuevas capacidades de detección, prevención y contención de amenazas en desarrollo en el ambiente.

55. Permite de forma automática la captura y el registro de acciones en la línea de comandos durante el desarrollo de ataques y acciones sospechosas.

56. Permite definir un repositorio de archivos obtenidos a partir de los endpoints monitoreados para análisis dinámica sandbox.

57. Debe permitir integración nativa con sistema de análisis machine learning y cognitiva que implemente la correlación de accesos y eventos de sistemas web proxy

58. Permitir la creación de snapshots para análisis forense post-mortem

59. Permitir la identificación de Indicadores de Compromiso (IOC) en su ambiente alineados a Mitre Attack

60. Permitir la creación de acciones automatizadas en las políticas de respuesta a incidentes

61. Soporte para integrarse con soluciones de terceros como (SIEM, IR management, SOAR, etc)

62. Permitir la actualización de los agentes instalados y bases de datos de antivirus en dispositivos de usuario final (desktop, laptop) ya sea a través de comunicación con una consola central (on-premise) dentro de la Red LAN asi como mediante una conexión a internet cuando el dispositivo no se encuentre dentro de la LAN

9.4.4 DNS SECURITY

A continuación, se detallan las especificaciones para adquirir la solución de DNS SECURITY, que permite controlar las conexiones hacia internet. De esta manera se logran mitigar los ataques de Phishing/malware vía Web y Ransomware.

A través de esta solución se verifican todos los sitios web a los que se conectan los usuarios de EANA, analizando si dichos sitios están catalogados como riesgosos, bloqueando el acceso. Así se evita que los usuarios sean víctimas de robo de identidad, robo de cuentas bancarias, descarga de software malicioso, etc.

La propuesta debe contemplar seguridad a nivel de red para toda EANA, como para usuarios móviles.

Las soluciones de DNS Security y Malware Protection deberán poder reportar a una única consola desde donde se puedan visualizar todos los eventos de seguridad de la red y además poder tomar acciones en caso de verificar algún equipo comprometido.

Características que debe cumplir:

1. La solución debe poder ser desplegada a todos los usuarios en minutos, con un filtrado hecho en la nube, sin Hardware para instalar o Software para actualizar
2. La solución debe poder contener amenazas sobre cualquier puerto y protocolo, usando DNS como base de inteligencia
3. La solución no deberá introducir latencia sobre el tráfico de los usuarios, permitiendo el bloqueo de peticiones hacia destinos maliciosos incluso antes de que se establezcan las conexiones
4. La solución deberá estar distribuida globalmente, comunicándose con IXP en todos los continentes, acortando así la ruta entre dos puntos. Debido a esto, la solución ofertada debe ser capaz de reducir la latencia en las conexiones para los usuarios
5. La infraestructura no deberá depender de apuntar a diferentes DNS en función de la localización geográfica. Todos deberán funcionar con las mismas direcciones.
6. La solución deberá poder contar con una infraestructura que haya mantenido la disponibilidad al 100%
7. Contar con un despliegue global dentro de la infraestructura de Internet que identifique conexiones maliciosas, deteniendo amenazas y ataques de manera automática, además de contener llamadas de Comando y Control realizadas por máquinas ya infectadas previniendo la exfiltración de datos.

8. La solución deberá contar con una categoría especial para identificar nuevos dominios solicitados a la infraestructura, ayudando a exponer dominios que son parte de amenazas emergentes (especialmente DGA o campañas de phishing)
9. La solución deberá contar con mecanismos de bloqueos configurables separados para reputaciones de dominios, tanto basados en categorías tradicionales como en bloqueos específicos para dominios de Malware, Comando y Control, Phishing y otros relacionados con amenazas.
10. Se deberá contar con un mecanismo de identificación de IP dinámicas para automatizar el descubrimiento y registro de nuevas IP que provea el ISP
11. La solución deberá contar con la posibilidad de desplegar un cliente ligero para aplicar políticas independientes de la red en la que se encuentre conectado el usuario, dentro o fuera de la red corporativa.
12. El agente deberá soportar por lo menos Windows Mac OS y Linux
13. El agente deberá convivir con la solución de VPN actual, permitiendo tener un solo cliente
14. El agente deberá permitir a la solución identificar conexiones IP sospechosas, enviarlas a la nube para análisis y bloquear conexiones maliciosas
15. Se deberá poder instalar un servidor local que permita la integración con la red local e identificar los equipos que originan tráfico malicioso.
16. El servidor local deberá poder instalarse usando 512 MB de RAM, 1 Core de CPU y 7 GB de espacio en disco
17. El servidor local deberá ser replicable de manera virtual para mayor escalabilidad y redundancia. No se aceptarán soluciones basadas en appliance.
18. El servidor local deberá soportar por lo menos VMWare ESXi y Hyper-V
19. El servidor local deberá poder integrarse con un servicio de Directorio Activo para identificar los usuarios que realizan las consultas DNS
20. La solución deberá poder cifrar y autenticar la información de DNS para mejorar la postura de seguridad
21. La solución debe poder permitir definir listas blancas y negras, además de permitir analizar URLs completos

22. La solución deberá poder interceptar automáticamente consultas de dominios sospechosos para que sean analizadas a nivel de URL y de archivos. Los archivos deberán ser analizados usando motores antivirus y de protección de malware avanzado
23. La solución deberá tener la capacidad de descifrar tráfico HTTPS enviado través del Proxy
24. La solución deberá poder identificar ataques dirigidos a EANA, comparando la información de la actividad global de un dominio con la actividad local del dominio en EANA
25. La solución debe contar con una plataforma tipo API para poder enviar eventos desde otras plataformas hacia la solución para aplicación de políticas de seguridad
26. La solución debe poder enviar información a un SIEM o Log Management
27. La solución debe detectar y reportar anomalías de tipo Fast Flux asociadas a un dominio
28. La solución deberá poder relacionar prefijos de IP con ASN, confirmando que un dominio está siendo hosteado en infraestructuras con otros dominios maliciosos. Esta misma solución deberá poder dar más información de las IP o los ASN asociados con el dominio
29. La solución deberá proveer la historia de cuándo fue etiquetado un dominio con una asociación de Malware
30. La solución deberá contar con una consola de investigación que provea toda la información que pueda de un dominio para realizar investigación de inteligencia contra amenazas, incluyendo IPs, redes y hashes de archivos
31. La solución debe identificar dominios relacionados y co-ocurrencias que identifiquen otros dominios que, con alta frecuencia estadística, sean consultados antes o después del dominio analizado
32. La solución deberá poder contar con un API específico de consulta de información a la herramienta de investigación para identificar todo lo conocido con respecto a un dominio
33. La solución debe permitir la generación de reportes recurrentes, enviados vía email, con formatos HTML y CSV
34. La solución debe poder permitir búsquedas de eventos de seguridad específicos por grupos o identidades para facilitar la identificación de problemas
35. La solución debe contar con reportería capaz de identificar y filtrar resultados de cada solicitud de dominios, URL e IP realizadas a la plataforma y refinar las búsquedas con filtros para identificar lo necesario

36. Se deberá contar con un mecanismo de identificación de uso de dominios relacionados con servicios de nube y poder incluso descubrir servicios catalogados como Shadow IT
37. La solución debe contar con un reporte particular de auditoría para cambios en la plataforma misma y guardar dicha información hasta 1 año

9.4.5 LICENCIAS SOLUCIÓN PARA MULTI-FACTOR AUTHENTICATION (MFA)

A continuación, se detallan las especificaciones para la adquisición, instalación, y puesta en marcha de una solución de Múltiple factor de autenticación.

Esta solución deberá integrarse con el acceso remoto VPN y se utilizara con aquellos usuarios que tengan acceso a información importante del Organismo y que por tal motivo requieren una validación más rigurosa.

La solución deberá contemplar estas características:

Autenticación y registración

1. La solución deberá permitir que los usuarios puedan enrolar múltiples dispositivos
2. La solución deberá permitir al usuario el dispositivo de autenticación
3. La solución deberá permitir que el usuario pueda administrar los dispositivos con los que se autenticará. A su vez, mediante la aplicación en sí deberá tener la capacidad de asignar este atributo a nivel usuario/grupo
4. La solución deberá implementar el método de autenticación del tipo push
5. El método push utilizado deberá utilizar llaves asimétricas
6. La solución deberá ser capaz de autenticar SMS, a su vez, la plataforma deberá poder enviar en un solo SMS múltiples OTPs
7. Los usuarios deberán poder autenticarse utilizando un hardware token
8. La solución deberá soportar hardware tokens del tipo OATTH compliant
9. La solución deberá poder generar un one-time passcode desde una aplicación mobile
10. La solución deberá contar con un mecanismo de bypasscode para autenticar.
11. El aprovisionamiento del a aplicación mobile para autenticación deberá poder realizarse a través del escaneado de un código QR

Administración

1. La solución deberá requerir doble factor de autenticación para los logins de los administradores o para usuarios determinados que así lo requieran.

2. La solución deberá tener la capacidad de controlar que usuarios/grupos accederán a ciertos tipos de factor de autenticación (ejemplo: push, llamada telefónica, SMS, etc)
3. La solución deberá proveer alguna herramienta de aprovisionamiento que permita realizar una sincronización de usuarios de AD
4. La solución podrá agregar usuarios vía mecanismos masivos para la importación (por ejemplo, archivos CSV)
5. La solución deberá permitir que los usuarios realicen la auto registración en la plataforma.
6. La solución deberá permitir que los usuarios se enrolen a través de un link enviado por la plataforma
7. La solución deberá ser capaz de organizar los usuarios en grupos.

Zero Trust

1. La solución deberá poder identificar dispositivos no manejados por la organización y bloquear el acceso
2. La solución deberá identificar que dispositivos están tratando de acceder a las aplicaciones protegidas
3. La solución deberá generar reportes acerca de los dispositivos administrados y no administrados para sistemas Windows, Mac, iOS, Android.
4. La solución deberá tener la capacidad de implementar políticas de acceso a aplicaciones (on- premise o cloud) dependiendo el tipo de dispositivo que el usuario use para autenticar.
5. La solución deberá comunicar al usuario, al momento de la autenticación, si los mismos no están habilitados a acceder a una aplicación utilizando un dispositivo no controlado por la organización
6. La solución deberá poder integrarse con diferentes MDM para poder identificar dispositivos confiables.

Licenciamiento

1. La solución deberá poder licenciarse por usuario y no por cantidad de aplicaciones a proteger.

9.5Cantidades totales de hardware y software

Tal como se mencionó anteriormente, los oferentes deberán considerar que el hardware se adquirirá durante las dos etapas mencionadas en el punto 6, las mismas conforman todos los nodos de la red ATN y corporativa. Los tipos de sitios que hay son:

Sitios críticos: sitios de ACC/cabeceras de FIR, más Aeroparque. *Total 6.*

> Aeroparque, Ezeiza, Córdoba, Comodoro Rivadavia, Resistencia y Mendoza conectados en la red SD WAN, más el sitio existente Bouchard y DC de contingencia en ARSAT (Benavidez).

Sitios de EAVAS. *Total 31.*

> Bahía Blanca, Laboulaye, Río Mayo, Choele Choel, Malargüe, Rosario, Piedra del Águila, Mar del Plata, San Juan, Chacharramendi, Neuquén, San Julián, Concordia, Pehuajó, Santa Rosa, El Calafate, Puerto Madryn, Sauce Viejo, Esquel, Reconquista, Tandil, Gualeguaychú, Río Cuarto, Tucumán, Ingeniero Jacobacci, Río Gallegos, Viedma, Junín, Río Grande, Villa Reynolds y Rincón de los Sauces.

Sitios RADAR. *Total 11.*

> Bariloche, Corrientes, La Rioja, Paraná, Posadas, Salta, San Luis, Ushuaia, Morteros, Quilmes, Roque Saenz Peña.

Sitios aeropuertos. *Total 20.*

> Base Marambio, La Plata, Campo de Mayo, Moreno, Catamarca, Morón, Chapelco, Paso de los Libres, El Palomar, San Fernando, FBO (Ezeiza), San Rafael, Formosa, Santa Rosa de Conlara, Goya, Santiago del Estero, Iguazú, Termas de Rio Hondo, Jujuy, Trelew.

Sitios EAVAS coubicados en una TELCO. *Total 10.*

> Ancasti, Andagalá, Ceres, Frias, La Posta, Marcos Juarez, Monte Quemado, Susques, Tartagal, Las Lomitas.

La distribución del hardware y licencias a adquirir se definirá en la etapa de planificación del proyecto. A continuación, se detallan las cantidades de equipamientos y licencias.

9.5.1 SD-WAN

Se deberá ofertar como mínimo las cantidades de equipos descritas debajo. Las licencias requeridas tanto para equipos nuevos como propios deberán incluir lo siguiente:

- Soporte de mantenimiento de los equipos (8x5xNBD)
- Licencia de sistema de gestión centralizado DNA y soporte de estas
- Licencias perpetuas de SDWAN y soporte de estas

EANA | NAVEGACIÓN AÉREA ARGENTINA

Ministerio de Transporte
Presidencia de la Nación

Etapa	*Descripción licencia o equipo*	*Fase*	*Cantidad*
Etapa 1	Nuevos Routers a proveer C8300 Licencia SD WAN de tráfico agregado, mínimo requerido: 200M (100 M bidireccional), por 3 años según las características definidas para el router en ítem anterior para la fase 1	Fase 1	1
		Fase 2 a 4	No requerido
	Nuevos Routers a proveer C1111 Licencia SD WAN de tráfico agregado, mínimo requerido: 20M (10 M bidireccional), por 3 años según las características definidas para el router en ítem anterior para la correspondiente fase.	Fase 1 a 3	No requerido
		Fase 4	3
	Licencias SD WAN para routers existentes Cisco ISR4431 Licencia SD WAN de tráfico agregado, mínimo requerido: 200M (100 M bidireccional), por 3 años según las características definidas para el router en ítem anterior para la fase 1.	Fase 1	4
		Fase 2 a 4	No requerido
	Licencias SD WAN para routers existentes Cisco ISR4321 Licencia SD WAN de tráfico agregado, mínimo requerido: 20M (10 M bidireccional), por 3 años según las características definidas para el router en ítem anterior para la correspondiente fase.	Fase 1	No requerido
		Fase 2	11
		Fase 3	8
		Fase 4	17
	Licencias SD WAN para routers existentes Cisco ISR4221 Licencia SD WAN de tráfico agregado, mínimo requerido: 20M (10 M bidireccional), por 3 años según las características definidas para el router en ítem anterior para la correspondiente fase.	Fase 1	No requerido
		Fase 2	11
		Fase 3	No requerido
		Fase 4	No requerido
Etapa 2	Nuevos Routers a proveer C8300 Licencia SD WAN de tráfico agregado, mínimo requerido: 200M (100 M bidireccional), por 3 años según las características definidas para el router en ítem anterior para la fase 1	Fase 5 a 8	No requerido
		Fase 9	1
	Nuevos Routers a proveer C1111 Licencia SD WAN de tráfico agregado, mínimo requerido: 20M (10 M bidireccional), por 3 años según las características definidas para el router en ítem anterior para la correspondiente fase.	Fase 5	10
		Fase 6	No requerido
		Fase 7	3
		Fase 8	3
		Fase 9	No requerido

	Licencias SD WAN para routers existentes Cisco ISR4431 Licencia SD WAN de tráfico agregado, mínimo requerido: 200M (100 M bidireccional), por 3 años según las características definidas para el router en ítem anterior para la fase 1.	Fase 5 a 8	No requerido
		Fase 9	4
	Licencias SD WAN para routers existentes Cisco ISR4321 Licencia SD WAN de tráfico agregado, mínimo requerido: 20M (10 M bidireccional), por 3 años según las características definidas para el router en ítem anterior para la correspondiente fase.	Fase 5	No requerido
		Fase 6	3
		Fase 7	4
		Fase 8	5
		Fase 9	No requerido
	Licencias SD WAN para routers existentes Cisco ISR4221 Licencia SD WAN de tráfico agregado, mínimo requerido: 20M (10 M bidireccional), por 3 años según las características definidas para el router en ítem anterior para la correspondiente fase.	Fase 5	No requerido
		Fase 6	No requerido
		Fase 7	No requerido
		Fase 8	13
		Fase 9	No requerido

9.5.2 SD-ACCESS

Se deberá ofertar como mínimo las siguientes cantidades de equipos, incluyendo el licenciamiento necesario para soportar las funcionalidades requeridas:

Etapa	*Descripción licencia o equipo*	*Fase*	*Cantidad*
Etapa 1	Switch de acceso de 48 puertos con POE+, 4 uplinks de 1/10G con soporte de SFP/SFP+ Licencias necesarias de software de gestión	Fase 1	8
		Fase 2 a 4	No requerido
	Switch de acceso de 48 puertos con POE+, 8 uplinks de 1/10G con soporte de SFP/SFP+ Licencias necesarias de software de gestión	Fase 1 a 4	No requerido
	Switch de acceso de 24 puertos con POE, 4 uplinks de 1/10G con soporte de SFP/SFP+ Licencias necesarias de software de gestión	Fase 1	7
		Fase 2	22
		Fase 3	8
		Fase 4	17
	Extensores de 12 puertos con POE+. Dos uplinks 1G SFP	Fase 1	10

	Licencias necesarias de software de gestión	Fase 2	15
		Fase 3	1
		Fase 4	2
	Cables stack para switches 50 cm, para los swithes de 24 y 48 puertos requeridos	Fase 1	15
		Fase 2	22
		Fase 3	8
		Fase 4	17
	1000BASE-T SFP transceiver module for Category 5 copper wire	Fase 1	12
		Fase 2	44
		Fase 3	16
		Fase 4	34
	1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM	Fase 1	26
		Fase 2	30
		Fase 3	2
		Fase 4	4
Etapa 2	Switch de acceso de 48 puertos con POE+, 4 uplinks de 1/10G con soporte de SFP/SFP+ Licencias necesarias de software de gestión	Fase 5 a 9	No requerido
	Switch de acceso de 48 puertos con POE+, 8 uplinks de 1/10G con soporte de SFP/SFP+ Licencias necesarias de software de gestión	Fase 5 a 8	No querido
		Fase 9	11
	Switch de acceso de 24 puertos con POE, 4 uplinks de 1/10G con soporte de SFP/SFP+ Licencias necesarias de software de gestión	Fase 5	No requerido
		Fase 6	20
		Fase 7	8
		Fase 8	24
		Fase 9	20
	Extensores de 12 puertos con POE+. Dos uplinks 1G SFP Licencias necesarias de software de gestión	Fase 5	No requerido
		Fase 6	2
		Fase 7	10
		Fase 8	15
		Fase 9	28
	Cables stack para switches 50 cm, para los swithes de 24 y 48 puertos requeridos	Fase 5	No requerido
		Fase 6	20

		Fase 7	8
		Fase 8	24
		Fase 9	31
	1000BASE-T SFP transceiver module for Category 5 copper wire	Fase 5	No requerido
		Fase 6	40
		Fase 7	16
		Fase 8	48
		Fase 9	24
	1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM	Fase 5	No requerido
		Fase 6	4
		Fase 7	20
		Fase 8	30
		Fase 9	78

9.5.3 WIFI

Etapa	*Descripción licencia o equipo*	*Fase*	*Cantidad*
Etapa 1	Access Point	Fase 1	49
		Fase 2	36
		Fase 3	13
		Fase 4	19
Etapa 2	Access Point	Fase 5 a 9	No requerido

9.5.4 Seguridad

Etapa	*Descripción licencia*	*Fase*	*Cantidad*
Etapa 1	NAC-SEGURIDAD	Fase 1	500
		Fase 2	300
		Fase 3	150
		Fase 4	250
	Licencias Cisco ISE VM	Fase 1	2 Medium 3 Small
		Fase 2 a 4	No requerido
	Firewall de nueva generación	Fase 1	1
		Fase 2 a 4	No requerido

	Licencias VPN	Fase 1	200
		Fase 2 a 4	No requerido
	Licencias de malware protection	Fase 1	1500
		Fase 2 a 4	No requerido
	DNS Security	Fase 1	250
		Fase 2 a 4	No requerido. Se consumen las licencias embebidas en los routers detallados en la sección 10.1.9
	Solución para multi-factor authentication (MFA)	Fase 1	50
		Fase 2 a 4	No requerido
Etapa 2	NAC-SEGURIDAD	Fase 5	20
		Fase 6	200
		Fase 7	200
		Fase 8	300
		Fase 9	800
	Licencias Cisco ISE VM	Fase 5	2 Medium 6 Small
		Fase 6 a 9	No requerido
	Firewall de nueva generación	Fase 5 a 9	No requerido
	Licencias VPN	Fase 5 a 9	No requerido
	Licencias de malware protection	Fase 5 a 9	No requerido
	DNS Security	Fase 5 a 9	No requerido
	Solución para multi-factor authentication (MFA)	Fase 5 a 9	No requerido

10. SERVICIOS PROFESIONALES

Los servicios profesionales necesarios para la instalación, configuración y puesta en marcha deberán llevarse a cabo en conjunto con el personal de EANA, teniendo en cuenta lo siguiente:

- Aplicación de mejores prácticas en las etapas de diseño, implementación y configuración

- Pruebas de conectividad de los sitios
- Pruebas de failover de la solución
- Asistencia on-site al día después de cada ventana

Para cumplimentar esta premisa los servicios profesionales serán divididos en las siguientes etapas:

- Etapa de Relevamiento
- Etapa de Diseño
- Etapa de Rack & Stage
- Etapa de Configuración
- Etapa de Migración
- Etapa de Aceptación

10.1 Requerimientos generales para el proyecto

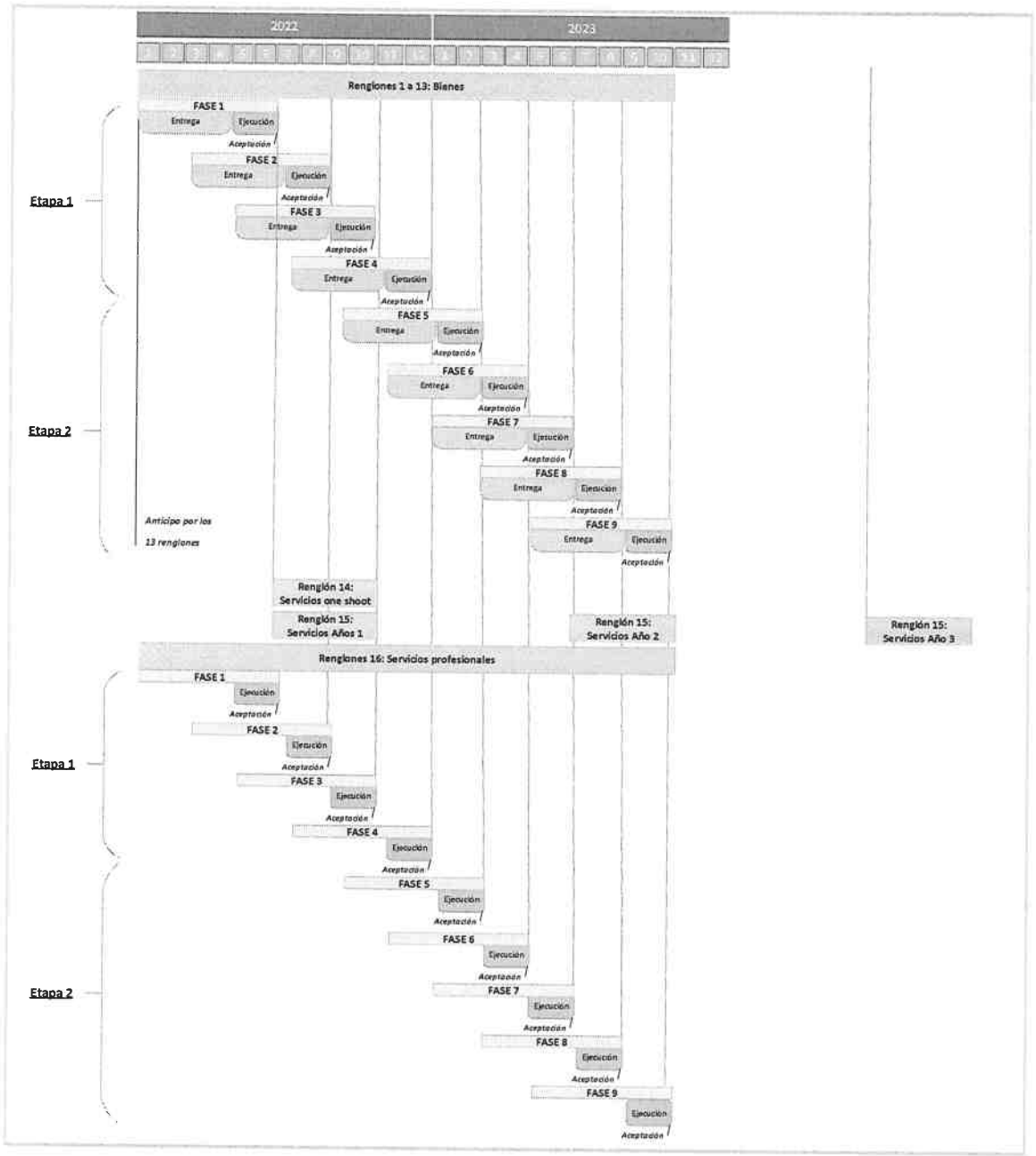
10.1.1 Cronograma de actividades

Los oferentes deberán presentar a EANA un cronograma de trabajo, teniendo en cuenta como base que el plazo de implementación por etapa no debe superar los 12 meses. El cronograma definitivo será aprobado por EANA en la reunión inicial con el adjudicatario.

El plan de proyecto debe ser acorde a la estrategia de Implantación que se detalla a modo orientativo en el siguiente gráfico:

EANA | NAVEGACIÓN AÉREA ARGENTINA

Ministerio de Transporte
Presidencia de la Nación



La entrega de los renglones 1 a 13, correspondiente a los bienes, deberá ser en 120 días, siendo a continuación la ejecución realizada en 60 días, así hasta finalizar las 9 fases.

Como se mencionó en el título 5, se deberá respetar el orden de ejecución de las fases de ambas etapas teniendo el oferente que presentar un plan de proyecto con el detalle de actividades y tareas, las etapas e hitos, presentando su calendario de ejecución y diagrama de tiempo.

10.1.2 Seguimiento del proyecto

Para el cumplimiento de este cronograma los oferentes designarán un Proyect Manager, como único líder de proyecto. EANA designara también un PM.

Ambos serán los responsables de:

- Revisar y documentar los objetivos del proyecto.
- Planificar las distintas etapas del proyecto y establecer un cronograma.
- Gestionar los RRHH asignados al proyecto para lograr el cronograma establecido.
- Supervisar las actividades del equipo de proyecto y llevar métricas de estas para poder identificar en forma temprana cualquier desvío.
- Establecer reuniones periódicas de revisión de avance y cumplimiento del cronograma.
- Definir e implementar un proceso de control de cambios.

Al inicio del proyecto, el Gerente de Proyecto de EANA se reunirá con el equipo de especialistas de la empresa proveedora para determinar todos los requisitos exigidos para la finalización satisfactoria de este proyecto.

El grupo tendrá como tareas:

- Confirmar los requisitos y expectativas de EANA.
- Priorizar requisitos.
- Identificar al personal que recibirá la transferencia de conocimientos.
- Discutir sobre los objetivos, escalafón de eventos y ciclos de revisión.
- Revisar los siguientes procedimientos, con el objetivo de esclarecer eventuales dudas:
- Revisión de la arquitectura y topología del área de TI involucrada en este proyecto,
- Sucesión de documentos,
- Control de cambios,
- Pruebas de Integración y Puesta en Producción de la Solución,
- Evaluación de la calidad.
- Producir una agenda de proyecto

10.2 Documentación

La documentación a entregar por el adjudicatario será mandatario para el avance del proyecto y marcará un hito del progreso de cada fase. Esta podrá ser en formato electrónico.

La documentación debe estar conformada por los documentos de: diseño de alto nivel (High Level Design – HLD), diseño de bajo nivel (Low Level Design - LLD), Plan de Implementación (Network Implementation Plan - NIP), procedimiento de rollback y contingencia y toda la documentación correspondiente a las etapas del proyecto (diseño, rack & stage, configuración, migración y aceptación).

10.3 Servicios avanzados de Cisco

Para el licenciamiento total de la solución se aceptará la opción de ofrecerlo en un formato de EA (enterprise agreetment).

Además, se requiere que el oferente incluya los Servicios Avanzados de Cisco para la implementación de todo el proyecto, contemplando el soporte en las etapas correspondientes a: desarrollo de requisitos de solución, solución de diseño, desarrollo del plan de pruebas, etc.

10.4 Capacitación

Dentro de los servicios profesionales, se deberá incluir la capacitación y transferencia de conocimiento de la totalidad de módulos y funcionalidades a implementar hacia los Ingenieros/Técnicos de EANA, al finalizar cada fase de las nueve correspondientes. Esto debe incluir la capacitación del proceso de contingencia y rollback hacia la red legacy de la etapa 2.

La capacitación será dictada de forma presencial y/o virtual a 10 ingenieros/técnicos de EANA. La misma podrá ocurrir en las oficinas de EANA o del adjudicatario según lo propuesto por este último, de lunes a viernes en el horario de 9 a 18 hs, con una carga horaria de 30 horas.

Se deberá proveer material en formato electrónico, de documentación del fabricante pertinente. El lugar de dictado será en dependencias de EANA, zona AMBA, a definir, al mismo tiempo que el proveedor generará una sesión de videoconferencia para personal remoto de EANA, durante el mismo.

Es requisito excluyente que toda la implementación, configuración y puesta en marcha sea realizada **en sitio con Ingenieros/Técnicos de EANA presentes** durante la totalidad de los trabajos.

11. RECEPCIÓN DEFINITIVA

A partir de la fecha de entrega de la solución de cada fase, EANA se reserva un plazo de 14 días destinado a efectuar pruebas del correcto funcionamiento de la totalidad de hardware y software productivos en los sitios en cuestión, incluyendo todas las funcionalidades descriptas en las especificaciones técnico funcionales requeridas en el presente documento.

Si en dicho plazo los bienes y/o servicios no alcanzaran los rendimientos, capacidades o cualidades exigidas, EANA intimará al Adjudicatario la entrega de los bienes o servicios faltantes hasta resolver la novedad, de cumplirse satisfactoriamente dichas verificaciones, EANA procederá a extender el Certificado de Recepción Definitiva de la fase correspondiente. El tiempo máximo admisible para que el adjudicatario resuelva el problema detectado estará regido por el TMRS descrito en el punto 13.1.

El adjudicatario deberá labrar el acta del ANEXO II – ACTA DE CONFORMIDAD DE LA PROVISIÓN DE SERVICIOS CONTRATADOS, que deberá ser firmada por ambas partes.

12. GARANTÍA DEL HARDWARE

El adjudicatario deberá garantizar que la provisión del hardware entregado e instalado cuente con tres (3) años de garantía, teniendo en cuenta la entrega realizada del equipamiento y la aceptación de la misma. El plazo de garantía comenzará a regir una vez realizada la recepción definitiva de cada fase sólo para los equipos provistos en dicha fase. Ver título 15 para detalle de las entregas parciales.

La reposición de partes por incidente deberá ser 8x5xNBD (día hábil posterior) con entrega en el Aeropuerto Internacional Ezeiza Ministro Pistarini, Km 33 1/2, Edificio Operativo EANA, Puerta 50, 4to Piso.

13. SOPORTE TÉCNICO

Se requiere soporte 7x24x365 a partir de la fecha de aceptación y puesta en marcha de la fase 1 de la etapa 1 y durante todo el periodo de implementación de la totalidad de las etapas y fases restantes.

El mismo deberá ser de manera remota o en sitio si el problema no puede ser resuelto de esa forma.

EANA-SE es la responsable de solicitar las órdenes de asistencia durante un problema en el servicio.

La notificación al Adjudicatario se realizará, como sigue:

> *Teléfono, helpdesk o correo electrónico enviado por personal del departamento de Comunicaciones de la gerencia de Ingeniería CNS.*

El Adjudicatario deberá proporcionar, número de teléfono, dirección de correo electrónico, o sistema de reportes de incidentes, donde las comunicaciones puedan efectuarse durante las 24 horas, los 365 días del año.

También, deberá especificar los contactos y la estructura de escalamiento de acuerdo al nivel de criticidad y tiempos de respuesta.

El Adjudicatario deberá proveer seguimiento de incidentes, a través del seguimiento de los tickets generados por el técnico de EANA-SE.

13.1 Acuerdos de niveles de servicio (SLA)

Las definiciones generales de la clasificación de la severidad de la falla serán las siguientes:

- Falla Crítica: una falla inherente al Sistema que resulta en la pérdida de las principales funciones del mismo. La función del Sistema está comprometida: El Sistema no puede cumplir su misión, pero puede ser restablecido, ya sea mediante la reconfiguración del Sistema o el uso de instalaciones de reserva.
- Falla mayor: causa la pérdida de funciones. La capacidad de los sistemas para llevar a cabo su misión está degradada y es perceptible para el usuario. Los usuarios pueden mantener la misión del sistema por otros medios, y el aumento de la carga de trabajo por el uso de estas alternativas está en un rango aceptable.
- Falla menor: una falla inherente al Sistema que no resulta en una pérdida de las funciones del Sistema. La capacidad del Sistema para cumplir su misión no se degrada.

El Tiempo Máximo de Restauración del Servicio (TMRS) será:

TIPO DE FALLA	TIEMPO DE RESPUESTA	TIEMPO DE REPARACIÓN	UNIDAD DE ATRASO EN EL TIEMPO DE REPARACIÓN
	Horas / Días	Horas / Días	Horas / Días
CRITICAS	15 MIN	2 hs +d	0.5hs
MAYORES	60 MIN	8 hs +d	2 hs
MENORES	60 MIN	48 hs +d	12 hs

La siguiente tabla establece los valores asignados a "d" en función de las distancias al centro de atención de los Oferentes más cercano al lugar donde se produjo el incidente (Km cero). Este valor solo aplicara si el incidente no pudo ser resuelto en forma remota y requiere la visita al sitio.

- 0 a 50 km= 1 hora
- 51 a 100 km=2 horas
- 101 a 200km= 4 horas
- más de 200km = 2 horas + el tiempo empleado en viaje por transporte público o propio más rápido.
- El valor "d" en caso alguno podrá superar las 8 horas.

14. PENALIDADES POR INCUMPLIMIENTO

Ante el incumplimiento de las obligaciones del Adjudicatario, se confeccionará un ACTA DE INCUMPLIMIENTO (**Anexo I – Modelo de Acta de Incumplimiento**) detallando las novedades encontradas y serán impuestas las PENALIDADES establecidas por la EANA-SE.

Si el Adjudicatario no cumpliese, parcial o totalmente, lo determinado en esta Especificación Técnica EANA-SE tendrá la facultad de imponer al mismo una multa, sin necesidad de interpelación judicial o extrajudicial alguna.

Las multas se calcularán sobre el monto de servicios profesionales de la siguiente forma:

- El porcentaje de multa se aplicará sobre el monto total de servicios procesionales de la fase en la que fue implementado el sitio dividido la cantidad de sitios de la fase
- Se aplicarán al siguiente hito de pago de cualquiera de las fases.

Las multas serán las siguientes:

1) Multa por TMRS: el monto de la multa a ser aplicada por incumplimiento de TMRS estipulado en el ítem 13.1, se calculará según el siguiente criterio:

Tiempo de restauración de Servicio	Monto de la multa por sitio
Criticas > 2 Hs	5% por cada hora
Mayores > 8 Hs	5% por cada hora

A los efectos del cómputo del Tiempo Máximo de Reparación y/o de Disponibilidad Técnica, se tomará como fecha y hora de puesta "Fuera de Servicio" o "Corte de Emisión", la de notificación de la novedad al Adjudicatario según los medios indicados en el ítem 13.

Se tomará como fecha y hora de puesta "En Servicio" cuando se compruebe con personal CNS que se ha reestablecido el servicio.

2) Multa cambio de partes se calculará según el siguiente criterio:

Tiempo de Recambio	Monto de la multa por sitio
> 8x5xNBD	5% por cada día

3) Multa por plazo de instalación: el monto de la multa a ser aplicada por incumplimiento de plazo de instalación estipulado en el ítem 11, se calculará según el siguiente criterio:

Tiempo de Instalación	Monto de la multa por sitio

> Plazo programado	5% por cada mes

15. PLAZO DE ENTREGA Y EJECUCIÓN

El plazo de ejecución del contrato será de 36 meses, debiéndose cumplir las entregas parciales de cada fase, corridos a partir de la fecha de emisión de la Orden de Compra.

La entrega del equipamiento de la fase 1, correspondiente a los bienes, deberá ser en 120 días de emitida la OC. Las fases 2 a 9 comenzarán con la aceptación final por parte de EANA de la fase predecesora. Ver título 10.1.1 con cronograma propuesto.

Las entregas estarán sujetas a las nueve fases del proyecto, a continuación, se describe el detalle de entregas parciales por fase.

		AÑO 1				*AÑO 2*					*Año 3*	
		Etapa 1				*Etapa 2*					*NA*	
#	*Ítem*	*Fase 1*	*Fase 2*	*Fase 3*	*Fase 4*	*Fase 5*	*Fase 6*	*Fase 7*	*Fase 8*	*Fase 9*	*NA*	*Total*
1	SFP 1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM	26	30	2	4	–	4	20	30	78	–	194
2	SFP 1000BASE-T SFP transceiver module for Category 5 copper wire	12	44	16	34	–	40	16	48	24	–	234
3	Router C1111-8P-DNA	–	–	–	3	10	–	3	3	–	–	19
4	Router C8300-1N1S-6T	1	–	–	–	–	–	–	–	1	–	2
5	Firewall FPR2110-NGFW-K9	1	–	–	–	–	–	–	–	–	–	1
6	Máquina Virtual R-ISE-VMM-K9=	2	–	–	–	2	–	–	–	–	–	4
7	Máquina VirtualR-ISE-VMS-K9=	3	–	–	–	6	–	–	–	–	–	9
8	Máquina Virtual SF-FMC-VMW-2-K9	1	–	–	–	–	–	–	–	–	–	1
9	Extensor LAN WS-C3560CX-12PC-S	10	15	1	2	–	2	10	15	28	–	83

10	Access Point C9105AXI-A	49	36	13	19	–	–	–	–	–	–	117
11	Switch C9300-48P-A	–	–	–	–	–	–	–	–	11	–	11
12	Switch C9300L-24P-4X-A	7	22	8	17	–	20	8	24	20	–	126
13	Switch C9300L-48P-4X-A	8	–	–	–	–	–	–	–	–	–	8
14	Servicios: Licencias de software por única vez	–	–	1	–	–	–	–	–	–	–	1
15	Servicios: Licencias de software por 3 años	–	–	1	–	–	–	–	1	–	1	3
16	Servicios: Servicios Profesionales	11,11%	11,11%	11,11%	11,11%	11,11%	11,11%	11,11%	11,11%	11,11%	–	1

Asimismo, dichas plazos parciales llevan asociados un hito de facturación que refleja los trabajos y entregables que el adjudicatario deberá entregar antes de la finalización de este.

16. HITOS DE PAGO

Los renglones 1 al 13 tendrán un anticipo del 10%, que podrá ser facturado posterior a la notificación de la Orden de compra y con el inicio del proyecto. Dicho anticipo será pagado contra póliza de caución presentada por el proveedor por el monto del anticipo correspondiente a los renglones de referencia. La entrega (90%) podrá ser facturada una vez realizada la recepción definitiva por fase. Ver título 10.1.1 con cronograma propuesto.

Los ítems de los renglones 14 y 15 correspondientes a las licencias de software podrán ser facturados de forma anual contraentrega, a mitad del primer año de ejecución del proyecto para el renglón 14 de única vez; y a mitad de cada año del contrato correspondiente para el renglón 15 de los servicios por 3 años. Ver título 10.1.1 con cronograma propuesto.

El renglón 16, podrá ser facturado con el cumplimiento y la aceptación de cada fase por parte de EANA S.E. Ver título 10.1.1 con cronograma propuesto.

17. LUGAR DE ENTREGA

Toda la mercadería deberá ser entregada en Aeropuerto Internacional Ministro Pistarini, Km 33 1/2, Edificio Operativo EANA-ANAC, Puerta 50, 4to Piso.

EANA | NAVEGACIÓN AÉREA ARGENTINA

Ministerio de Transporte
Presidencia de la Nación

18. ANEXO I – MODELO DE ACTA DE INCUMPLIMIENTO

A los ..... días del mes de ..... de 20..., en referencia a la factura xxx Nro. ..... emitida según Orden de Compra N° ....., (Licitación Pública /Privada – Contratación Directa) N° ....., por la Empresa ..... , CUIT N° ..... , con período mes de ..... de 20...., se procede a labrar la presente ACTA DE INCUMPLIMIENTO, según siguiente detalle:

- .....
  .....
  .....
  .....
  .....

Se labró la presente ACTA, en dos ejemplares, entregándose una copia para Cuentas a Pagar y otra a Gerencia de Compras, ambas pertenecientes a Gerencia Ejecutiva de Administración y Finanzas de EANA S.E CENTRAL.

Sin otro particular, saludo a usted atentamente.

.....
Contratista

.....
Contratante EANA S.E.

94

EANA | NAVEGACIÓN AÉREA ARGENTINA

Ministerio de Transporte
Presidencia de la Nación

19. ANEXO II – ACTA DE CONFORMIDAD DE LA PROVISIÓN DE SERVICIOS CONTRATADOS

Buenos Aires, ... de ..... de .....

Ref.: Conformidad de la provisión de servicios contratados

Se labra la presente acta entre ..... y la Empresa Argentina de Navegación Aérea S.E., para dejar constancia que el día de la fecha, conforme a la (Licitación Pública /Privada / Contratación Directa) Modo..... Nº .... Ejercicio Nº 20.... , Pliego de Condiciones Particulares (PCP), a la Especificación Técnica y a la Orden de Compra ....., el adjudicatario finalizó satisfactoriamente la provisión de los servicios, según el siguiente detalle:

- N° de etapa del proyecto
- N° de fase del proyecto

.....	.....
Representante EANA-SE	Representante adjudicatario
ACLARACIÓN:	ACLARACIÓN: .....
Sello y Cargo	Sello y cargo.....

20. ANEXO III – PLANILLA DE DATOS GARANTIZADOS

Renglón	*Descripción*	*Etapa*	*Fase*	*Cantidad*	*Título referenciado a ET*	*Cumple/No cumple*
1	1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM	1	1	26	9.5.2	
		1	2	30		
		1	3	2		
		1	4	4		
		2	6	4		
		2	7	20		
		2	8	30		
		2	9	78		
2	1000BASE-T SFP transceiver module for Category 5 copper wire	1	1	12	9.5.2	
		1	2	44		
		1	3	16		
		1	4	34		
		2	6	40		
		2	7	16		
		2	8	48		
		2	9	24		
3	C1111-8P-DNA	1	4	3	9.1.9	
		2	5	10		
		2	7	3		
		2	8	3		
4	C8300-1N1S-6T	1	1	1	9.1.9	
		2	9	1		
5	FPR2110-NGFW-K9	1	1	1	9.4.2	
6	R-ISE-VMM-K9=	1	1	2	9.4.1	
		2	5	2		
7	R-ISE-VMS-K9=	1	1	3	9.4.1	
		2	5	6		
8	SF-FMC-VMW-2-K9	1	1	1	9.4.2	
9	WS-C3560CX-12PC-S	1	1	10	9.2.3	
		1	2	15		
		1	3	1		
		1	4	2		
		2	6	2		

EANA | NAVEGACIÓN AÉREA ARGENTINA

Ministerio de Transporte
Presidencia de la Nación

		2	7	10		
		2	8	15		
		2	9	28		
10	C9105AXI-A	1	1	49	9.3	
		1	2	36		
		1	3	13		
		1	4	19		
11	C9300-48P-A	2	9	11	9.2.2	
12	C9300L-24P-4X-A	1	1	7	9.2.2	
		1	2	22		
		1	3	8		
		1	4	17		
		2	6	20		
		2	7	8		
		2	8	24		
		2	9	20		
13	C9300L-48P-4X-A	1	1	8	9.2.2	
14	Servicios: Licencias de software por única vez	Todas	Todas	Lo que corresponden	9.5	
15	Servicios: Licencias de software por 3 años	Todas	Todas	Lo que corresponden	9.5	
16	Servicios: Servicios Profesionales	Todas	Todas	Lo que corresponden	10	

ING. MALENA REINOSO
Gerenta de Ingeniería CNS
Empresa Argentina de Navegación Aérea
Sociedad de Estado