PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA MIGRACIÓN DE INFRAESTRUCTURA DE SERVIDORES AL CLOUD PARA EL INSTITUT CATALÀ DE NANOCIÈNCIA I NANOTECNOLOGIA (ICN2).

Exp. 2023-02 ICN2

1. OBJETO

El objeto de este contrato es la contratación de servicios IaaS y Paas seguros en modalidad Cloud público para la creación del centro de datos del ICN2 en un único proveedor CSP (Cloud Service Provider o Integrador), que ofrecerá, entre otras:

- Servicios IaaS (Servidores Virtuales, servicios de almacenamiento, servicios de BBDD y servicios de monitorización)
- Servicios de Escritorio o usuario virtual
- Servicios de Red y conectividad
- Servicios de Seguridad
- Servicios de Gestión IT
- Servicios Globales de puesta en marcha

La contratación de servicios IaaS y PaaS, será sobre la nube pública de Azure para dar respuesta a la totalidad de las necesidades del ICN2.

El servicio se prestará mediante la plataforma en la nube Microsoft Azure, en modalidad CSP.

El adjudicatario debe tener las herramientas necesarias para conocer el entorno del ICN2, con el objetivo de tener visibilidad de su infraestructura on-premise para el dimensionamiento de los recursos necesarios en Azure que permita alojar los sistemas detallados anteriormente tanto a nivel de computación, almacenamiento, seguridad y conectividad.

Se incluirá en la propuesta el proyecto para la transformación de la arquitectura on-premise del instituto hacia una solución basada en Cloud, incluyendo el diseño de esta arquitectura.

El periodo de vigencia del contrato será de 3 años desde su formalización más 2 prórrogas de 1 año de duración cada una.

2. PRESUPUESTO DE LICITACIÓN

El presupuesto total de licitación para el suministro descrito en el pliego de prescripciones técnicas ascenderá como máximo a **300.000,00 EUROS**, IVA INCLUIDO, con el siguiente desglose: base imponible: 300.000,00€ + 63.000,00€ (21% IVA).

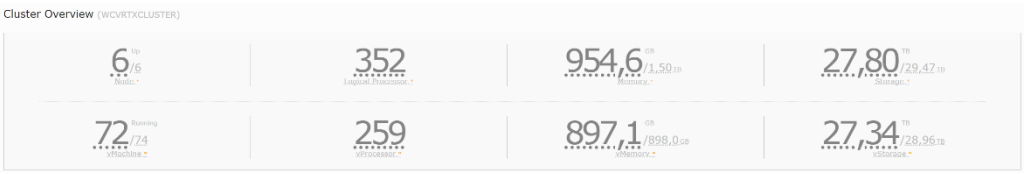
A los efectos previstos en el artículo 101 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, el valor estimado del contrato ascenderá a quinientos mil euros (500.000,00€).

A todos los efectos se entenderá que en las ofertas y en los precios aprobados están incluidos todos los gastos que la empresa adjudicataria debe realizar para el normal cumplimiento de las prestaciones contratadas, como son, los generales, beneficio industrial, salarios, financieros, benéficos, seguros, transportes y desplazamientos, honorarios del personal a su cargo, de comprobación y ensayo, materiales necesarios, tasas y toda clase de tributos, en especial el Impuesto sobre el Valor Añadido (IVA) y cualesquiera otros que pudieran establecerse o modificarse durante la vigencia del contrato, sin que por tanto puedan ser repercutidos como

partida independiente, sin perjuicio de los gastos adicionales e indeterminados económicamente derivados de los pliegos.

3. SITUACIÓN ACTUAL

Actualmente, el ICN2 dispone de un entorno de Hyper-V con el siguiente detalle:



Cluster Nodes

Name	State	Uptime	Domain	Total VM	Active vProcessor	Logical Processor	Used Memory	Free Memory	Total Memory
H001	Up	228 Days 17:33:6	icn2.net	15	40	56	157,2 GB	98,5 GB	255,7 GB
H002	Up	228 Days 17:33:9	icn2.net	10	51	56	193,7 GB	62,1 GB	255,7 GB
H003	Up	228 Days 17:33:18	icn2.net	6	29	56	105,7 GB	150,1 GB	255,7 GB
H004	Up	228 Days 17:33:34	icn2.net	5	36	56	152,1 GB	103,7 GB	255,7 GB
H005	Up	228 Days 17:33:44	icn2.net	20	41	56	170,2 GB	85,5 GB	255,7 GB
H006	Up	228 Days 17:33:14	icn2.net	18	62	72	175,8 GB	79,9 GB	255,7 GB

El dimensionamiento de las VMs es el siguiente:

Servidor	Sistema operativo	Núm. vCPU	Memoria RAM (MB)	Interfaces de red
bacs001	Windows Server 2012 R2 Standard	2	16.384	1
bccs001	Windows Server 2012 R2 Standard	2	8.192	1
c001n001	Windows Server 2012 R2 Standard	6	40.960	2
c001n002	Windows Server 2012 R2 Standard	6	40.960	2
c004n001	Windows Server 2012 R2 Standard	6	36.864	2
c004n002	Windows Server 2012 R2 Standard	6	36.864	2

Servidor	Sistema operativo	Núm. vCPU	Memoria RAM (MB)	Interfaces de red
c005n001	Windows Server 2012 R2 Standard	6	32.768	2
c005n002	Windows Server 2012 R2 Standard	6	32.768	2
c006n001	Windows Server 2012 R2 Standard	6	32.768	1
c10n1	Windows Server 2019 Standard	6	36.864	2
c10n2	Windows Server 2019 Standard	6	36.864	2
cas001	CentOS 7.9	1	2.048	1
cons001	Windows Server 2012 R2 Standard	1	4.096	1
cons002	Windows Server 2012 R2 Standard	1	4.096	1
cs001	Windows Server 2012 R2 Standard	1	2.048	1
cs002	Windows Server 2012 R2 Standard	1	2.048	1
csh001	Red Hat Enterprise Linux 7.9	1	4.096	1
css001	CentOS 7.9	2	4.096	1
ds001	Windows Server 2012 R2 Standard	1	4.096	1
ds002	Windows Server 2012 R2 Standard	1	4.096	1
eln001	Windows Server 2022 Standard	2	16.384	1
erp001	Windows Server 2012 R2 Standard	2	8.192	1

Servidor	Sistema operativo	Núm. vCPU	Memoria RAM (MB)	Interfaces de red
erp002	Windows Server 2012 R2 Standard	6	36.864	1
erp10	Windows Server 2019 Standard	4	16.384	1
hrs001	CentOS 7.9	4	8.192	1
hrs002	CentOS 7.9	2	4.096	1
hsis001	CentOS 7.9	1	2.048	1
ipm001	CentOS 7.9	1	4.096	1
is001	Windows Server 2012 R2 Standard	4	16.384	1
is002	Windows Server 2012 R2 Standard	4	16.384	1
is003	Windows Server 2012 R2 Standard	4	16.384	1
is004	Windows Server 2012 R2 Standard	4	16.384	1
is005	Windows Server 2012 R2 Standard	4	16.384	1
ldap001	CentOS 7.9	1	1.024	1
ldap002	CentOS 7.9	1	1.024	1
ls001	Windows Server 2012 R2 Standard	2	8.192	1
mos001	Windows Server 2019 Standard	8	8.192	1
ms001	CentOS 7.9	4	6.144	1
oms003	Windows Server 2012 R2 Standard	4	12.288	1

Servidor	Sistema operativo	Núm. vCPU	Memoria RAM (MB)	Interfaces de red
pms001	Windows Server 2012 R2 Standard	6	8.192	1
pms002	Windows Server 2012 R2 Standard	1	6.144	1
ras001	Windows Server 2012 R2 Standard	16	32.768	1
ras002	Windows Server 2012 R2 Standard	16	32.768	1
ras10	Windows Server 2019 Standard	16	32.768	1
ras11	Windows Server 2019 Standard	16	32.768	1
rascb001	Windows Server 2012 R2 Standard	2	4.096	1
rascb002	Windows Server 2012 R2 Standard	2	4.096	1
rascb10	Windows Server 2019 Standard	2	4.096	1
rascb11	Windows Server 2019 Standard	2	4.096	1
rods001	Windows Server 2012 R2 Standard	1	4.096	1
rods002	Windows Server 2012 R2 Standard	1	4.096	1
rs001	Windows Server 2012 R2 Standard	1	2.048	1
rs002	Windows Server 2012 R2 Standard	1	2.048	1
sms001	Windows Server 2012 R2 Standard	2	4.096	1

Servidor	Sistema operativo	Núm. vCPU	Memoria RAM (MB)	Interfaces de red
tcs001	Windows Server 2019 Standard	2	8.192	1
test001	Windows Server 2012 R2 Standard	2	8.192	1
test002	Windows Server 2019 Standard	8	16.384	1
tms001	CentOS 7.9	1	1.024	1
tss001	CentOS 7.9	1	4.096	1
was001	CentOS 7.9	2	2.048	1

4. SERVICIOS DE INFRAESTRUCTURA IaaS

El adjudicatario deberá considerar para la definición y ejecución del Plan de Migración el listado de todos los servidores virtuales detallados en el presente pliego, teniendo en cuenta que estos se alojarán en Microsoft Azure dentro de la Unión Europea.

Dado que las necesidades de uso de la plataforma Cloud pueden variar con el paso del tiempo, la distribución de los servicios es aproximada y podrán variar durante el periodo del servicio según las necesidades del ICN2. Si fuese necesario, los componentes definidos se podrán escalar a nivel superior o inferior en cualquier momento y de forma inmediata para dar respuesta a las necesidades del ICN2.

Los servicios se podrán ir activando y desactivando según se necesiten de forma dinámica. El adjudicatario indicará en su oferta cualquier limitación al respecto.

5. SEGURIDAD

5.1. Requerimientos obligatorios de los equipos de seguridad

5.1.1. Características generales de los equipos

- La propuesta deberá incluir durante la totalidad de la duración del contrato, así como las posibles prórrogas, todas las licencias y suscripciones necesarias para activar, en caso necesario, todas las funcionalidades asociadas a los requerimientos obligatorios que se listan a continuación.

- La solución debe incluir funcionalidades de control de aplicaciones, IPS, Antimalware, Webfilter, Antispam y web application firewall. Todas estas funcionalidades deben estar licenciadas para la duración del contrato.
- Los equipos deben disponer de la funcionalidad de Firewalls virtuales para crear entornos completamente diferenciales. Debe incluir al menos 10 Firewalls virtuales por equipo.
- La solución de seguridad debe permitir diferentes modos de funcionamiento, pudiéndose combinar entre los distintos Firewalls virtuales:
    - Modo transparente.
    - Modo routed y/o modo sniffer.
- Se deberá incluir en la propuesta, dentro de los propios equipos, la funcionalidad de auditoría propia del Sistema, que como resultado tenga un indicador o valor numérico de riesgo, así como puntuación negativa por cada parámetro auditado no cumplido. Estos parámetros que deben comprobarse son como mínimo: política de seguridad sin uso en los últimos 90 días, política de contraseñas débiles y comprobación del licenciamiento/soporte.
- La propia plataforma debe tener conectores automáticos con el objetivo de integrarse con identidades terceras y poder recoger información, direccionamiento ip, inventario de objetos y etiquetas. Esta funcionalidad deberá estar soportada en las appliances de seguridad (sin necesidad de consola adicional). En concreto se requieren las siguientes:
    - Cloud pública: Google Cloud, Azure, AWS, Oracle y AliCloud.
    - Cloud privada: VMware NSX y ESXi, Openstack, Kubernetes, Cisco ACI y Nuage.
    - Fuente de identidad: Active directory y Radius.
    - Fuentes de amenazas: Listado de ip, dominios y hashes de malware.
- La misma solución de seguridad debe permitir la creación de automatismos para:
    - Ante la detección de un host comprometido, los firewalls envían (todos a la vez): un email, una notificación tipo push a dispositivos Iphone, poder banear la dirección ip, invocar funciones AWS Lambda, Google functions, Azure Functions y Webhook.
    - Ante el cambio de configuración del firewall, un failover, reboot, actualización de firmas, de forma programada y cualquier evento del firewall, éste envíe (todos a la vez): un email, una notificación tipo push a dispositivos iPhone e invocar funciones AWS Lambda, Google functions, Azure Functions, AliCloud Function, pedido por CLI y Webhook.
- Capacidad de configuración de Proxy explícito por interfaz, con la funcionalidad de Proxy chaining en caso necesario, además de capacidad de caching.

5.1.2. Gestión

- La gestión debe ser de fácil uso e intuitiva.
- Capacidad de gestión de los equipos mediante acceso vía web (https) y terminal (ssh) por la total configuración de las políticas de seguridad de la plataforma.

- Quedarán excluidas aquellas soluciones que requieran una plataforma de gestión externa para gestionar y administrar la solución.
- Todos los cambios efectuados en los firewalls deben ser aplicados de forma inmediata, sin necesidad de compilar o similar.
- Creación de distintos tipos de usuario por la administración pudiendo aplicar diferentes roles o perfiles, así como definir redes de origen confiables. Es necesaria también la posibilidad de crear usuarios de tipo REST-API.
- Soporte de SNMP y sFlow.
- Exportación de logs vía SYSLOG, FTP, SCP y TFTP.

5.1.3. Rendimiento y mantenimiento

Cada uno de los dos equipos debe contar con el siguiente rendimiento:

- Las máquinas se contratan en modelo suscripción.
- VCPU de 8 cores.
- Capacidad de hasta 24 interfaces.
- Un mínimo de 10 dominios virtuales, pudiendo alcanzar 500.
- Posibilidad de contar con 200.000 políticas de firewalling.
- Un ancho de banda esperado en Azure de 4 Gbps.
- Throughput de Firewall de paquetes UDP de 1.550 Mbps (con Accelerated Networking en ON de 4 Gbps).
- 8.000 nuevas sesiones TCP por segundo.
- El throughput de IPS debe ser de 1.100 Mbps (con Accelerated Networking en ON de 3.900 Mbps).
- El throughput de conexiones HTTP de 1M por IPS debe ser de 1.160 Mbps (con Accelerated Networking en ON de 3.910 Mbps).
- El throughput de SSL Inspection debe ser de 780 Mbps (con Accelerated Networking en ON de 2160 Mbps).
- El throughput de Application Control debe ser de 1.150 Mbps (con Accelerated Networking en ON de 3.900 Mbps).
- El throughput de NGFW debe ser de 7.800 Mbps (con Accelerated Networking en ON de 1.770 Mbps).
- El throughput de Threat Protection debe ser de 790 Mbps (con Accelerated Networking en ON de 1.770 Mbps).
- El throughout de IPsec VPN (SHA2-256) para conexiones UDP de 1518 bytes debe ser de 1.400 Mbps (con Accelerated Networking en ON de 4.000 Mbps).

En lo que se refiere al mantenimiento, debe incluir 24x7.

5.1.4. Red

- Soporta protocolos RIP v1/v2, OSPF, ISIS, BGP, WCCP y Multicast per IPv4 e IPv6, Routing basado en política o PBR.
- Soporta Dual Stack IPv4 e IPv6 simultáneamente.
- Network address translation NAT IPv4, NAT64 i NAT66.
- DHCP server / DHCP Relay /DNS Server / DNS Proxy / NTP Server.

- 802.1Q VLANs y Point-to-Point Protocol over Ethernet (PPPoE).
- Capacidad de balanceo de servidores a nivel 4 para todos los servicios, como también posibilidad de hacer SSL off-loading para el tráfico HTTPS.
- Es necesario que la solución de seguridad tenga capacidades integradas de SD-WAN, en concreto:
- Balanceo inteligente de conexiones lógicas, indiferentemente del tipo de conexión WAN (MPLS, 3G/4G, FTTH, VPN, etc..).
- El número mínimo de conexiones lógicas que se pueden añadir al SD-WAN debe ser de 256.
- Verificación de la disponibilidad de Internet por cada una de las líneas, por protocolos http, ping y TWANP. El número de chequeos debe ser de al menos 100.
- Verificación de parámetros de calidad en tiempo real: jitter, packet loss y latencia por línea.
- Configuración de políticas de SD-WAN inteligente basado en origen (usuarios AD y dirección IP), en el destino (dirección IP, aplicaciones y/o servicios de Internet/aplicaciones) y en la línea con mejor calidad de aquel momento basado en valores de jitter, packet loss, latencia, tráfico de subida/bajada o ancho de banda, así como una combinación por pesos.
- En el caso de necesidad de licenciamiento o suscripciones para activar estas funcionalidades, será necesario que éstas estén incluidas en la propuesta durante la duración completa del contrato.
- Soporte de VXLAN y VXLAN VTEP por la extensión de redes de nivel 2 entre redes de nivel 3.
- El sistema propuesto debe tener una funcionalidad integrada de Traffic Shaping tanto de tráfico saliente como entrante, siendo capaz de reservar ancho de banda y marcar el tráfico con DSCP. Este traffic shaping debe basarse en aplicaciones y URLs a nivel global de perfil o por ip.

5.1.5. Visibilidad

- Los equipos firewall deben poder generar topologías gráficas físicas y lógicas, con la integración de otros firewalls del fabricante, a fin de poder ser capaz de ver en un extremo a extremo que está pasando en toda la red.

- Funcionalidad de consolidación de logs con distintos niveles de agrupación, en concreto: por origen, destino, aplicación, amenaza, websites y políticas para su visualización.
  Esta visualización debe ser tipo "Drill-down", es decir, poder seleccionar unos de los objetos agrupados e ir filtrando el resultado en base a esa selección, hasta saber el detalle completo.
  Estos requerimientos tendrán que poder cumplirse desde la misma GUI de los appliances, en tiempo real, y sin necesidad de una consola central de gestión.

5.1.6. Seguridad

- La licencia de seguridad debe cubrir lo siguiente:

  - Control de aplicaciones
  - Servicio de IPS
  - Protección Anti-Malware (que debe tener entre sus funcionalidades - antivirus, control malware para equipos móviles dentro del perímetro, anti-botnet, CDR, protección ante Virus Outbreak y servicio Sandbox en cloud)
  - Antispam
  - Servicio de filtrado web y vídeo.
- Capacidad de definir políticas de seguridad IPv4/v6 utilizando los siguientes parámetros de coincidencia:
  - Como origen (todas las opciones):
    - Capacidad de definir una y/o más de una interfaz de origen, incluyendo “año”. Así como también "zonas".
    - Capacidad de utilizar direcciones ip, rangos y/o redes, FQDN, países, servicios de internet y direcciones ip's reconocidas como origen de redes TOR, proxies anónimos (estas direcciones deben actualizarse automáticamente), así como los objetos exportados de los conectores mencionados en el apartado de características generales del equipo.
    - Capacidad de utilizar usuarios/grupos locales o AD.
    - Capacidad para declarar horarios o “schedule” tanto por día/hora como fecha máxima de vencimiento.
    - Capacidad de selección del servicio a utilizar.
- Como destino:
  - Capacidad de definir una y/o más de una interfaz de destino, incluyendo “año”. Así como también "zonas".
  - Capacidad de utilizar direcciones ip, rangos y/o red, así como objetos FQDN, países y servicios de internet.
- Capacidad de definir políticas de seguridad IPv4/v6 utilizando la siguiente parametrización:
  - Se debe poder seleccionar qué tráfico se analizará a nivel 4 y cuál a nivel 7, por política, sin excepción.
  - La configuración del NAT saliente debe poder configurarse dentro de cada una de las políticas de seguridad, de forma granular.
  - Las diferentes funcionalidades de seguridad avanzadas de nivel 7 se activarán de forma individual a nivel de política, nunca a nivel global. Además, estas se gestionarán con perfiles para ser granulares en los permisos. Estas funcionalidades son: antivirus, webfilter, DNS filter, Web Application Firewall, Control de aplicaciones, IPS y DLP.
  - Decidir a nivel de política qué tráfico SSL será descifrado por su análisis y cuál sólo a nivel de certificado.
  - A nivel de logging, es necesario que la solución permita activar el logging de sólo nivel 7, o tanto de nivel 4 más nivel 7. Es necesario también hacer captura de packets en la propia política.

- Capacidad de creación de reglas de DoS a nivel 3 y 4, pudiendo aplicar umbrales por servicios publicados donde poder filtrar por direcciones ip o países por: ip_src_session, ip_dst_session, tcp_syn_flood, tcp_port_scan, tcp_sp_src_sc,

tcp_sp_src icmp_flood, icmp_sweep, icmp_src_session, icmp_dst_session, sctp_flood, sctp_scan, sctp_src_session y sctp_dst_session.

- Con el fin de evitar el acceso de redes botnet, los firewalls deben tener una base de datos de reputación dinámica que bloquee los accesos a nivel de Interface.
- Visualización del número de usos y cantidad de tráfico de cada regla de seguridad, de forma ágil tanto en la propia sección de políticas de seguridad, así como dentro de la configuración de cada política. También hay que ver la última vez que se ha utilizado.

5.1.7. Control de aplicaciones

- Capacidad para identificar un mínimo de 1900 aplicaciones activas actuales (incluyendo aplicaciones web 2.0), como por ejemplo distinguir a Facebook, de una sub-aplicación Facebook-chat o post.
- 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).
- Aplicar técnicas de identificación de aplicaciones a todos los puertos TCP/UDP y no sólo en los más comunes.
- Capacidad para identificar aplicaciones bajo túneles HTTPS.
- Capacidad para identificar aplicaciones industriales como Modbus.
- Capacidad de creación de firmas de aplicaciones para reconocimiento personalizado. Es obligatorio que, en aquellas aplicaciones customizadas, también sean analizadas por motores de protección (IPS y antimalware).

5.1.8. IPS

- Capacidad para proteger tanto a servidores como a clientes con un mínimo de 10000 firmas de IPS, agrupadas por categoría, severidad, objetivo y protocolo. Ante la identificación de un ataque por IPS, el firewall debe capturar el tráfico en un archivo pcap para evidenciarlo y realizar un estudio posterior.
- Capacidad para identificar patrones de ataques basados en comportamiento o rated-base, a fin de bloquear intentos de ataques una vez superado un umbral de uso en un tiempo determinado.
- Capacidad de creación de firmas de IPS para un reconocimiento personalizado.

5.1.9. Antimalware

- Capacidad de detección de malware (virus, grayware, worns, etc…) basado en firmas conocidas o métodos avanzados de detección.
- Soporte de sandboxing en el cloud, con un tamaño mínimo de archivo de 100 MB indistintamente del tipo de archivo.
- Capacidad para la eliminación del contenido dinámico (macros, javascript, URL) explotable dentro de documentos ofimáticos y pdf, que se distribuyen por protocolos SMTP, IMAP y http.
- Capacidad de comprobación de si se trata de un archivo bueno o malo, en función del hashing y comparado con la BBDD del fabricante. Así como bloqueando mediante malware de repositorios externos de threat inteligence.

5.1.10. Webfilter

- Capacidad de categorizar más de 250 millones de páginas web en más de 60 categorías web para aplicar: block, monitor y aplicación de cuotas de tiempo o tráfico por categoría.
- Apoyo de protocolos http v1.0, 1.1 y 1.2.
- La base de datos de categorías web deberá consumirse como un servicio cloud en tiempo real y no podrá basarse únicamente en listados locales para tener la categorización de las url's lo más actualizado posible.
- Soporte para restringir el acceso a YouTube y Google en modo “safe search”.
- Soporte de rating por imágenes por URL.
- Apoyo para la creación de listas blancas/negras externas sin necesidad de licencia.

5.1.11. Otras funcionalidades de nivel 7

- Otras funcionalidades de nivel 7 que la propuesta debe incluir son:
    - DLP.
    - DNS Filter.
    - ICAP.
    - Web application firewall.

5.1.12. VPN

- El dispositivo admite hasta un máximo de 10.000 usuarios simultáneos VPN SSL, ya sea con o sin agente, pero en cualquier caso sin licencia adicional.
- El sistema propuesto deberá cumplir los estándares de la industria, sin el soporte externo adicional de hardware o módulos: IPSEC VPN (IPv4 e IPv6), PPTP VPN, L2TP VPN, SSL VPN y GRE sobre IPSEC.
- El sistema propuesto deberá soportar 2 modos de funcionamiento SSL VPN:
    - Sin cliente - Acceso web: para clientes remotos que sólo necesitan un navegador y no requiere la instalación de ningún agente, para acceder vía web a: HTTP / HTTPS Servidor intermediario, FTP, Telnet, SMB / CIFS, SSH, VNC y RDP.
    - Modo túnel: para equipos remotos que ejecutan una variedad de aplicaciones de cliente y servidor.
- Soporte de agregación de túneles VPN y balanceo por paquete pudiendo así añadir el ancho de banda de los accesos VPN IPsec entre sedes.
- Capacidad de integración del propio fabricante de doble factor de autenticación vía token móvil, así como por SMS y correo electrónico, integrado en la misma plataforma de seguridad. Este token también debe utilizarse para el acceso a la GUI de los equipos firewalls.

5.1.13. Controladora de acceso seguro integrada

- El sistema debe ser capaz de actuar como controladora de puntos de acceso wireless así como de switches del propio fabricante.
- La capacidad mínima de puntos de acceso debe ser de 512, y de switches de 64.
- En caso de necesidad de licenciamiento o suscripciones para activar la alta disponibilidad, será necesario que éstas estén incluidas en la propuesta durante la duración completa del contrato.
- La gestión de los APs y Switches se realizará desde la misma interfaz gráfica y CLI desde la que se gestiona el Firewall.

5.1.14. Logging y reporting

- Para el logging y reporting será necesario instalar una máquina virtual, o contar con herramienta nativamente compatible, para que los firewalls envíen en tiempo real los logs generados, cumpliendo los siguientes puntos:
    - Herramienta de monitoreo a tiempo real del tráfico filtrado por los distintos módulos de los equipos.
    - Herramienta de monitoreo histórico externa a los dispositivos, almacenamiento de logs, reportes, del tráfico analizado por los equipos con capacidad de realizar informes de 6 meses aproximadamente (incluir licenciamiento y soporte necesario durante toda la duración del contrato).
    - Reportes y alarmas en función de direcciones, puertos, protocolos.
    - Reportes y alarmas en función de usuarios y/o grupos de usuarios (AD/LDAP).
    - Poder analizar, correlacionar y realizar informes de la información de seguridad de forma centralizada.
    - Panel de control con vistas generales de usuarios destacables, aplicaciones, destinos, sitios web, vulnerabilidades, etc.
    - Modelos de informes preconfigurados, editables, modificables y exportables.
    - Gestión de eventos con generación de alertas automáticas a administradores.
    - Visor de logs en tiempo real o histórico, que permita distinguirlos entre tráfico, eventos y seguridad.
    - Visión de logs por dispositivo, dominios de administración o agregados.
    - Capacidad de filtrado y granularidad de análisis de logs.
    - Diseñador de alertas comprensible.
    - Posibilidad de generación de alertas por niveles de seguridad, eventos específicos, acciones o destinos y número de eventos en un determinado tiempo.
    - Capacidad de buscar alertas históricas.
    - Notificación de alertas por correo electrónico, SNMP o syslog.
    - Rotación de logs recopilados automática con envío de históricos a otros sistemas por email, FTP, HTTP, etc.
    - Visibilidad de los logs en formato TXT descargables.

- Vista comparada de patrones de tráfico y amenazas.
- Análisis exhaustivo de todas las actividades relacionadas con el tráfico y los dispositivos.
- Elaboración de informes sobre todas las actividades de tráfico y dispositivos.

El equipamiento de firewalling a adquirir debe ser 100% compatible con el equipo de recogida y análisis de logs que actualmente utilizamos en el instituto.

6. SERVICIOS DE IMPLANTACIÓN

6.1. Implantación y migración de servicios

El proyecto de implantación y migración de servicios a Azure, incluye las tareas detalladas a continuación:

- Diseño detallado de la solución y plan de pruebas.
- Preparación infraestructura:
  - Configuración cuentas para proyecto Microsoft Azure.
  - Creación grupos de recursos.
  - Creación redes virtuales.
  - Creación de subredes y tablas de rutas.
  - Creación cuentas de almacenamiento.
  - Despliegue máquina virtual de servicio On-Premise.
- Implementación comunicaciones:
  - Despliegue elementos de comunicaciones.
  - Enlace On-Premise a Azure.
  - Automatización failover comunicaciones.
  - Despliegue firewall en alta disponibilidad.
  - Configuración firewall.
- Implementación servicios de Azure Migrate:
  - Configuración servicio para la migración.
  - Comprobación del correcto funcionamiento del servicio.
  - Despliegue de agentes en los servidores objeto de migración.
  - Creación de planes de recuperación.
  - Activación de la primera sincronización de replicación.
- Pruebas de failover en entorno aislado:
  - Test-Failover en red aislada.
  - Ajuste de la configuración de las máquinas virtuales de acuerdo con las especificaciones del diseño (por ejemplo, cambio de dirección IP, desinstalación cliente de copias, etc.).
  - Documentación de los cambios de configuración y duración estimada de los mismos.
  - Pruebas de validación a nivel de sistemas.
  - Pruebas de aceptación a nivel funcional realizadas por el equipo del ICN2.
  - Pruebas aisladas de funcionamiento de los servidores por parte del ICN2.
  - Validación de las pruebas.
- Revisión resultados (Go/No Go):
  - Revisión de los resultados de las pruebas.

- Revisión de los tiempos necesarios para ajustar la configuración y ejecución de las pruebas de validación.
- Adecuación y validación del plan de migración.

- Paso a producción:
  - Realización de la migración de las VMs.
  - Ejecución del plan de intervención.
  - Verificación de la sincronización.
  - Parada servicios de aplicativos on-premise.
  - Última sincronización consistente.
  - Arranque VMs en Azure.
  - Comprobación del OS y comunicaciones.
  - Pruebas funcionales a realizar por parte del ICN2.
  - Validación de las pruebas.

6.2. Seguimiento del proyecto y control de calidad

6.2.1. Informes de seguimiento

Estos informes son elaborados semanalmente por el equipo de proyecto del licitador. Son informes breves que incluyen los apartados siguientes:

- Tareas finalizadas. Breve descripción de las tareas completadas en el período anterior (desde el último informe de seguimiento).
- Tareas en curso. Breve descripción de las tareas actualmente en curso.
- Tareas previstas. Breve descripción de las tareas que está previsto iniciar en el próximo período.
- Incidencias y alertas. Breve descripción de las incidencias y alertas detectadas. Se resalta especialmente el posible riesgo de desviación sobre la planificación. Se indicarán las acciones más relevantes y se informará de su cierre. Se clasifican las incidencias o alertas en:
  - Abiertas: sin resolver
  - Cerradas: las resueltas en el último período de seguimiento
  - Históricas (opcional): las resueltas en períodos anteriores.

Grado de avance. Se muestra la planificación de forma gráfica, indicando para cada tarea el grado de avance obtenido en el período.

6.2.2. Reuniones de seguimiento

Asistirán el director de proyecto del licitador, el jefe de proyecto, y los interlocutores principales del ICN2. Adicionalmente pueden asistir técnicos del licitador o internos del ICN2 para informar en detalle de algún aspecto del proyecto.

En la reunión se hace una lectura comentada del informe de seguimiento y se toman las decisiones necesarias para resolver posibles incidencias, asignación de recursos, etc. El licitador elabora y comparte el acta de cada reunión, en la que se indican los temas tratados y las decisiones tomadas.

6.2.3. Control de calidad

El control de calidad se fundamenta en el rigor con que se elaboran la propuesta y el diseño, y especialmente en el seguimiento estrecho y riguroso del proyecto. En este sentido, los informes de seguimiento y las correspondientes reuniones con el ICN2 son el instrumento principal de control de calidad.

Se presta una especial atención a las incidencias y alertas que puedan poner en peligro la planificación del proyecto.

Adicionalmente, los entregables del proyecto (diseño, sistemas implementados, procedimientos, documentación diversa, formación, etc.) seguirán un control interno con revisiones a varios niveles que garantizan la máxima calidad

6.3. Equipo de trabajo y roles

Para llevar a cabo la implementación del proyecto con garantías, el licitador propondrá un Equipo Técnico que permita asumir las funciones identificadas en el proyecto y que a la vez sea flexible con los cambios de prioridades o de funciones futuras.

Del mismo modo estos equipos serán proactivos. Es decir, además de realizar las tareas asociadas identificarán puntos de mejora, optimizarán los procesos y aportarán soluciones a los problemas detectados. Esta proactividad se llevará a cabo de una forma controlada evitando cualquier error humano.

Estos equipos deberán trabajar siempre en estrecha relación con el instituto y con los diferentes equipos involucrados, siempre bajo las directrices marcadas por el ICN2, pero siendo capaces de llevar a cabo el servicio con un nivel de supervisión y tutela mínimo.

El equipo debe integrar los siguientes perfiles: Jefe de Proyecto y Consultor/Ingeniero de Sistemas.

Por lo general, el equipo de la empresa licitadora deberá cumplir con la siguiente formación y experiencia:

- Formación
    - Licenciados o Ingenieros en Informática, Telecomunicaciones o Electrónica.
    - Postgraduados en Telemática o en Tecnología y Sistemas.
    - Continua formación especializada en productos y soluciones de sus áreas de competencia.
    - Certificaciones diversas en productos y soluciones del portfolio del licitador
- Experiencia

- Experiencia en los entornos requeridos en el presente pliego entre 1 y 5 años.

6.4. Consideraciones

- Se prevé realizar en nuestras instalaciones las tareas del proyecto que así lo requieran. Otras tareas en que no sea necesaria nuestra presencia podrán realizarse de forma remota.
- En caso de requerirse desplazamientos adicionales a los anteriores, el licitador entregaría una nueva valoración al respecto.
- Los servicios objeto de esta propuesta se realizarán dentro del horario que especifique el ICN2, excepto para las tareas en las que se indique explícitamente lo contrario. El horario habitual (no limitado al mismo) es el siguiente:
  - De Lunes a Jueves: De 08:00 a 18:00
  - Viernes: De 08:00 a 15:00
- El ICN2 designará un responsable, como punto focal, para toda la comunicación relativa al servicio.
- Se planificará la fecha de realización del servicio con anticipación suficiente. Este servicio será realizado de forma continuada.

7. MANTENIMIENTO DEL SERVICIO

Se requiere un soporte en modalidad 24x7 durante la vigencia del contrato entre el licitador y el ICN2, de los productos desplegados en Azure, basado en diferentes niveles de severidad (SLA) detallados a continuación:

- Severidad A (Crítico): En el caso que uno o más servicios no sean accesibles o no se puedan usar y los plazos de producción, operación o implementación se vean seriamente afectados, o hubiese un impacto severo en la producción o en la rentabilidad con varios usuarios o servicios afectados. Tiempo de respuesta: 1 hora.
- Severidad B (Urgente): El servicio se puede usar, pero de una forma deteriorada. La situación tiene un impacto moderado y se puede tratar durante las horas de oficina con un solo usuario o servicio parcialmente afectado. Tiempo de respuesta: 2 horas.
- Severidad C (Importante): La situación tiene un impacto mínimo. El problema es importante, pero no tiene un impacto significativo en el servicio actual ni en la productividad para nosotros con un único usuario que experimenta interrupción parcial, pero existe una solución aceptable. Tiempo de respuesta: 4 horas.

8. REQUISITOS GENERALES A CUMPLIR POR PARTE DEL LICITADOR

El licitador deberá tener presencia local en Barcelona y ofrecer soporte en castellano y catalán.

El licitador deberá acreditar 5 referencias reales en los últimos 3 años de implantación de soluciones que aborden cada uno de los siguientes ámbitos:

- Azure Windows Virtual Desktop
- Implantación/Migración en Microsoft Azure
- Implantación proyectos con Fortinet en Azure.
- Proyectos de DR

9. PLAZO DE EJECUCIÓN

La nueva infraestructura debe estar plenamente operativa 6 meses después del inicio del contrato.

10. INFORMACIÓN ADICIONAL:

Se podrá solicitar información adicional mediante envío de email a la siguiente dirección.

- **contracts@icn2.cat**

Bellaterra, a **25 de mayo** de 2023

L1-L2 Helpdesk support and Intranet Administrator[1]

[1] Documento con firma original custodiado en el expediente de contratación. Se publica documento sin firma por contener datos de carácter personal.