



VICEPRESIDENCIA,
CONSEJERÍA DE EDUCACIÓN
Y UNIVERSIDADES



Plan de Recuperación,
Transformación
y Resiliencia



Financiado por
la Unión Europea
NextGenerationEU

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL
CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE
EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO
MadQuantum-CM, FINANCIADO POR LA COMUNIDAD DE
MADRID Y POR EL PLAN DE RECUPERACIÓN,
TRANSFORMACIÓN Y RESILENCIA - FINANCIADO POR LA
UNIÓN EUROPEA - NextGenerationEU.
REDIMadrid - FUNDACIÓN IMDEA SOFTWARE**

PROCEDIMIENTO ABIERTO CON PLURALIDAD DE CRITERIOS

REF:SSL-MADQCI

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

Índice

1. Introducción	4
2. Objeto del contrato	5
2.1. Requisitos de información y publicidad	6
2.2. Requisitos de inventariado, identificación y etiquetado de inventario	7
2.3. Requisitos de confidencialidad y de gestión de la propiedad intelectual e industrial	8
2.4. Requisitos de exigencia medioambiental. Condiciones especiales de ejecución.	8
2.5. Requisitos de Inclusión de Logotipos en la Documentación	10
2.6. Compromiso de Firma de Documentación DACI	10
3. Requisitos Técnicos	11
3.1. Requisitos generales	11
3.2. Alimentación y condiciones de funcionamiento	12
3.3. Requisitos de Rendimiento y Capacidad	13
3.4. Requisitos de Interfaces de Red y Hardware	14
3.5. Requisitos de Funcionalidad de Seguridad Avanzada (NGFW/UTM)	16
3.5.1. Funcionalidades de Firewall y Control de Acceso	16
3.5.2. Funcionalidades de Detección y Prevención de Intrusiones (IDS/IPS)	20
3.5.3. Filtrado de Contenido, URL y Protección Antimalware	22
3.5.4. Inspección de Tráfico Cifrado (SSL/TLS)	25
3.5.5. Análisis de Tráfico en Tiempo Real y Detección de Anomalías	26
3.5.6. Características UTM Integradas	27
3.6. Requisitos de Acceso Remoto Seguro y Autenticación	28
3.7. Requisitos de Segmentación de Red Interna y Perfiles de Acceso	30
3.8. Requisitos de Integración con SIEM y Soluciones Empresariales	32
3.9. Requisitos de Cumplimiento de Normativas y Buenas Prácticas	34
3.10. Requisitos de Registro de Eventos y Monitorización	36
3.11. Requisitos Físicos, Ambientales e Implementación	38
3.12. Requisitos de Alta Disponibilidad y Continuidad	39

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

4. Escenario de valoración	40
4.1. Scaling equipos, PONERLO COMO JUICIO DE VALOR	46
4.2. Instalación, configuración y puesta en marcha	48
4.3. Requisitos para el Gestor del equipamiento de seguridad	49
4.4. Bolsa de horas	55
4.4.1. Operativa en la solicitud de la bolsa de horas	56
5. Soporte	56
6. Requisitos de Formación	65
7. Informes	66
7.1. Informes Regulares	66
7.2. Informes Especiales	67
8. Muestras de equipamiento/solución	67
9. Consultas y Contacto	68
10. Confidencialidad	68
11. Referencias bibliográficas	68
12. Glosario	69

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

1. Introducción

REDIMadrid es la Red Telemática de Investigación de la Comunidad de Madrid y en su trayectoria ha vivido la explosión de Internet que ha supuesto el desarrollo de las tecnologías de la información y las comunicaciones como elemento fundamental de la sociedad de la información.

El objetivo principal de la Red Telemática de Investigación de la Comunidad de Madrid es la provisión de una infraestructura de alta fiabilidad, flexibilidad y capacidad que permita la experimentación de una amplia gama de servicios telemáticos, así como la puesta en marcha de multitud de aplicaciones y proyectos de investigación.

Se pretende también mejorar y favorecer el desarrollo del trabajo cooperativo entre grupos docentes, investigadores y del colectivo científico en general de las diferentes universidades y centros de investigación de la Comunidad de Madrid y posiblemente de otras instituciones, así como la interacción de diferentes grupos de trabajo interdisciplinares dispersos, no necesariamente dentro del entorno académico.

Todos estos objetivos llevan al desarrollo de una serie de servicios que, de forma no exhaustiva, podemos ver listados a continuación:

- Servicios de Telefonía sobre IP / Videoconferencia.
- Servicios de Vídeo Bajo Demanda (VoD).
- Servicios de Teleeducación y Teleformación.
- Servicios de Telemedicina.
- Soporte de Redes Privadas Virtuales.
- Servicio de acceso a bases de datos multimedia (Bibliotecas Digitales).
- Servicios de Laboratorios Cooperativos (Laboratorios Virtuales).
- Sistemas de Tiempo Real de altas prestaciones.
- Experimentación de red piloto basada en IPv6 y QoS.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

- Experiencias de Supercomputación en Red.
- Comunicaciones cuánticas
- Servicios Anti-DDoS.
- Comunicaciones cuánticas.

La combinación de los servicios anteriores se concreta en la necesidad de gran capacidad de transporte a bajo coste y la posibilidad de su ampliación, así como la utilización de Protocolos de Internet (IP) y servicios de nivel 2.

Las necesidades de los investigadores están cambiando y eso exige una estructura de comunicaciones en la que el énfasis esté en los servicios diferenciados y en la utilización de la red como medio de colaboración para grupos cerrados de usuarios o como parte de grandes experimentos científicos de carácter regional, nacional e internacional.

En la actualidad es responsabilidad de la Fundación IMDEA Software la gestión de REDIMadrid. A efectos del presente pliego técnico se utiliza “REDIMadrid” e “IMDEA Software” indistintamente para referirse a la entidad que publica el pliego y que solicita propuestas para el suministro que se describe en dicho pliego.

2. Objeto del contrato

El objeto de la presente licitación es el suministro, instalación y soporte de equipamiento de seguridad, destinado a ser utilizados en la nueva red de infraestructura de comunicaciones cuánticas MadQCI.

Los principales objetivos de estos equipos de seguridad son, la finalización de tuneles VPN/SSL y securizar las comunicaciones dentro de la nueva red MadQCI.

En este contexto, la red MadQCI es un instrumento con el que se han vertebrado varios proyectos de investigación y desarrollo desde el 2006 hasta estos momentos, cuando se ha alineado con la visión y misión de las iniciativas Quantum Flagship y EuroQCI.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

Esta red provee la base de conocimiento, técnica y tecnológica necesaria para el despliegue de la infraestructura estable para comunicaciones cuánticas y basada en fibra óptica que aspira crear el Plan Complementario de Comunicación Cuántica en la Comunidad de Madrid.

Esta licitación forma parte del plan Complementario de Comunicaciones Cuánticas de la Comunidad de Madrid, proyecto MadQuantum-CM, financiado por la Comunidad de Madrid y la Unión Europea con fondos NextGeneration EU en el marco del Plan de Transformación, Recuperación y Resiliencia (Componente 17 Inversión 01).

El detalle, las características y la forma en que debe realizarse el suministro con garantía del equipamiento objeto de la presente licitación se establece en los apartados siguientes.

El equipamiento deberá cumplir las condiciones de hardware indicadas en el apartado 3 “Requisitos Técnicos”

Se solicita el suministro y el soporte del equipamiento así como la instalación y configuración de los equipos objeto del suministro, además de una bolsa de horas para posibles dudas/configuraciones futuras.

Así mismo también forma parte del presente procedimiento un servicio de formación del equipamiento suministrado por el adjudicatario.

2.1. Requisitos de información y publicidad

Los fondos que financian esta prestación tienen requisitos relativos a la información y publicidad de sus actuaciones. En consecuencia, el adjudicatario deberá incluir información o logos en la totalidad de los documentos, entregables, actos, etc. que formen parte de la ejecución del proyecto. En concreto, en toda la documentación que se genere susceptible de ser pública —como la formación abierta si se opta por ofertarla—, el adjudicatario deberá incorporar el conjunto de logos que figuran en la cabecera de este documento, así como el literal «Plan de Recuperación Transformación y Resiliencia, financiado por la Unión Europea – NextGenerationEU». El adjudicatario también observará lo requerido en la siguiente sección sobre inventariado, identificación y etiquetado.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

Si el adjudicatario quiere incluir su logo en la documentación, deberá ser aprobado por IMDEA y siempre deberá ir después del logo de la Comunidad de Madrid.

2.2. Requisitos de inventariado, identificación y etiquetado de inventario

Es responsabilidad del adjudicatario proporcionar la información de inventario necesaria para el correcto seguimiento de los activos de REDIMadrid. El adjudicatario se compromete a colaborar de forma diligente para proporcionar la información necesaria con la que gestionar de forma efectiva el inventario de REDIMadrid.

Los activos materiales y fungibles vendrán etiquetados con el etiquetado proporcionado por REDIMadrid. El etiquetado de inventario debe cumplir las siguientes características:

- Material resistente al desgaste, al agua, a los disolventes, a la luz, a altas temperaturas, a la abrasión y con alta resistencia a rotura.
 - Adhesivo anti-vandalismo, permanente, universal adaptable a distintas superficies.
 - Impresión con tinta indeleble de larga duración.
- Los activos materiales vendrán grabados con estampados en superficies directamente visibles, con medios indelebles. El adjudicatario debe adoptar el procedimiento mejor adaptado según el tipo de superficie, plástica o metálica, donde se realice el grabado. Se grabará la siguiente información, siendo en todo momento perfectamente legible:
- Logotipos: de REDIMadrid u otros definidos y proporcionados por REDIMadrid.
 - Código de inventario: si la hubiera, la codificación la proporcionará REDIMadrid.

En caso de sustitución del activo, el nuevo activo deberá ir etiquetado y grabado en iguales condiciones que el activo al que sustituye, de acuerdo a lo indicado en el punto [2.4](#) del presente pliego.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

2.3. Requisitos de confidencialidad y de gestión de la propiedad intelectual e industrial

El adjudicatario guardará la confidencialidad sobre el contenido de la prestación, los datos o información a la que pueda tener acceso y limitará su uso a los fines de la ejecución del contrato. IMDEA Software podrá exigir la firma de un acuerdo de confidencialidad que concrete este requisito.

El adjudicatario se compromete a la devolución de todos los activos de que haya dispuesto para la prestación del servicio contratado, ya sean documentación, materiales, intangibles o fungibles. En los casos en que REDIMadrid lo estime necesario podrá exigir al adjudicatario certificaciones de destrucción de documentos o eliminación de información de los equipos empleados para la realización de los servicios objeto del presente pliego.

2.4. Requisitos de exigencia medioambiental. Condiciones especiales de ejecución.

Los fondos que financian esta prestación tienen requisitos relativos a la exigencia medioambiental. En concreto, acorde al artículo 5 de la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia, el proyecto MadQuantum-CM debe cumplir con todos los siguientes extremos:

1. Las actividades que se desarrollan en el mismo no ocasionan un perjuicio significativo a los siguientes objetivos medioambientales, según el artículo 17 del Reglamento (UE) 2020/852, relativo al establecimiento de un marco para facilitar las inversiones sostenibles mediante la implantación de un sistema de clasificación (o «taxonomía») de las actividades económicas medioambientalmente sostenibles:
 - Mitigación del cambio climático.
 - Adaptación al cambio climático.
 - Uso sostenible y protección de los recursos hídricos y marinos.

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

- Economía circular, incluidos la prevención y el reciclado de residuos.
 - Prevención y control de la contaminación a la atmósfera, el agua o el suelo.
 - Protección y restauración de la biodiversidad y los ecosistemas.
2. Las actividades se adecuan a las características y condiciones fijadas para la componente 17, del Plan de Recuperación, Transformación y Resiliencia.
 3. Las actividades que se desarrollan en el proyecto cumplirán la normativa medioambiental vigente que resulte de aplicación.
 4. Las actividades que se desarrollan no están excluidas para su financiación por el Plan al no cumplir el principio DNSH, conforme a la Guía técnica sobre la aplicación del principio de «no causar un perjuicio significativo» en virtud del Reglamento relativo al Mecanismo de Recuperación y Resiliencia (2021/C 58/01)30, a la Propuesta de Decisión de Ejecución del Consejo, relativa a la aprobación de la evaluación del plan de recuperación y resiliencia de España y a su correspondiente Anexo.
 5. Las actividades que se desarrollan no causan efectos directos sobre el medioambiente, ni efectos indirectos primarios en todo su ciclo de vida, entendiendo como tales aquéllos que pudieran materializarse tras su finalización, una vez realizada la actividad.

En consecuencia, el adjudicatario se compromete a respetar los principios de economía circular y evitar impactos negativos significativos en el medio ambiente («DNSH» por sus siglas en inglés «do no significant harm») en la ejecución de las actuaciones llevadas a cabo.

Tras la firma del contrato, el adjudicatario entregará en el plazo máximo de VEINTE (20) días hábiles la autoevaluación justificativa de que las actuaciones a realizar en la ejecución del contrato cumplen con el principio “do not significant harm, DNSH”, “no causar perjuicio significativo al medioambiente” (memoria DNSH), en cumplimiento del artículo 17 Reglamento (UE) 2020/852 del Parlamento Europeo y del Consejo de 18 de junio de 2020.

Para la mitigación del cambio climático, se solicita la etiqueta ecológica EU.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

En el caso de sustitución total de productos, será necesario un informe o memoria explicativa en la que se deje constancia de que los nuevos productos son de una calidad equivalente a los iniciales y cumplen con los mismos criterios que los productos ofrecidos en la oferta, esta sustitución deberá aprobarse por la Fundación IMDEA Software.

Se establecerán controles periódicos de la calidad se atenderá a las cláusulas de penalización del PCAP para aquellas situaciones en las que se detecte que la calidad de los equipos suministrados no se ajusta con la indicada en la oferta presentada.

2.5. Requisitos de Inclusión de Logotipos en la Documentación

La documentación administrativa del contrato, incluyendo todos los informes que se remitan por el contratista, deberán contener un encabezado con logotipos de uso obligatorio. Si el contratista desea incluir su logotipo, deberá consultar la manera adecuada de hacerlo, teniendo que ser aprobado para asegurar el cumplimiento de las medidas de publicidad de los financiadores (Comunidad de Madrid y Ministerio de Ciencia e Innovación a través del Plan de Transformación y Resiliencia con Fondos NextGeneration-EU).

2.6. Compromiso de Firma de Documentación DACI

La presentación de una oferta conlleva el compromiso expreso de formalizar la firma de la documentación correspondiente a las "DACIs", tal y como se establece en los términos y condiciones recogidos en el Pliego de Cláusulas Administrativas Particulares (PCAP).

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

3. Requisitos Técnicos

En los siguientes subapartados se detallan los requisitos o funcionalidades mínimas que deben cumplir los equipos de seguridad ofertados por el licitador.

Esta especificación técnica define los requisitos técnicos y funcionales que debe cumplir el firewall de próxima generación (NGFW) a adquirir mediante licitación pública. Su objetivo es implementar una solución de seguridad perimetral e interna de alto rendimiento que garantice la protección de la infraestructura de gestión de MadQCI, proporcionando control de acceso granular, inspección profunda del tráfico y defensa avanzada contra amenazas.

El NGFW seleccionado deberá integrar en una plataforma unificada múltiples funcionalidades de seguridad, incluyendo firewall tradicional, NGFW, terminación de sesiones SSL, UTM (Unified Threat Management), IPS/IDS, filtrado de contenido y protección antimalware. Además, deberá cumplir con los estándares internacionales de seguridad y ser compatible con el entorno operativo existente en MadQCI, asegurando su correcta integración en la infraestructura actual.

Nota: En todos los requisitos, el término “el firewall” hace referencia a la solución NGFW completa (incluyendo hardware, software y servicios asociados) que se busca adquirir

Los requisitos enumerados en los siguientes apartados son requisitos mínimos de **obligado cumplimiento**. Las propuestas que ofrezcan características inferiores no serán tomadas en consideración en el presente procedimiento de adjudicación:

3.1. Requisitos generales

- Se requiere que todo el Suministro que se oferte no se encuentre incluido en procesos de discontinuidad, descatalogación o fin de vida del fabricante. Además, el adjudicatario deberá garantizar la vigencia del Suministro y Soporte, como mínimo, durante los **CINCO** años siguientes a la adjudicación del presente pliego.
- El equipamiento propuesto debe incluir las funcionalidades y prestaciones reque-

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

ridas en el presente pliego técnico, tanto las generales como las particulares. En este sentido, estas funcionalidades deben estar operativas y totalmente funcionales en las versiones de software que se liberen durante los, como mínimo, durante los **CINCO** años siguientes a la adjudicación del presente pliego.

- El equipamiento se suministrará aprovisionado y configurado con todos sus elementos redundados, en caso de que se soliciten, tales como fuentes de alimentación, ventiladores, así como cualquier otra tarjeta del plano de control adicional, que por arquitectura del equipamiento, pueda tener una configuración en redundancia.
- Los equipos deberán ocupar la menor huella de rack posible.
- La versión del sistema operativo que el adjudicatario instale en el equipo será la más actualizada y estable que exista en el momento del suministro, la cual implementará todas las funcionalidades especificadas en el presente pliego. En cualquier caso esta versión será consensuada con el personal de REDIMadrid. También se debe incluir todas aquellas licencias que fueran necesarias para utilizar dichas funcionalidades.
- Se incluirán todas las licencias necesarias y software necesario para el cumplimiento de las características requeridas durante la vida útil del equipamiento. Los equipos deberán mantener la funcionalidad descrita una vez finalizado el contrato, no dependiendo dicha funcionalidad de licencias con vigencia limitada a la duración del contrato, es decir, las licencias deben ser sin fecha de vencimiento.
- Debe tener interfaces de gestión via SSH y web HTTP/HTTPs con conectividad mínima 1Gbps, este puerto de administración fuera de banda debe servir para la administración del equipo sin interferir en el tráfico de datos regular.

3.2. Alimentación y condiciones de funcionamiento

- Se requiere que pueda instalarse en un rack o bastidor estándar. El adjudicatario debe suministrar todos los elementos accesorios para lograrlo, como los raíles adecuados para ello.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

- Deben poder operar en las condiciones típicas de temperatura, humedad... de los centros de datos en las universidades y con los estándares europeos de alimentación eléctrica.
- El suministro debe poder operar en entornos industriales o profesionales y estar listos para su despliegue en centros de cálculo y oficinas centrales en producción.
- Se requiere tipo de alimentación eléctrica AC 220V - 50Hz, con redundancia de fuente de alimentación si se solicita. Es decir, cada equipo tendrá al menos dos fuentes de alimentación, en una configuración automática de respaldo, en caso de que se solicite.

3.3. Requisitos de Rendimiento y Capacidad

El firewall propuesto deberá ofrecer un rendimiento suficiente para redes de alta velocidad, asegurando baja latencia incluso con funciones de seguridad avanzadas habilitadas.

1. **Throughput mínimo de firewall:** Deberá soportar un caudal mínimo de 19 Gbps de tráfico clásico de firewall (filtrado L3/L4) sin degradación, para manejar picos de carga en la red sin convertirse en un cuello de botella.
2. **Throughput mínimo de NGFW:** Deberá soportar un caudal mínimo de 9 Gbps de tráfico NGFW sin degradación, para manejar picos de carga en la red sin convertirse en un cuello de botella.
3. **Rendimiento con servicios UTM activados:** Con todas las funciones de seguridad avanzadas habilitadas (inspección DPI, IPS, antimalware, filtrado de URL, etc.), el dispositivo deberá mantener al menos 9 Gbps de throughput efectivo. Esto garantiza que el rendimiento siga siendo adecuado aun aplicando inspección profunda de paquetes y otras cargas de procesamiento intensivas.
4. **Sesiones concurrentes:** Deberá manejar al menos 2 Millones de sesiones concurrentes (conexiones activas) como mínimo. Idealmente, el diseño debe soportar varios cientos de miles o millones de sesiones para escalabilidad futura.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

5. **Nuevas conexiones por segundo:** Deberá poder establecer nuevas sesiones a una tasa sostenida de al menos 200.000 por segundo o superior, para soportar ráfagas de tráfico y numerosos intentos de conexión simultánea (por ejemplo, durante ramp-up de usuarios o reconexiones masivas tras una caída).
6. **Usuarios/VPN concurrentes:** Deberá soportar al menos 1800 usuarios remotos simultáneos conectados al NGFW mediante VPN u otras sesiones de acceso (p. ej. usuarios de VPN SSL).
7. **Baja latencia:** La inspección y el enrutamiento a través del firewall deben añadir una latencia mínima al tráfico (< 1 ms en condiciones de carga nominal para tráfico local). El dispositivo deberá incorporar técnicas de aceleración hardware/software para minimizar la latencia incluso con inspección profunda habilitada.
8. **Calidad de Servicio (QoS):** Deberá ser capaz de manejar tráfico con priorización y control de ancho de banda, aplicando QoS para garantizar el rendimiento de aplicaciones críticas bajo carga. Esto implica poder procesar colas de prioridad sin degradar el throughput total.
9. **Capacidad de cifrado acelerado (VPN):** El NGFW deberá contar con inspección SSL, de al menos 3,5Gbps.

3.4. Requisitos de Interfaces de Red y Hardware

El/los equipo/s NGFW deberá contar con interfaces de red de alta velocidad suficientes y la flexibilidad para integrarse en entornos de red existentes, soportando medios ópticos y eléctricos. Asimismo, el hardware deberá cumplir características de resiliencia y facilidad de integración física.

1. **Puerto de gestión dedicado:** Deberá incluir puerto de administración exclusivo 10/100/1000 Mbps fuera de banda para gestión sin interferir tráfico.
2. **Interfaces 10 Gigabit Ethernet (SFP+):** Deberá incluir al menos 8 puertos 10GE SFP+. Estos puertos deberán ser compatibles con transceptores estándar (SR/LR/10GBaseT) para conectar con la infraestructura de fibra/UTP existente.

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

3. **Interfaces Gigabit Ethernet ópticos (SFP):** Deberá incluir al menos 8 puertos GE SFP (puertos específicos GE o puertos duales 1GE/10GE). Estos puertos deberán ser compatibles con transceptores estándar (SR/LR/1000BaseTX) para conectar con la infraestructura de fibra/UTP existente.
4. **Soporte de enlace de respaldo/alta disponibilidad:** El NGFW deberá contar con, al menos, un puerto dedicado o la posibilidad de usar un puertos configurables para enlace de alta disponibilidad (HA) entre chasis (heartbeat/sincronización). Se describirá el requerimiento de interfaces para arquitecturas de alta disponibilidad. (ver sección de Alta Disponibilidad [3.12](#)).
5. **Agregación de enlaces (LACP):** Las interfaces de red deberán soportar IEEE 802.3ad (Link Aggregation), permitiendo combinar varios puertos físicos en un enlace lógico para mayor capacidad o redundancia
6. **Troncales VLAN (802.1Q):** Deberá soportar encapsulamiento VLAN estándar 802.1Q en sus puertos, permitiendo manejar múltiples subredes lógicas/taggeadas sobre una misma interfaz física (subinterfaces).
7. **Consola local:** El dispositivo deberá proveer un puerto de consola local (RJ-45 serie estándar y/o USB) para tareas de configuración inicial y resolución de problemas mediante acceso directo (CLI).
8. **Recursos de hardware internos:** Deberá contar con almacenamiento interno suficiente para logs, firmware y archivos de firmas.
9. **Fuente de alimentación redundante:** Para alta disponibilidad a nivel de hardware, el equipo deberá contar con fuentes de alimentación redundantes AC (doble PSU hot-swappable).
10. **Factor de forma y montaje:** El dispositivo deberá ser montable en rack estándar de 19" (preferiblemente 1U de altura, máximo 2U si se justifican requisitos de potencia). Se deberá suministrar con los kits de montaje en rack necesarios (rieles, tornillos) para su instalación física.
11. **Cumplimiento de estándares físicos:** El hardware deberá cumplir con normativas de seguridad eléctrica y compatibilidad electromagnética aplicables (p. ej., marcado CE, FCC, UL). También deberá soportar condiciones ambientales de operación

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

típicas de un centro de datos o sala de comunicaciones (temperatura, humedad, ventilación adecuada con ventiladores redundantes).

12. **Sistema operativo embebido y arranque dual:** El NGFW deberá operar con un sistema operativo dedicado en memoria. Deberá soportar arranque dual, manteniendo al menos dos versiones de firmware almacenadas para permitir revertir fácilmente a la versión previa en caso de fallo en una actualización, aumentando la resiliencia del sistema.
13. **Recuperación y respaldo de configuración:** Deberá facilitar la exportación e importación de la configuración del dispositivo. Esto incluye la posibilidad de guardar/restaurar la configuración vía GUI y CLI, ya sea al PC local, a un almacenamiento USB o a un servidor remoto (FTP/TFTP), en formatos legibles (texto plano o formatos estructurados como YAML/JSON).

3.5. Requisitos de Funcionalidad de Seguridad Avanzada (NGFW/UTM)

3.5.1. Funcionalidades de Firewall y Control de Acceso

1. **Stateful-firewall:** Deberá implementar filtrado de paquetes con inspección de estado (stateful) para tráfico IPv4 e IPv6, monitorizando conexiones establecidas y aplicando políticas de forma dinámica según el estado de la conexión.
2. **Política “deny by default”:** Deberá ser posible configurar una política por defecto de denegar todo el tráfico no autorizado explícitamente. El sistema debe facilitar la aplicación de este principio de “denegar por defecto”, permitiendo solo el tráfico que haya sido aprobado por políticas específicas.
3. **Control granular por IP/puerto/protocolo:** Deberá permitir crear reglas de acceso detalladas basadas en direcciones IP (origen/destino), puertos/servicios (TCP/UDP/ICMP/etc) y protocolos de capa 4. También debe soportar condiciones por rango de IP, subredes, rangos de puertos y grupos de servicios para mayor flexibilidad en la definición de políticas.
4. **Soporte de múltiples zonas de seguridad:** El firewall deberá manejar el concepto de zonas o dominios de seguridad (por ejemplo: zona “untrust” externa, zona

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

“trust” interna, zona DMZ, etc.). Cada interfaz o subinterfaz VLAN podrá asignarse a una zona, y las políticas se podrán definir entre zonas.

5. **Soporte de virtualización del firewall:** El firewall deberá soportar la virtualización en múltiples firewalls virtuales con administración diferenciada e interfaces virtuales asignados a cada uno de ellos.
6. **Protección contra spoofing y tráfico malicioso de capa 3/4:** Deberá incorporar mecanismos para prevenir ataques de suplantación de identidad (IP “spoofing”) y otros paquetes anómalos a nivel de red. Por ejemplo: verificación de “RPF check” en interfaces hacia internet, descarte de paquetes con direcciones inválidas o privadas en zonas indebidas, bloqueo de fragmentos malformados, etc..
7. **Tráfico IPv6:** Deberá soportar de forma nativa filtrado IPv6 con capacidades equivalentes a IPv4. Es decir, poder aplicar reglas de firewall, inspección profunda y demás funcionalidades de seguridad sobre tráfico IPv6, asegurando una protección consistente en entornos dual-stack.
8. **NAT y manejo de direcciones:** Deberá brindar funcionalidades completas de Traducción de Direcciones de Red (NAT), incluyendo NAT estático uno-a-uno, NAT dinámico/PAT (múltiples direcciones IR internas a una IP pública con diferentes puertos), y NAT inverso (DNAT) para publicación de servicios internos. Será posible configurar reglas de NAT por rango de IP, por puerto y definidas por zona (por ejemplo, NAT distinto para distintos enlaces WAN). También deberá soportar NAT para IPv6 (NAT64), si se requiere integración IPv4-IPv6.
9. **VPN site-to-site (IPsec):** El dispositivo deberá soportar túneles VPN IPsec para comunicación segura site to site. Esto incluye compatibilidad con estándares actuales (IKEv2, autenticación mediante certificados X.509 o PSK, cifrados fuertes como AES-256/ChaCha20, integridad SHA-2, PFS, etc.). Deberá permitir al menos 10 túneles IPsec concurrentes con throughput agregado significativo.
10. **VPN de acceso remoto (SSL/IPsec):** Además de las VPN entre sites, deberá soportar VPN de acceso remoto para usuarios individuales, preferiblemente usando SSL/TLS (VPN SSL) con cliente ligero o vía portal web, y/o vía IPsec con cliente. Los usuarios remotos podrán autenticarse con credenciales y 2FA (ver sección de Autenticación 3.6), estableciendo un túnel seguro hacia la red interna. Mínimo de 1800 usuarios concurrentes deberán poder utilizar la VPN.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

11. El cliente ligero deberá ser compatible con los sistemas operativos Windows, macOS y Linux. En el caso de Linux, será necesario que la instalación sea posible, como mínimo, en las distribuciones Ubuntu, Red Hat y Debian, garantizando su correcto funcionamiento y soporte en dichos entornos.
12. **VPN SSL con TLS1.3:** Deberá soportar TLS1.3 para túneles SSL.
13. **Inspección y control de aplicaciones (App Control):** En modo NGFW deberá identificar y controlar el tráfico a nivel aplicación (capa 7), más allá de puertos o protocolos básicos. Debe contar con una base de datos de firmas de aplicaciones comúnmente usadas (p.ej. redes sociales, streaming, P2P, mensajería, aplicaciones corporativas), permitiendo crear políticas para permitir, bloquear o limitar aplicaciones específicas o categorías enteras independientemente del puerto utilizado. Esto incluye detectar aplicaciones que intenten disfrazarse o usar puertos no estándar.
14. **Definición de aplicaciones personalizadas:** Además de la base de datos incorporada, deberá permitir al administrador definir firmas o aplicaciones personalizadas, para reconocer tráfico propio de REDIMadrid o aplicaciones no incluidas de fábrica. Por ejemplo, definir una aplicación por patrón de protocolo o puerto único y luego poder crear reglas sobre ella.
15. **Control basado en usuarios y grupos:** El sistema deberá integrarse con fuentes de identidad de usuarios (p. ej. Active Directory, LDAP, RADIUS) para aplicar políticas basadas en usuario o grupo, no solo IP. Es decir, debe soportar Identity-Based Policy, donde las reglas pueden referirse a grupos de AD. Esto implica que el firewall pueda mapear IP a usuarios autenticados de alguna forma (Single Sign-On, agentes, portal cautivo, etc.).
16. **Programación horaria de reglas:** Deberá permitir que las políticas de acceso (reglas firewall) puedan tener horarios definidos (time-based rules). Por ejemplo, posibilitar que ciertos accesos sólo estén permitidos en horario laboral y se bloqueen fuera de ese horario, mediante la asignación de calendarios o franjas horarias a las reglas.
17. **Calidad de Servicio por aplicación/usuario:** Deberá ser posible aplicar limitaciones de ancho de banda o prioridades en base a la aplicación o al usuario/grupo.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

18. **Alta concurrencia de políticas:** El firewall deberá soportar la creación de cientos de reglas de seguridad sin degradación significativa en el rendimiento. Es decir, su motor de políticas debe estar optimizado para manejar grandes rulesets. Se espera soportar al menos 1000 reglas distintas configurables, contemplando futuras expansiones en la matriz de control de acceso.
19. **Enrutamiento dinámico y segmentación de rutas:** Además de las capacidades de firewall, el equipo deberá soportar protocolos de enrutamiento dinámico estándar (RIP, OSPF, BGP) para integrarse plenamente en la topología de red de REDIMadrid. Asimismo, deberá manejar un número elevado de rutas estáticas (al menos 10.000) y permitir la segmentación del enrutamiento mediante VRFs separados por interfaz. Esto garantiza flexibilidad para arquitecturas de red complejas, permitiendo aislar tablas de rutas por contexto o cliente.
20. **Modos de operación L2/Transparente:** El firewall deberá ser capaz de operar no solo en modo enrutado (NAT/routing) sino también en modo transparente (bridge) a nivel 2. Incluso se valorará que ambos modos puedan usarse simultáneamente mediante instancias virtuales separadas. En modo transparente, el NGFW seguirá pudiendo aplicar políticas de seguridad, incluyendo traducción de direcciones (NAT) en tránsito si se requiere, y también permitir la terminación de túneles VPN IPsec/SSL aun cuando actúe como puente. Esta flexibilidad de modos facilita la integración en distintos escenarios de despliegue.
21. **ALG y seguridad para tráfico VoIP:** Deberá incorporar mecanismos específicos para gestionar tráfico de voz sobre IP de forma segura. En particular, el firewall soportará ALGs (Application Layer Gateways) para protocolos de voz comunes (SIP, H.323, SCCP, MGCP, etc.), abriendo dinámicamente los puertos efímeros (“pinhole opening”) necesarios para las llamadas y protegiendo a la vez contra usos maliciosos de dichos protocolos.
22. **Autenticación con portal y disclaimers:** Cuando se utilice autenticación de usuarios en las políticas de acceso, el sistema deberá ofrecer opciones de interacción con el usuario final, como la presentación de un *disclaimer* o mensaje de aceptación de condiciones, y la redirección automática a una URL/portal de autenticación captivo. Es decir, si una regla de firewall requiere identificación, el usuario deberá ser conducido a una página segura para autenticarse (p. ej., portal web), mostrando previamente un aviso legal o de uso aceptable configurable. Esta funcionalidad

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

permite implementar portales cautivos y cumplimiento de normativas informando a los usuarios antes de otorgarles acceso.

23. **Objetos de dirección MAC con “wildcards”:** Además de los objetos basados en IP, el firewall deberá permitir la creación de objetos de tipo dirección MAC con comodines (*wildcards*) para filtrado de tráfico a nivel 2. Esto significa poder definir reglas que apliquen a rangos de MAC (por ejemplo, por prefijo de fabricante OUI) u otros patrones, lo cual es útil para controlar dispositivos de cierto tipo independientemente de su IP.

3.5.2. Funcionalidades de Detección y Prevención de Intrusiones (IDS/IPS)

1. **Sistema de Prevención de Intrusiones integrado:** El NGFW deberá incorporar un IPS (Intrusion Prevention System) de próxima generación integrado, capaz de detectar y bloquear ataques a nivel de red y aplicación en tiempo real. Deberá monitorizar el tráfico en busca de firmas de ataques conocidos, exploits, anomalías de protocolo y comportamiento malicioso.
2. **Cobertura de firmas amplia y actualizable:** El IPS deberá contar con una base de datos amplia de firmas de ataques y vulnerabilidades (miles de firmas), cubriendo amenazas conocidas (por ejemplo, explotación de vulnerabilidades con CVE reconocidos, ataques DoS, scans, etc.). Esta base de datos debe actualizarse regularmente (idealmente diario o en tiempo real) por el fabricante para incluir nuevas amenazas emergentes.
3. **Prevención activa:** Ante la detección de un patrón malicioso, el sistema deberá poder bloquear activamente el tráfico correspondiente (no solo alertar). Es decir, funcionar en modo “inline” de prevención, descartando paquetes o reseteando conexiones sospechosas según políticas definidas, para evitar intrusiones. También podrá operar en modo de solo detección (IDS) si se configura así, pero el requisito principal es la capacidad de prevención.
4. **Bajo impacto en rendimiento:** El IPS deberá estar optimizado (vía hardware dedicado o algoritmos eficientes) para inspeccionar el tráfico a alta velocidad sin introducir latencia apreciable ni reducir significativamente el throughput por debajo de los requisitos.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

5. **Protección frente a exploits de día-cero (Zero-Day):** Además de firmas conocidas, el sistema debería emplear técnicas heurísticas o de detección de anomalías para identificar posibles ataques desconocidos o de día-cero basados en comportamiento sospechoso. Por ejemplo, detección de desbordes de búfer genéricos, secuencias típicas de exploit, o uso de inteligencia artificial para marcar tráfico anómalo.
6. **Personalización de firmas y excepciones:** Deberá permitir habilitar/deshabilitar firmas IPS individualmente o por grupos/categorías (p. ej. por tipo de servidor/protocolo) para afinar la protección y reducir falsos positivos. Asimismo, deberá ser posible crear excepciones (whitelist) para ciertas firmas o orígenes/destinos en caso de tráfico conocido que dispare la firma inadvertidamente.
7. **Firmas IPS personalizadas:** Además de la amplia base de datos de firmas provista por el fabricante, el sistema deberá permitir al administrador definir nuevas firmas IPS personalizadas. Es decir, poder crear reglas de detección propias para patrones de ataque específicos o amenazas emergentes no cubiertas de fábrica. Esto asegura que REDIMadrid pueda responder rápidamente ante ataques dirigidos o particulares creando sus propias firmas en el IPS.
8. **Detección granular de DoS/escaneo por umbrales:** El IPS deberá incluir mecanismos específicos para detectar ataques de denegación de servicio o exploración de red basados en umbrales estadísticos. Por ejemplo, identificar situaciones de “flooding” (cuando una sola IP destino recibe un volumen de conexiones por segundo por encima de un umbral definido), detección de “port scanning” (muchas conexiones nuevas por segundo desde una misma fuente a distintos puertos), o límites de sesiones simultáneas por origen/destino. Estos umbrales deberán ser configurables por el administrador, y al ser excedidos, el sistema deberá tomar acciones automáticas (bloquear tráfico, poner en cuarentena la IP atacante, etc.). Esto complementa las detecciones por firmas con protección contra ataques de fuerza bruta a nivel de tráfico.
9. **Detección de evasiones:** El IPS debe manejar tácticas de evasión comunes (fragmentación de paquetes, órdenes de TCP fuera de secuencia, payloads codificados, etc.) y aun así detectar los ataques. Debe reensamblar flujos y normalizar el tráfico de modo que los intentos de evadir la detección sean infructuosos.
10. **Alertas en tiempo real:** Cada evento de intrusión detectado deberá poder generar

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

alertas en tiempo real (para registro local, syslog, SIEM, etc., ver sección de registros) con información detallada: tipo de ataque, dirección origen/destino, puerto, firma activada, acción tomada (bloqueo/permitir), etc. Esto facilita la respuesta rápida ante incidentes.

11. **Modo IDS pasivo (“One-Arm IDS”):** Además del modo inline de prevención activa, el sistema deberá poder operar en un modo de solo detección completamente pasivo. Esto implica la posibilidad de conectar el NGFW a un puerto espejo (SPAN) o “tap” de red para monitorizar tráfico sin añadir latencia, actuando como un sensor IDS que no interfiere en la comunicación.

3.5.3. Filtrado de Contenido, URL y Protección Antimalware

1. **Filtrado de contenido web (URL Filtering):** El firewall deberá integrar funcionalidad de filtrado web por URL/categorías, permitiendo controlar el acceso de usuarios a sites web según políticas corporativas. Deberá incluir una base de datos de categorías de URLs (por ejemplo: redes sociales, noticias, juegos, pornografía, malware, etc.) mantenida y actualizada por el fabricante. Será posible bloquear, permitir o limitar el acceso a categorías enteras o URL específicas, así como crear listas blancas y negras personalizadas.
2. **Actualización de categorías en tiempo real:** La solución de filtrado web debe recibir actualizaciones frecuentes (diarias o en tiempo real) de la base de datos de categorización de sites, para incluir nuevos dominios y mantener la eficacia del filtrado frente a páginas de reciente aparición.
3. **Bloqueo de contenido según tipo de archivo:** Deberá ser posible filtrar o bloquear la transferencia de ciertos tipos de archivos a través del firewall (por ejemplo, adjuntos de correo o descargas HTTP/FTP). Esto incluye poder identificar extensiones/MIME (exe, zip, pdf, docx, etc.) y definir políticas para impedir descarga o subida de ficheros ejecutables o potencialmente peligrosos desde/red hacia segmentos no autorizados.
4. **Anti-Malware/Antivirus integrado:** La solución deberá incluir un motor de detección de malware y virus integrado, analizando el tráfico en busca de código malicioso incrustado en protocolos comunes (HTTP, HTTPS – previo descifrado

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

–, SMTP, FTP, etc.). Deberá detectar virus, spyware, trojanos, rootkits y demás malware conocidos mediante firmas de antivirus actualizables.

5. **Actualización de firmas de malware:** El motor antimalware deberá actualizar automáticamente sus firmas de virus/malware desde los servidores del fabricante con una frecuencia alta (al menos diaria o incluso varias veces por día) para proteger contra las amenazas más recientes. Se describirá el mecanismo.
6. **Análisis profundo de archivos (sandboxing):** La solución deberá ofrecer análisis en “sandbox” de archivos sospechosos que no coincidan con firmas conocidas. Es decir, la capacidad de enviar archivos adjuntos o descargados a un servicio de “sandbox” en la nube o local, donde se ejecuten en un entorno aislado para observar comportamientos maliciosos de tipo “zero-day”.
7. **Protección contra sites maliciosos (filtro DNS/URL maliciosas):** Deberá incluir mecanismos para bloquear el acceso a dominios o URL reconocidamente maliciosos o de phishing, consultando en tiempo real listas de reputación. Por ejemplo, si un usuario intenta navegar a un dominio de comando&control conocido, el firewall debe impedirlo. Esto puede lograrse via filtrado de DNS maliciosos, categorías de “malware” en filtro URL, o listas de threat intelligence integradas.
8. **Detección de contenido activo malicioso:** El sistema debe inspeccionar contenido activo en tráfico web o de documentos (p. ej. JavaScript, macros en documentos Office, PDFs con exploits) y detectar patrones maliciosos. Ante detección de payload malicioso embebido, deberá bloquear la transferencia del contenido al destino y generar alerta.
9. **Anti-Spam/Anti-Phishing:** La solución propuesta deberá contar con capacidad de filtrado antispam para correo electrónico, así como de detección de phishing.
10. **Detección de grayware y software no deseado:** La solución antimalware deberá ser capaz de identificar y bloquear no solo malware conocido, sino también categorías de software potencialmente no deseado (grayware). Esto incluye adware, Browser Helper Objects maliciosos (“hijackers” de navegador), keyloggers y otros programas espía que, si bien no son virus tradicionales, representan un riesgo para la seguridad o productividad. El NGFW deberá permitir aplicar políticas específicas contra estos programas (por ejemplo, bloquear adware mientras se permite

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

software legítimo), añadiendo granularidad en la protección más allá de virus y spyware convencionales.

10. **“Virus Outbreak Protection” y CDR:** Se deberán integrar técnicas avanzadas de protección antimalware como “Virus Outbreak Protection” y “Content Disarm & Reconstruction” (CDR). La primera permite reaccionar rápidamente ante brotes masivos de malware recién aparecidos, aplicando medidas temporales (como bloquear archivos sospechosos) incluso antes de disponer de firmas detalladas. La segunda (CDR) implica analizar documentos y archivos entrantes, eliminar o neutralizar el contenido activo potencialmente peligroso (por ejemplo, macros en documentos Office, scripts embebidos en PDFs) y reconstruir el archivo limpio antes de entregarlo al usuario. Con estas funciones, el firewall no solo detectará malware conocido, sino que minimizará el riesgo de amenazas de “día cero” limpiando preventivamente contenido sospechoso.
11. **Control por tamaño de archivo:** Deberá ser posible definir umbrales de tamaño de fichero para la inspección de contenido. Es decir, el administrador podrá establecer que el firewall bloquee (o permita sin inspección) archivos por encima de cierto tamaño en determinados protocolos o reglas. Esto previene que archivos excesivamente grandes (que pueden demorar mucho en escanear) saturen los recursos del sistema o evadan el análisis por “timeouts”.
12. **Mecanismos de descarga con inspección optimizada:** Para mejorar la experiencia del usuario sin comprometer la seguridad, el NGFW deberá soportar técnicas de descarga diferida con notificación. Esto significa que, al inspeccionar un archivo en descarga (por ejemplo, análisis antivirus de un fichero grande), el sistema puede ir enviando porciones iniciales inocuas al cliente junto con una indicación de “descarga en curso/escaneo en progreso”. De este modo el usuario ve actividad (no expira la conexión por “timeout”) mientras el firewall termina de escanear el resto del archivo. Si al final el archivo resulta limpio, la descarga continúa transparentemente; si es malicioso, se bloquea antes de entregar las partes peligrosas. Este mecanismo evita cortes de conexión y mejora la usabilidad cuando se aplican inspecciones profundas.
13. **Prevención de fuga de datos (DLP):** Se deberá incorporar funcionalidad de “Data Loss Prevention” integrada. El NGFW podrá inspeccionar el contenido saliente (y

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

entrante, según política) en busca de datos sensibles o restringidos de la organización, como podrían ser números de tarjeta de crédito, identificaciones personales (DNI/NIF), información clasificada, etc. El administrador podrá definir patrones o usar plantillas predefinidas para detectar este tipo de información en tráfico email, web u otros protocolos, y el sistema deberá bloquear o alertar cuando detecte una posible filtración de datos no autorizada fuera de la red corporativa.

3.5.4. Inspección de Tráfico Cifrado (SSL/TLS)

1. **Intercepción SSL/TLS (MITM):** El NGFW deberá ser capaz de interceptar y descifrar tráfico SSL/TLS tanto saliente como entrante (SSL Inspection) para aplicar las funciones de seguridad mencionadas (IPS, antimalware, filtrado URL) incluso cuando el tráfico esté cifrado. Deberá actuar como proxy/intermediario, descifrando la sesión, inspeccionando el contenido y volviendo a cifrar hacia el destino, de forma transparente para el usuario final.
2. **Compatibilidad con TLS 1.3 y cifrados modernos:** La solución de inspección SSL deberá soportar TLS 1.3 (y versiones previas TLS 1.2, 1.1) incluyendo los cifrados y protocolos más recientes, sin degradar las conexiones a versiones inseguras. Es decir, debe poder realizar intercepción de TLS 1.3 sin downgrading, manteniendo las características de seguridad (como Perfect Forward Secrecy) en la medida de lo posible durante la inspección.
3. **Rendimiento en inspección SSL:** Deberá poder manejar tráfico cifrado a gran volumen. El rendimiento con inspección SSL habilitada deberá ser acorde a un porcentaje significativo del throughput nominal del NGFW. Se espera que incorpore aceleración criptográfica para lograrlo.
4. **Gestión de certificados y CA propia:** El sistema deberá permitir la importación/instalación de certificados de autoridad (CA) propios de REDIMadrid para usarse en el “re-cifrado” TLS hacia los clientes internos. De igual forma, manejar listas de exclusión de sites a no inspeccionar (por ejemplo, banca online o servicios sensibles por privacidad) mediante reglas de bypass de la inspección. La administración de la inspección SSL debe ser granular.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

5. **Compatibilidad con clientes y validación:** La implementación debe ser compatible con la mayoría de clientes y dispositivos (navegadores, apps móviles), presentando certificados válidos “re-firmados” por la CA interna. También deberá validar los certificados de los servidores externos (revocación, fechas) y ofrecer opciones de política ante certificados no confiables (bloquear, permitir sin inspección, etc.).

3.5.5. Análisis de Tráfico en Tiempo Real y Detección de Anomalías

1. **Monitorización y análisis en tiempo real:** El firewall deberá analizar el tráfico en tiempo real, identificando patrones sospechosos o comportamientos anómalos instantáneamente. Más allá de firmas predefinidas, deberá implementar capacidades de analítica de flujo para detección de posibles amenazas que surjan de patrones de tráfico inusuales (por ejemplo, un host interno estableciendo conexiones a cientos de destinos distintos en poco tiempo).
2. **Detección de amenazas emergentes (Behavioral Analysis):** Deberá contar con tecnologías de análisis de comportamiento (p. ej. Machine Learning, heurísticas avanzadas) que complementen al IPS tradicional. Esto puede incluir evaluación de baselines de tráfico y alertar cuando un usuario/dispositivo excede su patrón normal (indicando posible compromiso).
3. **Identificación de usuarios de alto riesgo:** La solución debería ofrecer funcionalidad para calificar el riesgo de usuarios o hosts internos según sus actividades (por ejemplo, un usuario que visita sites web no permitidos frecuentemente o ejecuta descargas sospechosas podría marcarse con mayor riesgo). Esta información ayuda a tomar acciones proactivas en segmentación o políticas más estrictas para dichos usuarios.
4. **Correlación de eventos de seguridad:** Deberá integrar de forma unificada las diversas funciones de seguridad (firewall, IPS, filtrado, etc.) de modo que pueda correlacionar eventos y proveer una visión única de incidentes. Por ejemplo, si se detecta malware en un tráfico web de un host interno y luego intentos de conexión de ese host a un C&C, el sistema debe relacionar ambos sucesos. Esta correlación puede ocurrir en el propio dispositivo o en la plataforma de gestión centralizada.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

5. **Prevención de exploraciones y barridos:** El firewall/IPS deberá detectar patrones de escaneo de puertos o redes provenientes del exterior (o interior) y tomar medidas (bloquear IP origen temporalmente, alertar). Igualmente, deberá identificar intentos de fuerza bruta comunes (p. ej. múltiples intentos fallidos de login a un servicio) y permitir establecer políticas de bloqueo tras umbrales.
6. **Modo Tap/Monitor:** Además del modo en producción, la solución deberá soportar un modo de monitorización pasivo (tap mode) donde inspeccione tráfico sin interrumpirlo, solo para detección. Esto puede ser útil en etapas de despliegue o para análisis forense en paralelo.

3.5.6. Características UTM Integradas

1. **Gestión unificada de amenazas:** Todas las capacidades mencionadas (firewall, IPS, antimalware, filtrado, VPN, etc.) deberán estar integradas en una misma plataforma y administrables de forma centralizada/unificada. El NGFW debe comportarse como un solución UTM completa, simplificando la gestión al ofrecer políticas unificadas que combinen diferentes módulos (por ejemplo, una única regla puede incluir criterios de usuario + aplicación + categoría web + inspección IPS).
2. **Procesamiento en una sola pasada ("single-pass"):** La arquitectura interna del firewall debe aplicar las múltiples inspecciones de seguridad de forma eficiente, evitando procesar múltiples veces el mismo flujo de datos.
3. **Actualizaciones centralizadas de seguridad:** La plataforma deberá recibir actualizaciones automáticas para todos sus componentes de seguridad: firmas IPS, definiciones de aplicaciones, categorías web, firmas de antivirus, listas de reputación, etc., desde la nube del fabricante. Estas actualizaciones deben poder programarse en horarios específicos y con alta frecuencia, asegurando protección continua sin intervención manual constante.
4. **Modo fail-open/fail-close:** En caso de sobrecarga extrema del sistema o fallo de componentes de seguridad, deberá haber opciones configurables de tolerancia: por ejemplo, fail-open (dejar pasar tráfico sin inspección si el módulo de inspección falla, para no interrumpir la red) o fail-close (bloquear tráfico si no puede inspeccionarse, para máxima seguridad). La elección dependerá de la política de

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

REDIMadrid, pero la plataforma debe soportar al menos una de las modalidades de forma segura.

5. **Compatibilidad con arquitecturas de virtualización:** Aunque se trata de un appliance físico principalmente, sería positivo que el fabricante ofreciera opciones virtualizadas o en la nube de funcionalidad equivalente, para continuidad de estrategia multi-cloud o pruebas.

3.6. Requisitos de Acceso Remoto Seguro y Autenticación

1. **VPN SSL/TLS para acceso remoto:** Deberá proveer una solución de VPN basada en SSL/TLS para usuarios remotos, que permita el acceso seguro a la red "trust" desde Internet. Esto puede ser mediante un portal web VPN (acceso a aplicaciones internas via navegador) y/o un cliente VPN instalado en el equipo del usuario que establezca un túnel SSL. El tráfico VPN entrante se terminará en el firewall, el cual aplicará las políticas de seguridad correspondientes al tráfico de esos usuarios. Deberá soportarse TLS1.3 acorde a la RFC8446 del IETF.
2. **Autenticación de doble factor (2FA) en VPN:** La solución VPN deberá soportar autenticación de múltiples factores para usuarios remotos. Es decir, además de usuario/contraseña, requerir un segundo factor como código temporal (TOTP), token físico, notificación push o biometría. Se integrará con sistemas 2FA existentes vía RADIUS, SAML, LDAP u otros. Esto sigue las mejores prácticas NIST para acceso remoto seguro y es mandatorio para maximizar la seguridad de las conexiones externas.
3. **Protocolos VPN adicionales:** Además de SSL VPN, deberá soportar VPN IPsec para acceso remoto como opción (p.ej. compatibilidad con clientes IPsec/IKEv2 nativos de sistemas operativos). Esto proporciona flexibilidad a usuarios que prefieran ese método. La autenticación 2FA mencionada deberá ser posible también en conexiones IPsec/IKEv2 (vía EAP Radius o mecanismos similares).
4. **Autenticación de usuarios internos:** Para el control de acceso basado en identidad, el firewall deberá integrarse con servidores de autenticación internos (Active

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

Directory, LDAP, servidores RADIUS) para validar credenciales de usuarios internos. Esto puede lograrse mediante mecanismos como Single Sign-On (SSO) (por ejemplo, utilizando agentes que capturen logins de Windows AD) o mediante portal cautivo del propio firewall que solicite credenciales a un usuario desconocido en la red. El requisito es que los usuarios de la red “trust” puedan ser autenticados/transparentemente identificados para aplicar políticas según su perfil.

5. **Autenticación de administradores con 2FA:** El acceso a la consola de administración del firewall (GUI/CLI) deberá poder protegerse también con autenticación de doble factor para cuentas de administrador. Esto añade una capa extra para impedir accesos no autorizados a la configuración, cumpliendo también con requisitos de normativa (p. ej. PCI-DSS exige 2FA para acceso de administradores desde redes no confiables).
6. **Integración con directorios de usuarios:** La solución debe facilitar la sincronización de cuentas/grupos desde directorios existentes (ej., importar grupos de AD para usarlos en reglas). También deberá soportar RADIUS/TACACS+ para la autenticación y autorización de administradores de red que acceden al firewall, permitiendo gestionar permisos administrativos de forma centralizada.
7. **Control de acceso basado en roles (RBAC):** Deberá implementarse un sistema de roles de usuario para administración y para el portal VPN. Esto significa que se puedan definir perfiles de administrador con permisos granulares (por ejemplo, administrador de seguridad vs operador de monitorización vs auditor con solo lectura). Cada administrador se asignará a un rol que limita las acciones que puede realizar en la interfaz de gestión del firewall.
8. **Aceleración y capacidad VPN IPsec:** El dispositivo deberá aprovechar aceleración hardware para cifrado, permitiendo “throughputs” elevados en túneles VPN site-to-site.
9. **Túneles IPsec basados en política vs ruta:** Deberá soportarse tanto el modelo de VPN IPsec “route-based” (túnel vinculado a una interfaz virtual y rutas estáticas/dinámicas) como “policy-based” (reglas de firewall que disparan la VPN). Esta flexibilidad permite integrar el NGFW en entornos donde se prefiera una u otra configuración. Por ejemplo, algunos escenarios “legacy” usan VPN basadas en política para ciertos flujos; el equipo ofrecido deberá acomodar ese esquema

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

además del moderno basado en rutas, facilitando la migración y compatibilidad con diversos despliegues.

10. **Flexibilidad en puertos y protocolos VPN:** La solución VPN deberá tolerar entornos restrictivos. En concreto, se deberá poder configurar el puerto IKE (UDP 500/4500) en un valor no estándar si un ISP o NAT lo bloquea, facilitando el establecimiento de túneles IPsec aún tras firewalls de terceros. Asimismo, deberá soportarse tráfico VPN sobre IPv6 (túneles IPsec IPv6 nativos o “dual-stack”), garantizando compatibilidad con redes de nueva generación. Estas capacidades aseguran que las VPN funcionen incluso atravesando filtros estrictos o en entornos exclusivamente IPv6, otorgando máxima interoperabilidad.
11. **Agrupación de túneles (VPN redundante/agrupada):** Deberá contemplarse la posibilidad de configurar túneles IPsec agregados o redundantes hacia un mismo destino. Esto implica soportar modalidades de “tunnel bonding” o al menos conmutación por fallo/balanceo entre múltiples túneles IPsec que conecten dos sedes. Por ejemplo, si existen dos enlaces WAN diferentes, poder establecer dos túneles IPsec paralelos y agregarlos lógicamente para aumentar el ancho de banda utilizable o asegurar continuidad (si uno cae, el tráfico continúa por el otro automáticamente).
12. **Alcance y momento de evaluación VPN SSL** La solución de acceso remoto VPN SSL deberá realizar una verificación del dispositivo antes de otorgar acceso a recursos y de forma periódica durante la sesión (re-evaluación por intervalo y ante cambios de red/estado). Si el dispositivo no cumple, no se otorgará acceso o se aislará en cuarentena con permisos mínimos.
13. **Alcance y momento de evaluación VPN IPSec** La solución de acceso remoto VPN IPSec deberá realizar una verificación del dispositivo antes de otorgar acceso a recursos. Si el dispositivo no cumple, no se otorgará acceso o se aislará en cuarentena con permisos mínimos.

3.7. Requisitos de Segmentación de Red Interna y Perfiles de Acceso

1. **Múltiples zonas/segmentos internos:** Deberá soportar la definición de múltiples segmentos dentro de la red “trust”. Por ejemplo, poder subdividir la red “interna”

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

en VLANs o subredes separadas (segmentos para departamentos, invitados, servidores, IoT, etc.), con el firewall ejerciendo control de tráfico entre ellas. El firewall deberá soportar al menos 20 zonas lógicas distintas, permitiendo escalabilidad para futuras subdivisiones.

2. **Perfiles de seguridad diferenciados por segmento:** Para cada segmento o zona interna, deberá ser posible aplicar perfiles de políticas de seguridad diferentes. Por ejemplo, la red de invitados podría tener un perfil que limita mucho el acceso (solo navegación web filtrada), mientras la red de servidores tiene otro con inspección IPS intensiva y sin salida a Internet directa, etc. El firewall deberá permitir asignar conjuntos de reglas y configuraciones UTM por zona o grupo de usuarios, proporcionando esta diferenciación.
3. **Control de acceso interno estricto:** Deberá ser posible regular el tráfico Este-Oeste (lateral) dentro de la red trust, no solo el tráfico hacia/desde Internet. Esto implica que el firewall actúe como punto de control entre subredes internas, aplicando políticas que impidan accesos no autorizados entre departamentos o hacia servidores sensibles. Por ejemplo, bloquear que estaciones de trabajo accedan directamente a servidores DB excepto las permitidas.
4. **Aislamiento de invitados y BYOD:** El sistema deberá facilitar la creación de una zona de invitados/BYOD aislada de los recursos internos críticos. Este segmento tendrá políticas restrictivas (por ejemplo, solo acceso a internet y quizás a un portal específico) y el firewall deberá asegurar que no haya “routing” ni “bridging” inadvertidos hacia la LAN corporativa desde dicha zona. También se aplicarán perfiles de filtrado propios (por ejemplo, filtrado web más estricto en invitados).
5. **Segmentación basada en identidad:** Complementando la segmentación por red, la solución debe soportar segmentación definida por software basada en identidad o rol. Por ejemplo, dos usuarios conectados a la misma VLAN física, pero de departamentos distintos podrían tener aislamientos lógicos distintos gracias a políticas que usan la identidad del usuario. En esencia, el firewall podrá aplicar micro-segmentación a nivel de usuario o grupo dentro de la misma red física.
6. **Compatibilidad con estrategias Zero Trust:** Los mecanismos de segmentación deberán apoyar una arquitectura de Zero Trust Network, donde ningún usuario o

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

dispositivo interno es automáticamente confiable. Deberá ser posible exigir “re-autenticación” para ciertos accesos, monitorizar continuamente el tráfico interno y aplicar políticas adaptativas. Si bien la implementación completa de Zero Trust puede exceder el alcance del firewall por sí solo, el NGFW debe ofrecer las herramientas necesarias (segmentación, identidad, inspección interna) para implementarla progresivamente.

7. **Gestión centralizada de perfiles:** La creación y administración de estos perfiles de acceso segmentados deberá poder realizarse de forma centralizada, asegurando consistencia. Es decir, si en la plataforma de gestión se define un perfil de seguridad “Alto” y otro “Medio”, se podrán aplicar a distintas zonas fácilmente. Esto facilita la administración de múltiples segmentos con políticas comunes reutilizables.
8. **Rendimiento en segmentación interna:** El firewall deberá poder manejar el tráfico interno segmentado a alta velocidad, para que la inspección entre VLANs no introduzca cuellos de botella. Por ejemplo, si la red corporativa interna es de 10Gbps entre switches, el firewall deberá ser capaz de procesar flujos entre segmentos internos a velocidades cercanas sin latencia significativa, incluso aplicando las políticas de seguridad correspondientes.

3.8. Requisitos de Integración con SIEM y Soluciones Empresariales

1. **Integración con SIEM (Security Information and Event Management):** Deberá ser capaz de exportar eventos y registros de seguridad al sistema SIEM corporativo en tiempo real. Esto típicamente se logra mediante syslog (TCP/UDP) usando formatos estándar (por ejemplo, CEF, LEEF o formato propio documentado). El firewall debe permitir configurar múltiples destinos de log/SIEM, con facilidades para seleccionar qué eventos enviar. La integración debe cubrir eventos de tráfico, alertas IPS, detecciones de malware, eventos de autenticación, etc.
2. **Formato de logs estándar:** Los registros enviados deberán incluir todos los campos relevantes (fecha/hora, IP origen/destino, puertos, protocolo, acción tomada, usuario, regla coincidente, etc.) en un formato compatible con los principales SIEM

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

del mercado para minimizar esfuerzos de normalización. El fabricante proporcionará un conector/parsing específico para su formato en SIEM comunes (Splunk, QRadar, ArcSight, etc.).

3. **Integración con sistemas de gestión de identidades:** El firewall deberá poder integrarse con Active Directory/LDAP para información de usuarios. Adicionalmente, el NGFW deberá poder utilizar un servidor RADIUS o autenticación unificada SSO/SAML para autenticación tanto de usuarios VPN como administradores. La solución debe demostrar flexibilidad para trabajar con las plataformas de identidad existentes, evitando introducir sistemas aislados.
4. **Integración con plataformas de orquestación y respuesta (SOAR):** El firewall deberá ofrecer APIs o conectores que permitan su integración en flujos de orquestación (SOAR) o scripts de automatización. Por ejemplo, una API RESTful para extraer logs, agregar reglas temporales, o aislar un host automáticamente si el SIEM/SOAR determina que está comprometido. Esto habilita una respuesta más rápida ante incidentes de seguridad.
5. **Compatibilidad con soluciones NAC (Network Access Control):** El firewall deberá poder interoperar con soluciones NAC. Por ejemplo, soportar la recepción de VLAN de cuarentena o cambios dinámicos de políticas basados en la calificación de un “endpoint” evaluado por el NAC. Además, deberá poder proporcionar información al NAC (vía syslog o API) sobre actividad de un dispositivo.
6. **Feeding de inteligencia de amenazas externa:** Deberá soportar la importación de “feeds” de inteligencia de amenazas de terceros (bloque de IoCs – Indicadores de Compromiso). Por ejemplo, la capacidad de suscribirse a fuentes STIX/TAXII o listas de IP maliciosas públicas para automáticamente bloquear tráfico hacia/desde esas IPs o dominios. Esto permite ampliar la inteligencia del firewall más allá de la ofrecida por el fabricante, integrándolo con el ecosistema global de ciberseguridad.
7. **Integración con sandbox/cloud:** El fabricante deberá ofrecer una solución cloud de sandboxing o análisis avanzado, el firewall deberá integrarse fluidamente con ella, enviando muestras y recibiendo veredictos en tiempo real. Además, deberá poder aprovechar servicios en la nube de reputación de seguridad ofrecidos por el fabricante (por ejemplo, consultas “cloud” para categorizar una URL desconocida al momento).

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

8. **Interoperabilidad general:** En resumen, la solución no debe ser un silo cerrado; por el contrario, deberá demostrar interoperabilidad con estándares abiertos y herramientas comunes de la industria. Soporte para protocolos como SNMP v2/v3 (monitorización básico), SMTP (envío de alertas por correo), REST API/JSON, y formatos de exportación de configuraciones (XML/JSON) serán considerados en la evaluación.

3.9. Requisitos de Cumplimiento de Normativas y Buenas Prácticas

1. **Cumplimiento NIST SP 800-41:** El NGFW deberá ajustarse a las “Guías sobre Firewalls y Políticas de Firewall” de NIST SP 800-41 Rev.1. En particular, deberá permitir implementar políticas sólidas de filtrado, segmentación de red y gestión de reglas que sigan las recomendaciones de NIST. Esto incluye aspectos como: política por defecto de denegar, reglas lo más específicas posible, monitorización constante de logs de firewall, y capacidad de actualizar software para corregir vulnerabilidades (todos ellos principios presentes en NIST 800-41).
2. **Cumplimiento NIST SP 800-113:** El firewall y su componente VPN deberán alinearse con la “Guía de VPN SSL” de NIST SP 800-113. Esto implica proveer un acceso remoto seguro usando SSL/TLS con autenticación fuerte (como 2FA) tal como recomienda NIST, usar cifrados robustos aprobados (TLS 1.2/1.3, suites con PFS), proteger las credenciales y sesiones VPN, y ofrecer alta disponibilidad para servicios de acceso remoto críticos, siguiendo las mejores prácticas descritas en dicha guía.
3. **Cumplimiento ISO/IEC 27001:** La solución deberá ayudar a REDIMadrid a cumplir controles de la Norma ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información). En concreto, aportará a controles del Anexo A relacionados con seguridad de redes y comunicaciones (A.13), control de acceso (A.9) y gestión de incidentes (A.16). Por ejemplo, el firewall implementa controles de seguridad perimetral (A.13.1), permite segregación de redes (A.13.1.3), aplica políticas de control de acceso por usuario (A.9.1), y genera registros de eventos de seguridad para monitorización continuo (A.12.4), todos elementos que soportan la conformidad ISO 27001. Se valorará si el fabricante cuenta con certificación ISO 27001 para sus procesos de desarrollo y soporte.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

4. **Cumplimiento GDPR:** Si bien el Reglamento General de Protección de Datos (GDPR) de la UE se enfoca principalmente en datos personales, el firewall deberá aportar funcionalidades que ayuden a proteger dichos datos y a cumplir principios de privacidad por diseño. Por ejemplo:
 - a) **Cifrado/seguridad de los datos en tránsito:** mediante VPN y TLS se protege la confidencialidad de datos personales en comunicaciones.
 - b) **Registro de accesos:** deberá registrar accesos a sistemas que contengan datos personales, posibilitando detectar accesos no autorizados o brechas (obligación de informar brechas de seguridad).
 - c) **Minimización y retención:** deberá permitir configurar retención limitada de logs que contengan datos personales (ej. IPs asociables a personas), acorde a políticas de la empresa. También se valorará que soporte anonimización o filtrado de ciertos datos en los logs si se requiere por privacidad.
 - d) **Seguridad por defecto:** las políticas del firewall deberán poder configurarse para que, por defecto, bloqueen transferencias de datos personales hacia fuera salvo autorización (p. ej. bloquear servicios no aprobados de transferencia de archivos). En síntesis, el NGFW debe contribuir a una postura que facilite el cumplimiento de GDPR, ofreciendo medidas de seguridad técnicas robustas para proteger datos personales en las redes.
5. **Otras normativas y buenas prácticas:** Además de las anteriores, el firewall deberá alinearse con otros marcos reconocidos: por ejemplo, las recomendaciones del NIST Cybersecurity Framework (CSF) en la función Proteger (PR.PT-3: protección de comunicaciones de red), el estándar IEEE 802.1X si aplica para control de acceso, la norma IEC 62443 si se utiliza en entornos industriales, etc. (Estos no son requisitos explícitos para la licitación, pero demuestran un diseño conforme a las mejores prácticas de la industria).
6. **Certificación CCN-CERT:** Los equipos propuestos deberán estar certificados por el CCN-CERT, incluidos en el Catálogo CPSTIC en la categoría ENS ALTA, y contar con guías oficiales del CCN que describan su configuración y empleo seguro.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

3.10. Requisitos de Registro de Eventos y Monitorización

1. **Registro detallado de tráfico y amenazas:** El firewall deberá registrar en logs cada evento relevante de seguridad y de red, incluyendo al menos: conexiones bloqueadas por políticas (con detalle de regla aplicada), alertas de IPS (ataque detectado y bloqueado/permitido), sites/URLs bloqueados por filtrado, archivos malware detectados (y acción tomada), eventos de VPN (conexiones establecidas/terminadas), autenticaciones de usuarios (éxito o fallo) y cualquier otra incidencia de seguridad. Estos registros deben capturar detalles completos: “timestamp” con zona horaria, IP origen y destino, puertos/protocolos, nombre de la aplicación o firma detectada, usuario involucrado (si aplica), acción realizada por el firewall (permitir, bloquear, reconfigurar, etc.).
2. **Almacenamiento de logs localmente:** El dispositivo deberá contar con almacenamiento local suficiente para guardar logs históricamente, al menos a corto plazo. Por ejemplo, debería poder conservar localmente los eventos de los últimos 7 días a plena carga de eventos, para consulta rápida en caso de incidentes recientes sin depender de sistemas externos.
3. **Exportación de logs a servidor externo:** Adicional al almacenamiento local, deberá enviar todos los logs de forma confiable a sistemas externos de recolección (SIEM, syslog server central, etc.) para almacenamiento a largo plazo y correlación (requisito ya mencionado en integración SIEM). Debe garantizar la entrega segura de logs (por TCP, con opción de cifrado TLS para syslog). En caso de fallo de conexión al servidor de logs, el dispositivo deberá poder encolar temporalmente los eventos y reintentar envío, para no perder datos.
4. **Formato y estándar de logs:** Los logs deberán cumplir con formatos estándar (por ejemplo, syslog RFC 5424, con campos estructurados) o con esquemas fácilmente “parseables” (CSV, JSON). Cada evento debe identificarse claramente con un tipo/código de evento, severidad, etc., de modo que sea sencillo filtrarlos y analizarlos.
5. **Consola de monitorización en tiempo real:** La interfaz de administración deberá incluir una consola o dashboard de monitorización en tiempo real donde se puedan observar los eventos conforme ocurren. Por ejemplo, un visor de logs en vivo con actualización continua, gráficos de tráfico en tiempo real, top n (top

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

IP hablando, top aplicaciones, etc.). Esto permite al operador detectar actividad anómala instantáneamente.

6. **Alertas y notificaciones:** Deberá ser posible configurar alertas automáticas ante ciertos eventos críticos, de forma que notifiquen al personal de seguridad. Por ejemplo: detección de malware crítico, múltiples ataques IPS en poco tiempo, caída de enlace WAN, etc., deberían generar notificaciones vía correo electrónico, SNMP trap y/o integración con el SIEM que dispare un ticket. El sistema de logging/monitorización del firewall debe soportar esta creación de alertas con umbrales (por ejemplo, más de X eventos en Y minutos).
7. **Reportes periódicos:** La solución deberá ser capaz de generar informes (reports) ejecutivos o detallados sobre la actividad de la red y la seguridad. Por ejemplo: informe diario/semanal de uso de ancho de banda por aplicación, reporte de amenazas bloqueadas, cumplimiento de políticas (quién accedió a qué), etc. Estos informes deben poder programarse para enviarse automáticamente (en PDF/HTML) a correos designados, y personalizarse en rango de fechas y contenidos.
8. **Módulos de análisis avanzado:** Se valorará si el fabricante ofrece módulos adicionales de analítica de seguridad (por ejemplo, herramientas de análisis de logs con machine learning, detección de anomalías en logs, etc.) que se integren con el firewall. Aunque no es obligatorio, la existencia de un Security Analytics dedicado (on-premise o cloud) que procese los eventos del NGFW para encontrar patrones complejos sería un plus en la solución ofrecida.
9. **Sincronización horaria (NTP):** El dispositivo deberá soportar sincronización de reloj mediante NTP con servidores de tiempo confiables, de modo que todos los eventos registrados tengan “timestamps” precisos y consistentes con el resto de sistemas de REDIMadrid. Esto es crucial para correlación de eventos en el SIEM y auditorías forenses.
10. **Conservación de logs y capacidad:** El firewall deberá disponer de la capacidad de almacenamiento de logs en el equipo para aplicar buenas prácticas de rotación/retención de los mismos. El administrador deberá poder configurar políticas de retención (por ejemplo, “borrar logs locales mayores a 30 días”).
11. **Integridad de los logs:** Los registros de eventos deben resguardarse con integridad. Es decir, debe haber mecanismos para prevenir manipulación o borrado no

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

autorizado de logs (por ejemplo, que los administradores no puedan alterar el registro de auditoría). En lo posible, los logs enviados externamente deberían poder firmarse o al menos almacenarse en sistemas inmutables para garantizar su fiabilidad en caso de investigación.

3.11. Requisitos Físicos, Ambientales e Implementación

1. **Espacio y montaje:** El/los equipo/s deberá caber en los racks disponibles. Como se indicó, idealmente formato 1U cada equipo. Deberá incluir todos los accesorios de montaje necesarios. Se debe verificar que la profundidad del chasis es compatible con los racks estándar.
2. **Alimentación eléctrica:** Compatibilidad con la alimentación eléctrica local (por ejemplo, 220V AC en España) y frecuencia estándar. Las fuentes redundantes, si las hay, preferiblemente en tomas independientes.
3. **Indicadores y accesibilidad:** El dispositivo debe contar con indicadores LED claros para estado de alimentación, estado de alarma, actividad/enlace en cada puerto, etc., para facilitar revisión visual rápida. Los puertos de uso frecuente (consola, USB, gestión) deben ser fácilmente accesibles en el panel frontal.
4. **Cambio en caliente (hot-swap):** Se prefiere que componentes críticos sean modulares intercambiables en caliente, como las fuentes de poder o ventiladores, para poder reemplazarlos sin apagar el dispositivo. Esto minimiza el tiempo de inactividad en caso de fallos de hardware.
5. **Compatibilidad con cableado existente:** Los puertos ofrecidos (fibra SR/LR, cobre) deben ser compatibles con el cableado existente en las instalaciones. Cualquier requisito especial (p. ej. transceptores 100GE específicos) debe ser contemplado y provisto en la oferta para asegurar su funcionamiento (por ejemplo, si se ofrecen puertos SFP+, incluir transceptores compatibles con las fibras OM3 u OS2 – multimodo o monomodo - existentes).

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

3.12. Requisitos de Alta Disponibilidad y Continuidad

Para entornos críticos, el firewall deberá soportar configuración de alta disponibilidad (HA) que garantice la continuidad del servicio incluso si un dispositivo falla o requiere mantenimiento. Los requerimientos son:

1. **Alta Disponibilidad Activo-Pasivo:** El NGFW deberá soportar al menos un modo HA activo/pasivo donde un segundo aparato idéntico actúa como respaldo en espera (standby) y asume automáticamente la operación si el nodo activo falla. La conmutación (failover) debe ser transparente para las comunicaciones, manteniendo sesiones establecidas si es posible, o recuperándolas rápidamente en caso de interrupción.
2. **Sincronización de configuración y estado:** En modo HA, los dispositivos deberán sincronizar en tiempo real la configuración, las tablas de estado de conexiones, claves de cifrado (para VPN), contadores, etc., de modo que el equipo secundario esté listo para asumir el tráfico sin inconsistencias. Esta sincronización debe ocurrir por un enlace dedicado (heartbeat/HA link). Se describirán los requisitos de conectividad para la sincronización.
3. **Failover automático y manual:** El sistema HA deberá conmutar automáticamente ante detección de fallo (p.ej. ausencia de latido, interfaz caída, fallo de hardware/software). También se deberá poder forzar manualmente un failover (por ej., para pruebas o mantenimiento del activo).
4. **Retorno a principal (fallback):** Deberá soportarse el retorno automático o manual al nodo principal una vez recuperado, con mecanismos para evitar flapping (por ejemplo, tiempo de espera antes de reestablecer el rol activo). Se podrá configurar si el fallback es automático o requiere intervención del administrador.
5. **Múltiples modos HA:** Si el firewall soporta también modos de cluster activo-activo (balanceo de carga) o configuraciones de HA en grupo (más de 2 nodos), deberá indicarse.
6. **Monitor de enlaces y rutas:** La solución HA debe poder monitorizar tanto el estado de los chasis como la disponibilidad de enlaces de red cruciales (p. ej. enlace

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

WAN). Si el firewall activo pierde conectividad por fallo de un puerto o enlace crítico, debería poder disparar failover al secundario para aprovechar un enlace operativo. Esto asegura continuidad incluso en fallos de capa 1-2.

7. **Split-brain avoidance:** Deben existir mecanismos para evitar condiciones de split-brain (ambos nodos activos creyendo que el otro cayó). Por ejemplo, usando un segundo canal de monitorización o detectando actividad duplicada. Esto para prevenir que tanto activo como pasivo filtren tráfico simultáneamente causando problemas.
8. **Compatibilidad con HA a nivel de red:** El firewall en HA deberá integrarse bien con protocolos de redundancia de red externos (p. ej., si conecta a routers con VRRP/HSRP, switches con MC-LAG, etc.). Debe soportar, por ejemplo, MAC virtual o failover de IPs virtuales en sus interfaces para presentarse como una única puerta de enlace lógica ante la red. Estos detalles de integración se configurarán durante la implantación.

4. Escenario de valoración

El escenario propuesto para el despliegue de los nuevos NGFW se describe a continuación. Este escenario tiene como objetivo principal la integración de los NGFW en la red de gestión de MadQCI, ofreciendo un control seguro y eficiente para los usuarios que acceden a través de Internet, así como el control del acceso a la red de gestión proveniente de la UPM.

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

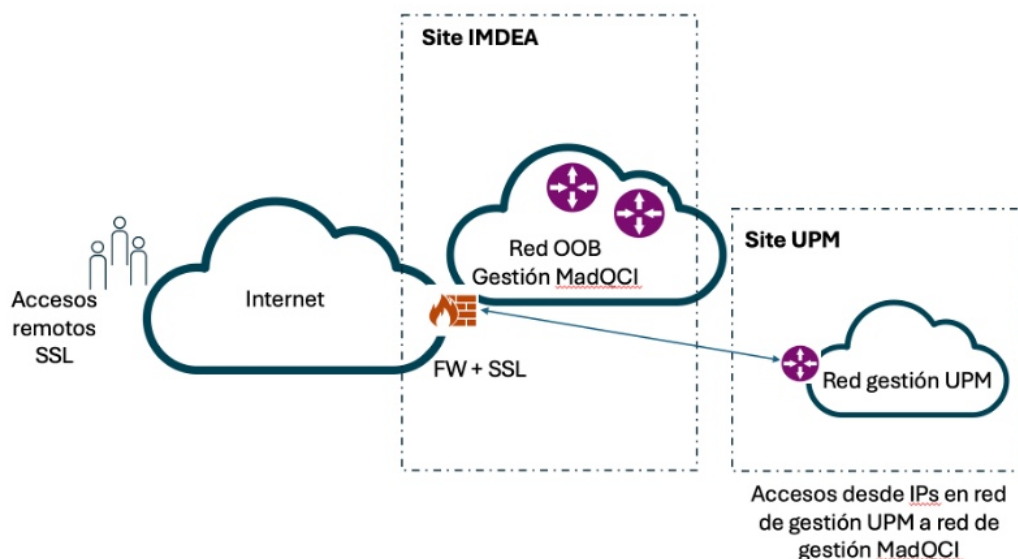


Figura 1: Esquema de escenario a valorar

En este contexto, el NGFW se establecerá como el punto de terminación para las conexiones SSL de los usuarios que provienen de Internet, gestionando y asegurando su acceso a la red de gestión de MadQCI. De manera simultánea, también se encargará de regular el acceso a esta misma red para los usuarios provenientes de la red de gestión de la UPM, garantizando una segmentación y control adecuado de ambos tipos de tráfico. El NGFW garantizará el acceso seguro para ambos orígenes de tráfico y una segmentación adecuada entre zonas externas e internas de MadQCI.

Se deberán cotizar todas las licencias necesarias para habilitar las funcionalidades demandadas en el escenario de valoración. El adjudicatario será responsable de garantizar que todas las funcionalidades descritas en el escenario de valoración quedan debidamente habilitadas, operativas y con soporte oficial del fabricante durante todo el período de vigencia de la contratación.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

Requisitos del NGFW

La solución propuesta debe cumplir con los siguientes requisitos para los NGFW, con el fin de garantizar el rendimiento, la seguridad y la escalabilidad necesarios para la operación y el crecimiento futuros de la infraestructura:

- **NGFW:** Se requiere dos dispositivos para una configuración de alta disponibilidad 1+1 en este caso. El/los equipo/s ha de contar con:
 - El/los NGFW debe contar con, al menos, 8 puertos 10GE SFP+ y 8 puertos GE SFP u 8 puertos 10GE/1GE SFP+/SFP.
 - El/los NGFW deberá disponer de fuentes AC de alimentación redundantes, es decir, al menos 2 PSU hot-swappable.
- **Funcionalidad Completa de los NGFW:** Los dispositivo debe ser capaz de ofrecer todas las funcionalidades de un NGFW de capa 7, incluyendo filtrado de tráfico, inspección profunda de paquetes y capacidades avanzadas de protección frente a amenazas.
- **Throughput de Firewall:** Cada NGFW debe ser capaz de manejar un mínimo de 19 Gbps para tráfico clásico de firewall (filtrado L3/L4), sin experimentar degradación en el rendimiento (pérdida de paquetes despreciable < 0.1 % y latencia añadida mínima).
- **Throughput de NGFW:** Debe soportar un throughput mínimo de 9 Gbps para tráfico inspeccionado como NGFW manteniendo sus mecanismos de detección de amenazas activos.
- **Rendimiento con Servicios UTM:** El dispositivo debe ser capaz de mantener un throughput de al menos 9 Gbps cuando se utilicen servicios Unified Threat Management (UTM) como antivirus, antispam, filtrado de contenido e IPS.
- **Sesiones Concurrentes:** El dispositivo debe ser capaz de manejar al menos 2 Millones sesiones concurrentes sin degradar su rendimiento ni agotar recursos de memoria.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

- **Nuevas Conexiones por Segundo:** Cada NGFW debe ser capaz de procesar un mínimo de 200.000 nuevas conexiones por segundo (CPS) en picos sostenidos.
- **Usuarios/VPN Concurrentes SSL:** Se debe permitir la conexión de al menos 1.500 usuarios simultáneos mediante VPN SSL sin degradar la experiencia de éstos (ancho de banda adecuado por usuario y baja latencia en sus comunicaciones).
- **Latencia adicional:** El objetivo es que la latencia adicional sea lo más baja posible; idealmente por debajo de unos pocos cientos de microsegundos en promedio para tráfico no cifrado a baja carga, y manteniéndose en el orden de milisegundos (1-5 ms) incluso bajo carga intensa o con inspección SSL.
- **Throughput de VPN SSL:** El throughput mínimo para VPN SSL debe ser de 3.5 Gbps para garantizar la transferencia segura de datos.
- **Rendimiento bajo carga mixta:** Cada NGFW habrá de mantener un rendimiento estable y cercano a los valores esperados en cada categoría (throughput, latencia, CPS, etc.) cuando todos estos tipos de tráfico ocurren a la vez.

El software y firmware del NGFW deberán estar actualizados a la última versión estable, con todas las licencias necesarias activadas para disponer de las prestaciones NGFW/UTM completas, aun así, en la fase de instalación, REDIMadrid decidirá en cual es la versión mas adecuada para instalar en los equipos NGFW.

Plataforma de Administración Centralizada

Se deberá proporcionar una plataforma de administración centralizada para gestionar de manera eficiente todos los dispositivos NGFW desplegados. Esta plataforma debe ser capaz de anticipar futuros despliegues y crecer conforme lo haga la infraestructura de seguridad. Además, esta plataforma de administración se instalará "on-premise", dentro de la infraestructura de virtualización de REDIMadrid, garantizando el control local y la integración con otros sistemas de gestión existentes.

Las características de esta plataforma están indicadas en el apartado [4.3](#)

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

Autenticación de Usuarios Remotos

La autenticación de los usuarios remotos se realizará mediante el protocolo TLSv1.3, con la integración de un sistema de autenticación centralizado que permita validar el acceso de los usuarios de forma segura. Adicionalmente, se requerirá la implementación de autenticación de doble factor (2FA) para fortalecer la seguridad del acceso remoto y garantizar que solo los usuarios autorizados puedan acceder a la red.

El firewall deberá realizar una verificación del dispositivo accediendo sobre la VPN SSL antes de otorgar acceso a recursos, así como de forma periódica durante la sesión (re-evaluación por intervalo y ante cambios de red/estado)

Las necesidades de autenticación se indican en el apartado [3.6](#)

Servicios Profesionales

El proveedor deberá ofrecer un conjunto integral de servicios profesionales con el fin de asegurar una implementación exitosa de la solución, así como garantizar su funcionamiento óptimo durante su ciclo de vida útil. Estos servicios deben ser completamente detallados y alineados con los requisitos establecidos en las diferentes fases del proyecto, asegurando que todas las necesidades del cliente sean cubiertas de forma eficiente y eficaz. A continuación, se especifican los servicios que deben ser proporcionados:

- **Mantenimiento y Soporte del Fabricante:** El proveedor deberá ofrecer un servicio de mantenimiento y soporte técnico que se ajuste a lo establecido en el apartado [5](#). Este soporte debe incluir actualizaciones periódicas de software, corrección de errores y asistencia ante cualquier tipo de incidencia que pueda surgir, garantizando la operatividad de la solución durante todo su ciclo de vida.
- **Diseño de la Solución y Elaboración de Planes de Pruebas y Despliegue:** El proveedor debe encargarse del diseño completo de la solución, teniendo en cuenta las necesidades específicas del cliente y el entorno en el que se implementará. Además, deberá elaborar un plan detallado de pruebas y despliegue, siguiendo el escenario planteado previamente. Este plan debe contemplar todas las fases del

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

proyecto, asegurando que la implementación se realice de manera ordenada y sin contratiempos.

- **Instalación Física del Equipamiento:** De acuerdo con lo establecido en el apartado 4.2, el proveedor será responsable de la instalación física de todo el equipamiento necesario para la implementación de la solución. Esto incluye la disposición adecuada de los dispositivos en los racks, el cableado necesario, la verificación del estado de los componentes y la validación de que todo el equipamiento esté correctamente conectado y en funcionamiento.
- **Configuración del Servicio de Acceso Remoto:** Se deberá configurar el servicio de acceso remoto para usuarios mediante las modalidades web y túnel VPN. Esta configuración permitirá a los usuarios remotos acceder de manera segura a los recursos de la red. Además, se deberán configurar hasta seis roles de acceso distintos, que servirán como modelo para futuros despliegues. Cada rol deberá ser personalizado según las necesidades de los diferentes tipos de usuarios y los niveles de acceso que requieren.
- **Documentación Completa de los Trabajos Realizados:** El proveedor deberá entregar toda la documentación relacionada con los trabajos realizados durante el despliegue de la solución. Esto incluirá los documentos de diseño (HLD) y los documentos de detalles de la solución (LLD), conforme a lo especificado en el apartado 4.2. La documentación debe ser detallada, clara y fácil de entender, para que el equipo de administración del cliente pueda gestionar y operar la solución de manera eficaz.
- **Bolsa de Horas Adicionales para Resolución de Dudas y Despliegue de Funcionalidades Adicionales:** De acuerdo con lo indicado en el apartado 4.4, el proveedor deberá ofrecer una bolsa de horas adicionales que el cliente podrá utilizar para resolver dudas adicionales que surjan después de la implementación, así como para el despliegue de funcionalidades adicionales según lo requerido. Estas horas deben ser flexibles y proporcionarse de manera oportuna cuando el cliente lo necesite.
- **Formación:** De acuerdo con lo establecido en el apartado 6, el proveedor deberá ofrecer formación a los técnicos y personal designado por el cliente. Esta formación debe estar orientada a garantizar que el personal esté capacitado para administrar,

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

operar y dar soporte a la solución una vez que haya sido implementada. La formación debe incluir tanto aspectos técnicos como operacionales, con el fin de cubrir todas las áreas necesarias para el uso efectivo de la solución.

4.1. Scaling equipos, PONERLO COMO JUICIO DE VALOR

Los equipos deben contar con la capacidad de escalabilidad, permitiendo ampliar su rendimiento y funcionalidades tanto con la licencia ofertada como, en caso de ser necesario, mediante la adquisición de licencias superiores no incluidas en la oferta inicial.

Esta capacidad de escalamiento debe garantizar que el sistema pueda adaptarse a futuras necesidades operativas sin requerir el reemplazo del hardware, permitiendo así una mayor flexibilidad y optimización de la inversión. Además, se deberá especificar claramente los niveles de ampliación disponibles y los requisitos asociados a cada uno de ellos.

-
1. **Escalabilidad vertical:** Se indicará si el NGFW cuenta con capacidades de ampliación o upgrades (por ejemplo, licencias o módulos adicionales) para aumentar throughput, sesiones o funcionalidades en el futuro, en caso de crecimiento de la demanda más allá de los mínimos establecidos.
 3. Interfaz de 100 Gigabit Ethernet: Se indicará si el NGFW cuenta con la opción de interfaces 100GE
 2. **Procesamiento en una sola pasada (single-pass):** Es deseable que la arquitectura interna aplique las múltiples inspecciones de seguridad de forma eficiente, evitando procesar múltiples veces el mismo flujo de datos. El proveedor deberá describir cómo su arquitectura maneja estas inspecciones múltiples de forma óptima.
 3. **Portal de autoservicio:** Se indicará si está disponible la integración con un portal de usuario donde los empleados puedan, por ejemplo, descargar el cliente VPN, ver sus sesiones activas, o administrar métodos 2FA (registrar tokens). Si está disponible el mismo, el firewall deberá integrarse con dicho portal seguro.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

4. **Certificaciones de producto:** Certificaciones de producto: (Requisito deseable) Se valorará fuertemente que el producto NGFW propuesto cuente con certificaciones de seguridad reconocidas, tales como Common Criteria EAL4+ (perfil de protección para firewall de red) o equivalentes, y certificación de módulo criptográfico FIPS 140-2/140-3 para sus componentes de cifrado. Tales certificaciones independientes brindan garantía adicional de que la solución ha sido evaluada según estándares estrictos de seguridad.
5. **Disipación térmica:** Deberá indicar la disipación de calor/BTU del equipo a carga máxima, para asegurar que la sala de servidores puede evacuar el calor generado. El/los equipo/s debe operar en el rango de temperatura ambiente típico de un CPD (ej. 0°C a 40°C) y humedad relativa estándar (10-85 % sin condensación). y Consumo máximo indicado para dimensionar UPS/SAIs (se debe proveer el dato de consumo en Watts).
6. **Ruido:** Si el firewall se instala en entorno de oficina, se valorará que tenga niveles de ruido bajos (dB) o modos de operación silenciosos; aunque si está en sala de servidores, esto es menos crítico. En cualquier caso, los ventiladores deben ser de velocidad variable según temperatura para optimizar la acústica y la vida útil.
7. **Documentación de instalación:** El proveedor deberá suministrar manuales de instalación físicos o digitales, y guías de rápido inicio (quick start) para facilitar el despliegue inicial. Se espera que en la propuesta se describa claramente el plan de instalación y configuración inicial que garantice una transición sin sobresaltos desde la infraestructura existente (si aplica).
8. **Licenciamiento para HA:** Se indicará si son necesarias licencias de software o suscripción necesaria para que ambos nodos en HA tengan las mismas funcionalidades.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

4.2. Instalación, configuración y puesta en marcha

Se requiere que el adjudicatario realice la entrega, instalación y configuración, de acuerdo a lo indicado en el apartado 4. El equipamiento deberá estar operativo en el lugar en el que debe realizarse la entrega, en este caso, en el PdP de IMDEA Software sito en Madrid (Pozuelo de Alarcón).

Para llevar a cabo la instalación de manera eficiente y sin contratiempos, es fundamental realizar un replanteo previo detallado. Este proceso debe incluir un análisis exhaustivo del entorno de instalación, considerando la disposición de los equipos, la accesibilidad a los puntos de conexión y la correcta distribución del cableado.

Además, se deberá contemplar la provisión e instalación de todo el cableado necesario, incluyendo tanto el cableado estructurado de datos como el cableado de potencia. Esto implica la planificación y disposición de los latiguillos de red, los patch cords, las canalizaciones adecuadas para la correcta organización de los cables y la identificación de cada uno de los segmentos de conexión.

- El/los equipo/s tiene que configurarse para tener capacidad de configurar de acuerdo a lo especificado en el apartado 4.
- Los SFPs que se deben ofertar son los necesarios para poner en servicio el escenario indicado en el apartado 4.
- Todo el hardware suministrado debe ser nuevo del fabricante, no podría ofertarse hardware refurbished o hardware compatible.
- La versión del sistema operativo que se instala en los equipos será la mas actualizada y estable que exista en el momento del suministro, la cual implementará todas las funcionalidades especificadas en el presente pliego. También se incluirán todas aquellas licencias que fueran necesarias para utilizar dichas funcionalidades. Esta versión será siempre consensuada con el personal de REDIMadrid, el cual decidirá en todo momento que versión sera finalmente instalada.
- El adjudicatario debe comprobar el correcto funcionamiento de todos los elementos objeto del suministro. El adjudicatario elaborará un informe mostrando la sa-

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

lida de los comandos adecuados que verifiquen el correcto funcionamiento del hardware antes de realizar la entrega a REDIMadrid.

- El adjudicatario estará obligado a proporcionar documentación técnica completa y detallada sobre la solución implementada. En concreto, deberá entregar los siguientes documentos:
 - **HLD (High-Level Design):** Un documento de diseño de alto nivel que describa la arquitectura general de la solución, incluyendo su estructura, componentes principales, esquemas de interconexión, flujos de comunicación y justificación técnica de las decisiones adoptadas. Este documento deberá ofrecer una visión global de cómo se integra la solución dentro del entorno existente y cómo cumple con los requisitos funcionales y operativos del proyecto.
 - **LLD (Low-Level Design):** Un documento de diseño de bajo nivel que proporcione información técnica detallada sobre la configuración, parametrización y especificaciones precisas de la solución implementada. Este incluirá diagramas de red, configuraciones de hardware y software, procedimientos de implementación, políticas de seguridad aplicadas y cualquier otra información relevante para garantizar la correcta operación, mantenimiento y escalabilidad del sistema.

Ambos documentos deberán entregarse en un formato estructurado y claro, permitiendo su fácil interpretación y utilización tanto para la gestión técnica del sistema como para futuras ampliaciones o modificaciones.

- el tipo de alimentación eléctrico del equipamiento suministrado será AC 220v-50Hz.
- Se requiere que pueda instalarse en un rack o bastidor estándar típicamente de 19 pulgadas.

4.3. Requisitos para el Gestor del equipamiento de seguridad

REQUISITOS DE ADMINISTRACIÓN Y GESTIÓN CENTRALIZADA

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

1. **Interfaz gráfica de administración (GUI):** Deberá proveer una interfaz web gráfica (HTTPS) para la administración del firewall, accesible vía navegador. La GUI debe ser intuitiva, mostrando paneles de estado, estadísticas de tráfico, alertas, etc., y permitiendo configurar todas las funciones (reglas, VPN, usuarios, etc.) con controles granulares. Debe soportar conexiones seguras (HTTPS/TLS) y ser accesible tanto por el puerto de gestión dedicado como, opcionalmente, por una interfaz de datos específica (según se configure).
2. **Interfaz de línea de comandos (CLI):** Además de la GUI, deberá contar con una CLI accesible por consola serie o SSH para administración avanzada o automatizada. La CLI debe permitir configurar todas (o la mayoría) de las funcionalidades, ejecutar diagnósticos y scripts. Es importante que el personal técnico pueda administrar el equipo vía CLI como alternativa, especialmente para scripting de configuraciones repetitivas o “troubleshooting” detallado.
3. **Gestión centralizada multi-dispositivo:** Si en el futuro REDIMadrid despliega múltiples firewalls (por ejemplo, en distintas sedes), deberá existir una plataforma de administración centralizada que permita gestionar todos los dispositivos de forma unificada. Esta plataforma podrá ser un software “on-premise” instalado en servidor propio proporcionada por el fabricante o una solución en VM de acuerdo al punto 4.3, y deberá posibilitar:
 - a) Administración de la configuración de múltiples NGFW desde una consola única.
 - b) Gestión de políticas globales: definir objetos, reglas o perfiles reutilizables y aplicarlos a múltiples firewalls para consistencia.
 - c) Distribución de cambios masivos: por ejemplo, agregar una regla y propagarla a todos los firewalls del grupo.
 - d) Visualización central de alertas y eventos de todos los dispositivos (ver sección 10 de registros).
4. **Capacidad de gestionar mínimo 50 dispositivos:** La plataforma centralizada (en caso de ser requerida) deberá escalar para soportar al menos 10 firewalls bajo su gestión, dado que REDIMadrid podría extender la solución a muchas sucursales u oficinas. Debe manejar jerarquías o agrupaciones (p. ej. políticas por región) para facilitar esta escala.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

5. **Roles y perfiles administrativos:** La solución de administración centralizada (y local) deberá soportar Control de Acceso Basado en Roles (RBAC) para la administración (como se mencionó en requisitos de autenticación). Podrá crearse usuarios administradores con distintos privilegios: p. ej., un operador que solo monitorea no podrá cambiar configuraciones; un administrador de red puede manejar reglas de firewall pero no tocar configuración global del sistema, etc. Esto permite delegar tareas sin exponer toda la configuración a todos los administradores.
6. **Registro de auditoría de cambios:** Es indispensable que cualquier cambio de configuración realizado por un administrador quede registrado en un log de auditoría indicando qué usuario realizó qué cambio y cuándo. Esto tanto en la administración local como en la central. Así se puede trazar históricamente modificaciones (cumpliendo también normativas como ISO 27001 y PCI en cambios controlados). Idealmente, la interfaz debería mostrar un historial de cambios e incluso permitir comparar configuraciones o revertir cambios recientes fácilmente (versionado de configuración).
7. **Administración de firmware y actualizaciones:** La herramienta de gestión debe facilitar la actualización de firmware de los dispositivos de forma controlada. Por ejemplo, poder cargar una nueva versión de software del firewall y programar su instalación en mantenimiento. También, gestionar las licencias y suscripciones de servicios (IPS, URL Filtering, soporte) de forma centralizada, mostrando expiraciones, facilitando renovaciones, etc.
8. **Acceso remoto seguro a la administración:** Deberá ser posible administrar el firewall de forma remota a través de Internet con seguridad. Para ello, se podrá hacer vía VPN (preferido) o habilitando acceso a la GUI/SSH por Internet a IPs específicas. En cualquier caso, el dispositivo debe soportar medidas de protección como restricción de IP origen, uso obligatorio de HTTPS/SSH, timeout de sesión y 2FA para administradores remotos.
9. **Usabilidad y ayudas:** La interfaz deberá contar con documentación/ayuda en línea para parámetros, mensajes de error claros, y plantillas o asistentes para las configuraciones comunes (wizards), de modo que reducir errores de configuración. Aunque esto es difícil de medir objetivamente, se valorará la ergonomía de la solución durante la evaluación (p. ej., creando una regla nueva paso a paso).

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

10. **Sistema operativo embebido y arranque dual:** El NGFW deberá operar con un sistema operativo dedicado en memoria. Deberá soportar arranque dual, manteniendo al menos dos versiones de firmware almacenadas para permitir revertir fácilmente a la versión previa en caso de fallo en una actualización, aumentando la resiliencia del sistema.
11. **Recuperación y respaldo de configuración:** Deberá facilitar la exportación e importación de la configuración del dispositivo. Esto incluye la posibilidad de guardar/restaurar la configuración vía GUI y CLI, ya sea al PC local, a un almacenamiento USB o a un servidor remoto (FTP/TFTP), en formatos legibles (texto plano o formatos estructurados como YAML/JSON).

ADMINISTRACIÓN Y GESTIÓN

- **Gestión Centralizada:** Administración unificada de políticas de seguridad, configuraciones y actualizaciones.
- **Gestión de Configuraciones:**
 - Creación, modificación y eliminación de reglas de firewall.
 - Uso de plantillas para replicar configuraciones.
 - Gestión centralizada de objetos y direcciones IP.
- **Control de Cambios y Versionado:**
 - Auditoría de cambios en la configuración.
 - Capacidad de revertir configuraciones previas en caso de fallo.
- **Administración Basada en Roles (RBAC):** Acceso diferenciado según perfil del usuario.

POLÍTICAS DE SEGURIDAD

- **Gestión de Políticas Globales:** Aplicación de políticas a múltiples dispositivos.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

- **Análisis de Políticas:** Herramientas de optimización y eliminación de reglas redundantes.
- **Segmentación de Red y Control de Aplicaciones:** Definición de reglas basadas en usuarios, aplicaciones y direcciones IP.

MONITOREO Y VISIBILIDAD

- **Panel de Control Centralizado:** Dashboard con métricas en tiempo real.
- **Registro y Auditoría:**
 - Registro centralizado de logs de tráfico y seguridad.
 - Exportación de logs a sistemas SIEM externos.
- **Alertas y Notificaciones:**
 - Notificación de eventos críticos.
 - Soporte para alertas por email, SNMP y Syslog.

AUTOMATIZACIÓN Y ORQUESTACIÓN

- **APIs de Integración:** Soporte para REST API y automatización con Ansible o Terraform.
- **Gestión Basada en Políticas Dinámicas:** Adaptación automática de reglas según cambios en la red.
- **Compatibilidad con Threat Intelligence:** Integración con plataformas de inteligencia de amenazas.

SEGURIDAD Y CUMPLIMIENTO

- **Cifrado de Comunicaciones:** Uso de TLS para comunicación segura.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

- **Cumplimiento de Normativas:** Soporte para GDPR, ISO 27001, PCI-DSS, NIST, etc.
- **Autenticación Multi-Factor (MFA):** Seguridad adicional para administradores.

BACKUP Y RECUPERACIÓN

- **Backups Programados:** Respaldo automático de configuraciones.
- **Planes de Recuperación:** Procedimientos de restauración ante fallos o ataques.

INSTALACIÓN Y LICENCIAS:

- Se deben suministrar sin coste adicional, todas las licencias necesarias para el correcto funcionamiento del sistema de gestión en los términos descritos en el presente procedimiento de licitación, estas tienen que ser sin fecha de finalización, es decir, tienen que ser licencias ilimitadas en tiempo.
- El software de gestión podrá ser instalado en hardware dedicado (1), o en hardware virtualizado(2).

(1) En caso de que el adjudicatario opte por la primera opción (1):

- Se debe incluir el servidor o servidores con todas las características técnicas necesarias para el correcto funcionamiento del sistema de gestión. Se debe incluir el sistema operativo y todas las licencias necesarias para estos servidores.
- El adjudicatario se encargará de realizar la instalación y la total configuración del sistema de gestión y del sistema operativo de los servidores para lo cual deberá comunicar previamente las necesidades de recursos al personal de REDIMadrid.

(2) En caso de que el adjudicatario opte por la segunda opción (2) las características que están disponibles actualmente en REDIMadrid y por tanto las que debe cumplir la plataforma para su uso correcto, son las siguientes:

- 32GB RAM.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

- 16 Core vCPU.
- KVM hypervisor.
- HDD 500GB.

4.4. Bolsa de horas

El proveedor deberá ofrecer una bolsa de horas adicionales que el cliente podrá utilizar para resolver cualquier duda técnica o operativa que pueda surgir después de la implementación de la solución, así como para el despliegue de funcionalidades adicionales que no estén contempladas inicialmente en el alcance del proyecto. La finalidad de esta bolsa es garantizar que el cliente pueda recibir asistencia continua y soporte adicional conforme se vayan presentando nuevas necesidades o desafíos tras la puesta en marcha del sistema.

En total, se deberán ofrecer 120 horas adicionales, las cuales podrán ser utilizadas a lo largo del periodo de soporte especificado en el apartado 5, o bien, si el licitador ofrece un periodo superior, estas horas podrán extenderse durante ese tiempo adicional.

Estas horas adicionales deben tener las siguientes características:

- **Flexibilidad:** Se podrán utilizar estas horas de manera flexible, en función de sus necesidades y prioridades, sin estar limitado a un número fijo de incidencias o tareas específicas.
- **Operativa bolsa:** La bolsa de horas deben ser proporcionadas de manera oportuna, de acuerdo a lo indicado en el apartado 4.4.1. El licitador deberá garantizar la disponibilidad de técnicos cualificados para atender cualquier incidencia o requerimiento dentro de un tiempo razonable.
- **Resolución de Dudas Técnicas:** Estas horas podrán ser utilizadas para resolver dudas que surjan sobre la solución implementada, su configuración o cualquier otro aspecto relacionado con su operación.
- **Despliegue de Funcionalidades Adicionales:** Si REDIMadrid necesita implementar nuevas funcionalidades o realizar modificaciones en la solución existente, podrá uti-

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

lizar las horas de la bolsa para la configuración e implementación de estas funcionalidades adicionales. El alcance de estas funcionalidades será acordado entre el cliente y el proveedor antes de su ejecución.

- **Informe de Uso de Horas:** El licitador deberá ofrecer un informe detallado sobre el uso de la bolsa de horas, especificando las tareas realizadas y el tiempo consumido, para garantizar la transparencia y el seguimiento adecuado por parte del cliente.

4.4.1. Operativa en la solicitud de la bolsa de horas

La solicitud para la prestación de la bolsa de horas se realizará con una antelación mínima de **3 días laborables**, con el fin de asegurar una adecuada planificación y asignación de los recursos necesarios para atender la solicitud de manera eficiente.

En situaciones de urgencia, cuando el requerimiento sea de carácter prioritario o necesite una atención más inmediata, el plazo de antelación se podrá reducir a **1 día laborable**. Sin embargo, se deberá garantizar que, a pesar de la reducción en el tiempo de solicitud, se mantenga la misma calidad en la ejecución del servicio, priorizando la rapidez sin comprometer el cumplimiento de los estándares acordados.

En ambos casos, el licitador deberá notificar a REDIMadrid dentro del plazo indicado para asegurar que el servicio pueda ser proporcionado dentro del tiempo requerido. Además, el licitador se compromete a hacer todo lo posible por cumplir con las solicitudes urgentes, manteniendo la flexibilidad necesaria para responder a situaciones imprevistas sin afectar la operación del cliente.

5. Soporte

Se requiere que el adjudicatario preste un servicio de Garantía para todos los componentes objeto del Suministro, además de los usados para la instalación del equipamiento.

El servicio de garantía tendrá una duración de, al menos, de **1 año** en modo NBD (Next Business Day), teniendo en cuenta que siempre se tiene que ofertar la garantía

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

para que el fin del soporte este sincronizada para que termine el 31/12 del año siguiente a la publicación de la petición de ofertas, además hay que tener en cuenta que el soporte en ningún caso entrara en servicio antes de la instalación del equipamiento.

Ejemplo aclaratorio:

- Fecha límite de presentación de ofertas 20/10/2025
- Instalación de equipamiento, por tanto, entrada en mantenimiento de los equipos 15/09/2025
- Garantía que se debe ofertar: desde 20/11/2025 hasta el 31/12/2026.

También esta incluida en el servicio de garantía la actualización de software de los equipamientos ofertados, al menos, una vez al año, incluida la actualización de los gestores, en caso de que estén ofertados.

El ámbito de responsabilidad de la garantía del adjudicatario incluirá toda aquella electrónica de comunicaciones, elementos para el acondicionamiento, componentes, materiales, elementos pasivos etc., que se haya suministrado como parte del contrato.

Este Suministro se va a integrar en una infraestructura de red en producción que tiene en vigencia un servicio de garantía prestado por un integrador concreto. Con objeto de que el funcionamiento global de toda la infraestructura de red sea óptimo, eficiente y su operatividad se vea como un conjunto perfectamente armonizado, es decir, que no existan conflictos, problemas o malentendidos entre los servicios de garantía (entre el existente y aquel objeto de este pliego), se requiere del adjudicatario una adaptación y dotación de flexibilidad en el servicio para lograr una perfecta coordinación. La coordinación del servicio de garantía es responsabilidad del adjudicatario, y se hará siempre bajo la supervisión y guía de IMDEA Software. Este servicio de garantía se prestará siguiendo los procedimientos que actualmente están en operación para el resto de la red.

El licitador deberá proporcionar al personal de REDIMadrid una cuenta de usuario para acceder a la web del fabricante, para poder hacer un seguimiento de los casos abiertos, abrir casos, consultas técnicas, acceder a documentación privada, así como obtener parches y actualizaciones o cualquiera de las nuevas versiones de software liberadas por el fabricante.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

El alcance del servicio de garantía incluye a todos los componentes objeto del Suministro y consiste en:

- Un conjunto de actuaciones correctivas, preventivas así como informativas. En concreto, se incluirán como mínimo las siguientes actuaciones, sin perjuicio de aquellas otras que el adjudicatario proponga:
 1. La gestión y resolución de las incidencias, hardware y software, que puedan surgir en los componentes objeto del Suministro
 2. Actuaciones correctivas donde se incluye la reposición e instalación de dichos componentes o piezas modulares que forman parte de estos componentes.
 3. Intervenciones programadas.
 4. Generación de informes.
 5. Soporte técnico.
- La garantía debe cubrir los siguientes niveles:
 - **Nivel 1/Tier 1:** Este es el nivel de soporte inicial, que cubre la responsabilidad de las incidencias básicas. El Nivel 1 recibirá alarmas que se enviarán desde los sistemas de gestión y se tendrán que tratar. Se realizará un trabajo proactivo de las incidencias también a través del sistema de monitorización.
 - **Nivel 2/Tier 2:** Soporte técnico teniendo en cuenta áreas del conocimiento más especializadas en la incidencia. De esta manera, el soporte de segundo nivel lo deben realizar personas especializadas en equipos de routing y expertas en soluciones de Service Provider, y que han de ser responsables de personarse físicamente en un PdP para solucionar un problema de Nivel 2 y/o de Nivel 3 con la ayuda del fabricante. También son responsables de realizar cambios de hardware si fuera necesario.
 - **Nivel 3/Tier 3:** Soporte técnico del fabricante, en el que se escalará la incidencia a Nivel 3 (fabricante) desde el Nivel 2. Los técnicos asignados a este nivel son expertos y serán responsables, no solo de ayudar al personal de los otros niveles 1 y 2, sino también para la investigación y el desarrollo de soluciones a los problemas nuevos o desconocidos teniendo en cuenta áreas del conocimiento más especializadas y conocimientos internos de fabricante.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

- La empresa adjudicataria establecerá un servicio de monitorización, recepción de alarmas y recepción de llamadas de incidencias 24x7x365 con su consiguiente procesamiento según los tiempos establecidos en la sección 5. Este centro de gestión de incidencias de red debe estar accesible por REDIMadrid al menos un 99,9 % del tiempo a través de teléfono con atención en castellano.
- El soporte Nivel 1 y Nivel 2 debe ofrecerse en idioma **Español**.
- Todas las necesidades y prestaciones que se requieren para la garantía especificada en este apartado deben ser proporcionadas directamente por el adjudicatario del contrato, entendiendo que el soporte de alto nivel (Nivel 3) se contratará directamente al fabricante original del hardware, permitiendo también que el soporte de Nivel 2 se contrate al fabricante original del hardware, en relación a lo anterior no se permite que el licitador contrate a otro integrador de los equipos licitados para realizar la garantía. A estos efectos, el adjudicatario tiene la responsabilidad de ser garante y responder de la correcta ejecución de la garantía por parte del fabricante, satisfaciendo los requisitos del presente documento, dado que su función es en algunos casos la de contratar el servicio de Nivel 3 con el fabricante con la garantía de calidad requerida y en otros traspasar el soporte de Nivel 2/3 al fabricante del hardware.
- IMDEA Software tendrá acceso directo, 24 horas al día, todos los días del año, al centro de soporte de los fabricantes de los componentes objeto del Suministro, vía teléfono, correo electrónico y herramienta o aplicación web de soporte al cliente, si existiera. IMDEA Software también tendrá acceso directo a la herramienta de ticketing para gestión de incidencias que tenga el fabricante, con objeto de poder abrir incidencias directamente o hacer seguimiento de aquellas que hubiera podido abrir directamente el adjudicatario. Con estos accesos, Red.es podrá realizar consultas técnicas, abrir incidencias, hacer seguimiento de incidencias que hubieran sido abiertas por el adjudicatario, acceder a documentación privada, así como obtener parches y actualizaciones o cualquiera de las nuevas versiones software liberadas por el fabricante que puedan ser cargadas y puestas en operación en los equipos.
- El adjudicatario proporcionará soporte técnico, cuando sea requerido por REDIMadrid, sobre el funcionamiento, operación y configuración (incluidas todas las funcionalidades soportadas en las versiones de software actuales y en aquellas

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

nuevas que pudieran ser instaladas durante la ejecución del contrato) de los componentes objeto del Suministro, así como para el análisis y gestión de cualquier anomalía.

- El licitador debe ser **partner o socio oficial de la máxima categoría** del fabricante del equipamiento suministrado para el equipamiento indicado en el punto 3. No obstante, también se permitirá la participación de partners con una categoría un paso inferior, siempre que acrediten que la oferta presentada cuenta con la adscripción de un técnico que posea la certificación más alta otorgada por el fabricante en el training de seguridad. del fabricante del equipamiento suministrado para el equipamiento indicado en el punto 3.
- Se considera incidencia a:
 - cualquier situación que suponga la interrupción o degradación de cualquiera de los servicios configurados y/o soportados por los componentes objeto del Suministro.
 - cualquier situación que suponga que alguna de las funcionalidades del equipo, aun cuando no afecte a los servicios configurados, no opere con total normalidad, esté degradada o interrumpida.
 - cualquier situación que suponga que la gestión del equipo no es viable o está degradada o no funciona con total normalidad.
 - cualquier situación que suponga que el sistema de alimentación eléctrica (rectificador y/o baterías) de los equipos ópticos en cualquiera de los Puntos de Presencia de no funciona con total normalidad.
- El adjudicatario deberá disponer del stock necesario para cumplir estos tiempos de respuesta. REDIMadrid se reserva el derecho de auditar dicho stock.
- Se entiende por Tiempo Máximo de Reposición de Hardware (TMRH) aquel que transcurre entre el momento en que el fabricante determina que hay que sustituir un elemento hardware y el momento en que llega al destino indicado en la gestión de la sustitución. El TMRH que se solicita en el presente contrato es de NBD (Next Business Day).
- Las incidencias se clasifican en tres tipos, en función de su severidad. El nivel de severidad de una incidencia será asignado y/o modificado por REDIMadrid. En

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

el momento de abrir una incidencia REDIMadrid asignará el nivel de severidad. Si la incidencia hubiera sido abierta por el adjudicatario, el nivel de severidad inicial podrá ser modificado por REDIMadrid. El adjudicatario solo podrá modificarlo para elevar la severidad. El adjudicatario necesitará el visto bueno de REDIMadrid para disminuir la severidad de una incidencia.

Nivel de severidad	Descripción	Tiempo de resolución *
Alto	Problemas que impiden o degradan el funcionamiento de todos o parte de los servicios o funcionalidades configurados en cualquiera de los equipos.	6 horas laborales/NBD para cambio hardware
Medio	Problemas que no afectan al funcionamiento de los servicios o funcionalidades configuradas	Dos días laborales
Bajo	Requerimientos de información y clarificación sobre aspectos técnicos relacionados con el funcionamiento operación y configuración de equipos	Cinco días laborales

Según esta clasificación, para cada nivel de severidad se requiere un tiempo de respuesta máximo en el que un técnico cualificado atenderá la incidencia:

Nivel de severidad	Tiempo de respuesta (incluido en el tiempo de resolución)
Alto	15 minutos
Medio	2 horas
Bajo	24 horas

*En el caso que se identifique como posible solución de la incidencia el reemplazo o sustitución hardware, el Tiempo de Resolución no forma parte del Tiempo de Total de la incidencia. No es así en el caso del Tiempo de Respuesta que si se incluye en el Tiempo de Resolución, así por ejemplo en un caso de severidad alta ocurrida en un PdP con Tiempo Máximo de Reposición de Hardware (TMRH) de NBD, el plazo máximo para corregir el fallo sería de 10 horas laborales, donde 6 horas laborales corresponden a la fase de análisis de la incidencia (o Tiempo de Resolución) y 4 horas corresponden al plazo máximo para realizar una correcta sustitución hardware el siguiente día laboral.

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

El horario de atención de los diferentes niveles de mantenimiento debe ser el siguiente:

Nivel de mantenimiento	Horario de atención
Atención de incidencias L1	24x7
Soporte L2	8x5 laborables
Soporte L3	8x5 laborales
Sustitución de repuestos on site	NBD

- Se define como tiempo total de una incidencia el comprendido entre el momento en que un problema se origina y el momento de su resolución, y por tanto, están incluidos en dicho periodo el tiempo de resolución y el tiempo de reposición de hardware, que son independientes entre sí, en caso que fuera necesaria dicha reposición para resolver la incidencia.
- El plazo se inicia cuando el centro de soporte del fabricante o del adjudicatario (lo que antes ocurra) identifiquen la sustitución del hardware como solución de la incidencia. El reloj que contabiliza el tiempo o plazo máximo para realizar la sustitución no se detiene hasta que el hardware no haya sido correctamente reemplazado. Así, por ejemplo, podrían ser necesarias actualizaciones del sistema operativo para que el nuevo hardware fuera reconocido o bien para que las features configuradas recuperaran la operatividad. La ejecución de estas tareas, y otras que fueran necesarias para la correcta operatividad del hardware en el conjunto de la red, quedan incluidas en el plazo máximo de reposición o sustitución.
- se mantendrá informado a REDIMadrid en todo momento y de manera detallada de cualquier acción a tomar para la resolución de la incidencia.
- Siempre que el adjudicatario gestione una incidencia de forma directa con el centro de soporte del fabricante, REDIMadrid estará siempre en copia de todos los mensajes intercambiados o mensajes de actualización en el seguimiento de la incidencia a través de la herramienta de ticketing que para este objeto tenía el fabricante.
- El adjudicatario mantendrá informado regularmente a REDIMadrid y a los clientes afectados sobre el proceso que se sigue para reparar el fallo, de acuerdo con los tiempos de actualización en función de su severidad.

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

Nivel de severidad	Descripción	Tiempo de Ac- tualización
Alto	Problemas que impiden o degradan el funcionamiento de todos o parte de los servicios o funcionalidades configurados en cualquiera de los equipos. Se incluyen los problemas que ocurran cuyo origen esté localizado en los latiguillos.	Cada hora en horario laboral.
Medio	Problemas que no afectan al funcionamiento de los servicios o funcionalidades configuradas.	Cada 3 horas en horario laboral.
Bajo	Requerimientos de información y clarificación sobre aspectos técnicos relacionados con el funcionamiento, operación y configuración de equipos.	Cada 6 horas en horario laboral.

- Una incidencia se cerrará cuando el NOC de REDIMadrid haya aceptado dicho cierre, lo que normalmente se producirá cuando el servicio se haya restablecido y estabilizado, se hayan eliminado o corregido las causas que originaban los problemas en el servicio y se haya informado al NOC de dichas causas y confirmado que éstas se han eliminado. Si después de cerrar una incidencia se vuelven a presentar los mismos fallos que se pensó que estaban resueltos se reabrirá la misma incidencia anterior.
- En un plazo no superior a 48 horas desde el cierre del caso, el adjudicatario enviará un informe detallado sobre la incidencia a REDIMadrid. Todos los informes deben realizarse en una plantilla que contiene un encabezado con logotipos de uso obligatorio en la documentación administrativa del contrato.

El informe recogerá, como mínimo, los siguientes datos:

- Hora de comienzo de la incidencia.
- Hora de fin de la incidencia.
- Descripción de la causa.
- Actuaciones para solucionarla.
- Datos de contacto de las personas que han participado en su resolución.

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

- Si el adjudicatario hiciera uso de una solución provisional para solventar la incidencia, se incluirá el detalle técnico de dicha solución y la propuesta de implantación de la solución definitiva (incluyendo tanto una descripción técnica como plazos)
 - Otros datos de interés.
-
- Una incidencia se volverá a abrir si se presentan de nuevo los mismos fallos que había sido dados por resueltos.
 - El adjudicatario deberá realizar las actuaciones remotas y/o in-situ como proporcionar el soporte técnico necesario para atender y solucionar las incidencias o problemas que puedan aparecer en los componentes objeto del suministro o en los servicios configurados y/o soportados sobre los mismos hasta que se restablezca su funcionamiento normal, es decir, el que tenía antes de que surgiera la incidencia o problema.
 - Dichas actuaciones consistirán, entre otras, en trabajo de diagnóstico de mal funcionamiento de los componentes objeto del suministro y/o las funcionalidades configuradas y/o soportadas sobre los mismos, modificación de configuraciones, carga de versiones de software, apertura de incidencias o casos con el fabricante, revisión de elementos pasivos, realización de bucles, soporte y colaboración técnica con cualquiera de los suministradores y proveedores de otros servicios conectados o relacionados directamente con los componentes objeto del Suministro. y si fuera necesario, la reposición o sustitución del componente o pieza modular del componente afectado por la incidencia.
 - Estas actuaciones podrán ser realizadas in-situ o bien en remoto, según la naturaleza de la incidencia requiera, para que la resolución sea eficiente y se mantenga la garantía y calidad de las prestaciones configuradas en los componentes objeto del Suministro.
 - Las actuaciones se realizarán a petición expresa de REDIMadrid, o de aquella empresa o institución en la que REDIMadrid delegue, o por iniciativa del adjudicatario como parte del proceso de resolución de la incidencia.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

6. Requisitos de Formación

A continuación se describen los requisitos de formación:

- Se requiere que le adjudicatario preste unas sesiones de formación de, al menos, 40 horas basadas en la gestión, operación, mantenimiento y sistema de gestión del equipamiento ofertado indicado en el 3, así como sobre la seguridad de redes en general
- El programa de formación debe seguir el programa o cursos de formación oficiales del fabricante del equipamiento ofertado, esto es, la formación no tiene que ser una formación realizada ad-hoc, sino que tiene que ser un (o varios) curso/s que se oferten actualmente en la formación oficial del fabricante.
- Aunque la formación tiene que ser una formación oficial de fabricante, se solicita que el licitador sea flexible y los cursos ofrecidos puedan ser modificados en parte (quitar temas de un curso oficial, o mezcla varios cursos) para que se adapten lo máximo posible a la expectativas de REDIMadrid.
- Las sesiones de formación se realizarán en castellano, aunque la documentación oficial puede estar redactada en inglés o en español.
- La formación estará destinada, al menos, para 6 personas.
- El licitador será responsable del suministro del material de formación a los asistentes a las sesiones, este material debe ser material oficial que este diseñado para los cursos oficiales.
- Se requiere que la formación sea impartida por personal con certificación oficial del fabricante del equipamiento incluido en la oferta, además el formador debe ser un formador oficial del fabricante con la titulación específica para poder impartir formación, esto es, el formador deberá tener una titulación y conocimientos acorde con la formación que se va a impartir, para este fin se solicitará datos del instructor antes de realizar la formación, REDIMadrid podrá decidir si el instructor está suficientemente formado.

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

- La formación debe incluir parte practica, esta parte practica se puede hacer sobre una maqueta física o lógica.
- La formación se realizará en el lugar y días que a tales efectos designe IMDEA Software, que debería ser físicamente en la sede de IMDEA Software.

7. Informes

7.1. Informes Regulares

El adjudicatario suministrará mensualmente a REDIMadrid un informe técnico, como máximo en los cinco días laborables siguientes al final del mes. Este informe se enviará por correo electrónico y contendrá, al menos, la información que a continuación se detalla:

- Hora de comienzo de la incidencia.
- Hora de fin de la incidencia.
- Descripción de la causa.
- Actuaciones para solucionarla.
- Otros datos de interés.

No obstante, esta estructura podrá ser modificada a petición de REDIMadrid en cualquier momento. Con la información de la que REDIMadrid disponga de las incidencias del mes se evaluará el informe enviado y, de ser necesario, se abrirá un periodo de diálogo para aclarar aquellos datos en los que se detecten discrepancias. El adjudicatario enviará un informe final actualizado.

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

7.2. Informes Especiales

REDIMadrid podrá solicitar un informe especial sobre un problema determinado. El adjudicatario deberá confirmar a REDIMadrid la recepción de la petición inmediatamente y suministrar un borrador del informe (causa del problema y acciones tomadas para su solución) en las 24 horas siguientes a la recepción de la petición. El informe completo deberá enviarse a REDIMadrid durante los cinco días laborables siguientes. El informe incluirá, al menos, descripción detallada y complete del problema y su impacto, resumen de todas las acciones llevadas a cabo para resolver el problema e información detallada de las medidas tomadas para prevenir la repetición del problema. El informe se enviará por correo electrónico.

8. Muestras de equipamiento/solución

REDIMadrid solicitará al licitador propuesto como adjudicatario del contrato la información que precise y que estime pertinente para comprobar la veracidad y cumplimiento de los requisitos establecidos en el presente documento o solicitados para su valoración, pudiéndose incluir entre dicha información y a criterio de REDIMadrid, muestras del equipamiento o producto ofertado, así como una maqueta donde se debería probar la solución que REDIMadrid considere necesaria.

La maqueta deberá estar preparada y disponible para la demostración 15 días naturales después de recibir la propuesta de adjudicación.

En el caso de que la Fundación comprobase que el material o solución ofertada por el ofertante incumple alguno de los requisitos mínimos establecidos o de los requisitos obtenidos por puntuación, dicha oferta no será tenida en cuenta.

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid - FUNDACIÓN IMDEA SOFTWARE

Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

9. Consultas y Contacto

Cualquier consulta en relación con el presente procedimiento de adjudicación debe dirigirse por correo electrónico a la dirección noc@redimadrid.es indicando:

Asunto: REF:SSL-MADQCI.

Cuerpo: nombre de la empresa, datos de la persona que realiza la consulta y texto de la consulta.

El plazo de recepción de consultas finalizará 24 horas antes del fin del plazo de presentación de ofertas. IMDEA Software no tendrá obligación de responder las consultas realizadas transcurrido dicho plazo.

10. Confidencialidad

El adjudicatario garantizará la seguridad y confidencialidad de toda la documentación e información sobre REDIMadrid de la que disponga, disponiendo los medios necesarios para ello. Esta obligación estará en vigor aun cuando el contrato haya llegado a su término o haya sido cancelado.

11. Referencias bibliográficas

- National Institute of Standards and Technology. (2009). *NIST SP 800-41 Revision 1: Guidelines on Firewalls and Firewall Policy*. Gaithersburg, MD: NIST.
- National Institute of Standards and Technology. (2010). *NIST SP 800-113: Guide to SSL VPNs*. Gaithersburg, MD: NIST.

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

- International Organization for Standardization / International Electrotechnical Commission. (2013). *ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements*. Ginebra, Suiza: ISO/IEC.
- PCI Security Standards Council. (2018). *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. White Plains, NY: PCI Security Standards Council.
- Unión Europea. (2016). *Reglamento (UE) 2016/679: General Data Protection Regulation (GDPR)*. Diario Oficial de la Unión Europea.
- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)*. Gaithersburg, MD: NIST.
- IEEE Standards Association. (2010). *IEEE 802.1X: Port-Based Network Access Control*. New York, NY: IEEE.
- International Electrotechnical Commission. (2013). *IEC 62443: Industrial communication networks – Network and system security*. Ginebra, Suiza: IEC.
- Common Criteria Recognition Arrangement. (2006). *Common Criteria for Information Technology Security Evaluation – Evaluation Assurance Level (EAL) 4+*. Bruselas, Bélgica: CCRA.
- National Institute of Standards and Technology. (2002/2019). *FIPS 140-2/140-3: Security Requirements for Cryptographic Modules*. Gaithersburg, MD: NIST.
- Internet Engineering Task Force. (2018). *RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3*. Recuperado de <https://www.rfc-editor.org/rfc/rfc8446>

12. Glosario

- **2FA:** Two-Factor Authentication
- **AD:** Active Directory

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

- **API:** Application Programming Interface
- **ATP:** Advanced Threat Protection
- **BYOD:** Bring Your Own Device
- **CA:** Certificate Authority
- **CDE:** Cardholder Data Environment
- **CLI:** Command Line Interface
- **CPS:** Connections Per Second
- **DB:** Database
- **DNAT:** Destination Network Address Translation
- **DoS:** Denial of Service
- **DPI:** Deep Packet Inspection
- **EAP:** Extensible Authentication Protocol
- **FCC:** Federal Communications Commission
- **GDPR:** General Data Protection Regulation
- **GUI:** Graphical User Interface
- **HA:** High Availability
- **HSRP:** Hot Standby Router Protocol
- **HTTP:** HyperText Transfer Protocol
- **HTTPS:** HyperText Transfer Protocol Secure
- **ICMP:** Internet Control Message Protocol
- **IDS:** Intrusion Detection System

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

- **IEEE:** Institute of Electrical and Electronics Engineers
- **IKEv2:** Internet Key Exchange version 2
- **IoC:** Indicators of Compromise
- **IoT:** Internet of Things
- **IP:** Internet Protocol
- **IPsec:** Internet Protocol Security
- **IPS:** Intrusion Prevention System
- **ISO/IEC:** International Organization for Standardization/International Electrotechnical Commission
- **LACP:** Link Aggregation Control Protocol
- **LDAP:** Lightweight Directory Access Protocol
- **LEEF:** Log Event Extended Format
- **MIME:** Multipurpose Internet Mail Extensions
- **MITM:** Man-in-the-Middle
- **NAC:** Network Access Control
- **NAT:** Network Address Translation
- **NGFW:** Next Generation Firewall
- **NIST:** National Institute of Standards and Technology
- **NTP:** Network Time Protocol
- **PCI-DSS:** Payment Card Industry Data Security Standard
- **PFS:** Perfect Forward Secrecy
- **PSK:** Pre-Shared Key

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

- **PSU:** Power Supply Unit
- **QoS:** Quality of Service
- **RBAC:** Role-Based Access Control
- **RFC:** Request for Comments
- **RFP:** Request for Proposal
- **RPF:** Reverse Path Forwarding
- **SAML:** Security Assertion Markup Language
- **SD-WAN:** Software-Defined Wide Area Network
- **SFP:** Small Form-factor Pluggable
- **SIEM:** Security Information and Event Management
- **SLA:** Service Level Agreement
- **SMTP:** Simple Mail Transfer Protocol
- **SNMP:** Simple Network Management Protocol
- **SOAR:** Security Orchestration, Automation, and Response
- **SP:** Special Publication
- **SSO:** Single Sign-On
- **SSL:** Secure Sockets Layer
- **STIX/TAXII:** Structured Threat Information Expression/Trusted Automated Exchange of Indicator Information
- **TOTP:** Time-based One-Time Password
- **TLS:** Transport Layer Security
- **UPM:** Universidad Politécnica de Madrid

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE
SUMINISTRO, INSTALACIÓN Y SOPORTE DE EQUIPAMIENTO DE
SEGURIDAD PARA EL PROYECTO MadQuantum-CM, REDIMadrid -
FUNDACIÓN IMDEA SOFTWARE**

**Proyecto MADQuantum-CM, financiado por la Comunidad de Madrid y por el Plan
de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea –
NextGenerationEU**

- **URL:** Uniform Resource Locator
- **USB:** Universal Serial Bus
- **UTM:** Unified Threat Management
- **VLAN:** Virtual Local Area Network
- **vDOM:** Virtual Domain
- **VPN:** Virtual Private Network
- **VRRP:** Virtual Router Redundancy Protocol
- **WAN:** Wide Area Network
- **XML:** Extensible Markup Language