Servicios de protección de origen

PLIEGO DE CONDICIONES TÉCNICAS

1. Índice

2. Introducción

CRTVE ofrece a sus usuarios contenidos a través de su página web y aplicaciones para dispositivos conectados. Para ello, las redes de distribución de contenidos (CDN) acceden a los servidores de CRTVE alojados en los diferentes centros de datos de CRTVE o en servicios de nube pública.

Dado que estos servidores deben ser accesibles desde Internet para poder ofrecer servicios a los usuarios, están expuestos a los ataques cibernéticos que buscan tanto impedir la distribución de contenidos de CRTVE como el acceso a los sistemas propios de CRTVE.

Para minimizar los riesgos asociados a estos ataques, como la pérdida de servicio y las intrusiones ilegítimas en los sistemas internos de CRTVE, es necesaria la contratación de servicios específicos de seguridad para los sistemas de origen implicados en la distribución de los contenidos de CRTVE en Internet.

3. Lotes y tipos de servicios

El expediente se divide en cuatro lotes, que se definen a continuación:

Lote 1: Servicio de protección DNS
Lote 2: Servicio de protección de aplicaciones (WAF)
Lote 3: Servicio protección de origen de directos
Lote 4: Servicio de respaldo de almacenamiento.

4. Lote 1: Servicios de protección DNS

CRTVE requiere el uso de un servicio de DNS distribuido que permita la mitigación y neutralización de ataques a los servidores de resolución de nombres (DNS) que prestan el servicio a CRTVE. En caso de que los servicios DNS dejen de funcionar correctamente, se afectará gravemente al servicio de la web y aplicaciones de CRTVE, impidiendo el acceso a las mismas.

Los tipos de ataque más frecuentes a los servicios DNS son la denegación de servicio basados en la saturación de los servidores de origen por sobrecarga de peticiones, tanto centralizados como distribuidos (DoS y DDoS), o mediante el envío de peticiones mal formadas que aprovechan fallos del protocolo DNS y TCP.

El servicio requerido actuará de forma habitual como servidor DNS secundario de los servidores DNS primarios de CRTVE para cada una de las zonas DNS que determine CRTVE.

Requisitos técnicos mínimos del servicio

Se enumeran, a continuación, los requisitos técnicos mínimos que debe cumplir el servicio de protección del DNS:

RL1.1. El servicio tendrá que actuar como servidor DNS primario o secundario de todas las zonas DNS gestionadas por CRTVE, entre las que estará la zona rtve.es. CRTVE determinará, para cada zona, si el servicio DNS del licitador funcionará como servidor DNS primario o secundario.

RL1.2. En el caso de funcionamiento como servidor DNS secundario, CRTVE indicará para cada zona cuál será su servidor primario.

RL1.3. En el caso de funcionamiento como servidor DNS secundario, deberá permitir transferencias de zona desde los servidores primarios mediante los protocolos AXFR e IXFR.

RL1.4. En el caso de funcionamiento como servidor DNS secundario, deberá permitir el uso de mensajes DNS NOTIFY por parte del servidor primario para forzar la actualización de zonas.

RL1.5. El servicio se ejecutará en los servidores del licitador alojados en una cloud y en diferentes zonas de disponibilidad.

RL1.6. De forma adicional al requisito se requiere que el servicio se ofrezca desde servidores con redundancia geográfica.

RL1.7. Descartar o rechazar peticiones que se hagan a puertos que no sean el estándar DNS (53 UDP y TCP).

RL1.8. El servicio tendrá que aplicar reglas de forma automática para evitar los ataques más comunes a los servicios DNS.

RL1.9. Evitar ataques directos por Query. El licitador debe poder limitar el número de peticiones, analizar las consultas DNS recibidas y priorizarlas. Se debe indicar con suficiente detalle técnico el modo en el que se aplica esta protección.

RL1.10. Evitar ataques PSRD (Pseudo Random Subdomain Attack).

RL1.11. Implementar todas las protecciones TCP normales para evitar ataques de tipo TCP State Load.

RL1.12. Evitar ataques de tipo DNS Reflection & Amplification Attack. Tienen que ofrecer una arquitectura capaz de evitar ataques de reflexión y amplificación.

RL1.13. Evitar ataques de tipo DNS Cache Poisoning Attacks.

RL1.14. Evitar ataques basados DNS Malformed Packets.

RL1.15. Limitar el tráfico de DNS de direcciones IP individuales que emiten una cantidad sospechosa de solicitudes, con diferentes umbrales para diferentes tipos de solicitudes.

RL1.16. Debe poder proporcionar servicio mediante DNSSec.

RL1.17. Debe poder utilizar anycast para el enrutamiento de peticiones a los servidores DNS que formen parte de la solución propuesta.

RL1.18. Bajo condiciones determinadas, tiene que poder restringir las respuestas a los servidores de nombres DNS legítimos reconocidos de los principales proveedores de servicios (como los de los principales ISP en España), eliminando así las solicitudes de los bots y otros atacantes. El servicio debe mantener una lista actualizada de servidores de nombres DNS legítimos reconocidos que cubra más del 90 por ciento de todo el tráfico de Internet.

RL1.19. Deben acreditar al menos dos referencias de clientes con más de 20 millones de usuarios únicos mensuales en la unión europea.

RL1.20. Deben actualizar el servicio con las últimas vulnerabilidades detectadas, así como indicar los plazos estimados para resolución de nuevas vulnerabilidades, y notificar a CRTVE sobre las mismas.

RL1.21. Deben indicar el tiempo estimado máximo de implementación de nuevas reglas para las nuevas amenazas detectadas; así como, entregar la documentación de las mismas en el formato y el tiempo indicado por el departamento de Ciberseguridad de CRTVE.

Para todas ellas, deben explicar con suficiente detalle técnico la forma en la que se implanta la protección, penalizándose aquellas propuestas que no indiquen con claridad y coherencia la implementación de las mismas. Además, se valorarán positivamente aquellas propuestas que incluyan protección frente a otros tipos de ataques a servidores DNS que sean de utilidad para CRTVE tales como: ofrecer el servicio desde proveedores de servicios cloud independientes entre sí, ofrecer la redundancia geográfica requerida entre diferentes países de la Unión Europea, y alojar el servicio en las redes de los principales ISP.

Se valorarán positivamente aquellas propuestas que permitan una mayor flexibilidad de configuraciones, así como la automatización de configuración mediante el uso de API.

Gestión y alertas

El servicio tiene que ofrecer un portal de gestión donde se puedan consultar diferentes parámetros relevantes del servicio, así como elaborar informes sobre los mismos. También se requiere un sistema de alertas automatizadas.

Las características mínimas que deben ofrecer el panel de control y alertas se establecen en los siguientes requisitos:

RL1.22. El servicio tiene que ofrecer un portal de gestión donde se puedan consultar diferentes parámetros relevantes del servicio, así como elaborar informes sobre los mismos. Los parámetros relevantes que se incluirán, como mínimo, serán:

a. Tráfico (peticiones DNS) por zona(s) a lo largo de un periodo de tiempo seleccionable. La granularidad mínima requerida es de 1 minuto, para un periodo seleccionado de 30 minutos.
b. Respuestas NXDOMAIN por segundo en ese periodo de tiempo.

RL1.23. El sistema de logs del servicio tendrá que entregar todos los logs de peticiones DNS de cualquier tipo que lleguen a la plataforma.

RL1.24. En cuanto a las alertas automatizadas, tiene que permitir el establecimiento de alertas basadas en umbrales relacionados con el servicio, que se enviarán por correo electrónico a destinatarios indicados por CRTVE. Como mínimo, deben configurarse alertas para los siguientes eventos:

a. High number of NXDOMAIN responses: el volumen de respuestas NXDOMAIN para una zona supere el umbral establecido por CRTVE.
b. High traffic DNS: el volumen de peticiones DNS para una zona supera un umbral establecido por CRTVE.
c. Failed zone transfer, cuando el servicio se utilice como DNS secundario.

Se valorarán positivamente aquellas propuestas que permitan la configuración de más alertas personalizadas, y la gestión avanzada desde el panel de control de forma autónoma por parte de CRTVE. También se valorarán positivamente aquellas propuestas que ofrezcan un menor desfase en las métricas con respecto al tiempo real.

5. Lote 2: WAF

CRTVE requiere de un servicio WAF que proteja los servidores de origen que alojan las aplicaciones que dan servicio a la web y aplicaciones conectadas.

Un servicio WAF (Web Application Firewall) analiza el tráfico de red enviado a las aplicaciones servidor, así como a las máquinas que las albergan (servidores). En ese análisis se buscan peticiones sospechosas y anómalas, que se desechan antes de su envío para prevenir los ataques a las aplicaciones y servidores de origen que las alojan.

Requisitos técnicos mínimos del servicio

El servicio requerido tiene que cumplir con los siguientes requisitos mínimos:

RL2.1. El servicio se ejecutará en los servidores del licitador alojados en una cloud con disponibilidad en diferentes zonas.

RL2.2. El servicio WAF debe ser válido como origen para las CDN utilizadas por CRTVE para distribuir los contenidos.

RL2.3. Tiene que tener capacidad para procesar de forma habitual 450 millones de peticiones mensuales, con un promedio diario de 2.000 peticiones por segundo, y máximos diarios de habituales de 4.000 peticiones por segundo. Es esperable que haya varios eventos con más 1.000.000 de usuarios simultáneos durante la vigencia de este servicio, por lo que la solución propuesta debe ser autoescalable para no añadir latencias adicionales en estos casos.

RL2.4. Tiene que permitir a CRTVE activar y desactivar reglas, así como activarlas en modo bloqueo y activarlas en modo logging de forma autónoma. El tiempo máximo para la aplicación de estos cambios será de 60 segundos.

RL2.5. Tiene permitir la definición de reglas, o modificar las ya existentes por parte de CRTVE.

RL2.6. La solución propuesta tendrá que recibir actualizaciones de reglas con suficiente frecuencia para evitar ataques que exploten nuevas vulnerabilidades encontradas.

RL2.7. Tiene que proteger las aplicaciones e infraestructura de origen de CRTVE frente a ataques de denegación de servicio, tanto centralizados (DoS) como distribuidos (DDoS). La protección frente a estos ataques consistirá en la mitigación del ataque mediante servicios automatizados que deben descartar el tráfico que se identifique como malicioso.

RL2.8. Tiene que proporcionar protección contra los 10 tipos de ataque principales según la catalogación OWASP.

RL2.9. Tiene que proporcionar protección contra las vulnerabilidades detectadas por CVE.

RL2.10. Tiene que proporcionar protección para la usurpación de cuentas de usuarios (Account Takeover en inglés).

RL2.11. Tiene que proporcionar reglas basadas en la ubicación geográfica de las direcciones IP.

RL2.12. Tiene que proporcionar al menos un servicio de reputación de IP actualizado con frecuencia, así como permitir el uso de sistemas de reputación de direcciones IP de terceros.

RL2.13. Tiene que permitir bloquear peticiones de user-agent reconocidos como maliciosos y también en función de cabeceras HTTP.

RL2.14. Tiene que permitir el bloqueo de peticiones desde un origen hacia una IP cuando se haya superado un umbral predefinido.

RL2.15. Tiene que ofrecer protección contra bots. Se valorarán positivamente aquellas propuestas que permitan identificar peticiones de bots legítimos, como GoogleBot o BingBot, y ofrezcan datos específicos sobre dichas peticiones.

RL2.16. Debe ofrecer una interfaz de usuario vía web, que permita la revisión de eventos, el acceso a estadísticas, y la autoprovisión de configuraciones por parte de CRTVE. Se valorará positivamente la facilidad de uso de la interfaz de usuario, atendiendo a parámetros subjetivos tales como la intuitividad, el uso de gráficos adecuados, la disposición de la información mostrada, la existencia de plantillas y asistentes para personalizar la información mostrada.

RL2.17. La solución propuesta tiene que permitir la protección de servidores de origen cuando éstos no sean accedidos desde una CDN. Para ello, deberá ofrecer módulos de aplicación instalables (plugins) en los servidores de CRTVE, que se comunicarán con el servicio WAF proporcionado para el análisis de las peticiones recibidas. Se requieren, al menos, plugins específicos para las siguientes aplicaciones:

- HAProxy
- Nginx Web Server
- Apache Web Server

RL2.18. La interfaz gráfica debe mostrar información detallada sobre las peticiones recibidas, tanto legítimas como sobre los ataques detectados, con una granularidad máxima de un (1) minuto y una retención de datos mínima de 30 días. Se valorarán positivamente las propuestas que ofrezcan una menor latencia en la presentación de datos y una retención de datos mayor.

Para cada requisito, las propuestas deben explicar con suficiente detalle técnico la forma en la que se implanta la protección, penalizándose aquellas propuestas que no indiquen con claridad y coherencia la implementación de las mismas. Asimismo, se valorarán positivamente aquellas propuestas que incluyan medidas de protección adicionales que sean de utilidad para CRTVE, tales como la gestión de respuestas ante bots utilizados para intentar el robo de cuentas, búsqueda de vulnerabilidades, uso fraudulento de formularios, el registro fraudulento de usuarios en la web, o los ataques DDoS. También se valorarán positivamente aquellas propuestas que ofrezcan la identificación de nuevos bots y de patrones de ataque a partir del análisis las peticiones recibidas.

Gestión y alertas

Además de los requisitos específicos de protección de origen, el servicio propuesto tiene que ofrecer las siguientes características:

RL2.19. Proporcionar un API que permita integrarse con herramientas de análisis de terceros. Se valorarán positivamente aquellas propuestas que ofrezcan un API con mayor funcionalidad tanto de obtención de datos como de configuración.

RL2.20. Proporcionar un panel de control de monitorización que permita obtener datos de acceso y ataques con el menor retraso posible con respecto al tiempo real. Se valorarán positivamente aquellas propuestas que ofrezcan un panel de control más detallado, con mayor capacidad de análisis de eventos, posibilidades de integración, retención de datos y facilidad de uso.

RL2.21. Proporcionar un servicio que permita definir alertas automatizadas a partir de umbrales recomendados por el licitador y adecuados a las necesidades del servicio de CRTVE. El servicio tiene que notificar de la activación de una alerta mediante correo electrónico, así como llevar a cabo las acciones previstas en caso de que esa alerta se detecte. Se valorarán positivamente aquellas propuestas que permitan una definición e integración más detallada de las alertas y las acciones asociadas a las mismas.

RL2.22. Se requiere compatibilidad con herramientas SIEM. Además, se requiere la integración del WAF con las herramientas SIEM utilizadas por CRTVE. Se valorarán la experiencia aportada por el licitador en integraciones para otros clientes, y la compatibilidad de la solución propuesta con sistemas SIEM de diferentes fabricantes.

6. Lote 3: Servicio de protección de origen de directos

La protección de los servicios de publicación de vídeo en directo a través de Internet (en inglés, streaming) es cada vez más importante, puesto que el consumo de estos contenidos se ve de forma natural por una parte cada vez mayor de los usuarios, y es fundamental para ofrecer un servicio multiplataforma donde se acerque el contenido a los usuarios. Y ya no solo para los usuarios de la web y aplicaciones de CRTVE, sino también para usuarios de otros agregadores de contenidos con los que CRTVE tiene acuerdos de distribución, como Radio Player o Samsung TV Plus, que usan como fuente las emisiones a través de Internet de CRTVE.

Una de las medidas de protección del origen más efectiva es la reducción de las peticiones hechas desde las CDN a los servidores de origen. De esta manera se hace posible la gestión de listas de servidores conocidos para autorizar dichas peticiones. Esta gestión permite impedir el acceso desde Internet a usuarios malintencionados sin limitar el acceso a otros usuarios legítimos.

Además, se reduce el ancho de banda necesario para proporcionar el servicio de streaming en directo, lo que permite una reducción de los recursos necesarios para atender las peticiones, y permite hacer la publicación de directos desde entornos de nube pública con un coste previsible e independiente de la audiencia del evento retransmitido.

Requisitos técnicos mínimos del servicio

Se requiere un servicio que cumpla con los siguientes requisitos mínimos:

RL3.1. Acceda una única vez a origen durante el tiempo de vida de un objeto, según se defina en la configuración del servicio o en la respuesta de los servidores de origen.

RL3.2. Entregue a las CDN los objetos requeridos por éstas para su distribución a los usuarios, modificando o manteniendo el tiempo de vida de los objetos (TTL) si se requiere.

RL3.3. La capacidad requerida para entregar a la CDN deberá ser suficiente para atender el tráfico requerido para entregar eventos de directo con más de 1 millón de usuarios simultáneos. Para validar esta característica, los licitadores deben indicar la capacidad máxima de su solución (en gigabit por segundo y peticiones por segundo) para la entrega de contenidos a CDN.

RL3.4. Tenga capacidad para 17 canales lineales ABR (Adaptive BitRate) con una calidad máxima de 1080p 24 horas al día, todos los días del año. Cada canal se emitirá en los formatos HLS y MPEG-DASH, con bitrate adaptativo de hasta de 4 calidades de vídeo diferentes, con un máximo aproximado de 10 Mbps por canal (4 calidades de vídeo y 3 calidades de audio por cada canal).

RL3.5. Tenga capacidad para asumir 40 canales temporales adicionales, en formatos HLS y MPEG-DASH, con una calidad máxima de 1080p. Cada canal se emitirá en los formatos HLS y MPEG-DASH, con bitrate adaptativo de hasta de 4

calidades de vídeo diferentes, con un máximo aproximado de 10 Mbps por canal (4 calidades de vídeo y 3 calidades de audio por cada canal).

RL3.6. Tenga capacidad para asumir 128 canales de radio, en formatos HLS y MPEG-DASH, con un bitrate máximo de 192 kbps. Cada canal se emitirá en los formatos HLS y MPEG-DASH, con bitrate adaptativo de hasta de 3 calidades de audio diferentes, con un máximo aproximado de 240 kbps (con 3 calidades de audio por cada canal).

RL3.7. Permita la autorización de acceso desde las CDN mediante el envío de una cabecera HTTP específica.

RL3.8. Ofrezca una lista actualizada y completa de las direcciones IP de los servidores que accederán a origen, de modo que se puedan configurar las reglas de acceso adecuadas en los firewalls de CRTVE.

RL3.9. Permita la entrega de contenido HTTP y HTTPS a las CDN, independientemente del protocolo (HTTP o HTTPS) utilizado para recuperar el contenido desde los servidores de origen de CRTVE.

RL3.10. Permita el acceso a diferentes orígenes de directo de CRTVE, mediante el uso de rutas diferentes solicitadas por los usuarios.

RL3.11. Los elementos que compongan la solución deben estar redundados, y no deben tener puntos únicos de fallo, ni requerir paradas para mantenimiento o actualización, dado que este servicio de protección de origen de directos afecta a uno de los elementos diferenciales y característicos de la presencia de CRTVE en Internet, como es la emisión de vídeo en directo

RL3.12. Se requiere que la solución propuesta ofrezca redundancia geográfica. Se valorarán positivamente aquellas propuestas cuyo servicio ofrezca redundancia geográfica en diferentes países de la Unión Europea.

RL3.13. La propuesta técnica debe ser compatible con cualquier CDN utilizada por CRTVE durante la vigencia del expediente.

RL3.14. Para asegurar la tolerancia a fallos del proveedor actual de CDN, las ofertas técnicas no podrán utilizar la tecnología de Fastly.

Para cada requisito de protección de la plataforma de origen de directos, las propuestas técnicas deben explicar con suficiente detalle técnico la forma en la que se implanta la protección, penalizándose aquellas propuestas que no indiquen con claridad y coherencia la implementación de las mismas. Asimismo, se valorarán positivamente aquellas propuestas que incluyan medidas de protección adicionales que sean de utilidad para CRTVE, como medidas adicionales de protección de acceso desde CDN y de identificación ante el origen. También se valorarán positivamente aquellas propuestas que permitan asumir el tráfico de directos entregado a los usuarios de la web y aplicaciones de CRTVE, en escenarios de fallo masivo del proveedor CDN, cuando CRTVE no disponga de un servicio de backup de CDN específico disponible.

7. Lote 4: Servicio de respaldo de almacenamiento

CRTVE ofrece a sus usuarios uno de los catálogos de vídeo y audio online en lengua española más extensos disponibles en Internet. Ofrece todos los contenidos de producción propia emitidos por CRTVE desde 2008 (año de inicio de la página web de CRTVE como portal de contenidos) así como los contenidos anteriores recuperados del archivo, incluyendo algunas de las series de mayor éxito (como "Cuéntame cómo pasó" o "Amar en tiempos revueltos").

Aunque el catálogo de contenidos disponible es muy amplio, la mayor parte del consumo se da en los contenidos más recientes mientras que el consumo de contenidos antiguos o poco populares ocurre con menor frecuencia. Este tipo de comportamiento de consumo donde un 20% o menos del total de contenidos genera el 80% o más del tráfico se denomina habitualmente long tail, por su nombre en inglés.

Este modelo de consumo es muy exigente en cuanto a los recursos de origen, ya que todos los contenidos deben estar disponibles a los usuarios en todo momento con la misma latencia. Sin embargo, dado que el contenido más popular es conocido permite asegurar la entrega de los contenidos más demandados mediante el almacenamiento de los mismos en un servicio de almacenamiento online, con alta disponibilidad, y liberando recursos de la plataforma de origen.

Asimismo, la distribución de ciertos contenidos usados por la web y aplicaciones de CRTVE, como ficheros de imágenes, json o xml, se beneficia del alojamiento en servicios de almacenamiento en cloud, con unas condiciones de acceso a origen estables, e independientes de la carga de trabajo de la plataforma de origen de CRTVE.

Por tanto, se requiere un servicio de almacenamiento online accesible desde Internet (en inglés, cloud storage) que permita el almacenamiento de contenido y su entrega a las CDN que distribuyan el contenido de CRTVE a los usuarios. El servicio tiene que cumplir con estos requisitos mínimos:

RL4.1. Almacenamiento cloud compatible con protocolo S3.
RL4.2. Capacidad mínima disponible de 12.000 terabytes (en adelante, TB).
RL4.3. Data Durability del 99.999999999% anual.
RL4.4. Consola de gestión y UI accesible vía web.
RL4.5. Distribución por buckets del contenido. Estos buckets deben servir como origen directo de las CDN, sin necesidad de servicios intermedios.
RL4.6. En el ámbito del cloud storage, se denomina zona de disponibilidad a los centros de datos en los que se alojan los servidores. Se requiere que la solución propuesta ofrezca, como mínimo, dos zonas de disponibilidad diferentes en países de la Unión Europea, dos zonas en Estados Unidos de América y otra en alguno de los siguientes países donde se ofrece el servicio RTVE Play+: Japón, Corea del Sur, Australia, India. En cada zona de disponibilidad, CRTVE debe poder almacenar 4.000 TB de datos.

RL4.7. Debe permitir la replicación automática entre zonas de disponibilidad ubicadas en el mismo continente.

RL4.8. Tráfico de salida ilimitado (sin egress cost).

RL4.9. Tráfico de entrada ilimitado (sin ingress cost).

RL4.10. Tráfico de replicación entre zonas de disponibilidad ubicadas en el mismo continente ilimitado (sin coste).

RL4.11. Llamadas API ilimitadas (sin coste).

RL4.12. Capacidad de subida desde los centros de datos de CRTVE igual o superior a 5 Gbps.

RL4.13. El servicio tendrá que ser compatible con la aplicación rclone desde sistemas Linux. Este aspecto se comprobará en las pruebas técnicas del servicio.

RL4.14. Capacidad de entrega de contenido a CDN igual o superior a 20 Gbps.

RL4.15. Todo el contenido debe estar disponible en todo momento para su consumo por parte de las CDN, independientemente de la popularidad o número de accesos recientes que haya tenido.

RL4.16. Los elementos que compongan la solución deben estar redundados, y no deben tener puntos únicos de fallo. Además, se valorarán positivamente aquellas propuestas cuyo servicio ofrezca redundancia geográfica en diferentes países.

RL4.17. Se requiere la capacidad de limitar el acceso por dirección IP al almacenamiento. Se valorarán positivamente aquellas propuestas que permitan aplicar políticas avanzadas de limitación de acceso al almacenamiento.

RL4.18. Para que el servicio ofrecido por CRTVE no se vea afectado, el adjudicatario del servicio tendrá que migrar todos los contenidos existentes en el almacenamiento actual al nuevo almacenamiento. El volumen estimado de datos a migrar es de 1,5 petabytes, en un almacenamiento del fabricante Wasabi. El adjudicatario del servicio tendrá que asumir los costes de migración, incluido el almacenamiento en el servicio actual, hasta completar la copia de los datos y la integración con la CDN. El plazo máximo para la migración es de 60 días desde la fecha de inicio del servicio.

Para el cómputo de uso del almacenamiento, se considerará como unidad el terabyte. Se considerará utilizado, cada terabyte o fracción usado durante un periodo de facturación (1 mes) en una zona de disponibilidad. Esto aplicará tanto al almacenamiento incluido en el término fijo (2.000 terabytes) como al almacenamiento adicional que se requiera. Ejemplo: si en un periodo de facturación se han ocupado 1,7 terabytes de almacenamiento, se considerarán consumidos 2 terabytes de datos. Si en el siguiente periodo de facturación se ocupan 0,9 terabytes de datos, se considerará consumido 1 terabyte. No se admitirán gastos por otros conceptos diferentes al almacenamiento de datos, que incluirá todos los servicios necesarios para su uso por parte de CRTVE.

El licitador deberá proporcionar instrucciones detalladas para la conexión y acceso al contenido, tanto desde PC con sistema operativo Windows y MacOS, así como desde línea de comandos en servidores con sistema operativo Linux.

Para cada requisito, las propuestas técnicas deben explicar con suficiente detalle técnico la forma en la que se implanta la protección, penalizándose aquellas propuestas que no indiquen con claridad y coherencia la implementación de las mismas. Asimismo, se valorarán positivamente aquellas propuestas que incluyan medidas de protección adicionales que sean de utilidad para CRTVE. Por ejemplo, gestión de usuarios y permisos, asignación de volúmenes a diferentes proyectos o priorización de acceso según el usuario.

También se valorarán positivamente aquellas propuestas que ofrezcan mejoras en la latencia de acceso, en la velocidad máxima y concurrencia en la subida de contenido. También se valorarán positivamente las funcionalidades adicionales que faciliten la gestión del contenido alojado en el servicio, como el acceso mediante diferentes protocolos al sistema de ficheros, la automatización de la gestión de contenidos mediante API, y opciones de personalización adicionales.

8. Pruebas técnicas

CRTVE realizará junto con cada licitador una batería de pruebas en la que se verificará el cumplimiento de todas las funcionalidades y requerimientos especificados en los apartados que describen cada tipo de servicio, así como para la validación de los elementos que se indican en cada una de las propuestas.

CRTVE lanzará un requerimiento por correo electrónico a todos los licitadores que hayan presentado ofertas a cada uno de los lotes, solicitando que ponga a disposición los recursos técnicos y humanos que resulten necesarios para completar esta fase de validación. Los licitadores tendrán la obligación de responder a este requerimiento y de poner a disposición de CRTVE estos recursos, en un plazo no superior a 48 horas a partir del momento en que CRTVE envíe el requerimiento. Para ello, deben indicar en sus ofertas técnicas, la información el correo electrónico de contacto más conveniente a tal efecto.
Los licitadores tendrán que superar todas y cada una de las pruebas técnicas. RTVE dispondrá de un plazo máximo de 14 días naturales, a contar a partir del momento en que CRTVE comunique al licitador el inicio de las pruebas, para realizar las pruebas y validaciones. Para este fin, se requiere acceso a las herramientas de gestión y de estadísticas del licitador, así como a cualesquiera servicios o subsistemas que el licitador oferte. En caso que algún elemento de los licitados no se ponga a disposición de RTVE para su oportuna revisión/prueba, la propuesta será declarada como no apta.

Es importante que los proveedores tengan en cuenta que, para esta fase de prueba del servicio, el licitador correrá con todos los costes que sean necesarios para realizar las pruebas, y la CRTVE no asumirá ninguno.

También ha de tener en cuenta que CRTVE no efectuará ningún tipo de modificación sustancial a los activos del servicio, para adaptarse a los requerimientos técnicos del proveedor y/o fabricante, si considera que estas pueden tener un impacto negativo importante sobre el servicio actual.

9. Modelo de relación, acompañamiento y seguimiento

El modelo de relación que se establecerá entre cada adjudicatario y CRTVE tiene como objetivo garantizar el control y el seguimiento del servicio que se tiene que proveer. También tiene como misión la trazabilidad y la supervisión de los proyectos que dicho servicio ejecutará.
Se requiere la asignación de un Technical Account Manager (TAM), que asistirá a CRTVE durante las fases de diseño de la solución y migración del servicio, así como durante el resto del tiempo de contrato para la operación del servicio. Este interlocutor técnico, se responsabilizará de asegurar la mejora continua del servicio, así como de gestionar o escalar las peticiones más urgentes y las incidencias más graves.

Gestión de incidencias y soporte técnico

Durante la prestación de los servicios descritos en este pliego, pueden encontrarse problemas en el servicio o bien requerirse asistencia técnica por parte de CRTVE para hacer cambios en la configuración de los servicios provistos por cada adjudicatario. Por ello, se requiere:

RC.1. Soporte técnico en castellano, tanto por teléfono con numeración española como por Internet.

RC.2. Se requerirá soporte técnico en castellano en horario 24x7 para la gestión de incidencias que afecten al servicio, así como para solicitudes de soporte técnico urgente.

RC.3. Las propuestas deberán indicar el tiempo máximo de respuesta ante peticiones de soporte por parte de CRTVE, tanto para incidencias del servicio como para peticiones de soporte.

RC.4. Herramientas web para la gestión del servicio. Deben ser 100% funcionales a través de, al menos, uno de los siguientes navegadores: Microsoft Edge, Firefox 136 o Google Chrome 134.

RC.5. Acceso a los casos de soporte abiertos y el histórico de los mismos.

RC.6. Acceso a una base de datos de conocimiento, en la cual se detallen los aspectos técnicos de configuración de los servicios, buenas prácticas y herramientas o metodologías de programación necesarias para la integración con los mismos.

RC.7. Se requieren 52 horas de servicios profesionales para la monitorización de eventos relevantes y tareas de configuración y gestión avanzadas. Se valorarán positivamente aquellas propuestas que ofrezcan horas adicionales de servicios profesionales. Estas horas de servicios profesionales no supondrán un coste adicional para CRTVE.

Tipificación de incidencias y peticiones

Dentro de esta asistencia técnica, identificamos diferentes tipos de incidencias y de peticiones, en función de su gravedad y/o relevancia para CRTVE.

Tipos de incidencias y peticiones:

- Críticas: Aquellas que requieren la intervención inmediata del proveedor para recuperar el funcionamiento habitual del servicio, evitar un fallo del mismo, la afectación grave de los servicios de origen de CRTVE o evitar un daño reputacional o económico para CRTVE.
- Altas: Aquellas en las que CRTVE requiere de la intervención rápida del proveedor del servicio, pero no tienen la gravedad suficiente, en el momento de abrir la petición, para ser consideradas críticas.
- Normales: Aquellas que no son definidas como críticas o altas por CRTVE.

Acuerdos de nivel de servicio

Se establecen diferentes acuerdos de nivel de servicio (ANS) para la atención de incidencias y peticiones.

Acuerdos de nivel de servicio para incidencias ocurridas fuera de los horarios de monitorización de eventos relevantes:

- Incidencias críticas: se requiere un tiempo de respuesta y atención de la incidencia inferior a 15 minutos. Se requiere un tiempo de solución de la incidencia inferior a 60 minutos.
- Incidencias altas: se requiere un tiempo de respuesta y atención de la incidencia inferior a 120 minutos. Se requiere un tiempo de solución de la incidencia inferior a 6 horas.
- Incidencias normales: El tiempo de respuesta sugerido es de 24 horas.

En el caso de las incidencias o peticiones surgidas durante los eventos relevantes para los que se haya solicitado monitorización específica, el tiempo máximo de respuesta y atención de la incidencia será de 5 minutos. En estos casos, el tiempo máximo de resolución de la incidencia o petición será de 30 minutos.
Será objeto de valoración la mejora de los acuerdos de nivel de servicio.

Las propuestas deberán indicar el tiempo máximo de respuesta ante peticiones de soporte por parte de CRTVE, tanto para incidencias del servicio como para peticiones de soporte.

Informes y estadísticas del servicio

CRTVE podrá obtener informes y estadísticas del servicio cuando lo considere necesario.
Para proporcionar a CRTVE esta información, el adjudicatario de cada lote debe proveer de herramientas web de para la obtención de reportes y estadísticas. Deben cumplir, al menos, estos requisitos:

RC.8. Ofrecer estadísticas sobre el uso del servicio, con una granularidad mínima de 24 horas. Los datos deben poder agruparse por días, semanas y meses manteniendo un histórico mínimo de 30 días.

RC.9. De forma automática deben estar disponibles, al menos, los datos referidos a los últimos tres meses.

RC.10. Gráficos y tablas. Todos los reportes anteriores deben poderse mostrar de forma gráfica y en forma de tablas.

RC.11. Reportes periódicos automáticos. Cualquiera de los reportes anteriores se debe poder enviar por email con la periodicidad deseada al conjunto de destinatarios establecido para cada reporte.

RC.12. Asimismo, las unidades facturadas deberán ser verificables a través de los valores de monitorización de tráfico real que proporcione la herramienta, no siendo válida dicha verificación a través de ninguna herramienta de facturación que no proporcione el detalle mínimo sobre el tráfico real de cada propiedad para el cálculo de la misma. A tal efecto se especificará en la propuesta cómo realizar dicha comprobación.

Automatización de cambios de configuración y provisión de servicios

Para permitir la automatización de las tareas de administración de cada uno de los servicios, los adjudicatarios deben proporcionar acceso a CRTVE a las API de gestión y provisión de servicios. CRTVE utilizará dichas API en función de sus necesidades.

Acompañamiento y mejora del servicio

CRTVE busca la mejora continua del servicio ofrecido a los usuarios, así como garantizar la máxima calidad del servicio. Para ello, CRTVE requerirá a los adjudicatarios de cada uno de los lotes la elaboración de un informe de evaluación periódico en el que se recojan los aspectos más destacables del servicio durante el periodo a evaluar, incluyendo las propuestas de mejora por parte del adjudicatario. La presentación de los informes se hará con periodicidad mensual, a través de Internet.

Dada la criticidad de los servicios de protección de la plataforma de origen, RTVE valorará el modelo de relación, acompañamiento y seguimiento propuesto por el licitador. Para tal fin tendrá que presentar en su propuesta el modelo, así como los perfiles involucrados en dicho acompañamiento, información que estará sujeta juicio de valor. Se requieren, como mínimo, 52 horas de servicios profesionales para estas tareas. Se valorarán positivamente aquellas propuestas que ofrezcan horas adicionales de servicios profesionales. Este acompañamiento no supondrá un coste adicional para RTVE.

10. Formato de las ofertas

Las ofertas deben contener:

- Resumen ejecutivo (máximo 5 páginas). Describiendo la oferta de forma resumida e incluyendo:
    - Contacto técnico para las aclaraciones necesarias y la coordinación de las pruebas técnicas. Se gestionará el contacto entre los licitadores y CRTVE a través de la dirección de compras de CRTVE.

- Para cada LOTE
    - Documentación técnica específica sobre el servicio.
    - Modelo de acompañamiento y perfiles.
    - Modelo de soporte.
    - Modelo de protección de origen.

Se penalizarán aquellas propuestas que no incluyan una información detallada, clara y concisa de la solución técnica propuesta.