Servicios de protección DNS

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 licita en un único lote: Servicios de protección DNS.

4. Descripción del servicio y requisitos técnicos.

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:

RT.1. El servicio tendrá que actuar como servidor DNS primario o secundario de todas las zonas DNS gestionadas por CRTVE, sin limitación en número, 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. Como referencia, el número de dominios de segundo y tercer nivel que CRTVE tiene registrados a su nombre, es de 399 dominios, y se gestionan zonas DNS adicionales, de dominios registrados por terceros para su uso por parte CRTVE.

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

RT.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.

RT.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.

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

RT.6. De forma adicional al requisito anterior, se requiere que el servicio se ofrezca desde servidores con redundancia geográfica por país.

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

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

RT.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.

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

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

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

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

RT.14. Evitar ataques basados DNS Malformed Packets.

RT.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.

RT.16. Debe poder proporcionar servicio mediante DNSSec.

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

RT.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.

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

RT.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.

RT.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.

RT.22. El servicio debe funcionar 24 horas al día, todos los días del año, con una disponibilidad igual o superior al 99,95%, medido de forma mensual. Se valorarán positivamente aquellas propuestas que ofrezcan mayor garantía de disponibilidad.

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:

RT.23. 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.

RT.24. El sistema de logs del servicio tendrá que entregar todos los logs de peticiones DNS de cualquier tipo que lleguen a la plataforma.

RT.25. 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. Asimismo, se valorarán otros aspectos de la interfaz de usuario del panel de control, como su usabilidad y capacidad de personalización.

5. 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, 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 5 días laborables, 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.

6. 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.

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 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.

7. 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.

- Documentación técnica específica sobre el servicio.
- Documento de ajuste a requisitos.
- 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.