

S-03250-2023

Servicio de Múltiple Factor de Autenticación (MFA)

MEMORIA JUSTIFICATIVA

JUSTIFICACIÓN DE LA NECESIDAD

RTVE dispone de múltiples servicios y aplicaciones accesibles desde el exterior para permitir el teletrabajo y el acceso desde distintos dispositivos cuando resulte necesario, tales como:

- Correo electrónico y sistema de colaboración Office365
- Extranet (Intranet accesible desde el exterior)
- VPN's de acceso a las redes de las distintas Áreas Técnicas (Corporación, TVE, RNE)
- Aplicaciones on-premises en RTVE aunque expuestas a internet, como el gestor documental VisuARCA, utilizadas por empleados y clientes
- Aplicaciones Cloud proporcionadas por terceros, como la plataforma de formación.
- Otros servicios

Asimismo, se dispone de varias VPN para acceso remoto a diferentes sistemas y aplicaciones, tanto Corporativas como técnicas, utilizadas por los sistemas de Producción de TVE y RNE.

Se dispone de diversos mecanismos de seguridad para el acceso a dichos servicios y aplicaciones:

- **Sistema de Gestión de Identidades y Control de Accesos**, que gestiona los usuarios, sus roles, y los permisos de acceso a cada aplicación o servicio, registra quien autoriza dicho acceso, y sincroniza los usuarios en todas las aplicaciones y servicios para que el usuario disponga de un código de usuario y contraseña único.
- **Directorio Activo corporativo**, que valida las credenciales de los usuarios y los servicios a los que tienen acceso en el momento que acceden a cada aplicación o servicio.
- Directorios independientes en cada Área técnica para autenticación de acceso a las respectivas VPN's de TVE y RNE

Estos mecanismos, proporcionan un alto nivel de seguridad, pero **resultan insuficientes** para evitar una intrusión, dado que los atacantes disponen de herramientas avanzadas y de ingeniería social con los que pueden llegar a conseguir usuarios y contraseñas, y utilizarlas suplantando al usuario con fines maliciosos.

Por ello, y ante el crecimiento exponencial que viene produciendo de ciberataques, resulta imprescindible la incorporación de un **Sistema de Autenticación Multifactor**, que permita dotar a RTVE de una seguridad adicional cuando se realizan accesos a sistemas corporativos desde el exterior.

Esta necesidad viene ratificada por organismos de referencia en ciberseguridad para empresas públicas, como son el Centro Criptológico Nacional (Ministerio del Interior) en su guía “Recomendaciones de seguridad para Autenticación Multifactor”.



Recomendaciones de Seguridad para Autenticación Multi-Factor

[Informe CCN-PYTEC nº7](#) 

La ventaja principal de utilizar autenticación multi-factor es que el compromiso de alguno de los factores de autenticación no es suficiente para que un atacante acceda de forma no autorizada a los recursos de la organización, ya que deberá obtener los demás factores. Hoy en día, con el auge de los ataques de phishing, ingeniería social, fuerza bruta o simple robo, es fundamental una autenticación multi-factor que utilice factores de distintas categorías, ya que cada categoría tiene sus fortalezas y distintas superficies de ataque.

así como la Oficina de Coordinación de Ciberseguridad en la Métrica A1 de su circular 1_22.



GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD

DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS



A1	Implantación del segundo factor de autenticación en el servicio de correo y los accesos remotos de los usuarios para teletrabajo.
-----------	---

Por definición, la autenticación multifactor combina al menos dos de los siguientes métodos para autenticar firmemente a un usuario:

- Algo que se sabe (normalmente una contraseña)
- Algo que se tiene (un dispositivo de confianza que no es fácil de duplicar)
- Algo que se es (biometría)



La autenticación es materialmente más fuerte cuando se despliega a través de dos canales / dispositivos diferentes. De esta forma un atacante debe comprometer dos redes para obtener acceso a la cuenta de un usuario.

Por ello, se requiere la contratación de una plataforma como servicio (en la nube) que permita implementar en RTVE el servicio de autenticación Multifactor (MFA), ofreciendo numerosas ventajas:

- Modelo de pago por uso.
- Capacidad de crecimiento dinámico según las necesidades.
- Plataforma gestionada íntegramente en cloud del proveedor
- Integración con los sistemas corporativos y técnicos previstos.

La contratación consiste en

- **Servicio de Plataforma Cloud MFA** para todos los usuarios de RTVE (internos y externos)
- **Administración y soporte del servicio** (tanto para enrolamiento de usuarios como para atención de incidencias en nivel 2, transferidas desde CAU RTVE)
- **Servicios Profesionales** evolución y mejora del sistema.

La solución MFA deberá poder gestionar acceso MFA por Radius y SAML (ambos) integrando cada aplicación con uno u otro protocolo según sea posible.

Actualmente, para el acceso MFA a O365 se utiliza en RTVE tanto MS Authenticator como SMS. El servicio MFA aquí solicitado NO gestionará inicialmente el acceso a O365 aunque deberá ser capaz de hacerlo técnicamente en caso de que en el futuro sea necesario.

INFORME DE INSUFICIENCIA DE MEDIOS

CRTVE se ve obligada a contratar el servicio al no disponer de medios técnicos propios que puedan realizar estos servicios, siendo necesario que lo realice una empresa que disponga de la infraestructura necesaria, así como los servicios de soporte 24x7.

LOTES DE LA CONTRATACIÓN

El expediente se plantea en un único lote que ampara el servicio integral de la plataforma con los servicios de administración y soporte necesarios que debe realizar el mismo proveedor, no pudiendo dividirse en distintos lotes pues no se podría garantizar el servicio al tratarse de una solución llave en mano.

JUSTIFICACIÓN DEL PROCEDIMIENTO

Se propone el trámite de este expediente por un procedimiento abierto sujeto a regulación armonizada, ya que no se dan los requisitos que establece la LCSP, para tramitar esta contratación por otro procedimiento distinto a este referenciado previamente.

Cualquier procedimiento abierto es garantía de transparencia e igualdad de trato entre los licitadores, y además garantiza mayor concurrencia.

EXISTENCIA DE PRESUPUESTO.

El presupuesto del CECO está aprobado y contempla esta contratación:

CECO	CC01SS2350 CIBERSEGURIDAD
Cuenta de Gasto	6234003 servicios de Gestión para Áreas Técnicas

Material	8200564 servicios en la nube (cloud)
----------	--------------------------------------

El valor estimado del contrato es el siguiente:

Desglose Costes	Contrato					Posible Prorroga	Total	
	Año 1	Año 2	Año 3	Año 4	Suma	Año 5		
Servicio MFA	400.800,0	378.800,0	324.800,0	324.800,0	1.429.200,0	324.800,0	1.754.000,0	
IMPORTE TOTAL							1.754.000,0	
POSIBLE AMPLIACION							214.380,0	15%
TOTAL MAXIMO							1.968.380,0	

Desglose Costes	Contrato	Prórroga	Total
Inversión	255.000,0	30.000,0	285.000,0
Gasto	1.174.200,0	294.800,0	1.469.000,0
Importe Total	1.429.200,0	324.800,0	1.754.000,0

Este importe se ha obtenido mediante estudio de alternativas existentes en el mercado. Al tratarse de una necesidad nueva no es posible realizar una comparativa con el coste actual.