ARGANDA DEL REY
AYUNTAMIENTO

MEMORIA O PROYECTO TÉCNICO

Expte. Núm.: 209/2024/27006
Asunto: Servicio de Autenticación MFA para usuarios Ayuntamiento de Arganda del Rey.

1. OBJETO DEL CONTRATO.

Este pliego de prescripción técnicas regula la contratación del Servicio de Licencias de Autenticación fuerte MFA para la integración de seguridad en el portal de entrada de Citrix, en las conexiones remotas al Ayuntamiento de Arganda del Rey, así como la autenticación MFA en el Active Directorio y entornos de Vmware-Vsphere-Vcenter del Ayuntamiento de Arganda del Rey, bajo el régimen jurídico establecido en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

2. ALCANCE DEL CONTRATO:

El servicio deberá cumplir con los siguientes requerimientos:

a) Licencias, incluyendo:

- Servicio de Licencias de usuario de la solución Multifactor de Autenticación para un total de 155 usuarios.

DESCRIPCIÓN	Unds	OBSERVACIONES
Subscripción Licencias RSA 155 Usuarios 3 años	155	Licencias Subscripción en Cloud
IDP SMS/Voice500x N-AMER ONLY Sub1Mo	1	Mantenimiento y Soporte 36 meses
Tokens Pack de 10 Unidades	1	Tokens Autenticación RSA MFA
Servicios de Insalación del Multifactor de Autenticación para los entornos de Vmware-vSphere-vCenter	1	Servicios de Implementación MFA para los entornos Vmware-Vsphere-Vcenter
Servicios Soporte y Mantenimiento 3 años	1	infraestructura Citrix virtual apps & desktop para acceso interno al entorno de virtualización Vmware-vSphere-vCenter

- Soporte 24x7 durante 3 años por parte del fabricante de la solución.

b) Situación Actual

El Ayuntamiento de Arganda del Rey actualmente tiene implementado la solución del fabricante RSA SecurID para la autenticación de MFA en los accesos de Citrix Netscaler y MFA en el Directorio Activo.

c) Servicios a realizar:

- Servicio de renovación de 155 licencias user/device del sistema de doble (2FA) autenticación con 36 meses de subscripción para los servicios descritos anteriormente
- Despliegue del servicio de doble validación para la integración del entorno de Virtualización para los accesos del entorno Vmware-vSphere-vCenter

- Análisis y diseño correspondientes al despliegue del Multifactor de Autenticación para el entorno de Vmware-vSphere-vCenter Integración con el proveedor de SMS si fuera necesario
- Integración con la solución de Token Software y Token Hardware, si fuera necesario.
- Pruebas de aceptación y puesta en producción.
- Documentación.
- Formación Área de Informática entornos del Multifactor de Autenticación para los entornos de Vmware-vSphere-vCenter
- Servicios de Mantenimiento y Soporte por parte del Integrador.

3. ESPECIFICACIONES GENERALES .

a. El producto seleccionado deberá reunir las siguientes características:
b. La solución debe permitir configurar diferentes métodos de autenticación (OTP, Token FIDO, notificación push de biometrías o Approve…) por tipo de aplicación.
c. El fabricante de la solución deberá contar con un programa de certificación de integraciones con otras soluciones tecnológicas que faciliten dicha tarea, tanto para aplicaciones on-premise como aplicaciones cloud (ejemplos: Citrix Netscaler, Windows. Office365…) bajo el mismo licenciamiento. El fabricante debe ofrecer la documentación técnica asociada a dichas integraciones de forma pública.
d. La solución propuesta debe permitir despliegues on-premise o híbridos, sin variar el coste de las licencias.
e. La solución propuesta debe incluir, por defecto, la posibilidad de implementar un portal SSO Web.
f. La solución debe contar con un portal “Self-service” para que los empleados de la organización registren los autenticadores.
g. Los accesos al portal Web Self Service así como de administración deberá contener el 2FA u otro método para la protección del usuario.
h. La solución debe soportar los siguientes autenticadores: Token Hardware propietario, Token Software (PC, Android, iOS) propietario, token FIDO, aplicación móvil multifactor (Windows, Android, iOS) propietaria y código OTP por SMS o locución.
i. La Aplicación móvil multifactor debe concentrar, al menos, los siguientes métodos de autenticación: biométrico, notificaciones de tipo push y código OTP. La descarga de esta aplicación debe estar disponible de forma gratuita en Google Play, App Store, Microsoft Store…
j. La solución debe permitir tener y gestionar varios tipos de autenticadores bajo la misma plataforma, de forma que se puedan adaptar los autenticadores al tipo de usuario.
k. La solución debe permitir encadenar una combinación de los autenticadores anteriores para aumentar la seguridad de los accesos. Por ejemplo, Token FIDO + Aplicación móvil multifactor (MFA).
l. La solución debe permitir el licenciamiento por usuarios nominales tanto en modo perpetuo como en modo suscripción.
m. La solución debe tener la posibilidad técnica de generar políticas en base al contexto del usuario, así como soportar autenticación basada en riesgo.
n. La solución debe contar con soporte 24x7 a nivel global por parte del fabricante.
o. La solución debe poder desplegarse sobre un Appliance Hardware preconfigurado, certificado y entregado por el fabricante en caso de que no fuera posible el despliegue en servidores de propósito general, VmWare o Hyper-V.
p. El fabricante de la solución deberá contar con, al menos, 20 años de experiencia desarrollando soluciones de autenticación fuerte (2FA).

q. Deberá soportar métodos de autenticación fuertes en los cuales el usuario final no requiera el uso de telefonía móvil.

4. CARACTERÍSTICAS TÉCNICAS ESPECIFICAS:

- La solución debe soportar los siguientes autenticadores. Token hardware propietario, Token software propietario soportada en Windows, Android e iOS, token FIDO, aplicación móvil multifactor propietaria soportada en Windows, Android e iOS, SMS y locución
- La solución debe permitir poder encadenar una combinación de los autenticadores anteriores. Por ejemplo, Token FIDO + App móvil Multifactor (MFA)
- La aplicación móvil multifactor debe soportar, al menos, los siguientes métodos de autenticación en la App: biométrico, push y OTP
- La solución debe poder permitir configurar diferentes métodos de autenticación (HW token, Biométrico, OTP…) por tipo de aplicación
- La solución debe poder proteger el acceso a escritorios de usuarios al menos para los siguientes sistemas operativos: Windows 10, Windows Server 2012R2, 2016, 2019,2022, MacOS, Linux
- La solución debe proveer un mecanismo de autenticación offline, para la caso de que el escritorio esté desconectado (por ejemplo cuando se encuentra en modo avión)
- La solución debe poder integrarse con herramientas tipo SIEM, para el intercambio de información de riesgo asociado a usuarios, y definir políticas de acuerdo a este riesgo
- En caso de alojar algún servicio en cloud, éste debe estar localizado geográficamente en la Unión Europea
- La solución debe proveer un SDK que permita el desarrollo de aplicaciones móviles MFA
- MFA - Tokens de hardware con contraseña de un solo uso basada en el tiempo (TOTP)
- La Solución debe soportar como mínimo las siguientes aplicaciones:
  - Citrix Netscaler
  - Microsoft Office 365
  - Microsoft Outlook Web Access
  - ArcGis
  - Cisco Meraki
  - Webex
  - Accesos a VPN Fortinet.
  - VMware accesos Vcenter
- Se deberán especificar los importes para cada uno de los Token referenciados (Token HW, Token SW, FIDO, SMS, Voice Call, etc), dichos precios deberán ser los soportados en caso de necesitarse adquirir alguno de los token durante la vigencia del contrato.

5. DOCUMENTACIÓN.

Será necesario incluir la documentación del Plan de Instalación que especifique la implantación del equipamiento en función de las cláusulas técnicas especificadas y que además deberá contar con los siguientes apartados:

Fases del Proyecto:

La oferta deberá explicar claramente en qué consiste el proyecto de implantación:

- Tareas a realizar en cada fase.
- Planificación temporal del Proyecto (Cronograma)
- Todos aquellos componentes activos/pasivos, Hardware, Software, licencias, etc., si fueran necesarios para cumplimentar el objeto del Proyecto, incluido su puesta en marcha y funcionamiento se considerarán que están incluidos, aunque no se especifiquen.
  -

Grupo de Trabajo:

- Los técnicos participantes en el proyecto deberán acreditar tener la formación necesaria.
- La propuesta incluirá la identificación y cualificación del personal técnico asignado al proyecto.

6. DOCUMENTACIÓN INSTALACIÓN

El adjudicatario entregará a la finalización de la instalación y configuración de la instalación con las siguientes especificaciones:

- La documentación generada durante la ejecución del contrato de propiedad exclusiva del Ayuntamiento de Arganda del Rey sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización de éste, que la daría en su caso previa petición formal del contratista con expresión del fin.

- El adjudicatario se compromete a entregar toda la documentación en soporte electrónico en formato PDF, sin protección de tipo alguno.

7. ESTRUCTURA NORMALIZADA Y CONTENIDO DE LAS OFERTAS.

Con independencia de que el licitador pueda adjuntar a su oferta cuanta información complementaria considere de interés, deberá estar obligatoriamente estructurada de la siguiente forma:

Índice

7.1. Características generales

- Identificación de la oferta.
- Alcance e importe económico.
- Ofertas a módulos/componentes individuales.
- Detalle y enumeración de todos los elementos necesarios para la realización del proyecto tanto de los los elementos activos como pasivos.
- Información detallada de todo el proyecto, con indicación del número de puertos, cableado, racks, regletas de alimentación, canalización, tipos de cableado, así como de todos los elementos detallados que se incluirán en el proyecto.
- En dicho proyecto se incluirá el cronograma de ejecución del proyecto
- Acatamiento con carácter general a las condiciones del pliego.

- Datos de empresa.
- Datos de empresa/s subcontratada/s.

7.2. Descripción de la solución técnica

Se incorporará al inicio de este apartado el resumen de los aspectos más significativos y relevantes de la solución ofertada.

Se deberá incluir información detallada de la oferta en relación con los requisitos de este pliego y siguiendo su misma estructura.

7.3. Equipo de trabajo

Datos relativos al Jefe de Proyecto.

Composición del equipo de trabajo que se propone ordenado por categorías profesionales.

7.4. Organización de los trabajos

Se definirán conjuntamente con la empresa adjudicataria y el Ayuntamiento los trabajos necesarios para el despliegue de la solución.

7.5. Datos económicos

Cada oferta incorporará la proposición económica de acuerdo con lo estipulado en el Pliego de Cláusulas Administrativas y Técnicas.

8. PLAZO DE EJECUCIÓN

El plazo de ejecución del proyecto será de 30 días.

9. DURACIÓN DEL CONTRATO

La duración del contrato será de 36 meses sin posibilidad de prórroga.

10. NIVEL DE SERVICIO

El Servicio se prestará en la medida de los posible durante el horario laboral, si no fuera posible al objeto de evitar cualquier tipo de interrupción para el personal del Ayuntamiento, los trabajos deberán realizarse fuera del horario de oficina, y si fueran necesarios fin de semana o nocturnos.

En Arganda del Rey, a 17 de septiembre de 2024