Plaza de la Constitución, 1 – 28943 Fuenlabrada (Madrid)
www.ayto-fuenlabrada.es

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA IMPLANTACIÓN DE UN SISTEMA DE DOBLE FACTOR DE AUTENTICACIÓN (2FA)

Expediente: 2024/SVS/000946

1. OBJETO

El Ayuntamiento de Fuenlabrada, en su estrategia para mejorar la ciberseguridad y tomando como referencia principal el Esquema Nacional de Seguridad, precisa implantar un sistema de **autenticación de doble factor** (2FA) para las validaciones de usuarios en **conexiones locales y remotas**, tanto para trabajadores del Ayuntamiento y sus Organismos Autónomos en modalidad presencial y remota, como en la conexión de proveedores externos.

Este proyecto se incluye dentro de los proyectos de cofinanciación por la Unión Europea a través del Fondo Europeo de Desarrollo Regional "**Programa operativo FEDER 2021-2027"** de la Comunidad de Madrid , **en la Línea de Potenciación de la Administración Pública Digital orientada a Ciudadanos y Empresas** para dar así respuesta a las necesidades de la región en el ámbito de las TIC, aprovechando sus capacidades para una mejora de los procesos y de los servicios prestados a los ciudadanos, considerando las necesidades de la Administración Local en su implementación. De esta manera, las actuaciones que se vayan a financiar buscan consolidar el desarrollo de una administración electrónica interoperable a nivel regional y local a través de inversiones en infraestructuras digitales, comunicaciones, gobierno de dato e IA; desarrollo de herramientas digitales y sistemas de información inteligente (software); o creación de servicios públicos digitales orientados a la ciudadanía y empresas, entre otras opciones.

El doble factor de autenticación permitirá que los usuarios se conecten a diferentes sistemas utilizando las credenciales proporcionadas y, una vez validadas, se les solicite un segundo factor, basado en una petición a un dispositivo como por ejemplo un teléfono móvil o un token físico. Una vez aprobado el segundo factor se le permitirá realizar el acceso a los sistemas. Con estas medidas se pretende mitigar el riesgo de suplantación de identidad añadiendo un nivel de seguridad extra mediante doble factor de autenticación, lo que también podrá garantizar la mejora de la seguridad, confidencialidad e integridad y disponibilidad en el servicio que se presta a la ciudadanía.

2. ALCANCE

Se precisa la implantación de una solución que permita aumentar la seguridad de los inicios de sesión y prevenir suplantaciones de identidad y accesos no autorizados mediante un segundo factor de autenticación adicional.
El Ayuntamiento de Fuenlabrada tiene en la actualidad los siguientes sistemas en los que, al menos, se hace necesaria la implementación de este doble Factor de autenticación:

- Acceso a sistemas Windows con validación a los Directorios Activos de la organización
- Acceso a aplicaciones Microsoft 365
- Conexiones remotas VPN (actualmente se gestionan mediante un firewall del fabricante Fortinet)

Se precisan un total de **1900 licencias de software WatchGuard AuthPoint MFA.**

Se precisan un total de **250 token físicos (AuthPoint Hardware Token)** para proporcionar a los usuarios que no tienen dispositivos móviles corporativos con conexión de datos.

Plaza de la Constitución, 1 – 28943 Fuenlabrada (Madrid)
www.ayto-fuenlabrada.es

3. REQUISITOS

La solución propuesta será llave en mano. El adjudicatario realizará las configuraciones necesarias en los diferentes sistemas para la implantación del 2FA, así como la personalización y distribución de los agentes en los equipos cliente.

El plazo de implantación será de 20 días a partir de la firma del contrato (susceptible de reducción a 15 días como mejora).

3.1. REQUISITOS GENERALES

Toda la gestión, control e integración será realizada en la nube desde un interfaz web que sea multi capa y multi cliente. Además, debe permitir ser operado por múltiples administradores con diferentes tipos de perfiles basados en roles y con autenticación multi factor.

La solución deberá integrarse con varios Directorios Activos.

3.2. ACTIVACIÓN Y FUNCIONALIDADES DE AUTENTICACIÓN

El fabricante de la solución debe soportar al menos estas 3 opciones en cuanto a la autenticación:

- Token en App. Móvil, a través de una aplicación gratuita para móviles o tablets en iOS y Android.
- Token hardware TOTP fabricado por el mismo fabricante del software para garantizar la información sensible del dispositivo.
- Token hardware TOTP fabricado por un tercero con claves secretas importadas usando el formato OATH PSKC (RFC 6030)

3.3. GESTIÓN DE USUARIOS

La creación de usuarios deberá ser posible, al menos, de dos maneras:

- Manual: registrando la información de usuario que debe incluir, como mínimo, id de usuario único, correo electrónico único, nombre y apellido.
- Automática a través de:
    - Directorio Activo Microsoft
    - Directorio Activo Azure
    - Base de datos estándar LDAP

Si el usuario ha sido creado manualmente, se debe proveer de un mecanismo para cambiar la contraseña a ese usuario.

Cada usuario deberá poder tener más de un token pero cada token debe ser completamente único.

Los tokens podrán ser añadidos y borrados. Además, deberán poder instalarse en más de un dispositivo portátil: móviles, tablets, etc. pero cada uno identificado unívocamente.

Además de la creación y sincronización automática a través de un sistema externo, los usuarios podrán autenticase a través de un servicio de directorio externo.

El sistema dispondrá de un servicio proxy/Gateway que se instalará en el CPD municipal para la comunicación con un Directorio Activo/LDAP interno, evitando así conexiones directas con Internet.

Se podrá definir un intervalo en la sincronización de usuarios entre 15 minutos y 24 horas.

Todas las peticiones de autenticación que usen usuarios sincronizados deberán ser realizadas por los diferentes Directorios Activos.

Plaza de la Constitución, 1 – 28943 Fuenlabrada (Madrid)
www.ayto-fuenlabrada.es

Los usuarios sincronizados deberán de ser capaces de seguir el mismo proceso de aprovisionamiento que los usuarios creados manualmente. Además, no deberán ser borrados de la solución a menos que sean borrados de la fuente de sincronización (Directorio Activo), propagando la acción a la nube. Cuando sean borrados en Directorio Activo, no serán borrados inmediatamente de la nube si no que entrarán en un estado donde no podrán autenticase y que será fácilmente identificable. Una vez que el usuario se encuentre en este estado, se podrá borrar manualmente.

Se requiere poder hacer consultas tipo LDAP para seleccionar mejor qué usuarios serán sincronizados y, por lo tanto, reciben un token o permitir la selección por grupos existentes apareciendo automáticamente cuando se conecte con la fuente de Directorio Activo/LDAP.

3.4. CONSOLA DE CONTROL

Plaza de la Constitución, 1 – 28943 Fuenlabrada (Madrid)
www.ayto-fuenlabrada.es

Se debe proporcionar un panel de control y visualización con, al menos, las siguientes funcionalidades:

- La solución debe de permitir la configuración de políticas de autenticación basadas en grupos de usuario, recursos protegidos, funcionalidades de riesgo y métodos de autenticación a ser usados.
- En el caso de que hubiera grupos de usuarios creados manualmente o grupos de usuarios procedentes Directorio Activo, todos ellos se podrán añadir en una o más políticas.
- Los usuarios deben poder ser visualizados y gestionados tanto si están creados localmente como si son sincronizados con un directorio externo.
- La solución podrá bloquear o desbloquear manualmente usuarios o tokens

La definición de los métodos de autenticación deberá estar disponible para los administradores y estos serán, entre otros:

- Contraseña
- Autenticación basada en Push
- Autenticación basada en Desafio/Respuesta
- Contraseña única basada en tiempo

Como parte de la solución, se incluirá un interfaz que permita configurar políticas de riesgo sin coste adicional.

La plataforma ofrecerá uno o varios ayudantes virtuales para que los administradores empiecen a operar con la solución en las funciones básicas: creación de grupos, usuarios y protección de recursos.

Se deberá poder personalizar el portal de acceso web y la imagen de los correos y notificaciones PUSH.

Las configuraciones tienen que poder determinar, como mínimo:

- Intentos de inicio de sesión consecutivos que un usuario puede realizar antes de bloquearlo automáticamente
- Intentos de autenticación consecutivos con un mismo token que un usuario puede realizar antes de bloquear el token

Con el fin de prevenir riesgos asociados a ingeniería social, los administradores de la plataforma deberán poder enviar una notificación Push a cualquier usuario y recibir su respuesta para estar seguros de que alguien es quién dice ser.

Se debe soportar autenticación multifactor para las siguientes aplicaciones:

- SAML
- Soluciones basadas en RADIUS y VPNs
- Servidores y estaciones de trabajo Windows con protección de inicio de sesión
- Estaciones de trabajo macOS con protección de inicio de sesión
- ADFS (Active Directory Federated Services)
- RDP (Remote Desktop Protocol)
- RD Web
- APIs de autenticación (REST) para portales web y aplicaciones desarrolladas internamente por la empresa

Plaza de la Constitución, 1 – 28943 Fuenlabrada (Madrid)
www.ayto-fuenlabrada.es

3.5. Funcionalidades del Proxy/Gateway

La herramienta deberá de aportar un pequeño componente de software (ligero) a instalar dentro de la red de la empresa para ser usado en casos específicos como:

- Comunicación RADIUS con cortafuegos o servicios de acceso remoto (Fortinet)
- Sincronización y autenticación con servidores de Directorio Activo/LDAP

La solución deberá funcionar en Windows, incluyendo máquinas virtuales. Deberá ser posible la totalidad de la configuración de forma remota en la nube.

El registro con el cliente debe ser seguro en la nube, impidiendo intrusos que se puedan conectar desde falsos proxys o gateways.

Las versiones actualizadas del software del proxy/Gateway se debe poder descargar desde la interfaz de la nube.

Se deberá implementar un mecanismo de alta disponibilidad con al menos 2 réplicas. La segunda asumirá el control cuando el proxy/Gateway principal falle.

3.6. Funcionalidades basadas en Riesgo

Deberá ser posible definir funcionalidades de riesgo y añadirlas de manera opcional a las políticas de autenticación. Estas funcionalidades se podrán combinar dentro de una misma política.

Una funcionalidad de riesgo deberá ser la localización de la red del usuario basada en dirección IP.

Se requiere que haya una funcionalidad basada en tiempo permitiendo la configuración de horas dentro de días de la semana y horas dentro de días específicos que se asociaran a las diferentes políticas con el fin de limitar su uso.

Se requiere que se pueda limitar el acceso por país desde el que se solicita la entrada, pudiendo limitar o permitir por política.

Plaza de la Constitución, 1 – 28943 Fuenlabrada (Madrid)
www.ayto-fuenlabrada.es

3.7. INFORMES

La solución proporcionará informes para los que se podrá definir un periodo de tiempo determinado y deben incluir, al menos:

- Actividad de autenticación de los usuarios, incluyendo autenticaciones exitosas y fallidas
- Uso por aplicación o recurso protegido en términos de autenticaciones exitosas y fallidas
- Actividad de activación de token
- Veces que se deniega una notificación Push
- Actividades de sincronización de Directorio Activo o sistemas basados en LDAP.
- Alertas y Notificaciones con posibilidad de mandarlas por correo electrónico, al menos para las siguientes condiciones:
    - Usuario deniega el Push de acceso
    - El Proxy/Gateway está desconectado o ha reconectado con la nube

- Ejecución de la sincronización en Directorio Activo o solución de LDAP
- Problemas con las cuentas de usuario: expiración de subscripción, gestión de delegación, etc.

- Información sobre licencias
- Número de recursos protegidos por tipo
- Información crítica, como, por ejemplo, notificaciones de tipo Push denegadas.

Debe tener la posibilidad de exportación de logs en tiempo real, con toda la información acerca del elemento que los accionó: origen, usuario, recurso, fecha y hora, etc…

3.8. FILTRADO DE CONTRASEÑAS

3.8.1. Scan de dominio en la dark web

La interfaz web dará la posibilidad a los administradores de la plataforma de comprobar un posible filtrado de credenciales que pertenezcan al dominio del Ayuntamiento de Fuenlabrada, dando la posibilidad de advertir a los usuarios y administradores de cambiar las contraseñas.

El servició dará una lista de bases de datos comprometidas con contraseñas filtradas que estén públicamente disponibles en la dark web, donde una o más cuentas de correo electrónico del domino han sido expuestas.

La plataforma deberá tener disponible un informe completo con todas las cuentas de correo expuestas y la correspondiente brecha de seguridad.

El informe anonimizará cualquier tipo de información personal.

El servicio se dará desde el mismo fabricante, con las bases de datos comprometidas estando seguras y actualizado cuando una nueva brecha de seguridad relativa a las contraseñas esté disponible en la dark web.

3.8.2. Scan de correo electrónico en la dark web

La interfaz web dará la posibilidad a los administradores de la plataforma de comprobar un posible filtrado de credenciales que pertenezcan a cuentas de correo electrónico específicas.

El servició dará una lista de bases de datos comprometidas con contraseñas filtradas que estén públicamente disponibles en la dark web, donde la dirección de correo electrónico buscada ha sido expuesta.

El servició comunicará, solo al propietario de la cuenta de correo electrónico y al personal que se especifique del Departamento STIC, un informe completo con la lista de brechas y parte de

Plaza de la Constitución, 1 – 28943 Fuenlabrada (Madrid)
www.ayto-fuenlabrada.es

las contraseñas expuestas para que el usuario compruebe si están siendo usadas en alguna otra credencial.

El informe no contendrá ningún tipo de información personal o de cualquier otro ámbito.

El servicio se dará desde el mismo fabricante, con las bases de datos comprometidas estando seguras y actualizado cuando una nueva brecha de seguridad relativa a las contraseñas esté disponible en la dark web.

4. FORMACIÓN

La oferta deberá incluir y especificar un mínimo de 1 jornada (de cuatro horas de duración mínima) de formación necesaria para realizar una transferencia de conocimiento que permita la explotación posterior del sistema por técnicos del Ayuntamiento de Fuenlabrada.

Por otra parte, el adjudicatario deberá elaborar y proporcionar una documentación o tutoriales que permita a los usuarios finales, de una forma sencilla, entender y utilizar los diferentes métodos de autenticación.

5. SOPORTE TÉCNICO 24x7x365

Se proporcionará el mantenimiento y asistencia técnica que permita asegurar el correcto funcionamiento, actualizaciones necesarias y consultas del Departamento STIC, así como la ayuda a la resolución de incidencias que se puedan presentar durante la duración del contrato.

El servicio contemplará:

- Soporte ofertado por el fabricante, por teléfono y en castellano,
- Service Packs y hotfixes: acceso a las mejoras técnicas del producto durante el tiempo de activación del servicio
- Web de soporte: Acceso a foros, blogs, información sobre últimas amenazas, enciclopedia de virus, informes, …
- Soporte técnico vía email por técnicos certificados en la solución implementada
- Acceso ilimitado al Helpdesk: sin límite de incidencias.

6. OBLIGACIONES DEL ADJUDICATARIO

La prestación de este servicio no creará, en ningún caso, ni bajo ninguna circunstancia, ningún vínculo laboral entre el personal técnico, asignado al proyecto por el empresario, y el Ayuntamiento de Fuenlabrada.

Plaza de la Constitución, 1 – 28943 Fuenlabrada (Madrid)
www.ayto-fuenlabrada.es

El contratista deberá cumplir, bajo su exclusiva responsabilidad, las disposiciones vigentes en materia laboral, de seguridad social y de prevención de riesgos laborales, debiendo tener a su cargo el personal necesario para la realización del objeto del contrato, respecto del que ostentará, a todos los efectos, la condición de empresario y asume la obligación de ejercer de modo real, efectivo y continuo el poder de dirección inherente a todo empresario.

Cuando la prestación del servicio objeto del presente contrato exigiera una contribución neta de recursos mayor a la prevista, por un periodo breve y determinado de tiempo, la empresa adjudicataria se compromete a aportar los recursos necesarios sin coste adicional.

7. SIGILO Y CONFIDENCIALIDAD DE LA INFORMACIÓN TRATADA

La empresa adjudicataria y el personal encargado de la realización de las tareas guardará secreto profesional sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligado a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.

Esta obligación no se limita al tiempo de ejecución del correspondiente contrato al que está asociado el proyecto indicado, sino que deberá ser respetada aun después de su cumplimiento o resolución.

Cualquier Información, fuese cual fuere su naturaleza (bien técnica, comercial, financiera, operacional o de otro tipo), en cualquier forma o soporte (ya sea verbal, escrita, grabada o de cualquier otro tipo), que pudiera ser facilitada por el Ayuntamiento de Fuenlabrada o cualquier tercero que tenga relaciones contractuales con el mismo, en relación con el objeto del presente pliego, será considerada como “Información Confidencial”, incluyéndose en esta categoría aquella información que fuese generada a partir de la Información Confidencial.

El adjudicatario y el personal encargado de la realización de las tareas se obligan a:

1. Utilizar o transmitir la Información Confidencial exclusivamente para los fines del objeto del contrato;

2. Restringir el acceso a la Información Confidencial únicamente a aquellas personas que necesiten conocerla para los fines del objeto del contrato, y asegurarse de que dichas personas conocen las obligaciones que les resultan aplicables en virtud de lo establecido en el presente documento;

3. No facilitar Información Confidencial a tercero alguno sin el previo consentimiento escrito del Ayuntamiento de Fuenlabrada, y asegurarse de que, en caso de haber obtenido dicha autorización, dicho tercero firma un compromiso de confidencialidad en términos equivalentes a los del presente documento.

Plaza de la Constitución, 1 – 28943 Fuenlabrada (Madrid)
www.ayto-fuenlabrada.es

8. GARANTÍAS DE BORRADO DE LOS DATOS AL RESOLVER EL CONTRATO

Una vez resuelto el contrato el proveedor del servicio no podrá conservar ningún dato, debiendo prever mecanismos que garanticen el borrado seguro de los datos cuando lo solicite Ayuntamiento de Fuenlabrada.

Estos mecanismos serán descritos en la oferta, siendo requerido al proveedor a la terminación del contrato una certificación de la destrucción de todos los datos. Certificación donde también se garantice, en caso de haber realizado subcontrataciones, que los subcontratistas han borrado los datos a los que hayan tenido acceso.

9. ETIQUETADO E INVENTARIADO.

Los elementos a suministrar deberán estar inventariados por lo que será necesario, para su control, disponer de la relación de números serie en formato CSV o similar.

10. LUGAR DEL SUMINISTRO.

Los elementos a suministrar se entregarán en la Casa Consistorial del Ayuntamiento de Fuenlabrada (Plaza de la Constitución, 1, Fuenlabrada)

En Fuenlabrada, a la fecha que figura en el pie de este documento que se firma electrónicamente con Código Seguro de Verificación.

Fdo.: José Martínez Castrejón
Técnico grado medio TIC

Plaza de la Constitución, 1 – 28943 Fuenlabrada (Madrid)
www.ayto-fuenlabrada.es