PRESCRIPCIONES TÉCNICAS PARA EL CONTRATO DE LA PRESTACIÓN DEL SERVICIO PARA INSTALAR UN SIEM (Security Information and Event Management), Y EL SUMINISTRO DE 600 AUTHPOINT HARDWARE TOKEN, SISTEMA DE ACCESO DOBLE FACTOR DE AUTENTICACIÓN – HERRAMIENTAS CCN-CERT, PARA EL AYUNTAMINTO DE CIUDAD REAL. Este contrato está cofinanciado con 40.900,00€, por el Plan de Recuperación, Transformación y Resiliencia.

Este proyecto se encuadra en el Plan de recuperación, transformación y resiliencia. Componente 11. Línea 5.- Proyecto Ciberseguridad.

PRIMERA.- ANTECEDENTES.

La infraestructura que este Ayuntamiento tiene es la siguiente:

- Máquinas virtualizadas en un cloud privado. La línea de comunicación entre el cloud y el Ayuntamiento es una línea punto a punto layer 2. de 1 Gb.
- En estas máquinas se tienen diferentes servidores: servidor de aplicaciones, servidor de Base de Datos, Servidor de activo directorio. Servidor de datos, etc. De estos servidores se hacen copia diaria y en dos sitios diferentes.
- Las aplicaciones con servicios web, están instaladas en un DMZ.
- En el Ayuntamiento está instalado de una forma centralizada, el Servidor de correo, el servidor Proxy, el servidor de control de tráfico de comunicaciones, y el servidor de la gestión de impresión centralizada con el software de Paper Cut.
- Las comunicaciones internas entre el Ayuntamiento y sus 50 sedes es mediante una Red de datos, en cada punto están tunelizadas y encriptada la información, con equipos certificados con el Esquema Nacional de Seguridad.
- De una forma centralizada tenemos distribuido el paquete de software de seguridad Nod32, mediante la herramienta ESET remote administrador.
- De igual manera, a través de la gestión de políticas, tenemos distribuidos la herramienta Microclaudia, herramienta facilitada por el Centro Criptológico Nacional (CCN-CERT). Centro de vacunación que proporciona protección frente a los malware de código ransomware. Esta protección está dirigida a los sistemas Windows y funciona mediante el uso de un agente ligero que se encarga del despliegue y la ejecución de las vacunas.
- Este Ayuntamiento tiene instalada un Dispositivo NAS de Sysnology, de varios discos en raid 5, con una capacidad de 45 Tb. En esta unidad se hacen copias de todos los discos de sistemas de los equipos del parque informático. Está programada para que una vez a la semana se realice copia de cada disco "C", (se mantienen las últimas 10 versiones).
- Hace unos meses, se adjudicó el proyecto de la puesta en marcha del ESQUEMA NACIONAL DE SEGURIDAD, desde la fecha de adjudicación se está trabajando en adaptar los sistemas a la normativa del citado ESQUEMA.
- Se detalla a continuación los trabajos que se están llevando a cabo a raíz de la Auditoria de Seguridad, con el objetivo de obtener el ESQUEMA NACIONAL DE SEGURIDAD.

- El Ayuntamiento de Ciudad Real, ha concluido y está en proceso de realización de diversos trabajos encaminados a la mejora de la ciberseguridad frente a amenazas, ataques y mejora de la respuesta y tratamiento de los incidentes. Los citados trabajos son:

- Microclaudia, sistema desplegado.
- LUCIA, sistema en proceso de implantación.
- Sonda SAT-INET, en proceso de implantación.
- Adecuación Esquema Nacional de Seguridad, para lo que se ha contratado los servicios de una consultora con la que se está trabajando.
- SOC, se dispone del servicio SOC prestado y coordinado con la empresa encarga de los sistemas de seguridad del Ayuntamiento.

SEGUNDA.- OBJETO DE CONTRATO.

Es objeto del presente contrato garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por las Administraciones Pública, y mejorar sus capacidades de prevención, detección y respuestas ante incidentes de ciberseguridad. Refuerzo de la ciberseguridad.

La necesidad del mismo se ha detallado en el punto de Antecedentes. Actualmente se está trabajando para conseguir el citado objetivo, entre las tareas que se están realizado, es la puesta en marcha del ESQUEMA NACIONAL DE SEGURIDAD, paralelamente se instalarán las herramientas definidas en el punto anterior, y uno de los puntos débiles que tenemos es la autenticación en nuestros sistemas, por ello pretendemos mejorarlo con un sistema de acceso doble factor de autenticación, ya que identificamos una serie de problemas en relación a la identificación-contraseñas, y se espera paliar con la implantación del citado doble factor de autenticación.

En el mismo contrato, se adjudicará una prestación de servicio para la instalación de un SIEM (Security Information and Event Management), software que analiza y almacena toda la actividad que sucede en la Infraestructura IT, del Ayuntamiento de Ciudad Real, con el objetivo de detectar posibles amenazas y evitar ciberataques.

Este contrato consta de 2 Lotes:

-Lote 1- Adquisición de 600 licencias de sistemas de doble factor de autenticación y 600 AuthPoint Hardware Token.

-Lote 2- Prestación servicio de una solución de ciberseguridad. Instalación de un SIEM, software que analiza y almacena toda la actividad que sucede en la Infraestructura IT, del Ayuntamiento de Ciudad Real.

TERCERA.- ETIQUETADO DIGITAL E HITOS DEL CONTRATO.

La presente actuación financiada el Plan de Recuperación, Transformación y Resiliencia – Componente 11 - por la Unión Europea – NextGenerationEU, queda definida en Resolución de concesión de Ayudas "Mediante orden TER/1204/2021, de 3 de noviembre, se aprobaron las bases reguladoras y se efectuó la convocatoria correspondiente a 2021, de subvenciones destinadas a la transformación digital y modernización de las Administraciones de las Entidades Locales, en el marco del Plan de Recuperación, Transformación y Resiliencia (BOE 6 de noviembre de 2021).

Etiquetado digital: Coeficiente para el cálculo de la ayuda a la transición digital 100%.
Los hitos de los que partimos para la celebración de este contrato son los siguientes:

Hito	Descripción del hito	Resumen	Fecha Límite	Formas de verificación
1	Licitación	Anuncio Licitación	30/07/2022	Publicación Plataforma Contratación.
2	Adjudicación Propuesta	Acuerdo de Adjudicación	25/09/2.022	Certificación Acuerdo de Adjudicación JGL.
3	Suministro, configuración de las llaves, y la Instalación y configuración del SIEM	Suministro Llaves, y configuración del Sistema (llaves y SIEM).	15/10/2.022	Fecha Inicio de trabajos de configuración. Acta de recepción.
4	Finalización y Puesta en Marcha	Acta de recepción de todos los trabajos.	30/12/2.022	Fecha de finalización.

LOTE – 1

CUARTA.- REQUERIMIENTO SOLUCIÓN MULTI-FACTOR.

- Solución de Multi-Factor de Autenticación basada en la nube.

La organización necesita implementar una solución de autenticación multi-factor para VPN/acceso remoto, aplicaciones en nube, protección de acceso a servidores y estaciones además de a portales web y aplicaciones que puedan ser desarrollados internamente. Es requisito que toda la gestión, control e integración esté realizada en la nube.

- Gestión centralizada en la nube.

Toda la gestión se debe poder realizar desde un interfaz web que sea multicapa y multi-cliente. Además, debe de permitir ser operado por múltiples administradores con diferentes tipos de accesos basados en roles y con autenticación multi-factor.

El panel de control y visualización debe de proveer, al menos, las siguientes funcionalidades:

- Autenticaciones establecidas y con éxito y falladas.
- 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 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.

Los logs deben de ser exportables y en tiempo real, con toda la información acerca del elemento que los accionó: origen, usuario, recurso, fecha y hora, etc.

Se debe de soportar multi-factor de autenticación 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.
- RDP.
- RD Web.
- APIs de autenticación (REST) para portales web y aplicaciones desarrolladas internamente por la empresa.

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 de estar visualizados y gestionados tanto si están creados localmente o sincronizados con un directorio externo.

La definición de los métodos de autenticación deberá de estar disponibles 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 de poder personalizar con el portal de acceso web y la imagen de los correos y notificaciones PUSH.

Las configuraciones tienen que poder determinar:

- 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.

Los informes a proveer por la herramienta durante un periodo de tiempo determinado deben de 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.

- Gestión de usuarios.

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

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

Si el usuario ha sido creado manualmente, se debe proveer un mecanismo a ese usuario para cambiar la contraseña. Cada usuario deberá poder tener más de un token pero cada token debe de 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.

La solución podrá bloquear o desbloquear manualmente usuarios o tokens.

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 parque de la empresa para la comunicación con un Directorio Activo/LDAP interno, evitando así conexiones con Internet.

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

Las contraseñas de usuarios externos (sincronizados a través de LDAP o Directorio Activo) no se almacenarán nunca en la nube. Todas las peticiones de autenticación que usen usuarios sincronizados deberán ser realizadas por el Directorio Activo.

Los usuarios sincronizados deberán de ser capaces de seguir el mismo proceso de aprovisionamiento que los usuarios creados manualmente. Además, no deberán de ser borrados de la solución al 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. La sincronización debe de poder ser probada antes de ser aplicada para comprobar su correcto funcionamiento.

- Funcionalidades SAML.

La herramienta debe soportar SAML 2.0 y actuar como Proveedor de Identidad (IdP) para poder ser integrada con aplicaciones en la nube que soporten SAML 2.0

Se debe de proporcionar una URL única como portal de autenticación para los usuarios (SAML IdP), y que pueda ser configurada para usar, al menos, los siguientes métodos de autenticación multi-factor:

- Basado en Push (online)
- Basado en Desafío/Respuesta (offline)
- Contraseña de uso único basada en tiempo (offline)

El portal SAML IdP debe de estar automáticamente provisionado en la nube, no en las instalaciones de la empresa y sin la necesidad de instalar servidores web o certificados auto firmados.

Los usuarios creados manualmente podrán cambiar sus password con posterioridad. Después de la autenticación, el usuario podrá ver la lista de aplicaciones a las que tiene acceso. Estas

aplicaciones deberán de ser mostradas con una interfaz amigable y presentando el icono de la aplicación junto con el nombre.

Las aplicaciones deben de estar integradas usando SAML para que los usuarios puedan acceder a todas ellas de una vez (single sign-on).

SAML requiere soportar la funcionalidad SAML logout para que cuando un usuario cierre la sesión de una aplicación protegida, la sesión con el portal SAML también termina.

Se requiere una posibilidad de integración con terceras partes usando dos métodos posibles:

- Configuración manual obtenida de un fichero de metadatos
- A través de una URL con metadatos

El fabricante deberá de aportar los pasos o guías anteriormente usadas en integraciones SAML con empresas externas o terceras partes (al menos 75). Estas empresas externas o terceras partes incluirán (entre otras): Microsoft 365, Box, Salesforce, Citrix, Dropbox, etc

Para Microsoft 365, deberá de soportar Autenticación Básica o Moderna. La opción Básica debería de ser considerada opcional.

- Funcionalidades VPN, Acceso Remoto y RADIUS.

La solución debe soportar autenticación RADIUS a través de un servicio proxy/Gateway y no directamente en la nube, por razones de seguridad.

El servicio de RADIUS deberá ser considerado y presentado como un servidor RADIUS, recibiendo peticiones dentro de la red y enviándolas de forma segura a la nube. El puerto usado en la comunicación RADIUS debe de ser configurable. Toda la configuración del servicio RADIUS debe de ser a través de la nube, evitando así la necesidad una gestión local o scripts.

El servicio RADIUS debe ser capaz de funcionar con los principales fabricantes de cortafuegos para Acceso Remoto y VPN.

Los métodos de autenticación del servicio RADIUS podrán ser (uno u otro):

- Contraseña seguida de una contraseña de uso único (OTP).
- Contraseña seguida de una confirmación de llegada de autenticación Push.

El servicio RADIUS deberá soportar VPNs PAP y MSCHAPv2, incluyendo IPSec, SSL-VPN, L2TP e IKEv2. Si los servicios de multi factor de autenticación y los servidores de acceso remoto/cortafuegos/UTMs son del mismo fabricante, deberá de ser posible una integración directa y única evitando el uso de un servidor RADIUS.

- Funcionalidades del Proxy/Gateway.

La herramienta deberá 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.
- Sincronización y autenticación con servidores de Directorio Activo/LDAP.

La solución deberá de 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. Los logs deben ser almacenados localmente.

El software del proxy/Gateway se debe poder descargar desde la interfaz de la nube. La última versión debe estar disponible en el caso de que no estuviera instalada. Se podrá implementar un mecanismo de alta disponibilidad con al menos 2 réplicas. La segunda asumirá el control cuando el proxy/Gateway principal falle.

- Funcionalidades basadas en Riesgo

Deberá ser posible una manera de definir funcionalidades de riesgo y añadirlas de manera opcional a las políticas de autenticación. Estas funcionalidades deberán poder combinarse 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 hora 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 donde se solicita la entrada, pudiendo limitar o permitir por política.

- Integraciones Adicionales.

Se requiere de un agente para Microsoft ADFS (Active Directory Federation Services) que permita la definición, a través de ADFS, de grupos de usuarios que usarán multi factor de autenticación. Esta integración deberá de proporcionar un interfaz que se pueda configurar con todas las opciones de autenticación: contraseña de uso único, Desafío/Respuesta y Push.

También se proporcionará un agente para Microsoft RD Web y acceso seguro.

Las APIs de autenticación, que usarán REST, estarán disponibles para la integración con aplicaciones tales como portales web y aplicaciones desarrolladas por la empresa.

- Funcionalidades Ventajosas.

Disponer de la capacidad de modificar el aspecto de la herramienta y añadidos con elementos corporativos, por ejemplo, logotipos.

Proveer localización lista para usar con todos los mensajes, al menos, en los siguientes idiomas para las aplicaciones del usuario final (IdP, email de activación, token, etc): inglés, español, francés, alemán, italiano, portugués, holandés, chino, coreano y thai.

- Factor de Autenticación.

Esta solución deberá aportar un factor de autenticación usando un token en una aplicación móvil junto con contraseña de uso única basada en OATH.

- Activación y Funcionalidades de Autenticación.

El fabricante de la solución debe soportar, al menos 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.
- TOTP hardware token, fabricado por el mismo fabricante para garantizar la información sensible del dispositivo.
- TOTP hardware token fabricado por un tercero con claves secretas importadas usando el formato OATH PSKC (RFC 6030).

La aplicación móvil deberá de soportar:

- Autenticación basada en Push (online).
- Autenticación basada en Desafío/Respuesta (offline) usando un código QR encriptado para reducir los ataques de ingeniería social.
- Contraseña de uso único (OTP).

Las autenticaciones basadas en Push deberán incluir contraseñas de uso único en la respuesta cuando la autenticación es aprobada. Estas autenticaciones deberán funcionar independientemente de

que los servicios de Apple o Google se vean afectados en su entrega. La aplicación deberá recuperar la información de la nube en unos pocos segundos garantizando el 100% de su efectividad.

Además, será necesario aportar una manera de comprobar (a través de la aplicación móvil) si el dispositivo ha sido modificado (rooteado, jailbreak, etc) o si tiene algún software malicioso instalado.

Debe ser capaz de funcionar con una activación online segura sin necesidad de que el usuario escriba nada. Las opciones de activación serán dos:

- Activación única a través de un link de correo electrónico
- Activación única a través de un código QR que será accesible a través de un portal

Cuando la activación sea a través de correo electrónico, debe soportar 2 opciones adicionales para que el usuario pueda activarlo a través de la pantalla del ordenador personal o el dispositivo:

- Un enlace, el cual, cuando sea ejecutado a través del dispositivo, deberá activar el token
- Un código QR que pueda ser leído a través de una pantalla

No habrá tokens disponibles en la activación a través de código QR o enlace de correo electrónico.

La activación siempre tendrá lugar en línea y la solución deberá asegurar que las credenciales de activación son usadas una única vez. Las credenciales del token deben ser creados usando el estándar DSKPP (OATH DSKPP – RFC 6023).

Deberá haber una opción para la personalización de la marca, pudiendo así definir la imagen por defecto y la etiqueta para el token móvil durante la activación.

Se requieren también la opción de usar tokens de hardware basados en 6 dígitos conforme al estándar OATH RFC 6238. Los tokens de hardware se provisionarán internamente de manera automática si son vendidos por el fabricante de la solución, o usando archivos semilla siguiendo el estándar OATH PSKC RFC 6030.

- Funcionalidades de Seguridad.

Las autenticaciones basadas en notificaciones tipo Push y en código QR deberán incluir al menos, el nombre del usuario intentando autenticarse, el día y la hora y el recurso al que se está accediendo.

Para autenticación SAML, la notificación Push y el mensaje del código QR tienen que incluir también detalles acerca de la localización física del dispositivo y navegador Web que intenta conectar.

Para autenticaciones en Windows y macOS, la notificación Push y el mensaje del código QR deberá incluir el nombre del dispositivo, sistema operativo y localización si es posible de determinar.

Los mensajes tipo Push y código QR deberán estar encriptados de manera que solo el usuario con el token correcto será posible de descifrarlos.

La protección de tokens se podrá hacer a través e PIN, individualmente. Además, si el dispositivo lo permite (Android o iPhone) se podrá proteger el token con huellas dactilares o reconocimiento facial.

Se requiere un método para identificar el token unívocamente en el dispositivo (DNA móvil).

Se podrá generar contraseñas de un solo uso inválidas si alguien es capaz de clonar la aplicación o el dispositivo, por completo, en otro.

No se podrán copiar o restaurar tokens en otro dispositivo.

Para migraciones seguras de tokens, se deberá de poder borrar el token del dispositivo antiguo y generar el nuevo token con nuevas semillas en el nuevo dispositivo.

Estas migraciones seguras deben de estar disponibles tanto cuando se quiera migrar un token o múltiples al mismo tiempo.

- Funcionalidades Ventajosas y de Usabilidad.

La localización incluirá mensajes, en al menos los siguientes lenguajes para aplicaciones de cara al usuario final (IdP, email de activación, aplicación móvil para el token, Agentes de inicio de sesión): inglés, español, francés, alemán, italiano, portugués, holandés, chino, coreano y thai.

Deberá permitir la instalación de software de terceros (Google Authenticator) con tokens compatibles para uso personal.

Los tokens compatibles de Google Authenticator podrán ser importados y restaurados de forma segura en diferentes dispositivos.

Además, se podrá personalizar el nombre del token y la imagen para mejor identificación por parte del usuario.

- Protección de inicio de sesión en Windows.

Se deberá poder instalar un agente en portátiles con Windows, servidores y estaciones para añadir funcionalidades de Windows Logon.

Deberá proteger el equipo cuando se reinicie o se bloquee.

El dominio y las cuentas locales deben estar protegidas con multi factor de autenticación.

Las versiones de Windows soportadas como mínimo deben de ser: Windows 8.1, Windows 10 y Windows Server 2008/2012/2016/2019.

Deberá soportar modos de funcionamiento online y offline:

- Online: cuando hay conexión disponible a Internet desde el equipo.
- Offline: cuando no hay conexión disponible a Internet desde el equipo.

El modo online deberá soportar autenticación basada en Push. El modo offline deberá soportar código QR and contraseña de un solo uso temporal (móvil o token hardware) como autenticaciones, donde en ambos casos, no requerirá conexión de datos con el teléfono móvil.

Deberá aparecer como un dialogo completo solo después de una autenticación de Windows, pero antes de completar el proceso de inicio de sesión.

No requerirá de conexión a Internet para validar la contraseña de Windows.

El software de protección de Windows estará disponible para descargar desde la nube y deberá ser la última versión disponible para Windows de 32 y 64 bits.

La instalación de podrá hacer en modo silencioso. Si el usuario pierde su token o dispositivo móvil, se dispondrá de un mecanismo seguro temporal de inicio de sesión sin multi-factor de autenticación.

El habilitar este modo de funcionamiento sin token, se hará de modo seguro, utilizando un Desafío/Respuesta y sin requerir conexión a Internet. Será necesario la aprobación de un administrador.

Este inicio de sesión sin login deberá llevar asociado cuando tiempo, en horas, está habilitado.

Este modo se deshabilitará automáticamente cuando el tiempo especificado se cumpla o la próxima vez que el usuario utilice el token.

Se deberá proteger el acceso por escritorio remoto (RDP) sin la necesidad de escribir otra vez el usuario y la contraseña. También se concederá acceso RDP a dispositivos protegidos con Microsoft RD web y Microsoft RD Gateway.

La herramienta permitirá la definición de usuarios específicos que no utilizarán multi-factor de autenticación, a través del portal de gestión en la nube. Estos usuarios podrán iniciar sesión solo en dispositivos concretos y de modo puntual.

- Protección de inicio de sesión en macOS.

Se deberá poder instalar un agente en estaciones con macOS para añadir funcionalidades de Windows Logon.

El agente deberá proteger el equipo cuando se reinicie o se bloquee.

Deberá soportar modos de funcionamiento online y offline:

- Online: cuando hay conexión disponible a Internet desde el equipo.
- Offline: cuando no hay conexión disponible a Internet desde el equipo.

El modo online deberá soportar autenticación basada en Push.

El modo offline deberá soportar código QR and contraseña de un solo uso temporal (móvil o token hardware) como autenticaciones, donde en ambos casos, no requerirá conexión de datos con el teléfono móvil.

No requerirá de conexión a Internet para validar la contraseña.

El software de protección de macOS estará disponible para descargar desde la nube y deberá ser la última versión disponible.

La instalación de podrá hacer en modo silencioso.

Si el usuario pierde su token o dispositivo móvil, se dispondrá de un mecanismo seguro temporal de inicio de sesión sin multi factor de autenticación.

El habilitar este modo de funcionamiento sin token, se hará de modo seguro, utilizando un desafío/respuesta y sin requerir conexión a Internet. Será necesario la aprobación de un administrador.

Este inicio de sesión sin login deberá llevar asociado cuando tiempo, en horas, está habilitado. Este modo se deshabilitará automáticamente cuando el tiempo especificado se cumpla o la próxima vez que el usuario utilice el token.

- Filtrado de contraseñas.

- 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 de la empresa, 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.

- 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, un informe completo con la lista de brechas y parte de 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.

- Formación

Se considerarán incluidas en el alcance del contrato las acciones formativas destinadas tanto a la correcta utilización, servicios, como a la administración y al mantenimiento del mismo.

- El adjudicatario será responsable de impartir esta formación y de proporcionar todos los medios materiales y personales necesarios para la correcta realización de la formación, estando todos los trabajos de formación incluidos en el precio de la oferta.
- Los trabajos de formación no podrán ser subcontratados ni se utilizará una plataforma digital.
- La formación será impartida por los mismos técnicos que realicen la implantación y mantenimiento para un mejor entendimiento y acceso directo por parte del Ayuntamiento.
- Deberá incluirse en la oferta el número de jornadas formativas y el perfil destinatario de cada una. Siendo un mínimo de 20 horas. Distribuidas en jornadas de 3 a 5 horas como máximo y no más de 2 días a la semana.
- La acción formativa se desarrollará dentro del primer mes de implantación.
- La distribución del número de horas y jornadas será a criterio del Ayuntamiento.
- Se deberá entregar manuales y documentos técnicos, en formato electrónico, con información relativa a los Sistemas, accesos y herramientas necesarias para la gestión. Estos documentos serán mantenidos y actualizados, con control de versiones por el adjudicatario durante la vigencia del contrato.

La empresa adjudicataria deberá disponer del certificado ISO 27001.

Para la puesta en marcha de esta solución, y con el objetivo de no hacer imprescindible el uso de un teléfono móvil personal, es necesaria la compra de:

Adquisición de 600 Licencias AuthPoint.
Adquisición de 600 AuthPoint Hardware Token.

LOTE – 2

QUINTA.- REQUERIMIENTO SOLUCIÓN DE CIBERSEGURIDAD PARA LA INSTALACIÓN DE UN SISTEMA SIEM.

Todos los sistemas informáticos se enfrentan a la necesidad de detectar y responder a los ataques en tiempo real. La realidad es que se tardan un tiempo en detectar una violación de la seguridad, tiempo que hay que reducir o eliminar para una respuesta rápida que proteja los sistemas y la información.

Igualmente, los sistemas informáticos requieren de un análisis profundo de la actividad en busca de situaciones, tráfico y acciones sospechosas para prevenir ataques o analizar en profundizar las causas y vectores de los ataques recibidos.

En la actualidad los sistemas instalados afrontan las amenazas con criterios y sistemas de Ciberseguridad. Se pretende avanzar un nivel para mejorar de forma proactiva la seguridad y utilizar criterios y herramientas de ciberinteligencia.

Ciberseguridad.

- El objetivo de la ciberseguridad, es proteger la información y los equipos informáticos.
- Activa procesos para solucionarlos distintos problemas que se generan ante un ataque, intrusión o por la mala utilización de un equipo.

Ciberinteligencia.

- Ayuda a la ciberseguridad para adelantarse con acciones de seguridad y fortalecer la protección
- En su estrategia de inteligencia utiliza la información para detectar amenazas y les permite situarse en una posición de ventaja para adelantarse a los riesgos.

El Ayuntamiento de Ciudad Real en su compromiso por la mejora de la seguridad informática viene realizando diversas actuaciones. Entre ellas el Ayuntamiento de Ciudad Real requiere la compra e instalación de un sistema SIEM.

SIEM (Security Information and Event Management) es un software que analiza y almacena toda la actividad que sucede en la infraestructura IT de una organización con el objetivo de detectar posibles amenazas y evitar ciberataques.

El SIEM pretende detectar de forma proactiva amenazas potenciales mediante la correlación de eventos. Para poder realizar estas acciones necesita procesar y monitorizar una gran cantidad de datos provenientes de múltiples fuentes de información.

En la actualidad el Ayuntamiento de Ciudad Real cuenta con un SOC externo (Centro de Operaciones de Seguridad se encargan de realizar un seguimiento y analizar la actividad en redes).

Entre las actividades que realiza se encuentra:

- Vigilancia y detección de amenazas en las actividades diarias de los sistemas de información y comunicaciones.
- Análisis de ataques y posibles amenazas
- Recuperar información perdida o dañada como consecuencia de ataques.
- Mejorar la capacidad de respuesta ante cualquier ataque.

La infraestructura del Ayuntamiento de Ciudad Real está basada en dispositivos Appliance SCCIM familia 200, 300 y 400. Siendo la familia 400 la implantada en los sistemas de firewall externo, firewall interno, servidor de túneles, servidor de correo, servidor proxy, Huawei, Active Directory.

Un SIEM recibe toda la información de los diferentes dispositivos/sistemas conectados, así como de los servidores, conexiones y cualquier elemento capaz de ofrecer información. Por tanto, el Ayuntamiento requiere un SIEM que pueda recibir, analizar y actuar sobre los dispositivos instalados. Es obligatorio que si fuera necesario cuente con las correspondientes certificaciones de los fabricantes como en el caso de los dispositivos de seguridad SCCIM.

Dentro de los tipos de seguridad informática, estaría englobada en los que se denominan Seguridad Pasiva, ya que tiene una función enfocada a la detección de amenazas.

Mediante técnicas de analítica integrada en el software, almacena estos datos para normalizarlos y establecer patrones que permitan descubrir desviaciones de la tendencia cuando estas pudieran resultar sospechosas.

El SIEM requerido debe cumplir las siguientes características:

- Software libre, se ofrecerá todo el código del software para su análisis y mejora.
- Plugins para fuentes de los sistemas actualmente instalados Cisco, VWMare, SCCIM, Huawey.
- Junto con el personal del Ayuntamiento, definir el alcance del proyecto, planificar las fases.
- Definir un set inicial de reglas que cubra las necesidades de detección. Este set de reglas podrá ampliarse en fases posteriores del proyecto, incluso combinarlo con trabajos de "caracterización de amenazas" para conocer qué gaps tenemos.
- Evaluar regularmente el funcionamiento del SIEM, incluir nuevas reglas de detección (casos de uso) lo cual redundará en una mejor postura de defensa de la organización
- Multiples licencias de dispositivos, posibilidad de instalar varios con correlación entre ellos. Se requerirá un mínimo de 20 dispositivos soportados.
- Sistema validado para la interacción con el SOC actualmente disponible.
- Personalización y programar reglas de detección que ayuden en la detección de acciones maliciosas.

Para la implantación y mantenimiento se requerirá:

a) Evaluación las necesidades, recursos disponibles y el nivel de madurez de la organización para determinar la integración correcta del SIEM. Realización de un informe de inicio y fin.
b) Evaluación del almacenamiento y hardware necesario, implantando un mínimo.
c) Puesta en marcha, configuración e integración.
   La puesta en marcha se realizará por personal técnico presencial en las instalaciones del Ayuntamiento de Ciudad Real con una reserva de 100 horas.
d) Formación en el despliegue y capacitación al personal del Ayuntamiento de Ciudad Real con sesiones de formación de máximo tres horas y dos días a la semana hasta un total de 100 horas. La formación será realizada por los mismos técnicos que realicen la implantación para una mejora calidad
e) Actualización del software e integración continuas mejoras.
f) Actualización continua de reglas. Evaluar regularmente el funcionamiento del SIEM, incluir nuevas reglas de detección
g) Soporte continuo 24x7 ante incidencias, consultas, etc. Integración continua de cuantos dispositivos se requieran.
h) Identificamos de posibles problemas y soporte para responder de forma ágil.
i) Un número de horas suficiente para la atención y soporte, incluyendo la formación necesaria para la implementación de nuevas reglas y métodos.

La empresa adjudicataria deberá tener una experiencia demostrada de al menos 5 años y disponer de certificado ENS nivel medio y certificado ISO 27001.

- Formación

Se considerarán incluidas en el alcance del contrato las acciones formativas destinadas tanto a la correcta utilización, servicios, como a la administración y al mantenimiento del mismo.

- El adjudicatario será responsable de impartir esta formación y de proporcionar todos los medios materiales y personales necesarios para la correcta realización de la formación, estando todos los trabajos de formación incluidos en el precio de la oferta.

- Los trabajos de formación no podrán ser subcontratados ni se utilizará una plataforma digital.

- La formación será impartida por los mismos técnicos que realicen la implantación y mantenimiento para un mejor entendimiento y acceso directo por parte del Ayuntamiento.

- Deberá incluirse en la oferta el número de jornadas formativas y el perfil destinatario de cada una. Siendo un mínimo de 100 horas. Distribuidas en jornadas de 3 a 5 horas como máximo y no más de 2 días a la semana.

- La acción formativa se desarrollará dentro de los primeros meses de implantación.

- La distribución del número de horas y jornadas será a criterio del Ayuntamiento.

- Se deberá entregar manuales y documentos técnicos, en formato electrónico, con información relativa a los Sistemas, accesos y herramientas necesarias para la gestión. Estos documentos serán mantenidos y actualizados, con control de versiones por el adjudicatario durante la vigencia del contrato.

SEXTA.- OBLIGACIONES PARA AMBOS LOTES.

- El adjudicatario estará obligado a:

- Se proporcionará información detallada de cuantas soluciones y actuaciones se realicen a requerimiento de los servicios técnicos para su comprobación y validación.

- Se realizarán cuantas reuniones y revisiones soliciten los servicios técnicos del Ayuntamiento con un mínimo:

  - Reunión presencial semanal en el periodo de implantación y durante los tres primeros meses del proyecto
  - Reunión presencial mensual para revisión del proyecto durante la vida del mismo.

- La propuesta técnica se deberá presentar en formato de papel y formato digital

SÉPTIMA.- CONFIDENCIALIDAD PARA AMBOS LOTES.

El adjudicatario estará obligado a tratar de de forma confidencial y reservada tanto la información recibida como la derivada de la ejecución del contrato, no pudiendo ser objeto de difusión, publicación o utilización para fines distintos a los establecidos en este pliego. Esta obligación seguirá vigente una vez que el contrato haya finalizado o haya sido resuelto.

A.-Tratamiento de datos para ambos lotes.

El adjudicatario queda expresamente obligado a mantener indefinidamente, absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, incluidos en el registro de actividades de tratamiento del Excmo. Ayuntamiento de Ciudad Real, que no podrá copiar o utilizar con fin distinto al que figura en este documento, ni tampoco ceder a otros ni siquiera a efectos de conservación.

El licitador quedrá obligado al cumplimiento de lo dispuesto en el Reglamento General de Protección de Datos (REGLAMENTO 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 de abril de 2.016 relativo a la protección de las personas físicas en lo que respecta al

tratamiento de datos personales y a la libre circulación de esstos datos y por el que se deroga la Directiva 95/46/CE).

El adjudicatario, según el párrafo anterior, tendrá las siguientes obligaciones:

El encargado del tratamiento y todo su personal se obliga a partir de la suscripción del presente contrato a:

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b. Tratar los datos de acuerdo con las instrucciones del responsalbe del tratamiento.

Si el encargado del tratamiento considera que alguna de las instrucciones infrigne el Reglamento General de Protección de Datos (Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2.016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE) o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediantamente al responsable.

c. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsalbe del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debe transferir datos personales a un tercer pais o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miebros que le sea aplicable, informára al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

d. No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten al tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de, al menos un mes, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los

derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

e. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

f. Garantizar que las personas autorizadas para tratar datos personales se compromentan, de forma experesa y por escrito, a respetar la confidencialidad.

g. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

h. Devolver al responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

i. Llevar por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

1.- El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

2.- Las categorías de tratamientos efectuados por cuenta de cada responsable.

3.- En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del Reglamanto General de Protección de Datos, la documentación de garantías adecuadas.

j. En el caso de llevar a cabo el encargo de tratamiento en sus locales, realizar un análisis de riesgos relativos al tratamiento objeto de encargo e implantar las siguientes medidas técnicas y organizativas de seguridad que resulten de aplicación a la luz de los resultados de dicho análisis –estas medidas sustituirán a las previstas en el punto 4.1. g) anterior- de las siguientes:

a) La seudoniminación y el cifrado de datos personales cuando sea procedente.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restarurar la disponisbilidad y el acceso a los datos personales de forma rápida, en caso de incidente físicio o técnico.

d) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

k. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

1.- Acceso, rectificación, supresión y oposición.

2.- Limitación del tratamiento.

3.- Portabilidad de datos.

4.- A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones indivualizadas automatizadas, ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección que indique el responsable. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, justamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

l. Notificar al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 72 horas, y a través del correo electrónico corporativo dispuesto al efecto, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

m. No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

a).- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b).- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c).- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d).- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

n. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

o. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

p. Poner a disposición del responsable toda la información necesari para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

q. Designar un delegado de protección de datos si resultare obligatorio su nombramiento y comunicar su identidad y datos de contacto al responsable.

B.-Cumplimiento del Esquema Nacional de Seguridad para el Lote 2:

El adjudicatario asumirá el cumplimiento de lo establecido en el Esquema Nacional de Seguridad (ENS) y en el Esquema Nacional de Interoperabilidad (ENI) en lo referido a la adopción de medidas de seguridad e interoperabilidad de los servicios de e-administración afectados por el pliego.

En este sentido, el adjudicatario se compromete expresamente a cumplir y velar por el cumplimiento legal establecido en cuanto a la adopción de las medidas de seguridad indicadasen los Reales Decretos 3/2010, de 8 de enero, ENS, Esquema Nacional de Seguridad y 4/2010, de 8 de enero – ENI, Esquema Nacional de Interoperabilidad.

El nivel de implantación de las medidas vendrá determinado por la categorización del sistema de información, determinado por el órgano competente sobre la valoración e importancia de la información que se maneja y los servicios prestados por el adjudicatario en la ejecución del pliego.

El adjudicatario garantizará los principios básicos y requisitos mínimos de protección requeridos en el Esquema Nacional de Seguridad, para una protección adecuada de la información. Es de aplicación que el adjudicatario garantice el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en aquellos medios electrónicos de los que sean responsables o sobre los que realizan la prestación de servicios.

Según el documento "obligaciones de los prestadores de servicios a las entidades públicas" del CNN, el adjudicatario tiene la obligación de documentar y ofrecer la siguiente información al Ayuntamiento:

- Descripción de servicios y modalidad.
- Información sobre la arquitectura de seguridad.
- Ubicación de la información.
- Medidas de seguridad implementadas.
- Cumplimiento de la normativa vigente de protección de datos.
- Incidentes de seguridad.
- Cadena de subcontratación y sus cambios.
- Seguimiento de los Acuerdos de Nivel de Servicio (SLA).

Los licitadores estarán obligados a incluir en su oferta, para el caso de ser adjudicatario, la ejecución de un "Plan de seguridad para el cumplimiento del ENS", donde describirán las medidas de seguridad y procedimientos que aplican en relación a la prestación del servicio, cubriendo todos los requisitos del R.D. 3/2010 y medidas de su anexo que les sean de aplicación en función de la categoría del sistema de información.

A petición de la Administración, el adjudicatario deberá remitirle los documentos de seguridad elaborados por el tratamiento de datos personales de aquélla.

La Administración se reserva el derecho de auditar en cualquier momento el nivel de cumplimiento de las medidas de seguridad de dicho documento, así como de las exigidas en el "Plan de seguridad para el cumplimiento del ENS" descrito anteriormente, y de las exigidas en el Reglamento General de Protección de Datos, y en el documento de seguridad relativo a secreto estadístico referido en el apartado 17.

Para ello la Administración deberá avisar al adjudicatario con 5 días de antelación de la realización de dicha auditoria. El adjudicatario deberá facilitar el acceso a los recursos que solicite la Administración para la correcta realización de la auditoría.

El adjudicatario deberá, en un plazo no superior a 3 meses, solventar sin coste para laAdministración, aquellas deficiencias detectadas en dicha auditoría cuando los recursos o servicios afectados sean de su competencia o estén incluidos en la prestación de los servicios que realiza.

OCTAVA.- PLAZO DE IMPLANTACIÓN.

Para el Lote – 1.- La puesta el marcha para el factor de doble autenticación, se contempla un máximo de 2 meses.

Para el Lote – 2.- Instalación de un SIEM, se contempla un máximo de 3 meses.

NOVENA.- DURACIÓN CONTRATO.

- La duración del presente contrato será:

- Para el Lote 1.- Doble factor de Autenticación, Suministro de llaves, tanto las licencias como la garantía será de 3 años, es decir desde la fecha de contratación, más 3 años de garantía. La garantía será a coste 0.

-Para el Lote 2.- Instalación solución SIEM, tanto el mantenimiento como las distintas licencias necesarias para su buen funcionamiento de este sistema, tendrá una garantía de 1 año. El mantenimiento para un funcionamiento óptimo, será a partir de esos 2 años, potestativo para el Ayuntamiento y obligatorio para el contratista por anualidad hasta un máximo de 2 años, a computar a partir de la finalización del año de garantía (es decir, el segundo año).

- Por lo que la duración total de este contrato para los 2 lotes es de 4 años.

DÉCIMA.- PRECIO DEL CONTRATO.

- El precio del presente contrato se desglosa en dos:

Lote 1 .- El precio base de licitación para el suministro de este lote asciende a 37.383,00€, más el I.V.A., correspondiente que suponen 7.850,43€, haciendo un total de 45.233,43€.

Lote 2.- El precio base de licitación para la prestación del servicio de la instalación del SIEM, asciende a 12.600,00€, más el I.V.A., correspondiente que suponen 2.646,00€, haciendo un total de 15.246,00€.

- El lote 1, desde la fecha de contrato, tiene 3 años garantía, por tanto la duración es de 4 años, los 3 años de garantía es coste 0 de mantenimiento.

- El Lote 2. El mantenimiento anual a partir de la garantía, asciende a 1.800,00€, por 2 años de mantenimiento el importe SIN I.VA. es de 3.600,00€, el I.V.A. correspondiente asciende a 756,00€, haciendo un total de 4.356,00€.

- Por tanto el coste total de este contrato por los 4 años, el suministro del lote 1, y la prestación del servicio del Lote 2, (incluido 3 años de garantía sin coste para el lote 1, y una año de garantía para el lote 2), y los dos años de mantenimiento (potestativo para el Ayuntamiento y obligatorio para el contratista), asciende a un total de 53.583,00€, más el 21% de I.V.A., correspondiente asciende a 11.252,43€, lo que hace un total por los 4 años de 64.835,43€, I.V.A., Incluido.

DÉCIMOPRIMERA.- FORMA DE PAGO.

- El pago para ambos lotes, se hará por mensualiades (10% del contrato), realizando la correspondiente acta de recepción, en el mes de Diciembre, se realizará el acta de recepción final y se abonará la totalidad del contrato, una vez que se firme la correspondiente acta de recepción mensual y final, de los trabajos exigidos en este pliego, se presentará la factura electrónica a través de la plataforma FACE.

- Para el Lote 2, pasado el periodo de garantía (de 1 año), y a potestad del Ayuntamiento (obligatorio para la adjudicataria), el mantenimiento del tercer y cuarto año, se ralizará trimestralmente, presentando la factura electrónica a través de la plataforma FACE.

DÉCIMOSEGUNDA.- DOTACIÓN PRESUPUESTARIA.

El importe del suministro para el Lote-1, por importe de 45.233,43€ (I.V.A., Incluido), se hará con cargo al crédito existente en el Presupuesto Municipal, partida 9201.62604.- Adquisición de llaves para doble factor autenticación.

El importe de la prestación para el Lote-2, por importe de 15.246,00€ (I.V.A., Incluido), se hará con cargo al crédito existente en el Presupuesto Municipal, partida 9201.22713.- Contrato SIEM (Ciberseguridad).

El importe por el mantenimiento, del Lote-2 correspondiente al tercer y cuarto año, se hará con cargo al crédito que deberá existir en el ejercicio 2.025 y 2.026, Presupuesto Municipal, partida 9202.22798 .- Contratos Mantenimiento Informático.

DÉCIMOTERCERA.- SERVICIO MANTENIMIENTO.

El mantenimiento debe cubrir de forma mínima y obligatoria los siguientes aspectos.

-Mantenimiento y soporte técnico permanente 24x7. Se incluye el soporte para ambos lotes.

-La empresa adjudicataria dispondrá de experiencia demostrada en instalaciones similares. Con infraestructura montada, funcionando y experiencia técnica.

-Se dispondrá de un número de horas suficientes que deberá soportar cualquier necesidad técnica de puesta en marcha y soporte continuado.

-Se incluirá en la oferta tanto el mantenimiento como la puesta en marcha, configuración, etc., para ambos lotes. Realizando tareas de soporte, configuración, revisión y mantenimiento.

- Las incidencias se registrarán en una herramienta de seguimiento y se proporcionará un número de incidencia. En dicha herramienta se reflejará el problema y paso a seguir hasta la resolución de la misma, así como el tiempo en cada paso desde la llamada.

1.1 Horario del servicio de soporte.

- El horario de atención telefónica estándar será de 9:00 a 18:00, ininterrumpidamente de lunes a viernes.

El licitador deberá especificar un teléfono de contacto, un teléfono del técnico asignado al proyecto y la disponibilidad del mismo o de un recurso equivalente. Adicionalmente las incidencias deberán de estar documentadas y dadas de alta por cuenta del licitador en la herramienta de seguimiento y control que el licitador ponga a disposición del Ayuntamiento de Ciudad Real.

1.2 Acuerdos de nivel de servicio.

Cada incidencia se clasificará en el momento de su apertura por el personal técnico del Ayuntamiento de Ciudad Real en función el impacto que tenga sobre los sistemas. Así las incidencias pueden considerarse como.

Leves, si los sistemas corporativos no se ven afectados, o Críticas, si la incidencia implica parada de servicios o impacta de alguna manera en los sistemas de la plataforma.

Para las incidencias correspondientes a los Servidores ó servicios que afecte a toda la configuración "Crítica", la respuesta deberá ser como máximo de 1 hora, ya que ésta afectaría a todos los clientes conectados a los mismos.

Para las incidencias correspondientes de escritorios puntuales "Leve", la respuesta será de 4 horas.

TIPO	TIEMPO DE RESPUESTA	TIEMPO DE RESOLUCIÓN
Crítica	1 hora	1 hora
Leve	4 horas	4 horas

1.3 Penalizaciones por incumplimiento.

Todas las desviaciones a la baja en el nivel de cumplimiento del servicio estarán asociadas a una compensación por parte del adjudicatario, no obstante, el Ayuntamiento podrá considerar como justificado un desvío en alguno de los parámetros del nivel de servicio cuando concurran causas razonables acreditadas por el proveedor y reducirá de forma acorde la penalización aplicada. Para establecer la compensación se definen dos niveles de incumplimiento: Leve y Crítica.

INCUMPLIMIENTO	DEVIACIÓN LEVE	DESVIACIÓN CRÍTICA
Tiempo de respuesta excedido en incidencia Leve-Crítica	Entre 2 y 3 horas	Entre 1 y 1:30 horas

Las compensaciones por incumplimiento del servicio quedan recogidas a continuación:

INCUMPLIMIENTO	PENALIZACIÓN POR INCUMPLIMIENTO LEVE	PENALIZACIÓN INCUMPLIMIENTO GRAVE
Tiempo de respuesta excedido en incidencia Leve-Crítica	2% de descuento en próxima factura. Máximo 10% acumulable.	4% de descuento en próxima factura. Máximo 20% acumulable.

Por otra parte, la reiteración de incumplimientos tanto leves como graves tendrá penalizaciones adicionales:

En el caso de que se den más de 3 incumplimientos leves en el plazo de una semana, serán considerados a todos los efectos como un incumplimiento grave.

En el caso de que se den más de 3 incumplimientos graves en el plazo de un mes, se compensará añadiendo un 10% de descuento en la próxima factura., y a todos los efectos será considerado como un incumplimiento grave.

- Trasvase de tecnología.

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete a facilitar, a las personas designadas por el Ayuntamiento a tales efectos, toda la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizadas para resolverlos. Se confeccionarán cuantos documentos, informes y descripciones se soliciten.

Toda la documentación se entregará en soporte digital para facilitar el tratamiento y reproducción de los mismos.

El adjudicatario deberá proporcionar al personal designado y a requerimiento del Ayuntamiento la documentación.

DÉCIMOCUARTA.- FORMACIÓN AL PERSONAL MUNICIPAL.

- Se consideran incluidas en el alcance del contrato las acciones formativas destinadas tanto a la correcta utilización, servicios, como a la administración y al mantenimiento de los dos lotes.

En cada uno de los lotes, se determina el plan de formación.

DÉCIMOQUINTA.- PENALIZACIÓN.

- Es una obligación esencial. El retraso de 15 días en las entregas marcadas, supondrá una penalización del 5% de contrato. Un Retraso de 1 mes supondrá una penalización del 10% de contrato. Un retraso en la implantación, superior a 1 mes será causa para la resolución del contrato.

-CAUSAS ESPECÍFICAS DE RESOLUCIÓN DEL CONTRATO POR INCUMPLIMIENTO DE OBLIGACIONES ESENCIALES.

- Trasvase de conocimiento. La empresa adjudicataria atenderá a cuentas cuestiones técnicas se soliciten y se hará documentalmente a cuantas solicitudes de información e informes sean necesarios. El no cumplimiento reiterado previo apercibimiento, será causa para la resolución del contrato.

- Si tras la puesta en marcha, las pruebas que realice el Ayuntamiento se considera que el proyecto implantado no se ajusta a lo exigido en el pliego y firmado en el contrato, será causa para la resolución del contrato.

- Con motivo de la importancia de este contrato para el Ayuntamiento de Ciudad Real, la adjudicataria pondrá a disposición del mismo una plataforma para poder registrar las incidencias (como se detalla en la claúsula Décimatercera, así quedarán grabadas las incidencias (fecha y hora), de tal manera que sí la empresa adjudicataria incumple en más de 5 ocasiones el tiempo de respuesta, como ha quedado establecido en citada cláusulas, será motivo de resolución de este contrato, este Ayuntamiento no puede estar durante mucho tiempo con un sistema que no esté operativo, ya que supondría incidencias a Informática por parte de los Servicios Municipales que no tengan en óptimas condiciones, los servicios de ambos lotes.

DÉCIMOSEXTA.- PRESENTACIÓN DE UNA DEMOSTRACIÓN DE LA PLATAFORMA CON UNA MAQUETACIÓN DE LA MISMA, EN EL AYTO. DE CIUDAD REAL.

- **Para el Lote – 1.-** Posterior a la mesa de Contratación para la apertura del sobre de la documentación Técnica, los responsables de este proyecto del Ayuntamiento elaborarán un calendario para que cada una de las ofertas presentadas puedan realizar una demostración de la solución ofertada.

- En esta presentación se requerirá una demostración de la solución del doble factor de autenticación, de todo lo que contempla este pliego.

- Las empresas que no puedan realizar esta demostración con sus maquetas correspondientes, quedarán excluidas.

- Las empresas deberán realizar la demostración de una forma clara y suficientemente explicativa, se hará detallando cada uno de los puntos exigidos en este pliego, serán las siguientes:

1.- Solución multi-factor. Activación y fun..de autenticación.....	de 0 – 5 Puntos.
2.- Gestión centralizada en la nube	de 0 – 3 Puntos.
3.- Gestión de usuarios	de 0 – 3 Puntos.
4.- Funcionalidades SAML	de 0 – 3 Puntos.
5.- Funcionalidades VPN, Acceso Remoto y RADIUS.....	de 0 – 3 Puntos.
6.- Funcionalidades del Proxy/Gateway	de 0 – 3 Puntos.
7.- Funcionalidades basadas en riesgo	de 0 – 3 Puntos.
8.- Integraciones adicionales	de 0 – 3 Puntos.
9.- Protección de inicio de sesión (login).....	de 0 – 5 Puntos.
10.- Filtrado de contraseñas (scan de dominio-correo electrónico)..	de 0 – 3 Puntos.

Total Puntos.... 34 Puntos.

- Para esta presentación, por este Ayuntamiento estarán presentes los siguientes responsables:

- El Jefe de la Sección de Informática.
- El jefe de administración electrónica.
- 2 Programadores de Informática.

- Cada uno de ellos, valorará independientemente cada uno de los apartados de la maqueta,

El máximo de puntos a valorar será de 34 * 4 = 136 Puntos.

Quedarán excluidas aquellas empresas que no consigan al menos el 75%, es decir las empresas que su valoración quede por debajo de 102 Puntos, no seguirán en el proceso de adjudicación.

-EXCLUSIÓN DEL PROCESO DE LICATACIÓN DE AQUELLAS OFERTAS QUE EN LA PROPUESTA TÉCNICA NO SE AJUSTE A LOS REQUISITOS DE LOS PLIEGOS.-

- A la hora de valorar la propuesta técnica expuesta, se excluirán aquellas ofertas que no concreten de forma suficiente, clara y extensa, los recursos utilizados para realizar la prestación del servicio, y el suministro.

DÉCIMOSEPTIMA.- OBLIGACIONES ESPECÍFICAS EN RELACIÓN AL PRTR.

La empresa contratista, o en su caso, la o las empresas subcontratistas, tienen la obligación de cumplir todo lo establecido en la Orden HFP/1030/2021, de 29 de Septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia y en la Orden HFP/1031/2021, de 29 de Septiembre, por la que se establece el procedimiento y formato de la información a proporcionar por las entidades del sector público estatal, autonómico y local, para el seguimiento del cumplimiento de metas y objetivos ejecución presupuestaria y contable de las medidas de los componenes del Plan de Recuperación, Transformación y Resiliencia y demás normativa específica, y especialmente:

-Los participantes en la ejecución del Plan de Recuperación, Transformación y Resilicneica, tienen que atender estrictamente a lo que establece la normativa española y europea en relación con la prevención, detección y correción del fraude, la curropción y los conflictos de intereses y a los pronunciamientos que al respecto de la protección de los intereses financieros de la Unión Europea hayan realizado o puedan realizar las instituciones de la Unión Europea. Son de aplicación las definiciones de fraude, corrupción y conflicto de intereses contenidas a la Direciva (UE) 2017/1371, sobre la lucha contra el fraude que afecta a los intereses financieros de la Unión Europea (Directiva PIF), y en el Reglamento (UE,Euratom) 2018/1046 del Parlamento Europeo y del Consejo, de 18 de Julio de 2.018, sobre las normas financieras aplicables al presupuesto general de la Unión (Reglamento financiero de la UE).

- El contratista garantizará el pleno cumplimiento del principio de "no causar un perjuicio significativo al medio ambiente" (principio DNSH) y, en su caso, el etiquetado climático y digital, de acuerdo con lo que se preveé en el Plan de Recuperación, Transformación y Resiliencia, aprobado por Consejo de Ministros el 27 de abril de 2.021 y por el Reglamento (UE) núm. 2.021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2.021, por el cual se establece el Mecanismo de

Recuperación y Resiliencia, así como con el requerido en la Decisión de Ejecución del Consejo relativa a la aprobación de la evaluación del plan de recuparación y resiliencia de España.

- El contratista está obligado a garantizar la visibilidad de la financiación de la Unión Europea de acuerdo con aquello que establece el artículo 9.3b) de la Orden HFP/1030/2.021, de 29 de Septiembre, por la cual se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.

- La participación en la licitación que se refiere el presente pliego supone la asunción por parte de los licitadores de la obligación de cumplimiento de las medidas contenidas en el Plan de medidas antifraude y anticorrupción aprobado por el Excmo. Ayuntamiento de Ciudad Real.

- Por otra parte, la empresa cntratista, y también, en su caso, la o las empresas subcontratistas, debe cumplir las obligaciones de información previstas en el artículo 8.2 de la Orden HFP/1030/2.021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia, que incluyen los siguientes aspectos:
- NIF del contratistas o subcontratistas.
- Nombre o razón social.
- Domicilio fiscal del contratista y, en su caso, de los subcontratistas.
- Aceptación de la cesión de datos entre las administraciones públicas implicadas para dar cumplimiento a lo que prevé la normativa euroepa que es de aplicación y de conformidad con la Ley Orgánica 3/2.018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.
- Declaración responsable relativa al compromiso de cumplimiento de los principios transversales establecidos en el PRTR y que pudieran afecta al ámbito objeto de gestión.

- Asímismo, la empresa contratistas, o en su caso, la o las empresas subcontratistas, tienen la obligación de aportar la información relativa al titular real del beneficiario final de los fondos en la forma prevista en el artículo 10 de la Orden HFP/1031/2.021, de 29 de septiembre, por la que se establece el procedimiento y formato de la información a proporcionar por las entidades del sector público estatal, autonómico y local para el seguimiento del cumplimiento de metas, y objetivos ejecución presupuestassria y cotnable de las medidas de los componentes del Plan de Recuperación, Transformación y Resiliencia.

- La empresa contratista debe facilitar la información que le sea requerida para acreditar el cumplimiento puntual de los hitos y objetivos del componente concreto del Plan a la consecución del que contribuye el contrato.

- La empresa contratista debe cumplir las obligaciones en materia medioambiental, así como las obligaciones asumidas en materia de etiquetado verde y etiquetado digital.

- La empresa debe cumplir los compromisos en materia de comunicación, encabezamientos y logotipos que se contienen en el artículo 9 de la Orden HFP/1030/2.021, de 29 de septiembre.

Ciudad Real, 25 de Mayo de 2.022

Fdo: Juan Vicente Guzmán González

Jefe Sección Informática.