Excmo. Ayuntamiento de
LOS REALEJOS

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL SUMINISTRO DE SUSCRIPCIONES DE LICENCIAS DE USO DE PRODUCTOS DE LOS FABRICANTES WATCHGUARD, SOLARWINDS DAMEWARE, BARRACUDA Y HORNET SECURITY CON SERVICIO DE SOPORTE

1. OBJETO

El Excmo. Ayuntamiento de Los Realejos desea contratar el suministro de licencias de uso y servicios de soporte durante la duración del contrato de las soluciones que a continuación se relacionan:

- Lote 1: Software de antivirus corporativo del fabricante Watchguard: Renovación del suministro de licencias de uso para Endpoint y ampliación con el módulo gestión de parches Watchguard Patch Management o equivalente.
- Lote 2: Software de gestión remota del fabricante Solarwinds Dameware: Renovación del suministro de licencias de uso para software de control remoto.
- Lote 3: Appliance de copias de seguridad del fabricante Barracuda: Renovación del suministro de licencias de uso, servicio de soporte, reemplazo y almacenamiento paralelo en la nube.
- Lote 4 Software Antispam del fabricante Hornet Security, Total Protection Enterprise Backup o equivalente: Mejora de módulo y suministro de licencias de uso para cubrir el servicio de seguridad antispam del servidor de correos actual (suite Microsoft 365) incluyendo las copias de seguridad de la suite.

2. ALCANCE Y REQUISITOS DEL SERVICIO

2.1 Escenario actual de soluciones y licenciamientos

Actualmente el Excmo. Ayuntamiento de Los Realejos cuenta en su poder con las siguientes licencias agrupadas por fabricante:

2.1.1 Watchguard

Producto	Núm. de Serie	Cant.	Fecha fin
WatchGuard EPDR	A150G0F2G-YFTQ	301	24/04/2024

2.1.2 Solarwinds Dameware

Producto	Número de Serie	Cantidad	Fecha fin
SolarWinds DameWare Remote Support [formerly DameWare NT Utilities]	60249	6 técnicos	24/04/2024

2.1.3 Barracuda

Producto	Número de Serie	Tipo de soporte	Fecha fin
Barracuda Backup Appliance 890	BAR-BS-2169526	Energize Updates	24/04/2024
Barracuda Backup Appliance 890	BAR-BS-2169526	Instant Replacement	24/04/2024
Barracuda Backup Appliance 890	BAR-BS-2169526	Cloud Storage	24/04/2024

2.1.4 Hornet Security

Producto	Cantidad	Fecha fin
Hornet Security Spam and Malware Protection	397	24/04/2024

2.2 Productos objeto de Licenciamiento y Soporte

Conforme a lo anterior se desea contratar el suministro de licencias de uso de las soluciones que a continuación se relacionan para dar continuidad a los licenciamientos existentes. Los licitadores deberán de presentar en el anexo correspondiente de la oferta económica un listado de precios anuales unitarios de los productos del lote al que se presenta. En base a este listado, el Ayuntamiento podrá contratar las licencias que se necesiten durante la duración del contrato hasta llegar un máximo económico fijado a partir de una previsión de licencias máximas indicadas a continuación. En el caso de los lotes 1, 2 y 4, el número de licencias es un valor estimado, el número de licencias mínimas contratadas con el fin de asegurar al licitador la viabilidad económica de su propuesta será siempre igual o superior al 80% de las cantidades reflejadas en este listado.

2.2.1 Lote 1 Antivirus Watchguard EPDR y gestión de parches

Producto	Cant.
WatchGuard EPDR	360 licencias
Watchguard Patch Management o equivalente	360 licencias

Se desea dar continuidad al antivirus existente (Watchguard EPDR) aumentando las licencias contratadas según estimación inicial de 301 a 360.

2.2.1.1 Características de la solución de gestión de parches

También se desea ampliar el producto con la posibilidad de realizar gestión de parches y así poder administrar las vulnerabilidades de los sistemas operativos y las aplicaciones de terceros en estaciones de trabajo y servidores de Windows, macOS y Linux. para el mismo número de licencias en una solución integrada del tipo Watchguard Patch Management o equivalente con las siguientes características.

La solución debe estar integrada con el actual endpoint con el fin de no tener que desplegar nuevos agentes ni consolas de administración facilitando de esta manera la gestión de toda la solución de seguridad.

Se desea tener una visibilidad centralizada y en tiempo real del estado de seguridad de las vulnerabilidades de software, los parches faltantes, las actualizaciones y el software no compatibles, así como herramientas para todo el ciclo de administración de la revisión: desde la detección y la planificación hasta la instalación y la supervisión.

Esta solución tiene como objetivo:

- Auditar, supervisar y priorizar las actualizaciones del sistema operativo y las aplicaciones. Con una vista desde un solo panel ofreciendo visibilidad centralizada, actualizada y completa del estado de seguridad de la organización con respecto a las vulnerabilidades, los parches y las actualizaciones pendientes de los sistemas y cientos de aplicaciones.

- Reducir sistemáticamente la superficie de ataque creada por las vulnerabilidades del software con el objetivo de evitar incidentes. Controlar los parches y las actualizaciones con una herramienta de administración en tiempo real y de fácil uso.

- Contener y corregir ataques de aprovechamiento de vulnerabilidades enviando de manera inmediata actualizaciones o parches desde la consola. Permitiendo que los equipos afectados puedan aislarse del resto de la red.

Funcionalidades

Las funcionalidades que ha de tener la solución son las siguientes:

Detección:

- Vista desde un solo panel con información en tiempo real de todas las computadoras vulnerables, los parches pendientes y el software no compatible (EOL), junto con su estado de corrección. Información detallada sobre parches y actualizaciones pendientes, detalles de boletines de seguridad relevantes (CVE).
- Búsqueda automática de parches disponibles en tiempo real o en intervalos periódicos (3, 6, 12 o 24 horas).
- Notificación de parches pendientes en detecciones de vulnerabilidades.
- Capacidad de aislar, parchear y anular el aislamiento de computadoras y servidores.

Planificación y tareas de instalación de parches y actualizaciones:

- Configuración según la importancia y el software que se debe parchear.
- Programación de ejecución inmediata, única o repetida en intervalos regulares (fecha/hora).
- Capacidad de controlar los reinicios de la computadora y configurar excepciones.
- Reversión para desinstalar un parche que pueda provocar un conflicto inesperado con una configuración existente.
-

Supervisión del estado de actualizaciones y el endpoint mediante:

- Panel de control y listas prácticas. Reportes de alto nivel y detallados.
- Listas de computadoras actualizadas y computadoras con actualizaciones pendientes con errores.
-

Administración granular basada en grupos y roles con diferentes permisos:

- Visibilidad basada en roles de las computadoras vulnerables, los parches y los paquetes de servicio.

Control centralizado de actualizaciones, parches y software:

- Capacidad de desactivar Windows Update y administrar las actualizaciones del sistema operativo de manera centralizada.
- Capacidad de excluir parches específicos por versión y tipo.
- Capacidad de excluir software (p. ej., Java).
- Capacidad de guardar en caché los parches descargados.

2.2.1 Lote 2 Gestión Remota Dameware

Producto	Cantidad
SolarWinds DameWare Remote Support [formerly DameWare NT Utilities]	7 técnicos

Se desea dar continuidad al sistema de gestión remota existente (Dameware Remote Support) aumentando las licencias contratadas de 6 a 7 técnicos estimados.

2.2.3 Lote 3 Appliance de copias de seguridad Barracuda

Producto	Tipo de soporte
Barracuda Backup Appliance 890	Energize Updates
Barracuda Backup Appliance 890	Instant Replacement
Barracuda Backup Appliance 890	Cloud Storage

Se desea dar continuidad al sistema de copias de seguridad existente (Barracuda Backup Appliance 890) dando continuidad a los soportes asociados a la misma de Energize Updates, Instant Replacement y Cloud Storage.

2.2.4 Lote 4 seguridad de correo electrónico con copias de seguridad Hornet Security

Producto	Cantidad
Hornet Security Total Protection Enterprise Backup.	400 licencias

Se desea evolucionar el producto Hornet Security Spam and Malware actual a una versión de seguridad de correo electrónico con copias de seguridad compatible con la nueva solución de correo electrónico que se está implantando actualmente en la entidad (Outlook de la Suite Microsoft 365), con licenciamientos Microsoft 365 Empresa Estándar, Microsoft 365 Empresa Básico y Microsoft Exchange Online Plan 1.

Es por ello que se desea el suministro estimado de 400 licencias de la solución Hornet Security Total Protection Enterprise Backup o equivalente. Incluyendo en la misma consola de administración en la nube de antispam y antimalware, el ATP (Amenazas Avanzadas Persistentes), Archiving, cifrado, continuity, firmas de correo y backup de toda la Suite M365 (email, calendarios, tareas, contactos, onedrive, sharepoint, teams) de manera ilimitada en tiempo y en tamaño de datos.

2.2.4.1 Características de la solución de seguridad de correo electrónico con copias de seguridad

- La solución deberá estar basada en arquitectura altamente disponible que permita garantizar el nivel de servicio acordado.
- La solución deberá ser ofrecida directamente, desde la infraestructura del proveedor (solución cloud), no on-premise.
- La arquitectura utilizada garantizará la capacidad de escalado de la solución, permitiendo iniciar el despliegue, en un entorno ajustado a las necesidades iniciales de la entidad y que evolucionará conforme a lo que requiera la entidad.
- La solución deberá integrar, las funcionalidades de seguridad de correo electrónico y backup, dentro de un mismo panel de administración web, sin necesidad de instalación de software adicional.
- La solución deberá poseer la capacidad, de añadir buzones de correo electrónico seguro, dentro de la infraestructura en nube del fabricante en caso de ser necesario, que serán administrados desde la misma plataforma.
- El fabricante de la solución deberá contar con el certificado de conformidad con el ENS al menos en categoría MEDIA.

Filtrado

- Solución perimetral para el filtrado de spam, virus y contenido no deseado en tráfico SMTP (correo electrónico).
- Deberá proteger, escanear y filtrar el correo entrante y saliente.
- Deberá soportar, la tecnología de cifrado TLS (Transport Layer Security), al menos en versión TLS 1.2.
- Deberá poder forzar la transmisión de correo, utilizando una capa de transporte segura (TLS) a los destinatarios que sean configurados (por IP, dominio o dirección de correo).

Filtros de Conexión

- Deberá disponer de diversos métodos de filtrado que dependiendo del resultado obtenido rechazarán o marcarán el correo electrónico como spam para la posterior validación del usuario si éste lo desea.
- Deberá contar el Servicio de Reputación del fabricante o con más de un motor de verificación de reputación de IP.
- Deberá proporcionar algún mecanismo para que el administrador indique direcciones IP, que deben ser bloqueadas.
- Para el correo saliente deberá verificar y controlar que:

    - No realice “Open Relay”.
    - Emitir avisos al administrador, si la dirección IP origen, se encuentra en listas negras.

- Deberá aplicar técnicas de Greylisting, basándose en si la IP origen está en una RBL.
- Deberá permitir la creación, para cada domino gestionado, de listas negras y blancas que contengan direcciones IPv4, emails y dominios.
- Deberá soportar protección, contra ataques de tipo Denegación de servicio (DoS).
- Deberá soportar filtrado de conexiones, basándose en las tecnologías DNSBL y SPF.
- Deberá soportar el uso de validaciones del dominio origen, basándose en la existencia de registros MX del mismo.
- Deberá soportar la comprobación de la existencia del destinatario, para eliminar el spam entrante, que se envía a cuentas inexistentes.
- En caso de que el correo entrante tuviera cabeceras de firma DKIM, el filtrado de correo entrante deberá realizar la comprobación de dichas cabeceras, validando el dominio asociado al firmado DKIM.

Filtrado antimalware

- Deberá de poder analizar, todos los correos entrantes y salientes.
- Deberá disponer de actualización permanente, del componente de filtrado de virus, con las ultimas firmas y/o actualizaciones.
- Deberá realizar filtrado de correos, con ficheros adjuntos potencialmente peligrosos: ejecutables, etc.
- Debe disponer de la posibilidad de cuarentena, de mails infectados.
- El Administrador, puede seleccionar criterios de notificación, informando o no al destinatario del mail infectado, mediante un informe al usuario final que pueda ser personalizado.
- El Filtrado Antivirus debe operar en línea: Debe tener la posibilidad, de retener completamente los correos infectados, dirigidos a usuarios finales y nunca entregarlos y realizar un análisis en paralelo del correo infectado.

Filtros de Contenido Antispam

- El administrador, debe poder configurar listas blancas (remitentes permitidos) y negras (remitentes bloqueados) por usuario, dominio y entidad.
- El administrador debe poder configurar reglas específicas, que aplicarán al correo entrante y/o saliente y que podrán definirse, a nivel de entidad.

- En las reglas definidas por el administrador, se debe de poder definir condiciones basadas como mínimo, en:

    - El origen del correo.
    - El destino del correo.
    - El contenido del asunto.
    - El cuerpo del mensaje.
    - En el tipo o contenido de los adjuntos.
    - En el tamaño del correo.
    - Existencia de ciertas cabeceras en el correo.

- Deberá de permitir el uso de expresiones en la definición de las reglas.
- Entre las condiciones de las reglas, debe existir la capacidad de poder examinar el contenido de ficheros adjuntos legibles en formato texto.
- Permitir establecer dominios sobre las que no se realizará la opción de marcado.
- Actualización periódica de reglas y filtros.
- Disponer al menos de un motor capaz de detectar correo spam, independientemente del idioma del correo, del formato y codificación.
- Deberá permitir la realización del filtrado de contenido de los mensajes basado en la puntuación de los correos.
- Deberá tener la capacidad de separar en cuarentenas separadas accesibles por los usuarios finales el correo spam no solicitado y el correo comercial solicitado (también conocido como listas de distribución comerciales a las que el usuario se haya suscrito).
- Los usuarios finales deberán poder elegir si se les debe entregar el correo comercial solicitado en su bandeja de correo o quedar retenido en el servicio antispam.
- Los reportes de cuarentena deberán cumplir:

    - Personalización completa, al menos, de logo de la entidad, disclaimer, dirección de remitente y texto.
    - Previsualización, del contenido de los correos en cuarentena.
    - Generación de reportes de manera, al menos, horaria y configurable en base a usuario.
    - Posibilidad de generar un reporte para todo el dominio.
    - Posibilidad de decidir qué tipo de correo, se muestra en el reporte de usuario, así como las acciones que el usuario puede realizar (visualizar o liberar).

Filtros de contenido Anti-phishing (prevención de suplantación de identidad)

- Deberá realizar filtrado, mediante estándares que permitan detectar la suplantación de identidad, de posibles dominios remitentes. Dichas técnicas, serán, como mínimo DKIM y DMARC.
- Deberá permitir la configuración avanzada, sobre la matriz de decisión para las validaciones SPF, DKIM y DMARC.
- El análisis mediante el filtro de comprobación SPF permitirá la configuración basada en “envelope from”, “header from” o ambos.
- Deberá contemplar la utilización de diferentes técnicas o mecanismos para identificar tales correos:
    - Reconocimiento de intenciones
    - Verificar integridad y autenticidad de metadatos de correo
    - Falsificación de remitentes por similitud

- Detección de solicitud de información confidencial

Continuidad y disponibilidad del servicio de correo electrónico corporativo

- Deberá retener (encolar) durante un mínimo de 7 días el correo que, una vez procesado por los filtros, tenga algún error temporal de entrega a los servidores de correo de la organización, bien por fallos en las líneas de comunicaciones o por indisponibilidad temporal del servicio de correo de la entidad. Este servicio deberá realizar reintentos periódicos de entrega de los correos retenidos sin intervención manual de los administradores de la solución.
- El servicio deberá poder realizar entrega de los correos, una vez procesados, a uno o varios servidores de correo de la organización. Se podrán definir distintas prioridades de entrega e incluso poder realizar un balanceo de la carga entre varios servidores de correo donde se encuentren alojados los buzones de los usuarios finales de la organización.

Filtrado de Amenazadas Avanzadas (ATP)

- Deberá disponer de la capacidad de proteger los mensajes entrantes frente a software malintencionado (virus, troyanos, gusanos, etc) tanto conocido como desconocido (hora cero).
- El filtrado de amenazas avanzadas debe operar en línea: Debe tener la capacidad de retener completamente los correos infectados dirigidos a usuarios finales y nunca entregarlos y realizar un análisis en paralelo del correo infectado.
- Si procede, serán sometidos al análisis heurístico de ATP. En caso de que el correo analizado contenga archivos adjuntos infectados con malware, estos serán reflejados en la cuarentena del sistema. Los procesos de análisis de ficheros por ATP deberán ser reflejados en las estadísticas.
- Debe realizar un análisis exhaustivo de los ficheros adjuntos en los correos por técnicas de detección heurísticas (tales como Sandboxing) para poder identificar posibles amenazas por comportamiento y no debe apoyarse en la detección de amenazas por firmas de malware previamente conocidas.
- Debe poder analizar las URLs adjuntas en documentos o el cuerpo de los correos.
- Para ofrecer una máxima protección, el sistema deberá realizar un análisis de las URLs referenciadas en un correo recibido por un usuario en el momento en que el usuario abra el enlace, para evitar de este modo los ataques de campañas de malware donde se produzcan cambio del contenido referenciado en las URLs enviadas a las víctimas.
- El análisis de URLs deberá ser ofrecido en modo “proxy” y no mediante el análisis del resultado de ejecución del enlace citado.
- La tecnología utilizada para la protección de correos no deberá realizar modificación alguna en los adjuntos de los correos, tales como deshabilitar macros o scripts. La información transmitida al usuario, tras procesarse la capa de protección contra amenazas avanzadas, debe garantizar que el correo se mantiene íntegro una vez se procesado al entregarse al usuario final.
- Debe poseer una tecnología de detección de amenazas avanzadas y persistentes que sea resistente a técnicas de evasión mediante las cuales los programas malware analizados puedan ocultar su comportamiento malicioso en determinados entornos de análisis y puedan pasar sin ser detectados.
- Deberá proporcionar acceso a informes sobre los archivos analizados en el “Sandbox”

donde, como mínimo, estará disponible la siguiente información:

- Hash del Archivo.
- Score de la solución ante la amenaza.
- Resumen de todos los procesos detectados tanto de comportamiento, de análisis de red y procesos estáticos.
- Capturas de pantallas del entrono virtual al ejecutar el fichero/archivo.
- Análisis de más motores AV contra terceras plataformas (por ejemplo, VirusTotal).

Filtros avanzados de prevención de suplantación de identidad – Filtros anti-fraude del CEO

- La solución ofertada debe proporcionar una protección efectiva frente a intentos de suplantación de identidad dirigidos a personal de alto valor dentro de la organización (whaling / spear phishing), identificando como mínimo:

  - El uso fraudulento de nombres de personas de la organización.
  - El uso fraudulento de direcciones electrónicas de la organización.
  - Uso fraudulento de protocolo.
  - Análisis de patrones de contenido.
  - Verificación de integridad y autenticación.
  - Detección de “Spy out”.
  - Identificación de datos fingidos.

Técnicas de análisis adicionales

- Técnicas de freezing o congelación para correos que no puedan ser clasificados inmediatamente. Estas técnicas nunca excederán un tiempo de análisis mayor a 15 minutos.
- Avisos en tiempo real a los administradores cuando una amenazada avanzada (APT) sea detectada por cualquiera de los motores.
- Posibilidad de aviso a los administradores en el caso de que un correo ya entregado sea detectado posteriormente como malicioso (Alertas ExPost).

Filtrado antimalware

- Deberá de poder analizar todos los correos entrantes y salientes.
- Deberá disponer de actualización permanente del componente de filtrado de virus con las ultimas firmas y/o actualizaciones.
- Deberá realizar filtrado de correos con ficheros adjuntos potencialmente peligrosos: ejecutables, etc.
- Debe disponer de la posibilidad de cuarentena de mails infectados.
- El Administrador puede seleccionar criterios de notificación, informando o no al destinatario del mail infectado mediante un informe al usuario final que pueda ser personalizado.
- El Filtrado Antivirus debe operar en línea: Debe tener la posibilidad de retener completamente los correos infectados dirigidos a usuarios finales y nunca entregarlos y realizar un análisis en paralelo del correo infectado.

Continuidad y disponibilidad del servicio de correo electrónico corporativo

- Deberá retener (encolar) durante un mínimo de 90 días el correo que, una vez procesado por los filtros, tenga algún error temporal de entrega a los servidores de correo de la organización, bien por fallos en las líneas de comunicaciones o por indisponibilidad temporal del servicio de correo de la entidad. Este servicio deberá realizar reintentos periódicos de entrega de los correos retenidos sin intervención manual de los administradores de la solución.
- El servicio deberá poder realizar entrega de los correos, una vez procesados, a uno o varios servidores de correo de la organización. Se podrán definir distintas prioridades de entrega e incluso poder realizar un balanceo de la carga entre varios servidores de correo donde se encuentren alojados los buzones de los usuarios finales de la organización.
- El servicio deberá tener la posibilidad de ofrecer una solución de contingencia que almacenaje de correos entrantes y salientes por un periodo mínimo de 90 días y permita el uso de una interfaz web de emergencia en caso de caída del servidor principal de destino.

Firmas y exención de responsabilidad (Disclaimer)

- Permitirá la configuración de Firmas y Avisos Legales corporativos de manera unificada desde el mismo panel de control del resto de servicios y basada en grupos, desde la consola de administración del servicio.
- Las firmas configuradas podrán integrar de manera automática las variables situadas en el Directorio Activo de Azure de Microsoft, recogiendo los atributos de cada cuenta, para rellenarlo automáticamente.

Encriptación mediante certificados.

- Firma digital automática y encriptación de correos electrónicos salientes mediante S/MIME y PGP: Protección de los correos electrónicos contra la modificación no autorizada o la lectura por parte de terceros durante su transmisión a través de redes públicas.
- Gestión automática de certificados y almacenamiento de claves: el proveedor se encarga de obtener e instalar los certificados necesarios. Estos se guardan en un almacén central de certificados.
- Certificados de correo electrónico personal: Se utilizarán certificados codificados de 2048 bits de una de las autoridades de certificación (CA). Cuando se encripta con S/MIM, cada usuario recibe su propio certificado. También se podrán importar y utilizar certificados suministrados por la entidad.
- Configuración individual y definición de pautas de cifrado: En el panel de control se podrá definir los tipos de cifrado que desea utilizar para contactar con los socios de comunicación: TLS, S/MIME, PGP o Websafe. Puede aplicarse global o individualmente, para usuarios concretos, grupos o dominios. También se podrá definir cómo proceder si la clave de un destinatario no está disponible.
- Opción de prueba de idoneidad de la encriptación: En el panel de control se podrá comprobar qué opciones de cifrado tiene el interlocutor. Para ello, se introducirá la dirección de correo electrónico del destinatario y se mostrará qué tecnología de cifrado puede utilizarse en la comunicación con esa dirección.
- Comunicación confidencial a través de Websafe: Aunque el interlocutor no pueda recibir correos electrónicos cifrados, se garantiza el cifrado y la confidencialidad de la comunicación por correo electrónico con determinadas personas.
- Descifrado automático de correos electrónicos entrantes: Si se dispone de la clave pública del remitente, los correos electrónicos se descifran automáticamente y se entregan al

destinatario.
- Gestión de certificados de usuario desde la misma consola: Pueden solicitarse, renovarse u obtenerse permanentemente nuevos certificados para los usuarios a través del panel de control (PGP S/MIME).

Archivado

- Se requiere solución de Archivo automático ilimitado, sin posibilidad de realizar cambios ni modificaciones en la información archivada: Con un archivado a prueba de auditorías, de todos los correos electrónicos, entrantes, salientes e internos que se almacenen automáticamente en su forma original directamente a su llegada.
- Deberá disponer de Registro de auditoría/rastreo de auditoría: Registro de todos los accesos al archivo de correos electrónicos, que contenga entre otras cosas, el nombre de usuario y la dirección IP del usuario y no pueda editarse ni eliminarse. El administrador podrá ver el registro de auditoría en cualquier momento.
- Plazos de conservación: Se podrá configurar el plazo de archivo de 6 meses a 10 años para cumplir las normas de protección de datos de las diferentes áreas.
- Amplia búsqueda de texto completo en el archivo siguiendo varios criterios: Pueden utilizarse criterios de búsqueda individuales, como la fecha, el remitente, el destinatario y el asunto, para reducir los parámetros de búsqueda y determinar con precisión los mensajes que se buscan y encontrarlos más rápidamente.
- Recuperación y restablecimiento de correos electrónicos archivados: Si los correos electrónicos de un usuario se borran accidentalmente en el servidor de correo, que puedan recuperarse desde el archivo.
- Que tenga la opción de archivo de correos electrónicos internos, que sean almacenados a prueba de auditorías desde el momento en que se archivan y se pueden buscar y recuperar del mismo modo que los correos electrónicos entrantes y salientes.
- Los administradores no deben tener acceso a los correos electrónicos archivados de los usuarios. Sólo que puedan verse los metadatos.
- Exportación de los datos archivados: Todo el archivo de correo electrónico que pueda exportarse fácilmente y en cualquier momento.
- Clasificación clara de los archivos en caso de cambios de las direcciones de correo: Si un usuario recibe una nueva dirección de correo electrónico, que los mensajes archivados puedan asignarse a esta nueva dirección para que el usuario pueda seguir accediendo a los datos.

Backup M365

- La solución debe contar con la capacidad de hacer copia de seguridad y restauración sobre las siguientes funcionalidades de Microsoft 365: Exchange Online, Sharepoint, Onedrive y Teams.
- Las copias de seguridad se deben realizar múltiples veces al día de manera automatizada, sin necesidad de configuración previa.
- El almacenamiento de las copias de seguridad se debe realizar en centros de datos redundados situados en la Unión Europea y los servidores deberán ser gestionados por el propio fabricante del servicio.
- La solución deberá contar con múltiples opciones de restauración total y granular, basando las mismas incluso en elementos.
- Las copias de seguridad se conservarán por un periodo de tiempo indefinido, desde la

primera copia, hasta que la entidad deje de utilizar el servicio.

- Las copias de seguridad realizadas se almacenarán en centros de datos no gestionados por Microsoft.
- La solución contará con la posibilidad de realizar copias de seguridad de ficheros localizados en equipos de usuario final sobre sistema operativo Windows (7, 8, 8.1, 10).
- La solución de backup de Teams realizará copias de seguridad de los chats individuales, de grupos y de reuniones, así como de las imágenes adjuntas en las mismos.
- La solución de backup de Teams realizará copias de seguridad sobre las conversaciones en canales públicos y privados, así como de las imágenes adjuntas en las mismos.
- La solución permitirá exportar múltiples correos directamente a un PST o a un archivo ZIP.
- Almacenamiento ilimitado, incluido en el precio por usuario/mes.

Administración

- La gestión y administración tanto de la solución de correo electrónico corporativo como de la solución de seguridad deberá ser ofrecida y gestionada desde el mismo Panel de Control
- La solución de permitir integración con la nube de Microsoft 365, sin necesidad de configuración en el entorno de Microsoft 365, para la sincronización, como mínimo, de dominios, buzones e información sobre servidores destino.
- Deberá almacenar como mínimo 90 días los correos filtrados (Spam, etc.) y poder ser consultados de forma gráfica desde el panel web de administrador.
- La solución deberá tener la posibilidad de gestionar un Split domain para entornos híbridos desde el propio panel, mediante diferenciación asignación de usuarios a los diferentes entornos de correo electrónico.
- La solución debe disponer de la posibilidad de integrar la información ofrecida en el Log de Correo con un sistema SIEM.
- La solución debe disponer de la posibilidad de integrar con sistemas SOAR a través del uso de su API.
- Los administradores podrán recibir, en tiempo real, una notificación de alerta cuando una amenazada avanzada sea detectada por los motores.
- Debe de contemplar al menos los siguientes perfiles de administración:

    - Administrador Global: administrará todos los dominios y usuarios de la plataforma.
    - Administrador de Estadísticas: Tendrá acceso a los reportes gráficos estadísticos.
    - Administrador Técnico: Podrá administrar la cuarentena de correo así como el Log de Correo.
    - Usuario: la solución es trasparente a los usuarios, teniendo a su disposición un panel desde donde podrá acceder a su buzón de correo, tanto el considerado válido como el no válido, además de gestionar algunas propiedades de filtrado que se aplicarán exclusivamente para él.

- Los usuarios finales del servicio (empleados de la entidad) deben poder acceder a una consola de seguridad donde podrán:

    - Revisar sus correos bloqueados en la cuarentena del sistema, permitiendo su desbloqueo.
    - Administrar su lista personal de remitentes permitidos (whitelist) o bloqueados (blacklist).

- Configurar el reporte de cuarentena y personalizar el horario de envío.
- Administrar el filtro relacionado con Listas de Distribución comerciales.

- El administrador debe de poder habilitar o deshabilitar el acceso de los usuarios a las consolas de administración.
- La solución deberá de contemplar un entorno multi-idioma, contemplándose como mínino castellano, inglés, alemán y francés.
- La solución debe permitir visualizar en tiempo real u online el tráfico de correos entrantes y salientes.
- Compatible con los principales navegadores Web existentes (Firefox, Chrome, Safari, Internet Explorer, etc).
- Deberá de permitir la personalización de la consola de gestión, para dominios y entidad permitiendo adaptar la consola a las diferentes imágenes corporativas.
- Acceso a la consola autenticado y cifrado usando el protocolo https.
- Deberá de permitir la sincronización automática de usuarios realizando consultas al servidor LDAP, LDAP sobre SSL o SMTP.
- Deberá permitir la sincronización automática de usuarios mediante la utilización de un sistema API de provisión integrado con los sistemas de Microsoft 365.
- Deberá de permitir la auditoría de las acciones realizadas por el administrador y los usuarios del sistema. Se registrará como mínimo la siguiente información para cada acción:

  - Fecha.
  - Acción.
  - Datos relacionados con la acción.
  - Resultado de la acción.
  - Usuario que realiza la acción.

- Deberá de permitir que los administradores de empresa gestionen la cuarentena de los usuarios de manera centralizada.
- Deberá de permitir que el administrador delegue la gestión de la cuarentena a los usuarios finales usando como mínimo:

  - Consola web de usuario final.
  - Informes automáticos de resumen enviados por correo electrónico a cada usuario de forma periódica, permitiendo a los usuarios la reclasificación de correos desde dicho informe sin necesidad de entrar en su consola de gestión de usuario final.

- La solución deberá de disponer de un sistema de almacenamiento de trazas o logs en tiempo real que permita desglosar e independizar los ficheros de las transacciones de correo (logs) para cada dominio, permitiendo el acceso y consultas online mediante la consola de administración.
- Desde la consola de administración se permitirá la realización de búsquedas en los logs utilizando como mínimo lo siguientes filtros:

  - Por dominio.
  - Por asunto del correo.
  - Por dirección origen del correo.
  - Por dirección destino del correo.

- Por IP origen.
- Por clasificación (Spam, valido, entrante rechazado, saliente rechazado, listas de correo, avisos de virus, etc…).

- Desde la consola de administración se permitirá la aplicación de acciones sobre el resultado de las búsquedas en los logs, permitiendo como mínimo:

  - Marcar uno o varios correos como correo spam.
  - Marcar uno o varios correos como correo válido.
  - Enviar el remitente a la lista blanca de la empresa.
  - Enviar el remitente a la lista negra de la empresa.
  - Ver la IP origen del mensaje.

- Deberá de contemplar un informe grafico de resumen donde se muestre como mínimo, la clasificación de los correos entrantes y salientes de los últimos 90 días. Debe de mostrarse información relativa al correo rechazado, valido, spam y correo con virus.
- Los administradores de la solución deberán poder decidir quién es el grupo de usuarios VIP sin limitación del número.

2.3 Soporte Técnico Adicional

Para cada lote el adjudicatario deberá incluir una bolsa de horas anual de soporte técnico adicional a la del fabricante que será consumida a petición del Excmo. Ayuntamiento de Los Realejos. Los licitadores deberán de presentar en el anexo correspondiente de la oferta económica el precio unitario de esta bolsa de horas (€/h). En base a este precio, el Ayuntamiento podrá contratar las horas que necesite durante la duración del contrato hasta llegar un máximo económico fijado a partir de sus previsiones anuales. En ningún caso la entidad estará obligada a consumir este soporte anual en su totalidad ni parcialmente.

El Excmo. Ayuntamiento de Los Realejos comunicará al adjudicatario los incidentes y peticiones mediante estos canales como mínimo: Correo electrónico, llamada telefónica y por formulario de gestión de incidencias que el adjudicatario proponga. Los canales telemáticos han de estar disponibles de forma ininterrumpida. La asistencia telefónica y soporte técnico remoto deberá estar disponible de 8:00 a 16:00 horas de lunes a viernes (hora canaria).

En el caso de tener que realizar actualizaciones, deberá ofrecerse el soporte técnico necesario para realizarlas fuera del horario habitual de trabajo si éstas pueden afectar a la continuidad del servicio y si así lo estima oportuno el Excmo. Ayuntamiento de Los Realejos.

Una vez realizada la comunicación de la incidencia, el adjudicatario deberá ponerse en contacto con el personal del departamento de Servicios Informáticos del Excmo. Ayuntamiento de Los Realejos (tiempo de respuesta) y resolverlo (tiempo de resolución). Para ello el adjudicatario podrá dar soporte técnico de forma remota o enviar, a su costa, a un técnico de su organización al Excmo. Ayuntamiento de Los Realejos, en la Avda. Canarias nº6 para que analice y resuelva la incidencia.

La prestación del servicio puede estar sujeta a incidentes que pueden comprometer el mantenimiento de unos niveles de servicio adecuados. En este sentido y para evitar que estos incidentes impacten en la menor medida posible en la prestación del servicio, se establecen unos criterios de priorización de incidentes que permitan ofrecer unos tiempos de respuesta y resolución correctos. Estos criterios de priorización quedan recogidos en 2 tipos: Normal y críticos.

- Normales: Incidentes que no implican la detención total del servicio o que o comprometen la seguridad del mismo en cualquiera de sus parámetros.
- Críticos: Incidentes que implican la detención total del servicio o que pueden comprometer la seguridad del mismo.

Se tendrá también en cuenta la apertura de tickets para la resolución de dudas que denominaremos peticiones.

Antes de que transcurra el tiempo de resolución, el adjudicatario deberá haber cumplido sus obligaciones de mantenimiento, entendiéndose por haber cumplido, sin perjuicio de lo dispuesto en este pliego:

a) Haber corregido la incidencia comunicada.
b) Haber facilitado la documentación que, de una forma clara y sencilla, transmita a las personas del Excmo. Ayuntamiento de Los Realejos, un pleno conocimiento de la corrección de la incidencia del programa informático y del funcionamiento de la aplicación informática corregida y que permita asegurar la formación del personal.
c) Haber facilitado el soporte para que la corrección de la incidencia esté instalada en la solución si fuese necesario.

2.3.1 Acuerdo de nivel de servicio

Con el fin de facilitar esta parte del servicio, el adjudicatario incluirá en su propuesta un acuerdo de nivel de servicio para el soporte técnico adicional que incluya los datos que a continuación se recogen y con estos tiempos de partida mínimos.

Tarea	Tiempo de respuesta	Tiempo de resolución
Peticiones o consultas	16 horas	24 horas
Incidencia Normal	6 horas	8 horas
Incidencia Crítica	1 horas	4 horas

Todas las tareas descritas anteriormente dispondrán de monitorización que permita un seguimiento del grado de cumplimiento de los niveles de servicio. El adjudicatario proporcionará al Excmo. Ayuntamiento de Los Realejos un informe semestral que indicarán el cumplimiento de los niveles de servicio. Este informe se pondrá a disposición del Excmo. Ayuntamiento de Los Realejos durante la primera semana de cada mes.

3. OTRAS CONSIDERACIONES

3.1. Medios adscritos

Las obligaciones asumidas por el adjudicatario deberán ser cumplidas por personal técnico debidamente especializado en cada una de las aplicaciones de que se trate.

El adjudicatario se compromete a disponer del suficiente número de personas con los conocimientos técnicos adecuados para asegurar el oportuno cumplimiento de sus obligaciones.

3.2 Confidencialidad

El adjudicatario se obliga a tratar confidencialmente, y a no reproducir, publicar ni difundir ninguna información que puedan conocer en función de su relación contractual. Una vez extinguido el contrato cada parte borrará y destruirá toda la información que sobre la presente relación haya almacenado en cualquier soporte o haya reproducido por cualquier procedimiento.

3.3. Representación de la Propiedad Intelectual

El adjudicatario ostenta la propiedad o la representación (partner) del propietario del producto objeto del contrato de mantenimiento y deberá demostrarlo fehacientemente en la propuesta. Todas las mejoras, actualizaciones y modificaciones del mismo, incluida la documentación y manuales relacionados deberán estar a disposición del Excmo. Ayuntamiento de Los Realejos durante el periodo del contrato.

3.5. Localización del soporte lógico y de los datos

En los casos que proceda, el almacenamiento de datos ha de estar localizado dentro del Espacio Económico Europeo o en países que de una u otra forma garanticen un nivel adecuado de protección de los datos de carácter personal conforme a la legislación vigente.

En todo caso, el contratista tiene la obligación de presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos. Y el Excmo. Ayuntamiento de Los Realejos deberá dar su conformidad a dicha ubicación y a la participación de terceras empresas para estos fines si así ocurriese.

Asimismo, los licitadores deben indicar en su oferta, si tienen previsto subcontratar los servidores o los servicios asociados a los mismos, el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.

Igualmente tienen la obligación específica de someterse en todo caso a la normativa nacional y de la Unión Europea en materia de protección de datos, sin perjuicio de la condición especial de ejecución de sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos y que además tiene la consideración de obligación contractual esencial.

El contratista tiene la obligación de comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en la declaración a que se refiere la letra anterior.

Los apartados indicados tienen la consideración de obligaciones esenciales a los efectos previstos en el artículo 211. 1 f) de la LCSP.

3.6. Protección de datos

Debido a la naturaleza del servicio objeto del presente contrato, la empresa adjudicataria puede tener que realizar tratamientos automatizados de ficheros del Excmo. Ayuntamiento de Los Realejos que contengan datos de carácter personal. En cualquier caso, será el Excmo. Ayuntamiento de Los Realejos quien decida sobre la finalidad, contenido y uso del tratamiento de los datos, limitándose la empresa adjudicataria a utilizar dichos datos, única y exclusivamente para los fines que figuran en el presente contrato y siempre por cuenta del Excmo. Ayuntamiento de Los Realejos.

El Excmo. Ayuntamiento de Los Realejos únicamente permitirá el acceso a datos de carácter personal a la empresa adjudicataria cuando sea necesario para la ejecución del objeto del presente Contrato.

La empresa adjudicataria en cumplimiento con la normativa vigente en protección de datos de carácter personal, entre ellas el Reglamento (UE) 2016//679 de 27 de abril de 2016 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales se compromete a:

- No aplicar o utilizar los datos personales obtenidos, para fines distintos a los que figuren en el presente Contrato y sus Anexos, ni cederlos a terceros, ni siquiera para su conservación.
- Guardar secreto profesional respecto de los mismos, aun después de finalizar sus relaciones con El Excmo. Ayuntamiento de Los Realejos.
- Trasladar las obligaciones citadas en los párrafos anteriores al personal que dediquen al cumplimiento del presente Contrato y sus Anexos.

Cumplida la prestación contractual, la empresa adjudicataria deberá destruir todos los datos de carácter personal tratados.

3.10. Informes

La empresa deberá presentar un informe semestral como reporte de las actuaciones realizadas bajo la bolsa de horas del soporte técnico, con los errores corregidos, actualizaciones y mejoras instaladas y los tiempos de respuesta y de resolución para cada actuación realizada como justificación de la misma.

3.11. Duración

El servicio de mantenimiento objeto del presente contrato se prestará por **TRES años** a partir de la fecha que se indique en el contrato. El contrato no será prorrogable.

3.12. Formato y contenido de la propuesta

Con carácter general, la información presentada debe estar estructurada de forma clara y concisa.

El Excmo. Ayuntamiento de Los Realejos se reserva el derecho a exigir a los licitadores que presenten documentación que acredite la veracidad de la información presentada en la oferta, o bien información adicional sobre el contenido de la misma, estando el licitador obligado a ello.

El Excmo. Ayuntamiento de Los Realejos podrá requerir a los licitadores que formulen por escrito las aclaraciones necesarias para la comprensión de algún aspecto de sus proposiciones. En ningún caso se admitirá que en proceso de aclaraciones el licitador varíe los términos expresados en su propuesta. Sólo se admitirá la información que facilite el análisis de la solución propuesta inicialmente.

Se presentará un breve resumen de las características de la solución y módulos presentados, los datos de las licencias propuestas para mantener y las características del soporte técnico propuesto.

DILIGENCIA: Se pone para hacer constar que el Pliego de Prescripciones Técnicas que antecede, numerado de la página 1 a la 18, ha sido aprobado mediante Decreto de la Concejalía de Servicios Generales nº 2024/731, de fecha 4 de marzo de 2024, rectificado mediante Decreto de la Concejalía de Servicios Generales nº 2024/749, de fecha 5 de marzo de 2024.

Documento firmado electrónicamente