Mutua Montañesa
Mmuy fácil

Exp: S00014699

Pliego Técnico
Servicio de soporte de licencias EDR, ITSM, Exclaimer

Fecha de impresión: 20/05/2022 10:40

Índice

1. INTRODUCCIÓN

Mutua Montañesa requiere para su operativa el suministro servicios y licencias para los siguientes productos:

- Servicio EDR (Endpoint Detection Response)
- Service Desk Manager Plus y servicios implantación
- Servicio Exclaimer

La presente licitación se estructurará en lotes uno para cada uno de los productos/servicios requeridos debido a que su naturaleza es diferente, y puede ejecutarse de forma independiente, ya que no pone en riesgo la correcta ejecución de cada servicio de forma separada.

El software ITSM y el servicio de Exclaimer vienen vinculados a un expediente anterior que quedó desierto, con número de expediente 2022-002-022.

2. LOTE 1: SERVICIO EDR

Mutua Montañesa está concienciada con la necesidad de invertir en tecnología y como en este caso en Seguridad con el fin de proteger uno de sus principales activos, como es los sistemas de información de la organización. Por este motivo, se publica la presente licitación para la implantación de un sistema de protección del puesto de trabajo mediante un sistema EDR avanzado.

2.1. OBJETO

Dotar a Mutua Montañesa de un sistema de protección del puesto de trabajo, moderno con un amplio ecosistema de protecciones que permitan a Mutua Montañesa abordar las distintas necesidades en este ámbito sin necesidad de abordar complejos proyectos de integración entre herramientas.

Mutua Montañesa tras un análisis de mercado realizado en 2021 procedió a la adquisición de licencias de uso de la plataforma Crowdstrike por destacar en el mercado de los EDR. La apuesta por esta tecnología se ha demostrado acertada a nivel local por la efectividad del producto y a nivel general por la evolución en los análisis de mercado más prestigiosos como son Gartner en el que se ve la evolución al alza de esta plataforma de protección EDR

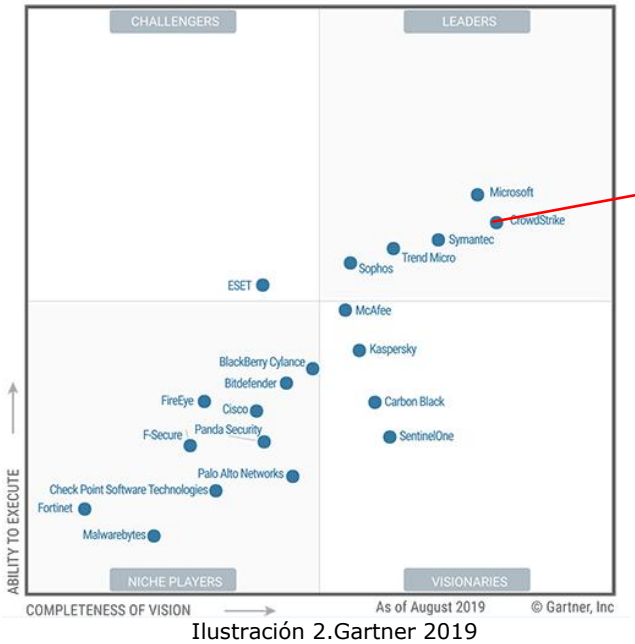

Ilustración 2.Gartner 2019

Ilustración 1. Gartner 2021

Por este motivo, Mutua Montañesa, tiene como objetivo, continuar y reforzar el uso de esta plataforma, como elemento de seguridad EDR

2.2. ALCANCE

El alcance de este lote es la compra inicial asegurada de 165 licencias pudiéndose llegar a lo largo de la vida del contrato a un máximo de 300 licencias, por dispositivo (físico o Virtual) para proteger a los equipos de Mutua Montañesa, ante un posible cambio de plataforma que pueda impactar en el nº de licencias requeridas. Se contempla una, pudiéndose incrementar la compra a lo largo del periodo de vida del contrato.

2.3. REQUERIMIENTOS TÉCNICOS

Mutua Montañesa posee actualmente 150 licencias de Crowdstrike Falcon Endpoint Protection Enterprise con los módulos de Insight y Prevent.

2.3.1. REQUERIMIENTOS TÉCNICOS

Mutua Montañesa requiere el suministro y derecho de uso, actualización y soporte de 165 licencias de Falcon Endpoint Protection, durante 3 años, con los siguientes componentes mínimos:

- Prevent, Control and Respond
- Threat Graph Standard
- Falcon Insight EDR

Dentro del alcance de este lote el adjudicatario deberá así mismo dar soporte sobre la instalación existente cubriendo tareas como:

- Resolución de dudas de uso de los sistemas
- Soporte ante una detección para el diagnóstico del evento
- Ayuda y seguimientos de incidencia de producto
- Seguimiento y ajustes post-despliegue

El proveedor/fabricante deberá disponer de un sistema de soporte a las posibles incidencias que surjan durante la vigencia del presente concurso respondiendo según los ANS que se recogen en este pliego. Dicho soporte será accesible por Web/Teléfono/Mail en idioma castellano para incidencias normales, pudiéndose emplear el Ingles en incidentes de prioridad alta.

Por último, el proveedor deberá estar certificado para la implantación de las herramientas descritas en este pliego

2.3.2. MANTENIMIENTO Y SOPORTE

El mantenimiento facilitado por el proveedor deberá corresponder como mínimo con el Express Support que el fabricante contempla al menos los siguientes aspectos de valor:

- Actualizaciones de la versión.
- Actualizaciones de productos.
- Soporte a incidencias.
- Asistencia técnica y aprendizaje.
- Informes periódicos del estado de la plataforma

2.3.3. ANS

Los ANS establecidos serán los que se siguientes según es definición de Severidad y tiempo de respuesta:

- Severidad 1: Existencia de un problema, si posibilidad de resolución/mitigación que afecta a equipos de misión crítica o que presenta posibilidad de pérdida/corrupción de datos
  - Objetivo de Respuesta: en los 60 min siguientes a la notificación
- Severidad 2: Existencia de un problema afectando a servicios críticos, pero permiten continuar la actividad con restricciones
  - Objetivo de Respuesta: en las 2 horas siguientes a la notificación
- Severidad 3: Existencia de un problema con un efecto limitado en las operaciones de negocio
  - Objetivo de Respuesta: Mismo hora del siguiente día laborable
- Severidad 4: Existencia de un problema que no afecta a la operatividad del negocio.
  - Objetivo de Respuesta: a lo largo del siguiente día laborable

3. LOTE 2: SERVICIOS Y LICENCIAS SERVICE DESK PLUS

Desde el área de Tecnología y Sistemas de Mutua Montañesa se coordina el SGSI (Sistema de Gestión de la Información de Mutua Montañesa). Este sistema de gestión está alineado con el Esquema Nacional de Seguridad como marco de referencia para la gestión de los servicios de TI de Mutua Montañesa.

Los procesos de gestión de incidencias, la gestión de incidentes de seguridad, configuraciones, la gestión de problemas o cambios, la gestión de la continuidad, así como otros procesos de control de las medidas de seguridad implantadas, son prioritarios para velar por el cumplimiento de este modelo de gestión.

Para el control y seguimiento de estos procesos actualmente Mutua Montañesa está utilizando una herramienta de Help Desk denominada Service Desk Plus, en su modalidad Standard, con un licenciamiento para 15 usuarios técnicos.

3.1. OBJETO

El objeto del presente procedimiento es establecer las condiciones técnicas que regirán la contratación del suministro de las licencias de la herramienta ITSM así como los servicios profesionales para su instalación y configuración.

De manera general se solicita:

- Suministro licencias producto Service Desk Plus Enterprise
- Servicios Profesionales configuración producto.
- Instalación y Migración incidencias Helpdesk sistema actual.
- Soporte

Se pretende con esta contratación y renovación del sistema de Service Desk Plus, orientar tanto los procesos como las herramientas disponibles hacia una gestión más avanzada de los servicios TI atendiendo a las mejores prácticas en esta materia. Se pretende implantar una solución que permita gestionar una CMDB y los procesos de gestión TI habituales.

En este sentido, se debe tomar como referencia con relación al modelo de gestión, el estándar ISO 27001 y el Esquema Nacional de Seguridad.

3.2. ALCANCE

Se estima el suministro de las siguientes licencias:

- ServiceDesk Plus Multi-Language Enterprise - Annual Subscription fee for 10 Technicians (500 nodes).

Se requiere los servicios profesionales para la instalación en un entorno on premise de la versión Service Desk Plus Enterprise más reciente.

Se estima los servicios profesionales para la configuración de los siguientes grupos de funcionalidades:

- Service Desk: funciones para soportar la operativa de apertura de "tickets" (incidencias, peticiones, cambios) entre usuarios y soporte.
- CMDB: funciones de gestión del inventario de servicios TI y sus componentes, relaciones, atributos, etc.
- Funciones necesarias para soportar los principales procesos de gestión TI sobre los servicios IT definidos y sus componentes, según describen los estándares/modelos de referencia indicados.

- Funciones de gestión del conocimiento relativo a la resolución de problemas más típicos que ofrezcan posteriormente un sistema de autoayuda al usuario.

Entendemos que para la ejecución de estos servicios profesionales como mínimo el adjudicataria deberá dedicar 20 jornadas de trabajo.

3.3. REQUERIMIENTOS TÉCNICOS

3.3.1. SITUACIÓN ACTUAL

Mutua Montañesa dispone del sistema Service Desk Plus edición standard en su versión 9.0, como herramienta de ticketing para la gestión del soporte correctivo de los procesos de IT, muy vinculados a la gestión de incidencias.

Actualmente, nuestro sistema tiene una configuración del módulo HelpDesk, Usuarios, donde fundamentalmente está parametrizado la gestión de incidentes adaptado a los flujos de Mutua Montañesa con la incorporación de campos específicos y una gestión de SLA. También tenemos configurado la autenticación con el Active Directory.

Asimismo, en este entorno disponemos de un histórico de incidencias y solicitudes que necesitamos migrar al nuevo entorno. En este sentido, entendemos que es suficiente con migrar únicamente las solicitudes abiertas, y tener un backup a modo de fichero con toda la información de las incidencias cerradas, en caso de que sea requerido la revisión del histórico.

3.3.2. NUEVO SISTEMA SERVICE DESK PLUS

3.3.2.1. Aspectos Generales

La plataforma debe estar alineada con las mejores prácticas del Esquema Nacional de Seguridad, y debe ser una herramienta capaz de gestionar, de modo general:

- La definición de los servicios y sus componentes, recogiendo sus relaciones y el significado de las mismas, de modo que sea posible registrar y posteriormente, generar informes relativos a las diferentes peticiones, cambios, incidencias, etc. en los distintos elementos y sus afecciones a los servicios o a otros elementos.
- Recoger los distintos roles asociados a los servicios y sus componentes: responsables, técnicos al cargo del mantenimiento, etc. de modo que sea posible automatizar asignaciones de ciertos tipos de tareas a los roles designados.
- Gestionar los niveles de servicio requeridos para los distintos elementos y conectar la herramienta con sistemas que permitan su seguimiento.
- Gestionar las peticiones, cambios, incidencias, problemas, etc. relativos a los servicios o sus componentes.
- Generar informes sobre todos estos aspectos

En cualquiera de los ámbitos de la solución podrán definirse campos adicionales, que serán dinámicos en función del registro (ítem CMDB, registro de Service Desk o inventario). La

configuración de estos campos deberá poder realizarse desde el interface web, sin necesidad de programación. Podrá adjuntarse cualquier fichero de información adicional.

El sistema contará con métodos de generación de métricas o indicadores configurables, que permita realizar un análisis de situación actual y pasada, así como análisis de tendencias. Las métricas deberán ser parametrizables, y accesibles desde el interface web.

El sistema contará con un conjunto de reportes por defecto, ofreciendo facilidades para adaptar dichos reportes, modificándolos según las necesidades corporativas, y añadiendo nuevos reportes específicos. Los reportes deberán admitir visualización on-line, así como exportación al menos a formatos abiertos, PDF, texto u hojas de cálculo que permitan su tratamiento externo.

Las diferentes pantallas (listados, informes,..) admitirán exportación a formatos abiertos (csv, pdf, imágenes,…) para su posterior utilización. En su generación admitirán filtrado por los campos comunes (fechas, categoría del registro, tipo del registro, cliente, prioridad,…).

El sistema dispondrá de distintos niveles de acceso configurables por perfiles, permitiendo controlar qué perfiles de usuarios o técnicos pueden visualizar los diferentes ítems de información o realizar ciertas acciones.

Se valorará que el sistema cuente con la opción de registrar la actividad de accesos (quién y cuándo se accede a cada registro) así como cambios en los campos de los registros.

3.3.2.1. Arquitectura de la solución

La solución se instalará en un entorno on premise de Mutua Montañesa, que se suministrará con el sistema operativo instalado, y la empresa adjudicataria será la encargada de realizar la instalación de la solución. Es requerido que, en la oferta, el licitador nos indique las características mínimas para la implantación de la solución.

Mutua Montañesa facilitará una maquina virtual Windows Server 2022 o inferior, instalada y configurada con todos los parches de S.O. actualizados y la solución de EDR existente en la organización. El resto de las configuraciones, productos, licencias, etc. deberán ser aportados por el proveedor y acordados con Mutua Montañesa en el arranque del proyecto.

La plataforma debe contar con una interface 100% web, tanto para la administración del sistema como para su uso, sin necesidad de instalar software adicional en los equipos, salvo el destinado a la recolección de datos de invetario para equipos cliente windows. El portal web de los usuarios deberá ser compatible con los principales navegadores web (IE, Firefox, Chrome,..). La validación de usuarios y la gestión de los mismos deberán estar integrados con el DA de la organización. El interfaz web ofrecerá:

1. Portal de usuarios.
2. Portal de técnicos encargados de la resolución de las peticiones o incidencias.
3. Portal de gestores con cuadro de mando y funciones de generación de informes relativos al servicio, elementos o procesos de los que sean responsables.
4. Portal de administradores de la herramienta. El portal de usuarios podrá ser totalmente configurable, con la opción de añadir los logotipos corporativos, mensajes de bienvenida y alertas/avisos. Desde el portal de usuario podrán publicarse distintos links configurables, para acceder a otros sistemas web corporativos, o incluso a enlaces externos.

3.3.2.1. Service Desk (Helpdesk)

El software de Service Desk **gestionará las incidencias, peticiones, problemas, cambios y entregas relativas a elementos de inventario y/o CMDB de forma totalmente integrada**. Este punto de integración es muy importante, y una mejora sustancial para tener recogido el ciclo de vida de una incidencia y su afectación al inventario.

El flujo deberá poder parametrizarse para adaptarse a las necesidades concretas de la organización, y deberá cubrir todo el ciclo de vida, desde el registro inicial, hasta el cierre final. Las incidencias o peticiones podrán relacionarse con otras incidencias, peticiones, problemas, RFCs o tópicos de conocimiento. Cualquiera de los módulos de gestión de incidencias, peticiones, problemas, cambios o entregas deberá estar integrado y tener acceso directo a cualquiera de los CIs almacenados en el módulo de gestión de la configuración (CMDB). Las relaciones deberán ser bidireccionales.

La herramienta incorporará métodos para clasificar las incidencias en distintos tipos y categorías. Se podrán configurar las categorías de incidencias necesarias, enlazarlas jerárquicamente en los niveles necesarios y asociar categorías o tipos a tipos de CIs.

Las incidencias y peticiones podrán priorizarse en base al impacto y urgencia de las mismas. Se valorará la existencia de algún mecanismo que permita establecer las reglas de prioridad lo más amplio posible utilizando los campos disponibles (tipos, categorías, elementos afectados, intervalos de tiempo transcurridos, campos propios que indiquen prioridades o impactos,..).

Flujos de autorización

En función de la clasificación de la incidencia o petición, el sistema será capaz de gestionar un flujo de autorizaciones previo a la atención del registro. Los perfiles autorizadores no serán necesariamente personal técnico de soporte.

Sistemas Autoayuda

Además, la aplicación gestionará las comunicaciones con el usuario a través de un portal web para que cualquier usuario de la organización pueda conocer el estado de sus incidencias dadas de alta. El portal de los usuarios contará con opciones de autoayuda, permitiendo a los usuarios la consulta de FAQs o tópicos de conocimiento previamente publicados por el personal de soporte, y que permita la resolución rápida de incidencias o peticiones sin necesidad de contactar con el personal de soporte.

Contará con opciones de integración de chat para que los usuarios contacten con los técnicos de soporte. El portal podrá ser configurable, permitiendo ordenar, acumular, filtrar las pantallas de datos en función de los campos de los registros (categorías, tipos, prioridades,… o bien los campos personalizados definidos) sin necesidad de programación. El sistema permitirá configurar plantillas. Debe poder definirse que perfil de usuarios pueden utilizar ciertas plantillas o haber modelos diferentes para usuarios o técnicos.

Alta incidencias o peticiones automáticas

El sistema admitirá el alta de nuevas incidencias o peticiones realizadas directamente por los técnicos de soporte en su nombre de los usuarios. Debe poder configurarse qué perfiles de técnicos pueden dar de alta dichos registros. El sistema admitirá el alta de nuevas incidencias o peticiones mediante el envío de correos electrónicos a cuentas de e-mail (POP3, IMAP). Deberán poderse configurar distintas cuentas asociadas a la creación de distintos tipos o categorías o reglas para la creación en función de los campos que incluya el

mensaje. También admitirá el alta de nuevas incidencias o peticiones directamente a partir de cambios detectados en la infraestructura. El sistema registrará el origen de la notificación de la incidencia o petición, admitiendo distinguir al menos la recepción de incidencias desde el portal web de usuarios (registro de origen automático), origen en correos electrónicos, origen mediante llamada telefónica o cualquier otro origen configurable. Los cambios de estado en la incidencia o petición podrán ser notificados de manera automática por la herramienta vía correo electrónico, dirigido tanto a los usuarios finales como a los técnicos de soporte. Deben poder manejarse distintos mensajes para los usuarios o internos entre los técnicos de soporte. El sistema deberá contabilizar de manera automática el tiempo invertido en cada etapa del ciclo de vida, así como guardar el histórico de dicho ciclo de vida.

Notificaciones automáticas, escalado y SLAs

El sistema permitirá notificar a los técnicos cuando existan registros en su bandeja de entrada que hayan excedido un umbral de tiempo (configurable) sin haber sido atendidos. Permitirá configurar reglas para el escalado jerárquico de incidencias / peticiones que superen un umbral configurable del SLA asignado así como enviar notificaciones automáticas como aviso.

En función de la clasificación de la incidencia o petición, el sistema será capaz de calcular automáticamente SLAs basados en tiempos de atención, escalados o resolución. Deberán tenerse en cuenta diferentes calendarios y horarios de servicio en estos cálculos. Cualquiera de las acciones documentadas por los técnicos de soporte podrá ser marcada para ser visible al usuario final o privada, para uso interno de los técnicos de soporte. El cierre podrá realizarse por el propio usuario una vez validado. En el momento del cierre de las incidencias o peticiones, el usuario podrá contestar una encuesta de valoración (global y/o vinculada a tipos concretos de incidencias/peticiones) totalmente configurable por parte de los técnicos de soporte. Los registros podrán ser confirmados y cerrados por el usuario directamente desde el interface web, momento en el que el sistema podrá ser configurado para realizar una encuesta de satisfacción.

Ante la circunstancia de que el usuario final no cierre la incidencia o petición en un tiempo razonable, el sistema deberá ofrecer mecanismos configurables para su cierre automático. En el momento del cierre de la incidencia o petición, el sistema deberá calcular de manera automática al menos:

- tiempo real de resolución
- tiempo real de cierre
- horas invertidas en las acciones realizadas
- grado de cumplimiento del SLA establecido

3.3.2.1. CMDB

El módulo de gestión de configuración (CMDB) deberá estar integrado con el módulo de inventario permitiendo el alta automática de CIs tecnológicos detectados por el inventario y con los módulos de gestión de incidencias, problemas, peticiones, cambios.

El nivel de automatización para la gestión de CIs a partir del inventario, deberá ser configurable, permitiendo indicar qué tipos de activos deben ser automáticamente catalogados como CIs vinculados y dispondrá de opción de bloquear la modificación de CIs si no existen RFCs vinculadas. Se deberán poder definir reglas para configurar qué tipos de CIs se pueden dar de alta, tipos de relaciones entre tipos de CIs.

Las relaciones entre CIs asociados a activos del inventario podrán gestionarse de manera automática. Se admitirá la creación de relaciones manuales. Se valorará que contemplen un valor que refleje el peso, importancia o impacto de la relación.

Se deberá poder definir el ciclo de vida para cada tipo de CI y los estados compatibles con cada tipo.

Se deberán poder configurar distintos niveles de profundidad (detalle de información) en función del tipo de CI, y campos de información diferenciados en función del tipo de CI seleccionado. El conjunto de tipos de datos para los campos de información deberá ser amplio para permitir los usos más comunes (textos, listas desplegables, opciones,...).

Las relaciones, bien sean automáticas o manuales, deberán visualizarse en modo de listados y en representación gráfica. El modo gráfico de relaciones permitirá moverse entre los distintos CIs, mostrando el grado de importancia o impacto de cada una de las relaciones y su tipo y soportará búsquedas filtradas por tipos de CIs, de relaciones, profundidad a partir de un CI inicial.

El modo gráfico deberá visualizar de manera rápida aquellos CIs en los que existan cambios sobre la situación monitorizada, en situación de fallo, con incidencias,..

El sistema admitirá modificar el estado (disponible/no disponible) de elementos de la CMDB desde herramientas externas que miden la disponibilidad de la infraestructura.

Se valorará que la herramienta incorpore herramientas para la gestión de la seguridad de la información o los servicios alineada con los requisitos del Esquema Nacional de Seguridad:

- Gestión del valor de los ítems de información y servicios.
- Propagación de valores hacia elementos inferiores a través de las relaciones entre CIs.
- Análisis de riesgos de los sistemas de información definidos o enlace a herramientas que lo permitan

3.4. SERVICIOS PROFESIONALES

La contratación del servicio llevará asociadas una serie de tareas para el desarrollo del proyecto que estimamos que deberá realizarse en 3 meses de duración desde la adjudicación del servicio.

En primer término, se requiere la instalación del nuevo entorno y migración de las incidencias abierta del actual sistema de Mutua Montañesa. En este punto será requerida la configuración inicial del producto para poder poner en funcionamiento el módulo de help desk (gestión incidencias, problemas y gestión de cambios), así como las funcionalidades básicas del CMDB para dar soporte a la gestión de incidencias y éstas puedan estar relacionadas.

Asimismo, se requiere la revisión en más profundidad de los procesos IT relacionados con el control de medidas de seguridad del ENS y su aplicación a las medidas de control implantadas en Mutua Montañesa.

Para la configuración el entorno, a continuación, enumeramos el volumen de elementos de configuración (CIs): hardware, aplicaciones software, servicios, y personas que forman parte del sistema TI.

Además, identificaremos los atributos principales de cada elemento de configuración que entendemos mínimos para su puesta en marcha.

A modo de referencia actualmente gestionamos en nuestro inventario la siguiente cantidad de dispositivos. En verde se marca los dispositivos que entendemos como Nodos en el cómputo de licencias.

Resumen de elementos inventario actual.

Etiquetas de fila	Activo	Srv. Tecnico	STOCK	Total general
Armario	1		2	3
Cabina de Discos	5		1	6
Cinta	1			1
Compartidor	5		13	18
Controlador			1	1
Disco Duro	4		15	19
Firewall	3		2	5
Gestor Correo			2	2
Grabadora DVD	4			4
Hub	1		1	2
Impresora	1			1
Impresora Multifunción B/N	55	1		56
Impresora Multifunción Color	36			36
Lector Cód. Barras	1			1
PC	27	2	32	61
Portátil	59	9	68	136
Maquina Virtual	80			80
Proyector Informático	2		4	6
Router	3		30	33
SAI	1			1
Scanner	1		1	2
Semáforo	1			1
Serv. Dedic.	13		3	16
Sistema Sonido	25		1	26
Switch	51		19	70
Tablet	53	2	10	65
TFT	293	4	82	379
ThinClient	227	18	137	382
Transceiver	3		7	10
Unidad de Cintas	1		6	7
WebCam	35		2	37
Lector Tarjetas			1	1
PDU	6			6
Proxy			1	1
Antena Wifi	10			10
Monitor	3			3
TV	28			28
Telefono Movil	15		15	30

4. LOTE 3: SERVICIO EXCLAIMER

Mutua Montañesa posee una infraestructura de correo electrónico basado en Microsoft Exchange 2007, sobre el que hay implementado un sistema de firma al pie de correos electrónicos Exclaimer Signature Manager Exchange.

Dentro del plan de contratación de Mutua Montañesa para este 2022, está prevista la implantación de un nuevo sistema de correo basado en Office 365 por lo que el uso de este sistema de firma onpremise dejara de tener efecto. Sin embargo, hasta que dicha actualización se produzca, algo que en ningún caso será más tarde de un año, es necesario seguir manteniendo el actual sistema de firma por lo que se requiere la contratación del mantenimiento del sistema de firma actual Exclaimer Signature Manager Exchange para 500 buzones durante un año.

4.1. ALCANCE

Se estima el suministro del producto Excalimer Signature Manager Exchage para 500 buzones por 12 meses de servicio.