



Irun, 29 de abril de 2022
Behin behineko Idazkaria/La Secretaria Acctal.



PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR LA CONTRATACIÓN DEL SUMINISTRO DE UNA SOLUCIÓN ANTISPAM Y DE RELAY DE CORREO

1.- Objeto del contrato

El objeto del presente contrato es el suministro de una solución antispam y de relay de correo para los dominios irun.org y bidaso-activa.com de acuerdo a las condiciones y prescripciones que se establecidas en el presente Pliego de Prescripciones Técnicas.

Asimismo la oferta contemplará los aspectos siguientes:

- Configuración de la herramienta de acuerdo a las necesidades y requerimientos del Ayuntamiento de Irun para un correcto funcionamiento de la herramienta
- Formación en la herramienta a los técnicos municipales.
- Debe estar incluida la mano de obra y desplazamientos de los técnicos especializados en caso necesario.
- Si bien el Ayuntamiento de Irun dispone de técnicos que pueden realizar la gestión de la herramienta, se requerirá un servicio de asistencia por parte de la empresa adjudicataria durante los 3 años del contrato. Dicho servicio de asistencia deberá garantizar unos tiempos de respuesta adecuados en el caso de necesitar intervenciones de los técnicos, para subsanar el malfuncionamiento de la herramienta. Dichos tiempos de asistencia deberán ser los siguientes:
 - Asistencia telefónica 8x5, también vía web y correo-e.
 - Soporte de respuesta a incidencias debe ser igual o inferior a 4 horas en días laborables (lunes a viernes).
 - Soporte de respuesta a consultas debe ser igual o inferior a 8 horas en días laborables (lunes a viernes).

La oferta contemplará una descripción detallada del procedimiento a seguir en los casos de apertura de incidencia por malfuncionamiento o de consulta técnica, tanto en la modalidad telefónica, web o correo-e.

En la descripción de los procedimientos de apertura de incidencia se deberá contemplar como "tiempo de respuesta" el que transcurre desde la comunicación de una avería o malfuncionamiento hasta que se produce una intervención, se ofrezca información útil sobre el problema reportado o directamente se exponga una posible solución del Servicio Técnico. Es decir, la mera contestación a efectos de acuse de recibo de la incidencia, o asignación de número de caso, no se considerará como una solución a la incidencia y, por lo tanto, como tiempo de respuesta oficial.

- La clasificación de las incidencias, en función de su importancia y criticidad se clasificarán en críticas, urgentes o leves, siendo los tiempos máximos de respuesta los siguientes:
 - o Incidencia Crítica : <= 5 horas
 - o Incidencia Urgente : <= 9 horas
 - o Incidencia Leve : <= 24 horas

*El tiempo de resolución de las incidencias atendidas por el fabricante no está incluido en estos tiempos indicados para resoluciones por parte de la empresa.

Estos tiempos de respuesta los podrán mejorar las empresas en sus ofertas

- Acceso a la base de conocimiento del fabricante.





- Se debe incluir la gestión de escalados al fabricante que se consideren pertinentes por el adjudicatario ante una incidencia no resuelta en primer nivel.
- Elaboración de documentación relativa a la instalación y configuración de la herramienta que entregará al Departamento de Informática del Ayuntamiento de Irun. La empresa adjudicataria se comprometerá a mantener actualizada la documentación sobre la instalación y configuración de los elementos objeto de estos servicios, en la medida que sufran cambios durante el periodo de vigencia del contrato

Es requisito indispensable que la empresa ofertante tenga algún nivel de partenariado con la solución propuesta y deberá acreditar dicho partenariado a través de un documento expedido por el fabricante de la solución.

2.- Descripción de las instalaciones

El Ayuntamiento de Irun dispone de un servidor de correo con Microsoft Exchange en el que se alojan los siguientes dominios de correo:

- irun.org
- bidaso-activa.com

Entre los dos dominios el Ayuntamiento de Irun tiene alrededor de 750 buzónes de correo y el Ayuntamiento quiere adquirir una solución antispam y de relay de correo **para 810 licencias.**

El Ayuntamiento de Irun también dispone de grupos de correo de distribución con dirección propia que no deben de contabilizarse dentro del nº de licencias.

Aparte de los correos enviados por las trabajadoras y trabajadores municipales, también se enviarán boletines de noticias masivos a través del servicio de relay de la herramienta. Estos envíos masivos se realizan a alrededor de 12.000 destinatarios, debiendo el servicio de relay ser capaz de gestionar dichos envíos.

3.- Requisitos de la solución antispam y de relay de correo

Los requisitos que deberá cumplir la solución antivirus y de relay de correo ofertada deberán ser los siguientes para cada uno de los siguientes aspectos:

General

- 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, es decir, que no se deberá instalar en equipos en la red interna del Ayuntamiento de Irun.
- La arquitectura utilizada garantizará la capacidad de escalado de la solución, permitiendo iniciar el despliegue en un entorno ajustado a las necesidades iniciales del Ayuntamiento de Irun y que evolucionará conforme lo requiera el Ayuntamiento de Irun.

- La solución deberá permitir la integración de los servicios de filtrado de correo con futuros servicios de archivado y encriptación de correo que el Ayuntamiento de Irun desee incorporar.

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 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 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.
- Deberá proteger el sistema de correo del cliente contra ataques individuales y selectivos tales como Spearphishing, Blended Attacks, Advanced Persistent Threats, Ransomware y CEO Fraud
- Para identificar posibles ataques, los correos del cliente considerados sospechosos se analizarán con las siguientes técnicas de filtrado:
 - Sandboxing: Los archivos adjuntos sospechosos se abren o ejecutan en varios entornos protegidos y separados en los que se analiza su comportamiento en cuanto a efectos dañinos. Se consideran particularmente sospechosos los archivos adjuntos que contienen código ejecutable.
 - Link Scanning: Se prueban las URLs incluidas en correos o archivos adjuntos y se analiza su comportamiento.
 - Link Rewriting: Las URLs incluidas en los correos se sustituyen por otras que dirigen hasta su contenido a través de Web Filter. Si es preciso, se analiza el comportamiento de los archivos descargados mediante Sandboxing. Los contenidos clasificados por Web Filter como potencialmente peligrosos se bloquean.
 - Targeted Fraud Forensics: Filtros heurísticos para identificar ataques selectivos que comprueban la autenticidad e integridad de metadatos y contenidos de correos, identifican y bloquean identidades de remitentes falsas, identifican contenidos falsificados, ataques a datos especialmente sensibles y, particularmente, a aquéllos relativos a pagos (p. ej., datos de tarjetas de crédito, facturas, órdenes de pago), así como ataques selectivos a personal especialmente expuesto del cliente (p. ej., Contabilidad, CFO, CEO, Controlling).
 - Freezing: "Congelación" temporal de correos sospechosos. Los correos "congelados" se procesan de nuevo con filtros actualizados al cabo de unos minutos.
 - Malicious Document Decryption: Los archivos adjuntos cifrados en formato de Office, archivos comprimidos y archivos PDF se abren antes de entregarse al destinatario para comprobar si contienen software malicioso siempre que la contraseña pueda reconstruirse a partir del correo.
 - Alertas Ex-Post: Si, al cabo de un tiempo, se descubre que un correo entregado debe ser clasificado como potencialmente peligroso, el equipo de seguridad informática de la empresa cliente recibe una alerta al respecto

- 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 puede configurar listas blancas (remitentes permitidos) y negras (remitentes bloqueados) por usuario, dominio y cliente.
- El administrador puede configurar reglas específicas que aplicarán al correo entrante y/o saliente y que podrán definirse a nivel de cliente.
- En las reglas definidas por el administrador se debe 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 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.
- Permite establecer dominios sobre las que no se realizará la opción de marcado.
- Actualización periódica de reglas y filtros.
- Dispone 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 antispham.
- Los reportes de cuarentena deberán cumplir:
 - Personalización completa, al menos, de logo de cliente, 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 del Ayuntamiento de Irun. 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.

4.- Para futuras ampliaciones de servicio de seguridad, el proveedor deberá poder ofrecer, en la misma plataforma, las siguientes soluciones avanzadas en seguridad de correo:

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 deberá operar en línea: Deberá 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,
- Deberá 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.
- Deberá 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.
- Este análisis de URLs deberá ser ofrecido en modo "proxy" y no solo 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.
- Deberá poseer una tecnología de detección de amenazas avanzadas y persistentes (ATP) 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
 - "Puntuación del 1 al 10" de cada fichero analizado por la solución ante las amenazas, basándose en técnicas de red, de comportamiento y análisis estático.
 - Informe de resumen de todos los procesos detectados tanto de comportamiento, de análisis de red y procesos estáticos
 - Capturas de pantallas del entorno virtual al ejecutar el fichero/archivo.
 - Comprobación y análisis de más motores Antivirus contra terceras plataformas (por ejemplo, VirusTotal).

Servicio de Archiving

La herramienta deberá disponer de un servicio de archivado que cumpla con las siguientes condiciones:

- Los correos del cliente se archivan en los propios sistemas informáticos del fabricante de un modo auditable.
- Los correos archivados están disponibles para su acceso a través de Internet por parte de usuarios autorizados. Existen opciones de búsqueda de correos archivados por diversos criterios y contenidos que facilitan la localización de determinados correos en el archivo. Los usuarios autorizados pueden disponer una nueva entrega de los correos archivados a los sistemas del cliente de modo interactivo.
- El acceso por parte de usuarios autorizados se efectúa a través de una interfaz web (Control Panel) o de una aplicación web dinámica que debe estar disponible tanto para Android como para iOS.
- El periodo de archivo y determinadas excepciones al proceso de archivo pueden definirse a nivel de dominio, grupo o usuario.
- Se garantizará la disponibilidad de los correos archivados para el cliente, durante el periodo previamente configurado por éste en años completos a partir del año natural siguiente a aquél en el que se haya enviado o recibido el correo archivado en cuestión.
- El periodo de archivo predeterminado será de 5 años, pudiendo el cliente modificar la configuración, aplicándose dichos cambios a los correos recibidos a partir del momento en que se realicen, pero no de modo retroactivo.
- Los usuarios autorizados pueden marcar correos como "privados". Los correos marcados como "privados" dejarán de ser accesibles desde el archivo.
- Se garantizará a los usuarios autorizados la accesibilidad a los correos archivados, por regla general, las 24 horas del día, todos los días del año, con excepción de los periodos de mantenimiento.

- Ciertos usuarios con autorizaciones especiales podrán establecer un acceso especial a todos los correos archivados de un periodo determinado (acceso de auditoría, p. ej., con objeto de una auditoría externa). El establecimiento y el uso de los accesos de auditoría se registran.

- Se archivarán los siguientes correos:

- a) Correos enviados a terceros

- b) Correos enviados al cliente por parte de terceros

- c) Correos facilitados por el cliente para su archivo a través de interfaces acordadas (correos internos, opcional).

- El archivo cumple las disposiciones legales relativas al archivo electrónico de correos actualmente vigentes, y la herramienta hará cuanto esté de su mano para garantizar el cumplimiento de las disposiciones legales incluso en caso de que éstas cambien.

- Se garantizará la asistencia técnica a usuarios autorizados

- Se garantizará la confidencialidad frente a terceros de los datos archivados y otros secretos comerciales del cliente que se revelen en el contexto del presente contrato. La obligación de confidencialidad perdurará más allá del fin del presente contrato.

Descripción del servicio Email Encryption

- La herramienta cifra y firma correos salientes y descifra correos entrantes del cliente en sus propios sistemas informáticos conforme a las directivas definidas.

- Los correos salientes se firman mediante S/MIME siempre que se disponga de las claves privadas necesarias en el almacén de certificados.

- Los usuarios autorizados del cliente pueden configurar las normas de cifrado de correos salientes

- En función de las normas que haya definidas, los correos salientes pueden tratarse de diversos modos:

- a) Transmitirse cifrados con la clave pública del destinatario mediante S/MIME o PGP.

- b) Transmitirse sin cifrar, pero a través de un canal cifrado con TLS.

- c) Facilitarse al destinatario de modo seguro.

- d) Transmitirse sin cifrar.

- Si la directiva requiere la transmisión cifrada, pero no se dispone de la clave pública necesaria del destinatario en el almacén de certificados y la transmisión por TLS (de estar configurada) no es compatible con el servidor de recepción, los correos salientes destinados al destinatario en cuestión se rechazan y no se transmiten.

- Los correos entrantes cifrados mediante S/MIME o PGP se descifran automáticamente siempre que se disponga de la clave privada necesaria del remitente en el almacén de certificados.



- Las claves públicas se extraen automáticamente de las firmas de los correos entrantes y se almacenan en el almacén de certificados.
- Se garantizará la confidencialidad de las claves privadas del cliente depositadas en el almacén de certificados. La obligación de confidencialidad perdurará más allá del fin del presente contrato.

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

- La solución ofertada deberá 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 amenaza 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)

Administración

- La gestión y administración de la solución de seguridad deberá ser ofrecida y gestionada desde el mismo Panel de Control
- La solución deberá permitir integración con la nube de Microsoft365, sin necesidad de configuración en el entorno de Microsoft 365, para la sincronización, como mínimo, de dominios, buzones e información sobre servidores destino.
- 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 deberá disponer de la posibilidad de integrar la información ofrecida en el Log de Correo con un sistema SIEM.

- Los administradores podrán recibir, en tiempo real, una notificación de alerta cuando una amenaza avanzada sea detectada por los motores
- Deberá 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 transparente 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 su organización) deberán 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 deberá 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 mínimo castellano, inglés y alemán.
- La solución deberá 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 empresa, permitiendo adaptar la consola a las diferentes imágenes corporativas.
- Acceso a la consola autenticado y cifrado usando el protocolo https.
- Deberá 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 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 permitir que los administradores de empresa gestionen la cuarentena de los usuarios de manera centralizada.
- Deberá 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 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 y con un periodo mínimo de retención de esta información de 90 días.
- 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 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 en cuanto a número.

5.- Firmas de correo y disclaimer

CARACTERÍSTICAS

- Integración de Active Directory : Las firmas creadas de todos los usuarios se rellenaran automáticamente con los datos de contacto del perfil de Active Directory. Incluso los ajustes más pequeños se sincronizarán inmediatamente por LDAP y se mantendrán actualizados
- Importación de código fuente HTML de firmas existentes utilizando el código fuente HTML. El diseño, el formato y las imágenes insertadas se conservarán en su totalidad. Los cambios añadidos que puedan verse directamente en el editor.
- Cumplimiento legal: Deberá complementar las firmas con un disclaimer para cumplir con la información obligatoria en la comunicación por correo electrónico.
- Diseño flexible: Además de los archivos de imagen, también podrá colocar enlaces y formatos de texto en la posición que se desee en el disclaimer.
- Función de previsualización: Después de editar en el editor WYSIWYG („What you see is what you get“), se podrá ver anticipadamente la plantilla para los diferentes grupos de usuarios.
- Banner publicitario con control ampliado: Se deberá complementar las firmas de correo electrónico de la empresa con banners publicitarios originales, que se podrán activar o desactivar con unos pocos clics y crear durante la asignación de grupos.
- Comunicación y redes seguras: Se podrán colocar en las redes sociales botones con enlace a la empresa en cada uno de tus correos electrónicos salientes para aumentar el conocimiento de la marca.
- Pantalla optimizada para móviles: Dado que la mayoría de los emails enviados se basan en HTML, los clientes de correo electrónico móvil podrán ver archivos de imágenes sin problemas. La firma del correo electrónico o el disclaimer se añadirá al correo electrónico después de su envío



- Asignación grupal: Para cada usuario creado en Active Directory se podrá crear una firma individual o un disclaimer para cada grupo

6.- Requisitos del servicio de relay de correo

El relay de correo debe de disponer de un pool de direcciones IP suficiente como para evitar en todo momento que los correos enviados desde el dominio irun.org o bidasoa-activa.com tengan problemas de entrega por estar incluida la IP de salida del correo en listas negras. Dicho pool de Ip's deberá estar compuesto al menos por 20 Ip's diferentes. En caso de producirse problemas con el envío o recepción de correos debido a la inclusión de las Ip's de relay en listas negras, se considerará como una falta grave y se aplicaran las penalizaciones recogidas en la contratación.

7.- Requisitos y valores de servicio requeridos para la solución

- La tasa de detección de spam mensual deberá ascender como mínimo al 99,9% de media en relación a todos los correos recibidos por los dominios del Ayuntamiento de Irun en el periodo analizado. Esto requiere que todos los correos entrantes se entreguen por SMTP a los sistemas mediante modificación de los registros MX de los dominios del Ayuntamiento de Irun
- La tasa de falsos positivos media mensual se deberá situar por debajo del 0,00015% respecto a los correos limpios recibidos por dominios del Ayuntamiento de Irun en el periodo analizado. Esta tasa no incluye aquellos correos que hayan sido enviados a través de servidores mal configurados (no conformes a RFC), "open relays" verificados o clientes de correo mal configurados
- La disponibilidad en el tráfico de correo vía SMTP ascenderá al 99,99% de media anual. Esto requiere que todos los correos entrantes se envíen directamente por SMTP a los sistemas mediante modificación de los registros MX. En el cálculo de la disponibilidad no se incluyen las labores de mantenimiento planificado, las cuales se efectúan, en la medida de lo posible, en horario nocturno (CET) durante los fines de semana.
- La tasa de detección de virus media anual ascenderá como mínimo al 99,99% respecto a los correos recibidos por los dominios del Ayuntamiento de Irun en el periodo analizado
- El soporte tiene que ser 24x7 ofrecido como mínimo en español
- El fabricante de la solución deberá garantizar el acceso al panel de control de la herramienta una disponibilidad del 99,9%, de media mensual. Quedan expresamente excluido de la disponibilidad los problemas en el entorno de hardware y software del Ayuntamiento de Irun y los problemas de conexión en las telecomunicaciones.

- Los plazos de entrega medios de los correos serán inferiores a 30 segundos, con plazos de entrega máximos de 3 minutos.
- Los correos en cuarentena se almacenarán y pondrán a disposición de los usuarios autorizados por el cliente durante un periodo de tres meses. Si el Ayuntamiento de Irun lo requiere, se informará a los usuarios sobre los nuevos correos que se hayan puesto en cuarentena (por regla general, una vez al día).
- Los usuarios autorizados podrán acceder desde Internet a los correos en cuarentena. Los usuarios autorizados podrán hacer que se entreguen los correos en cuarentena a los sistemas del cliente de modo interactivo.
- Los usuarios autorizados por el Ayuntamiento de Irun (p. ej., empleados de soporte técnico o administradores) podrán supervisar al completo el tráfico de todos los correos de la organización a través de un panel de control que permita realizar un seguimiento en directo de los correos bloqueados (rechazados) de los últimos 7 días.
- En caso de que el fabricante vaya a realizar trabajos de mantenimiento y reparación programados que vayan a interrumpir o restringir la prestación de servicios y el acceso al panel de gestión de la herramienta, deberá informar a los técnicos del Ayuntamiento de Irun con antelación. No obstante el fabricante deberá realizar los trabajos de mantenimiento durante los períodos de uso reducido y en especial, durante el fin de semana.
- Lo indicado anteriormente, no se tendrá en cuenta cuando el fabricante tenga que realizar actuaciones urgentes e inmediatas para evitar amenazas específicas a la seguridad e integridad de los sistemas
- Las paradas programadas no se incluirán en el cálculo de la disponibilidad del panel de control, pero las paradas programadas no pueden exceder un total de 3 horas al mes

8.- Requisitos para el proceso de instalación de la solución

La instalación de la herramienta se realizará in situ en las dependencias del Ayuntamiento de Irun, por técnicos con experiencia contrastada en la herramienta de la empresa adjudicataria de acuerdo al siguiente procedimiento:

Primera fase:

Al menos 3 jornadas in situ en dependencias del Ayuntamiento de Irun que contemplaran los siguientes aspectos:

- Recogida de datos de la configuración del correo del Ayuntamiento de Irun
- Instalación y configuración de la herramienta.
- Jornada de formación en la herramienta a los técnicos del Ayuntamiento de Irun
- Entrega de la documentación de la instalación así como un manual de la herramienta.



Segunda fase:

2 jornadas in situ en las dependencias del Ayuntamiento de Irun en aproximadamente 15 días desde la fecha de realización del despliegue que incluirá:

- Un análisis del funcionamiento de la herramienta en ese periodo.
- Una jornada de formación a los técnicos del Ayuntamiento de Irun con la herramienta funcionando en real, explicando las configuraciones definitivas que se hayan realizado
- Se complementará la documentación entregada al final de la fase 1 con las configuraciones definitivas.

En el periodo comprendido entre la primera y segunda fase la empresa adjudicataria deberá proporcionar al Ayuntamiento de Irun el contacto de un técnico con el que los Técnicos del Ayuntamiento de Irun se puedan poner en contacto para aclarar dudas o problemas que se puedan detectar. El periodo entre estas 2 fases se considera muy importante para una correcta configuración de la herramienta y evitar posibles incidencias de falsos positivos.

9.- Servicio de soporte por parte de la empresa adjudicataria

9.1 Alcance

Se debe ofrecer un servicio REMOTO de gestión de la plataforma implantada. Este servicio supone la gestión de la plataforma por personal con experiencia contrastada en ella, encargándose del funcionamiento, configuración, actualización y gestión de las diferentes incidencias que puedan suceder.

9.2 Características

El servicio de soporte ofrecido por la empresa deberá incluir al menos los siguientes aspectos:

- ANÁLISIS Y GESTIÓN DE INCIDENCIAS DE PRODUCTO:

En caso de producirse una incidencia en el producto instalado, se proporcionará asistencia realizando las siguientes tareas:

- Análisis de la incidencia y propuesta de resolución en base a la experiencia de los técnicos
- Apertura y seguimiento de la incidencia con el fabricante en caso de no resolverse con las indicaciones anteriormente propuestas

Durante todo el proceso, el personal técnico de la empresa informará puntualmente a los técnicos del Ayuntamiento de Irun en base a los canales de comunicación establecidos con el propio cliente (Mail, teléfono, etc.)

- CONSULTAS SOBRE EL PRODUCTO CONTRATADO:

Los técnicos del Ayuntamiento de Irun podrán consultar al departamento de soporte de la empresa adjudicataria información sobre:

- Nuevas versiones del producto.

- Parches.
- Funcionalidades (nuevas o ya adquiridas por el cliente).
- Dudas al respecto del funcionamiento de la plataforma.

- INTERVENCIONES DE SOPORTE REMOTAS SOBRE LA CONSOLA.

Respecto a las eventuales incidencias que se puedan producir sobre la consola de gestión de la herramienta, la empresa adjudicataria realizará la operativa para la resolución de la incidencia.

La operativa de intervenciones de soporte remotas, aplicación de medidas extraordinarias y actualizaciones críticas, será la siguiente:

- La empresa solicitará la realización de intervención, mediante el envío de un mail a los técnicos del Ayuntamiento de Irun.
- La fecha para comenzar los trabajos será dentro de un plazo de tiempo razonable, en horario laboral y de mutuo acuerdo entre los técnicos del Ayuntamiento de Irun y la empresa adjudicataria.
- Durante todo el proceso los técnicos de la empresa adjudicataria informará puntualmente a los técnicos del ayuntamiento de Irun a través de los canales de comunicación que se establezcan (E-mail, teléfono, etc.).

- SERVICIO 24X7

La herramienta ofertada deberá de disponer de un servicio de 24x7 ofrecido por el fabricante de la solución.

10.- Ofertas

La oferta económica incluirá todos los gastos que se deriven del cumplimiento de las condiciones estipuladas en este pliego. No se abonarán otros conceptos ni aumentos de la oferta presentada.

En Irun, a fecha de la firma

Eusebio Hernández
Técnico de Sistemas

POSTARAKO ANTISPAM ETA ERRELE SOLUZIO BATEN HORNIKUNTZAREN KONTRATAZIOA ARAUTZEKO BALDINTZA TEKNIKOEN PLEGUA

1. Kontratuaren xedea

Baldintza teknikoaren plegu honek finkatzen dituen baldintzetan irun.org eta bidaso-activa.com domeinuetako postarako antispam eta errele soluzio bat hornitzea da kontratu honen xedea.

Eskaintzek honako hauek hartu beharko dituzte barnean:

- Tresna Irungo Udalen behar eta eskakizunen arabera konfiguratzeko, behar bezala funtziona dezan.
- Udaleko teknikariak tresnaren funtzionamenduan trebatzea.
- Teknikari espezializatuen eskulana eta joan-etorriak beharrezkoa denean.
- Irungo Udalean tresna kudea dezaketen teknikariak izanda ere, kontratuak irautean duen hiru urteetan laguntza zerbitzua ematea. Tresnak oker funtzionatzen badu eta teknikariak konpondu behar badute erantzuna emateko epeak egokiak izatea bermatu beharko da; hain zuzen ere, honako hauek:

- Telefono, web eta posta elektronikoko bidez, 8 x 5
- Gorabeheretako erantzuteko, lanegunetan (astelehenetik ostiralera bitartean), lau ordu edo gutxiago
- Kontsultetako erantzuteko, lanegunetan (astelehenetik ostiralera bitartean), lau ordu edo gutxiago

Zehatz-mehatz, eskaintzek deskribatu beharko dute zer prozedurari jarraituko zaion telefonoaren, webgunearen zein posta elektronikokoaren bidez tresnaren funtzionamendu okerrarengatik gorabeherarik sortzen denean edo kontsulta teknikorik dagoenean.

Tresnaren funtzionamendu okerrarengatik gorabeherarik sortzen denerako prozedurei buruzko atalean, matxura bat edo tresnaren funtzionamendu okerra jakinarazten denetik enpresa esleipendunak esku hartzen edo jakinarazitako arazoari buruzko informazio baliagarria ematen duen arte edo Zerbitzu Teknikoak zuzenean soluzio posible bat eskaintzen duen arte igarotzen den epea hartuko da "erantzuna emateko epea"; hau da, gorabeheraren berri jaso izana adierazteko ondorioetarako erantzute hutsa edo kasu zenbakia esleitze hutsa ez da hartuko gorabehera konpontzetzat, eta, horrenbestez, ezta erantzun ofiziala ematetzat.

- Gorabeheren sailkapena. Garrantziaren eta kritikotasunaren arabera, kritikoak, urgenteak edo arinak izan ahalko dira gorabeherak, eta honako hauek izango dira bakoitzari erantzuna emateko gehieneko epeak:
 - o Gorabehera kritikoak <= 5 h
 - o Gorabehera urgenteak <= 9 h
 - o Gorabehera arinak <= 24 h

*Fabrikatzailearen ardura diren gorabeherak konpontzeko epea ez da sartuko enpresak erantzuna emateko epearen barruan.

Enpresen eskaintzek erantzuna emateko epe hobeak proposatu ahalko dituzte.

- Fabrikatzailearen jakintza basera sartzea.
- Gorabeheraren bati lehen mailan erantzuten ez zaionean eskalatzea kudeatzea



- Tresnaren instalazio eta konfigurazioari buruzko dokumentazioa prestatzea eta Irungo Udaleko Informatika Departamentuari entregatzea. Kontratuaren indarraldian aldatzen diren heinean kontratatzen diren zerbitzuen barruko elementuen instalazio eta konfigurazioari buruzko dokumentazioa egunean izateko konpromisoa hartuko du enpresa esleipendunak.

Ezinbesteko baldintza da enpresa eskaintzaileak proposatutako soluzioarekiko lankidetzaz izatea eta egiaztatuko da soluzioaren fabrikatzaileak emandako dokumentu baten bidez.

2. Instalazioen deskripzioa

Irungo Udalak badu Microsoft Exchangeko posta zerbitzari bat, posta domeinu hauek ostatatzen dituena:

- irun.org
- bidasoa-activa.com

Bi domeinuen artean, 750 postontzi inguru ditu Irungo Udalak, eta, orain, **810 lizentziatarako** antispam eta errele soluzio bat eskuratu nahi du.

Irungo Udalak ere baditu banaketarako posta-taldeak, berezko helbidea dutenak, eta ez dira lizentzia-kopuruaren barruan zenbatu behar.

Udal langileek bidalitako mezuez gain, albiste masiboen buletinak ere bidaliko dira tresnaren errele zerbitzuaren bidez. Bidalketa masibo horiek 12.000 hartzaile ingururi egiten zaizkie, eta errele zerbitzuak bidalketa horiek kudeatzeko gai izan behar du.

3. Postarako antispam eta errele soluzioaren eskakizunak

Eskakizun hauek bete beharko ditu postarako eskaintzen den antibirus eta errele soluzioak

Orokorrak

- Oso arkitektura eskuragarrian oinarritu beharko du, eta hitzartzen den zerbitzu maila ziurtatu.
- Hornitzaileak bere azpiegituratik eskaini beharko du zuzenean; hau da, ezingo du ekipamendurik instalatu Irungo Udalaren barne sarean.
- Erabiltzen den arkitekturak soluzioaren eskalatze ahalmena bermatuko du: Irungo Udalaren hasierako beharretara egokitutako ingurune batean martxan jartzeko aukera eman, eta Irungo Udalaren eskakizunen arabera bilakatu.
- Posta iragazteko zerbitzuak eta Irungo Udalak aurrerago sartu nahi dituen artxibatze eta enkriptatze zerbitzuak integratzeko aukera eman beharko du.

Iragazketa

- SMTP trafikoan (posta elektronikoan) spama, birusak eta nahi ez den edukia iragazteko soluzio perimetrala izan beharko du.
- Sartzen eta irteten diren mezuak babestu, eskaneatu eta iragazi beharko ditu.
- TLS Transport Layer Security zifratze teknologia (gutxienez, TLS 1.2 bertsioa) baliatzeko aukera eman beharko du.
- Garraio geruza seguru bat (TLS) erabiliz IP, domeinu edo helbide bidez konfiguratzen diren hartzaileei posta transmititzea behartzeko aukera eman beharko du.

Konexio iragazkiak

- Iragazketa metodo bat baino gehiago izan beharko du, emaitzaren arabera mezuak baztertzen edo spam gisa markatu eta erabiltzaileak baliozkotu ditzan uzten dituen.
- Fabrikatzailearen ospe zerbitzua izan beharko du, edo IP helbidearen ospea egiaztatzeko motor bat baino gehiago.
- Administrazioaileak blokeatu beharreko IP helbideak adierazteko mekanismoren bat izan beharko du.
- Irteten diren mezuei dagokienez, zera egiaztatu eta kontrolatu beharko du:
 - "Open relay" delakoa ez erabiltzea
 - Jatorrizko IP helbidea zerrenda beltzen batean badago administrazioaileari abisua helaraztea
- Jatorrizko IP helbidea RBL batean badago, greylisting teknikak aplikatu beharko ditu.
- IPv4 helbideen, helbide elektronikoaren eta domeinuen zerrenda beltz eta zuriak sortzeko aukera eman beharko du, kudeatzen den domeinu bakoitzerako.
- Zerbitzua ukatzen duten erasoak (DoS motako erasoak) kontra babesteko aukera eman beharko du.
- DNSBL eta SPF teknologietan oinarrituz, konexioak iragazteko aukera eman beharko du.
- Jatorrizko domeinuaren MX erregistrorik baden kontuan izanik, hura baliozkotzeko aukera eman beharko du.
- Hartzailea baden egiaztatzeko aukera eman beharko du, existitzen ez diren kontuetara bidaltzen den spama ezabatzeko.
- Sartzen diren mezuek DKIM sinadura goiburuak badituzte, iragazkiak egiaztatu egin beharko ditu, DKIM sinadurarekin lotutako domeinua baliozkotuz.

Malwarearen kontrako iragazkiak



- Sartzen eta irteten diren mezu guztiak analizatzeko gai izan beharko du.
- Birusak iragazteko osagaia etengabe eguneratu beharko du (azken sinadurak eta/edo eguneraketak izan beharko ditu).
- Arriskutsuak izan daitezkeen eranskinak (exekutagarriak, etab.) dituzten mezuak iragazi beharko ditu.
- Bezeroaren posta sistema babestu beharko du banakako erasoetatik eta eraso selektiboetatik, hala nola Spearphishing, Blended Attacks, Advanced Durent Threats, Ransomware eta CEO Falld.
- Egon daitezkeen erasoak identifikatzeko, honako iragazteko teknika hauen bidez aztertuko dira susmagarritzat jotzen diren bezeroaren mezuak:
 - Sandboxing: fitxategi erantsi susmagarriak hainbat ingurune babestu eta bereizitan irekitzen edo exekutatzen dira, eta horietan aztertzen da haien portaera ondorio kaltegarriei dagokienez. Bereziki susmagarritzat jotzen dira kode exekutagarria duten fitxategi erantsiak.
 - Scanning esteka: mezuetan edo fitxategi erantsietan sartutako URLak probatzen dira eta haien portaera aztertzen da.
 - Rewriting esteka: mezuetan sartutako URLen orde, edukira Web Filter bidez eramango duten beste batzuk jarriko dira. Beharrezkoa bada, Sandboxing bidez aztertuko da deskargatutako fitxategien portaera. Web Filter-en arabera arriskutsuak izan daitezkeen edukiak blokeatu egingo dira.
 - Targeted Falld Forensics: iragazki heuristikoak dira metadatuaren eta postako edukien benetakotasuna eta osotasuna egiaztatzen duten eraso selektiboak identifikatzeko, igorle faltsuen identitateak identifikatu eta blokeatzeko, eduki faltsuak identifikatzeko, datu bereziki sentikorrekiko erasoak identifikatzeko eta, bereziki, ordainketei buruzkoak (adibidez, kreditu-txartelen datuak, fakturak, ordainketa-aginduak), bai eta eraso selektiboak ere arrisku handiena duten bezeroaren langileei (adibidez, kontabilitatea, CFO, CEO, Controlling).
 - Freezing: mezu susmagarriak aldi baterako "izoztea". Mezu "izoztuak" berriro prozesatuko dira eguneratutako iragazkiekin minutu batzuen buruan.
 - Malicious Document Decryption: Office formatuan zifratutako fitxategi erantsiak, fitxategi konprimatuak eta PDF fitxategiak hartzaileari eman aurretik irekitzen dira, software maltzurra duten egiaztatze, betiere pasahitza postatik berreraiki badaiteke.
 - Ex-Post alertak: denbora baten buruan ikusten bada emandako mezu bat arriskutsu gisa sailkatu behar dela, enpresa bezeroaren segurtasun informatikoko ekipok alerta bat jasoko du horri buruz.
- Mezu infektatuak berrogeialdian jartzeko aukera eman beharko du.

- Administratzaileak jakinarazpenak bidaltzeko irizpideak hautatzeko aukera eman beharko du; alegia, infektatutako mezuen hartzaileei azken erabiltzailearentzako txosten pertsonalizagarri bat bidali ala ez erabakitzeko aukera eman beharko du.
- Birusen kontrako iragazkiak online funtzionatu beharko du: azken erabiltzaileentzako mezu infektatuak osorik atxiki eta inoiz ez entregatzeko eta aldi berean mezu infektatuak analizatzeko aukera eman beharko du.

Spamaren kontrako edukiko iragazkiak

- Administratzaileak zerrenda zuriak (baimentzen diren igorleenak) eta beltzak (blokeatzen diren igorleenak) konfiguratzeko aukera eman beharko du, erabiltzailearen, domeinuaren eta bezeroaren arabera.
- Administratzaileak sartzen eta/edo irteten diren mezuei aplikatu behar zaizkien eta bezero mailan defini daitezkeen arau espezifikoak konfiguratzeko aukera eman beharko du.
- Gutxienez honako hauetan oinarritzen diren baldintzak definitzeko aukera eman beharko du administratzaileak definitzen dituen araei dagokienez:
 - Mezuen jatorria
 - Mezuen hartzaileak
 - Gaiaren edukia
 - Mezuen gorputza
 - Eranskin mota edo eranskinen edukia
 - Mezuen tamaina
 - Goiburu jakin batzuen existentzia
- Arauak definitzerakoan espresioak erabiltzeko aukera eman beharko du.
- Arauen baldintzen artean testu formatuko fitxategi erantsi irakurgarrien edukia aztertu ahal izateko aukera eman beharko du.
- Markatu ezin diren domeinuak ezartzeko aukera eman beharko du.
- Arau eta iragazkiak aldi-aldi eguneratuko ditu.
- Mezuen hizkuntza, formatua eta kodetzea gorabehera spam mezuak detektatzeko gai den motor bat izan beharko du.
- Mezuen edukia mezuen puntuazioan oinarrituz iragazteko aukera eman beharko du.
- Eskatu gabeko spam mezuak eta eskatutako mezu komertzialak (bestela esanda, erabiltzaileak harpidetzen diren banaketa zerrenda komertzialak) berrogeialdi



desberdinetan jartzeko eta azken erabiltzaileek berauek kudeatzeko aukera eman beharko du.

- Azken erabiltzaileek eskatutako mezu komertzialak beren postontzian nahi dituzten edo antispam zerbitzuan atxiki nahi dituzten hautatzeko aukera eman beharko du.
- Berrogeialdiei buruzko txostenek baldintza hauek bete beharko dituzte:
 - Gutxienez bezeroen logoak, erantzukizunari uko egiteko testua, igorleen helbideak eta testua osorik pertsonalizatzeko aukera ematea
 - Berrogeialdian jarritako mezuen edukiaren aurrebista ikusteko aukera ematea
 - Gutxienez ordutegi jakin bati jarraikiz sortzea eta erabiltzaileek txostenen sorrera konfiguratzeko aukera ematea
 - Domeinu osorako txosten bat sortzeko aukera ematea
 - Erabiltzaileentzako txostenetan zer mezu mota azaltzen diren eta erabiltzaileek zer egin dezaketen (bistaratzeko edo askatzeko dituzten) erabakitze aukera ematea

Phishingaren kontrako edukiko iragazkiak (erabiltzaileen identitatea ordeztearen kontrako prebentzioa)

- Domeinu igorleek identitatea ordeztu duten detektatzeko estandarren bidez (gutxienez, DKIM eta DMARC tekniken bidez) egin beharko du iragazketa.
- SPF, DKIM eta DMARC egiaztapen protokoloetarako erabaki matrizean oinarritutako konfigurazio aurreratua baliatzeko aukera eman beharko du.
- SPF egiaztapen iragazkiaren bidezko analisiak "envelope from", "header from" edo biak oinarri dituen konfigurazioa baliatzeko aukera eman beharko du.
- Mezuak identifikatzeko teknika edo mekanismo desberdinak erabiltzeko aukera eman beharko du:
 - Asmoaren bereizketa
 - Posta metadatuaren osotasun eta egiazkotasunaren egiaztapena
 - Antzekotasun bidezko igorleen faltsutzea
 - Isilpeko informazioa eskuratzeko eskaeren detekzioa

Posta elektronikoko korporatiboaren jarraitutasun eta eskuragarritasuna

- Gutxienez zazpi egunez atxiki (ilaran jarri) beharko ditu behin iragazkiek prozesatuta antolakundearen posta zerbitzariari entregatuak izaterakoan aldi baterako erroreren bat (dela komunikazio lineen akatsen ondoriozkoa, dela Irungo Udalaren posta zerbitzua aldi

baterako erabilgarri ez dagoelako gertatutakoa) izan duten **mezuak**, eta atxikitako mezuak soluzioaren administratzaileek eskuz ezer egin gabe entregatzen saiatu beharko du aldian-aldian.

- Behin prozesatuta mezuak antolakundeko posta zerbitzari bati edo gehiagori entregatzeko aukera eman beharko du. Alde horretatik, mezuak entregatzeko lehentasunak zehazteko aukera eman beharko du, eta are karga antolakundeko azken erabiltzaileen postontziak ostatatzen dituzten posta zerbitzarien artean banatzeko aukera ere.
- Destinoko zerbitzari nagusia erortzen bada sartzen eta irteten diren mezuak gutxienez 90 egunez biltegiratzeko eta larrialdiko web interfaze bat erabiltzeko kontingentziatzeko soluzio bat **eskaintzeko aukera** eman beharko du.

4.- Etorkizunean segurtasun-zerbitzua zabaltzeko, hornitzaileak honako irtenbide aurreratu hauek eskaini ahal izango ditu postaren segurtasunari dagokionez, plataforma berean:

Mehatxu aurreratuen iragazketa (ATP)

- Sartzen diren mezuak asmo txarreko softwareen aurrean (birusak, troiarrak, harrak, etab.), bai ezagunak bai ezezagunak, babesteko gaitasuna izan behar du (zero ordua).
- Mehatxu aurreratuen iragazketak linean jardun beharko du: azken erabiltzaileei bidalitako mezu kutsatuak erabat atxikitzeko gaitasuna izan beharko du eta ez ditu inoiz entregatuko, eta kutsatutako postaren analisi paraleloa egin beharko du.
- Hala badagokio, ATPren analisi heuristikoa egingo zaie. Aztertutako postak malwarez kutsatutako fitxategi erantsiak baditu, horiek sistemaren berrogeialdian islatuko dira. ATP bidez fitxategiak aztertzeko prozesuak estatistiketan jaso beharko dira.
- Mezueta fitxategi erantsien azterketa sakona egin beharko du, detektatzeko teknika heuristikoa erabilita (adibidez, Sandboxing), portaerak ekar ditzakeen mehatxuak identifikatu ahal izateko, eta ez du oinarritu behar alde aurretik ezagutzen diren malware izenpeko mehatxuen detekzioan.
- Dokumentuei edo mezuen gorputzei erantsitako URLak analizatu ahal izango ditu.
- Ahalik eta babes handiena eskaintzeko, erabiltzaileak esteka irekitzen duen unean jasotako mezu elektronikoko URLen analisia egin beharko du sistemak, horrela, biktimei bidalitako URLetan aipatutako edukia aldatzen duten malware kanpainen erasoak saihesteko.
- URLen analisi hori "proxy" moduan eskaini beharko da, eta ez aipatutako estekaren exekuzioaren emaitzaren analisiaren bidez bakarrik.
- Posta babesteko erabiltzen den teknologia ez du inolako aldaketarik egin behar mezuen eranskinetan, hala nola makroak edo scriptak desgaitu. Mehatxu aurreratuen aurkako babes geruza prozesatu ondoren, erabiltzaileari helarazitako informazioak bermatu behar du posta osorik mantenduko dela prozesatu ondoren azken erabiltzaileari ematean.
- Mehatxu aurreratuak eta iraunkorrak atzemateko teknologia (ATP) izan beharko du, ihes tekniken aurkakoa, teknika horien bidez, aztertutako malware programek beren portaera maltzurra ezkutatu ahal izango baitute analisi ingurune jakin batzuetan, eta detektatu gabe igaro ahal izango baitira.



- “Sandbox” unitatean aztertutako fitxategiei buruzko txostenetarako sarbidea eman beharko du, eta, bertan, gutxienez, informazio hau egongo da eskuragarri:
 - Fitxategiaren hash-a
 - Aztertutako fitxategi bakoitzaren “1etik 10era bitarteko puntuazioa”, mehatxuen aurrean emandako soluzioagatik, sare eta portaera tekniketan eta analisi estatikoan oinarrituta.
 - Atzemandako prozesu guztien laburpen txostena, portaerari, sare analisiari eta prozesu estatikoei dagokienez.
 - Ingurune birtualeko pantailen kapturak fitxategia/artxiboa exekutatzean.
 - Hirugarren plataformen aurkako antibirus motor gehiago egiaztatzea eta aztertzea (adibidez, VirusTotal).

Archiving zerbitzua

Tresnak honako baldintza hauek beteko dituen artxibatze zerbitzua izan beharko du:

- Bezeroaren mezuak fabrikatzailearen sistema informatikoetan bertan artxibatuko dira, ikuskatzeko moduan.
- Baimendutako erabiltzaileek Internet bidez eskuratzeko moduan daude artxibatutako mezuak. Badaude artxibatutako mezuak hainbat irizpideren eta edukiren arabera bilatzeko aukerak; horiek erraztuko baitute artxiboan mezu jakin batzuk aurkitzea. Artxibatutako mezuak bezeroaren sistemetara modu interaktiboan entregatzeko aukera dute baimendutako erabiltzaileek.
- Web-interfaze baten bidez (Control Panel) edo Android nahiz iOS sistemetarako erabilgarri egon behar duen web aplikazio dinamiko baten bidez sartuko dira baimendutako erabiltzaileak.
- Artxibatze aldia eta artxibatze prozesuaren salbuespen jakin batzuk domeinu, talde edo erabiltzaile mailan defini daitezke.
- Artxibatutako mezuak bezeroarentzat eskuragarri egongo direla bermatuko da, bezeroak aurrez konfiguratutako epean, urte osoetan, artxibatutako posta bidali edo jaso eta hurrengo urte naturaletik aurrera.
- Aurrez zehaztutako artxibo aldia 5 urtekoa izango da. Bezeroak konfigurazioa aldatu ahal izango du, eta aldaketa horiek egiten diren unetik aurrera aplikatuko zaizkie jasotako mezuei, baina ez atzeraeraginez.
- Baimendutako erabiltzaileek "pribatu" gisa marka ditzakete mezuak. "Pribatu" gisa markatutako mezuak ez dira artxibotik eskuragarri egongo.
- Baimendutako erabiltzaileei, oro har, eguneko 24 orduetan eta urteko egun guztietan bermatuko zaie artxibaturiko mezuak eskuratzeko aukera, mantentze aldietan izan ezik.
- Baimen bereziak dituzten erabiltzaile batzuek aldi jakin bateko mezu artxibatu guztietarako sarbide berezia ezarri ahal izango dute (auditoretza sarbidea, adibidez, kanpo auditoria bat egiteko). Auditoria sarbideen ezarpena eta erabilera erregistratu egingo dira.

- Honako mezu hauek artxibatuko dira:

a) Hirugarrenei bidalitako mezuak.

b) Hirugarrenek bezeroari bidalitako mezuak.

c) Bezeroak adostutako interfazeen bidez (barneko mezuak, aukerakoak) artxibatzeko emandako mezuak.

- Artxiboak gaur egun indarrean dauden mezuen artxibo elektronikoari buruzko lege xedapenak betetzen ditu, eta tresnak bere esku dagoen guztia egingo du lege xedapenak beteko direla bermatzeko, baita horiek aldatzen badira ere.

- Laguntza teknikoa bermatuko zaie baimendutako erabiltzaileei.

- Artxibatutako datuen eta kontratu honen testuinguruan agertzen diren bezeroaren beste sekretu komertzial batzuen konfidentzialtasuna bermatuko da hirugarrenen aurrean. Konfidentzialtasun betebeharrak kontratu honen amaieratik haratago iraungo du.

Email Encryption zerbitzuaren deskribapena

- Tresna honek bezeroak bidaltzen dituen mezuak zifratzen eta sinatzen ditu eta bezeroari iristen zaizkion mezuak deszifratzen ditu bere sistema informatikoetan, definitutako zuzentzarauen arabera.

- Bidaltzen diren mezuak S/MIME bidez sinatzen dira, baldin eta ziurtagirien biltegian beharrezko gako pribatuak badaude.

- Bezeroaren erabiltzaile baimenduek bidaltzen diren mezuak zifratzeko arauak konfiguratu ditzakete.

- Definitu diren arauen arabera, hainbat modutan trata daitezke bidaltzen diren mezuak:

a) Hartzailearen gako publikoarekin zifratuta transmititu S/MIME edo PGP bidez.

b) Zifratu gabe transmititu, baina TLS duen kanal zifratu baten bidez.

c) Hartzaileari modu seguruan eman.

d) Zifratu gabe transmititu.

- Zuzentzarauak transmisio zifratua eskatzen badu, baina ziurtagirien biltegian hartzailearen beharrezko gako publikoa ez badago eta TLS bidezko transmisioa (konfiguratuta badago) ez bada bateragarria harrera zerbitzariarekin, kasuan kasuko hartzaileari bidalitako mezuak baztertu egingo dira eta ez dira transmitituko.

- S/MIME edo PGP bidez zifratuta jasotzen diren mezuak automatikoki deszifratuko dira, baldin eta bidaltzailearen gako pribatua ziurtagiri biltegian jasota badago.

- Gako publikoak automatikoki aterako dira jasotzen diren mezuen sinaduretatik, eta ziurtagirien biltegian gordeko dira.



- Ziurtagirien biltegian jasotako bezeroaren gako pribatuen konfidentzialtasuna bermatuko da. Konfidentzialtasun-betebeharrak kontratu honen amaieratik haratago iraungo du.

Identitatea ordezteko prebenitzeko iragazki aurreratuak – CEOren iruzurraren aurkako iragazkiak

- Eskaintzen den soluzioak egiazko babesa eman beharko du erakundearen barruan balio handiko langileei zuzendutako identitatea ordezteko ahaleginen aurrean (whaling/spear phishing), gutxienez honako hauek identifikatuta:
 - Erakundeko pertsonen izenak iruzurrez erabiltzea.
 - Erakundearen helbide elektronikoak iruzurrez erabiltzea.
 - Protokoloa iruzurrez erabiltzea.
 - Eduki-ereduen analisisa.
 - Osotasuna eta autentifikazioa egiaztatzea.
 - "Spy out" detektatzea.
 - Gezurrezko datuak identifikatzea.

Analisi teknika gehigarriak

- Berehala sailkatu ezin diren mezuatarako freezing edo jzozte teknikak. Teknika horiek ez dute inoiz 15 minututik gorako analisi denbora gaindituko.
- Administrazioaileei denbora errealean jakinarazi behar zaie, edozein motorrek mehatxu aurreratua (APT) detektatzen duenean.
- Administrazioaileei abisatzeko aukera, jada emandako mezu bat gero maltzurtzat jotzen bada (ExPost alertak).

Administrazioa

- Segurtasun soluzioaren kudeaketa eta administrazioa kontrol panelak berak eskaini eta kudeatu beharko ditu.
- Soluzioak aukera eman behar du Microsoft365 hodeiarekin integratzeko, Microsoft 365en ingurunean konfiguratu beharrik gabe, domeinuak, postontziak eta helmugako zerbitzariei buruzko informazioa sinkronizatzeko, gutxienez.
- Soluzioak ingurune hibridoetarako Split domaina paneletik bertatik kudeatzeko aukera izan behar du, erabiltzaileak posta elektronikoko ingurune desberdinei esleituta.
- Soluzioak aukera izan beharko du Postako Logean eskainitako informazioa SIEM sistema batekin integratzeko.

- Administratzaileek alerta jakinarazpena jaso ahal izango dute denbora errealean, motorrek mehatxu aurreratua detektatzen badute.
- Honako administrazio profil hauek izan beharko ditu gutxienez:
 - Administratzaile orokorra: plataformaren domeinu eta erabiltzaile guztiak administratuko ditu.
 - Estatistiken administratzailea: estatistika txosten grafikoak eskuratzeko aukera izango du.
 - Administratzaile teknikoa: postako berrogeialdia eta postako loga administratu ahal izango ditu.
 - Erabiltzaileak: soluzioa gardena da erabiltzaileentzat, eta panel bat izango dute eskura euren postontzian sartzeko, bai baliozkotzat jotzen denean, bai balio ez duenean. Horrez gain, haientzat bakarrik aplikatuko diren iragazteko propietate batzuk kudeatuko ditu.
- Zerbitzuaren azken erabiltzaileek (erakundeko langileak) segurtasun kotsola batean sartzeko aukera izan behar dute, eta bertan honako hauek egin ahal izango dituzte:
 - Sistemako berrogeialdian blokeatutako mezuak berrikusi, desblokeatzea ahalbidetuz.
 - Baimendutako bidaltzaileen (whitelist) edo blokeatutako bidaltzaileen (blacklist) zerrenda pertsonala administratu.
 - Berrogeialdi txostena konfiguratu eta bidalketa ordutegia pertsonalizatu.
 - Banaketa zerrenda komertzialekin lotutako iragazkia administratu.
- Administratzaileak aukera izan behar du erabiltzaileei administrazio kontsoletara sarbidea gaitzeko edo desgaitzeko.
- Soluzioak hizkuntza anitzeko ingurunea izan beharko du, eta gutxieneko gisa hartuko dira gaztelania, ingelesa eta alemana.
- Soluzioak aukera eman behar du sartzen eta irteten diren mezuen trafikoa denbora errealean edo online ikusteko.
- Bateragarria izan behar du web nabigatzaile nagusiekin (Firefox, Chrome, Safari, Internet Explorer, etab.).
- Kudeaketa kotsola domeinuetarako eta enpresetarako pertsonalizatzeko aukera eman beharko du, kotsola irudi korporatiboetara egokitzeke parada emanaz.
- Kotsolarako sarbidea, autentifikatua eta zifratua, https protokoloa erabilita.
- Erabiltzaileak automatikoki sinkronizatzeko aukera eman beharko du, LDAP zerbitzariari SSL edo SMTP-ri buruz kontsultak eginez.
- Erabiltzaileak automatikoki sinkronizatzeko aukera eman beharko du, Microsoft 365 sistemekin integratutako API hornidura sistemaren bidez.



- Sistemaren administratzaileak eta erabiltzaileek egindako ekintzak ikuskatzeko aukera eman beharko du. Ekintza bakoitzerako honako informazio hau erregistratuko da gutxienez:
 - Eguna.
 - Ekintza.
 - Ekintzarekin lotutako datuak.
 - Ekintzaren emaitza.
 - Ekintza zein erabiltzailek egin duen.
- Enpresa administratzaileek erabiltzaileen berrogeialdia modu zentralizatuan kudeatzeko aukera eman beharko du.
- Administratzaileak berrogeialdiaren kudeaketa azken erabiltzaileen esku uztea ahalbidetu beharko du, gutxienez honako hauek erabilia:
 - Azken erabiltzailearen web kotsola.
 - Erabiltzaile bakoitzari aldizka posta elektronikoz bidalitako laburpen txosten automatikoak, erabiltzaileei txosten horretatik mezuak birsailkatzeko aukera emanez, azken erabiltzailearen kudeaketa kotsolan sartu beharrik gabe.
- Soluzioak trazak edo logak denbora errealean biltegitatzeko sistema izan beharko du, domeinu bakoitzerako posta transakzioen (logak) fitxategiak banakatu eta independizatzeko aukera emango duena, administrazio kotsolaren bidez online sartu eta kontsultak egin ahal izateko, eta informazioa atxikitzeko 90 eguneko gutxienezko epearekin.
- Administrazio kotsolatik logetan bilaketak egin ahal izango dira, gutxienez honako iragazki hauek erabilia:
 - Jabari bidez.
 - Mezuaren gaiaren bidez.
 - Postaren jatorrizko helbidearen bidez.
 - Postaren helmugako helbidearen bidez.
 - Jatorrizko IParen bidez.
 - Sailkapenaren arabera (Spam, baliozkoa, sartzen dena baztertua, irteten dena baztertua, posta zerrendak, birus abisuak, etab.).
- Administrazio kotsolak aukera emango du logetan bilaketen emaitzetan ekintzak aplikatzeko. Honako hauek egin ahal izango dira gutxienez:
 - Mezu bat edo gehiago spam gisa markatu.
 - Mezu bat edo gehiago baliozko mezu gisa markatu.

- Bidaltzailea enpresaren zerrenda zurira bidali.
- Bidaltzailea enpresaren zerrenda beltzera bidali.
- Mezuaren jatorrizko IPa ikusi.
- Laburpen txosten grafiko bat izan beharko du, eta, bertan, gutxienez azken 90 egunetan sartutako eta ateratako mezuen sailkapena agertu beharko da. Baztertutako mezuei, baliozkoei, spam-ari eta birusak dituzten mezuei buruzko informazioa erakutsi behar da.
- Soluzioaren administratzaileek VIP erabiltzaileen taldea zein den erabakitzeak aukera izan beharko dute, kopuruari dagokionez mugarik gabe.

5.- Posta sinadurak eta disclaimerra

EZAUGARRIAK

- Active Directory-ren integrazioa: erabiltzaile guztien sinadurak automatikoki beteko dira Active Directory-ren profileko harremanetarako datuekin. Doikuntza txikiak ere berehala sinkronizatuko dira LDAPren bidez, eta eguneraturik mantenduko dira.
- Lehendik dauden sinaduren HTML iturburu kodea inportatzea, HTML iturburu kodea erabilita. Txertatutako diseinua, formatua eta irudiak oso-osorik gordeko dira. Zuzenean editorean ikus daitezke egindako aldaketak.
- Legea betetzea: sinadurak disclaimer batekin osatu beharko ditu, posta elektronikoaren bidezko komunikazioan nahitaez eman beharreko informazioa betetzeko.
- Diseinu malgua: irudi fitxategiez gain, estekak eta testu formatuak ere jarri ahal izango dira disclaimerrean, nahi den tokian.
- Aurrebistaratzeko funtzioa: WYSIWYG editorean editatu ondoren ("What you see is what you get"), aurrez ikusi ahal izango da erabiltzaile talde bakoitzerako txantiloia.
- Kontrol zabalagoko publizitate bannerra: enpresaren posta elektronikoko sinadurak publizitate banner originalekin osatu behar dira. Horiek klik gutxi batzuekin aktibatu edo desaktibatu ahal izango dira, eta taldeak esleitzean sortu.
- Komunikazioa eta sare seguruak: enpresarako esteka duten botoiak jarri ahal izango dira sare sozialetan zuretik irteten den mezu elektronikoko bakoitzean, marka hobeto ezagutzeko.
- Mugikorretarako pantaila optimizatua: bidalitako mezu elektronikoko gehienak HTMLn oinarritzen direnez, posta elektronikoko mugikorretako bezeroek arazorik gabe ikusi ahal izango dituzte irudien fitxategiak. Posta elektronikoaren sinadura edo disclaimerra bidali ondoren erantsiko zaio posta elektronikoari.
- Talde esleipena: Active Directory-n sortutako erabiltzaile bakoitzarentzat banakako sinadura edo talde bakoitzarentzako disclaimerra sortu ahal izango da.



6.- Postako relay zerbitzuaren baldintzak

Postako relay zerbitzuak IP helbideen pool egokia izan behar du, une oro saihestu ahal izateko irun.org domeinutik edo bidasoa-activa.com domeinutik bidalitako mezuek entrega arazoak izatea postaren irteerako IPa zerrenda beltzetan sartuta dagoelako. IPen pool horrek 20 IP desberdin eduki behar ditu gutxienez.

Relay IPak zerrenda beltzetan egoteagatik mezuak bidaltzeko edo jasotzeko arazoak sortzen badira, hutsegite larritzat hartuko da, eta kontratazioan jasotako zigorrak aplikatuko dira.

7.- Soluziorako eskatzen diren zerbitzu baldintzak eta balioak

- Hileko spamen detekzio tasa, batez beste, % 99,9koa izango da gutxienez, aztertutako aldian Irungo Udalaren domeinuetatik jasotako posta guztiei dagokienez. Horretarako, sartzen diren mezu guztiak SMTP bidez entregatu behar zaizkie sistemei, Irungo Udalaren domeinuetako MX erregistroak aldatuz.
- Hileko batez besteko positibo faltsuen tasa % 0,00015 baino txikiagoa izango da aztertutako aldian Irungo Udalaren domeinuetatik jasotako mezu garbiei dagokienez. Tasa horretan ez dira sartuko gaizki konfiguratutako zerbitzarien bidez (RFCrekin bat ez datozenak), egiaztatutako "open relay-en" bidez edo gaizki konfiguratutako posta bezeroen bidez bidalitako mezuak.
- SMTP bidezko posta trafikoaren erabilgarritasuna batez beste % 99,99koa izango da gutxienez. Horretarako, sartzen diren mezu guztiak zuzenean bidali behar dira SMTP bidez sistemetara, MX erregistroak aldatuta. Erabilgarritasunaren kalkuluan ez dira sartuko planifikatutako mantentze lanak, haiek, ahal den neurrian, asteburuetan egiten baitira gaueko ordutegian (CET).
- Birusak atzemateko urteko batez besteko tasa % 99,99koa izango da gutxienez, aztertutako aldian Irungo Udalaren domeinuetatik jasotako mezuei dagokienez.
- Euskarriak gutxienez 24x7 izan behar du, gaztelaniaz eskainia.
- Soluzioaren fabrikatzaileak tresnaren kontrol panelera sarbidea bermatu beharko du, batez beste % 99,9ko eskuragarritasuna izan behar baitu hilean. Eskuragarritasun horretatik kanpo geratuko dira, berariaz, Irungo Udalaren hardwarearen eta softwarearen inguruko arazoak eta telekomunikazioetako konexio-arazoak.
- Mezuak entregatzeko batez besteko epeak 30 segundotik beherakoak izango dira, eta entregatzeko gehieneko epeak, berriz, 3 minutukoak.
- Berrogeialdian dauden mezuak hiru hilabetez gordeko dira eta bezeroak baimendutako erabiltzaileen eskura jarriko dira. Irungo Udalak eskatzen badu, berrogeialdian jarri diren mezu berrien berri emango zaie erabiltzaileei (normalean, egunean behin).

- Baimendutako erabiltzaileak Internetetik sartu ahal izango dira berrogeialdian dauden mezueta. Baimendutako erabiltzaileek berrogeialdian dauden mezuak bezeroaren sistemetara modu interaktiboan entregarazi ahal izango dituzte.
- Irungo Udalak baimendutako erabiltzaileek (esate baterako, euskarri teknikoko langileak edo administratzaileak) erakundeko mezu guztien zirkulazioa osorik gainbegiratu ahal izango dute kontrol panel baten bidez, azken 7 egunetako mezu blokeatuen (baztertuen) zuzeneko jarraipena egin ahal izateko.
- Fabrikatzaileak programatutako mantentze eta konponketa lanak egin beharko baditu, eta lan horiek zerbitzuak ematea eta tresnaren kudeaketa panelerako sarbidea eten edo mugatuko balute, Irungo Udaleko teknikariei jakinarazi beharko die aldez aurretik. Hala ere, fabrikatzaileak erabilera txikiko aldietan egin beharko ditu mantentze lanak eta, bereziki, asteburuetan.
- Arestian adierazitakoa ez da kontuan hartuko fabrikatzaileak berehalako eta presazko jarduerak egin behar dituztenean, sistemen segurtasunaren eta osotasunaren aurkako berariazko mehatxuak saihesteko.
- Programatutako geldialdiak ez dira sartuko kontrol panelaren erabilgarritasunaren kalkuluan, baina programatutako geldialdiak ezin dira hilean 3 orduetik gorakoak izan.

8. Soluzioa instalatzeko prozesurako eskakizunak

Enpresa esleipendunaren barruan tresna erabiltzeko esperientzia egiaztatua duten teknikariei instalatzeko dute tresna, Irungo Udalaren bulegoetan bertan, prozedura honi jarraikiz:

Lehenengo fasea

Zera egingo da, hiru egunez gutxienez, Irungo Udalaren bulegoetan bertan:

- Irungo Udalaren posta zerbitzuaren konfigurazioari buruzko datuak bildu
- Tresna instalatu eta konfiguratu
- Irungo Udaleko teknikariak tresnan trebatu
- Instalazioari buruzko dokumentazioa eta tresna erabiltzeko eskuliburua entregatu

Bigarren fasea

Zera egingo da, bi egunez gutxienez, Irungo Udalaren bulegoetan bertan, tresna martxan jartzen denetik hamabost egunera gutxi gorabehera:

- Tresnak martxan jarri zenetik nola funtzionatu duen analizatu
- Tresna martxan dela Irungo Udaleko teknikariak tresnan trebatu eta behin betiko konfigurazioa azaldu
- Lehenengo fasearen bukaeran entregatutako dokumentazioa osatu, behin betiko konfigurazioari buruzkoa entregatuta



Lehenengo eta bigarren fasearen artean, enpresa esleipendunak enpresaren barruan tresna erabiltzeko kontaktu bat adierazi beharko dio Irungo Udalarri, Udaleko teknikariak zalantzak argitzeko eta antzematen dituzten arazoak konpontzeko harremanetan jarri ahal izan daitezen. Izan ere, bi faseen arteko aldia oso garrantzitsua da tresna behar bezala konfiguratzeko eta positibo faltsuen ondoriozko gorabeherarik ez izateko.

9.- Enpresa esleipendunaren laguntza zerbitzua

9.1 Irismena

Ezarritako plataforma kudeatzeko URRUNEKO zerbitzua eskaini behar da. Zerbitzu hori emateko, esperientzia egiaztatua duten langileek kudeatu behar dute plataforma, eta gerta daitezkeen gorabeheren funtzionamenduaz, konfigurazioaz, eguneratzeaz eta kudeaketaz arduratuko dira.

9.2 Ezaugarriak

Enpresak eskaintzen duen laguntza zerbitzuak honako alderdi hauek jaso beharko ditu gutxienez:

- PRODUKTUAREN GORABEHEREN AZTERKETA ETA KUDEAKETA:

Instalatutako produktuan gorabeheraren bat gertatuz gero, laguntza emango da honako zeregin hauek eginda:

- Gertakariaren azterketa eta ebazpen proposamena, teknikarien esperientzian oinarrituta.
- Intzidentzia ireki eta fabrikatzailearekin jarraipena egin, arestian proposatutako jarraibideekin konpondu ez bada.

Prozesu osoan zehar, enpresako teknikariek unean-unean jakinaraziko diete Irungo Udaleko teknikariei, bezeroarekin berarekin komunikatzeko ezarritako bideak oinarri hartuta (posta elektronikoa, telefonoa, etab.).

- KONTRATATUTAKO PRODUKTUARI BURUZKO KONTSULTAK:

Irungo Udaleko teknikariek honako informazio hau kontsultatu ahal izango diote enpresa esleipendunaren euskarri den sailari:

- Produktuaren bertsio berriak.
- Partxeak.
- Funtzionalitateak (berriak edo bezeroak eskuratuak).
- Plataformaren funtzionamenduari buruzko zalantzak.

- KONTSOLAREN GAINEKO URRUNEKO EUSKARRI ESKU HARTZEAK.

Tresna kudeatzeko kontsolan gerta daitezkeen gorabeherari dagokienez, enpresa esleipendunak egingo ditu gorabehera konpontzeko jarduerak.

Hona hemen urruneko euskarriko esku hartzeen, ezohiko neurrien aplikazioaren eta eguneratze kritikoen prozedura:

- Enpresak esku hartzeko eskatuko die Irungo Udaleko teknikariei mezu elektronikoa bat bidalita.

- Lanak arrazoizko epean hasiko dira, lanorduetan eta Irungo Udaleko teknikariak eta enpresa esleipenduna ados jarrita.
- Prozesu osoan zehar, enpresa esleipenduneko teknikariek Irungo Udaleko teknikariei informazioa emango diete ezartzen diren komunikazio kanalen bidez (posta elektronikoa, telefonoa, etab.).

- 24X7 ZERBITZUA

Eskaintako tresnak 24x7 zerbitzua izan beharko du, soluzioaren fabrikatzaileak eskainia.

10.- Eskaintzak

Agiri honetan ezarritako baldintzak betetzearen ondoriozko gastu guztiak jasoko ditu eskaintza ekonomikoak. Ez da bestelako kontzepturik ordainduko, ez eta aurkeztutako eskaintzaren igoerarik ere.

Irunen, sinaduraren datan.

Eusebio Hernández
Sistemetako teknikaria