

Documento Técnico
Servicio de intercambio seguro de ficheros



INDICE DEL DOCUMENTO

1	Objetivo.....	3
2	Condiciones técnicas.....	3
3	Gestión del Servicio	5
3.1	Seguimiento del Servicio.....	5
4	Entregables	6
4.1	Formación.....	6
5	Soporte técnico	6
5.1	Actualizaciones y correcciones	6
5.2	Soporte	6

1 Objetivo

La ciberseguridad y los riesgos de privacidad son uno de los factores de riesgo mas relevantes de Sareb en estos momentos, La transferencia de archivos es vital en el flujo de los procesos de negocio, así como la comunicación corporativa. Las soluciones de transferencia de archivos gestionada (MFT) aportan soluciones de valor en cuanto a encriptación, gestión, escalabilidad, integración y auditoría.

El objeto del contrato consiste en el suministro y puesta en marcha de una solución tecnológica para el intercambio seguro de información (MFT) con terceros. Este intercambio deberá garantizar la transferencia y seguridad entre emisor y receptor, sin necesidad de instalación de software adicional en ninguno de los extremos, manteniendo la trazabilidad y confidencialidad e impidiendo el acceso a los ficheros en el ínterin.

Esta herramienta cubrirá las siguientes necesidades

- Políticas de acceso de usuarios que permitan definir quién podrá acceder a los repositorios de intercambio de ficheros
- Auditoria de accesos para dar trazabilidad al uso de la plataforma de intercambio de ficheros.
- Proporcionar un entorno gráfico en el que puedan generar enlaces de acceso (para la compartición de ficheros por parte de terceros) y acceder al repositorio.
- Ofrecer a los usuarios externos un entorno gráfico sencillo desde el que puedan compartir o descargar ficheros en un entorno de fácil manejo.
- Generación de notificaciones cuando los ficheros sean incorporados para avisar de su disponibilidad para la descarga.
- Generación de alertas en caso de intentos de uso no autorizados o ante determinados eventos considerados críticos.
- Disponer de escalabilidad en el producto, haciendo posible ir añadiendo nuevos usuarios o más espacio de almacenamiento.
- Capacidad de gestionar los ficheros (caducidad, etc.)

2 Condiciones técnicas

La solución técnica o herramienta deberá cumplir los siguientes requerimientos técnicos.

Transferencia. La transferencia de los ficheros deberá ser realizada a través de medios propios securizados y nunca a través de software de mercado, como el correo electrónico.

Interfaz de usuario, amigable y gráfico, de fácil comprensión y uso.

Servicio SaaS/PaaS. No debe ser requerida instalación de ningún software en los equipos receptores o emisores.

Accesibilidad por terceros. No se requerirá de instalaciones o descargas de software en los equipos de los destinatarios/terceros. Estos no requerirán de instrucciones, siendo el uso del software intuitivo y de fácil uso.

Políticas. La herramienta debe mantener políticas configurables y granulares que filtren o permitan acciones sobre los ficheros, con respecto al usuario, la acción, etc. Existirá una gestión de políticas (consulta, revisión, trazabilidad, etc.).

Usuarios. Debe existir una gestión de usuarios, que será realizada por perfiles de administración

Acceso de usuario corporativo. Los usuarios corporativos deben poder acceder mediante credencial, con MFA (si así se requiere) y existirá una integración SSO con MS AD.

Autonomía. La herramienta debe poder ser utilizada por los usuarios, sin intervención habitual de los administradores.

Auditoría. La herramienta deberá tener capacidad para generar informes de auditoría, donde se recojan todas las acciones de forma detallada, sobre cada uno de los ficheros.

Alertas. Debe permitir a los administradores el establecimiento de controles ante determinados hechos (intentos de autenticación fallidos, volumen elevado de apertura de los ficheros protegidos...).

Integración con otros sistemas. Soportando capacidades de integración utilizando estándares, APIs etc. para permitir su interoperabilidad con las aplicaciones que faciliten la transferencia de los ficheros a intercambiar. Debe además ser compatible con una amplia variedad de versiones de estas aplicaciones y de Sistemas Operativos.

Ofimática. Capacidad para la integración con plataformas de Microsoft, como Teams y Outlook mediante Pluggins

Dispositivos. La herramienta soportará dispositivos PC, Tablet o Smartphone en los diferentes sistemas operativos más extendidos (Windows, MAC, Linux, iOS, Android...).

Cifrado. Se garantizará la confidencialidad de los ficheros intercambiados, cifrando estos, tanto en su almacenamiento, como en los intervalos y medios de transferencia (en su transferencia).

Formato. El software debe ser capaz de transferir cualquier archivo sin restricciones de formato.

Zero Trust. Asegurando que durante todos los procesos se evita el uso de permisos innecesarios o no son permitidos ninguno.

Concurrencia. Se debe garantizar, al menos una concurrencia de 25 usuarios.

Confidencialidad end to end. La herramienta debe garantizar que únicamente el emisor y el receptor/es permitidos, tienen acceso a los ficheros en cada flujo/repositorio.

DLP. la herramienta dispondrá de un filtro de prevención de fugas de la información (DLP). que permita detectar potenciales brechas de datos y monitorizarlos. El DLP debe permitir establecer reglas de filtrado de información en función de destinatarios o contenidos.

Altas automatizadas/invitación. La herramienta, en el proceso de envío, debe generar invitaciones que serán enviadas por correo electrónico a los destinatarios, incorporando la información necesaria (en el cuerpo del mensaje o mediante enlaces informativos) del procedimiento. El proceso no debe requerir ninguna intervención por parte de la compañía, administradores o emisor. Se debe garantizar que la descarga de ficheros es únicamente viable, para la cuenta o cuentas receptoras.

Sesiones seguras. Las sesiones inactivas serán cerradas pasado un determinado plazo de tiempo (máximo 15 minutos) para evitar que haya sesiones abiertas que puedan ser utilizadas por terceros.

Entrega. La herramienta, asegurará y trazará la entrega/descarga de los ficheros.

Caducidad. Los ficheros tendrán una caducidad en el sistema de almacenamiento, así como será configurable un periodo de caducidad de estos. Transcurrido ese tiempo, los ficheros serán eliminados completamente y no existirá copia alguna.

Malware. la herramienta contará con detección y bloqueo de malware en todo el flujo de transferencia de ficheros y almacenamiento.

Infraestructura. Se permitirán transferencias de al menos 100GB de tamaño total y en número ilimitado o muy elevado de ficheros. Este almacenamiento será dedicado exclusivamente a Sareb.

Integridad. Los datos y ficheros deben ser almacenados de forma que se garantice su disponibilidad e integridad, Además se debe facilitar la correcta restauración, en caso de necesidad.

Sesiones concurrentes. No debe permitirse el sostenimiento o apertura de una segunda sesión mientras la primera permanezca activa.

Compliance. Conformidad y certificaciones: ISO 27001, 27701 (GDPR), ENS (AA PP)

Disponibilidad de la herramienta. La infraestructura deberá estar disponible siete días a la semana y 24 horas al día, la completitud del año (7x24)

RTO (Recovery Time Objective). El RTO estimado debe comprometerse en 99,99%

3 Gestión del Servicio

El servicio a nivel global contará con un responsable interno de Sareb, que durante la duración del servicio ejecutará actividades de aseguramiento de Calidad, Seguimiento y Control del Servicio y del Proveedor.

La gestión de la mejora continua se revisará a través de su reflejo en los niveles de servicio estipulados en los SLAs y el grado de satisfacción de los usuarios.

El proveedor garantizará un contacto fluido dentro del horario de servicio especificado. Deberá proporcionar un método o métodos de contacto que garanticen la atención de incidencias y demandas, permitiendo y garantizando el cumplimiento de los SLAs

3.1 Seguimiento del Servicio

- **Reuniones puntuales a petición de Sareb:** Sareb tendrá la potestad de solicitar, con una antelación de 24horas, las reuniones que estime necesarias al proveedor adjudicatario para tratar algún tema relevante del servicio o cerrar algún nuevo requerimiento a implantar.

4 Entregables

El proveedor realizará una serie de reportes e informes periódicos sobre el estado de la concienciación y de forma específica, sobre algún punto particular, que Sareb estime necesario, para la toma de decisión o de conocimiento.

Documentación inicial:

- **Documentación de la solución**, con la información necesaria para la administración y uso. Y si así fuese necesario la información técnica relevante y de integración con los sistemas de Sareb

Reporting mensual:

- **Informe mensual de cumplimiento de SLA**. Mensualmente y dentro de los cinco primeros días del mes siguiente.
- **Información de actualizaciones de la solución**. Informando de los cambios y mejoras en la plataforma/solución, así como la aplicación de las mismas.

4.1 Formación

En caso de requerimiento por parte de Sareb, el adjudicatario, deberá impartir una formación a los usuarios de la herramienta (en número de empleados de hasta un 20% mayor al número de licencias).

Esta formación irá acompañada de la debida documentación.

5 Soporte técnico

5.1 Actualizaciones y correcciones

El proveedor o fabricante ofrecerán, durante la vigencia de las licencias, el acceso a las nuevas versiones y actualizaciones, así como a los parches y correcciones de errores relativas a dicho software.

Mantenimiento Correctivo: El mantenimiento del software para que esté permanentemente operativo ante problemas que pudieran aparecer y que no hubiesen sido detectados anteriormente. La comunicación de estos problemas, errores o incidencias se efectuará en la forma que determine el contratista (vía telefónica, vía internet etc...).

5.2 Soporte

Debe existir un servicio de soporte sobre la herramienta, con una disponibilidad de, al menos, 8 horas diarias durante la jornada laboral y siempre teniendo en cuenta el horario laboral de Madrid.

Para incidencias críticas o de indisponibilidad, el proveedor garantizará que se trabajará en el restablecimiento del servicio de forma ininterrumpida, 7x24.

El servicio de soporte y resolución de incidencias se prestará de forma remota (sin presencialidad en las oficinas Sareb), . En caso de requerimiento de Sareb o necesidades puntuales, como reuniones, etc. el proveedor del servicio deberá trabajar in-situ en las instalaciones de Sareb en Madrid.

El idioma de interlocución, documentación, webs, etc. con Sareb y sus colaboradores será el castellano.

El calendario laboral, se ajustará al de la ciudad de Madrid. El licitador indicará el horario laboral de trabajo del equipo, debiendo este encontrarse, entre las 8AM y las 19PM.

Sareb no proporcionará servicio técnico sobre ningún elemento ajeno al mismo o de terceros, como líneas de comunicación, software o equipamientos informáticos.

Sareb, dispondrá de un interlocutor principal del servicio, siendo este quien consensue, dirige y propone reuniones de seguimiento y valide los trabajos realizados y realice el seguimiento del servicio.

Sareb mantiene una serie de proveedores que prestan sus servicios de administración sobre las plataformas de infraestructura, puesto cliente y Ciberseguridad, a los que se deberá tener en cuenta en la parte de comunicación y colaboración, en caso de necesidad.