(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 676 693**

(51) Int. CI.:

G06F 21/00 (2013.01)
G06F 15/16 (2006.01)
G06F 17/00 (2006.01)
G06F 21/62 (2013.01)
G06F 21/41 (2013.01)
G06Q 10/10 (2012.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.10.2013 PCT/US2013/065646**

(87) Fecha y número de publicación internacional: **24.04.2014 WO14063030**

(96) Fecha de presentación y número de la solicitud europea: **18.10.2013 E 13847778 (1)**

(97) Fecha y número de publicación de la concesión europea: **14.02.2018 EP 2909770**

(54) Título: **Método y sistema informatizados para gestionar un entorno de intercambio colaborativo seguro en red**

(30) Prioridad:

19.10.2012 US 201261715989 P
07.12.2012 US 201261734890 P
14.03.2013 US 201361783868 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.07.2018

(73) Titular/es:

INTRALINKS, INC. (100.0%)
150 East 42nd Street
New York, New York 10017, US

(72) Inventor/es:

LANDY, JOHN;
FORD, CHRISTOPHER TODD;
LIRIO, DARIO R.;
MCCARTHY, KEVIN L.;
MIHARIA, ANUPAM;
MORPARIA, HARSHAL;
PLANTE, PHILLIP J.;
PORZIO, MATTHEW A.;
ROZIN, LIVIU;
SOTNIKOV, ANVER;
WELLSCHLAGER, MATTHEW T.;
WHINSTON, STEPHEN ALEXANDER;
WHITCHELO, PHILIP A.;
BRANTON, GRANT;
PARASCANDOLO, MARK RICHARD;
YICK, JOHNSON JUN SING;
CALLISON, WADE MICHAEL;
SIDDIQUI, FAHIM y
CROWELL, TALBOTT

(74) Agente/Representante:

RIZZO, Sergio

DESCRIPCIÓN

Método y sistema informatizados para gestionar un entorno de intercambio colaborativo seguro en red

CAMPO DE LA INVENCIÓN

[0001] La presente invención se refiere al contenido seguro en red.

ANTECEDENTES

[0002] A pesar de la disponibilidad de Internet, aún no existe una manera satisfactoria para que la gente de diferentes empresas u otras entidades se beneficie de la seguridad de la red privada, como para el trabajo colaborativo entre empresas de forma cotidiana y para alianzas *ad hoc*, es decir, diferentes conjuntos de entidades que se reúnen para funcionar como una mega o meta entidad, durante algún proyecto en particular. En estos casos, el tiempo y coste de conectar una red entre dos o más empresas u otras entidades y ponerse de acuerdo en un estándar o paquete de *software* común constituye un obstáculo para las soluciones en red convencionales. Además, cualquier proceso nuevo para el intercambio de contenido en el pasado ha requerido generalmente que el usuario adopte nuevos componentes, aplicaciones y hábitos de flujo de trabajo que tienden a perturbar la rutina de flujo de trabajo diario normal del usuario, por ejemplo, cuando se trabaja dentro de la empresa y con el uso personal. Utilizar Internet solamente sigue siendo imperfectamente seguro para el intercambio de información confidencial sin algunos procesos de cifrado seguros previamente establecidos, y ha sido laborioso e infructuoso, en especial con el creciente uso actual de dispositivos personales, que se están incorporando al flujo de trabajo. Existe la necesidad para estos sistemas y para los usuarios de utilizar los sistemas de manera que no los fuercen a adoptar nuevas infraestructuras, *software* y procesos empresariales y personales en su flujo de trabajo diario a fin de conseguir un entorno de trabajo prolongado compartido y potencialmente seguro.

[0003] Por consiguiente, aún existen problemas sin resolver asociados a los diferentes grupos de empresas u otras entidades relacionados con compartir de manera segura por un entorno en red global en expansión. El documento de patente US2009/0328171 expone un almacenamiento remoto seguro de medios electrónicos, en el que una aplicación segura virtual reside en un servidor que proporciona almacenamiento, presentación y acceso cifrados a medios electrónicos críticos.

[0004] El documento de patente US2011/093471 describe un sistema que proporciona un único repositorio de datos. El sistema permite a los usuarios definir y utilizar políticas de gobernanza de información que ayuden a automatizar y sistematizar diferentes tareas de vigilancia. En algunos ejemplos, las organizaciones pueden enviar datos por *push* en cualquier formato de datos de terceros a los sistemas descritos en el presente documento. Los sistemas pueden permitir que el personal responsable de cumplimiento o de TI detecte cuándo un fichero legalmente se ha cambiado o borrado. Los sistemas también pueden proporcionar una interfaz de usuario de panel unificada. Desde una interfaz de panel, los usuarios pueden llevar a cabo búsquedas, participar en flujos de trabajo de gestión de datos colaborativos, obtener informes de gestión de datos, y ajustar las políticas.

[0005] El documento de patente US2009/100060 describe un método que incluye recibir el contenido de un fichero a proteger y la información de permisos que representa uno o más usuarios permitidos y que incluye una o más restricciones de utilización de contenido correspondientes a los usuarios permitidos. El método también incluye generar un fichero de aplicación web que incluya el contenido en un formato presentable por una aplicación web segura capaz de gestionar la utilización del contenido según las restricciones de utilización del contenido. Tras recibir una solicitud de un usuario de un dispositivo informático, el contenido del fichero protegido se presenta al usuario a través de la aplicación web segura, solo si el usuario es un usuario permitido de los usuarios permitidos, mientras restringe la utilización del contenido presentado según una restricción de utilización de contenido correspondiente a los usuarios permitidos.

[0006] "Setting Sharing Permissions for Google Docs and Google Sites", Kent State University, XP055278582 describe la creación, el guardado y la carga de documentos. El usuario puede crear un enlace para compartir que solo los usuarios de la misma universidad que el solicitante pueden utilizar para ver el documento, aunque para ello deberán iniciar sesión en su cuenta. De forma alternativa, puede crearse un enlace que pueda ver todo el mundo, aunque para ello no se requiere ningún inicio de sesión. También es posible establecer el acceso de la gente como "PUEDE EDITAR, PUEDE VER, O NINGUNO". También es posible elegir si quiere que la gente tenga que INICIAR SESIÓN o no para ver el documento.

RESUMEN

[0007] Varios aspectos de la presente invención se definen en las reivindicaciones independientes. Algunas características preferidas se definen en las reivindicaciones dependientes.

[0008] La presente exposición describe métodos y sistemas para gestionar intercambios colaborativos seguros en red, incluyendo al menos uno de entre un recurso de preguntas y respuestas, un recurso de canal privado y de inicio de sesión único, un recurso de intercambio de documentos sin autentificación, una sincronización del

contenido basado en metadatos, un historial de actividad de intercambio de ficheros, una gestión de colaboración, un geoetiquetado, un archivo HAR, y similares.

[0009] En modos de realización, un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red puede comprender establecer, por un servidor de intercambio seguro hospedado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión de usuario que permite que uno o más usuarios accedan al servidor de intercambio seguro mediante al menos un dispositivo informático cliente, donde el uno o más usuarios es de al menos una segunda entidad empresarial intermedia, donde las comunicaciones entre el servidor de intercambio seguro y cada uno del uno o más usuarios es mediante una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión de al menos un usuario para el al menos un usuario de la segunda entidad empresarial; recibir un contenido de datos informáticos de al menos un usuario de una tercera entidad empresarial; recibir de al menos un usuario de la tercera entidad empresarial una indicación de permiso para que el usuario de la segunda entidad empresarial acceda al contenido de datos informáticos; permitir, por el servidor de intercambio seguro, el acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está hospedado por la entidad empresarial intermedia; conceder, por el servidor de intercambio seguro, el acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial; y proporcionar, por el servidor de intercambio seguro, un recurso de gestión de preguntas y respuestas mediante el cual al menos un usuario de la segunda entidad empresarial y al menos un usuario de la tercera empresa intercambian preguntas y respuestas de manera segura en relación con el asunto del contenido de datos informáticos. En modos de realización, el intercambio de preguntas y respuestas puede rastrearse mediante el recurso de gestión de preguntas y respuestas. El intercambio de preguntas y respuestas puede archivarse mediante el recurso de gestión de preguntas y respuestas. Puede marcarse una pregunta para responderse basándose en metadatos extraídos de la pregunta mediante el recurso de gestión de preguntas y respuestas.

[0010] En modos de realización, un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red puede comprender establecer, por un servidor de intercambio seguro hospedado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión único de usuario que permite que un usuario acceda al servidor de intercambio seguro mediante al menos un dispositivo informático cliente con una autentificación de inicio de sesión único, donde el usuario es de al menos una segunda entidad empresarial, donde las comunicaciones entre el servidor de intercambio seguro y el usuario es mediante un acceso de canal privado al servidor de intercambio seguro mediante una red de comunicaciones; almacenar, por el servidor de intercambio seguro, al menos los datos de autentificación de inicio de sesión único de un usuario para el usuario de la segunda entidad empresarial; recibir un contenido de datos informáticos de un usuario de una tercera entidad empresarial; recibir del usuario de la tercera entidad empresarial una indicación de permiso para que el usuario de la segunda entidad empresarial acceda al contenido de datos informáticos; permitir, por el servidor de intercambio seguro, el acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está hospedado por la entidad empresarial intermedia; y conceder, por el servidor de intercambio seguro, acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial. El método puede comprender además un segundo procedimiento de autentificación de datos de inicio de sesión único de usuario que se establece para el usuario de la segunda entidad empresarial para el intercambio de contenido de datos informáticos con un usuario de una cuarta entidad empresarial, donde el segundo procedimiento de autentificación de datos de inicio de sesión único de usuario establece un acceso de canal privado entre el usuario de la segunda entidad empresarial y la cuarta entidad empresarial que está aislada de forma segura del intercambio de acceso de canal privado entre el usuario de la segunda entidad empresarial y el usuario de la tercera entidad empresarial.

[0011] En modos de realización, un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red puede comprender establecer, por un servidor de intercambio seguro hospedado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión de usuario que permite que uno o más usuarios accedan mediante al menos un dispositivo informático cliente al servidor de intercambio seguro, donde el uno o más usuarios es de al menos una segunda entidad empresarial, donde las comunicaciones entre el servidor de intercambio seguro y cada uno del uno o más usuarios es a través de una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión de al menos un usuario para el al menos un usuario de la segunda entidad empresarial; recibir un contenido de datos informáticos de un usuario de una tercera entidad empresarial; recibir de al menos un usuario de la tercera entidad empresarial una indicación de permiso para que el usuario de la segunda entidad empresarial acceda al contenido de datos informáticos, donde la indicación de permiso comprende un acceso sin autentificación restringido al contenido de datos informáticos; permitir, por el servidor de intercambio seguro, el acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está hospedado por la entidad empresarial intermedia; y conceder, por el servidor de intercambio seguro, acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial, donde la concesión de acceso comprende una

restricción de acceso. La restricción del acceso puede ser un límite de tiempo para acceder al contenido de datos informáticos.

[0012] En modos de realización, un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red puede comprender establecer, por un servidor de intercambio seguro hospedado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión de usuario que permite que uno o más usuarios accedan al servidor de intercambio seguro mediante al menos un dispositivo informático cliente, donde el uno o más usuarios es de al menos una segunda entidad empresarial intermedia, donde las comunicaciones entre el servidor de intercambio seguro y cada uno del uno o más usuarios es mediante una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión de al menos un usuario para el al menos un usuario de la segunda entidad empresarial; recibir un contenido de datos informáticos de al menos un usuario de una tercera entidad empresarial; recibir de al menos un usuario de la tercera entidad empresarial una indicación de permiso para que el usuario de la segunda entidad empresarial acceda al contenido de datos informáticos; permitir, por el servidor de intercambio seguro, el acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está hospedado por la entidad empresarial intermedia; conceder, por el servidor de intercambio seguro, el acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial; y proporcionar, por el servidor de intercambio seguro, un recurso de sincronización que permita al usuario de la segunda entidad empresarial sincronizar el contenido de datos informáticos para al menos un dispositivo informático cliente, donde la decisión de si sincronizar o no se basa en una regla de sincronización basada en un criterio asociado con el contenido de datos informáticos. Los criterios pueden almacenarse como metadatos adjuntos al contenido de datos informáticos. Los criterios pueden ser la ubicación del contenido de datos informáticos.

[0013] En modos de realización, un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red puede comprender establecer, por un servidor de intercambio seguro hospedado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión de usuario que permite que uno o más usuarios accedan al servidor de intercambio seguro mediante al menos un dispositivo informático cliente, donde el uno o más usuarios es de al menos una segunda entidad empresarial intermedia, donde las comunicaciones entre el servidor de intercambio seguro y cada uno del uno o más usuarios es mediante una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión de al menos un usuario para el al menos un usuario de la segunda entidad empresarial; recibir un contenido de datos informáticos de al menos un usuario de una tercera entidad empresarial; recibir de al menos un usuario de la tercera entidad empresarial una indicación de permiso para que el usuario de la segunda entidad empresarial acceda al contenido de datos informáticos; permitir, por el servidor de intercambio seguro, el acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está hospedado por la entidad empresarial intermedia; conceder, por el servidor de intercambio seguro, acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial, donde el acceso al contenido de datos informáticos comprende el acceso a contenido del contenido de datos informáticos y al historial del contenido de datos informáticos, donde el historial del contenido de datos informáticos se mantiene por un recurso de actividad de intercambio de ficheros. El contenido de datos informáticos puede estar sincronizado con versiones anteriores del contenido de datos informáticos en al menos un dispositivo informático cliente del usuario de la segunda entidad empresarial para sincronizar ambos cambios al contenido del contenido de datos informáticos y al historial del contenido de datos informáticos.

[0014] En modos de realización, un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red puede comprender establecer, por un servidor de intercambio seguro hospedado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión de usuario que permite que uno o más usuarios accedan mediante al menos un dispositivo informático cliente al servidor de intercambio seguro, donde el uno o más usuarios es de al menos una segunda entidad empresarial, donde las comunicaciones entre el servidor de intercambio seguro y cada uno del uno o más usuarios es a través de una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión de al menos un usuario para el al menos un usuario de la segunda entidad empresarial; recibir un contenido de datos informáticos de un usuario de una tercera entidad empresarial; recibir de al menos un usuario de la tercera entidad empresarial una indicación de permiso para que el usuario de la segunda entidad empresarial acceda al contenido de datos informáticos, donde la indicación de permiso comprende una restricción de retención de contenido; permitir, por el servidor de intercambio seguro, el acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está hospedado por la entidad empresarial intermedia; y por el servidor de intercambio seguro, conceder acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial, donde el acceso concedido está limitado por la restricción de retención de contenido. La restricción de retención de contenido puede ser una restricción de retención condicionada a la oferta, donde se elimina el acceso al contenido de datos informáticos cuando no se cumple una condición de la oferta presentada por el usuario de la segunda entidad empresarial al usuario de la tercera

entidad empresarial. La restricción de retención de contenido puede establecer un periodo de tiempo durante el cual el usuario de la tercera entidad empresarial tiene acceso al contenido de datos informáticos. La restricción de retención de contenido prohíbe al usuario de la tercera entidad empresarial al menos una de entre imprimir, copiar y compartir el contenido de datos informáticos. La restricción de retención de contenido puede prohibir al usuario de la tercera entidad empresarial almacenar el contenido de datos informáticos en al menos un dispositivo informático especificado.

[0015] En modos de realización, un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red puede comprender establecer, por un servidor de intercambio seguro hospedado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión de usuario que permite que uno o más usuarios accedan mediante al menos un dispositivo informático cliente al servidor de intercambio seguro, donde el uno o más usuarios es de al menos una segunda entidad empresarial, donde las comunicaciones entre el servidor de intercambio seguro y cada uno del uno o más usuarios es a través de una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión de al menos un usuario para el al menos un usuario de la segunda entidad empresarial; recibir un contenido de datos informáticos de un usuario de una tercera entidad empresarial, donde el contenido de datos informáticos comprende al menos un atributo geográfico que indica la ubicación de un evento en el historial del contenido de datos informáticos; recibir de al menos un usuario de la tercera entidad empresarial una indicación de permiso para que el usuario de la segunda entidad empresarial acceda al contenido de datos informáticos; permitir, por el servidor de intercambio seguro, el acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está hospedado por la entidad empresarial intermedia; y conceder, por el servidor de intercambio seguro, acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial. El evento en el historial del contenido de datos informáticos puede ser al menos una creación del contenido de datos informáticos, edición del contenido de datos informáticos, transmisión del contenido de datos informáticos. El evento en el historial del contenido de datos informáticos puede ser una ubicación en la que se visualizó el contenido de datos informáticos.

[0016] En modos de realización, un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red puede comprender establecer, por un servidor de intercambio seguro hospedado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión de usuario que permite que uno o más usuarios accedan al servidor de intercambio seguro mediante al menos un dispositivo informático cliente, donde el uno o más usuarios es de al menos una segunda entidad empresarial intermedia, donde las comunicaciones entre el servidor de intercambio seguro y cada uno del uno o más usuarios es mediante una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión de al menos un usuario para el al menos un usuario de la segunda entidad empresarial; recibir un contenido de datos informáticos de al menos un usuario de una tercera entidad empresarial; recibir de al menos un usuario de la tercera entidad empresarial una indicación de permiso para que el usuario de la segunda entidad empresarial acceda al contenido de datos informáticos; permitir, por el servidor de intercambio seguro, el acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está hospedado por la entidad empresarial intermedia; conceder, por el servidor de intercambio seguro, acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial; y proporcionar, por el servidor de intercambio seguro, un recurso de archivo para almacenar el contenido de datos informáticos en relación con al menos uno de los usuarios de la segunda entidad empresarial y la tercera entidad empresarial, donde el recurso de archivo almacena el contenido de datos informáticos emulando el acceso al servidor de intercambio seguro por el al menos uno de los usuarios de la segunda entidad empresarial y la tercera entidad empresarial. El recurso de archivo puede establecer un estado inmóvil de acceso para el intercambio entre el al menos uno de los usuarios de la segunda entidad empresarial y la tercera entidad empresarial.

BREVE DESCRIPCIÓN DE LAS FIGURAS

[0017] La invención y la siguiente descripción detallada de determinados modos de realización de la misma se podrán entender haciendo referencia a las siguientes figuras:

La Fig. 1 representa un diagrama de bloques de primer nivel de la presente invención.

La Fig. 2 representa las funciones de un servidor en un modo de realización de la presente invención.

La Fig. 3 representa un diagrama de bloques funcional para el recurso de comunidad en un modo de realización de la presente invención.

Las Figs. 3A-3R representan modos de realización de la interfaz de usuario del recurso de comunidad.

La Fig. 4 representa un diagrama de bloques funcional para un recurso de votación de enmiendas en un modo de realización de la presente invención.

La Fig. 4A representa un organigrama para un flujo de proceso de un modo de realización del recurso de votación de enmiendas.

Las Figs. 4B-4H representan modos de realización de una interfaz de usuario de un recurso de votación de enmiendas.

La Fig. 5 representa un diagrama de bloques funcional para el recurso de firma electrónica segura en un modo de realización de la presente invención.

Las Figs. 5A-5G representan modos de realización de la interfaz de usuario del proceso de firma electrónica.

La Fig. 6 representa un diagrama de bloques funcional para el recurso de panel en un modo de realización de la presente invención.

Las Figs. 6A-6K representan modos de realización de la interfaz de usuario del recurso de panel.

La Fig. 7 representa un diagrama de bloques funcional para el recurso de correo electrónico integrado en un modo de realización de la presente invención.

Las Figs. 7A-7M representa modos de realización de la interfaz de usuario del recurso de correo electrónico integrado.

La Fig. 8 representa un diagrama de bloques funcional para el recurso de visor en un modo de realización de la presente invención.

Las Figs. 8A-8G representan modos de realización del recurso de visor.

La Fig. 9 representa un diagrama de bloques funcional para el recurso de interfaz para dispositivos móviles en un modo de realización de la presente invención.

Las Figs. 9A-9S representan modos de realización de la interfaz de visualización para dispositivos móviles.

La Fig. 10 representa un diagrama de bloques funcional para un recurso para compartir y dejar de compartir en un modo de realización de la presente invención.

La Fig. 10A representa un organigrama de procesos ilustrativo que en parte describe una interacción mediante la utilización del recurso para compartir y dejar de compartir.

La Fig. 11 representa un organigrama de procesos ilustrativo para un recurso de archivo.

[0018] Aunque la invención se ha descrito en relación con determinados modos de realización preferidos, otros modos de realización se entenderán por un experto en la materia y se incluyen en el presente documento.

DESCRIPCIÓN DETALLADA

[0019] La presente invención puede utilizarse para un servicio de intercambio seguro (conocido de forma alternativa como un "intercambio" o "servicio de intercambio" a lo largo de esta exposición) donde se requieren muchos tipos de comunicaciones entre diferentes partes que se asocian para un proyecto u operación temporal, pero que por ser competidores o por otras razones no son adecuados para utilizar una red de comunicaciones permanente (como una intranet o una red de empresa, como una LAN o WAN) como las que pueden utilizarse para un único organismo público, una única compañía, u otra única empresa o institución. Los proyectos de operaciones que implican operaciones financieras y proyectos que implican acuerdos legales complejos (como fusiones, adquisiciones, y similares) son situaciones para las que los métodos y sistemas descritos en el presente documento son particularmente adecuados; no obstante, estos no son necesariamente el único tipo de proyectos apropiados, ya que cualquier proyecto en el que las partes necesiten compartir información confidencial entre entidades, fuera de los límites de la red de una única entidad, puedan beneficiarse de los métodos y sistemas descritos en el presente documento.

[0020] En un ejemplo, las operaciones dentro del sector bancario pueden proporcionar una situación en la que sea particularmente pertinente un servicio de intercambio seguro, en la que se formen consorcios *ad hoc* bajo el liderazgo de uno o más bancos principales para permitir que un número de bancos asociados o agentes participen en un préstamo importante a un prestatario. Tales préstamos se han vuelto muy comunes y pueden implicar préstamos superiores a mil millones de dólares. La sindicación de estos grandes préstamos se utiliza ya que ningún banco está preparado para prestar una cantidad tan alta a un único cliente. De manera convencional, las condiciones propuestas de un préstamo se negocian entre el prestatario y los bancos principales, tras consultarlo cada uno con sus asesores, como consejeros jurídicos, consultores de relaciones públicas, contables y compañías aseguradoras. En algunos ejemplos, algunos asesores pueden ser asesores internos como empleados de una entidad determinada y por consiguiente constituir un equipo interno. Sin embargo, los asesores en muchos ejemplos pueden estar asociados de manera independiente con entidades externas como bufetes de abogados o empresas de contabilidad importantes, y por consiguiente constituir o bien equipos externos o combinaciones de los anteriores. El (los) banco(s) principal(es) negocia con el prestatario para llegar a los términos y condiciones para el préstamo, como el tipo de interés, el cuadro de interpretación, los valores, y las tasas del banco por procesar y sindicalizar el préstamo. El banco principal puede acceder a financiar todo el préstamo, en cuyo caso el banco principal utiliza la sindicación para crear subpréstamos entre él y otros bancos para recaudar los fondos necesarios para el préstamo. Todas estas transacciones requieren la gestión de

ingentes cantidades de documentación, la mayoría de la cual es confidencial y cuya exposición podría dar resultar en grandes daños al prestatario o prestamistas. Por lo tanto, sería deseable proporcionar un intercambio tal como se ha descrito que permita una transmisión de documentos segura entre los usuarios por una red de comunicaciones global sin requerir que los usuarios se comuniquen previamente para establecer un método de cifrado. En este ejemplo, el servicio de intercambio puede proporcionar un nivel adecuado de seguridad con respecto a cada una de las operaciones compartidas, entre empresas que normalmente serían fuertes competidores, con numerosos documentos confidenciales que las empresas no quieren compartir de manera incontrolada entre otros miembros del grupo de proyecto de préstamo o que sean accesibles en general a personas ajenas. En particular, asegurar las comunicaciones de manera sustancial es de máximo interés para todas las partes en una operación de préstamos sindicados: el prestatario, el banco principal, y los bancos asociados. Un sistema de red virtual proporcionado a través del intercambio puede ofrecer sin problemas una garantía considerable para asegurar que la información y las comunicaciones entre todas las varias partes son seguras.

[0021] En modos de realización, el intercambio puede permitir la transmisión y recepción electrónica de documentos confidenciales por una red de comunicaciones global como Internet para distribuir documentos electrónicos que contengan datos o información sensible para entidades seleccionadas, para notificar a los destinatarios previstos de la disponibilidad de estos documentos, para rastrear el acceso, descargar y cargar tales documentos, y similares.

[0022] En modos de realización, solo pueden acceder al intercambio ordenadores autorizados mediante la utilización de un procedimiento de inicio de sesión adecuado, que incluye nombre de usuario y contraseña. Las comunicaciones dentro del intercambio pueden establecer una sesión de comunicación basada en un protocolo de seguridad seleccionado, y posteriormente los mensajes se transmiten utilizando este cifrado seguro. Las comunicaciones pueden intercambiarse a través de una sesión de comunicación encriptada segura mediante la utilización de un protocolo de cifrado seleccionado, y puede denegar el acceso si no puede establecerse una sesión segura a un nivel de seguridad deseado.

[0023] En modos de realización, el intercambio puede proporcionar un servicio totalmente abastecido y preconfigurado para usuarios, en el que una vez que la empresa del usuario ha establecido una cuenta a través del intercambio, los documentos en formato electrónico pueden cargarse a la web segura mantenida mediante el servidor principal de intercambio, donde una variedad de opciones de comunicaciones colaborativas seguras pueden elegirse incluyendo el almacenamiento de documentos, correo electrónico, difusión de vídeo, videoconferencias, uso de pizarras interactivas y similares, para aumentar y gestionar el acceso interactivo a los documentos, incluyendo una interfaz gráfica de usuario para gestionar las interacciones del usuario con un o más intercambios.

[0024] En modos de realización, el intercambio puede proporcionar una web segura para colocar los documentos y mensajes a transmitir en una red virtual segura y permite a los usuarios autorizados leer o editar mensajes según su nivel de autorización. Cualquier documento que se edite puede estar disponible inmediatamente en el sistema de manera que otras personas implicadas en el intercambio tengan acceso a los documentos editados o modificados de manera inmediata. Además, el intercambio puede proporcionar un seguimiento de cada documento para permitir a los usuarios seleccionados ver quién ha tenido acceso a los mensajes y documentos y quién ha modificado o editado cualquiera de los documentos.

[0025] En modos de realización, el intercambio puede proporcionar un cortafuegos centralizado que pueda emplearse para proteger información confidencial de manera que nadie acceda a esta información sin autorización. Un cortafuegos, como los que se utilicen de manera efectiva en las intranets corporativas, pueden emplearse en cada intercambio. Los grupos de usuarios, como en una red virtual, pueden tratarse como una oficina corporativa remota y restringirse por protocolos de cortafuegos del acceso incontrolable a la información de otros usuarios. Además, si se necesita, pueden establecerse respectivos cortafuegos entre usuarios para evitar que un usuario acceda a la información en el sitio web anfitrión de otro usuario. El intercambio puede ser particularmente adecuado para la comunicación entre múltiples grupos independientes de usuarios, dado que un cortafuegos centralizado simplifica la logística de que cada usuario tenga que conceder acceso por separado mediante sus propios respectivos cortafuegos locales. En una arquitectura tan centralizada, el servidor principal, en lugar de procesarse en cada respectivo usuario, puede procesar convenientemente los datos de seguridad de acceso del servidor. De manera similar, la recuperación y la copia de seguridad del sistema pueden manejarse mejor por un sistema de recuperación y de copia de seguridad centralizado, en lugar de llevar a cabo estas tareas de recuperación por separado en una multiplicidad de sitios web locales.

[0026] Tal como se representa en la Fig. 1, una pluralidad de usuarios del servicio de intercambio 110 del servicio de intercambio pueden intercambiar datos, como documentos, mensajes, datos y similares, entre un servidor principal 102 seguro y una pluralidad de ordenadores de usuario 104, 104A, 104B a través de una red 108 (por ejemplo, Internet) de manera segura, como que solo accedan ordenadores de usuario autorizados mediante la utilización de un procedimiento de inicio de sesión aceptable. En modos de realización, los ordenadores de usuario pueden interactuar con la red mediante un servidor de red, un servidor de correo electrónico, y similares, y conjuntamente con una intranet de empresa, donde haya un cortafuegos entre el

ordenador de usuario y la red, y donde el intercambio se lleve a cabo entre los ordenadores de usuario y el ordenador principal mediante un intercambio seguro a través de la red y mediante un servidor de red, un servidor de correo electrónico, y similares. En otro modo de realización, los ordenadores de usuario pueden interactuar en el intercambio con el servidor principal a través de la red aunque lejos de o en ausencia de la intranet de empresa y del cortafuegos de empresa. Por ejemplo, el usuario puede ser capaz de acceder al intercambio cuando esté en casa, como utilizando un ordenador portátil de empresa, un ordenador personal, un dispositivo móvil, y similares.

[0027] En modos de realización, el servidor principal 102 de intercambio puede estar distribuido por una pluralidad de equipos servidores, y por tanto el servidor principal 102 debe considerarse como un ejemplo ilustrativo de uno de estos múltiples servidores. De este modo, los equipos servidores pueden trabajar juntos para proporcionar un acceso esencialmente ininterrumpido a un gran número de usuarios en varias plataformas con diversas velocidades de comunicaciones. Los ordenadores de servidor pueden funcionar con *software* de gestión de servidores que a su vez puede ser el responsable de la coordinación de servicios, de mantener el estado del sistema, monitorización, seguridad y otras funciones administrativas. En modos de realización, un ordenador de usuario que presenta un navegador web adecuado puede acceder directamente al servidor principal, donde el intercambio puede que no necesite proporcionar a cada usuario *software* de aplicación de suscripción, como que incluya módulos de *software* para el acceso, activación, visualización, comunicaciones, y similares, en relación con el servicio de intercambio.

[0028] En modos de realización, cuando se inicia un intercambio de datos, como al recibir un documento en el servidor principal 102 conectado a una base de datos de alojamiento 112, el servidor principal puede extraer la dirección del destinatario previsto y crear una notificación al (a los) destinatario(s) de la existencia de datos en el servidor principal. La notificación puede contener la URL para el servidor principal. No obstante, el destinatario puede no ser capaz de acceder al mensaje a menos que el destinatario esté autorizado a usar el sistema, como que el destinatario necesite ser un usuario registrado y tener una contraseña asignada para acceder a los datos, u otro repositorio en el servidor principal donde se almacenan los datos, como en una base de datos del usuario 108, 108A, o 108B. Si al destinatario previsto se le concede acceso al servidor principal, entonces el destinatario puede localizar el mensaje previsto para él explorando todos los mensajes a los que se le haya concedido acceso.

[0029] Mientras que la notificación enviada al destinatario previsto puede enviarse utilizando un protocolo de Internet estándar sin cifrado, una vez que el usuario contacta con el servidor principal, el servidor puede establecer una sesión de comunicación cifrada segura utilizando un protocolo de cifrado seleccionado. El servidor principal puede denegar el acceso si no puede establecerse una sesión segura a un nivel de seguridad deseado, como un cifrado de 128-bit.

[0030] En modos de realización, los servicios de intercambio para diferentes usuarios pueden utilizar bases de datos de servidor 108, 108A, 108B separadas estructuradas por *software*. Por ejemplo, la empresa "A" y la empresa "B" pueden utilizar el mismo servidor principal 102 seguro, pero los datos de cada empresa pueden mantenerse en bases de datos 108A y 108B separadas, aunque quizá en el mismo recurso físico de almacenamiento de datos. Esta característica ofrece la ventaja de permitir que el servidor principal se adapte para cada empresa. Por ejemplo, cuando el usuario externo accede al servidor principal, el servidor principal puede reconocer al usuario y asociarlo con una empresa particular de entre la empresa A y la B. Utilizando este reconocimiento, el servidor principal puede presentar una interfaz de navegación personalizada que haga que el servidor principal se parezca a la empresa seleccionada. Para el usuario externo, puede parecer que se han conectado directamente al servidor de la empresa en lugar de al servidor principal. Por consiguiente, la presente invención puede permitir que un usuario mande datos de forma segura de modo que la conexión de red sea sustancialmente transparente para el usuario. Además, el sistema puede proporcionar una personalización del servidor principal remoto para cada uno de una pluralidad de usuarios diferentes de modo que un usuario externo que acceda al servidor remoto puede aparecer como conectado a un cliente servidor interno.

[0031] La Fig. 2 muestra detalles adicionales en relación con el *software* del servidor que puede incorporarse fácilmente en el servidor principal 102, incluido un recurso de comunidad 202, un recurso de votación de enmiendas 204, un recurso de firma electrónica 208, un recurso de panel 210, un recurso de correo electrónico integrado 212, un recurso de visualización 214, un recurso de interfaz de dispositivo móvil 218, un recurso de servicio de red 220, un recurso de distribución 222, un recurso de interfaz 224, un recurso de conversión de formato 228, un recurso de inicio de sesión 230, un recurso de cifrado 232, un recurso de utilización 234, un recurso de sindicación 238, un recurso de identificación de transacción 240, un recurso de enlace 242, un recurso de autorización de usuario 244, un recurso de lector autorizado 248, un recurso de editor autorizado 250, un recurso de notorización 252, un recurso multimedia 254, un recurso de comentarios 258, y un recurso de correo electrónico 260.

[0032] Por ejemplo, el recurso de distribución 222 puede permitir que el servidor principal distribuya datos electrónicamente mediante la utilización de comunicaciones seguras entre la pluralidad de usuarios. El recurso de utilización 234 puede permitir que el servidor principal monitorice el uso de la red para permitir que se facture a los usuarios por el servicio de red. El servidor principal puede establecerse para gestionar una pluralidad de

redes virtuales separadas de manera simultánea, representando cada una de estas redes virtuales un cliente diferente, como la empresa A y la empresa B. Además, un recurso de comunidad 202 puede establecer que los usuarios de diferentes empresas sean expuestos a un otro evento si las diferentes empresas no han tenido ningún contacto previo (por ejemplo, a través de un intercambio compartido), y un recurso de panel 210 puede permitir que empresas gestionen intercambios, documentos, contactos, comunicaciones, preferencias y similares.

[0033] El servidor principal puede ofrecer un elevado nivel de seguridad para todos los datos empleando conexiones de redes sustancialmente seguras, y por medio de tecnologías de cifrado y seguridad desarrolladas para redes como las que se pueden incorporar fácilmente en el recurso de cifrado 232. De forma adicional, el servidor principal puede proporcionar un control del acceso de máxima seguridad mediante el recurso de autorización de usuario 244 que puede permitir que solo el personal autorizado acceda a los mensajes individuales y a documentos y comunicaciones relacionados. El recurso de visualización 214 puede ser capaz de proteger documentos de una visualización, impresión, guardado, y similares, no autorizados, y un recurso de interfaz de dispositivo móvil 218 puede permitir la visualización segura en un dispositivo móvil, como una tableta personal que se utilice lejos de la red de empresa. El recurso de correo electrónico integrado 212 puede facilitar la habilidad de añadir contenido a un intercambio mediante la utilización de un correo electrónico ordinario, como el que se envía a una dirección de correo electrónico segura determinada.

[0034] El servidor principal puede dar a cada usuario la habilidad de enlazar de manera electrónica o de intercomunicarse mediante un recurso de enlace 242 con cualquier número de otros usuarios. Aunque los datos pueden estar formateados preferiblemente de una manera particular, como la que pueda implementarse fácilmente con un programa de intercambio de documentos disponible en el mercado, pueden adaptarse otros formatos utilizando un recurso de conversión de formato 228 adecuado. El recurso multimedia 254 también puede utilizarse para procesar los datos en un formato adecuado para la presentación al usuario en otras formas distintas del texto, como audio, imágenes fijas o en movimiento, y similares.

[0035] El visor de red virtual también puede incluir un recurso de visualización multimedia configurado, por ejemplo, para: visualizar memorandos interactivos multimedia o de medios mixtos mediante decodificadores adecuados, como decodificadores de audio, decodificadores de imágenes fijas del Grupo Conjunto de Expertos en Fotografía (JPEG), y decodificadores de imágenes en movimiento del Moving Picture Experts Group (MPEG). El visor de red virtual también puede permitir varias opciones de comunicaciones colaborativas como correo electrónico, videoconferencias y pizarras interactivas que se habilitan para una transacción determinada de acuerdo con las instrucciones del usuario apropiado. Por supuesto, la serie de capacidad multimedia y las opciones de comunicaciones colaborativas pueden variar dependiendo de los varios recursos de *software* colaborativo disponibles para el usuario.

[0036] El recurso de notarización 252 puede estar dispuesto para certificar de manera electrónica cualquier dato electrónico transmitido a los usuarios, como incorporando tecnología de firma electrónica, y similar. El recurso de servicio de red 220 puede utilizarse convenientemente para visualizar varios datos en relación con el servicio de red como servicios adicionales que pueden estar disponibles por el servicio de red para los usuarios. Los recursos mencionados anteriormente pueden trabajar en conjunto con el recurso de correo electrónico 260, el recurso de interfaz 224, y similares, para enviar avisos de datos para el intercambio y la interfaz con la que enviar datos de forma segura.

[0037] Un visor de red virtual o un explorador puede proporcionar convenientemente al usuario final una interfaz gráfica fácil de utilizar para datos y otra información particularmente confidencial en el servicio de red virtual del servicio de red. El servicio de red virtual puede proporcionar una identificación de servicios disponibles en la red virtual además de una variedad de opciones para acceder y extraer datos. El visor de red virtual puede incluir el recurso de identificación de transacción 240 que, por ejemplo, puede permitir que un usuario encuentre y acceda a la información rápidamente. El visor de red virtual puede proporcionar automáticamente una conexión adecuada al usuario con el servicio de red virtual mediante un recurso de inicio de sesión 230. El visor también puede pedir al usuario que introduzca una o más contraseñas o identificaciones que deban ser reconocidas por o bien el recurso de editor autorizado 250 o bien el recurso de lector autorizado 248 a fin de acceder a la información de una base de datos.

[0038] Para mayor comodidad de los usuarios, algunos datos ofrecidos a través del servicio de red virtual pueden designarse como documentos multimedia interactivos que incluirán vídeos, gráficos, audio, y otros elementos multimedia. Las comunicaciones multimedia pueden proporcionar al usuario una gran variedad de información además de aquella proporcionada por más datos de texto estándar.

[0039] A modo de ejemplo, un escritorio de sindicación, es decir, uno o más individuos autorizados para responsabilizarse de la gestión de una transacción sindicada, de un usuario principal puede ser capaz de difundir y/o enviar de manera selectiva correos electrónicos procesados por el recurso de sindicación 238 para asociar usuarios y viceversa. Por ejemplo, los datos de la modificación procesados por el recurso de votación de enmiendas 204 puede utilizarse para someter a votación los cambios a un documento de transacción entre usuarios autorizados. El documento modificado puede distribuirse de manera conveniente por correo electrónico utilizando el recurso de correo electrónico 260 para proporcionar a los usuarios asociados información

actualizada sobre la transacción. Las enmiendas o mensajes pueden unirse al documento en el sitio web anfitrión del servicio de red donde puedan verse por lo general accediendo al servicio de red virtual que está autorizado para acceder al documento. Los correos electrónicos o enmiendas también pueden descargarse para imprimirse o para adjuntarse a los documentos locales. De manera similar, los datos de comentarios en relación con una transacción pueden procesarse mediante el recurso de comentarios 258 para la distribución apropiada a los usuarios autorizados. Los documentos de transacción pueden estar firmados por los usuarios autorizados mediante el recurso de firma electrónica 208.

[0040] Haciendo referencia a la Fig. 3, el recurso de comunidad 202 puede proporcionar recursos de comunidad, social y similares, como parte del sistema, como por ejemplo para poder expandir la lista de contactos de un usuario a través de la exposición a otros usuarios que utilicen o estén asociados de otro modo con los recursos y más generalmente para hacer que los usuarios encuentren y contacten más fácilmente a otros usuarios que puedan tener intereses comunes. El recurso de comunidad 202 puede permitir a los usuarios de la comunidad 302, como la pluralidad de usuarios del servicio de intercambio 110 y la pluralidad de usuarios de otras comunidades 304, que se encuentren entre ellos utilizando perfiles específicos para la industria, como lo establece un gestor de perfiles 308, para encontrar otros usuarios de la comunidad, invitar a usuarios para comunicarse mandando invitaciones mediante un gestor de comunicaciones 310, ver el estado de la invitación que se ha mandado o recibido, y similares. Mediante una interfaz de usuario de comunidad 312 y un gestor de perfiles 308, un gestor de comunicaciones 310, un recurso de búsqueda de perfiles 314 asociados, el recurso de comunidad 202 puede proporcionar al usuario una mayor visibilidad de la pluralidad de usuarios del sistema, permitir que manifiesten cómo quieren que los vean, controlar si quieren que les vean, determinar si pueden participar o no, permitirles ser anónimos (por ejemplo, solo el perfil), permitir que otros usuarios puedan verlos por completo, permitir que estén disponibles para los usuarios de sólo una industria en particular, y similares. Si un usuario se encuentra en una industria en particular, pueden ser capaces de ver una descripción básica de esa comunidad, además de otras industrias que el usuario determine que puedan beneficiarle. El sistema puede estar provisto de una ventana de perfil en la interfaz de usuario de comunidad 312 que se configura basándose en las especificaciones técnicas o de la industria, como para capitales de inversión, fusiones y adquisiciones, finanzas, jurídico, y similares. Puede haber una variedad de diferentes tipos de perfiles de usuario disponibles, como, en relación con las transacciones, un lado comprador, un lado inversor, un lado asesor, un lado experto, un lado vendedor, y similares. La interfaz de usuario de comunidad 312 puede proporcionar una configuración de usuario mediante un asistente paso a paso de un proceso, donde el usuario selecciona industrias, subconjuntos de industrias, y similares. Los usuarios pueden ser tan específicos o tan generales como deseen, y situarse en la comunidad como buscando oportunidades, presentando oportunidades, presentándose como expertos a los que se les solicitará que moderen, y similares. El sistema puede proporcionar información sobre la ubicación, especificar un tipo de operación, especificar un tamaño de operación, y similares, para ayudar a las personas que busquen estos perfiles. El usuario puede ser capaz de cargar adjuntos, ejemplos, y similares. Puede proporcionarse una configuración de visibilidad, como disponible para los miembros de la comunidad, donde el usuario puede ser capaz de mantenerse anónimo de manera opcional. Si el usuario elige no ser anónimo, entonces pueden ser visibles para los usuarios de manera inmediata, pero seguir protegidos en el sistema. En un ejemplo, un usuario puede ser un "comprador" y un "asesor", donde pueden ver su propio perfil o subperfil, editar el subperfil, añadir otro perfil, y similares.

[0041] En modos de realización, el recurso de comunidad 202 puede proporcionar funciones de búsqueda a través del recurso de búsqueda de perfiles 314, como comenzar una nueva búsqueda, guardar las búsquedas, guardar el historial de búsquedas, y similares, para empezar a interactuar con los perfiles de los usuarios. El buscador puede ser capaz de buscar por industria específica, inversores, tamaño de la operación, tipo de la operación, geografía, tipo de perfil, y similares. El usuario puede empezar una búsqueda y generar los resultados incluyendo los subperfiles en el sistema que coincidan con los criterios de búsqueda. Asimismo, puede haber una variedad de niveles de visibilidad asociados con las búsquedas. Por ejemplo, una búsqueda puede devolver tres coincidencias pero donde solo una sea de un usuario que es un usuario anónimo. En este ejemplo, la información específica puede ocultarse, pero con la habilidad de ver más atributos generales del perfil, como un título de usuario. También puede haber indicadores de búsqueda asociados con contactos, coincidencias, búsquedas previas, y similares, como con un icono para indicar una comunicación pasada, y similares. En modos de realización, el usuario puede utilizar un filtro para encontrar un grupo en el que el usuario quiera hacer una selección múltiple, cogerlo y moverlo a otra lista.

[0042] Otra característica del recurso de comunidad puede ser un "índice de actividad", o una característica similar, como para evaluar lo activo que está un usuario en el sistema. Por ejemplo, un usuario que lleve a cabo actividades en el sistema puede proporcionar una vista cualificada que indique si son un comprador de fusiones y adquisiciones actual o no, como por ejemplo mostrando lo activos que están. El sistema también puede encontrar información que indique actividad de otras fuentes, e importar esa información al sistema, proporcionando por consiguiente una mejor indicación del nivel de actividad del usuario en el sistema, como por ejemplo en cuántas operaciones pueden estar trabajando.

[0043] Otra característica del recurso de comunidad puede permitir que un usuario persuada a otros usuarios que son anónimos para que sean visibles a fin de iniciar una interacción con ellos. Por ejemplo, un usuario puede

contactar con un usuario anónimo y añadirlo al intercambio después de que se haya aceptado la invitación para conectar. El usuario puede hacer "clic" en el usuario anónimo y enviarles una invitación. En este ejemplo, el usuario que la envía puede volverse más visible al usuario anónimo que está siendo invitado. Puede proporcionarse una línea de asunto y una nota sobre por qué el usuario está interesado en contactar con ellos. Una "lista de invitaciones" puede mostrar qué invitaciones se han enviado, y el sistema puede proporcionar un hilo de historial para la actividad del usuario.

[0044] En modos de realización, el sistema puede mantener anónima la información de un usuario hasta que el usuario acepte una invitación del usuario que invita, pero donde el usuario anónimo pueda seguir interactuando con el usuario que invita mientras sigue siendo anónimo. Por tanto, el sistema puede proporcionar un recurso de interacción sólido a nivel del perfil (correo electrónico, etc.) sin necesitar que realmente acepte la invitación, y permitir un diálogo continuado sin revelar quiénes sean (por ejemplo, para conseguir información adicional, aclaraciones, etc.). Como la interacción va de un lado a otro, el objetivo puede ser acabar en un estado de aceptación, pero el sistema también puede proporcionar un medio para bloquear las comunicaciones, como por ejemplo después de que el usuario "acepte" o "rechace". El sistema puede mantener una interacción hasta que el usuario proporcione una aceptación, momento en el que la información de contacto del usuario puede hacerse visible, proporcionar una descarga de información del perfil, incluir el usuario en una lista de contactos, ser recomendado para un intercambio, y similares. Una vez que el usuario acepte, ambas partes pueden ser visibles entre ellas, incluido proporcionar un historial de la interacción.

[0045] Haciendo referencia a la Fig. 3A, el recurso de comunidad puede proporcionar una interfaz de usuario para que el usuario interactúe con el recurso de comunidad, como con una pestaña de perfil para un usuario. En modos de realización, puede añadirse un nuevo perfil a través de la interfaz de usuario. Haciendo referencia a la Fig. 3B, la interfaz de usuario puede disponer la identificación de un subfichero, selección de una industria, selección de una geografía, configuración de los detalles de perfil, configuración de visibilidad, ajustar una política de privacidad, y similares. En modos de realización, puede proporcionarse una vista para configurar la visibilidad, donde el usuario puede especificar la visibilidad para los miembros de la comunidad, como ser visible para los miembros de la comunidad, visible pero anónimo para los miembros de la comunidad (por ejemplo, se ocultan la información de contacto y el (los) adjunto(s)), visible solo el usuario, y similares. Haciendo referencia a la Fig. 3C, se proporciona un ejemplo para un vendedor de fusiones y adquisiciones que busca inversores, incluyendo el perfil un foco de industria (materiales), tamaño de las operaciones (< 25 millones de $), geografía (Asia/Pacífico), tipo de operación (venta/fusión de una entidad completa), visibilidad (anónimo), y similares.

[0046] La interfaz de usuario del recurso de comunidad puede proporcionar una pluralidad de etiquetas, como un centro, intercambios, tareas, documentos, personas, aprobaciones, mantenimiento, formularios, calendario, paneles, datos de los fondos, colaboración, y similares. Haciendo referencia a la Fig. 3D, una pestaña de personas incluye contactos, grupos, comunidad y similares, y una pestaña de comunidad puede mostrar invitaciones comunitarias. Cuando se visualiza la pestaña de comunidad, pueden visualizarse resultados de búsqueda, no visualizarse ningún resultado de búsqueda, un botón para comenzar una nueva búsqueda, y similares. La Fig. 3E muestra un ejemplo de un resultado de búsqueda, incluyendo dos usuarios visibles, un usuario anónimo, y similares.

[0047] Puede haber medidas que el usuario pueda tomar con respecto a un resultado de búsqueda, como contactar, abrir una invitación, ver en detalle, descargar una vCard, solicitar que se añada un usuario al intercambio, gestionar el acceso de un usuario al intercambio, y similares. Cuando un usuario es anónimo, puede proporcionarse un indicador de esto en lugar de su nombre, como "Usuario Anónimo", espacios en blanco en la ubicación, el número de teléfono, la información de contacto por correo electrónico, empresa, etc. La Fig. 3F proporciona un ejemplo de una interfaz para redactar una invitación. A los usuarios que reciban una invitación se les puede pedir que acepten o rechacen la invitación, y el usuario que la envía puede recibir las respuestas como una alerta de correo electrónico (por ejemplo, como está disponible bajo la sección de invitaciones comunitarias de la interfaz de usuario). La invitación puede incluir un asunto, nota, número de usuarios a los que se le envía la invitación, información sobre el usuario que la envía (por ejemplo, nombre, dirección de correo electrónico, número de teléfono), una función de CC, y similares. Puede proporcionarse una invitación a un usuario visible, un usuario anónimo, usuarios conectados, usuarios desconectados, y similares. Mandar una invitación correctamente puede dar como resultado un acuse de recibo, como una alerta de invitación, una alerta de texto, y similares. La Fig. 3G muestra un ejemplo de una indicación de "alerta enviada". Una indicación de una alerta enviada correctamente también puede incluir una indicación de dialogo, un título de la invitación, el cuerpo de la invitación, y similares. Los usuarios que reciban una nota pueden ser capaces de responder directamente a la dirección de correo electrónico del usuario que envía la invitación, tal como se muestra en un ejemplo en la Fig. 3H. La Figura 3I muestra un ejemplo de qué información de usuario puede dejarse en blanco cuando el usuario es un usuario anónimo, como la información de la dirección de correo electrónico, la organización, la posición, el sector, el área funcional, la información de la dirección, el (los) número(s) de teléfono, el número de fax, y similares. La Fig. 3J muestra al menos una parte de la información que puede estar oculta, como en este ejemplo en el que el usuario es un asesor/experto en fusiones y adquisiciones, su especialidad es la banca de inversión, el ámbito de enfoque industrial (por ejemplo, industriales, financieros, servicios públicos, servicios de telecomunicación, sanidad, tecnología de la información, energía, consumo discrecional, materiales, productos

básicos de consumo), tamaño de las operaciones, geografía y similares. La Fig. 3K muestra un ejemplo de una bandeja de entrada de un usuario que muestra una alerta de invitación. La Fig. 3L muestra un ejemplo de las opciones disponibles para el destinatario de una invitación, como aceptarla o rechazarla, donde la Fig. 3M muestra un modo de realización de la pantalla de "rechazar invitación, y las Figs. 3N y 3O muestran una visión general de un modo de realización para las invitaciones enviadas, recibidas, aceptadas, rechazadas y similares. La Fig. 3P muestra un hilo de comunicaciones abierto entre dos usuarios en relación con una invitación, donde como se muestra, las opciones de aceptar-rechazar pueden seguir presentándose al destinatario de la invitación hasta que acepte o rechace la invitación. La Fig. 3Q muestra un modo de realización de la búsqueda de contactos.

[0048] La Fig. 3R representa un ejemplo del flujo de contacto entre dos usuarios. Tal como se muestra, el usuario 1 ha configurado un subperfil que incluye configurar su visibilidad a anónimo. El usuario 2 lleva a cabo una búsqueda comunitaria y encuentra al usuario 1, donde el usuario 2 abre una(s) página(s) de detalles del usuario. El usuario 2 envía luego una solicitud al usuario 1 anónimo, donde el usuario 1 recibe la solicitud (como en su bandeja de entrada del correo electrónico) y ve la invitación en la interfaz de usuario de comunidad El usuario 1 tiene entonces la opción de aceptar o rechazar la invitación, donde el usuario 1 después cierra la ventana de respuesta. El usuario 2 es capaz de ver el estado de la solicitud, como a través de una búsqueda, donde el usuario 2 ve la solicitud, ve el estado de aceptar o rechazar. El usuario 1 puede ver el hilo de notas aceptadas/rechazadas.

[0049] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, incluyendo el método establecer, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión de cliente que permite que al menos un dispositivo informático cliente de una pluralidad de dispositivos informáticos cliente controlados por usuarios de una pluralidad de entidades empresariales acceda al servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente se realiza a través de una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibir contenido de un primero de la pluralidad de dispositivos informáticos cliente; permitir, por el servidor de intercambio seguro, el acceso al contenido para un subconjunto de la pluralidad de dispositivos informáticos mediante un recurso de acceso de contenido de intercambio, donde el recurso de acceso de contenido de intercambio está gestionado por al menos una entidad empresarial de la pluralidad de entidades empresariales; conceder, por el servidor de intercambio, acceso al contenido a un segundo de una pluralidad de dispositivos informáticos clientes cuando el servidor de intercambio seguro recibe del segundo de la pluralidad de dispositivos informáticos cliente sus datos de autentificación de inicio de sesión de cliente siempre y cuando el segundo de la pluralidad de dispositivos informáticos cliente sea uno del subconjunto de la pluralidad de dispositivos informáticos; y proporcionar un recurso comunitario de intercambio donde los usuarios de la pluralidad de dispositivos informáticos cliente establezcan un perfil informativo que se ponga a disposición de otros usuarios de la pluralidad de ordenadores cliente y que estén habilitados para que interactúen entre ellos basándose en el contenido del perfil informativo.

[0050] En modos de realización, el acceso al servidor de intercambio por procesadores cliente puede hacerse mediante un servidor principal controlado por la entidad empresarial que controla el procesador cliente. Los dispositivos informáticos cliente pueden ser al menos uno de los que pertenezcan y que estén gestionados por al menos una de la pluralidad de entidades empresariales. Los dispositivos informáticos cliente pueden pertenecer a usuarios individuales. El servidor de intercambio seguro puede ser al menos uno de una pluralidad de servidores de intercambio seguro. El contenido puede ser al menos uno de entre un documento, una hoja de cálculo, un mensaje, datos, una imagen, contenido de audio, contenido de vídeo, contenido multimedia, y similares. El contenido puede trasladarse al servidor de intercambio seguro mediante una transmisión de datos cifrada.

[0051] En modos de realización, el contenido del perfil informativo puede incluir información de contacto, asociación empresarial, etc. El recurso comunitario de intercambio puede dotar a los usuarios de recursos para mandar una invitación a otro usuario para establecer una comunicación. Después de que se haya enviado la invitación, el recurso comunitario de intercambio puede proporcionar una situación relacionada con la invitación siendo al menos una de entre enviada, recibida y leída. El perfil informativo para el usuario que la envía puede estar restringido a anónimo hasta que el usuario que recibe la invitación la acepta para establecer una comunicación. El recurso comunitario de intercambio puede proporcionar un control de visualización del perfil informativo, donde el control de la visualización permite que otros usuarios, un grupo seleccionado de usuarios, y similares visualicen el perfil informativo. El recurso comunitario de intercambio puede proporcionar una interfaz gráfica de usuario mediante la cual un usuario gestiona su perfil informativo e interactúa con otros usuarios, donde la interfaz gráfica de usuario incluye una interfaz de motor de búsqueda, proporciona un índice de actividad para medir lo activo que está un usuario en el recurso comunitario de intercambio, y similares. Un perfil informativo puede estar clasificado por actividad profesional, como por ejemplo incluyendo un vendedor, comprador, inversor, experto, y similares. El perfil informativo puede incluir credenciales para un individuo, una

indicación de un área de interés (por ejemplo, un tipo de proyecto en el que un individuo esté interesado en participar), y similares.

[0052] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, estableciendo, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación para los datos de autentificación de inicio de sesión de un cliente que permite que al menos uno de una pluralidad de dispositivos informáticos cliente controlados por usuarios de al menos dos entidades empresariales acceda al por lo menos un servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente de usuarios se realiza mediante una red de comunicaciones; almacenando, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión del al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibiendo, de un primero de la pluralidad de dispositivos informáticos cliente, contenido; asociando el acceso, por el servidor de intercambio seguro, al contenido para un subconjunto de la pluralidad de dispositivos informáticos de usuario mediante un recurso de acceso a contenido de intercambio, el recurso de acceso al contenido de intercambio gestionado por al menos una de la pluralidad de entidades empresariales; concediendo, por el servidor de intercambio, acceso al contenido del servidor de intercambio seguro a un segundo de la pluralidad de dispositivos informáticos cliente de usuarios cuando el servidor de intercambio seguro recibe datos de autentificación de inicio de sesión de un cliente por parte del segundo de la pluralidad de dispositivos informáticos cliente de usuarios y que dependen del segundo de la pluralidad de dispositivos informáticos cliente de usuarios , siendo uno del subconjunto de la pluralidad de dispositivos informáticos cliente de usuario; y proporcionando un recurso comunitario de intercambio donde los usuarios de la pluralidad de dispositivos informáticos cliente establecen un perfil informativo que se pone a disposición de otros usuarios de la pluralidad de ordenadores cliente y que estén habilitados para que interactúen entre ellos basándose en el contenido del perfil informativo, en el que la interacción se ejecuta como una interacción anónima, donde la interacción anónima proporciona un subconjunto de contenido del perfil informativo.

[0053] Haciendo referencia a la Fig. 4, el recurso de votación de enmiendas 204 puede establecer la gestión, integración y facilitación de un proceso donde los clientes de agencias que ejecuten una transacción (por ejemplo, un préstamo sindicado) puedan votar sobre las modificaciones o enmiendas de una transacción o del contenido de una transacción, incluyendo un proceso verificable 402, métrica de votación agregada 404, procesamiento de voto centralizado 408, y similares. El proceso de verificación 402 puede utilizar documentación de voto, formularios de consentimiento, seguimiento de páginas de firma, distribución digital, recogida de votos, y presentación de páginas de firma, y similares, donde estos documentos pueden ser completamente localizables. La distribución, recogida de votos y presentación de páginas de firma pueden hacerse en línea, acelerando el proceso y asegurando mejor la transparencia. La métrica de votación agregada 404 puede utilizar cálculos de votos ponderados para el porcentaje de consentimiento, la visualización de respuestas (por ejemplo, qué acreedores han hecho qué), y similares, donde los cálculos de los votos pueden ponderarse por un porcentaje de compromiso, y donde una representación visual de las respuestas de los usuarios puede hacer que sea más fácil ver qué usuarios han intervenido, y cuáles son esas intervenciones. El procesamiento de voto centralizado 408 puede incluir el envío de alertas de recordatorios, la finalización de tareas de aprobación, la finalización de un voto, y similares. Las características del recurso de votación de enmiendas 404 pueden incluir plantillas de enmiendas para una rápida configuración y presentación, votación de acreedores que incluye recogida de páginas de firma (por ejemplo, presentando de manera electrónica las páginas de firma), listas de tareas para el consentimiento, una interfaz de usuario para votos de modificaciones 410 para monitorizar el progreso y las estadísticas (por ejemplo, seguimiento del grupo, recordatorios simplificados, exportación para el recuento y el informe de los votos), enmiendas en intercambios existentes, y similares.

[0054] Haciendo referencia a la Fig. 4A, representa un diagrama de flujo del proceso de un modo de realización para el recurso de votación de enmiendas, donde un equipo de la agencia inicia la consulta de la respuesta del voto 420, como por ejemplo incluyendo documentos, modificaciones, páginas de firma, fechas de vencimiento, alertas automáticas, y similares. Entonces, los acreedores pueden recibir una alerta 422, que incluye la asignación de tareas, como por ejemplo para los asesores externos, el equipo de la agencia, los participantes (p.ej., acreedores), y similares. Pueden descargarse documentos (p.ej., memorandos, páginas de firma) y monitorizarse 424. Las páginas de firma, como un memorando 428 con una página de firma 430, pueden firmarse 432 y presentarse 434 como una respuesta. Los participantes (por ejemplo, la agencia administradora, los asesores externos) pueden recibir la respuesta de los votos 438. En un proceso externo, los votos pueden ponderarse 440, como por ejemplo basándose en cantidades de dólares consignados en los registros de un agente. El proceso puede finalizarse 442, como con totales contabilizados (por ejemplo, para un equipo de agencia bancaria), donde se notifica a los miembros del proceso (por ejemplo, acreedores y prestatarios en un proceso de préstamo). En modos de realización, el recurso de votación de enmiendas puede reducir o eliminar el proceso manual relacionado con la recogida de votos y el proceso de consentimiento, como el asociado con un proceso de carga, y ayuda al usuario a priorizar de manera eficiente una estrategia de recogida de votos.

[0055] En un ejemplo, en un préstamo sindicado, una agencia bancaria puede estar a cargo y tener un número de acreedores apoyando ese préstamo, a menudo cientos o incluso más de un millar de estos acreedores.

Según se proponen enmiendas o modificaciones, cada una puede necesitar diseminarse, hacer que los usuarios reaccionen a ella (como proporcionando información, haciendo selecciones, y similares), devolverse con los documentos apropiados a la agencia bancaria, y similares. Un proceso típico tradicionalmente se lleva a cabo sin conexión, donde los bancos están obligados a tener la firma a bolígrafo de las autoridades firmantes y volver a presentarlo a la agencia bancaria. Además del ejemplo, cuando surge una nueva enmienda, la agencia bancaria puede crear un nuevo entorno de intercambio de transacción para el proceso de enmienda. Mediante un enlace de datos los grupos de miembros acreedores de esos grupos pueden verse empujados al nuevo entorno de intercambio, de manera que cada uno de ellos aparezca como un participante del intercambio. Los datos relacionados con todas las posiciones actuales de los acreedores (las cantidades de sus posiciones financieras respecto al préstamo o préstamos particular(es)) también pueden verse empujadas al intercambio, de manera que esté disponible para un procesamiento adicional. En modos de realización, la posición actual de un usuario con respecto a la estructura de la transacción puede tener relación con la votación, como en la importancia que se da al voto de un usuario, las cantidades mínimas en relación con la enmienda, y similares. Tales cantidades pueden almacenarse y recuperarse para que el intercambio las procese. Por ejemplo, una agencia bancaria puede pedirles a los acreedores que confirmen que entienden sus posiciones en el proceso, todos o algunos de los datos en relación a las posiciones pueden introducirse previamente en el sistema y llevarse a cabo en la transacción, y similares.

[0056] En modos de realización, el recurso de votación de enmiendas puede permitir la denominación para una votación de enmienda, una fecha para la votación, una distribución de los votos, la inclusión de documentos asociados, un recurso para la firma con el que se puedan presentar las páginas, incluir instrucciones para los votantes, un proceso para la aprobación, un paso para que los asesores externos lo revisen, y similares. Una vez que se envía el anuncio para el voto, un agente administrador puede ser capaz de visualizar las tareas que han salido, a qué individuos y grupos, y el estado de la votación. Las características del recurso de votación de enmiendas pueden incluir la importación y exportación de datos sobre el compromiso, un soporte del flujo de trabajo de la recogida de votos de enmiendas, la creación de configuraciones para plantillas de votos, la configuración de formularios de elección, la visualización de un panel de interfaz gráfica de usuario para votos de enmiendas, la configuración de páginas de firma, acceso para que un administrador complete tareas, un recurso para la definición de votos de enmiendas específicos para clientes, y similares. La importación y la exportación puede incluir la capacidad del usuario para ingresar datos en una estructura de operaciones de manera automática (por ejemplo, desde un fichero de origen), crear una lista de grupos acreedores e información sobre el compromiso de los tramos en un nuevo intercambio de operaciones, conciliar una estructura de operaciones existente, generar informes (por ejemplo, enumerando cantidades del compromiso para cada participante, actualizando los compromisos, etc. El soporte del flujo de trabajo de la recogida de votos de enmiendas puede incluir el soporte de una pluralidad de diferentes tipos de enmienda y permitir que los usuarios creen definiciones de proceso disponibles para un tiempo de ejecución, y similares, donde los diferentes tipos de enmienda pueden incluir un simple sí-no, un sí-no con firma, consiento-no consiento, modificar y ampliar, y similares El flujo de trabajo de la recogida de votos de enmienda puede incluir la especificación de las fechas de vencimiento y el tiempo, la recogida de opiniones electorales, la distribución de la documentación, la capacidad para editar los parámetros de voto, y similares. La creación de configuraciones de plantillas de votos puede incluir el soporte de una configuración de plantillas de votos, de manera que encapsule el proceso de voto de enmiendas para una gestión del control de documentos, incluyendo que los usuarios establezcan propietarios, monitores y elementos de voto una vez, y los reutilicen para votos posteriores; proporcionar un lenguaje, instrucciones y documentación consistente a través de las transacciones y votos; establecer tipos de voto que se ajusten según sea necesario, y similares. El formulario de elección puede estar configurado para permitir que los usuarios generen de forma dinámica formularios de elección basados en las relaciones entre los participantes de los grupos (por ejemplo, que los acreedores tengan solo visibilidad para los casos a los que tienen acceso). La visualización de un panel de votaciones de enmiendas puede incluir ver una lista de múltiples enmiendas iniciadas para una transacción en particular, ver detalles del proceso (por ejemplo, la lista de acreedores y su estado correspondiente como el progreso en relación a una tarea), ver la información de contacto y adicional de los participantes, y similares. La configuración de la página de firmas puede incluir un texto personalizado, un logotipo, y similares, donde los usuarios pueden actualizar y mantener sus propias páginas de firma personalizadas, por ejemplo, para todas las transacciones, por transacción, por voto, etc.

[0057] Continuando con el ejemplo del préstamo sindicado, un acreedor puede recibir una alerta por correo electrónico de que están invitados a un nuevo proceso de tarea de enmienda. Después, se les puede pedir que inicien sesión, donde se les integra en el flujo de tareas que procede de la alerta. Las tareas pueden incluir instrucciones, revisión de documentos, opiniones de elecciones, y similares. La información introducida previamente puede proporcionarse también en relación con la tarea. El usuario puede registrar su voto y guardar cualquier enmienda asociada con sus elecciones. Sus elecciones y enmiendas pueden ser imprimibles, donde el usuario puede coger ese documento y llevárselo al signatario para que lo firme. En este ejemplo, toda la información, incluidas las instrucciones, pueden incluirse en la copia impresa para el acreedor, y donde las firmas indiquen el consentimiento legal. De este modo, puede haber un único punto de entrada de información, donde el acreedor recibe el documento a firmar, lo firma, y se proporciona un recurso para volver a cargarlo al sistema. En modos de realización, una firma electrónica descrita en el presente documento también puede utilizarse para formar el documento e introducirlo en el sistema.

[0058] En modos de realización, puede proporcionarse a un usuario la interfaz de usuario 410 para ver los cambios que están ejecutando las enmiendas, para ver las tareas generadas y el estado en el que están, para ver tareas individuales para un acreedor particular, para ver las páginas de firmas (por ejemplo, donde se lleva toda la información de las opciones de elección), etc. También pueden proporcionarse campos personalizados, como, por ejemplo, para permitir que los usuarios cambien los compromisos. En modos de realización, los usuarios pueden ver la información según se van ingresando los datos, incluso antes de que se apliquen las firmas. Un usuario puede necesitar llevar a cabo un cálculo, por ejemplo, para ponderar cada voto para ver lo cerca que están de llevar a cabo la enmienda. El sistema puede permitirle al usuario exportar datos a un documento (por ejemplo, una hoja de cálculo) para llevar a cabo el cálculo de manera separada del sistema, y para monitorizar el proceso de enmienda y los cambios al mismo. Por ejemplo, y continuando con el ejemplo de la sindicación del préstamo, un agente administrador puede interesarse más en monitorizar los niveles de respuesta y los desafíos para los niveles actuales de compromiso. Por ejemplo, si se ve que solo tres usuarios tienen algún reto en sus cantidades comprometidas, entonces el administrador puede necesitar encargarse primero de ello, que puede ser una prioridad si existe una discrepancia. El usuario también puede estar interesado en aquellos que están planeando intervenir (por ejemplo, aumentar su compromiso, reducir su compromiso, por cuanto cambiaría su compromiso, y similares). Finalmente, la agencia bancaria puede tener la última palabra, y por tanto el sistema puede darles prioridad, y de este modo permitirles decidir si permiten los cambios o no.

[0059] Las Figs. 4B-4H representan modos de realización de una interfaz de usuario de un recurso de votación de enmiendas. La Fig. 4B ilustra un listado y gráfico de un panel de un modo de realización que muestra el estado de una votación de enmiendas de un usuario, donde el gráfico expuesto muestra un gráfico circular de "no consiente", "consiente" y "sin respuesta", además de un listado de estados específicos de votaciones de enmiendas. La Fig. 4C muestra una notificación de usuario de que se le ha asignado una tarea de votación de enmienda. La Fig. 4D muestra una interfaz de usuario para la distribución de un voto de enmienda. La Fig. 4E muestra las opciones disponibles para que el usuario vote la enmienda, incluyendo "aceptar" o "discrepar" con el compromiso de "30 000 000 USD". La Fig. 4F muestra un listado de un estado de una tarea de votación de enmiendas para un usuario. La Fig. 4G muestra una página de firma siendo presentada por un usuario, incluyendo una nota que dice: "Les adjunto mi página de firma, para su revisión", La Fig. 4H muestra un estado y un listado actualizado para las tareas de votación de enmiendas del usuario.

[0060] En modos de realización, un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, incluyendo el método establecer, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión de cliente que permite que al menos un dispositivo informático cliente de una pluralidad de dispositivos informáticos cliente controlados por usuarios de una pluralidad de entidades empresariales acceda al servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente se realizan a través de una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibir contenido de un primero de la pluralidad de dispositivos informáticos cliente; permitir, por el servidor de intercambio seguro, el acceso al contenido para un subconjunto de la pluralidad de dispositivos informáticos mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está gestionado por al menos una entidad empresarial de la pluralidad de entidades empresariales; conceder, por el servidor de intercambio, acceso al contenido a un segundo de una pluralidad de dispositivos informáticos clientes cuando el servidor de intercambio seguro recibe del segundo de la pluralidad de dispositivos informáticos cliente sus datos de autentificación de inicio de sesión de cliente siempre y cuando el segundo de la pluralidad de dispositivos informáticos cliente sea uno del subconjunto de la pluralidad de dispositivos informáticos; y proporcionar un recurso de votación de enmiendas para llevar a cabo un proceso de votación cuando el contenido se corresponde a una enmienda propuesta para un acuerdo en el que el recurso de votación de enmiendas permite a los usuarios del subconjunto de la pluralidad de dispositivos informáticos votar la enmienda propuesta.

[0061] En modos de realización, el acceso al servidor de intercambio por procesadores cliente puede hacerse mediante un servidor principal controlado por la entidad empresarial que controla el procesador cliente. Los dispositivos informáticos cliente pueden ser al menos uno de los que pertenezcan y que estén gestionados por al menos una de la pluralidad de entidades empresariales. Los dispositivos informáticos cliente pueden pertenecer a usuarios individuales. El servidor de intercambio seguro puede ser al menos uno de una pluralidad de servidores de intercambio seguro. El contenido puede ser al menos uno de entre un documento, una hoja de cálculo, un mensaje, datos, una imagen, contenido de audio, contenido de vídeo, contenido multimedia, y similares. El contenido puede trasladarse al servidor de intercambio seguro por medio de una transmisión de datos cifrada.

[0062] En modos de realización, el proceso de votación de la enmienda propuesta puede rastrearse, como una trazabilidad que incluye rastrear la documentación del voto, los formularios de consentimiento, las páginas de firma, la distribución digital, la recogida de votos, la presentación de páginas de firma, y similares. El recurso de votación de enmiendas puede establecer la agregación de una métrica de votación para rastrear el proceso de

votación entre los usuarios del subconjunto de la pluralidad de dispositivos informáticos, como agregar métricas de votación utilizando cálculos de votaciones ponderados para el porcentaje del consentimiento y visualización de respuestas. El recurso de votación de enmiendas puede proporcionar un panel de votos de interfaz gráfica de usuario para observar el progreso y las estadísticas, como donde el seguimiento del progreso y las estadísticas incluye el seguimiento de grupo, recordatorios, exportación para el recuento y el informe de los votos, y similares. El recurso de votación de enmiendas puede establecer una ponderación relativa de los votos entre los usuarios de las votaciones. El recurso de votación de enmiendas puede establecer una gestión de los procesos de la votación incluyendo una fecha para el voto, una lista de distribución del voto, inclusión de documentos asociados, recurso para presentar páginas de firmas, inclusión de instrucciones para los votantes, un proceso de aprobación, una etapa para que el asesor externo lo revise, y similares. Un voto puede emitirse como un voto de sí-no, un voto de sí-no con firma, un consentimiento, etc. Puede proporcionarse un formulario de votación, donde el formulario de votación está configurado para permitir que los usuarios generen de manera dinámica formularios de votación, como por ejemplo donde los formularios de votación generados de manera dinámica estén basados en las relaciones de los usuarios participantes. El formulario de votación puede incluir un texto o logotipo personalizable de usuario.

[0063] Haciendo referencia a la Fig. 5, el recurso de firma electrónica segura 208 (también llamados "recurso de firma-e" o "firma-e" en el presente documento) puede permitir el proceso de proporcionar documentos para su firma y para que un usuario firme de manera electrónica y reenvíe los documentos firmados electrónicamente al remitente. En modos de realización, el recurso de firma electrónica 208 puede proporcionar una visualización segura de la firma del documento, como a través del reconocimiento facial 504 para determinar el número de personas que visualizan el monitor en el que se está llevando a cabo la firma electrónica y/o utilizando una fotografía digital de un usuario para verificar si los usuarios son quienes dicen ser, utilizando autentificación biométrica 508, utilizando un ofuscamiento de la pantalla 510 para asegurar que solamente los usuarios autorizados están viendo el documento para su firma, y similares. Por ejemplo, un dispositivo informático que se está utilizando para la firma electrónica puede tener una cámara que vea y detecte el entorno circundante para determinar cuántas personas están viendo la pantalla en ese momento, y si existe una condición en la que no haya solo una persona mirando la pantalla, la pantalla puede ofuscar el documento a firmar electrónicamente, como difuminándolo, borrándolo, tapándolo, etc. Por ejemplo, si el dispositivo informático detecta que nadie está mirando o que mucha gente está mirando la pantalla, la pantalla puede borrar el documento. En otro ejemplo, el dispositivo informático puede utilizar una cámara para hacer coincidir la cara de la persona que mira la pantalla con una imagen almacenada de la persona que está autorizada para firmar electrónicamente, y si coincide, permitir que se continúe con el proceso de firma electrónica. En otro ejemplo, puede requerirse una coincidencia biométrica para permitir que se continúe con el proceso de firma electrónica, como mediante el uso de una coincidencia de un iris tal como se ve a través de una cámara, de una huella dactilar electrónica mediante un lector de huellas digitales para introducirlo al dispositivo informático, o de cualquier otro método de identificación biométrica conocido en la técnica. En modos de realización, las condiciones para permitir un proceso de firma electrónica para continuar pueden almacenarse en un perfil de usuario 512, donde si las condiciones (por ejemplo, número de personas mirando, coincidencia de autorización a través de imágenes y/o biométrica) no se cumplen, el documento puede ofuscarse.

[0064] La Fig. 5A muestra un modo de realización de una interfaz de usuario para activar un proceso de firma electrónica para un intercambio. Nótese que un usuario solo puede ser capaz de ver el documento, o la parte del documento, para el que se aplica la firma electrónica. Por ejemplo, mediante el recurso de visualización, las partes del documento que no procedan pueden bloquearse de alguna manera descrita en el presente documento. La Fig. 5B muestra una barra de herramientas para la firma electrónica, donde el usuario puede hacer clic en un icono de firma electrónica para iniciar (o terminar) un proceso de firma electrónica. La Fig. 5C muestra un modo de realización de cómo un usuario puede mover una firma electrónica arrastrando la firma electrónica con el ratón. El usuario puede llevar a cabo un número de funciones del documento, como buscar, ampliar, rotar, desplazarse por las páginas, etc. En modos de realización, si el usuario mueve una parte de la firma electrónica a una posición que la coloque fuera de la página, la función de firma puede desactivarse (por ejemplo, desaparece la firma electrónica) para evitar situar la firma electrónica en una posición que en la que no se muestre la firma electrónica completa en el documento una vez se haya completado el proceso. Una vez que el usuario haya colocado la firma electrónica, puede aplicar la firma y completar el proceso. La Fig. 5D muestra un ejemplo de un cuadro de diálogo para completar el proceso de firma electrónica, incluyendo una nota de confirmación para el usuario sobre la colocación final de la firma electrónica, donde se permite que el usuario vuelva a la colocación de la firma electrónica si no está satisfecho. El usuario, una vez satisfecho, puede guardar la aplicación de firma electrónica y su colocación, tal como se ilustra en la Fig. 5E. Tal como se muestra en la Fig. 5F, si hay cambios sin guardar cuando el usuario intente cerrar la aplicación, puede aparecer un aviso notificando al usuario de que existen cambios sin guardar y preguntándoles si quieren guardarlos o salir sin guardar. La Fig. 5G muestra un cuadro de diálogo de un modo de realización para cancelar una e-firma, mostrando botones de control para confirmar si quiere cancelar o continuar.

[0065] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, incluyendo el método establecer, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio

de sesión de cliente que permite que al menos un dispositivo informático cliente de una pluralidad de dispositivos informáticos cliente controlados por usuarios de una pluralidad de entidades empresariales acceda al servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente se realizan a través de una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibir contenido de un primero de la pluralidad de dispositivos informáticos cliente; permitir, por el servidor de intercambio seguro, el acceso al contenido para un subconjunto de la pluralidad de dispositivos informáticos mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está gestionado por al menos una entidad empresarial de la pluralidad de entidades empresariales; conceder, por el servidor de intercambio, acceso al contenido a un segundo de una pluralidad de dispositivos informáticos clientes cuando el servidor de intercambio seguro recibe del segundo de la pluralidad de dispositivos informáticos cliente sus datos de autentificación de inicio de sesión de cliente siempre y cuando el segundo de la pluralidad de dispositivos informáticos cliente sea uno del subconjunto de la pluralidad de dispositivos informáticos; y proporcionar un recurso de firma electrónica para gestionar un proceso de firma del contenido recibido por al menos uno del subconjunto de la pluralidad de dispositivos informáticos, en el que el recurso de firma electrónica incluye una interfaz de visualizador de firma que restringe la visualización del contenido a firmar.

[0066] En modos de realización, el acceso al servidor de intercambio por procesadores cliente puede hacerse mediante un servidor principal controlado por la entidad empresarial que controla el procesador cliente. Los dispositivos informáticos cliente pueden ser al menos uno de los que pertenezcan y que estén gestionados por al menos una de la pluralidad de entidades empresariales. Los dispositivos informáticos cliente pueden pertenecer a usuarios individuales. El servidor de intercambio seguro puede ser al menos uno de una pluralidad de servidores de intercambio seguro. El contenido puede ser al menos uno de entre un documento, una hoja de cálculo, un mensaje, datos, una imagen, contenido de audio, contenido de vídeo, contenido multimedia, y similares. El contenido puede transferirse al servidor de intercambio seguro a través de una transmisión de datos cifrada.

[0067] En modos de realización, el recurso de firma electrónica puede incluir una interfaz gráfica de usuario de firma electrónica para presentar el contenido a firmar. La visualización restringida puede ser un usuario firmante que solo puede ver aquellas partes del contenido que el usuario firmante está autorizado a ver. La visualización restringida puede ser un usuario firmante que solo puede ver aquellas partes del documento para las que se aplica la firma.

[0068] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, estableciendo, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación para los datos de autentificación de inicio de sesión de un cliente que permite que al menos uno de una pluralidad de dispositivos informáticos cliente controlados por usuarios de al menos dos entidades empresariales acceda al por lo menos un servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente de usuarios se realiza mediante una red de comunicaciones; almacenando, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión del al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibiendo, de un primero de la pluralidad de dispositivos informáticos cliente, contenido; asociando el acceso, por el servidor de intercambio seguro, al contenido para un subconjunto de la pluralidad de dispositivos informáticos de usuario mediante un recurso de acceso a contenido de intercambio, el recurso de acceso al contenido de intercambio gestionado por al menos una de la pluralidad de entidades empresariales; concediendo, por el servidor de intercambio, acceso al contenido del servidor de intercambio seguro a un segundo de la pluralidad de dispositivos informáticos cliente de usuarios cuando el servidor de intercambio seguro recibe datos de autentificación de inicio de sesión de un cliente por parte del segundo de la pluralidad de dispositivos informáticos cliente de usuarios y que dependen del segundo de la pluralidad de dispositivos informáticos cliente de usuarios, siendo uno del subconjunto de la pluralidad de dispositivos informáticos cliente de usuario; y proporcionando un recurso de firma electrónica para gestionar un proceso de firma del contenido recibido por al menos uno del subconjunto de la pluralidad de dispositivos informáticos, donde el recurso de firma electrónica verifica la identidad del usuario firmante a través de la caracterización biométrica utilizando datos biométricos del usuario firmante previamente almacenados.

[0069] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, estableciendo, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación para los datos de autentificación de inicio de sesión de un cliente que permite que al menos uno de una pluralidad de dispositivos informáticos cliente controlados por usuarios de al menos dos entidades empresariales acceda al por lo menos un servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente de usuarios se realiza mediante una red de comunicaciones; almacenando, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión del al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibiendo, de un primero de la pluralidad de dispositivos informáticos cliente, contenido; asociando el acceso, por el servidor de intercambio seguro, al

contenido para un subconjunto de la pluralidad de dispositivos informáticos de usuario mediante un recurso de acceso a contenido de intercambio, el recurso de acceso al contenido de intercambio gestionado por al menos una de la pluralidad de entidades empresariales; concediendo, por el servidor de intercambio, acceso al contenido del servidor de intercambio seguro a un segundo de la pluralidad de dispositivos informáticos cliente de usuarios cuando el servidor de intercambio seguro recibe datos de autentificación de inicio de sesión de un cliente por parte del segundo de la pluralidad de dispositivos informáticos cliente de usuarios y que dependen del segundo de la pluralidad de dispositivos informáticos cliente de usuarios, siendo uno del subconjunto de la pluralidad de dispositivos informáticos cliente de usuario; y proporcionando un recurso de firma electrónica para gestionar un proceso de firma del contenido recibido por al menos uno del subconjunto de la pluralidad de dispositivos informáticos, reuniendo el recurso de firma electrónica un documento firmado electrónicamente que incluye firmas de una pluralidad de usuarios, cada uno de los cuales ha tenido acceso a solo un subconjunto del contenido para el cual eran los firmantes.

[0070] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, estableciendo, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación para los datos de autentificación de inicio de sesión de un cliente que permite que al menos uno de una pluralidad de dispositivos informáticos cliente controlados por usuarios de al menos dos entidades empresariales acceda al por lo menos un servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente de usuarios se realiza mediante una red de comunicaciones; almacenando, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión del al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibiendo, de un primero de la pluralidad de dispositivos informáticos cliente, contenido; asociando el acceso, por el servidor de intercambio seguro, al contenido para un subconjunto de la pluralidad de dispositivos informáticos de usuario mediante un recurso de acceso a contenido de intercambio, el recurso de acceso al contenido de intercambio gestionado por al menos una de la pluralidad de entidades empresariales; concediendo, por el servidor de intercambio, acceso al contenido del servidor de intercambio seguro a un segundo de la pluralidad de dispositivos informáticos cliente de usuarios cuando el servidor de intercambio seguro recibe datos de autentificación de inicio de sesión de un cliente por parte del segundo de la pluralidad de dispositivos informáticos cliente de usuarios y que dependen del segundo de la pluralidad de dispositivos informáticos cliente de usuarios , siendo uno del subconjunto de la pluralidad de dispositivos informáticos cliente de usuario; y proporcionando un recurso de firma electrónica para gestionar un proceso de firma del contenido recibido por al menos uno del subconjunto de la pluralidad de dispositivos informáticos, donde el recurso de firma electrónica proporciona una visualización segura del contenido tal como se presenta a un usuario firmante a través de una pantalla de ordenador del dispositivo informático cliente del usuario firmante, donde el dispositivo informático cliente del usuario incluye una cámara integrada para visualizar el entorno alrededor del usuario firmante y un recurso de detección facial para reconocer al usuario firmante, detectando si el usuario firmante es el único individuo presente en el entorno visualizado, y si no, ofuscando la visualización del contenido. La ofuscación puede consistir en borrar la pantalla, distorsionar la visualización del contenido, y similares. La detección del usuario firmante por el recurso de detección facial puede llevarse a cabo comparando una imagen de una imagen facial del usuario firmante previamente almacenada con el rostro detectado en el entorno visualizado.

[0071] Haciendo referencia a la Fig. 6, el recurso de panel 210 puede proporcionar recursos organizados para gestionar intercambios entre la pluralidad de usuarios del servicio de intercambio 110, difundir entre los usuarios de múltiples grupos de usuarios, separar los entornos de intercambio, y similares. Por ejemplo, para fusiones y adquisiciones corporativas o un grupo de capitales de inversión, el panel puede proporcionar a los usuarios la habilidad de coger su información, crear un perfil y exponer la información a otras partes (por ejemplo, a inversores de capitales de inversión que muestren el rendimiento de sus fondos individuales). El panel puede presentar la información de manera organizada, permitir la carga de información mediante un importador de información 602, proporcionar permisos 604 para ver información, permitir la exportación de información a través de un exportador de información 608, y similares. El recurso de panel puede proporcionar al usuario acceso a y presentación de datos estructurados y sin estructurar, acceso a visualizaciones que proporcionen un formato personalizado o términos familiares a una categoría particular de cliente de transacción (por ejemplo, fondos, documentos de inversión, estados de cuenta de capital, equipo de inversión), y similares, que también pueden restringir la visualización de un usuario al contenido que le sea aplicable a ellos o a la categoría específica de la transacción. En un ejemplo de capitales de inversión, el usuario puede configurar el panel para satisfacer sus necesidades específicas, como incluir accesorios útiles 610 para visualizar, información relacionada con el mercado (por ejemplo, fondos disponibles). Un accesorio de fondos puede establecer una selección de un fondo, proporcionando una visión general e información del rendimiento, y similares. También puede haber subaccesorios que proporcionen funcionalidades adicionales a un accesorio. El usuario también puede tener múltiples paneles, como para diferentes intercambios, diferentes mercados, diferentes operaciones, y similares. Un panel puede manejar la información que está disponible a otros usuarios, y otro panel puede manejar todos los ficheros personales que estén disponibles y no estén disponibles a otros usuarios. El recurso de panel puede proporcionar también una característica de conformidad, como para monitorizar los cambios realizados en cada panel.

[0072] En un ejemplo en el que se establece un intercambio de ficheros, un usuario administrador 612 puede colocar los ficheros en un directorio de ficheros de entrada, donde los ficheros pueden tener una nomenclatura que dice en qué accesorios introducirán los datos. El sistema puede crear una configuración, ejecutar un proceso para introducir los datos, asegurar que es correcto antes de permitir el acceso, etc. De este modo, los datos pueden considerarse "datos de etapa" antes de permitir el acceso, y "datos de producción" una vez que se aprueben. Una vez que el usuario se encuentra cómodo con una visualización, puede proceder y publicar los datos por etapas en "producción". El sistema puede cargar los datos como un archivo CSV, crear archivos de permiso, y similares. En modos de realización, a un usuario específico se le puede proporcionar una visualización en un panel pero se le puede dar solo acceso a uno o más registros en el panel. Por ejemplo, el usuario puede ver solo un fondo particular, en lugar de todos los fondos. Si seleccionan ese fondo, pueden ver datos secundarios asociados con ese fondo. Pero sin permiso, los demás fondos (o datos secundarios) no se muestran. Un modelo de permisos puede dar acceso a los usuarios a registros específicos del panel. En un ejemplo de fusiones y adquisiciones, un usuario puede ser capaz de ver todas las operaciones activas que está gestionando una organización, un determinado equipo de recursos humanos puede estar autorizado a ver el panel, y similares, donde a las entidades específicas se les proporcionan permisos.

[0073] El panel puede tener funcionalidades estándar y opcionales, como opciones de filtrado estándar, conversión de documentos a formato PDF, y similares. Puede facilitarse un catálogo de accesorios, como para la visualización de textos, gráficos y tablas, seguimiento de documentos, y similares.

[0074] El panel puede permitir la gestión de ficheros a nivel de documento, a nivel de registro, y similares, como para permitir que un usuario añada registros y gestione información. Un usuario puede ser capaz de añadir contenido nuevo, introducir la información requerida, refrescar la pantalla (por ejemplo, por operación), etc. El usuario puede ser capaz de editar y borrar registros existentes, mostrar una relación primaria-secundaria, y similares. El usuario puede querer elegir el primario y encontrar el documento en el intercambio y enlazarlo al documento primario. El sistema puede tener la capacidad de gestionar registros individuales, como para datos del panel, pero también para permisos. El usuario puede ser capaz de coger un registro primario y proporcionar permiso a uno de los muchos usuarios para permitirle el acceso a estos primarios. En modos de realización, el sistema puede proporcionar un recurso de verificación, como para monitorizar quién está añadiendo registros y permisos.

[0075] Haciendo referencia a la Fig. 6A, se muestra un ejemplo de un diseño para un listado de fondos disponibles e información de los fondos, proporcionando una pluralidad de columnas para el contenido. Las Figs. 6B-6D ilustran la edición del fondo de ejemplo, como la edición del contenido específico de una columna. La Fig. 6E muestra una alerta para una condición bajo la cual el usuario no puede guardar las ediciones, como porque el usuario ya no tenga la última versión de los datos (por ejemplo, se hayan cargado nuevos datos u otro usuario haya editado el documento desde que se abrió el panel). En este ejemplo, puede proporcionarse un botón de control para actualizar los datos del panel. La Fig. 6F muestra un ejemplo de un cuadro de diálogo para crear un nuevo fondo en el diseño de ejemplo. Las Figs. 6G-6H muestran cuadros de diálogo para adjuntar un documento. Las Figs. 6I-6K muestran una interfaz de usuario para dar permisos en relación con el fondo de ejemplo, incluyendo proporcionar un identificador del usuario que quiera cambiar los permisos.

[0076] Haciendo referencia a la Fig. 7, el recurso de correo electrónico integrado 212 puede proporcionar la capacidad de añadir contenido a un intercambio utilizando un correo electrónico habitual, como, por ejemplo, enviado a una dirección de correo electrónico designada. Este recurso puede ser especialmente importante respecto a los usuarios que hacen circular documentos e información fundamental por correo electrónico, y donde exista la tendencia de perderle la pista en algún momento. Los usuarios pueden utilizar el recurso de correo electrónico integrado del sistema para almacenar el correo electrónico en un repositorio seguro 702, y para poder decirle a la gente que mande correos electrónicos a este repositorio como parte de un proceso empresarial. El administrador de intercambio 712 entonces puede revisar y procesar la información adicionalmente. Esto puede simplificar la curva de aprendizaje de la utilización de cualquier aplicación web. Si el administrador está muy informado, puede no necesitar que todas las contrapartes gasten tiempo aprendiendo a utilizar la aplicación. Simplemente envían el contenido a un intercambio. Otras características pueden incluir una dirección de correo electrónico asociada con una carpeta en un intercambio, un número máximo de correos electrónicos permitidos en un intercambio (por ejemplo, un usuario puede definir un límite), un recurso de conversión de correos electrónicos 704, una lista blanca y una lista negra 708 de usuarios, notificaciones 710 de éxito y/o error, y similares. En modos de realización, el correo electrónico integrado puede limitarse solo a usuarios autorizados, como a los que ya están en el intercambio, incluidos en una lista blanca, etc.

[0077] Los casos de utilización del correo electrónico integrado pueden incluir el envío de documentos de análisis para su revisión, un método para tener programas para revisar a un tercero (por ejemplo, para crear cuentas mientras se asegura que la tercera parte no toma el control de los adjuntos que contengan información privada), y similares. Además, el sistema puede proporcionar permisos de carpetas en la carpeta del correo electrónico que se puede utilizar para evitar el uso incorrecto. Para el cumplimiento, el usuario puede ser capaz de guardar las comunicaciones en un archivo 714 y monitorizar qué se ha hecho en relación con las comunicaciones.

[0078] En modos de realización, puede disponerse cualquier intercambio con un correo electrónico integrado como característica. Un administrador o cliente puede pasar por el proceso, como por ejemplo definiendo dónde se almacena en el sistema la dirección de correo electrónico del remitente, utilizando campos personalizados para el campo de "de", almacenando el mensaje como un correo electrónico, limitando los correos electrónicos máximos que puede aceptar, eligiendo la carpeta con la que se asociará, y similares. Por consiguiente, una ubicación de una carpeta puede asignarse a una dirección de correo electrónico (por ejemplo, con el dominio predefinido pero con el prefijo disponible para la definición del usuario final). El usuario puede seleccionar usuarios para incluirlos en la característica, establecer una configuración de alertas y de notificaciones (por ejemplo, alertas de problemas, de que se añadió algo), y similares. Puede incluirse una lista blanca, como por ejemplo para quién debería poder enviar correos electrónicos en el intercambio (por ejemplo, podrían ser dominios o incluso direcciones). Si un usuario no está en la lista blanca, entonces podría no ser capaz de enviar correos electrónicos al intercambio. Puede incluirse una lista negra, donde el usuario pueda elegir usuarios para que rechacen la inclusión en el intercambio.

[0079] El recurso de correo electrónico integrado puede crear una estructura de carpetas con una carpeta asignada predefinida, y crear una subcarpeta para cada correo electrónico que se envíe al intercambio, como con el asunto como el título de cada carpeta. El contenido de las carpetas puede incluir entonces cualquier documento adjunto. El contenido del correo electrónico integrado puede organizarse como cualquier intercambio, donde se añaden nuevos correos electrónicos según van llegando. El sistema puede configurarse para mandarlo a un grupo o a uno solo. Por ejemplo, un usuario puede mandar la carpeta a una persona para revisarla pero no darle al destinatario el derecho a reenviar, imprimir, o guardar el documento. El permiso puede aplicarse a los documentos como cualquier otro documento descrito en la presente memoria, como por ejemplo quién puede revisar la correspondencia, quién puede modificarla, guardarla, imprimirla, etc. En modos de realización, puede proporcionarse un recurso de desencadenamiento de eventos 718 donde un correo electrónico recibido puede desencadenar un evento, como una tarea, un proceso, y similares. Por ejemplo, si llega un contrato puede desencadenar un proceso de renovación. En otro ejemplo, puede desencadenarse un proceso de enmienda con la recepción de un correo electrónico.

[0080] En modos de realización, el recurso de correo electrónico integrado puede incluir la recopilación de correos electrónicos de varias partes en una base de datos estructurada para su posterior gestión y procesamiento por un administrador de intercambio de información fundamental, eliminar la curva de aprendizaje de la utilización de una aplicación web para cargar documentos a la nube, permitir que partes internas-externas específicas publiquen documentos en una carpeta web que puede compartirse con individuos predefinidos a varios niveles de control, y similares. Los componentes pueden incluir una dirección de correo electrónico asociada con una carpeta en un intercambio, un número máximo de correos electrónicos permitidos en un intercambio, una definición de opciones de conversión de correos electrónicos, una lista blanca, una lista negra, notificaciones de éxito y/o error, y similares. En un ejemplo, pueden procesarse las solicitudes futuras o de clientes, como para una empresa de inversión que necesita presentar documentos para su análisis, un banco que busca una manera de tener programas para revisar a una tercera parte para crear nuevas cuentas mientras se aseguran de que la tercera parte no toma el control de los adjuntos que contengan información privada, un banco que tenga necesidades de cumplimiento como la necesidad de archivar todas las comunicaciones que tienen (por ejemplo, poniéndolos en copia y respondiendo al sistema en todas las correspondencias), etc. La Fig. 7A muestra una introducción al correo electrónico integrado al usuario, y un botón de control para comenzar el proceso. En modos de realización, puede haber un número de pasos/opciones en la ejecución del correo electrónico integrado, como elegir opciones básicas, asignar carpetas, seleccionar destinatarios de alertas, crear una lista blanca, crear de una lista negra, habilitar-deshabilitar el sistema, y similares. La Fig. 7B muestra un ejemplo de cuadro de diálogo para la selección de opciones básicas, incluyendo una selección de campo personalizado para el "de" de un correo electrónico, cómo puede almacenarse el contenido del cuerpo de un correo electrónico entrante, definiciones para el número máximo de correos electrónicos que deben aceptarse en el intercambio, y similares. Las Figs. 7C-7F muestra cuadros de diálogo para la selección de una carpeta en relación con la asignación de carpetas, con la Fig. 7E mostrando una alerta para cuando se utilice una dirección de correo electrónico duplicada. La Fig. 7G ilustra la selección de usuarios y su configuración de alertas. La Fig. 7H muestra un modo de realización que advierte que hay un dominio duplicado o una dirección de correo electrónico asociada con la creación de una lista negra. La Fig. 7I muestra una posible lista de comprobación en relación con la habilitación del sistema, tal como se muestra en la figura para la selección de un campo personalizado, la asignación de dos carpetas, carpetas en las que se asigna el correo electrónico, ningún número máximo especificado de correos electrónicos, dos dominios incluidos en una lista blanca, y un domino incluido en una lista negra. La Fig. 7J muestra una interfaz de usuario presentada al usuario una vez que el correo electrónico integrado está activado, mostrando pestañas para enumerar opciones, carpetas asignadas, destinatarios de alertas, listas blancas, listas negras, y similares, y mostrando específicamente las opciones del correo electrónico integrado. Las Figs. 7K-7M muestran ejemplos del contenido y cuadros de diálogo proporcionados en relación con la pestaña de carpetas asignadas.

[0081] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, incluyendo el método establecer, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio

de sesión de cliente que permite que al menos un dispositivo informático cliente de una pluralidad de dispositivos informáticos cliente controlados por usuarios de una pluralidad de entidades empresariales acceda al servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente se realizan a través de una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibir contenido de un primero de la pluralidad de dispositivos informáticos cliente; permitir, por el servidor de intercambio seguro, el acceso al contenido para un subconjunto de la pluralidad de dispositivos informáticos mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está gestionado por al menos una entidad empresarial de la pluralidad de entidades empresariales; conceder, por el servidor de intercambio, acceso al contenido a un segundo de una pluralidad de dispositivos informáticos clientes cuando el servidor de intercambio seguro recibe del segundo de la pluralidad de dispositivos informáticos cliente sus datos de autentificación de inicio de sesión de cliente siempre y cuando el segundo de la pluralidad de dispositivos informáticos cliente sea uno del subconjunto de la pluralidad de dispositivos informáticos; y proporcionando un recurso de entrada de correo electrónico seguro para aceptar correos electrónicos sin seguridad de fuera del intercambio dentro del entorno seguro de intercambio de datos informáticos colaborativo, donde el correo electrónico sin seguridad se recibe y almacena como un correo electrónico seguro en el servidor de intercambio seguro.

[0082] En modos de realización, el acceso al servidor de intercambio por procesadores cliente puede hacerse mediante un servidor principal controlado por la entidad empresarial que controla el procesador cliente. Los dispositivos informáticos cliente pueden ser al menos uno de los que pertenezcan y que estén gestionados por al menos una de la pluralidad de entidades empresariales. Los dispositivos informáticos cliente pueden pertenecer a usuarios individuales. El servidor de intercambio seguro puede ser al menos uno de una pluralidad de servidores de intercambio seguro. El contenido puede ser al menos uno de entre un documento, una hoja de cálculo, un mensaje, datos, una imagen, contenido de audio, contenido de vídeo, contenido multimedia, y similares. El contenido puede trasladarse al servidor de intercambio seguro por medio de una transmisión de datos cifrada.

[0083] En modos de realización, la aceptación de correos electrónicos sin seguridad puede depender de un listado controlado almacenado en el servidor de intercambio seguro, donde el listado es un listado blanco que especifica los correos electrónicos permitidos, un listado negro que especifica los correos electrónicos que no están permitidos, y similares. La recepción de un correo electrónico sin seguridad puede desencadenar un evento, donde el evento desencadenado es la iniciación de un proceso de enmienda de contenido, la iniciación de un nuevo intercambio, la distribución del correo electrónico dentro del intercambio, el almacenamiento del correo electrónico en un recurso de archivo seguro, y similares. El correo electrónico puede asociarse automáticamente con el área de contenido en el intercambio basándose en el remitente del correo electrónico, en la línea de asunto del correo electrónico, en la dirección del destinatario dentro del intercambio y el contenido del correo electrónico, y similares.

[0084] Haciendo referencia a la Fig. 8, el recurso de visualización 214 puede proporcionar una protección de visualización segura 802 contra una visualización, impresión, guardado, y similares no autorizados, como por ejemplo sin tener que instalar *software* cliente personalizado (por ejemplo, sin instalar nada más aparte de Adobe Flash). Los documentos en determinados formatos, como los productos de Microsoft Office, documentos en PDF, y similares, pueden ser compatibles con la protección. Por ejemplo, para un documento PDF puede aparecer un aviso de seguridad de que un usuario solo tiene permitido ver el documento. No obstante, si el usuario intenta imprimir la pantalla, la pantalla puede distorsionarse, como, por ejemplo, pasando a un estado borroso. En modos de realización, el usuario puede que necesite presionar la tecla Enter para hacer visible el documento. El usuario puede ser capaz de avanzar y retroceder página, rotar, ampliar, y similares. El sistema puede proporcionar marcas de agua en el documento, de manera que si un usuario tiene permitido imprimir la pantalla, el documento la imprimirá con la marca de agua. El recurso de visualización puede incluir además funciones como la visualización de anotaciones 804 en el visor, conectividad con el recurso de firma electrónica 208 (por ejemplo, con una herramienta de "sello"), visibilidad del documento basada en detección de rostro, protección del documento contra fisgones (por ejemplo, limitar automáticamente la visualización del documento, también llamado enfoque, basado en la detección de un segundo rostro), informes de acceso 808 al documento a nivel de página/detallado, protección del documento 810 utilizando un cifrado basado en el reconocimiento facial, una característica de texto a voz (por ejemplo, como la Siri de Apple®), controles basados en gestos con la mano 814 (por ejemplo, control del desplazamiento basado en movimientos mano-puño), uso de pizarras interactivas en tiempo real 818, videochat seguro 820 (por ejemplo, uno a uno, en grupo), y similares. En modos de realización, el recurso de visualización puede incluir un componente de comentario de audio, como, por ejemplo, para permitir que un usuario introduzca comentarios en el documento mediante dictado de voz, para que el recurso de visualización reproduzca los comentarios en audio, para proporcionar un resultado en audio para varios aspectos del documento, y similares.

[0085] En modos de realización, el visualizador puede ser capaz de detectar rostros y aumentar la seguridad basada en el reconocimiento facial, como a través de la utilización de la cámara conectada o integrada con el dispositivo informático que se utiliza para ver contenido. El visualizador también puede utilizar una "visualización

segura", como, por ejemplo, donde la persona que ve el documento solo vuelve visible una parte de un documento. La visualización segura puede implementar medidas de seguridad (por ejemplo, borrar la pantalla, distorsionar la pantalla, subir la pantalla) basadas en el movimiento ocular, el movimiento del rostro, la presencia de un segundo rostro, etc. El tiempo de visualización puede monitorizarse y notificarse, verificarse, y similares, basándose en cuánto tiempo ha estado el usuario mirando al documento, donde la monitorización, notificación, verificación y similares pueden proporcionarse inmediatamente. El cifrado y descifrado de documentos puede proporcionarse basándose en los permisos del documento. Por ejemplo, si el documento solo puede abrirlo un número específico de personas, la detección de rostro puede utilizar el rostro del autor, o de cualquier otro usuario con permiso para cifrar el documento, y precisar que se detecte el mismo rostro para poder "desbloquear" el documento. Entonces, el cifrado del rostro puede "grabarse" y utilizarse como firma electrónica, con lo que vincula el rostro al perfil del usuario. El registro del tiempo de visualización puede ser a nivel del documento, por página, etc. Por ejemplo, un dispositivo informático que se está utilizando para visualizar un documento puede tener una cámara que vea y detecte el entorno circundante para determinar cuántas personas están viendo la pantalla en ese momento, y si existe una condición donde no haya solo una persona mirando la pantalla, la pantalla puede ofuscar el documento que se está visualizando, como difuminándolo, borrándolo, tapándolo, etc. Por ejemplo, si el dispositivo informático detecta que nadie está mirando o que mucha gente está mirando la pantalla, la pantalla puede dejar el documento en blanco. En otro ejemplo, el dispositivo informático puede utilizar una cámara para hacer coincidir la cara de la persona que mira la pantalla con una imagen almacenada de la persona que está autorizada para acceder y visualizarlo, y si coincide, permitir que se continúe con el proceso de acceso y visualización. En otro ejemplo, puede requerirse una coincidencia biométrica para permitir que se continúe con el proceso de visualización, como mediante el uso de una coincidencia de un iris tal como se ve a través de una cámara, una huella dactilar electrónica mediante un lector de huellas digitales para introducirlo al dispositivo informático, o cualquier otro método de identificación biométrica conocido en la técnica. En modos de realización, las condiciones para permitir un proceso de acceso y visualización para continuar puede almacenarse en un perfil de usuario, donde si las condiciones (por ejemplo, número de personas mirando, coincidencia de autorización a través de imágenes y/o biométrica) no se cumplen, el documento puede ofuscarse o el acceso puede denegarse.

[0086] En modos de realización, los vendedores pueden extraer estadísticas de visualización para la inteligencia empresarial en una transacción estratégica, como mediante un CIO con una empresa, un analista de *marketing*, o cualquier usuario que pueda beneficiarse de conocer qué contenido se está leyendo y qué contenido no se está leyendo.

[0087] En modos de realización, el visor puede proporcionar un recurso de búsqueda para buscar en un documento. El sistema puede permitir destacar un resultado de búsqueda, destacar una posición seleccionada del documento, y similares. El sistema puede proporcionar recursos para anotar, marcar, comentar, etc., en un documento, como anotaciones privadas para el usuario, una anotación compartida para otros usuarios, y similares. El sistema puede proporcionar una visualización segura del documento, donde solo son visibles algunas partes del documento. Por ejemplo, un usuario puede querer enseñar a otro usuario solo una parte seleccionada del documento. La visualización segura del documento puede permitir también a un usuario aumentar el tamaño de la ventana de visualización del documento, lo que puede asegurar mejor que las personas que estén cerca de ti solo ven las partes relevantes del documento. Otra característica de la visualización segura del documento puede incluir distorsionar aquellas porciones del documento que no se seleccionan para visualizar, como emborronando esas secciones. La visualización segura del documento puede reaccionar al movimiento ocular del usuario, como desplazando el documento según cambia la dirección de la mirada del usuario, distorsionando o bloqueando la visualización del documento si el usuario aparta la mirada del visualizador, y similares.

[0088] El recurso de visualización puede tener la capacidad de manejar determinados formatos de documentos de manera estándar. Por ejemplo, el sistema puede convertir documentos de Microsoft Word y PowerPoint a documentos en formato PDF, abrir hojas de cálculo (por ejemplo, Microsoft Excel), en un visor de hojas de cálculo, y similares. Por ejemplo, cuando se abre un documento de Excel, puede representarse sobre la marcha, descifrarse sobre la marcha según se desplaza el usuario, recuperarlo del servidor y cifrarlo sobre la marcha, y similares.

[0089] Las Figs. 8A-8G representan modos de realización del recurso de visualización, como para su uso en una hoja de cálculo, procesador de textos, y similares, donde las Figs. 8B-8D representan modos de realización del recurso de visualización tal como se aplica a una hoja de cálculo, y las Figs. 8E-8G representan modos de realización del recurso de visualización tal como se aplica a los procesadores de texto. La Fig. 8A ilustra las funciones del recurso de visualización respecto a un documento de hoja de cálculo de muestra, donde (1) muestra una barra de herramientas, (2) muestra un contador de hojas/páginas, (3) muestra una caja de búsqueda en el documento, (4) muestra la interfaz de enfoque, y (6) muestra una barra de desplazamiento. La Fig. 8B muestra una función de búsqueda y resultados de muestra, donde (1) muestra la ventana de búsqueda, (2) muestra una ventana de resultados de búsqueda, (3) muestra cómo pueden agruparse los resultados por página/nombre de la hoja de cálculo, (4) muestra un término de búsqueda destacado, y (5) muestra un mensaje desplegado, como si algunos resultados de búsqueda se visualizasen antes de que se completase la búsqueda

en todo el documento. La Fig. 8C ilustra un modo de realización de la función de enfoque, donde solo es visible una parte del documento. La Fig. 8D muestra un cuadro de diálogo que responde a un usuario que hace clic en el icono de imprimir. Nótese que puede restringirse la impresión tal como se describe en el presente documento, donde el cuadro de diálogo puede mandar una alerta al usuario identificando las restricciones. La Fig. 8E ilustra las funciones del recurso de visualización respecto a un documento de procesamiento de texto de muestra, donde (1) muestra una barra de herramientas, (2) muestra un contador de páginas/hojas, (3) muestra un cuadro de búsqueda de un documento, (4) muestra la interfaz del enfoque, y (6) muestra una barra de desplazamiento. La Fig. 8F muestra un conjunto de resultados de búsqueda de muestra. La Fig. 8G ilustra un número de funciones de recurso de visualización relacionadas con una orden de impresión, incluyendo (1) un icono de impresión, (2) una ventana de documento sombreada, (3) una ventana de impresión, (4) opciones de impresión, (5) el rango de páginas a imprimir, (6) un botón de cancelar donde si el usuario cancela la impresión, la función de sombreado puede apagarse y volver a revelar el documento, (7) un botón de control de "siguiente" para cerrar la ventana previa a la impresión y abrir un diálogo de impresión del sistema operativo.

[0090] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, incluyendo el método establecer, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión de cliente que permite que al menos un dispositivo informático cliente de una pluralidad de dispositivos informáticos cliente controlados por usuarios de una pluralidad de entidades empresariales acceda al servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente se realizan a través de una red de comunicaciones; almacenar, por el servidor de intercambio seguro, los datos de autentificación de al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibir contenido de un primero de la pluralidad de dispositivos informáticos cliente; permitir, por el servidor de intercambio seguro, el acceso al contenido para un subconjunto de la pluralidad de dispositivos informáticos mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está gestionado por al menos una entidad empresarial de la pluralidad de entidades empresariales; conceder, por el servidor de intercambio, acceso al contenido a un segundo de una pluralidad de dispositivos informáticos clientes cuando el servidor de intercambio seguro recibe del segundo de la pluralidad de dispositivos informáticos cliente sus datos de autentificación de inicio de sesión de cliente siempre y cuando el segundo de la pluralidad de dispositivos informáticos cliente sea uno del subconjunto de la pluralidad de dispositivos informáticos; y proporcionar un recurso seguro de visualizador del contenido para que el usuario visualice de manera segura el contenido en el dispositivo informático cliente del usuario, donde la visualización segura se proporciona a través de una restricción de la visualización basada en una acción del usuario.

[0091] En modos de realización, el acceso al servidor de intercambio por procesadores cliente puede hacerse mediante un servidor principal controlado por la entidad empresarial que controla el procesador cliente. Los dispositivos informáticos cliente pueden ser al menos uno de los que pertenezcan y que estén gestionados por al menos una de la pluralidad de entidades empresariales. Los dispositivos informáticos cliente pueden pertenecer a usuarios individuales. El servidor de intercambio seguro puede ser al menos uno de una pluralidad de servidores de intercambio seguro. El contenido puede ser al menos uno de entre un documento, una hoja de cálculo, un mensaje, datos, una imagen, contenido de audio, contenido de vídeo, contenido multimedia, y similares. El contenido puede trasladarse al servidor de intercambio seguro por medio de una transmisión de datos cifrada.

[0092] En modos de realización, la restricción de la visualización puede ofuscar la vista del contenido cuando la acción del usuario es un intento de imprimir la pantalla, un aviso de seguridad cuando la acción del usuario es un intento de ver el documento, una marca de agua insertada en el contenido cuando la acción es un usuario imprimiendo el contenido, y similares. El dispositivo informático cliente puede ser un dispositivo informático cliente móvil, como uno personal del usuario, y configurado para la visualización segura del contenido mediante la entidad empresarial.

[0093] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, estableciendo, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación para los datos de autentificación de inicio de sesión de un cliente que permite que al menos uno de una pluralidad de dispositivos informáticos cliente controlados por usuarios de al menos dos entidades empresariales acceda al por lo menos un servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente de usuarios se realiza mediante una red de comunicaciones; almacenando, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión del al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibiendo, de un primero de la pluralidad de dispositivos informáticos cliente, contenido; asociando el acceso, por el servidor de intercambio seguro, al contenido para un subconjunto de la pluralidad de dispositivos informáticos de usuario mediante un recurso de acceso a contenido de intercambio, el recurso de acceso al contenido de intercambio gestionado por al menos una de la pluralidad de entidades empresariales; concediendo, por el servidor de intercambio, acceso al contenido del servidor de intercambio seguro a un segundo de la pluralidad de dispositivos informáticos cliente

de usuarios cuando el servidor de intercambio seguro recibe datos de autentificación de inicio de sesión de un cliente por parte del segundo de la pluralidad de dispositivos informáticos cliente de usuarios y que dependen del segundo de la pluralidad de dispositivos informáticos cliente de usuarios, siendo uno del subconjunto de la pluralidad de dispositivos informáticos cliente de usuario; y proporcionando un recurso de acceso a contenido de intercambio para que el usuario pueda ver de manera segura el contenido en el dispositivo informático cliente del usuario, donde se proporciona una restricción de la visualización basada en una acción del usuario, dectándose la acción del usuario mediante una cámara integrada que funciona en conjunto con el recurso de reconocimiento facial en el dispositivo informático cliente y siendo la restricción de la visualización una ofuscación de la visualización del contenido cuando el usuario es observado, dado que la visualización del contenido por parte de otras personas es un riesgo. El usuario puede ser observado con otras personas en la visualización de la cámara, con una mirada que esté lejos del dispositivo informático cliente, y similares.

[0094] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, estableciendo, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación para los datos de autentificación de inicio de sesión de un cliente que permite que al menos uno de una pluralidad de dispositivos informáticos cliente controlados por usuarios de al menos dos entidades empresariales acceda al por lo menos un servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente de usuarios se realiza mediante una red de comunicaciones; almacenando, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión del al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibiendo, de un primero de la pluralidad de dispositivos informáticos cliente, contenido; asociando el acceso, por el servidor de intercambio seguro, al contenido para un subconjunto de la pluralidad de dispositivos informáticos de usuario mediante un recurso de acceso a contenido de intercambio, el recurso de acceso al contenido de intercambio gestionado por al menos una de la pluralidad de entidades empresariales; concediendo, por el servidor de intercambio, acceso al contenido del servidor de intercambio seguro a un segundo de la pluralidad de dispositivos informáticos cliente de usuarios cuando el servidor de intercambio seguro recibe datos de autentificación de inicio de sesión de un cliente por parte del segundo de la pluralidad de dispositivos informáticos cliente de usuarios y que dependen del segundo de la pluralidad de dispositivos informáticos cliente de usuarios, siendo uno del subconjunto de la pluralidad de dispositivos informáticos cliente de usuario; y proporcionando un recurso de monitorización del visualizador del contenido para monitorizar la visualización del contenido por parte del usuario en su dispositivo informático cliente, donde la monitorización se proporciona mediante una cámara integrada que funciona en conjunto con un recurso de reconocimiento facial en el dispositivo informático cliente.

[0095] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, estableciendo, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación para los datos de autentificación de inicio de sesión de un cliente que permite que al menos uno de una pluralidad de dispositivos informáticos cliente controlados por usuarios de al menos dos entidades empresariales acceda al por lo menos un servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de dispositivos informáticos cliente de usuarios se realiza mediante una red de comunicaciones; almacenando, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión del al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibiendo, de un primero de la pluralidad de dispositivos informáticos cliente, contenido; asociando el acceso, por el servidor de intercambio seguro, al contenido para un subconjunto de la pluralidad de dispositivos informáticos de usuario mediante un recurso de acceso a contenido de intercambio, el recurso de acceso al contenido de intercambio gestionado por al menos una de la pluralidad de entidades empresariales; concediendo, por el servidor de intercambio, acceso al contenido del servidor de intercambio seguro a un segundo de la pluralidad de dispositivos informáticos cliente de usuarios cuando el servidor de intercambio seguro recibe datos de autentificación de inicio de sesión de un cliente por parte del segundo de la pluralidad de dispositivos informáticos cliente de usuarios y que dependen del segundo de la pluralidad de dispositivos informáticos cliente de usuarios, siendo uno del subconjunto de la pluralidad de dispositivos informáticos cliente de usuario; y proporcionando un recurso de monitorización del visualizador del contenido para monitorizar la visualización del contenido por parte del usuario en su dispositivo informático cliente, donde se genera un informe del acceso a la visualización del contenido que proporciona estadísticas relacionadas con el tiempo que el usuario pasa viendo partes del documento. La parte del contenido puede ser a nivel detallado de una página del contenido, a nivel detallado de todo el documento, y similares. El informe de acceso a la visualización del contenido puede contemplar la monitorización y presentación de informes de verificación para el usuario que visualiza del contenido. Las estadísticas pueden utilizarse para desarrollar una inteligencia empresarial.

[0096] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, estableciendo, por un servidor de intercambio seguro controlado por una entidad empresarial intermedia, un procedimiento de autentificación para los datos de autentificación de inicio de sesión de un cliente que permite que al menos uno de una pluralidad de dispositivos informáticos cliente controlados por usuarios de al menos dos entidades empresariales acceda al por lo menos un servidor de intercambio seguro, donde las comunicaciones entre el servidor de intercambio seguro y la pluralidad de

dispositivos informáticos cliente de usuarios se realiza mediante una red de comunicaciones; almacenando, por el servidor de intercambio seguro, los datos de autentificación de inicio de sesión del al menos un cliente para cada uno de la pluralidad de dispositivos informáticos cliente; recibiendo, de un primero de la pluralidad de dispositivos informáticos cliente, contenido; asociando el acceso, por el servidor de intercambio seguro, al contenido para un subconjunto de la pluralidad de dispositivos informáticos de usuario mediante un recurso de acceso a contenido de intercambio, el recurso de acceso al contenido de intercambio gestionado por al menos una de la pluralidad de entidades empresariales; concediendo, por el servidor de intercambio, acceso al contenido del servidor de intercambio seguro a un segundo de la pluralidad de dispositivos informáticos cliente de usuarios cuando el servidor de intercambio seguro recibe datos de autentificación de inicio de sesión de un cliente por parte del segundo de la pluralidad de dispositivos informáticos cliente de usuarios y que dependen del segundo de la pluralidad de dispositivos informáticos cliente de usuarios, siendo uno del subconjunto de la pluralidad de dispositivos informáticos cliente de usuario; y proporcionando un recurso de control del visualizador del contenido para la visualización del contenido controlada por el usuario en su dispositivo informático cliente, donde el control está al menos permitido en parte mediante una cámara integrada que funciona en conjunto con un recurso de reconocimiento del movimiento en el dispositivo informático cliente. El control puede actualizarse mediante la monitorización de los gestos que hace el usuario con la mano, monitorizando los movimientos oculares del usuario, mediante la monitorización de los movimientos de cabeza del usuario, y similares. El control puede estar permitiendo la visualización del contenido, sintonizando una página en la visualización del contenido, insertando una firma en el contenido, cerrando una sesión de visualización del contenido, y similares.

[0097] Haciendo referencia a la Fig. 9, el recurso de interfaz de dispositivo móvil 218 puede proporcionar recursos de manera que pueda utilizarse un dispositivo móvil 902 mientras se mantiene el entorno de intercambio seguro proporcionado por el servidor principal 102 tal como se describe en el presente documento, como para una tableta (por ejemplo, un iPad), un teléfono inteligente, y similares, donde por ejemplo al dispositivo móvil se le proporciona la funcionalidad mediante el recurso de firma electrónica 208, el recurso de visualización 214, y similares. Los recursos proporcionados normalmente mediante el servidor principal 102 tal como se muestra en la Fig. 2 pueden proporcionarse en parte o por completo en el dispositivo móvil, de manera que el dispositivo móvil pueda utilizarse cuando el dispositivo móvil no tenga conectividad con el servidor principal 102. Por ejemplo, el usuario puede ser capaz de iniciar sesión en la misma interfaz como cuando están trabajando a través de un ordenador fijo, como en su ordenador personal, y ver su lista de intercambios, todos sus documentos, todos sus contactos, y similares. Utilizando un iPad como ejemplo, todos los documentos del usuario pueden estar cifrados cuando se envían al iPad, y descifrados para su visualización, de manera que ninguna información se descifra y se almacena en el iPad. Un usuario puede no ser capaz de imprimir y guardar desde un dispositivo móvil, y se le puede proporcionar un visualizador seguro de documentos, tal como se describe en el presente documento, como una visualización parcial, control del movimiento ocular, marcas de agua, y similares.

[0098] Las Figs. 9A-9K representan modos de realización de la interfaz de visualización para dispositivos móviles. La Fig. 9A muestra vistas de intercambio público vs. privado, donde pueden verse 3 intercambios tal como se restringen por las declaraciones públicas-privadas, se ven 31 intercambios cuando se pueden ver todos los intercambios, y pueden verse 15 intercambios si solo se visualizan los intercambios móviles. La Fig. 9B muestra funciones para acceder a los intercambios, carpetas, ficheros, etc. Nótese que puede mostrarse un mensaje si un usuario intenta acceder a un intercambio o entidad sin la declaración requerida. La Fig. 9C muestra ejemplos de visualizaciones de documentos públicos vs. privados. La Fig. 9D muestra ejemplos de añadir una clasificación de documentos, donde puede proporcionarse un botón de control de documentos para cargarlos, puede especificarse una apropiación, y similares. La Fig. 9E muestra ejemplos de usuarios y grupos públicos y privados. Las Figs. 9F-9G muestran ejemplos de informes de acceso a los documentos. La Fig. 9H muestra vistas públicas vs. privadas de documentos. Las Figs. 9I-9K muestran ejemplos de subidas de archivos a los intercambios.

[0099] En modos de realización, puede proporcionarse una aplicación de visualización segura para un dispositivo móvil para establecer una visualización segura 802, como para una tableta (por ejemplo, un iPad), un teléfono inteligente, o un ordenador portátil. En diversos modos de realización expuestos en el presente documento, el usuario de un dispositivo móvil puede ser un empleado u otro individuo asociado con una entidad empresarial. En modos de realización, los usuarios pueden incluir empleados o individuos asociados con las entidades empresariales que sitúan documentos en intercambios de datos seguros así como empleados o individuos asociados con entidades empresariales separadas que recuperan documentos de intercambios de datos seguros o ven o consumen documentos en intercambios de datos. Las entidades en cada caso pueden separarse de manera adicional de una entidad empresarial intermedia que aloja uno o más intercambios de datos seguros. El usuario de un dispositivo móvil puede ser capaz de iniciar sesión en la aplicación de visualización segura, como cuando el usuario está trabajando mediante un dispositivo móvil para ver una lista de intercambios, todos los documentos del usuario relacionados con el intercambio, todos los contactos del usuario relacionados con el intercambio, u otra información, donde la aplicación pueda residir en el dispositivo móvil. En modos de realización, el usuario puede ser capaz de iniciar sesión en la aplicación de visualización segura si el dispositivo está o no conectado a un intercambio, mientras en otros modos de realización algunas o todas las características de la aplicación pueden estar limitadas a situaciones donde se mantiene una conexión con el

intercambio, o a situaciones en las que la aplicación se ha conectado a un intercambio en un determinado periodo de tiempo antes de utilizar la aplicación de visualización segura. La aplicación de visualización segura puede requerir que el usuario introduzca un número de identificación personal (PIN), contraseña, u otra indicación de autentificación (incluyendo opcionalmente indicadores de autentificación biométrica) a fin de acceder a la aplicación.

[0100] Un usuario puede ser capaz de marcar un documento como favorito accediendo al documento desde un dispositivo móvil, un ordenador personal, un portal web, un intercambio o similares. La aplicación de visualización segura puede permitir que un usuario vea una lista de documentos que se han marcado como favoritos. El usuario puede ser capaz de seleccionar un documento individual de la lista y ver el documento en el dispositivo móvil. La aplicación de visualización segura puede monitorizar qué documentos y versiones de los mismos se han seleccionado, y cuándo los usuarios han visto los documentos o las versiones de los mismos. La aplicación de visualización segura puede monitorizar las versiones de los documentos, incluyendo cuándo un usuario ha visto cada versión de un documento, si la aplicación de visualización segura está o no conectada a un intercambio durante la visualización, como, por ejemplo, almacenando los datos relevantes sobre la visualización en el dispositivo móvil para que un intercambio los envíe o recupere cuando el dispositivo móvil está conectado, o mandando información de la visualización en el momento de la visualización desde el dispositivo móvil al intercambio relevante. La aplicación de visualización segura puede comunicar la información monitorizada a un intercambio. La información monitorizada puede comunicarse a un intercambio de manera inmediata si el dispositivo móvil está conectado a un intercambio. Si el dispositivo no está conectado actualmente al intercambio, la información monitorizada puede comunicarse a un intercambio cuando la aplicación de intercambio segura se conecta después a un intercambio. Un intercambio puede poner a disposición un documento para que un usuario lo marque como favorito. Un intercambio puede proteger un documento para evitar que un usuario lo marque como favorito para descargarlo, y similares. Un documento protegido puede restringirse de modo que no se vea sin conexión, puede restringirse de modo que no se imprima la pantalla, puede restringirse de modo que solo lo vea el personal autorizado, y similares.

[0101] La autorización para la visualización puede establecerse por varios métodos, como mediante el reconocimiento facial utilizando una cámara integrada o algún otro tipo de detección biométrica, servicios basados en la ubicación, conectividad de red, etc. Tal como se describe en el presente documento, puede utilizarse una cámara integrada para detectar el rostro del usuario autorizado, el iris del usuario autorizado, la presencia de otras personas en el campo visual de la cámara, etc., y cuando detecta la presencia de un individuo no autorizado, colocar restricciones en la visualización, tal como se describe en el presente documento. Una cámara integrada puede utilizarse en conjunto con una capa de restricción de la visualización, como una lámina física sobre el visualizador del dispositivo móvil, como una pantalla de privacidad (por ejemplo, un filtro polarizador que evite la visualización fuera de un ángulo de visión restringido) o por manipulación del visualizador para dificultar la visualización desde fuera del ángulo. De este modo, la cámara integrada se preconfigura para ver cualquier individuo que sea capaz de ver la pantalla del dispositivo dentro del ángulo restringido de visión de la pantalla de privacidad. Los servicios basados en la ubicación pueden utilizarse para restringir la visualización activando o desactivando la autorización de visualización por parte de un usuario, basada en la ubicación geográfica del usuario. Por ejemplo, el usuario puede no estar autorizado para ver un documento en particular en determinados países, fuera de su país de origen, fuera de una pequeña área geográfica alrededor de una oficia o empresa, alrededor del domicilio del usuario, en una ruta de transporte conocida (por ejemplo, un vuelo que el usuario tenga reservado), etc. Una autorización del usuario para la visualización puede determinarse al menos en parte en la conectividad de red del dispositivo móvil, como con la red de empresa, una red de confianza, una red WiFi, y similares. Por ejemplo, un usuario puede no estar autorizado a descargarse un documento seguro mediante una red móvil, como cuando no están conectados a una red WiFi o por cable. La autorización para la visualización puede ser una combinación de estos y otros parámetros relacionados, donde los parámetros y controles basados en la restricción se controlan mediante un administrador de sistema, como almacenados en un perfil de usuario, determinados por reglas, y similares.

[0102] Si el usuario está conectado a un intercambio mediante una conexión de red autorizada, un usuario puede marcar el documento como favorito y entonces el documento puede descargarse y almacenarse de manera segura en el dispositivo móvil del usuario, como cifrándolo y/o facilitando un formato de archivo especializado e inusual que solo sea accesible por la aplicación móvil segura. Si un dispositivo móvil no está conectado a un intercambio, o si la conexión del dispositivo móvil no tiene suficiente ancho de banda para descargar el documento desde un intercambio, un documento que el usuario haya marcado como favorito puede etiquetarse como favorito por el usuario, y más tarde descargarse y almacenarse de manera segura en el dispositivo móvil del usuario cuando el usuario se conecta al intercambio y la conexión tiene suficiente ancho de banda. La descarga pospuesta puede ocurrir automáticamente o puede ocurrir después de que el usuario inicie más tarde la descarga o confirme que aún se desea la descarga. La aplicación de visualización segura puede alertar al usuario de que se está llevando a cabo la descarga, proporcionar un indicador de progreso de la descarga al usuario, o descargar el fichero en segundo plano sin alertar al usuario.

[0103] El documento puede descargarse sobre una conexión segura entre el intercambio y la aplicación de visualización segura. El documento puede almacenarse en una ubicación segura a la que se pueda acceder solo

por la aplicación de visualización segura, una ubicación de memora encriptada, o una ubicación de memora segura de otra forma. El cifrado utilizado puede ser cualquier esquema de cifrado conocido por un experto en la materia, como un cifrado AES-128, un cifrado AES-192, un cifrado AES-256, etc.

[0104] Puede restringirse un documento en un intercambio de manera que solo pueda accederse a él mediante la aplicación de visualización segura, o puede permitirse el acceso mediante cualquier aplicación que sea compatible con el formato del documento. En modos de realización, puede accederse al documento por la aplicación de visualización segura si el usuario está o no conectado a un intercambio. Puede proporcionarse un ajuste, que puede seleccionar un administrador, para permitir que el administrador restrinja cómo o cuando puede accederse a un documento. Por ejemplo, un ajuste puede permitir que un documento solo sea accesible por la aplicación de visualización segura. Otro ajuste puede permitir que un documento sea accesible por la aplicación de visualización segura y por cualquier otra aplicación que sea compatible con el formato del documento. En modos de realización, el administrador de un intercambio puede configurar el ajuste, como trabajando dentro de una entidad empresarial intermedia, o trabajando para una entidad que coloque documentos en un intercambio. Puede seleccionarse el ajuste para un documento individual, una carpeta del documento, o un grupo de documentos. Un documento que se ponga a disposición para que pueda accederse por cualquier aplicación que sea compatible con el documento puede editarse por otra aplicación y volverse a guardar en un intercambio a través de la aplicación móvil segura sin conexión.

[0105] Un intercambio puede verificar los cambios a los documentos mediante indicadores de modificación, o "marcas de modificación", en los documentos que un usuario ha marcado como favorito. Estos indicadores pueden indicar cuándo se han hecho los cambios a los elementos a los que se ha accedido mediante un intercambio, de manera que pueda hacerse una determinación si le ha ocurrido cualquier modificación a un documento, fichero, etc. entre el tiempo que el usuario se conectó por última vez al intercambio. Las marcas de modificación pueden adoptar la forma de metadatos almacenados en o asociados con un documento, fichero, etc., una etiqueta, o un recurso similar para monitorizar la información de la situación o el estado. Un intercambio puede verificar las marcas de modificación en los documentos que un usuario ha marcado como favoritos cuando el usuario se conecta a un intercambio y entra en la aplicación de visualización segura. Un documento puede borrarse del dispositivo móvil si sus marcas de modificación indican que la versión del documento del dispositivo móvil no es la versión actual. Un documento puede marcarse como obsoleto cuando un usuario se introduce en la aplicación de visualización segura si no es la versión más actual del documento. En modos de realización, el documento obsoleto puede ser visible al usuario. El documento obsoleto puede incluir un indicador para comunicar al usuario que el documento no es la versión actual del documento. Puede denegarse el acceso a un documento obsoleto. Puede descargarse la versión actual del documento. La descarga de la versión actual puede ocurrir de manera automática o a petición del usuario o tras una respuesta confirmatoria a una oferta para la versión actual. El usuario puede descargar inmediatamente la versión actual en el momento en el que el usuario selecciona el documento para la visualización. La descarga puede producirse si el usuario está o no conectado a la aplicación de visualización segura. Una indicación visual puede alertar al usuario de que se está descargando un documento. El usuario puede no ser capaz de acceder a un documento si la descarga de la versión más reciente no se completa antes de que el usuario se desconecte del intercambio.

[0106] Las Figs. 9L-9S representan capturas de pantalla de un modo de realización de una aplicación de visualización segura. La Fig. 9L muestra una pantalla de la aplicación de visualización segura pidiéndole a un usuario que configure un PIN. La Fig. 9M muestra una pantalla de la aplicación de visualización segura que obliga a un usuario a introducir un PIN. La Fig. 9N muestra una pantalla de la aplicación de visualización segura que un usuario utiliza para seleccionar un ajuste. La Fig. 9O muestra una lista de documentos que un usuario que está conectado al intercambio ha seleccionado como favoritos. La Fig. 9P muestra un documento que un usuario ha seleccionado cargándose para su visualización. La Fig. 9Q muestra una pantalla de la aplicación de visualización segura que permite que un usuario seleccione un documento como favorito cuando el dispositivo móvil está conectado a un intercambio. La Fig. 9R muestra una pantalla de la aplicación de visualización segura con una indicación que muestra que un documento que se ha puesto a disposición mediante la aplicación de visualización segura está disponible para abrirse en una aplicación diferente. La Fig. 9S muestra documentos que están disponibles para que los vea un usuario cuando un dispositivo móvil no está conectado a un intercambio y el dispositivo móvil incluye una aplicación de visualización segura.

[0107] La aplicación móvil de visualización segura sin conexión puede utilizarse cuando un usuario quiera acceder a un documento, en especial a uno que esté sujeto a una revisión frecuente, cuando no haya conexión entre el dispositivo móvil y el intercambio. La aplicación de visualización móvil de visualización segura sin conexión puede utilizarse también en situaciones en las que un documento esté sujeto a una política corporativa que requiere el acceso solo a la versión actual del documento. La aplicación de visualización móvil segura sin conexión ayuda a asegurar que se cumplen las políticas corporativas que requieren la prevención del acceso a versiones del documento reemplazadas y pueden ser utilizadas como prueba de que el usuario accedió a la versión actual del documento. La aplicación de visualización móvil segura sin conexión también permite que los usuarios colaboren en los documentos con otros usuarios a través de un intercambio, cuando los documentos no están sujetos a ningún requisito de cumplimiento corporativo en relación a la accesibilidad de la versión.

[0108] En modos de realización, la presente invención puede establecer aspectos tecnológicos relacionados con la arquitectura, componentes estructurales, recursos, datos, comunicaciones, análisis, informes, materiales, componentes entrantes, procesos, algoritmos, etc. La arquitectura, los componentes estructurales, y el recurso pueden incluir un soporte multilingüístico, asociación de metadatos, procesamiento del contenido del documento, distribución del contenido del documento, geoalmacenamiento distribuido, y similares. La relación entre los componentes puede incluir una integración de CRM, un conector del personal de ventas, integración de HCM, integración de ERP, integración de ECM, integración de aprendizaje virtual, y similares. Los datos, las comunicaciones, los análisis, y los informes pueden incluir informes del historial del usuario, informes de actividad, informes de permiso, informes de acceso, informes de cumplimiento y verificación, paneles configurables, informes del autoservicio (por ejemplo, personalizados, programados, *ad hoc*), gestión de carpetas IMAP, integración exdata, y similares.

[0109] En modos de realización, la presente invención puede establecer aspectos de productos relacionados con características, atributos, beneficios, resultados, beneficios funcionales, seguridad, etc. Los productos pueden incluir una integración desde una sala de datos segura, una bifurcación pública-privada en el mercado de préstamos, dispositivos móviles seguros, y similares. Las características, atributos y beneficios pueden incluir documentos protegidos para iPad, informes recuperados, *branding*, canales, alertas, gestión de tareas, gestión de procesos multitareas, indización automática, migración, automatización (por ejemplo, automatización ILIA), especialización (por ejemplo, campos personalizados, flujo de trabajo personalizado), soporte de ficheros muy grandes, gestión de documentos (por ejemplo, revisar y aprobar, registro de entrada y de salida, control de versiones), interfaz de usuario personalizable, bandeja de entrada unificada, y similares. Las características de los productos pueden incluir alertas personalizadas, servicios del comprador, adición en masa de ficheros y carpetas, indizar información de manera dinámica, búsqueda y filtros avanzados y federados, campos y etiquetas personalizadas, integración con formatos de documentos de terceras partes (por ejemplo, productos de Microsoft Office), añadir y gestionar usuarios y grupos, subidas de varios archivos, comentarios, almacenamiento compatible, visualización de documentos en formato nativo, inteligencia empresarial basada en informes de actividad, componentes de preguntas y respuestas, asignación de enlaces, visualización segura sin complementos, comunicaciones y colaboraciones unificadas (por ejemplo, notificación de la presencia, hilos de discusión, de chats y de mensajería instantánea, foros y wikis), capacidad de administración, formularios electrónicos, y similares. La seguridad puede incluir gestión de derechos bajo demanda, acceso y autentificación (por ejemplo, acceso a nivel de contenido y de documento, autentificación multifactorial, inicio de sesión único), cifrado de datos, monitorización y verificación, seguridad intraestructural (por ejemplo, protección de sistemas, verificaciones de seguridad), seguridad personal, seguridad de procesos, cifrado, marcas de agua, y similares.

[0110] En modos de realización, la presente invención puede establecer usos relacionados con aspectos del mercado, aplicaciones, entornos de utilización, condiciones de uso, ecosistemas, cadenas de valor, integración de sistemas, etc. Las aplicaciones pueden incluir un repositorio corporativo, colaboración en equipo extendida, administración de la transferencia de ficheros, extranet segura, gestión del ciclo de vida del proyecto, presentación de informes a la junta directiva, extranet jurídica, repositorio jurídico, colaboración jurídica, administración de la transferencia de ficheros, presentación de informes y auditoría reguladora, extranet segura, gestión de auditoría financiera, captación de fondos, comunicación con inversores, gestión de contratos, formularios reguladores, comunicación de la junta directiva, integración de la característica de conformidad, encargado de acceso, financiación del capital del proyecto, colaboración en proyectos, gestión de la cadena de suministro, fabricación por contrato, etc. Los mercados pueden incluir finanzas, sindicación de préstamos, fusiones y adquisiciones (por ejemplo, gestión de relaciones y actividades de *marketing*, interacciones con clientes, envío documentos y contratos legales para formular observaciones, editar, y firma), inversiones alternativas, banca comercial, banca de inversión, quiebra y reestructuración, desarrollo corporativo, construcción, ciencias de la vida, productos farmacéuticos, biotecnología, energía y servicios públicos, gestión de casos de tasas de servicios públicos, seguros, telecomunicaciones, administración de los ciclos de vida de los proyectos, tecnología de la información, servicios jurídicos, gobierno, fabricación, bienes raíces, medios de comunicación y entretenimiento, etc. Los entornos de utilización pueden incluir desarrollo corporativo, repositorio corporativo, finanzas corporativas, legislación corporativa, ingeniería, recursos humanos, *marketing*, servicios generales, investigación y desarrollo, cumplimiento y seguridad, línea de negocio, etc. Las condiciones de uso pueden incluir, quiebra y reestructuración, presentación de informes a la junta directiva, desarrollo y licencias comerciales, activación de webs clínicas, colaboración de equipos extendida, captación de fondos, ofertas públicas de venta (OPV), portales de inversores, informes para inversores, extranet jurídica, administración de transferencia de ficheros, fusiones y adquisiciones, colocaciones privadas, gestión del ciclo de vida del proyecto, presentación de informes y auditoría regulatoria, gestión de casos regulatorios, distribución de documentos de seguridad, extranet segura, financiación estructurada, préstamos sindicados, sala de datos virtual, etc.

[0111] Los métodos actuales para compartir ficheros informáticos no son suficientemente seguros ya que un usuario puede cometer errores al enviar información, como con un único clic errante, y enviar información confidencial a manos equivocadas sin que haya manera de recuperar los materiales enviados. De manera alternativa, puede proporcionarse información confidencial a un socio de confianza que posteriormente deje una empresa o departamento, a un vendedor donde la empresa del usuario cambia posteriormente los vendedores, a alguien de fuera de la empresa que posteriormente es considerado un riesgo para la distribución de información

confidencial, y similares, en los que al remitente le gustaría revocar el acceso al contenido compartido. La presente invención puede establecer métodos y sistemas para compartir contenido de manera segura (por ejemplo, contenido de datos informáticos, como documentos, presentaciones, hojas de cálculo, correos electrónicos, entradas de blog, textos, y similares) que permitan "dejar de compartir" el contenido que se ha compartido previamente. El recurso para dejar de compartir contenido puede implementarse asociando el contenido con una característica de protección segura, como mediante la gestión de derechos digitales (DRM), cifrado, permisos, y similares. En modos de realización, cada elemento de contenido puede compartirse con la característica de protección, donde la característica de protección específica un usuario o grupo de usuarios que están autorizados para acceder al contenido para visualizarlo. Después, cuando el contenido se comparte con ese usuario, el acceso al contenido puede revocarse en cualquier momento (por ejemplo, cambiando la DRM, quitando el acceso a la clave, cambiando los permisos, y similares). Además, si el remitente del contenido controla la característica de protección, entonces el remitente tiene control vitalicio completo de cualquier contenido que distribuya o al que permita el acceso.

[0112] El recurso seguro para dejar de compartir puede utilizarse para compartir contenido de manera segura además de los recursos protectores de su empresa (por ejemplo, permitiendo el acceso de manera segura más allá del cortafuegos de la empresa del remitente), para usuarios de otras empresas, en espacios públicos, a usuarios sin intención de conseguir el contenido, y similares, donde el remitente mantiene el control completo del acceso al contenido, sin importar dónde o a quién se le haya distribuido el contenido. De este modo, se facilita el intercambio de manera segura del contenido a lo largo de los límites corporativos a nivel de usuario y a nivel de contenido individual (por ejemplo, a nivel de un documento individual). De manera adicional, el proceso permite que un usuario que quiera dejar de compartir un contenido lo haga de manera discreta, permitiendo que el remitente revoque el acceso sin tener que contactar o rastrear a los destinatarios, que pueden no tener ninguna indicación de que se les ha revocado el acceso. Con el recurso para dejar de compartir, el contenido simplemente deja de ser accesible. Y la revocación del acceso puede no ser solo para el contenido original, sino para todas las versiones del documento, como las copias almacenadas en varios dispositivos y entornos informáticos (por ejemplo, almacenados en el escritorio, tableta, teléfono móvil inteligente, en una aplicación, mediante un navegador, etc.), copias enviadas a terceras partes, y similares. Y como la característica de protección puede aplicarse a todas las versiones que se hayan modificado (por ejemplo, versiones editadas, versiones con control de cambios, versiones con comentarios, versiones firmadas, y similares), también puede revocarse el acceso a versiones modificadas del contenido cuando se revoca el acceso al contenido original.

[0113] En modos de realización, el acceso a contenido compartido puede requerir una autentificación de acceso a un recurso seguro, como un servidor de intercambio seguro. Esto es, incluso si el contenido se ha compartido con un usuario, el usuario solo puede ser capaz de ver el contenido si se autentifica su acceso. La autentificación puede ser un inicio de sesión manual para verificar que el usuario que está intentando acceder al documento es un usuario que aparece en la lista de acceso al contenido. De forma alternativa, un usuario que tenga acceso puede establecer un dispositivo informático que esté ligado a su autentificación personal, como mediante el recurso seguro. Por ejemplo, un usuario autorizado puede asociar su autorización personal a su dispositivo informático portátil (por ejemplo, una tableta o un teléfono inteligente), como donde el dispositivo informático portátil tenga una contraseña para acceder al dispositivo, asegurando por consiguiente que la persona que solicita el acceso desde el dispositivo móvil es el usuario autorizado.

[0114] En modos de realización, el proceso de seguridad que protege el contenido, como un documento a subir y compartir, puede incorporar una pluralidad de etapas de protección. Por ejemplo, cuando se sube un documento puede ejecutarse un análisis de virus, pueden establecerse permisos, puede crearse un índice de búsqueda, puede aplicarse protección digital, el documento puede convertirse (p. ej., formateado), el documento puede cifrarse, y similares, donde el cifrado puede aplicarse individualmente a cada contenido nuevo, como a través de claves de cifrado generadas de manera aleatoria. Cuando se solicite una descarga del documento, como cuando un usuario autorizado está descargándose una parte del documento compartido, puede generarse una clave aleatoria con una identificación de clave para ese documento en particular en el que el documento está cifrado con la clave aleatoria. Puede dividirse una clave maestra entre una base de datos y un sistema de ficheros, donde la clave aleatoria cifrada y el identificador de clave aleatoria se almacenan en la base de datos, y la clave aleatoria puede cifrarse con la clave maestra, y similares. Entonces, pueden aplicarse permisos, análisis de virus, marcas de agua, protección digital, y similares, antes de entregar del documento.

[0115] En modos de realización, el recurso para dejar de compartir puede habilitar el control del acceso hasta a nivel de contenido individual, como con la creación de un nuevo documento, que puede formar parte de o ser el comienzo de una línea de trabajo social colaborativo, permitiendo que los usuarios compartan el contenido, y luego inicien y perpetúen las conversaciones e interacciones en torno a esos contenidos. Las líneas de trabajo social pueden permitir hilos de debate, ámbitos de actividad y otros recursos comunes de interacción social, que pueden utilizar el contenido como la base organizativa. El proceso de dejar de compartir un documento puede deberse a la eliminación del contenido de la línea de trabajo, a la retirada de la línea de trabajo, a la eliminación completa del contenido individual, y similares.

[0116] La presente exposición describe una solución de intercambio seguro del contenido y de la productividad para compartir contenido confidencial y no confidencial entre empresas por una red de comunicación global

como Internet, incluyendo cortafuegos de empresas exteriores. La presente exposición puede proporcionar un entorno seguro de intercambio de contenido y de colaboración que vaya más allá del cortafuegos de la empresa; estableciendo un entorno de flujo de trabajo constante de usuario de doble uso que aloje contenido de intercambio seguro y personal sin la necesidad de que un usuario adopte sustancialmente un nuevo proceso de flujo de trabajo y aplicaciones; proporcionando interfaces seguras para la visualización de documentos utilizando dispositivos informáticos móviles, como tabletas con interfaces táctiles (por ejemplo, incluyendo la incorporación de dispositivos personales del usuario); y similares.

[0117] La necesidad de un espacio de intercambio de contenido más allá del cortafuegos se ha creado por la confluencia de la evolución de la tecnología (por ejemplo, la virtualización y la informática en la nube, la innovación del factor de forma portátil, herramientas de inteligencia empresarial de "macrodatos"), cambios organizativos (por ejemplo, colaboración entre empresas en rápido crecimiento, fragmentación global de la empresa, equipos multidisciplinarios, cambios demográficos), cambios en el papel de la tecnología de integración (por ejemplo, reducción de la complejidad y los costes, presión para un valor empresarial medible, "informatización" de la TI de la empresa, y "trae tu propio dispositivo"), asuntos reguladores y gubernamentales (por ejemplo, incremento de la regulación, amenazas a la ciberseguridad), y similares que aumenten de manera colectiva la importancia de una colaboración fácil y segura de documentos y contenido más allá del cortafuegos de la empresa. Otras soluciones han adoptado una variedad de enfoques para ocuparse de fragmentos de estos requisitos, pero aún hay importantes necesidades insatisfechas para los directores, líderes empresariales, y usuarios de tecnología de la información, incluyendo en el ámbito de la integración de seguridad/control, facilidad de uso, funcionamiento continuo a lo largo de diferentes modos de intercambio, y similares.

[0118] En modos de realización, el sistema puede incluir métodos y sistemas para proporcionar una única estructura para mejorar las formas más comunes de intercambio de contenido más allá del cortafuegos, mejorando la productividad individual y de equipo a lo largo de la empresa extendida mientras proporciona seguridad y cumplimiento unificados para la TI y los líderes empresariales; permitir que los usuarios continúen el intercambio más allá del cortafuegos de la manera en que prefieran con una interfaz de usuario única que aumente la seguridad y productividad del correo electrónico, de las carpetas sincronizadas y compartidas, gestión externalizada del contenido empresarial, y herramientas empresariales de colaboración social; integrarse con servicios de sincronización e intercambio centrados en el consumidor en la medida de lo posible para habilitar su uso seguro y conforme dentro de la empresa; mejorar las formas de colaboración a las que los usuarios ya están acostumbrados, y no requerir la adopción de nuevas formas de trabajar o destinos de colaboración; enfocar la colaboración única y compartir los requisitos de la empresa extendida y complementar otros sistemas de empresa, y similares.

[0119] En modos de realización, una necesidad para un sistema de intercambio comprensivo puede incluir una facilidad de uso y una interfaz de usuario intuitiva; con permisos de seguridad detallados, para ayudar a asegurar que individuos no autorizados no puedan abrir documentos; la habilidad de controlar el contenido después de compartirlo (por ejemplo, la habilidad de retirar un documento), permitiendo que un usuario recupere y destruya datos de manera remota, como utilizando una sala de datos virtual; herramientas de productividad integradas en el intercambio de contenido, consolidando una pluralidad de inicios de sesión y contraseñas de usuario; la habilidad de integrarse en la infraestructura existente, para eliminar la necesidad de una pluralidad de herramientas de intercambio; proporcionando múltiples canales de colaboración a fin de integrar los métodos y sistemas en tantas plataformas de productividad como sea posible, etc.

[0120] Haciendo referencia a la Fig. 10, la presente invención describe un recurso de acceso a contenido de intercambio 1008 en conjunto con el servidor de intercambio seguro 1002 que mejora la seguridad con la que una pluralidad de usuarios 1004 colaboran libremente, incluido mediante una pluralidad de diferentes recursos y dispositivos de intercambio de contenido, mientras proporcionan un control vitalicio de su contenido. Por ejemplo, supongamos que un usuario mandó datos de ventas trimestrales a una antigua empresa de contabilidad, los registros de empleados a alguien de fuera del departamento de recursos humanos, el contrato equivocado al vendedor equivocado. Cuando un usuario "deja de compartir", el acceso al contenido puede revocarse de manera instantánea, incluido cualquier contenido que pueda haber de copias del contenido original. En modos de realización, el usuario puede tener control vitalicio total de cada uno de los elementos de contenido, como documentos, correos electrónicos, comunicaciones, y similares. En modos de realización, el contenido puede almacenarse y monitorizarse en una base de datos segura 1012. Los usuarios pueden compartir y revocar el acceso al contenido hasta a nivel de documento, proporcionando un lugar seguro para subir los archivos y compartirlos entre dispositivos. De este modo, se proporciona a los usuarios un recurso seguro de almacenamiento para la información confidencial de la empresa, donde los usuarios sean capaces de trabajar de manera más segura, como con su infraestructura existente (por ejemplo, integración permanente con aplicaciones como Microsoft Outlook, SharePoint, y similares). El recurso para dejar de compartir puede permitir que un usuario cree una nueva línea de trabajo, que suba los documentos de manera segura, y trabaje con equipos que estén habilitados para colaborar de forma segura. Además, el recurso para dejar de compartir puede proporcionar informes, verificaciones, sumarios, y similares mediante un recurso de panel, como una vista general de todas las líneas de trabajo, ajustes de seguridad personalizados, la habilidad de añadir nuevos participantes, proporcionar informes automatizados, y similares. El recurso de acceso a contenido de intercambio

1008 puede utilizar un recurso de autentificación de datos de inicio de sesión del usuario 1010 para autentificar el acceso de los usuarios al contenido, donde puede existir la opción de tener un inicio de sesión único en conjunto con otros inicios de sesión de usuario. En modos de realización, el inicio de sesión puede utilizar una función *hash* de seguridad al redirigir una URL, como para proteger el inicio de sesión contra ataques de *phishing*. El inicio de sesión único puede extenderse a dispositivos móviles, incluidos dispositivos móviles personales, donde puede utilizarse una tabla de consulta para verificar que el usuario tenga capacidad de entrar con un inicio de sesión único o no.

[0121] En modos de realización, puede proporcionarse un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red. El servidor de intercambio seguro 1002, como, por ejemplo, gestionado por una entidad empresarial intermedia, puede establecer un procedimiento de autentificación de datos de inicio de sesión de usuario que permita que un usuario acceda al servidor de intercambio seguro, donde el servidor de intercambio seguro puede almacenar datos de autentificación de inicio de sesión para cada uno de la pluralidad de usuarios, como en una base de datos segura. Los usuarios pueden acceder al servidor de intercambio seguro mediante una pluralidad de diferentes dispositivos informáticos, aplicaciones, canales de comunicaciones, y similares. El usuario puede ser uno de una pluralidad de usuarios 1004 que funcionen para una pluralidad de otras entidades empresariales (por ejemplo, los usuarios pueden ser empleados de la misma entidad empresarial o los usuarios pueden estar trabajando para diferentes entidades empresariales), donde los usuarios de otras entidades empresariales se comunican con el servidor de intercambio seguro mediante una red de comunicaciones, como una red de área extensa (por ejemplo, Internet). Para compartir un elemento de contenido informático, un primero de una pluralidad de usuarios puede pedir un acceso compartido desde el servidor de intercambio seguro a un elemento de contenido a por lo menos un segundo de una pluralidad de usuarios. La gestión para el acceso al contenido puede hacerse mediante un recurso de acceso a contenido de intercambio 1008 gestionado por la entidad empresarial intermedia. Después de que el servidor de intercambio reciba el contenido desde el primero de una pluralidad de usuarios, puede conceder el acceso compartido al contenido cuando el servidor de intercambio seguro recibe del segundo de la pluralidad de usuarios sus datos de autentificación de inicio de sesión (siempre y cuando el segundo de la pluralidad de usuarios sea uno del subconjunto de la pluralidad de usuarios a los que se le permite el acceso compartido). El segundo de la pluralidad de usuarios entonces puede solicitar una copia del contenido del servidor de intercambio seguro, donde se hace una copia del contenido. Además, el segundo de una pluralidad de usuarios puede copiar de manera adicional el contenido en una pluralidad de dispositivos informáticos diferentes, hacer cambios, revisiones, anotaciones y similares a una nueva versión del contenido, enviar el contenido a otros usuarios, mandar el contenido a personas y a dispositivos informáticos más allá de los límites de las entidades empresariales, y similares. Para dejar de compartir el contenido, el primero de una pluralidad de usuarios puede pedirle al servidor de intercambio seguro que revoque el acceso compartido al contenido al segundo de la pluralidad de usuarios. Como resultado, el servidor de intercambio seguro revoca el acceso por el segundo usuario al contenido, como mediante el cifrado y los recursos de DRM descritos en el presente documento. Además, esta revocación del acceso del segundo usuario al contenido puede aplicarse de manera similar a todos los ejemplos del contenido en la pluralidad de usuarios, donde la revocación del acceso compartido al contenido revoca el acceso a todas las versiones del contenido compartido y a todas las copias del contenido hechas por la pluralidad de usuarios. De manera similar, cualquier individuo que no tenga la autoridad para acceder al contenido puede no tener la habilidad de acceder a cualquier versión del contenido. En modos de realización, pueden borrarse copias del contenido desde el servidor seguro de datos, donde el borrado del acceso a la copia del contenido es una revocación de la gestión de derechos digitales del contenido. La gestión de derechos digitales del contenido puede controlarse en parte por el primero de la pluralidad de usuarios, incluyendo la revocación del acceso al contenido mediante los cambios en la gestión de derechos digitales asociada con el contenido. El contenido puede ser un contenido cifrado seguro. Los usuarios pueden ver de manera segura el contenido mediante un recurso de visualización seguro. Los usuarios pueden estar conectados a una red pública que esté fuera del cortafuegos para la entidad empresarial que los gestiona. Los usuarios pueden acceder al contenido mediante un dispositivo informático personal que no sea propiedad de la entidad empresarial que los gestiona, como, por ejemplo, mediante un ordenador personal, un dispositivo móvil personal, y similares. Los usuarios, mediante un recurso de panel, pueden interactuar con el recurso de acceso a contenido de intercambio, donde el recurso de panel puede proporcionar informes que muestran la actividad relacionada con el intercambio del contenido. El recurso de panel puede ser accesible mediante entornos de terceras partes. El recurso de panel puede monitorizar la ubicación y la versión del contenido compartido en dispositivos informáticos accesibles por el al menos segundo de la pluralidad de usuarios.

[0122] La Fig. 10A proporciona un ejemplo no limitativo de cómo puede proporcionar la presente invención un flujo de trabajo mejorado entre individuos colaborativos. En este escenario de flujo de trabajo, un trabajador del conocimiento de una empresa, "Fred", (por ejemplo, un abogado interno) está colaborando con un responsable principal de información, "George", que trabaja en la misma empresa que Fred, y un socio externo, "Pam" (por ejemplo, un abogado externo). Como se muestra, en la primera etapa 1021, Fred puede sincronizar los archivos de su ordenador personal, como con recursos en la nube. Estos recursos pueden incluir la sincronización con recursos de salas de datos seguras virtuales, recursos de sincronización de equipos de terceras partes que sean compatibles con la presente invención, y similares, y pueden ponerse a disposición mediante el recurso de panel. En una segunda etapa 1022, Fred también puede acceder a sus archivos y tener la habilidad de sincronizar los

dispositivos que George haya aprobado, como mediante una sala de datos segura virtual, un recurso de política de empresa o de empresa compartida, y similares. En una tercera etapa 1023, Fred puede ver el estado de un proyecto en el que Pam y él estén trabajando, como mediante el recurso de panel. Como parte de una plantilla del proceso, se le puede recordar que envíe un fichero a Pam para que lo revise. En una cuarta etapa 1024, Pam puede recibir el fichero en su iPad, donde lo abre para revisarlo, como mediante el recurso de visualización en un dispositivo móvil. En una quinta etapa 1025, ahora Fred puede querer compartir algunos ficheros confidenciales con Pam, como a través de un recurso de sala de datos segura virtual, con la habilidad de "retirar" el documento de Pam en cualquier momento a través del recurso para dejar de compartir. Además, Fred puede pedirle a Pam que anote, revise, marque, corrija, y similares, el fichero que está compartiendo, como a través de una aplicación de creación de contenido (por ejemplo, un procesador de texto, una aplicación de hoja de cálculo, una aplicación de presentaciones, una herramienta de medios), el recurso de votación de enmiendas, el recurso de firma electrónica, a través del recurso de visualización segura, y similares. En una sexta etapa 1026, basándose en el destinatario y la inspección del contenido, Fred puede ver que sus acciones son arriesgadas y decide remediarlas, como dejando de compartir el documento para que Pam no tenga acceso, tal como se implementó mediante el recurso de panel, y similares. Entonces, él puede, por ejemplo, elegir compartir los archivos como de solo lectura. En una séptima etapa 1027, Pam recibe una notificación del sistema en su ordenador Macintosh, por ejemplo, a través del recurso de panel. En una octava etapa 1028, Pam hace anotaciones en el fichero de solo lectura en la aplicación de Mac, y completa la tarea, por ejemplo, a través de una aplicación con la que Pam está familiarizada y que está integrada para mayor facilidad de uso en el entorno de flujo de trabajo familiar creado por la presente invención. En una novena etapa 1029, Fred ve que Pam ha acabado su tarea, por ejemplo, mediante el recurso de panel, y abre el fichero anotado y lo sincroniza (por ejemplo, a través de SharePoint). En una décima etapa 1030, Fred gestiona los elementos de trabajo en equipo en contraste con un horario, y cuando todas las tareas se han completado, cierra el proyecto. Por ejemplo, el proyecto puede haber sido un proyecto de sindicación de préstamo, y una vez completado, Fred puede eliminar por completo la accesibilidad a los documentos y comunicaciones que se transmitieron durante la transacción, por ejemplo, retirando el acceso a cualquier documento que se haya transmitido durante la ejecución del proyecto. En una undécima etapa 1031, Pam puede revocar los ficheros cuando se haya completado el proyecto, y los ficheros se borran de sus dispositivos, por ejemplo, retirando el sistema los ficheros tal como los ha rastreado el sistema en una base de datos segura creada para el proyecto (que en sí misma puede borrarse una vez se haya completado el proyecto). En una duodécima etapa 1032, George puede ver una actividad de intercambio arriesgada en su sistema de gestión de eventos de seguridad, y en una decimotercera etapa 1033, ver un informe de cumplimiento en un sistema de gobernanza, gestión de riesgos y cumplimiento (GRC), por ejemplo, mediante la monitorización a través del recurso de panel. En modos de realización, puede iniciarse un hilo de flujo de trabajo en un intercambio entre otras entidades empresariales, con individuos seleccionados en una microtransacción, desde un hilo de correos electrónicos, y similares. En modos de realización, un usuario puede estar habilitado para crear un concepto de un gran proyecto y utilizar capacidades de microtransacción para dividir el gran proyecto en proyectos más pequeños que puedan volverse a enlazar al gran proyecto. Un usuario puede ser capaz de crear tareas desde su bandeja de entrada del correo electrónico, convertir un hilo de correos electrónicos en una tarea, despejar una tarea convirtiendo el correo electrónico en una línea de trabajo, hacer de un intercambio una extensión de un correo electrónico, y similares.

[0123] En modos de realización, el sistema puede establecer la habilidad de borrar contenido de forma remota desde un dispositivo mientras que el dispositivo esté fuera de línea o no esté conectado a una red. Esta capacidad puede implementarse proporcionando una concesión a una aplicación de escritorio cuando se inicie, y tenga un inicio de sesión satisfactorio, tal como está configurado por una política mediante una consola de administración. Cuando un dispositivo está encendido y haya expirado un periodo de concesión sin un inicio de sesión satisfactorio durante el periodo de concesión, el sistema puede iniciar un borrado de archivos, como ocurriría si el dispositivo se hubiese perdido o robado. Esta aplicación puede ser un servicio de escritorio separado que se ejecuta en el dispositivo en segundo plano (por ejemplo, se suspende y se activa en intervalos de tiempo predefinidos). Cuando se enciende un dispositivo, la aplicación puede registrar los valores de la fecha/hora de vencimiento de la concesión de un inicio de sesión previo satisfactorio. En otro ejemplo, el servicio puede intentar conectarse a un servidor, y si detecta que la conexión falla continuamente pasadas la fecha y hora de vencimiento de la concesión, puede asumir que o bien el dispositivo ya no necesita ejecutar la aplicación, o que puede haber sido robado o perdido. En el caso de que un dispositivo se encuentre o reutilice posteriormente, el contenido puede volverse a sincronizar para el usuario una vez que inicien sesión de manera satisfactoria en la aplicación. Pueden existir concesiones duras o blandas implementadas en el sistema. En el ejemplo de una concesión dura, los ficheros pueden borrarse permanentemente en el equipo local cuando la concesión vence. En una concesión blanda, en lugar de borrar los datos, el sistema puede moverlos a una ubicación aleatoria en el disco donde un usuario no pueda encontrarlos. Por ejemplo, el sistema puede modificar el atributo de la carpeta para los datos, como "+S +H". Configurar estos atributos lo marcará como un fichero del sistema operativo importante, de manera que el sistema operativo no mostrará los datos incluso si la configuración permite la visualización de ficheros y carpetas ocultas. En modos de realización, el sistema puede establecer el borrado automático de documentos, independientemente de si el dispositivo está en línea o no, basado en un intervalo de fecha/hora. Por ejemplo, configurar un intervalo de fechas para que la vida de los documentos esté entre una fecha/hora y otra, momento en el que se borrarán todos los documentos y carpetas relacionados. El sistema

también puede borrar documentos, carpetas, escritorio, y similares, después de un número predeterminado de intentos de inicio de sesión fallidos, donde el sistema puede volver a proporcionar el acceso tras la restauración de los privilegios de acceso.

[0124] En modos de realización, el sistema puede establecer el borrado remoto de documentos mediante un recurso de acceso local limitado, en el que el usuario puede tener acceso a un documento, carpeta, y similares, solo mediante una aplicación local cifrada. De este modo, los ficheros siguen encriptados en un equipo de usuario y el único modo de acceder a ellos es utilizar la aplicación que descifrará los documentos. La aplicación local también puede incrustarse, tal como se describe en el presente documento, como a través de un navegador, donde un usuario solo puede tener acceso a documentos con credenciales que se asocian a la llave de cifrado. La aplicación local puede ser una aplicación de visualización, donde los documentos están distribuidos a través de un motor de distribución, pero donde el usuario solo puede ver los documentos utilizando el visualizador que descifraría el documento para su visualización.

[0125] En modos de realización, el sistema puede integrar la capacidad de intercambio con otros entornos de terceras partes, como incluyendo las soluciones existentes de intercambio de ficheros (por ejemplo, Dropbox, Google Drive, SkyDrive, Box.com, MediaFire, SugarSync, TitanFile, YouSendIt, SparkleShare, Ubuntu One) que proporcionan almacenamiento en la nube, sincronización de archivos, *software* cliente, y similares. Además de intercambiar recursos, la presente invención también proporciona una opción de "compartir" dentro de otras soluciones de flujo de trabajo diario de terceros, como herramientas de escritorio (por ejemplo, Microsoft Office, iWork, Google Docs, OpenOffice, y similares), y herramientas de empresa (Enterprise DB, herramientas de CRM, herramientas analíticas), y similares, donde sin salir de la interfaz de la aplicación o herramienta del tercero, la presente invención puede permitir que el contenido se comparta fuera de la empresa con otra parte, pero con la sala de datos segura y las características de visualización seguras tal como se describen en el presente documento (por ejemplo, la habilidad de monitorizar el acceso y la visualización, la habilidad de tener una visualización anotaciones de "solo lectura", la visualización segura en un dispositivo móvil, la habilidad de retirar un documento), y similares. De manera adicional, la presente invención puede ser capaz de interactuar con procesos de intercambio seguro basados en modelos, como teniendo eventos de entrada y acciones de salida en consonancia con estos (por ejemplo, Outlook recibe un correo electrónico de un proceso seguro y señala una acción, LinkedIn permite que un usuario vea y apruebe un elemento de votación corporativa).

[0126] En modos de realización, el sistema puede permitir que una organización maximice el valor del contenido al equilibrar la libertad para compartir con el control y monitorización necesarios proporcionados por el sistema, que amplía la manera en la que trabaja la organización, por ejemplo, permitiéndoles que compartan y accedan al contenido donde sea necesario, controlando y monitorizando el contenido dondequiera que vayan, coordinar el trabajo entre las personas, organizaciones y dispositivos como una extensión natural de herramientas y experiencias familiares. El sistema puede establecer un recurso global de servicios completos como un "socio" dondequiera que vaya el usuario, proporcionando visibilidad y control de contenido centrado en el trabajo, libertad para colaborar, y similares. El sistema puede proporcionar un estándar de confianza para la seguridad de la información "más allá del cortafuegos", proporcionando automatización y monitorización de la política de información corporativa, extendiendo una experiencia de usuario y una infraestructura existente familiar, y similares. De manera colectiva, los métodos y sistemas de la presente invención pueden establecer una "estructura" de intercambio basada en el objetivo para permitir una colaboración comprensiva.

[0127] En modos de realización, el sistema puede establecer una conectividad, seguridad, productividad y similares, mejoradas, en relación con un entorno de trabajo colaborativo compartido. La productividad puede incluir la habilidad de asignar y gestionar acciones de empresa centradas en los documentos (por ejemplo, la firma electrónica), gestión de tareas de proyectos, y similares, por ejemplo, para proporcionar plataformas de intercambio de documentos más estructuradas (por ejemplo, más que solo el correo electrónico, que puede ser una comunicación *ad hoc*). La seguridad puede incluir permisos basados en ficheros y en roles, fuera del cortafuegos, retirada de permisos de documentos, de contenido del documento automático y de la clasificación de seguridad, y similares. La conectividad puede incluir una conexión única segura a las herramientas de intercambio de documentos a través de dispositivos, acceso seguro a una plataforma de ECM interna para partes externas, integración de seguridad de carácter empresarial en las herramientas de sincronización e intercambio existentes, y similares, por ejemplo, para permitir acceso donde lo necesite el cliente y la habilidad de actualizar fácilmente los documentos, independientemente de dónde se encuentre el usuario. El sistema puede proporcionar características analíticas avanzadas para mejorar la productividad, como el cumplimiento de las verificaciones, versionado y monitorización de documentos, contextualización de documentos, análisis del rendimiento histórico, analítica predictiva, optimización de la productividad de las tareas, etc. El sistema también puede incluir características colaborativas sociales para mejorar las interacciones en los proyectos, como comunicaciones mejoradas en el flujo de trabajo, gestión segura del proyecto, colaboración basada en la tableta, coedición sincronizada, colaboración social, una capa social en torno a las aplicaciones empresariales, y similares.

[0128] En modos de realización, el sistema puede establecer la sincronización e intercambio para el profesional empresarial individual, incluyendo una pluralidad de canales (por ejemplo, cliente de escritorio de Windows, navegador web, Microsoft Outlook para Windows, soporte para iOS [como una aplicación nativa para

el iPhone y el iPad]), características (por ejemplo, sincronización de ficheros y carpetas de escritorio; intercambio seguro de ficheros desde el escritorio, navegador, y iOS; notificaciones *push*, hilos y comentarios de discusión colaborativa; registro automático del usuario), para el trabajo con un objetivo empresarial (por ejemplo, mandar una copia para descargarla, compartir el acceso a un fichero situado en el centro para su revisión), la administración (por ejemplo, informes de la actividad predefinidos, como para el cumplimiento; informes de contabilidad verificación predefinidos, como para facturar); política de grupo centralizada, como para los defectos de seguridad), seguridad (por ejemplo, con fuertes cifrados y permisos para cada archivo; acceso a los ficheros de solo lectura basado en el navegador; fichero integrado de gestión de derechos de información (IRM), y gestión de derechos digitales (DRM); revocación del acceso al archivo, seguridad de los dispositivos móviles; verificación de complicidad completa), y similares. El término "trabajar con un objetivo empresarial" puede incluir la habilidad de los usuarios de intercambiar archivos "con objetivo". Por ejemplo, el objetivo puede venir en forma de tareas del documento que pueden asignarse a destinatarios, donde el sistema puede dejar que los usuarios manden ficheros para su revisión, para su anotación, comentarios, etc. Por ejemplo, el sistema puede querer dar a los usuarios la habilidad de combinar tareas de documentos (verbos) en flujos de trabajo *ad hoc* y guardarlos como una plantilla, a la que también puede hacerse referencia como un grupo de verbos. En un ejemplo, si un administrador tiene que preparar dispositivas para una reunión de la junta directiva, puede empezar un flujo de trabajo de una "junta directiva" que incluya varias tareas de documentos y los individuos responsables. Un empleado puede tener una tarea de comentar en el paquete de diapositivas, otro realiza la tarea de revisar y aprobar el material, y el administrador realiza la tarea de firmar el documento para los auditores después de que se hayan completado las primeras dos tareas.

[0129] En modos de realización, el sistema puede establecer una colaboración en el documento y "trabajo" basado en el objetivo, incluyendo una pluralidad de canales (por ejemplo, un soporte nativo para Android, iPhone y similares; complementos para las aplicaciones de Microsoft Office, integración del conector de SharePoint; un cliente Mac [como la sincronización de un fichero/carpeta]), características (sincronización de carpetas y ficheros de escritorio para Mac; intercambio de ficheros con objetivo, como para la gestión de tareas y asignación de trabajo basado en documentos; creación de calendarios; finalización de tareas en el documento; anotación y edición colaborativa; colaboración y publicación desde aplicaciones, como el registro/verificación), para el trabajo con objetivo empresarial (por ejemplo, elementos de trabajo como enviar para la revisión y aprobación, mandar para hacer comentarios y anotaciones, pedir la edición de un documento, mandarlo para firmarlo electrónicamente, pedir el formulario de finalización), administración (por ejemplo, administración masiva de usuarios mediante un directorio activo, *branding* y personalización de la interfaz de usuario, planificación y creación de informes), seguridad (por ejemplo, registro de dispositivos, filtros para la prevención de la pérdida de datos, como recordatorios a los usuarios cuando comparten archivos de manera arriesgada; borrado del dispositivo remoto), y similares.

[0130] En modos de realización, el sistema puede establecer una integración empresarial y una administración del proceso empresarial, incluyendo una pluralidad de canales (por ejemplo una API de integración publicada, integración de aplicaciones de terceros, Outlook para Mac), características (por ejemplo, creación de plantilla de trabajo, espacios de colaboración en equipo, gestión de proyectos y avances, edición del documento en el navegador), para trabajos con objetivo empresarial (por ejemplo, personalización de los elementos de trabajo, como combinar tareas de documentos para crear procesos empresariales ligeros *ad hoc*), administración (por ejemplo, procesos empresariales escritos por usuarios y administradores), seguridad (por ejemplo, prevención de pérdida de datos, como bloqueando las acciones inseguras; integración del gestor de información de seguridad (SIM) y del gestor de eventos de seguridad (SEM); llaves de cifrado administradas por clientes; integración del sistema de gobernanza, gestión de riesgos, y cumplimiento (GRC)), y similares. Por ejemplo, las características expuestas (por ejemplo, un recurso para dejar de compartir para retirar documentos tal como se ha descrito en el presente documento) puede integrarse en herramientas diarias, como en *software* de comunicaciones (por ejemplo, Microsoft Outlook, Gmail), navegadores (por ejemplo, Windows Explorer, Firefox, Safari), aplicaciones de planificación de recursos empresariales (ERP), sistemas jurídicos, sistemas de colaboración, y similares, y para hacerlo fácilmente disponible y fácil de usar. Todos estos sistemas tienen la necesidad de distribuir documentos fuera del cortafuegos de la empresa a usuarios que no se registren en estos sistemas diariamente, e integrando estas capacidades se permite que los usuarios compartan, verifiquen, para el cumplimiento, y similares para documentos dentro de las aplicaciones de usuarios. En un ejemplo, supongamos que el personal de ventas está haciendo un presupuesto para un cliente en una aplicación de terceros, como por ejemplo Salesforce.com. Normalmente, los usuarios tendrían la habilidad de enviar el presupuesto directamente por correo electrónico, o descargar el documento y mandarlo por correo electrónico, donde no haya ninguna revisión o cumplimiento dentro de la aplicación de terceros para estos presupuestos. Con el uso de una capacidad integrada, el documento se enviaría directamente desde la aplicación de terceros con las capacidades de cumplimiento y revisión del intercambio seguro del sistema, la habilidad de retirar (dejar de compartir) documentos, y estaría disponible desde dentro de la aplicación de terceros. El servicio integrado puede tener los componentes estándar para hacer que este servicio sea posible, como autentificación mediante el inicio de sesión único, visualizador de ficheros, definición de políticas, verificaciones, aprovisionamiento del dispositivo, cumplimiento y perfiles de usuario, y similares, donde estos se construirían como un servicio y se integrarían directamente en las aplicaciones empresariales estándar. Las reglas también pueden implementarse en el sistema integrado, como con una gama de seguridad (por ejemplo, que va desde público hasta de máxima

seguridad), protección de captura de pantalla y de visualización, control del dispositivo, verificaciones obligatorias, y similares.

[0131] En modos de realización, puede proporcionarse un recurso de gestión de preguntas y respuestas 262, donde un grupo colaborativo de usuarios puede intercambiar preguntas y respuestas, como en un proyecto, y donde al menos un usuario puede gestionar el intercambio a través del recurso de gestión de preguntas y respuestas. Por ejemplo, los usuarios pueden ser compradores y vendedores en una transacción, donde los compradores hacen preguntas y los vendedores responden preguntas. En otro ejemplo, los usuarios pueden ser clientes y representantes expertos de un producto, servicio, operación, y similares, donde los clientes hacen preguntas y los representantes expertos las responden. Mediante el recurso de gestión de preguntas y respuestas, el al menos un usuario puede gestionar entonces el intercambio (como identificándose como un coordinador de preguntas y respuestas). De forma alternativa, cada usuario del intercambio puede utilizar el recurso de gestión de preguntas y respuestas para gestionar el intercambio, creando por consiguiente un entorno de preguntas y respuestas dinámico y colaborativo. Las características y funciones de gestión del recurso de gestión de preguntas y respuestas puede incluir la habilidad de localizar intercambios de preguntas y respuestas, archivar el historial de un intercambio y resolución de preguntas y respuestas, proporcionar el recurso para importar grandes cantidades de preguntas al intercambio, quitar una pregunta del intercambio una vez que ha sido respondida, emparejar preguntas para responderlas a un individuo o grupo de individuos basándose en unos criterios de metadatos extraídos de la pregunta, y similares. A un intercambio de preguntas y respuestas se le puede proporcionar un estado de la pregunta, un estado de delegación, y un indicador de urgencia, y similares, y marcarse tal como se propone, nueva, en proceso, cerrada, preguntas frecuentes, y similares. Las preguntas y respuestas pueden clasificarse, buscarse, organizarse, y similares basándose en un criterio, como por fecha de emisión, estado, categoría, identificador de la pregunta, palabra clave, prioridad, y similares. Un usuario o coordinador puede asignar uno o más criterios a una pregunta, como un nivel de prioridad (por ejemplo, alta, media, baja), lo cual puede ayudar a los expertos a prestar más atención a los asuntos más importantes.

[0132] En un ejemplo, supongamos que un grupo de individuos que participen en una transacción de adquisición, donde haya compradores y vendedores, donde haya un número de compradores y vendedores en cada lado de la posible transacción, y donde los compradores y vendedores tengan distintos papeles y experiencia en relación con la adquisición. Un comprador puede hacer una pregunta a los vendedores. Mediante el recurso de gestión de preguntas y respuestas, la pregunta puede presentarse a los vendedores, donde un vendedor examina la pregunta, y después del intercambio, la pregunta se resuelve. El recurso de gestión de preguntas y respuestas puede monitorizar el intercambio, archivar el intercambio, quitar la pregunta del debate, retirar la pregunta de una fila de preguntas pendientes que se presentaron a los compradores y/o vendedores (como mediante una interfaz de panel), y similares. Además, la pregunta puede emparejarse a un vendedor o comprador en particular para responderla y solucionarla, como basándose en unos criterios de experiencia de usuario asociados al usuario (por ejemplo, el usuario se identifica como "legal", "financiero", "técnico", etc. El emparejamiento también puede determinarse mediante un recurso de gestión de preguntas y respuestas que utilice características o metadatos asociados con la pregunta para emparejar la pregunta al individuo más adecuado para responder a la pregunta. Por ejemplo, la pregunta puede contener una palabra, serie, frase, etc., que coincida con los criterios de una pregunta financiera, y de este modo la pregunta se destina a usuarios al otro lado del intercambio que representan las finanzas. En modos de realización, una vez que se resuelve el intercambio de preguntas y respuestas, el recurso de gestión de preguntas y respuestas puede marcar la pregunta como resuelta, quitar la pregunta del intercambio, archivar el intercambio, y similares.

[0133] En modos de realización, un usuario puede importar grandes cantidades de preguntas y/o de respuestas al intercambio mediante el recurso de gestión de preguntas y respuestas. Por ejemplo, un comprador y/o un vendedor de un intercambio puede tener un conjunto de preguntas frecuentes y/o respuestas que sean relevantes para el intercambio, e importarlas al intercambio. En un ejemplo, un comprador puede tener un conjunto estándar de preguntas para un vendedor, como dónde se ha desarrollado el conjunto estándar de preguntas a lo largo del tiempo. Para facilitar esta importación, el recurso de gestión de preguntas y respuestas puede aceptar la importación en masa en una pluralidad de formatos y desde una pluralidad de aplicaciones de ordenador (por ejemplo, importadas al sistema desde un libro de Microsoft Excel).

[0134] En modos de realización, la entrada de un usuario a un intercambio puede ser un acceso autentificado, un acceso sin autentificación, un acceso semiautentificado, y similares, tal como se ha descrito en el presente documento. Por ejemplo, la gestión de un intercambio puede requerir que el usuario se autentifique como teniendo los privilegios para gestionar el intercambio, para visualizar el intercambio, y similares, pero un usuario no autorizado puede ser capaz de introducir una pregunta en el intercambio, y recibir una respuesta de dentro del grupo del intercambio, pero no tener acceso al contenido de dentro del intercambio que requiera autentificación. En modos de realización, una pregunta y/o una respuesta de un usuario sin autentificación puede mostrar una indicación de ello a otros usuarios del intercambio.

[0135] En modos de realización, la pregunta y/o respuesta en un intercambio puede incluir enlaces a información adicional en relación con la pregunta y/o con la respuesta. Por ejemplo, la pregunta puede pedir datos, y el usuario que responde a la pregunta puede proporcionar un enlace para dirigir al usuario a la ubicación de los datos.

[0136] En modos de realización, el recurso de gestión de preguntas y respuestas puede proporcionar la habilidad de retractarse, corregir o redactar preguntas y/o respuestas como parte del intercambio. Por ejemplo, un usuario puede proporcionar una respuesta, pero luego resulta que es incorrecta. En este ejemplo, la respuesta puede retractarse o corregirse de manera opcional. En modos de realización, los usuarios en el intercambio pueden ser informados cuando se ejecute una retracción, corrección o redacción.

[0137] En modos de realización, el recurso de gestión de preguntas y respuestas puede proporcionarse a través de una interfaz de panel de usuario para gestionar el entorno de preguntas y respuestas, como para aumentar la usabilidad del cliente, proporcionar operaciones (por ejemplo, delegar, cerrar, retirar, responder, cambiar la prioridad, etc., en relación con un intercambio de preguntas y respuestas), establecer un recurso para importar y exportar contenido asociado con un intercambio de preguntas y respuestas, gestionar la prioridad (por ejemplo, incluyendo gestionar, votar, cuestionar, etc., la prioridad de una pregunta), proporcionar recursos de filtrado para preguntas y respuestas, la habilidad de volver a abrir una pregunta cerrada (por ejemplo, para cambiar la respuesta, para volver a abrir la discusión, para solicitar respuestas adicionales), alertas para cambios en preguntas y/o respuestas, la habilidad de que un respondedor guarde un borrador de la respuesta antes de publicarla, y similares.

[0138] En modos de realización, puede proporcionarse un único recurso de inicio de sesión único 264, donde se les puede proporcionar a los usuarios u organizaciones que utilicen el sistema un canal de acceso privado a un intercambio, como mediante un inicio de sesión único al sistema con acceso protegido. Un Canal puede proporcionar una manera para implementar una parte privada en el sistema, como mediante un portal que permita que los usuarios vean solo aquellos intercambios que permita el Canal. Por ejemplo, un Canal puede ser una lista de marcas permisibles combinada con un Proveedor de Identidad ("IdP"). Cuando un usuario se autentificación por este IdP, puede considerarse que ese usuario está en el Canal asociado, y su visualización de datos permitidos por el IdP puede restringirse por la del Canal. En este ejemplo un Canal es, esencialmente, un modelo virtual privado del sistema. En los despliegues de clientes, donde la interfaz de usuario del sistema está alojada por terceros, este sistema puede asegurar mejor que no haya fugas de datos entre dominios de intercambios permitidos por separado. Los Canales privados pueden asegurar que la información de un cliente solo pueden verla sus usuarios con inicio de sesión único. Los Canales privados pueden proporcionar un medio para asegurar que los usuarios no ven información de otras organizaciones mientras utilizan el inicio de sesión único, incluso si tienen permiso para ver los intercambios de otras organizaciones. En un ejemplo, si un usuario está registrado en el sistema utilizando una conexión de inicio de sesión único de la Empresa A, verán los intercambios y los datos solo de la Empresa A, incluso aunque el usuario pueda tener acceso a intercambios de otras organizaciones mediante otros privilegios de acceso. Este recurso puede respaldar a organizaciones que quieran autentificar usuarios externos a través del inicio de sesión único. Por ejemplo, los clientes de Ciencias de la Vida e Inversiones Alternativas que mantengan su propio portal pueden querer que su comunidad de usuarios se autentifique utilizando un inicio de sesión único. En otro ejemplo, un doctor de Johns Hopkings puede estar haciendo ensayos clínicos con dos compañías farmacéuticas diferentes, y si el doctor accede mediante el canal de la página web de la Empresa A, entonces solo ve la información de la Empresa A. Esta funcionalidad es especialmente útil dondequiera que un cliente quiera tener un portal privado en un escenario con muchos inquilinos.

[0139] En modos de realización, el sistema puede establecer un aprovisionamiento en demanda, automático y basado en el contexto. Por ejemplo, un cliente puede crear una página web donde un usuario pueda introducir credenciales. Cuando creen una cuenta (por ejemplo, un nuevo empleado), el sistema puede disponer de manera automática un intercambio para ellos, donde el empleado inicia sesión por su estructura. El inicio de sesión único puede verificar que la persona tiene permiso, y automáticamente configura una cuenta para ese usuario, donde se trataría a todo el mundo de esa organización como si estuviesen registrados en la organización. Esto es, una vez que han iniciado sesión, el usuario puede moverse con el canal y acceder a la información sin volver a iniciar sesión, como basándose en el contexto proporcionado mediante el usuario, la organización, y similares. En modos de realización, el contexto puede proporcionarse etiquetando al usuario para permitir futuros inicios de sesión. Por ejemplo, una empresa puede querer proporcionar a un bufete de abogados el acceso a determinados datos en un intercambio, y mediante un aprovisionamiento basado en el contexto, el bufete de abogados puede estar etiquetado no solo para permitirles que vuelvan a acceder sin iniciar sesión, sino que solo se les permitirá ver el contenido de la organización que se proporcione a través del canal privado. Por consiguiente, el acceso de un usuario a determinada información está limitado al contexto de dónde inicien sesión.

[0140] En consecuencia, puede proporcionarse un recurso de intercambio de documentos sin autentificación 268, donde los gestores de intercambio pueden ser capaces de marcar participantes del intercambio específicos que tienen permitido saltarse el proceso de inicio de sesión (por ejemplo, saltándose pasos que requieren que proporcionen su nombre de usuario y contraseña), cuando descarguen los documentos, como desde alertas. Por ejemplo, cuando un usuario permitido intenta acceder a un documento mediante una URL de documento especial en una alerta de correo electrónico, el documento puede empezar a descargarse, sin pedirle al usuario ninguna autentificación adicional. La URL de documento especial puede permitir este acceso para cada documento para el usuario del intercambio específico durante un periodo de tiempo, como una semana, un mes,

y similares, desde el momento en el que se envía la alerta. El sistema puede identificar a los usuarios a los que se les mandó la alerta, donde los informes de acceso pueden indicar que el usuario particular ha visto el documento, incluso aunque no se requiera una autentificación. Cada participante del intercambio que esté marcado para permitir este acceso puede tener una indicación visual en la vista de lista de usuario, para puntualizar que tienen un tipo diferente de derechos de acceso. Este tipo de acceso puede ser específico para un intercambio determinado, y puede no ser necesariamente transferible entre intercambios. Esta funcionalidad puede ser especialmente útil para clientes que están distribuyendo contenido a individuos y organizaciones que acceden a servicios con muy poca frecuencia, donde estos individuos experimentan constantemente retos al iniciar sesión y utilizar el servicio a causa de la falta de uso regular, y normalmente experimentan un olvido del nombre de usuario y la contraseña. Por ejemplo, un cliente inversor solo puede enviar contenido de manera trimestral, y quiere permitir a un subconjunto de inversores que tengan acceso a sus extractos sin autentificación. En lugar de mandar documentos a estos inversores por correo electrónico, el sistema podría permitir a los administradores del fondo que manden extractos mediante este servicio sin autentificación, satisfaciendo por consiguiente la necesidad de los inversores de memorizar un nombre de usuario y una contraseña. En modos de realización, se le puede proporcionar al usuario un enlace para acceder al contenido, donde después de proporcionar de manera opcional una confirmación de quién es el usuario (por ejemplo, una dirección de correo electrónico), el documento puede descargarse. El uso de este sistema puede permitir que los usuarios objetivo reciban acceso especial al documento (por ejemplo, a través de alertas, enlaces de correo electrónico, y similares) y monitorizar su acceso al documento (por ejemplo, para una revisión jurídica y de seguridad), y similares. Los usuarios que no necesitan iniciar sesión pueden identificarse con un icono o identificador especial, como cuando los administradores ven una lista de usuario. Los informes de acceso al documento también pueden actualizarse cuando se activa el enlace (por ejemplo, cuando se hace clic), y el acceso atribuido al usuario que tenía permiso para utilizar el documento. Como el acceso al contenido puede habilitarse y monitorizarse mediante un enlace URL, entonces el sistema puede limitar la distribución al quitarle el permiso a una URL (lo que dejaría la URL inactiva). Como el usuario no conoce la URL, no puede tener acceso si la URL está inactiva.

[0141] El uso de acceso sin autentificación al contenido puede tener muchas aplicaciones. Por ejemplo, una organización puede querer proporcionar información disponible públicamente, donde el sistema de acceso sin autentificación proporciona a los usuarios públicos acceso al documento sin "permisos", pero permite a la organización que proporcione la información con un medio para monitorizar el acceso a la información. Por ejemplo, una organización puede querer hacer público un "avance", como en relación con una oportunidad de inversión. La organización ahora es capaz de monitorizar el acceso a la información.

[0142] En modos de realización, el uso de acceso sin autentificación puede permitir que una organización envíe el acceso a la información sin ingresar datos previamente en una lista de contactos con usuarios con acceso seguro. La organización solo puede necesitar tener una lista de direcciones de correo electrónico a los que mandar el enlace URL, sin la necesidad de credenciales por parte del usuario.

[0143] En modos de realización, el sistema puede utilizar un proceso de semiautentificación, como que requiera que el usuario proporcione un número de identificación personal (PIN), como el determinado por el usuario o por la organización que proporciona el enlace URL.

[0144] En modos de realización, puede proporcionarse un recurso de sincronización 270 para la sincronización de contenido basado en metadatos, donde el sistema pueda utilizarse para proporcionar la sincronización e intercambio de contenido, como entre los varios dispositivos informáticos de un único individuo, un grupo de individuos, una empresa, y similares, donde la sincronización puede ser selectiva, como que el usuario elija qué ficheros se sincronizan, qué dispositivos informáticos se sincronizan, qué individuos pueden compartir mediante la sincronización, y similares. El usuario también puede establecer reglas por las que se selecciona la sincronización, como reglas asociadas con la ubicación del dispositivo informático (por ejemplo, no sincronizarse cuando el dispositivo informático no está en una red segura, en un país extranjero, y similares), un número de versión del documento (por ejemplo, sincronizando la revisión más reciente de un documento), y similares, donde la regla se basa en los metadatos sincronizados con el documento. En modos de realización, los documentos pueden geoetiquetarse, y mediante ese geoetiquetado el proceso de sincronización puede determinar si sincronizar o no. Un usuario puede no ser capaz de identificar una carpeta determinada para sincronizarla con un grupo de individuos, sino también sincronizar solo la última versión de un documento De este modo, un usuario añadido al grupo de sincronización puede no tener todas las versiones antiguas de un documento sincronizado. Esta capacidad puede ayudar al usuario a tomar decisiones que puedan reducir la carga de trabajo durante la sincronización y ciclos libres para sincronizar contenido más crítico.

[0145] En modos de realización, puede proporcionarse un recurso de actividad de intercambio de ficheros 272 para empaquetar y archivar el historial del intercambio del fichero entre individuos en un intercambio. El intercambio de ficheros archivado puede almacenarse en un proceso similar como el de los correos electrónicos, y situarse en un archivo para futuras búsquedas (por ejemplo, para litigios o para solicitudes de descubrimiento electrónico). Con el archivo del intercambio de ficheros almacenado en un formato similar que el de los correos electrónicos, la búsqueda de intercambios y la búsqueda de correos electrónicos pueden llevarse a cabo juntas, donde el correo electrónico y los archivos de intercambios de ficheros parecen ser, o de verdad son, un único

archivo consultable. Este archivo también puede compartirse con otros individuos en el intercambio, puede sincronizarse con otros dispositivos activos con individuos en un intercambio, y similares. El archivo de la actividad de intercambio puede ser a nivel de intercambio, a nivel de usuario, a nivel de documento, y similares. Por ejemplo, un archivo a nivel de documento puede incluir el propio documento más todo el historial del documento (por ejemplo, el historial de visualización, quién editó el documento, cuándo se firmó el documento, y similares), de manera que cuando se encuentra este nuevo historial archivado, como en una búsqueda, puede recuperarse describiendo su contenido y su historial.

[0146] En modos de realización, puede proporcionarse un recurso de gestión de colaboraciones 274 donde en el transcurso de un intercambio colaborativo, los usuarios pueden tener documentos intercambiados y comunicaciones, contenido compartido, dispositivos sincronizados, y similares, donde puede proporcionarse el recurso de gestión de colaboraciones para gestionar el intercambio de contenido y la retención, intercambio y persistencia de contenido compartido. Por ejemplo, el usuario puede querer quitar cualquier rastro del intercambio una vez que este se ha terminado. El usuario puede querer controlar la cantidad de tiempo que un destinatario puede tener o ver un documento tras su entrega. El usuario puede querer controlar la habilidad de imprimir, enviar, ver, el documento en varias plataformas, en varios dispositivos, con determinados individuos y/u organizaciones, y similares. El recurso de gestión de colaboración puede incluir una política de retención de documentos que determine las reglas según las cuales se retienen los documentos. Por ejemplo, los documentos pueden etiquetarse con una etiqueta de retención de documento que borra el documento en un número determinado de días, hasta un evento de avance (por ejemplo, cuando se firma un documento, después de que se haya visualizado), y similares. En un ejemplo, un documento que ofrece un servicio o producto puede etiquetarse de manera que, si el destinatario de la oferta la rechaza, el documento se borra. De forma alternativa, la oferta del documento puede ser mediante un enlace, y el enlace se desactiva después de que el destinatario rechace la oferta. El documento puede etiquetarse con un permiso basado en la duración, como que el documento se borrará, o el enlace se desactivará, cuando se cierre al final de un periodo de tiempo. El documento puede etiquetarse para una visualización temporal, como que solo sea visible durante poco tiempo cuando el documento se visualiza en un dispositivo móvil. Por ejemplo, un destinatario puede tener diferentes permisos de visualización y retención para el mismo documento dependiendo del dispositivo en el que están visualizando el documento, donde pueden tener permiso para ver el documento durante una semana en un ordenador, pero solo durante unos minutos en un teléfono móvil inteligente. De forma alternativa, puede ser un enlace al documento el que tiene un tiempo limitado para su activación. Esta forma de intercambio no persistente puede permitir al usuario compartir documentos de forma urgente, sin la preocupación de que el documento se retenga más allá del tiempo deseado. Por ejemplo, un banquero puede distribuir una investigación de perspectivas. Pero la investigación es propiedad del banco, y el banquero necesita controlar el acceso a la investigación. Una opción puede ser que el banquero distribuya la investigación mediante un enlace URL, donde la URL se etiqueta para controlar el acceso mediante la política de retención. En modos de realización, la política de retención puede imponer una retención en una distribución por grupos, proporcionando diferentes privilegios de retención a diferentes destinatarios, y monitorizar las acciones de visualización y ejecutar limitaciones de retención de la visualización para los usuarios de la distribución.

[0147] En modos de realización, un recurso de geoetiquetado 278 puede proporcionarse, donde un documento puede geoetiquetarse como para indicar dónde se ha creado un documento, desde dónde se ha enviado, recibido, editado, visualizado, y similares. Geoetiquetar un documento puede incluir información que se adjunta y viaja con el documento a través de la distribución, intercambio, modificación, y archivo. La información del geoetiquetado puede incluir información geográfica de la ubicación (por ejemplo, ciudad, estado, territorio, país, región, código postal, latitud y longitud), una ubicación de la empresa (por ejemplo, nombre de la empresa, dirección de la empresa, unidad de negocio), una ubicación de la red (por ejemplo, una red segura, una red de empresa, una red pública, una red inalámbrica), una ubicación del almacenamiento (por ejemplo, ubicación del archivo, almacenamiento de unidad miniatura, DVD), y similares. En un ejemplo, un usuario de la Empresa A puede crear un documento en San Francisco, donde la información de la ubicación puede incluir el nombre de la empresa y la ciudad, además de otra información como la hora, la fecha y el nombre del usuario. Entonces, el documento puede distribuirse a otros dos usuarios en dos países diferentes que trabajen con dos empresas diferentes, donde esta información se adjunta a un historial geográfico del documento (por ejemplo, almacenado en metadatos junto con el documento). Puede adjuntarse información adicional al documento según se edita, redistribuye, y finalmente se archiva. Puede buscarse la información de geolocalización, como, por ejemplo, durante su vida como documento activo o mientras se almacene en el archivo. El geoetiquetado de los datos puede habilitar mejor la detección del historial del documento (y el contenido del mismo), como para búsquedas jurídicas o de descubrimientos electrónicos.

[0148] En modos de realización, puede proporcionarse un recurso de optimización de ficheros de entrada, donde las reglas y/o información sobre las acciones del documento aumentan la eficiencia con las que se ejecutan las tareas, en especial las tareas grandes. Por ejemplo, cuando se intente añadir una carpeta con un nombre específico, puede comprobar y abrir la etiqueta de las carpetas, comprobar si una etiqueta de la carpeta ya está abierta, y si la carpeta abierta actual es diferente a la carpeta nueva, entonces cerrar la carpeta existente y abrir la nueva etiqueta de la carpeta.

[0149] En modos de realización, puede proporcionarse un recurso de archivo 280, como, por ejemplo, donde exista la necesidad de entregar archivos en el mismo día o al día siguiente, como en una manera rápida y eficiente de crear archivos HTML (*snapshots*) de intercambios sin dejar huella en él. En modos de realización, un fichero de archivo API, creado mediante llamadas de API, puede permitir una automatización del sistema que disminuya el tiempo de envío además de mejorar otras consideraciones clave para archivos, incluyendo fiabilidad, eficiencia, tiempo de producción, escalabilidad, predictibilidad, simplicidad del proceso, apoyo, necesidades del mercado, cumplimiento de verificaciones, cumplimiento de las normas de seguridad, costes, etc. La herramienta también podría incorporar lógica que permita la división de un único intercambio en múltiples volúmenes y la división a nivel de carpeta o a nivel de documento. Además de desplegar archivos HTML, la herramienta puede modificarse desde dentro del fichero de configuración solo para descargar metadatos. Hacerlo puede permitir que la herramienta proporcione informes completos de metadatos similares a los informes de bases de datos especializadas en carpetas y documentos.

[0150] Las características del recurso de archivo pueden incluir la creación de cartas de confirmación automáticas (por ejemplo, que incluyan la firma electrónica), estructuras de nombres y de puntos de vista configurables (por ejemplo, por número de identificación de usuario, dirección de correo electrónico, grupo de intercambio, grupo compuesto), inmovilización de intercambios automatizada para crear grupos no permitidos, archivarlos desde un intercambio inmovilizado para comprobar el papel de un usuario antes de la inmovilización y la suplantación contra viejos perfiles (inactivos), creación de cartas de inmovilización, y similares. La Fig. 11 ilustra un ejemplo de proceso de archivo, incluyendo la autentificación y suplantación de usuarios 1114, recogida de metadatos 1108 (por ejemplo, incluyendo informes, como informes de permiso, informes de carpetas, informes de documentos, informes de puntos de vista, y similares), descarga y procesamiento de datos 1110, y creación de un archivo 1112.

[0151] El diseño del recurso de archivo puede incluir una rutina en dos partes que primero suplantará rápidamente y de manera eficiente un usuario y descargará todos los documentos y carpetas a las que tengan visibilidad. El segundo camino puede ser crear un fichero HTML que sea una representación del intercambio en la que el usuario final pueda navegar a fondo para llegar a los documentos. La funcionalidad esencial del recurso de archivo puede incluir la descarga del alcance de usuario para un usuario seleccionado, la habilidad de suplantar a cualquier usuario de un intercambio si se inicia sesión con un rol de administrador o un administrador oculto, una interacción mínima del usuario, procedimientos de descarga automática (que pueden ocurrir de manera secuencial), la habilidad de dividir volúmenes de archivo basados en un tamaño definido especificado, procesar la mensajería relacionada con un proceso de división, soporte de codificación UTF-8 de nombres de carpetas y documentos, modo de depuración para un inicio de sesión avanzado y para resolver problemas, verificar ficheros para una actividad de monitorización (por ejemplo, inicios de sesión de usuario satisfactorios, intercambio de números de identificación desde donde descargar, ficheros descargados, advertencias, errores de sistema), habilidad de dividir un intercambio en un n volúmenes basándose en el tamaño de los volúmenes, dividirlo a un nivel determinado (por ejemplo, a nivel de documento, nivel de carpeta), descarga de preguntas y documentos adjuntos, habilidad de inmovilizar un intercambio en varios estados (por ejemplo, inmovilización total [la fase del intercambio se suspende, y todos los usuarios que no sean revisores se cambian a revisores], inmovilización parcial [la fase del intercambio se pone en preparación, y todos los usuarios que no sean previsualizadores o revisores se cambian a previsualizadores]), inmovilización activa [la fase del intercambio se pone en Abierto, y luego todos los usuarios que no sean previsualizadores o revisores se cambian a previsualizadores]), habilidad de desbloquear un intercambio y revertirlo a un estado previo (por ejemplo, en relación con el rol de usuario y la fase de intercambio), y similares.

[0152] La estructura funcional del recurso de archivo puede incluir un modelo, una vista, un controlador, y similares. Por ejemplo, el rol del modelo puede ser hacer llamadas a los controladores, que son las clases que mantienen todos los controladores. El modelo también puede proporcionar una respuesta específica que se analiza en el objeto de modelo, que puede mantener la respuesta de la "capa de controlador" lejos de la vista y del "controlador local". Dentro de la visualización, el usuario puede ser capaz de introducir sus credenciales de inicio de sesión (esto también puede ser donde los ficheros (por ejemplo, ficheros de Excel) se crean y se leen. Puede haber una pantalla de estado que se actualiza con los eventos. En la visualización, también puede ser que el usuario sea capaz de ver si el proceso se ha completado con algún error. Puede haber múltiples controladores, como uno para encargarse de eventos locales y un segundo dentro de la capa combinada que crea una solicitud web. La aplicación local puede coger las entradas de usuario y encargarse de los eventos de botón, llamar a los modelos de una capa combinada, contener la lógica de negocios para procesar la respuesta del modelo de capa combinada, y similares. La capa combinada puede ser capaz de ejecutar comandos, y cuando se da una respuesta, puede analizarse en los objetos de respuesta de modelos.

[0153] El proceso de archivo puede estar diseñado para ser ejecutado por un individuo capacitada a diferencia de un usuario en un intercambio. El proceso puede utilizar una combinación de llamadas de API públicas y privadas. Las acciones relacionadas con esta herramienta pueden incluir iniciar y cerrar sesión, obtener carpetas, obtener documentos, descargar documentos, descargar datos adjuntos de preguntas y respuestas, obtener todas las categorías, obtener todas las preguntas utilizando carpetas inteligentes, obtener todas las configuraciones del espacio de trabajo, actualizar la fase del espacio de trabajo, obtener un informe del alcance del usuario, crear un

grupo, obtener un grupo, obtener todos los detalles y grupos del espacio de trabajo, obtener todos los detalles y usuarios del espacio de trabajo, añadir un usuario existente al grupo, y similares.

[0154] Aunque la invención se ha descrito en relación con determinados modos de realización preferidos, otros modos de realización se entenderán por un experto en la materia y se incluyen en el presente documento.

[0155] Los métodos y sistemas descritos en el presente documento pueden utilizarse en parte o por completo mediante una máquina que ejecute *software* del equipo, códigos de programa, y/o instrucciones en un procesador. La presente invención puede implementarse como un método en el equipo, como un sistema o aparato como parte de o en relación con el equipo, o como un producto de programa informático incorporado en un soporte legible por ordenador que se ejecute en uno o más de los equipos. El procesador puede formar parte de un servidor, cliente, infraestructura de red, plataforma informática móvil, plataforma informática estacionaria, u otra plataforma informática. Un procesador puede ser cualquier tipo de dispositivo computacional o de procesamiento capaz de ejecutar instrucciones de programa, códigos, instrucciones binarias y similares. El procesador puede ser o incluir un procesador de señales, un procesador digital, un procesador integrado, un microprocesador, o cualquier variante como un coprocesador (coprocesador matemático, coprocesador gráfico, coprocesador de comunicación, y similares) y similares que pueden facilitar directa o indirectamente la ejecución de un código de programa o unas instrucciones de programa almacenadas en el mismo. Además, el procesador puede permitir la ejecución de múltiples programas, hilos y códigos. Los hilos pueden ejecutarse simultáneamente para mejorar el rendimiento del procesador y para facilitar operaciones simultáneas de la aplicación. A modo de implementación, los métodos, los códigos de programa, las instrucciones de programa y similares descritos en el presente documento pueden implementarse en uno o más hilos. El hilo puede generar otros hilos que pueden tener asignadas prioridades asociadas con ellos; el procesador puede ejecutar estos hilos basándose en la prioridad o cualquier otra orden basándose en instrucciones proporcionadas en el código del programa. El procesador puede incluir memoria que almacene métodos, códigos, instrucciones y programas tal como se ha descrito en el presente documento y en otra parte. El procesador puede acceder a un medio de almacenamiento mediante una interfaz que puede almacenar métodos, códigos, e instrucciones tal como se ha descrito en el presente documento y en otra parte. El medio de almacenamiento asociado con el procesador para métodos de almacenamiento, programas, códigos, las instrucciones de programa u otro tipo de instrucciones capaces de ser ejecutadas por el dispositivo informático o de procesamiento puede incluir, pero sin carácter limitativo uno o más de entre un CD-ROM, DVD, memoria, disco duro, memoria USB, RAM, ROM, caché, y similares.

[0156] Un procesador puede incluir uno o más núcleos que puedan aumentar la velocidad y rendimiento de un multiprocesador. En modos de realización, el procesador puede ser un procesador de doble núcleo, procesadores de cuatro núcleos, otros multiprocesadores a nivel de chip, y similares que combinen dos o más núcleos independientes (llamados pastillas).

[0157] Los métodos y sistemas descritos en el presente documento pueden utilizarse en parte o por completo mediante un equipo que ejecute *software* del equipo en un servidor, cliente, cortafuegos, puerta de enlace, concentrador, enrutador, u otro *hardware* de equipo y/o de red. El programa de *software* puede estar asociado con un servidor que puede incluir un servidor de ficheros, un servidor de impresión, un servidor de internet, un servidor de intranet, y otras variantes, como un servidor secundario, un servidor principal, un servidor distribuido, y similares. El servidor puede incluir una o más memorias, procesadores, soportes legibles por ordenador, medios de almacenamiento, puertos (físicos y virtuales), dispositivos de comunicación, e interfaces capaces de acceder a otros servidores, clientes, equipos, y dispositivos mediante un medio por cable o inalámbrico, y similares. El servidor puede ejecutar métodos, programas o códigos tal como se ha descrito en el presente documento y en otros sitios. Además, otros dispositivos requeridos para la ejecución de métodos tal como se describen en esta solicitud pueden considerarse como una parte de la infraestructura asociada con el servidor.

[0158] El servidor puede proporcionar una interfaz a otros dispositivos incluyendo, pero sin carácter limitativo, clientes, otros servidores, impresoras, servidores de bases de datos, servidores de impresión, servidores de fichero, servidores de comunicación, servidores distribuidos, y similares. De forma adicional, este acoplamiento y/o conexión puede facilitar la ejecución remota de un programa a través de la red. Las redes de algunos o todos estos dispositivos pueden facilitar el procesamiento paralelo de un programa o método, en una o más ubicaciones sin desviarse del alcance de la invención. Además, cualquiera de los dispositivos adjuntos al servidor mediante una interfaz puede incluir al menos un medio de almacenamiento capaz de almacenar métodos, programas, códigos, y/o instrucciones. Un repositorio central puede proporcionar instrucciones de programas a ejecutar en diferentes dispositivos. En esta implementación, el repositorio remoto puede actuar como un medio de almacenamiento para el código del programa, instrucciones y programas.

[0159] El programa de *software* puede asociarse con un cliente que puede incluir un cliente de fichero, cliente de impresión, cliente de dominio, cliente de internet, cliente de intranet, y otras variantes como cliente secundario, cliente principal, cliente distribuido, y similares. El cliente puede incluir uno o más de entre memorias, procesadores, soportes legibles por ordenador, medios de almacenamiento, puertos (físicos y virtuales), dispositivos de comunicación, e interfaces capaces de acceder a otros clientes, servidores, equipos, y dispositivos mediante un medio por cable o inalámbrico, y similares. El cliente puede ejecutar métodos,

programas o códigos tal como se han descrito en el presente documento y en otros sitios. Además, otros dispositivos requeridos para la ejecución de métodos tal como se describen en esta solicitud pueden considerarse como una parte de la infraestructura asociada con el cliente.

[0160] El cliente puede proporcionar una interfaz a otros dispositivos incluyendo, pero sin carácter limitativo, servidores, otros clientes, impresoras, servidores de bases de datos, servidores de impresión, servidores de fichero, servidores de comunicación, servidores distribuidos, y similares. De forma adicional, este acoplamiento y/o conexión puede facilitar la ejecución remota de un programa a través de la red. Las redes de algunos o todos estos dispositivos pueden facilitar el procesamiento paralelo de un programa o método, en una o más ubicaciones sin desviarse del alcance de la invención. Además, cualquiera de los dispositivos adjuntos al cliente mediante una interfaz puede incluir al menos un medio de almacenamiento capaz de almacenar métodos, programas, aplicaciones, códigos, y/o instrucciones. Un repositorio central puede proporcionar instrucciones de programas a ejecutar en diferentes dispositivos. En esta implementación, el repositorio remoto puede actuar como un medio de almacenamiento para el código del programa, instrucciones y programas.

[0161] Los métodos y sistemas descritos en el presente documento pueden utilizarse en parte o por completo mediante infraestructuras de red. La infraestructura de red puede incluir elementos como dispositivos informáticos, servidores, enrutadores, concentradores, cortafuegos, ordenadores personales, dispositivos de comunicación, dispositivos de enrutación, y otros dispositivos activos y pasivos, recursos y/o componentes tal como se conocen en la técnica. El (los) dispositivo(s) informáticos y/o no informáticos asociado(s) con la infraestructura de la red puede(n) incluir, aparte de otros componentes, un medio de almacenamiento como una memoria USB, un búfer, una pila, una RAM, una ROM, y similares, Los procesos, métodos, códigos de programa, instrucciones descritos en el presente documento y en otros sitios pueden ser ejecutados por uno o más de los elementos infraestructurales de la red.

[0162] Los métodos, códigos de programa e instrucciones descritos en el presente documento pueden implementarse en una red celular que tiene múltiples celdas. La red celular puede o bien ser una red de acceso múltiple por división de frecuencia (FDMA) o una red de acceso múltiple por división de código (CDMA). La red celular puede incluir dispositivos móviles, torres de telefonía, estaciones base, repetidores, antenas, torres, y similares. La red celular puede ser una red GSM, GPRS, 3G, EVDO, en malla, u otros tipos de red.

[0163] Los métodos, códigos de programa, e instrucciones descritos en el presente documento y en otros sitios pueden implementarse en o mediante dispositivos móviles. Los dispositivos móviles pueden incluir dispositivos de navegación, teléfonos móviles, asistentes digitales personales móviles, ordenadores portátiles, ordenadores de bolsillo, ultraportátiles, buscapersonas, libros electrónicos, reproductores de música, y similares. Estos dispositivos pueden incluir, aparte de otros componentes, un medio de almacenamiento como una memoria USB, un búfer, una RAM, una ROM, y uno o más dispositivos informáticos. Los dispositivos informáticos asociados con dispositivos móviles pueden estar habilitados para ejecutar códigos de programas, métodos, e instrucciones almacenadas en los mismos. De forma alternativa, los dispositivos móviles pueden configurarse para ejecutar instrucciones en colaboración con otros dispositivos. Los dispositivos móviles pueden comunicarse con estaciones base interconectadas con servidores y configuradas para ejecutar códigos de programa. Los dispositivos móviles pueden comunicarse en una red P2P, una red de malla, u otras redes de comunicaciones. El código de programa puede almacenarse en el medio de almacenamiento asociado con el servidor y ejecutado por un dispositivo informático integrado en el servidor. La estación base puede incluir un dispositivo informático y un medio de almacenamiento. El dispositivo de almacenamiento puede almacenar códigos de programas e instrucciones ejecutadas por los dispositivos informáticos asociados con la estación base.

[0164] El *software* del equipo, códigos de programa y/o instrucciones pueden almacenarse y/o puede accederse a ellas en medios de lectura electrónica que pueden incluir: componentes informáticos, dispositivos, y medios de grabación que conserven datos digitales utilizados para la informática durante algún intervalo de tiempo; almacenamiento semiconductor conocido como memoria de acceso aleatorio (RAM); almacenamiento masivo normalmente utilizado para un almacenamiento más permanente, como discos ópticos, formas de almacenamiento magnético como discos duros, cintas, tambores, tarjetas y otros tipos; registros, memoria caché, memoria volátil, memoria no volátil; almacenamiento óptico como CD, DVD; medios extraíbles como una memoria *flash* (por ejemplo, *pendrives*), disquetes, cinta magnética, cinta de papel, tarjetas perforadas, discos RAM independientes, unidad Zip, almacenamiento en masa extraíble, fuera de línea, y similares; otras memorias informáticas como memoria dinámica, memoria estática, almacenamiento de lectura/escritura, memorias cambiables, de solo lectura, de acceso aleatorio, de acceso secuencial, de ubicación direccionable, de archivo direccionable, de contenido direccionable, almacenamiento conectado a la red, red de área de almacenamiento, códigos de barras, tinta magnética, y similares.

[0165] Los métodos y sistemas descritos en el presente documento pueden transformar elementos físicos y/o o intangibles desde un estado a otro. Los métodos y sistemas descritos en el presente documento también pueden transformar datos que representen elementos físicos y/o intangibles desde un estado a otro.

[0166] Los elementos descritos y representados en el presente documento, incluyendo en diagramas de flujo y en diagramas de bloques a lo largo de las figuras, implican límites lógicos entre los elementos. No obstante, según las prácticas de ingeniería de *software* o *hardware*, los elementos representados y las funciones de los

mismos pueden implementarse en equipos mediante medios ejecutables por ordenador que presenten un procesador capaz de ejecutar instrucciones de programa almacenados en el mismo como una estructura de *software* monolítico, como recursos de *software* independiente, o como recursos que emplean rutinas externas, códigos, servicios, entre otros, o cualquier combinación de estos, y todas estas implementaciones pueden estar dentro del alcance de la presente exposición. Ejemplos de estos equipos pueden incluir, pero sin carácter limitativo, asistentes digitales personales, ordenadores portátiles, ordenadores personales, teléfonos móviles, otros dispositivos informáticos portátiles, equipo médico, dispositivos de comunicación por cable o inalámbricos, transductores, chips, calculadoras, satélites, tabletas, libros electrónicos, accesorios, dispositivos electrónicos, dispositivos con inteligencia artificial, dispositivos informáticos, equipos de red, servidores, enrutadores, y similares. Asimismo, los elementos representados en el diagrama de flujo y el diagrama de bloque u otro componente lógico pueden implementarse en un equipo capaz de ejecutar instrucciones de programa. Por consiguiente, mientras que los dibujos y descripciones anteriores exponían aspectos funcionales de los sistemas expuestos, ninguna disposición de *software* para implementar estos aspectos funcionales debe inferirse de estas descripciones a menos que se afirme de manera explícita o quede claro de otro modo por el contexto. De forma similar, se apreciará que las varias etapas identificadas y descritas anteriormente pueden variar, y que el orden de etapas puede adaptarse a aplicaciones particulares de las técnicas expuestas en el presente documento. Todas estas variaciones y modificaciones están destinadas a incluirse dentro del alcance de esta exposición. En consecuencia, la representación y/o descripción de un orden para varias etapas no debe entenderse como que necesita un orden particular de ejecución para estas etapas, a menos que lo requiera una aplicación particular, o se afirme de manera explícita o quede claro de otro modo por el contexto.

[0167] Los métodos y/o procesos descritos anteriormente, y las etapas de los mismos, pueden realizarse en *hardware*, *software* o en cualquier combinación de *software* y *hardware* adecuada para una aplicación en particular. El *hardware* puede incluir un ordenador de uso general y/o un dispositivo informático especializado o un dispositivo informático específico o un componente o aspecto particular de un dispositivo informático específico. Los procesos pueden realizarse en uno o más microprocesadores, microcontroladores, microcontroladores integrados, procesadores de señales digitales programables u otros dispositivos programables, así como memorias internas y/o externas. Los procesos también pueden, o en su lugar, estar incorporados en un circuito integrado para aplicaciones específicas, una matriz de puertas programable, un conjunto lógico programable, o cualquier otro dispositivo o combinación de dispositivos que pueda configurarse para procesar señales electrónicas. Se apreciará adicionalmente que uno o más de los procesos puedan realizarse como un código ejecutable informático capaz de ejecutarse en un medio legible por ordenador.

[0168] El código ejecutable por ordenador puede crearse utilizando un lenguaje de programación estructurado, como C, un lenguaje de programación orientado a objetos como C++, o cualquier lenguaje de programación de alto y bajo nivel (incluyendo lenguajes ensambladores, lenguaje de descripción de *hardware*, y tecnologías y lenguajes de programación de bases de datos) que puedan almacenarse, compilarse o interpretarse para ejecutarse en uno o más de los dispositivos anteriores, además de combinaciones heterogéneas de procesadores, arquitecturas de procesadores, o combinaciones de diferente *software* y *hardware*, o cualquier otro equipo capaz de ejecutar instrucciones de programa.

[0169] Por consiguiente, en un aspecto, cada método descrito anteriormente y combinaciones de los mismos pueden incorporarse en un código ejecutable por ordenador que, al ejecutarlo en uno o más dispositivos informáticos, lleva a cabo las etapas del mismo. En otro aspecto, los métodos pueden incorporarse en sistemas que lleven a cabo las etapas de los mismos, y pueden distribuirse a través de dispositivos en un número de maneras, o todas las funcionalidades pueden integrarse en un dispositivo especializado independiente o en otro *hardware*. En otro aspecto, los medios para llevar a cabo las etapas asociadas con los procesos descritos anteriormente pueden incluir cualquier *hardware* y/o *software* descrito anteriormente. Todas estas modificaciones y combinaciones están destinadas a incluirse dentro del alcance de la presente exposición.

[0170] Mientras que la invención se ha expuesto en conexión con los modos de realización preferidos mostrados y descritos en detalle, varias modificaciones y mejoras de la misma se pondrán de manifiesto para aquellos expertos en la materia.

REIVINDICACIONES

1. Un método para gestionar un entorno de intercambio de datos informáticos colaborativo seguro en red, comprendiendo dicho método:

establecer, por un servidor de intercambio seguro hospedado por una entidad empresarial intermedia, un procedimiento de autentificación de datos de inicio de sesión de usuario que permite a uno o más usuarios, mediante al menos un dispositivo informático cliente, acceder al servidor de intercambio seguro, donde el uno o más usuarios es de al menos una segunda entidad empresarial, donde las comunicaciones entre el servidor de intercambio seguro y cada uno del uno o más usuarios es mediante una red de comunicaciones.

almacenar, por el servidor de intercambio seguro, al menos los datos de autentificación de inicio de sesión de un usuario para el al menos un usuario de la segunda entidad empresarial;

recibir un contenido de datos informáticos de al menos un usuario de una tercera entidad empresarial;

recibir de al menos un usuario de la tercera entidad empresarial una indicación de permiso para que el usuario de la segunda entidad empresarial acceda al contenido de datos informáticos mediante un dispositivo informático móvil designado, donde la indicación de permiso comprende una política de retención de contenido;

permitir, por el servidor de intercambio seguro, el acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial en el dispositivo informático móvil designado mediante un recurso de acceso a contenido de intercambio, donde el recurso de acceso a contenido de intercambio está hospedado por la entidad empresarial intermedia; y

conceder, por el servidor de intercambio seguro, acceso al contenido de datos informáticos al usuario de la segunda entidad empresarial en el dispositivo informático móvil designado mediante un recurso de visualización segura, cuando el servidor de intercambio seguro recibe los datos de autentificación de inicio de sesión, donde el recurso de visualización segura restringe la visualización del contenido de los datos informáticos, tal como los presenta el dispositivo informático móvil designado, a solo el al menos un usuario autentificado de la segunda entidad empresarial en el dispositivo informático móvil designado, donde el acceso concedido está limitado por la política de retención de contenido.

2. El método de la reivindicación 1, donde la política de retención de contenido es una restricción de retención condicionada a la oferta, donde se elimina el acceso al contenido de datos informáticos cuando no se cumple una condición de oferta presentada por el usuario de la segunda entidad empresarial al usuario de la tercera entidad empresarial.

3. El método de la reivindicación 1, donde la política de retención de contenido establece un periodo de tiempo durante el cual el usuario de la tercera entidad empresarial tiene acceso al contenido de datos informáticos.

4. El método de la reivindicación 1, donde la política de retención de contenido prohíbe al usuario de la tercera entidad empresarial al menos una de entre imprimir, copiar y compartir el contenido de datos informáticos.

5. El método de la reivindicación 1, donde la política de retención de contenido prohíbe al usuario de la tercera entidad empresarial almacenar el contenido de datos informáticos en al menos un dispositivo informático especificado.

6. El método de la reivindicación 1, donde el dispositivo informático móvil designado es al menos uno de entre un teléfono inteligente, un dispositivo, y un ordenador portátil.

7. El método de la reivindicación 1, donde el al menos un usuario de la segunda entidad empresarial, en el dispositivo informático móvil designado, se descarga el contenido de datos informáticos al dispositivo informático móvil designado una vez se le ha concedido el acceso.

8. El método de la reivindicación 7, donde el al menos un usuario de la segunda entidad empresarial en el dispositivo informático móvil designado está autorizado a ver el contenido de datos informáticos cuando no hay conexión entre el dispositivo informático móvil designado y el servidor de intercambio.

9. El método de la reivindicación 8, donde el contenido de datos informáticos descargado no puede imprimirse.

10. El método de la reivindicación 8, donde el contenido de datos informáticos descargado no puede copiarse.

11. El método de la reivindicación 8, donde el contenido de datos informáticos descargado sólo es accesible a través del recurso de visualización seguro.

12. El método de la reivindicación 8, donde el contenido de datos informáticos descargado se modifica y se transmite al servidor de intercambio seguro.

13. El método de la reivindicación 12, donde el contenido de datos informáticos modificado se indica como habiendo sido modificado en metadatos almacenados en o asociados con el contenido de datos informáticos.

14. El método de la reivindicación 1, donde el permiso de acceso está limitado al acceso de sólo la versión actual del contenido de datos informáticos.

15. El método de la reivindicación 1, donde el recurso de visualización seguro monitoriza la visualización del contenido de datos informáticos.

16. El método de la reivindicación 15, donde se informa de la visualización monitorizada al servidor de intercambio.

17. El método de la reivindicación 1, donde el recurso de visualización segura autentifica el permiso para visualizar el contenido a través del reconocimiento facial utilizando un sensor.

18. El método de la reivindicación 1, donde el recurso de visualización seguro autentifica el permiso para visualizar el contenido a través del reconocimiento facial utilizando una cámara.

19. El método de la reivindicación 18, donde la cámara es una cámara integrada en el dispositivo informático móvil designado, y el recurso de visualización seguro reacciona a la dirección de la mirada bloqueando la visualización del contenido de datos informáticos si el usuario aparta la mirada del dispositivo informático móvil designado.

20. El método de la reivindicación 17, donde el sensor es un sensor integrado y es un sensor biométrico.

21. El método de la reivindicación 1, donde el recurso de visualización segura restringe la visualización distorsionando aquellas partes del contenido de datos informáticos que no se seleccionen para la visualización.

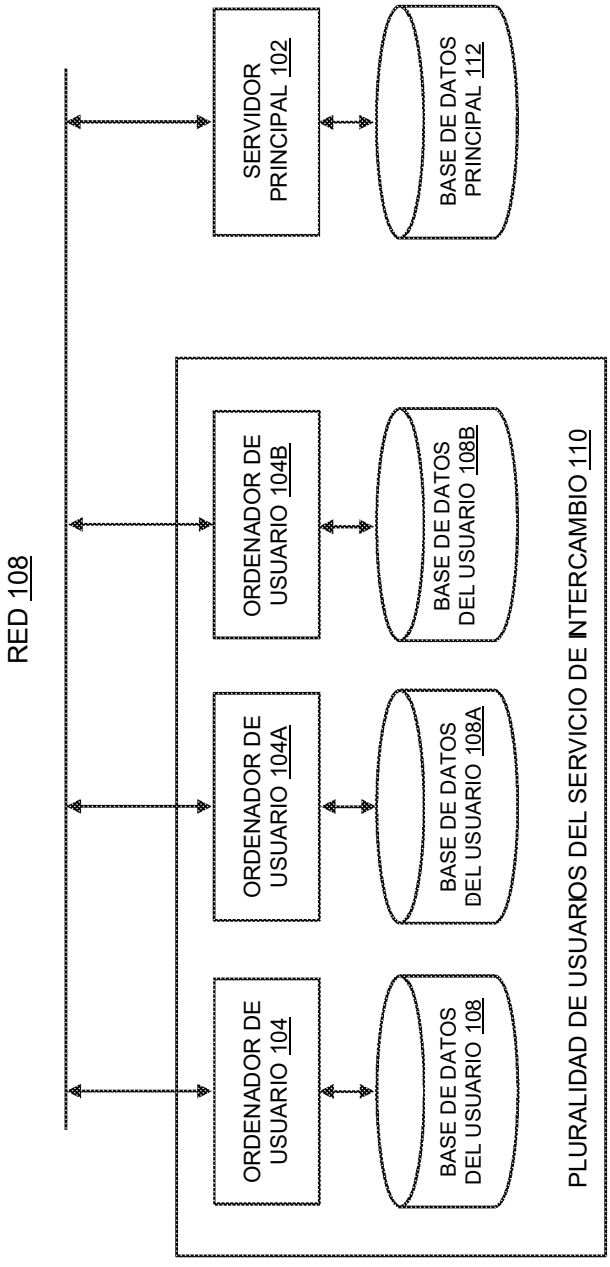

RED 108
SERVIDOR PRINCIPAL 102
BASE DE DATOS PRINCIPAL 112
ORDENADOR DE USUARIO 104B
BASE DE DATOS DEL USUARIO 108B
ORDENADOR DE USUARIO 104A
BASE DE DATOS DEL USUARIO 108A
ORDENADOR DE USUARIO 104
BASE DE DATOS DEL USUARIO 108
PLURALIDAD DE USUARIOS DEL SERVICIO DE INTERCAMBIO 110

Fig. 1

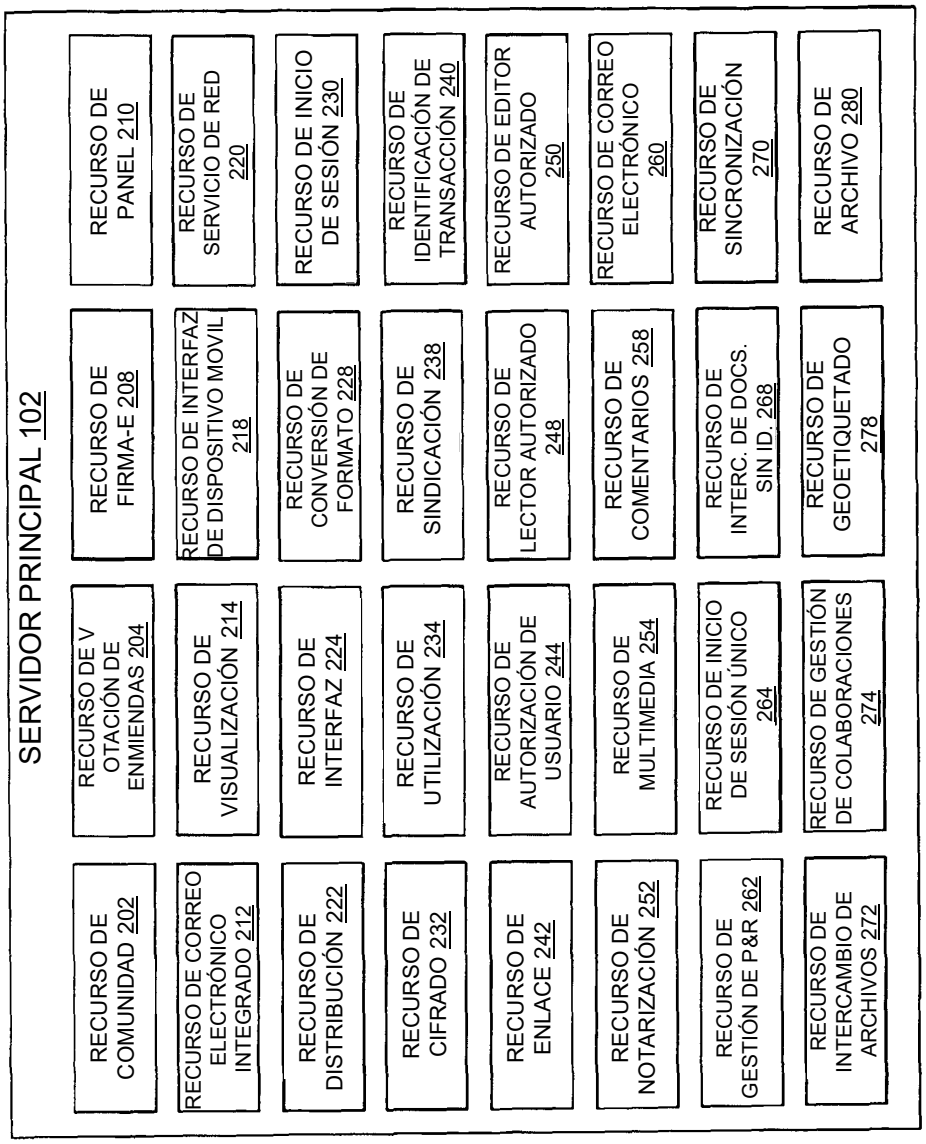

SERVIDOR PRINCIPAL 102
RECURSO DE COMUNIDAD 202
RECURSO DE V OTACIÓN DE ENMIENDAS 204
RECURSO DE FIRMA-E 208
RECURSO DE PANEL 210
RECURSO DE CORREO ELECTRÓNICO INTEGRADO 212
RECURSO DE VISUALIZACIÓN 214
RECURSO DE INTERFAZ DE DISPOSITIVO MOVIL 218
RECURSO DE SERVICIO DE RED 220
RECURSO DE DISTRIBUCIÓN 222
RECURSO DE INTERFAZ 224
RECURSO DE CONVERSIÓN DE FORMATO 228
RECURSO DE INICIO DE SESIÓN 230
RECURSO DE CIFRADO 232
RECURSO DE UTILIZACIÓN 234
RECURSO DE SINDICACIÓN 238
RECURSO DE IDENTIFICACIÓN DE TRANSACCIÓN 240
RECURSO DE ENLACE 242
RECURSO DE AUTORIZACIÓN DE USUARIO 244
RECURSO DE LECTOR AUTORIZADO 248
RECURSO DE EDITOR AUTORIZADO 250
RECURSO DE NOTARIZACIÓN 252
RECURSO DE MULTIMEDIA 254
RECURSO DE COMENTARIOS 258
RECURSO DE CORREO ELECTRÓNICO 260
RECURSO DE GESTIÓN DE P&R 262
RECURSO DE INICIO DE SESIÓN ÚNICO 264
RECURSO DE INTERC. DE DOCS. SIN ID. 268
RECURSO DE SINCRONIZACIÓN 270
RECURSO DE INTERCAMBIO DE ARCHIVOS 272
RECURSO DE GESTIÓN DE COLABORACIONES 274
RECURSO DE GEOETIQUETADO 278
RECURSO DE ARCHIVO 280

Fig. 2

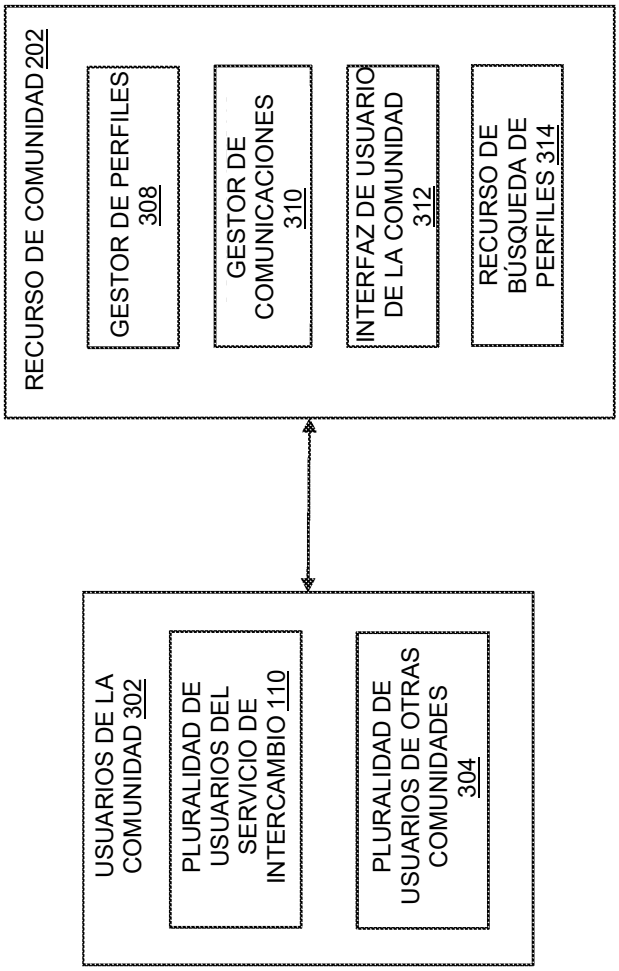

RECURSO DE COMUNIDAD 202
GESTOR DE PERFILES 308
GESTOR DE COMUNICACIONES 310
INTERFAZ DE USUARIO DE LA COMUNIDAD 312
RECURSO DE BÚSQUEDA DE PERFILES 314
USUARIOS DE LA COMUNIDAD 302
PLURALIDAD DE USUARIOS DEL SERVICIO DE INTERCAMBIO 110
PLURALIDAD DE USUARIOS DE OTRAS COMUNIDADES 304

Fig. 3

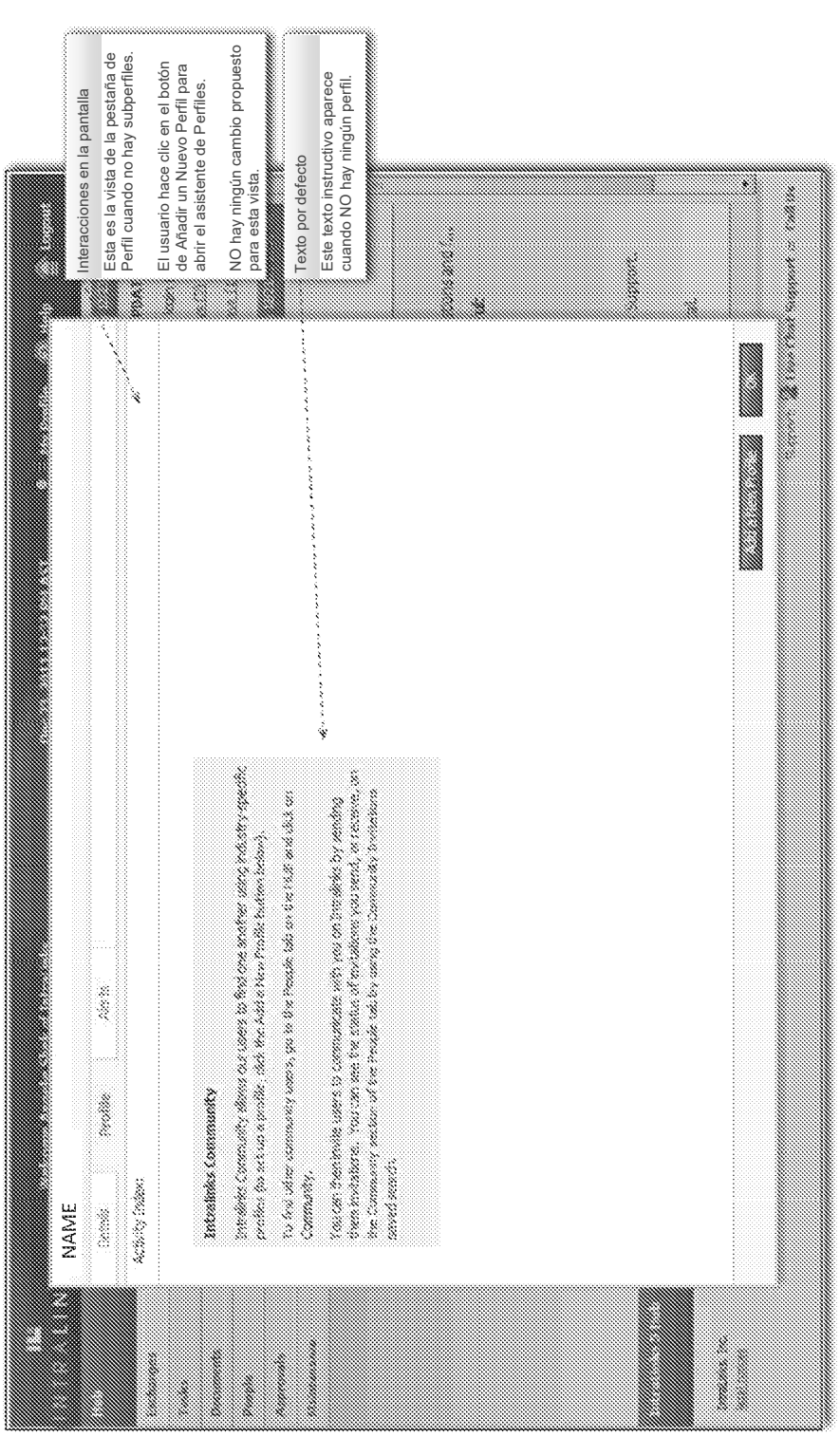

Configuración del perfil – Paso 1
NAME
Interacciones en la pantalla
Esta es la vista de la pestaña de Perfil cuando no hay subperfiles.
El usuario hace clic en el botón de Añadir un Nuevo Perfil para abrir el asistente de Perfiles.
NO hay ningún cambio propuesto para esta vista.
Texto por defecto
Este texto instructivo aparece cuando NO hay ningún perfil.

Fig. 3A

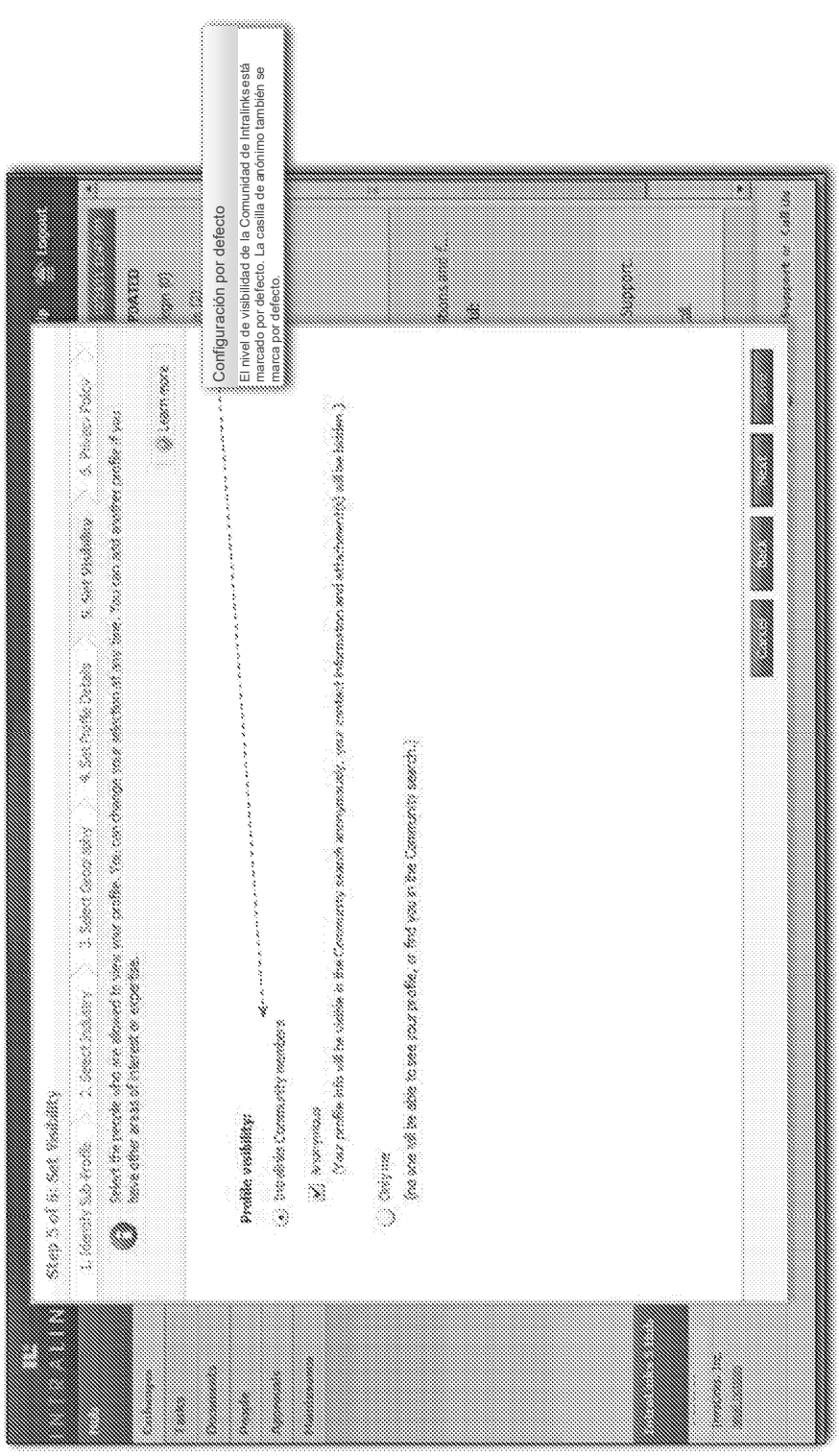

Visibilidad - Anónimo
Configuración por defecto
El nivel de visibilidad de la Comunidad de Intralinks está marcado por defecto. La casilla de anónimo también se marca por defecto.

Fig. 3B

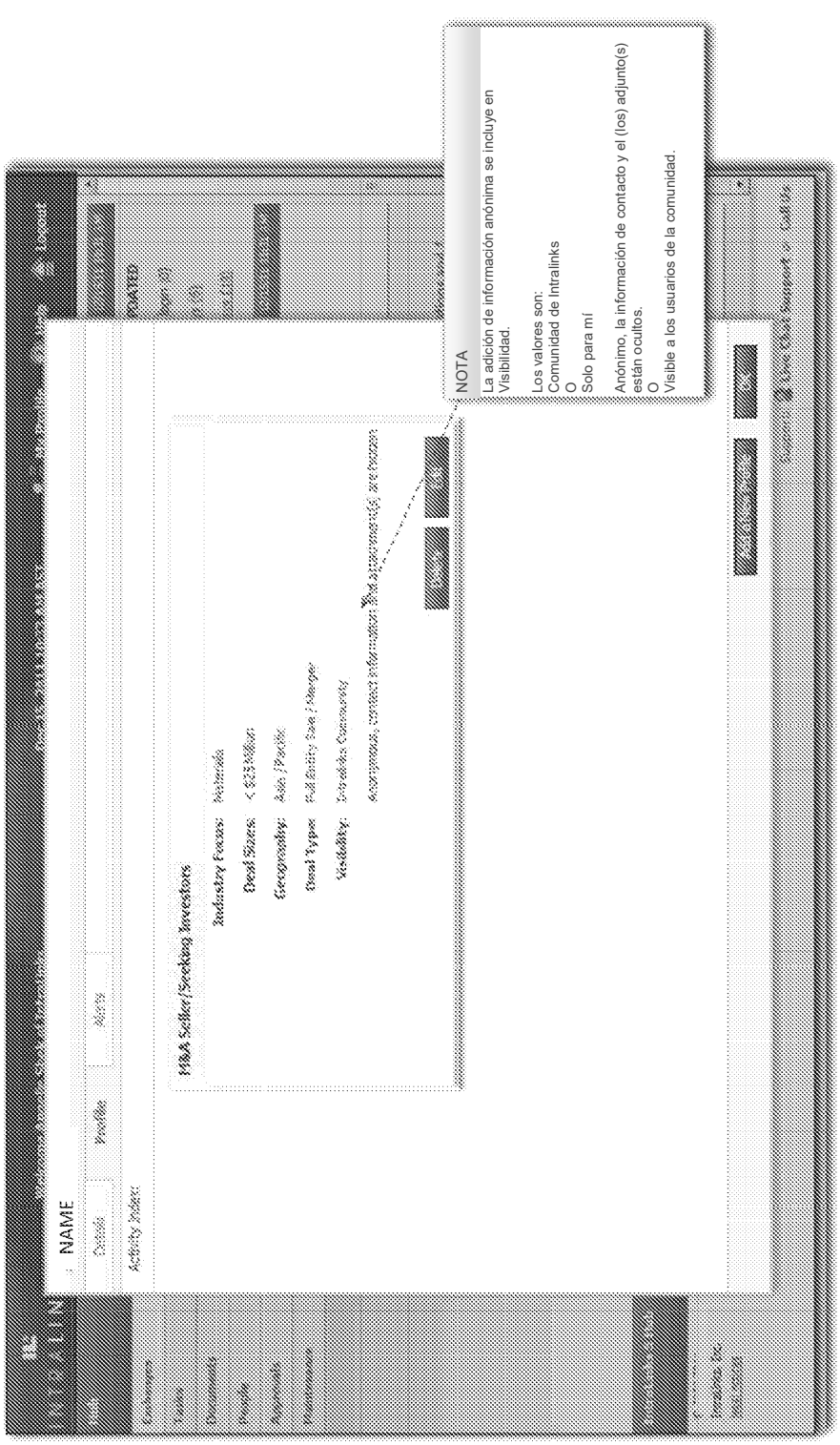

Configuración del perfil – Paso 3
NAME
NOTA
La adición de información anónima se incluye en Visibilidad.
Los valores son:
Comunidad de Intralinks
O
Solo para mí
Anónimo, la información de contacto y el (los) adjunto(s) están ocultos.
O
Visible a los usuarios de la comunidad.

Fig. 3C

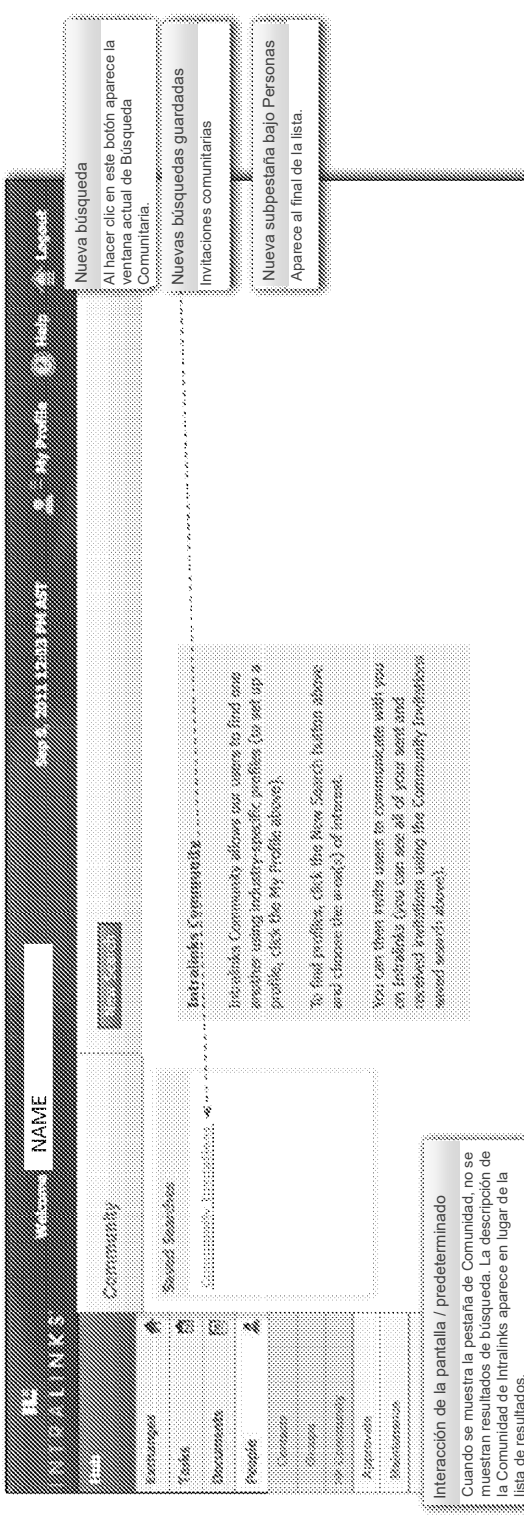

Comunidad – defecto
Welcome NAME
Community
Saved Searches
Intralinks Communities
Nueva búsqueda
Al hacer clic en este botón aparece la ventana actual de Búsqueda Comunitaria.
Nuevas búsquedas guardadas
Invitaciones comunitarias
Nueva subpestaña bajo Personas
Aparece al final de la lista.
Interacción de la pantalla / predeterminado
Cuando se muestra la pestaña de Comunidad, no se muestran resultados de búsqueda. La descripción de la Comunidad de Intralinks aparece en lugar de la lista de resultados.
El usuario debe hacer clic en Nueva Búsqueda para que aparezca la ventana de búsqueda comunitaria (sin cambios en la ventana de búsqueda comunitaria, o en su funcionamiento).
NO hay opciones de visualización o acciones cuando la pantalla está en el estado predeterminado.
NOTA
Cuando un usuario hace clic en la pestaña de Personas, la subpestaña de Contactos sigue siendo la ventana que se muestra por defecto.
NOTA
Personas > Contactos no contiene NINGUNA referencia a Comunidad (y, por lo tanto, no se muestran las búsquedas guardadas, ni la información sobre la visibilidad del perfil en la lista de resultados).

Fig. 3D

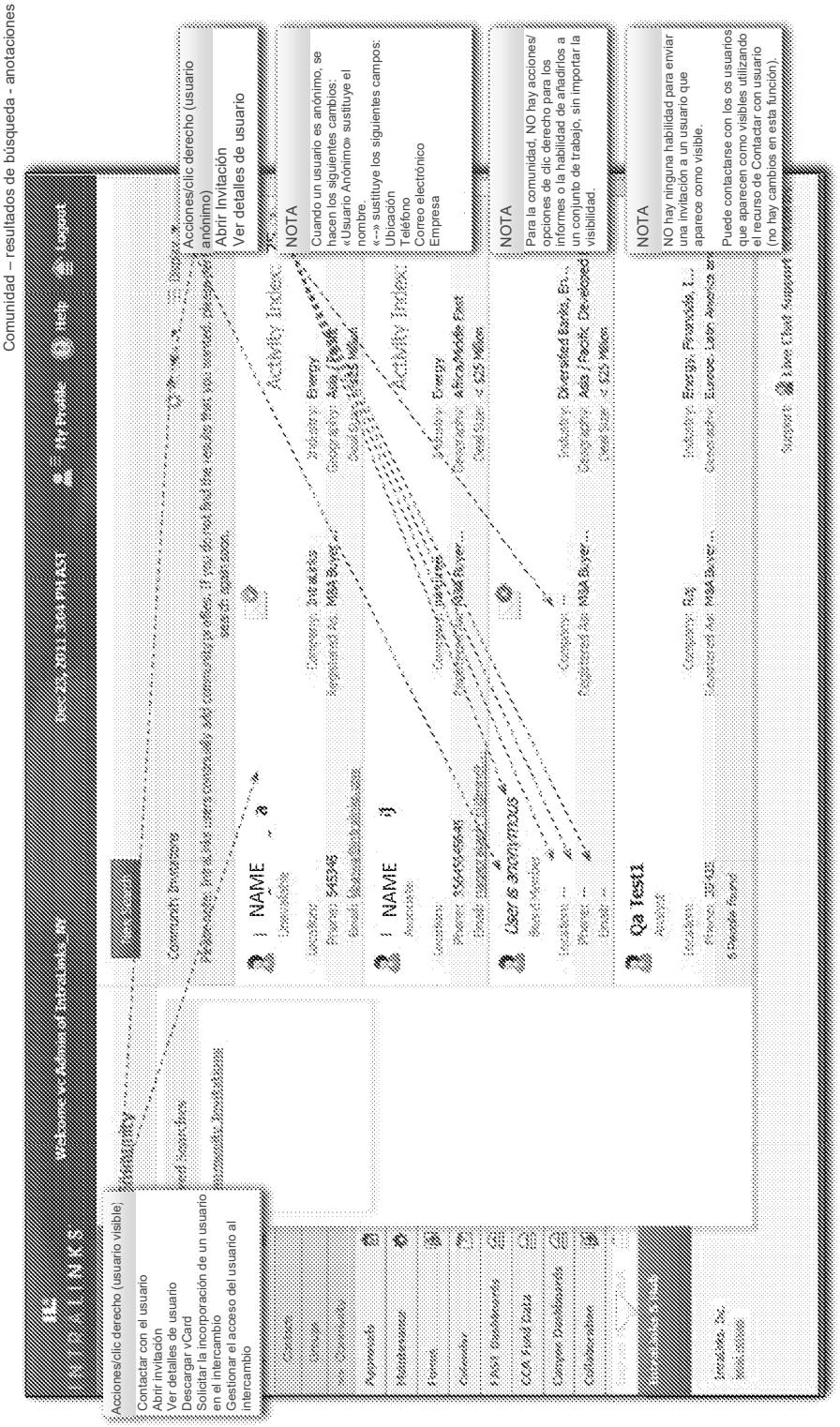

Comunidad – resultados de búsqueda - anotaciones
Acciones/clic derecho (usuario visible)
Contactar con el usuario
Abrir invitación
Ver detalles de usuario
Descargar vCard
Solicitar la incorporación de un usuario en el intercambio
Gestionar el acceso del usuario al intercambio
Acciones/clic derecho (usuario anónimo)
Abrir Invitación
Ver detalles de usuario
NOTA
Cuando un usuario es anónimo, se hacen los siguientes cambios:
«Usuario Anónimo» sustituye el nombre.
«---» sustituye los siguientes campos:
Ubicación
Teléfono
Correo electrónico
Empresa
NOTA
Para la comunidad, NO hay acciones/opciones de clic derecho para los informes o la habilidad de añadirlos a un conjunto de trabajo, sin importar la visibilidad.
NOTA
NO hay ninguna habilidad para enviar una invitación a un usuario que aparece como visible.
Puede contactarse con los os usuarios que aparecen como visibles utilizando el recurso de Contactar con usuario (no hay cambios en esta función).

Fig. 3E

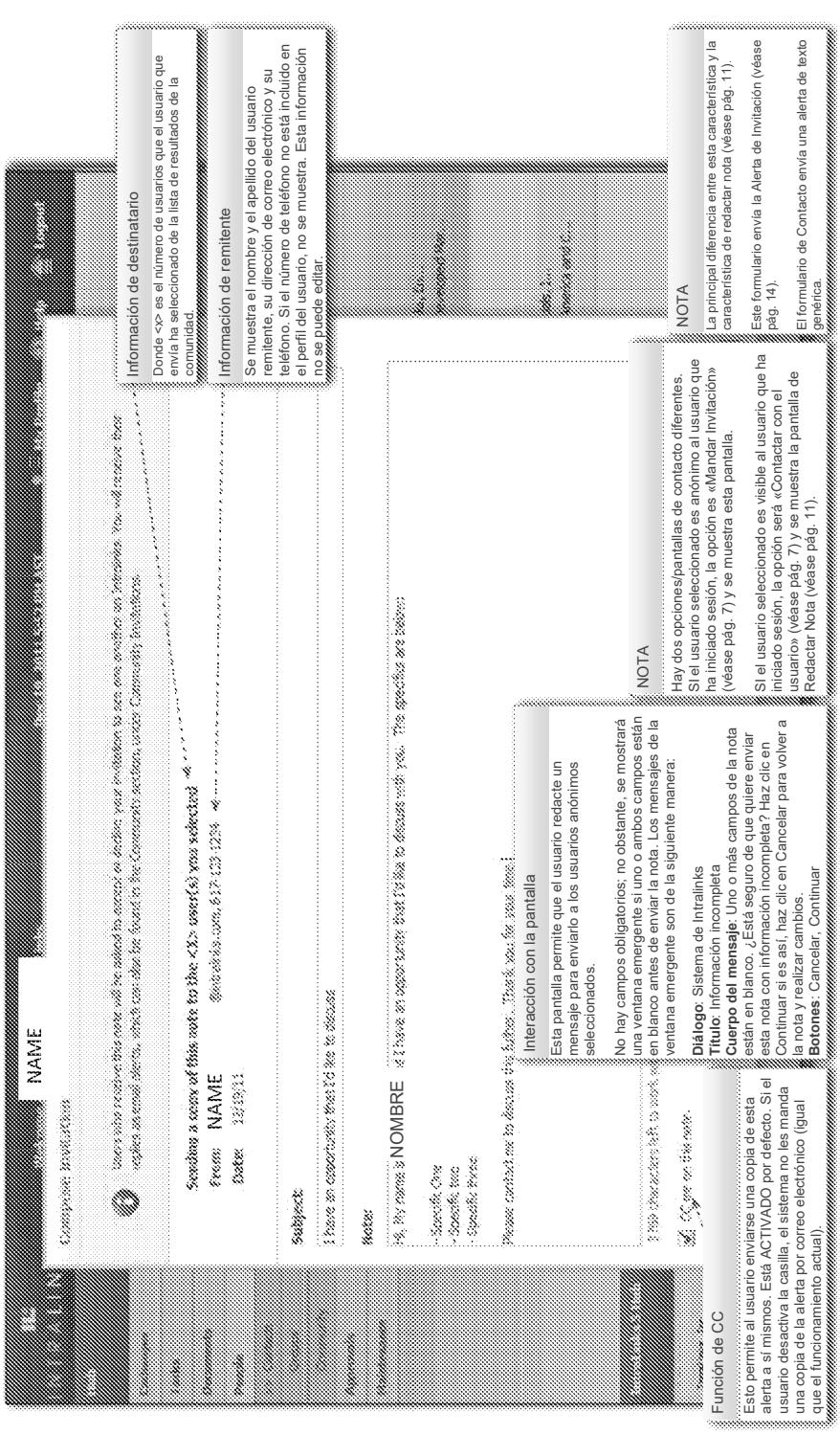

Resultados de búsqueda – redactar invitación – anotaciones
NAME
Información de destinatario
Información de remitente
NOTA
NOTA
Función de CC

Fig. 3F

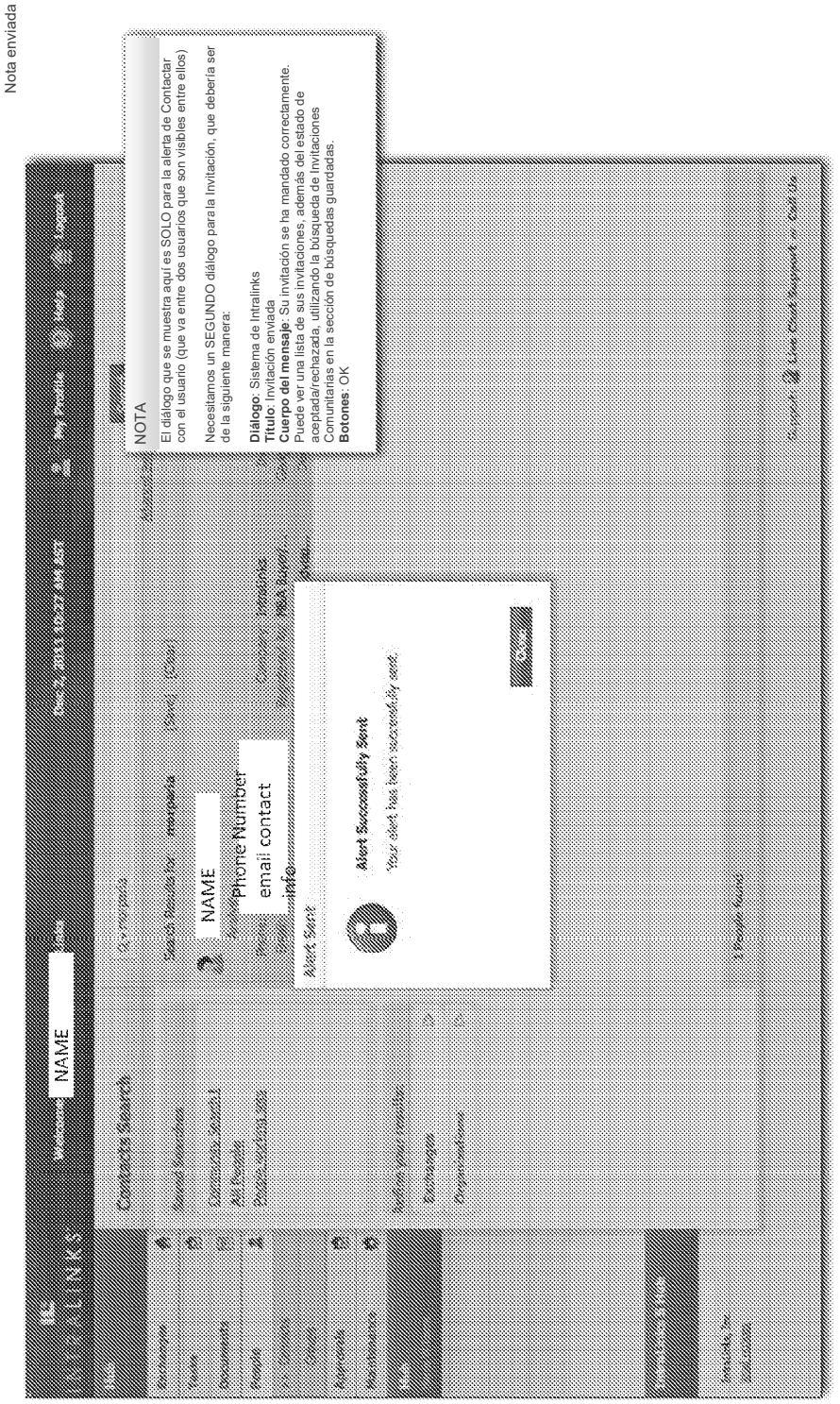

Nota enviada
NAME
NOTA
El diálogo que se muestra aquí es SOLO para la alerta de Contactar con el usuario (que va entre dos usuarios que son visibles entre ellos)
Necesitamos un SEGUNDO diálogo para la Invitación, que debería ser de la siguiente manera:
Diálogo: Sistema de Intralinks
Título: Invitación enviada
Cuerpo del mensaje: Su invitación se ha mandado correctamente. Puede ver una lista de sus invitaciones, además del estado de aceptada/rechazada, utilizando la búsqueda de Invitaciones Comunitarias en la sección de búsquedas guardadas.
Botones: OK
NAME
Phone Number
email contact
info
Alert Sent
Alert Successfully Sent
Your alert has been successfully sent.
OK

Fig. 3G

Resultados de búsqueda – redactar NOTA
NAME
Compose Note
Seeding a copy of this note to the <X> user(s) you selected
from: NOMBRE
Subject:
Note:
NOTA
Este es un cambio de la interfaz de usuario SOLO para esta característica. El método para el envío, la alerta de formato, y la ventana emergente de éxito que existen actualmente para esta característica NO cambian. El cambio de esta interfaz de usuario solo es alinear los dos métodos de alerta comunitaria: Contactar con el usuario y Mandar Invitación.
NOTA
La diferencia entre este formato y el formato de la pantalla de Redactar Invitación (véase pág. 8):
Este formulario envía la alerta de texto genérica.
El otro formulario envía la Alerta de Invitación.

Fig. 3H

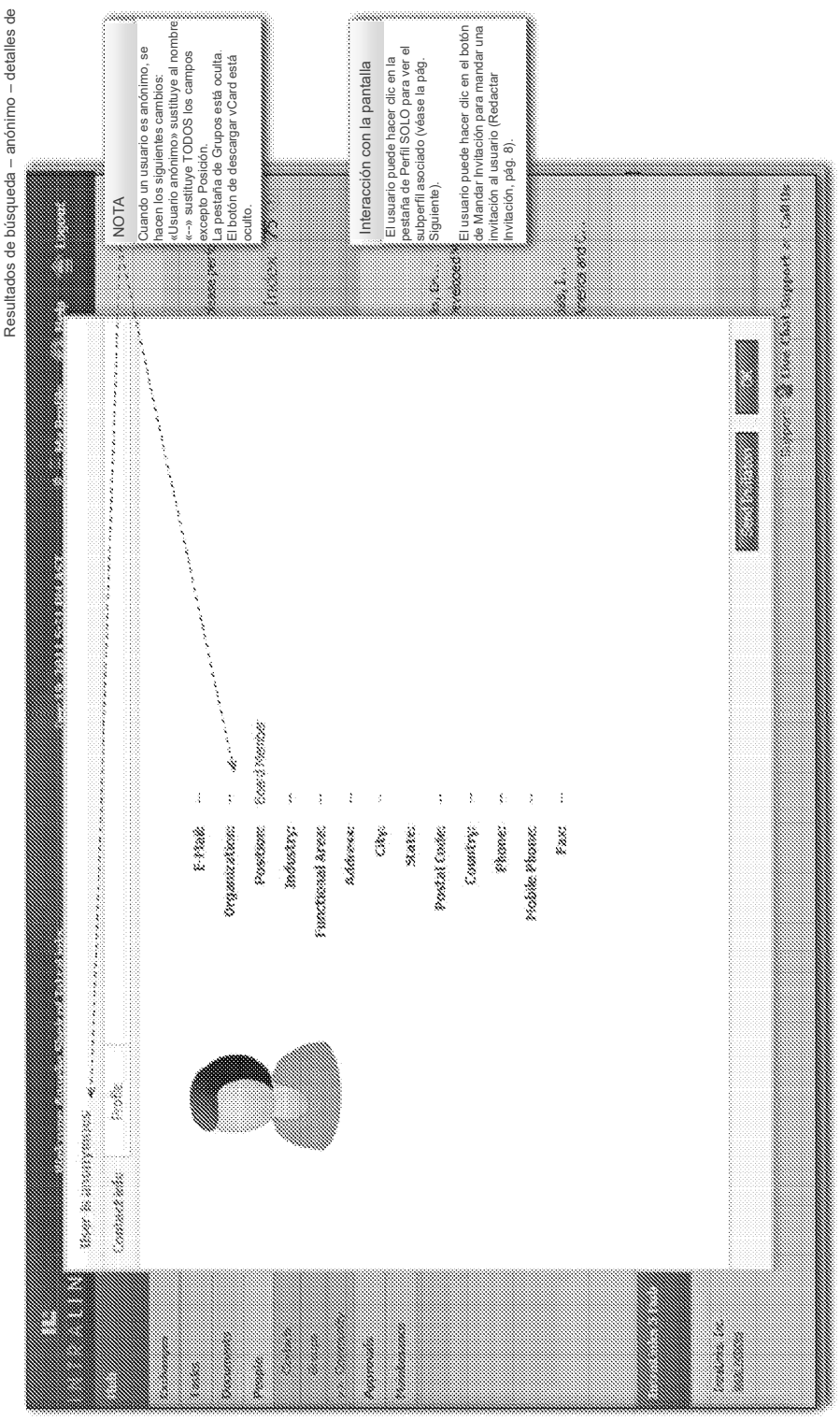

Resultados de búsqueda – anónimo – detalles de
NOTA
Cuando un usuario es anónimo, se hacen los siguientes cambios:
«Usuario anónimo» sustituye al nombre «---» sustituye TODOS los campos excepto Posición.
La pestaña de Grupos está oculta.
El botón de descargar vCard está oculto.
Interacción con la pantalla
El usuario puede hacer clic en la pestaña de Perfil SOLO para ver el subperfil asociado (véase la pág. Siguiente).
El usuario puede hacer clic en el botón de Mandar invitación para mandar una invitación al usuario (Redactar invitación, pág. 8).

Fig. 3l

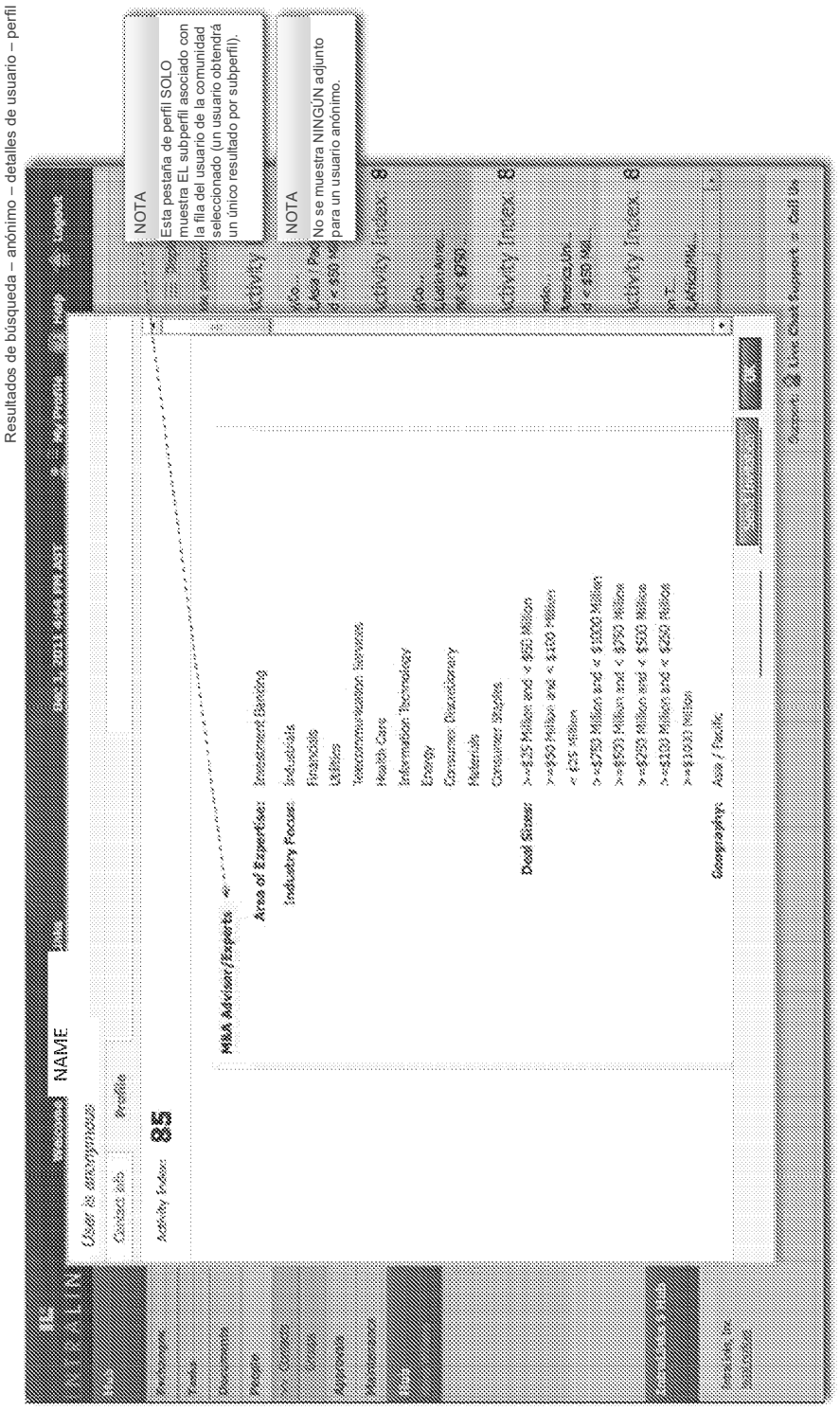

Resultados de búsqueda – anónimo – detalles de usuario – perfil
NAME
User is anonymous
Profile
85
NOTA
Esta pestaña de perfil SOLO muestra EL subperfil asociado con la fila del usuario de la comunidad seleccionado (un usuario obtendrá un único resultado por subperfil).
NOTA
No se muestra NINGÚN adjunto para un usuario anónimo.

Fig. 3J

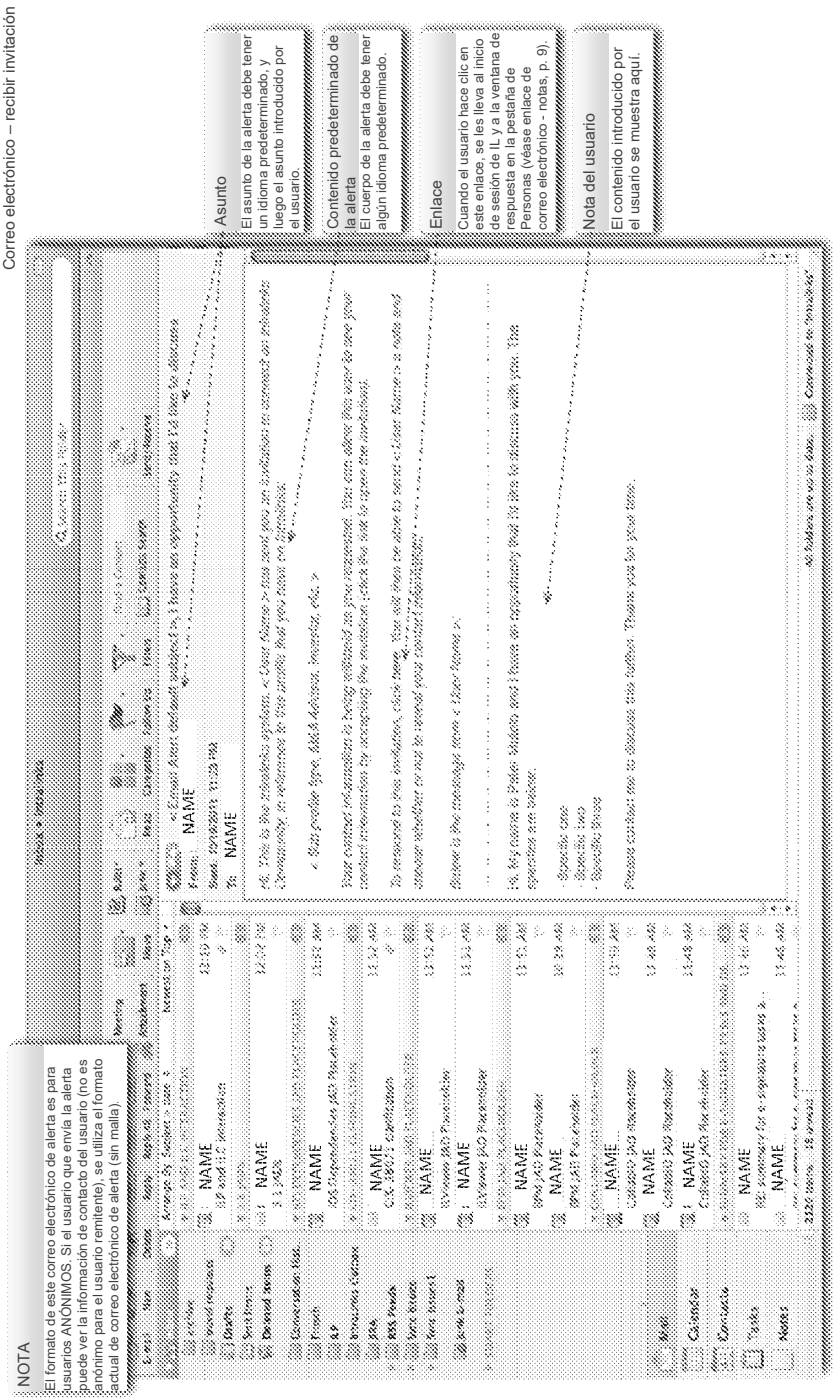

Correo electrónico – recibir invitación
NOTA
El formato de este correo electrónico de alerta es para usuarios ANÓNIMOS. Si el usuario que envía la alerta puede ver la información de contacto del usuario (no es anónimo para el usuario remitente), se utiliza el formato actual de correo electrónico de alerta (sin malla).
Asunto
El asunto de la alerta debe tener un idioma predeterminado, y luego el asunto introducido por el usuario.
Contenido predeterminado de la alerta
El cuerpo de la alerta debe tener algún idioma predeterminado.
Enlace
Cuando el usuario hace clic en este enlace, se les lleva al inicio de sesión de IL y a la ventana de respuesta en la pestaña de Personas (véase enlace de correo electrónico - notas, p. 9).
Nota del usuario
El contenido introducido por el usuario se muestra aquí.

Fig. 3K

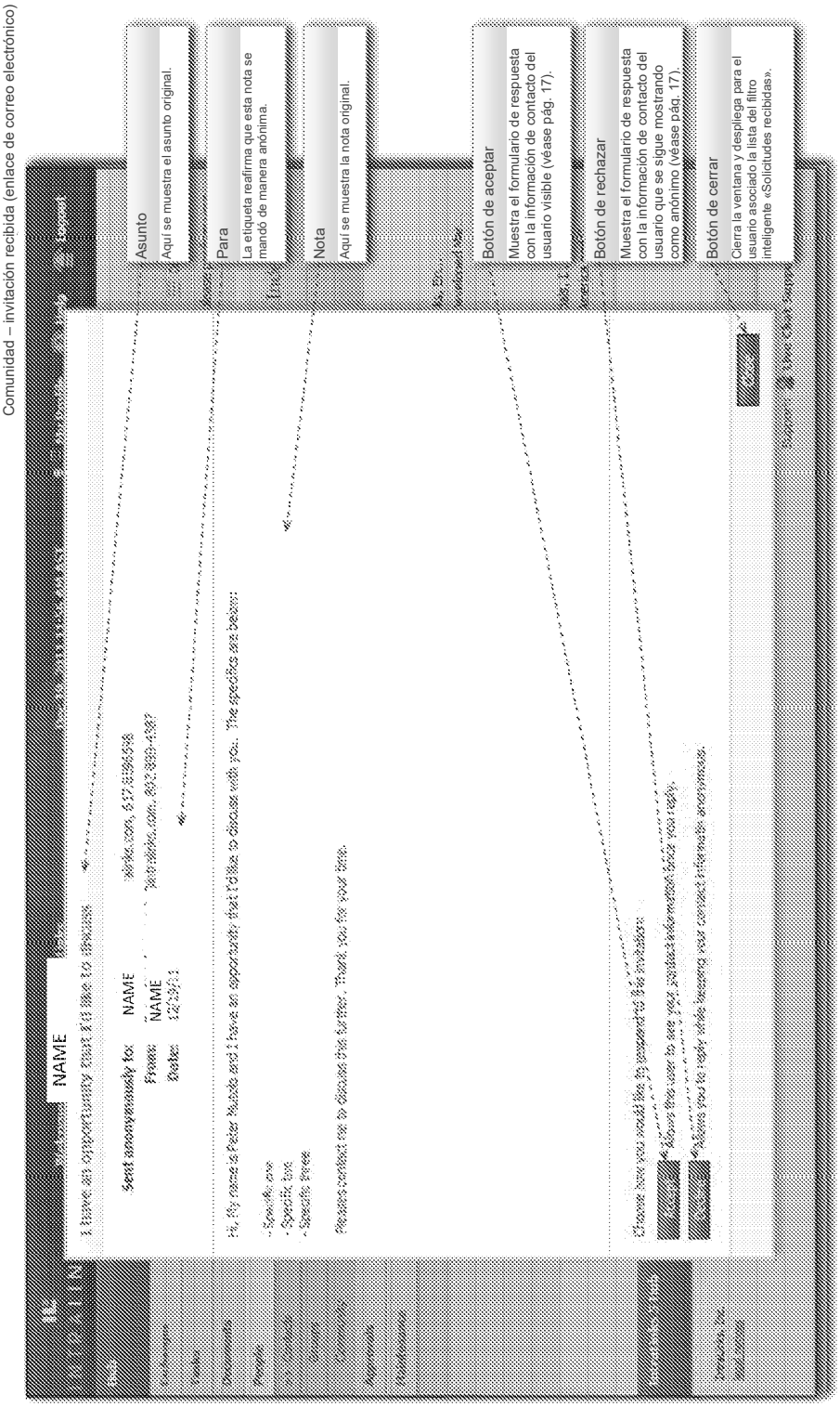

Comunidad – invitación recibida (enlace de correo electrónico)
Asunto
Aquí se muestra el asunto original.
Para
La etiqueta reafirma que esta nota se mandó de manera anónima.
Nota
Aquí se muestra la nota original.
Botón de aceptar
Muestra el formulario de respuesta con la información de contacto del usuario visible (véase pág. 17).
Botón de rechazar
Muestra el formulario de respuesta con la información de contacto del usuario que se sigue mostrando como anónimo (véase pág. 17).
Botón de cerrar
Cierra la ventana y despliega para el usuario asociado la lista del filtro inteligente «Solicitudes recibidas».

Fig. 3L

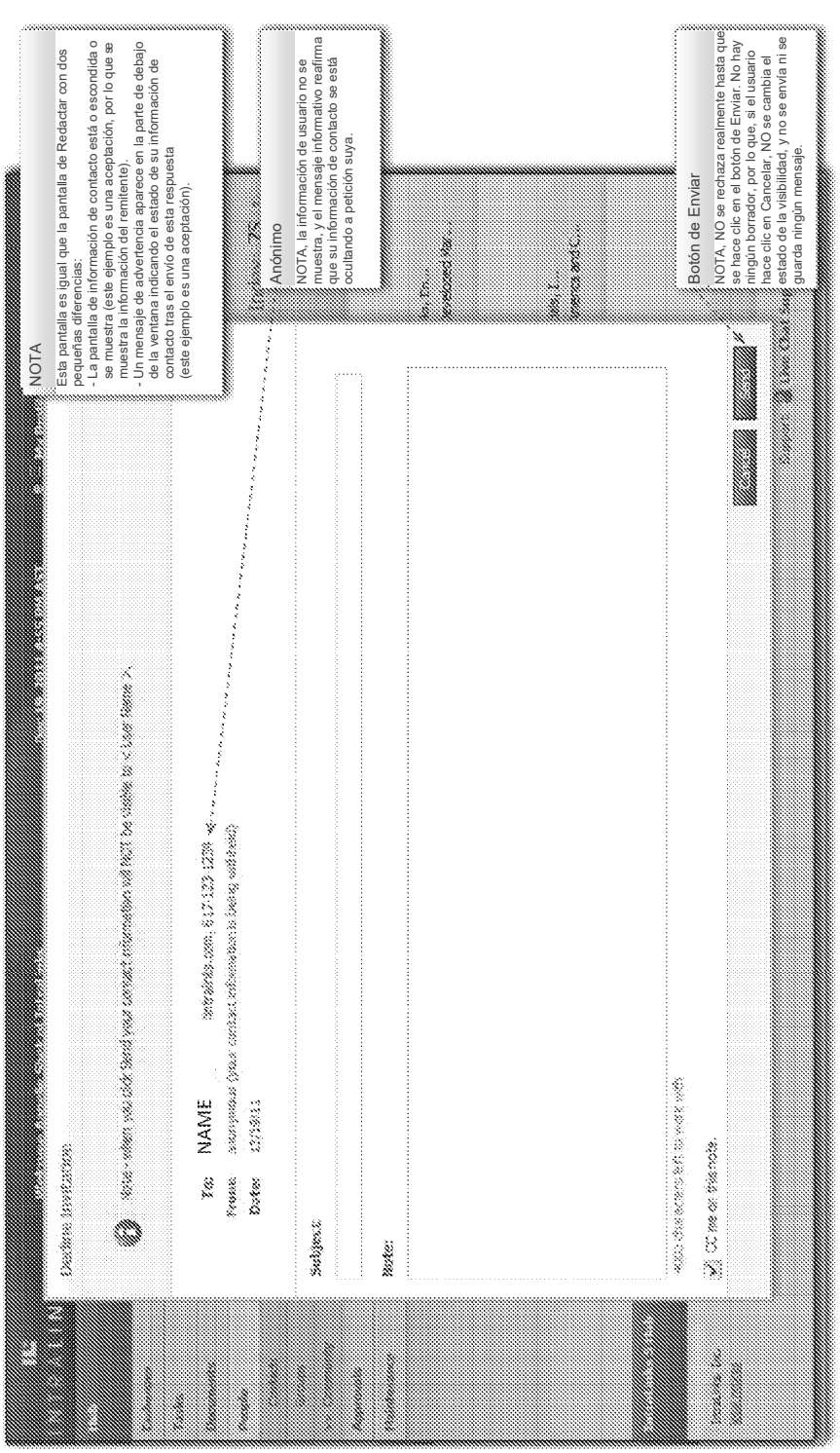

Comunidad – redactar respuesta – rechazada
NOTA
Esta pantalla es igual que la pantalla de Redactar con dos pequeñas diferencias:
- La pantalla de información de contacto está o escondida o se muestra (este ejemplo es una aceptación, por lo que se muestra la información del remitente)
- Un mensaje de advertencia aparece en la parte de debajo de la ventana indicando el estado de su información de contacto tras el envío de esta respuesta (este ejemplo es una aceptación).
Anónimo
NOTA, la información de usuario no se muestra, y el mensaje informativo reafirma que su información de contacto se está ocultando a petición suya.
Botón de Enviar
NOTA, NO se rechaza realmente hasta que se hace clic en el botón de Enviar. No hay ningún borrador, por lo que, si el usuario hace clic en Cancelar, NO se cambia el estado de la visibilidad, y no se envía ni se guarda ningún mensaje.

Fig. 3M

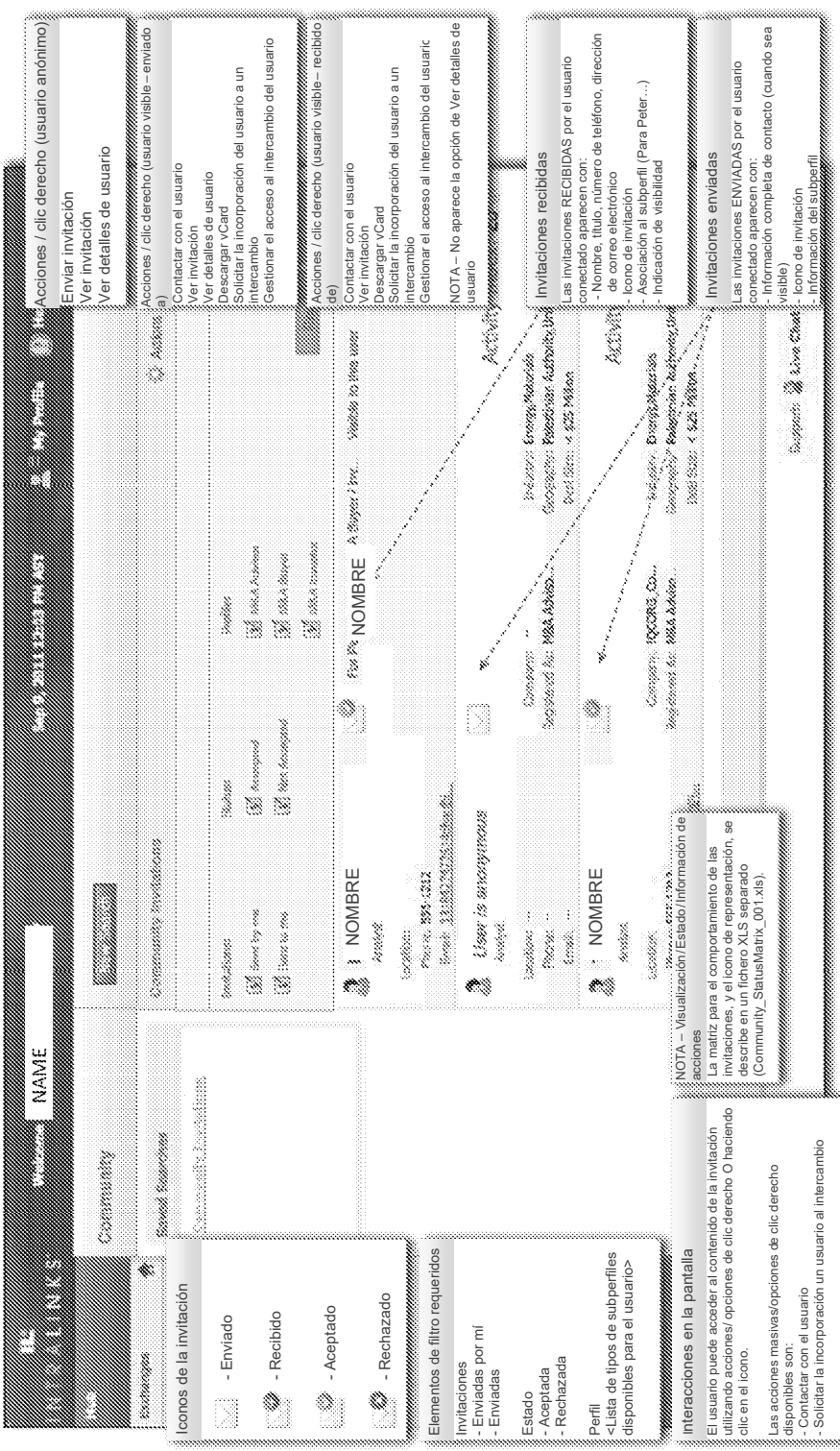

Búsqueda guardada de invitaciones de comunidad – anotaciones
Acciones / clic derecho (usuario anónimo)
Enviar invitación
Ver invitación
Ver detalles de usuario
Acciones / clic derecho (usuario visible – enviado a)
Contactar con el usuario
Ver invitación
Ver detalles de usuario
Descargar vCard
Solicitar la incorporación del usuario a un intercambio
Gestionar el acceso al intercambio del usuario
Acciones / clic derecho (usuario visible – recibido de)
Contactar con el usuario
Ver invitación
Descargar vCard
Solicitar la incorporación del usuario a un intercambio
Gestionar el acceso al intercambio del usuario
NOTA – No aparece la opción de Ver detalles de usuario
Invitaciones recibidas
Las invitaciones RECIBIDAS por el usuario conectado aparecen con:
- Nombre, título, número de teléfono, dirección de correo electrónico
Icono de invitación
Asociación al subperfil (Para Peter…)
Indicación de visibilidad
Invitaciones enviadas
Las invitaciones ENVIADAS por el usuario conectado aparecen con:
- Información completa de contacto (cuando sea visible)
Icono de invitación
Información del subperfil
Iconos de la invitación
- Enviado
- Recibido
- Aceptado
- Rechazado
Elementos de filtro requeridos
Invitaciones
- Enviadas por mí
- Enviadas
Estado
- Aceptada
- Rechazada
Perfil
<Lista de tipos de subperfiles disponibles para el usuario>
Interacciones en la pantalla
El usuario puede acceder al contenido de la invitación utilizando acciones/ opciones de clic derecho O haciendo clic en el icono.
Las acciones masivas/opciones de clic derecho disponibles son:
- Contactar con el usuario
- Solicitar la incorporación un usuario al intercambio
NOTA – Visualización/Estado/Información de acciones
La matriz para el comportamiento de las invitaciones, y el icono de representación, se describe en un fichero XLS separado (Community_StatusMatrix_001.xls).

Fig. 3N

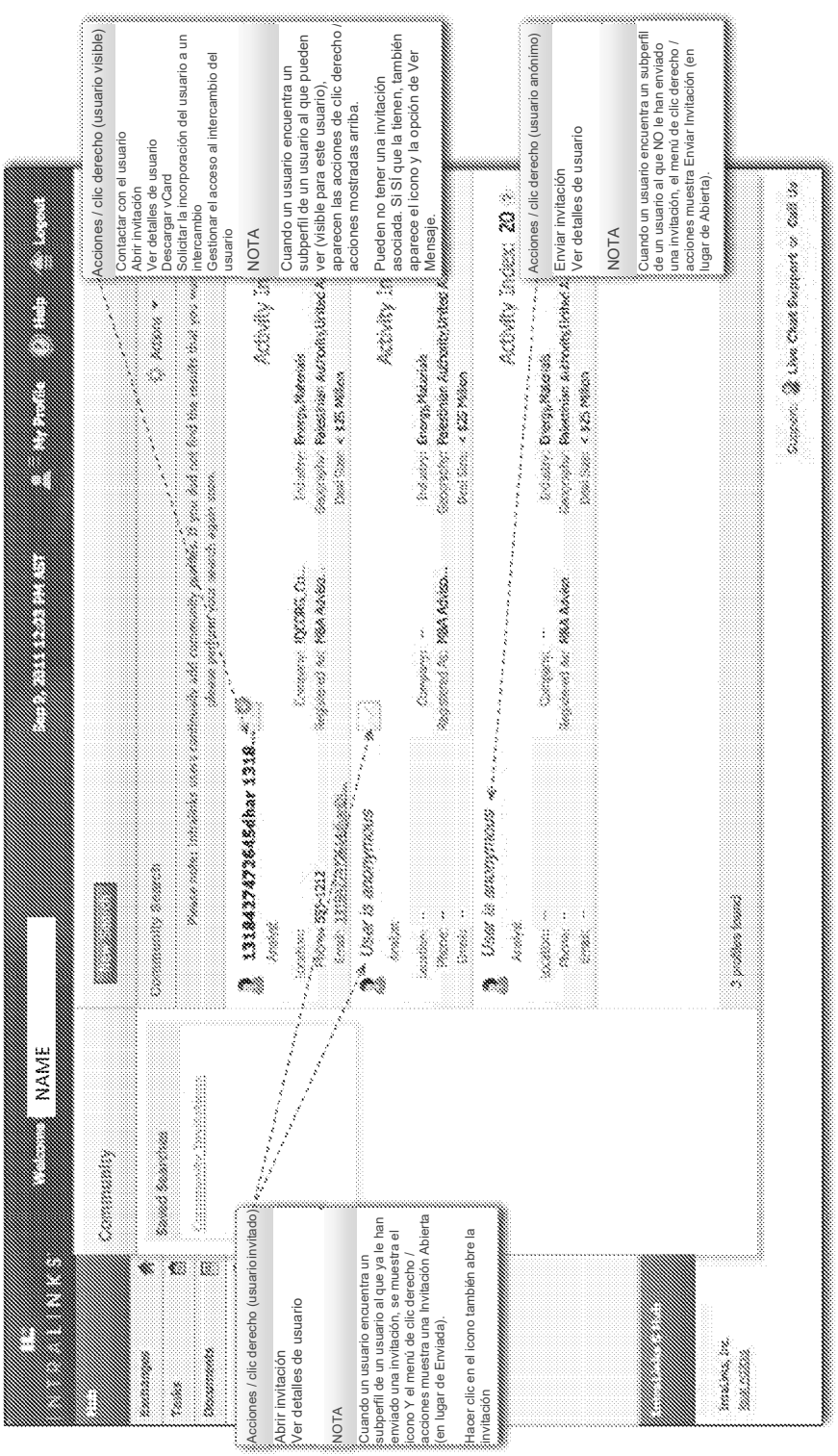

Resultados de búsqueda – lista – con invitados
NAME
Community
Acciones / clic derecho (usuario visible)
Contactar con el usuario
Abrir invitación
Ver detalles de usuario
Descargar vCard
Solicitar la incorporación del usuario a un intercambio
Gestionar el acceso al intercambio del usuario
NOTA
Cuando un usuario encuentra un subperfil de un usuario al que pueden ver (visible para este usuario), aparecen las acciones de clic derecho / acciones mostradas arriba.
Pueden no tener una invitación asociada. Si SÍ que la tienen, también aparece el icono y la opción de Ver Mensaje.
Acciones / clic derecho (usuario invitado)
Abrir invitación
Ver detalles de usuario
NOTA
Cuando un usuario encuentra un subperfil de un usuario al que ya le han enviado una invitación, se muestra el icono Y el menú de clic derecho / acciones muestra una invitación Abierta (en lugar de Enviada).
Hacer clic en el icono también abre la invitación
Acciones / clic derecho (usuario anónimo)
Enviar invitación
Ver detalles de usuario
NOTA
Cuando un usuario encuentra un subperfil de un usuario al que NO le han enviado una invitación, el menú de clic derecho / acciones muestra Enviar Invitación (en lugar de Abierta).

Fig. 3O

Resultados de búsqueda – Ventana emergente de solicitud – usuario receptor

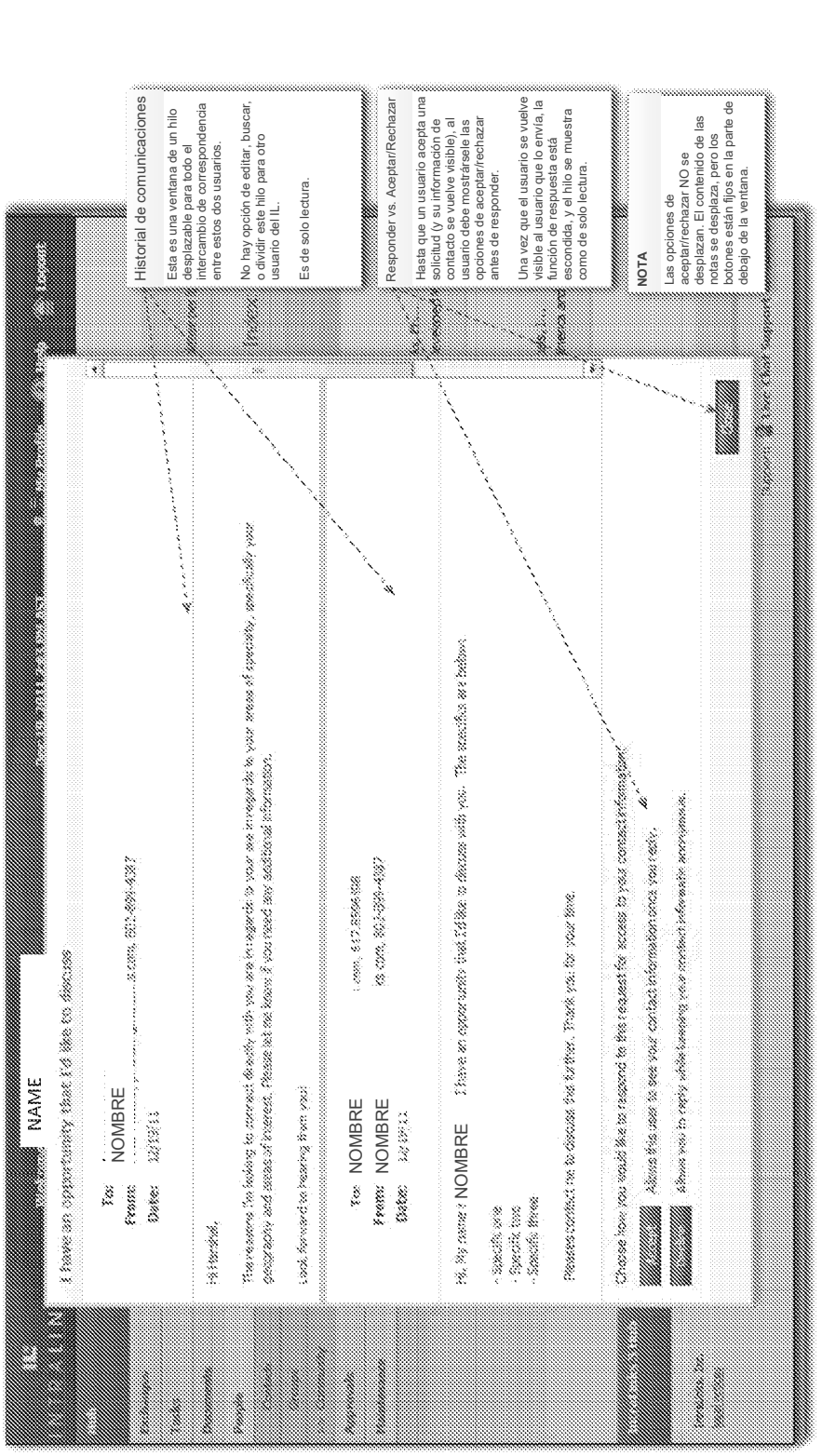


Fig. 3P

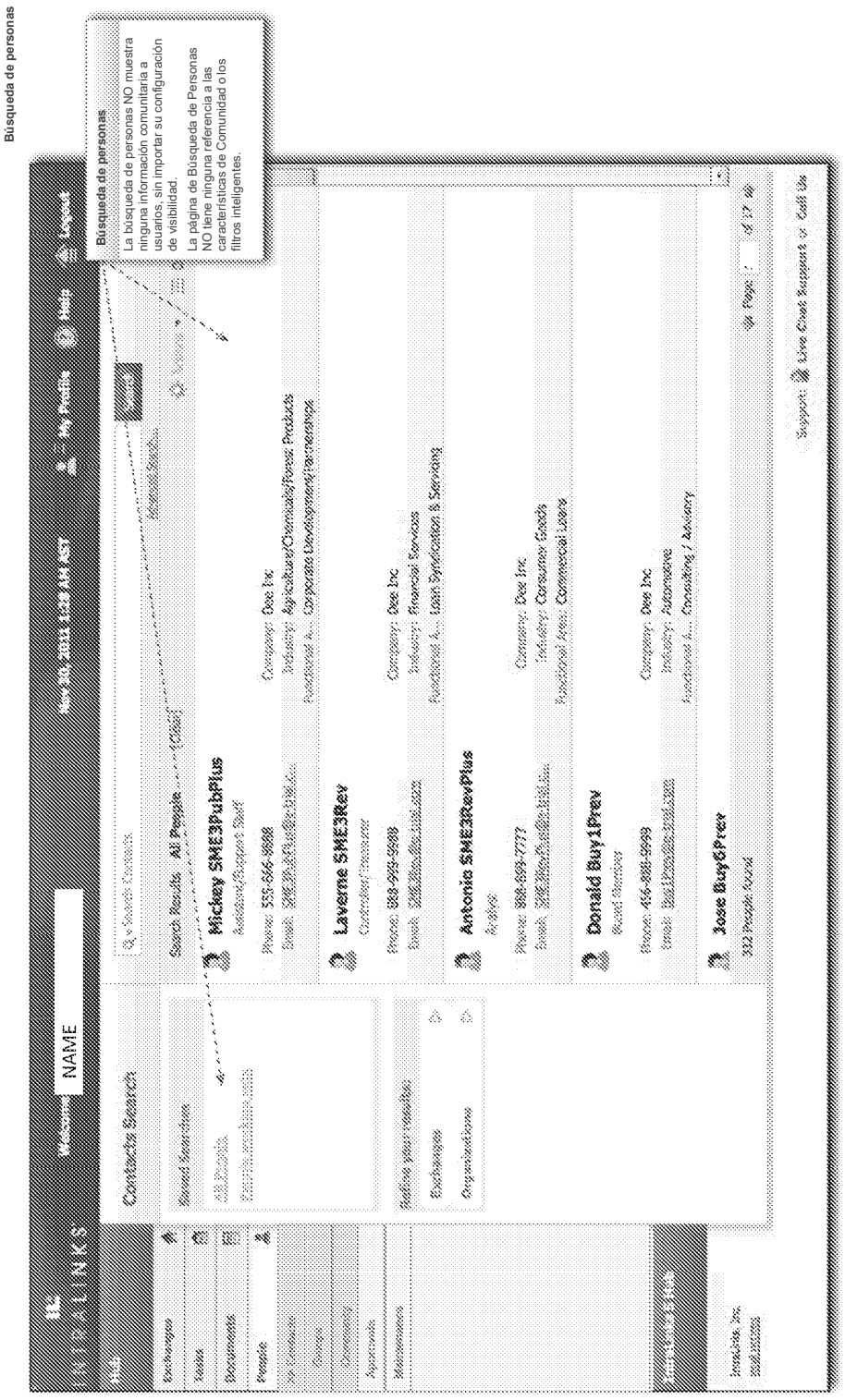

Búsqueda de personas
Búsqueda de personas
La búsqueda de personas NO muestra ninguna información comunitaria a usuarios, sin importar su configuración de visibilidad.
La página de Búsqueda de Personas NO tiene ninguna referencia a las características de Comunidad o los filtros inteligentes.
Contacts Search
Search Results: All People
Mickey SME3PubPlus
Laverne SME3Rev
Antonia SME3RevPlus
Donald Buy1Prev
Jose Buy6Prev

Fig. 3Q

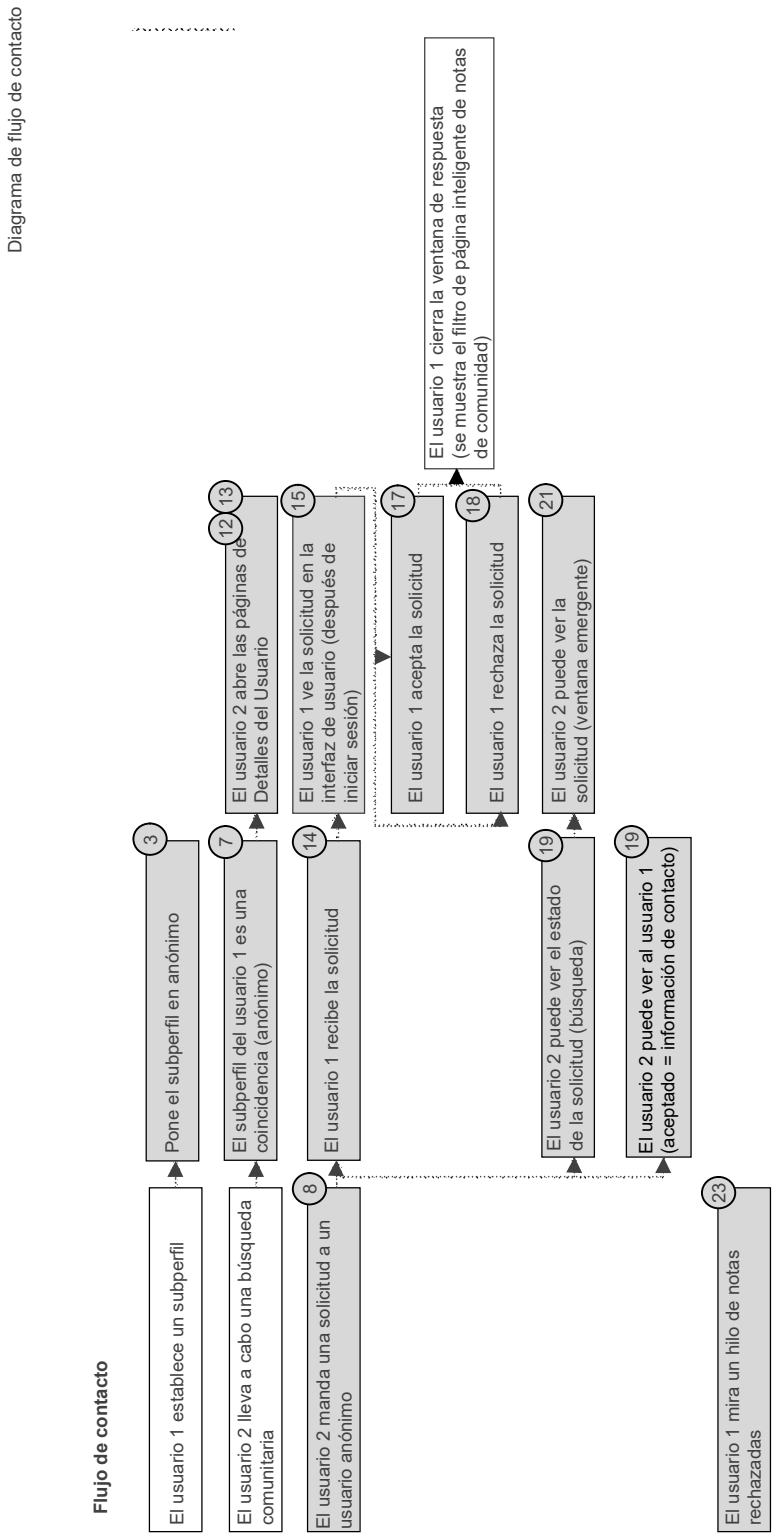


Diagrama de flujo de contacto
Flujo de contacto
El usuario 1 establece un subperfil
El usuario 2 lleva a cabo una búsqueda comunitaria
El usuario 2 manda una solicitud a un usuario anónimo
El usuario 1 mira un hilo de notas rechazadas
3
Pone el subperfil en anónimo
7
El subperfil del usuario 1 es una coincidencia (anónimo)
14
El usuario 1 recibe la solicitud
8
12
13
El usuario 2 abre las páginas de Detalles del Usuario
15
El usuario 1 ve la solicitud en la interfaz de usuario (después de iniciar sesión)
17
El usuario 1 acepta la solicitud
18
El usuario 1 rechaza la solicitud
El usuario 1 cierra la ventana de respuesta (se muestra el filtro de página inteligente de notas de comunidad)
19
El usuario 2 puede ver el estado de la solicitud (búsqueda)
19
El usuario 2 puede ver al usuario 1 (aceptado = información de contacto)
21
El usuario 2 puede ver la solicitud (ventana emergente)
23

Fig. 3R

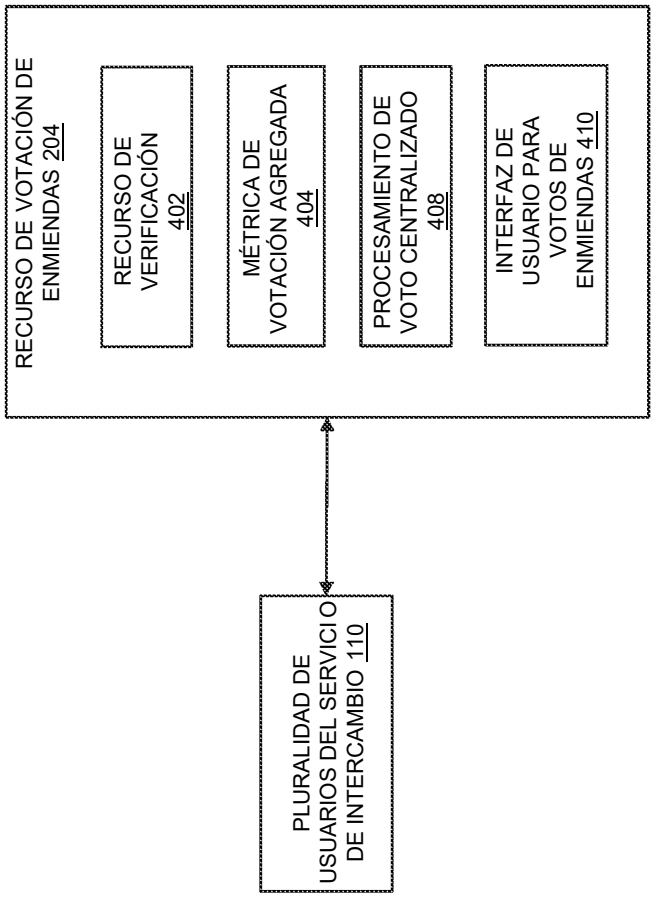

RECURSO DE VOTACIÓN DE ENMIENDAS 204
RECURSO DE VERIFICACIÓN 402
MÉTRICA DE VOTACIÓN AGREGADA 404
PROCESAMIENTO DE VOTO CENTRALIZADO 408
INTERFAZ DE USUARIO PARA VOTOS DE ENMIENDAS 410
PLURALIDAD DE USUARIOS DEL SERVICIO DE INTERCAMBIO 110

Fig. 4

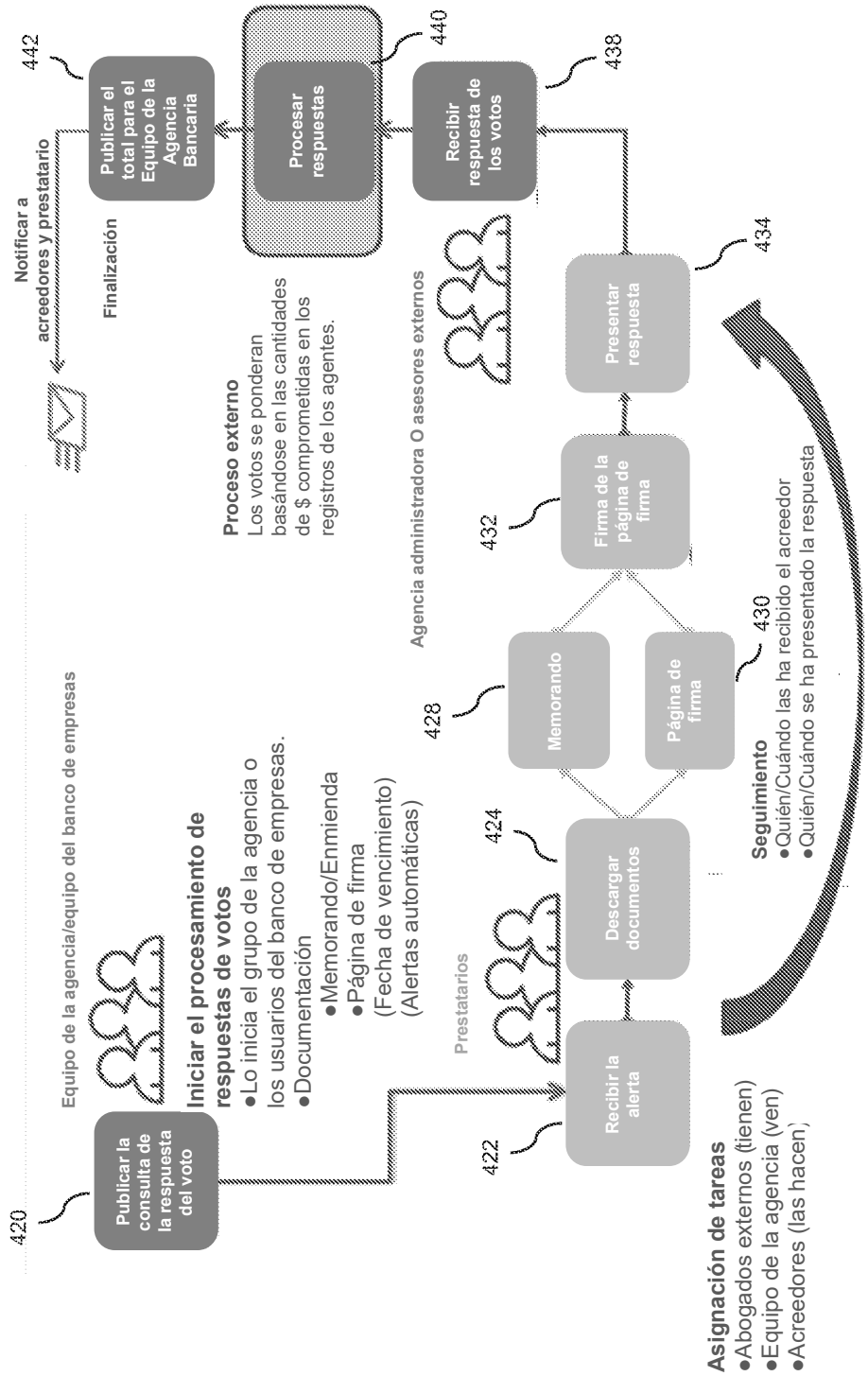

420
Publicar la consulta de la respuesta del voto
Equipo de la agencia/equipo del banco de empresas
Iniciar el procesamiento de respuestas de votos
●Lo inicia el grupo de la agencia o los usuarios del banco de empresas.
●Documentación
●Memorando/Enmienda
●Página de firma
(Fecha de vencimiento)
(Alertas automáticas)
422
Recibir la alerta
Prestatarios
424
Descargar documentos
428
Memorando
Página de firma
430
Seguimiento
●Quién/Cuándo las ha recibido el acreedor
●Quién/Cuándo se ha presentado la respuesta
Asignación de tareas
●Abogados externos (tienen)
●Equipo de la agencia (ven)
●Acreedores (las hacen)
432
Firma de la página de firma
Agencia administradora O asesores externos
434
Presentar respuesta
438
Recibir respuesta de los votos
440
Procesar respuestas
Proceso externo
Los votos se ponderan basándose en las cantidades de $ comprometidas en los registros de los agentes.
442
Publicar el total para el Equipo de la Agencia Bancaria
Finalización
Notificar a acreedores y prestatario

Fig. 4A

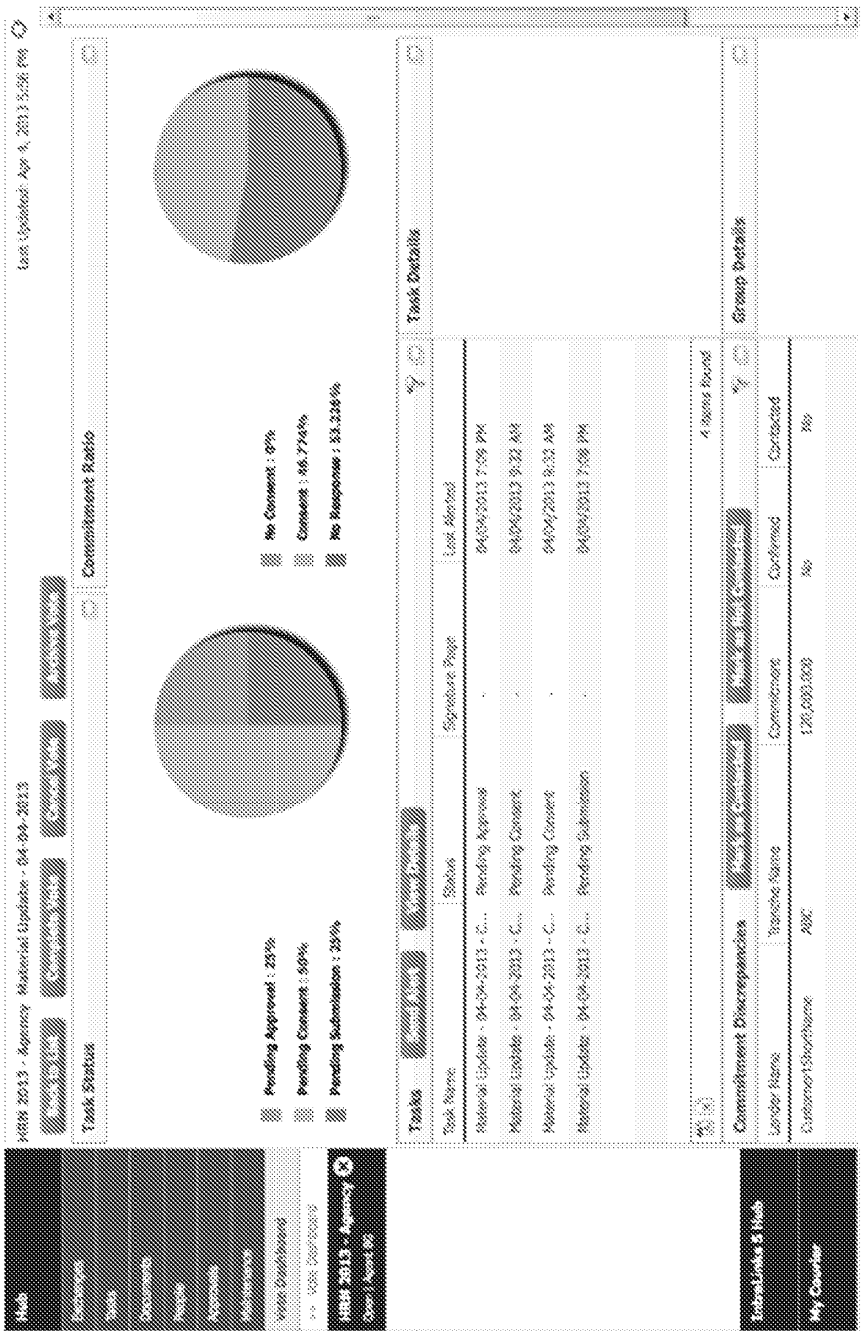

Task Status
Pending Approval : 33%
Pending Consent : 16%
Pending Submission : 33%
No Comment : 0%
Contact : 16.774%
No Response : 33.334%
Tasks
Task Details
Commitment Discrepancies
Group Details

Fig. 4B

From: NAME, EMAIL,
Subject: Business process assignment alert
Date: March 27, 2013 5:10:28 PM EDT
To: NAME, EMAIL,
Reply-To: NAME, EMAIL,
Hide
Log into the Service
Amend & Extend - 03.2013 has been assigned to you.
Exchange:AMEN 2013 - Agency
Business Process Name: Amend & Extend - 03.2013
NAME
A task has been assigned to you. Log into IntraLinks and check your task list.
Task Name: Pending Consent
Link: <LINK>
Contact IntraLinks Support:
CONTACT INFORMATION
Quick Links:
Alert Settings
Email Support
Retrieve Your Password

Fig. 4C

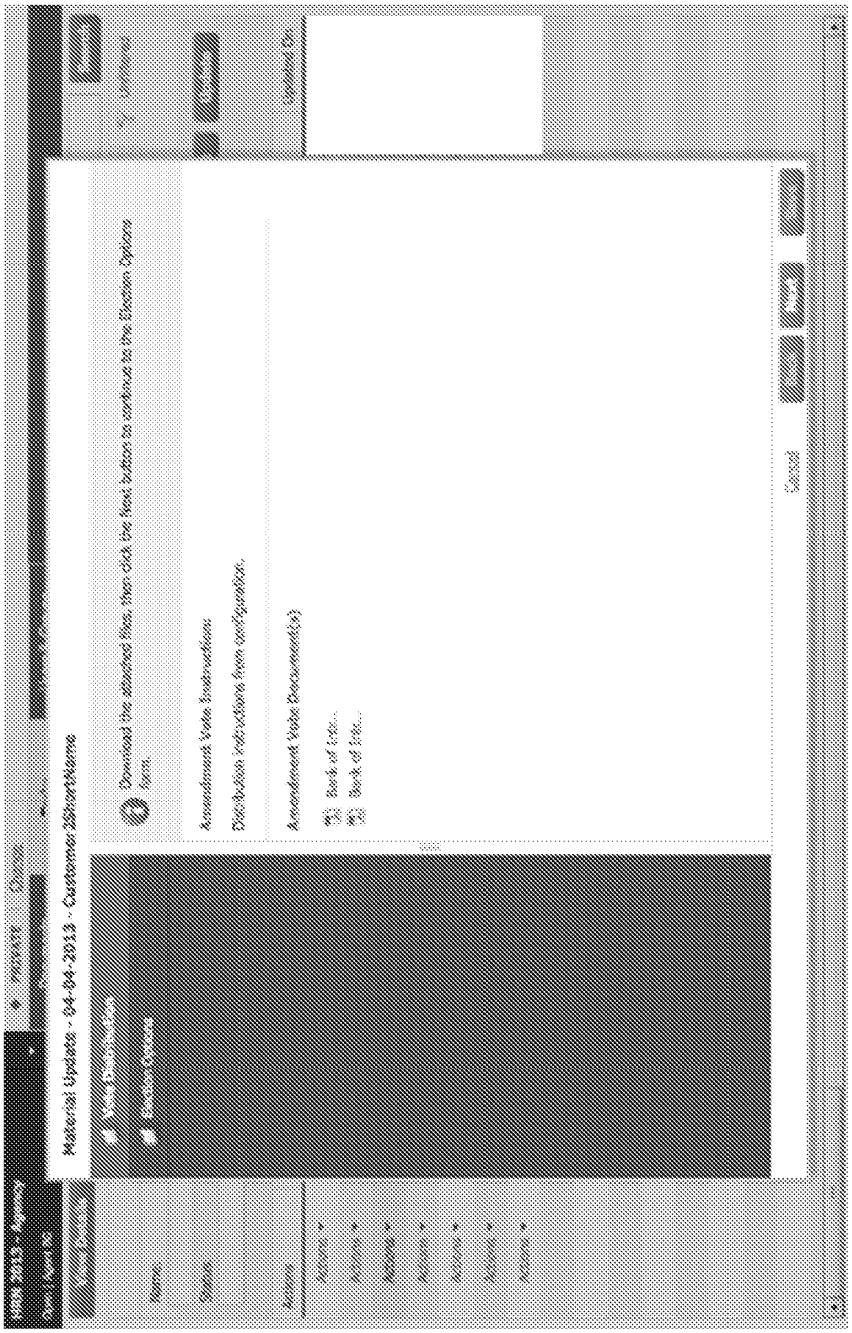

Material Update - 04-04-2013 - Customer Shareholders
Vote Instruction
Amendment Vote Instruction
Amendment Vote Document(s)
Bank of Inv...
Bank of Inv...
Cancel

Fig. 4D

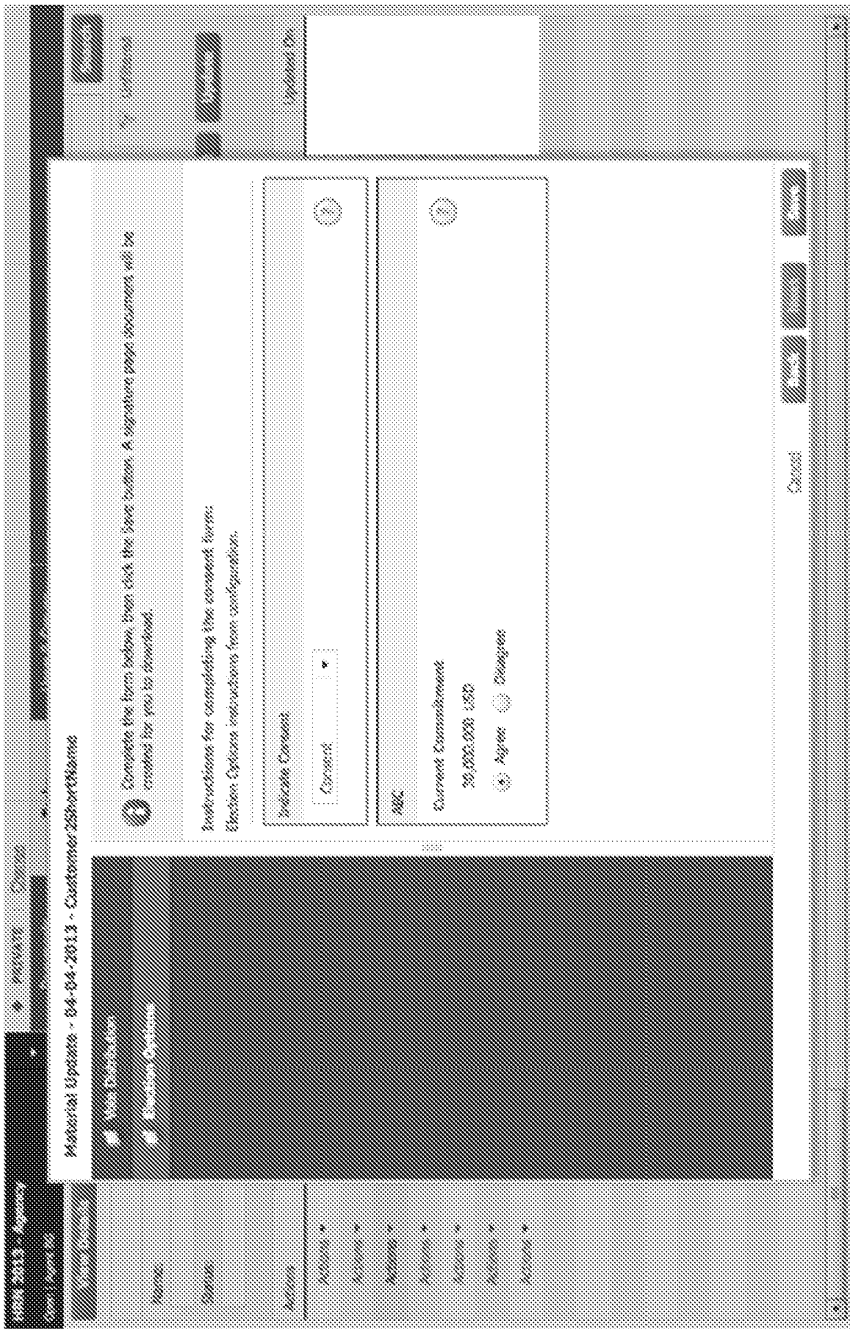

Material Update - 04-04-2013 - Customer2ShortName
Compete the form below, then click the Save button. A signature page document will be created for you to download.
Instructions for completing the consent form:
Election Options instructions from configuration.
Select Consent
Consent
ABC
Current Commitment
30,000,000 USD
Agree
Delegate
Cancel
Save
Upload File

Fig. 4E

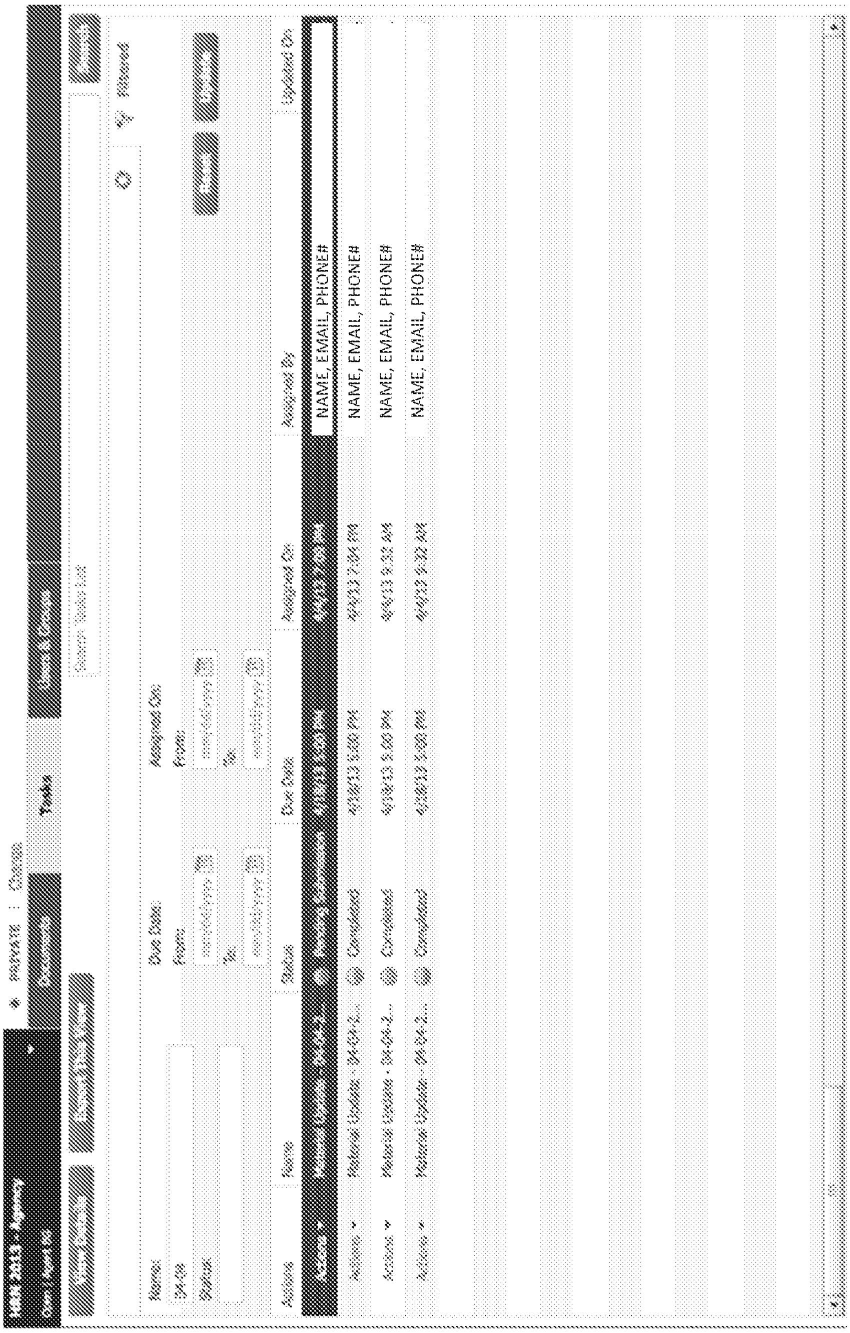

NAME, EMAIL, PHONE#
NAME, EMAIL, PHONE#
NAME, EMAIL, PHONE#
NAME, EMAIL, PHONE#

Fig. 4F

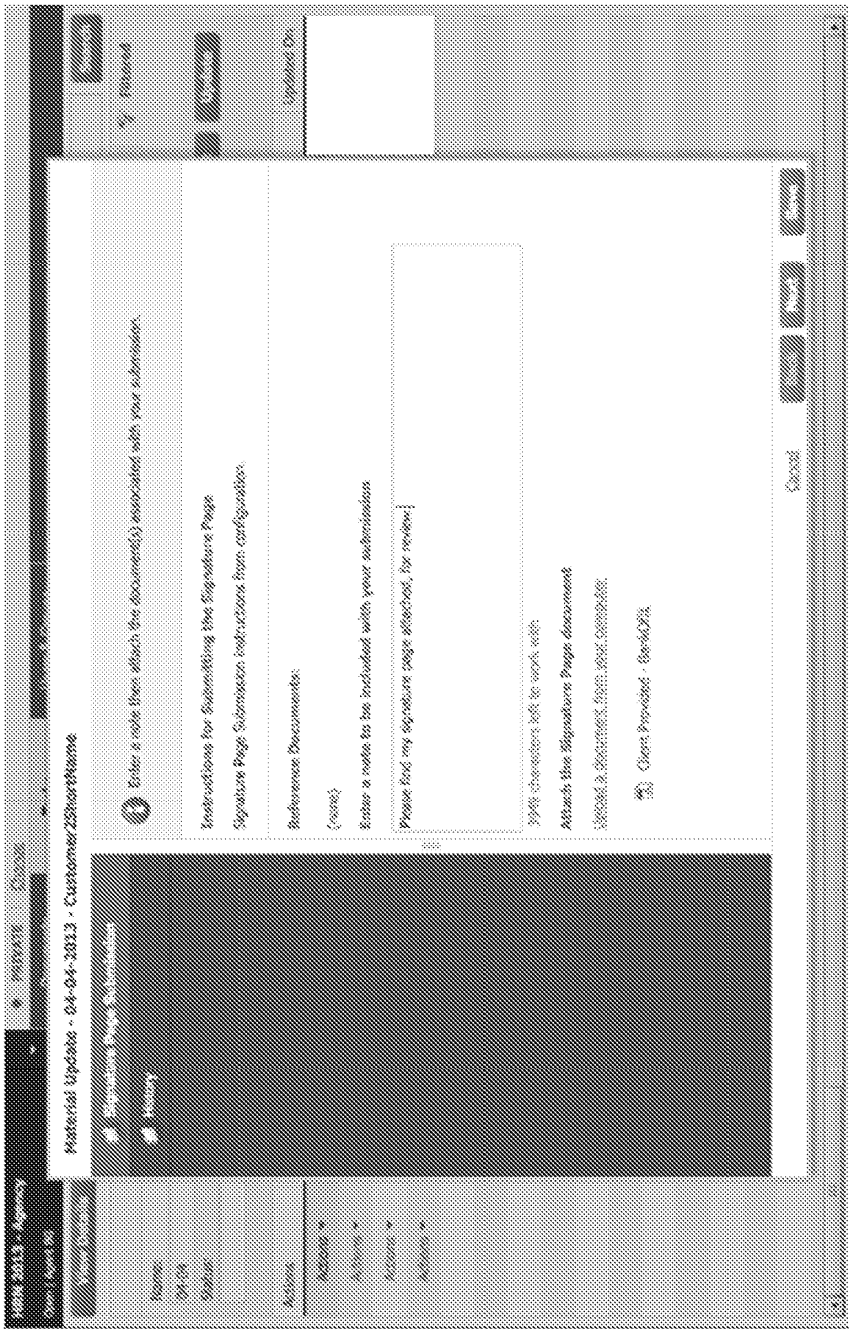


Fig. 4G


Tasks
Actions
Name
Status
Due Date
Assigned On
Assigned To
Updated On
NAME, EMAIL, PHONE#
Completed
Cancelled

Fig. 4H

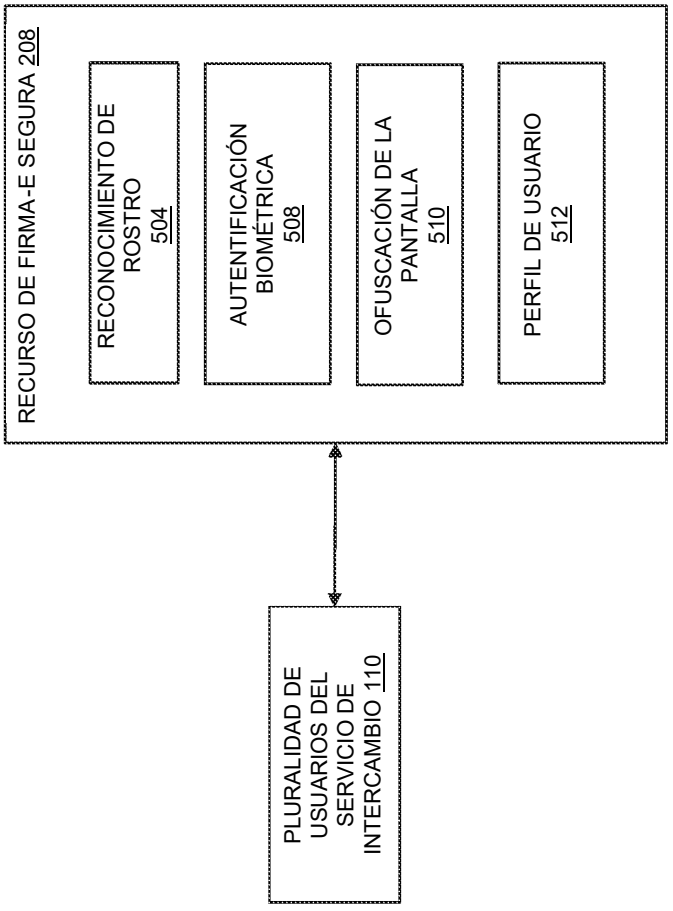
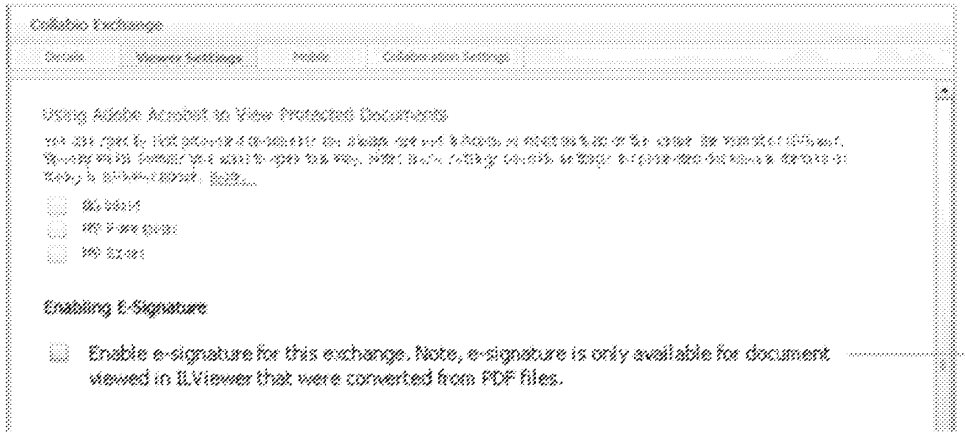

RECURSO DE FIRMA-E SEGURA 208
RECONOCIMIENTO DE ROSTRO 504
AUTENTIFICACIÓN BIOMÉTRICA 508
OFUSCACIÓN DE LA PANTALLA 510
PERFIL DE USUARIO 512
PLURALIDAD DE USUARIOS DEL SERVICIO DE INTERCAMBIO 110

Fig. 5

Hay dos tareas de usuario:
1. Activar una firma electrónica para un intercambio
2. Firmar electrónicamente un documento.

Activar la firma electrónica para un intercambio



La casilla para **Activar la firma electrónica para un documento** en los ajustes de Ajustes de Visualización del Intercambio activa una firma-e para el intercambio y posibilita que la firma-e esté desactivada si es necesario.

Fig. 5A

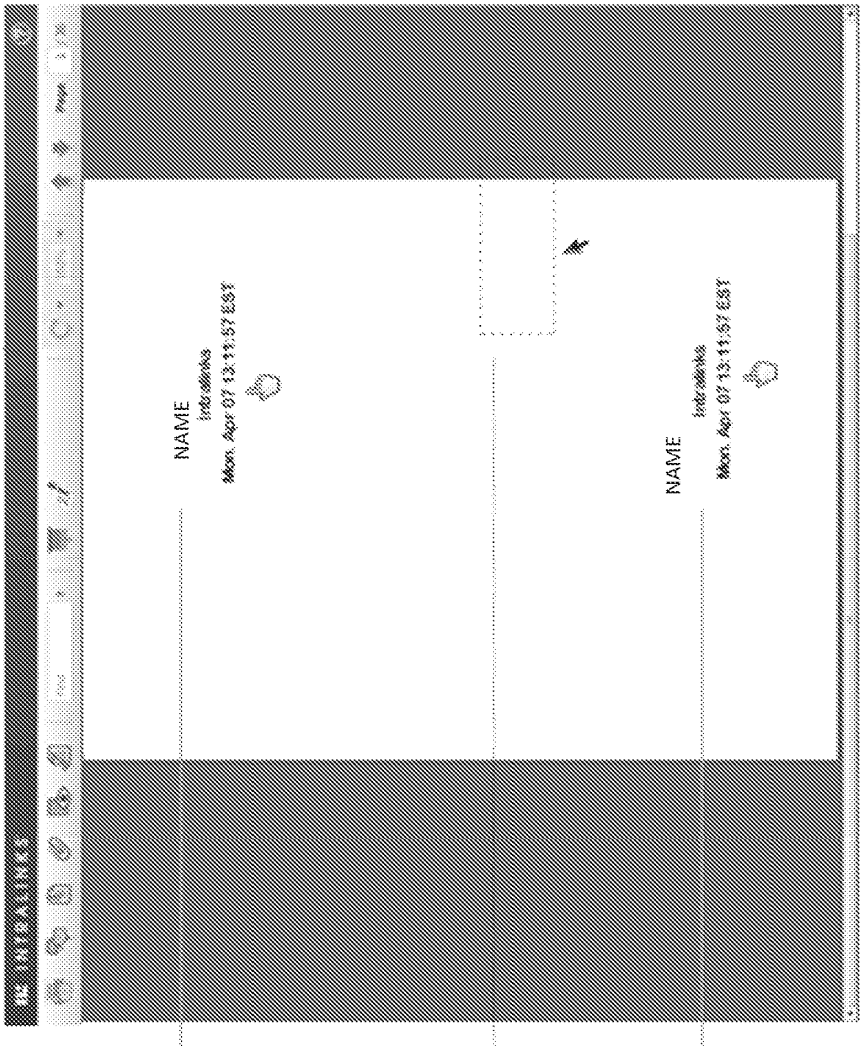
Firma electrónica de un documento (1 de 4)

1. La barra de herramientas aparece con el icono de firmae si la firma-e se ha activado en las propiedades. Si no, no aparecerá. Nótese que también se ha añadido un botón de Guardar. Guardar estará desactivado hasta que se haya aplicado al menos una firma.

2.El usuario hace clic en el icono de firma-e. El icono se activa y aparece una ventana emergente para empezar con la firmæ. Los usuarios pueden volver a hacer clic enel icono para desactivar la firma electrónica y cancelar el proceso de firma actual. Nota: los controles de rotar y ampliar están desactivados. Estas funciones, cuando están activadas, no muestran con exactitud cómo será la firma cuando se aplique.

3. El usuario lee las instrucciones y hace clic en OK.

Fig. 5B



4. Una vez que el usuario hace clic en «OK», aparece la firma con el cursor estilo mano. El usuario puede mover la firma arrastrando el ratón.

Nótese que el usuario puede tener una interacción limitada con la barra de herramientas y la barra de desplazamiento. Pueden utilizar buscar, ampliar, rotar, avanzar y retroceder página. Las demás funciones cancelarán la firma.

Si cualquier parte del cursor sale del área del documento, la firma desaparecerá y el cursor volverá a su estado por defecto. Esto asegura que la firma entera puede verse en el documento.

5. El usuario hace clic en el botón del ratón para aplicar la firma.

Fig. 5C

6. Aparece la siguiente ventana emergente.

Si el usuario selecciona «Sí», desaparece la ventana emergente de Confirmación de la Firma Electrónica y procede al paso 7.

Si el usuario selecciona «No», el usuario vuelve al paso 4 y se le permite volver a colocar la firma.

7. La firma se aplica, el botón de firma pasa de activarse a desactivarse y el botón de «Guardar» pasa a estar activo.

Fig. 5D

Si el usuario hace clic en «Guardar»…

Si el usuario hace clic en Guardar, el ILV empezará a guardar el fichero. Aparecerá una ventana emergente con animación informando al usuario que pueden esperar o cerrar el ILV.

Fig. 5E

Si el usuario cierra la ventana del navegador y hay cambios sin guardar…

Si hay cambios sin guardar en el ILV y el usuario intenta cerrar la ventana del navegador, aparecerá una ventana emergente que notificará al usuario de que hay cambios sin guardar y le preguntará si quieren guardarlos o cerrar sin guardar.

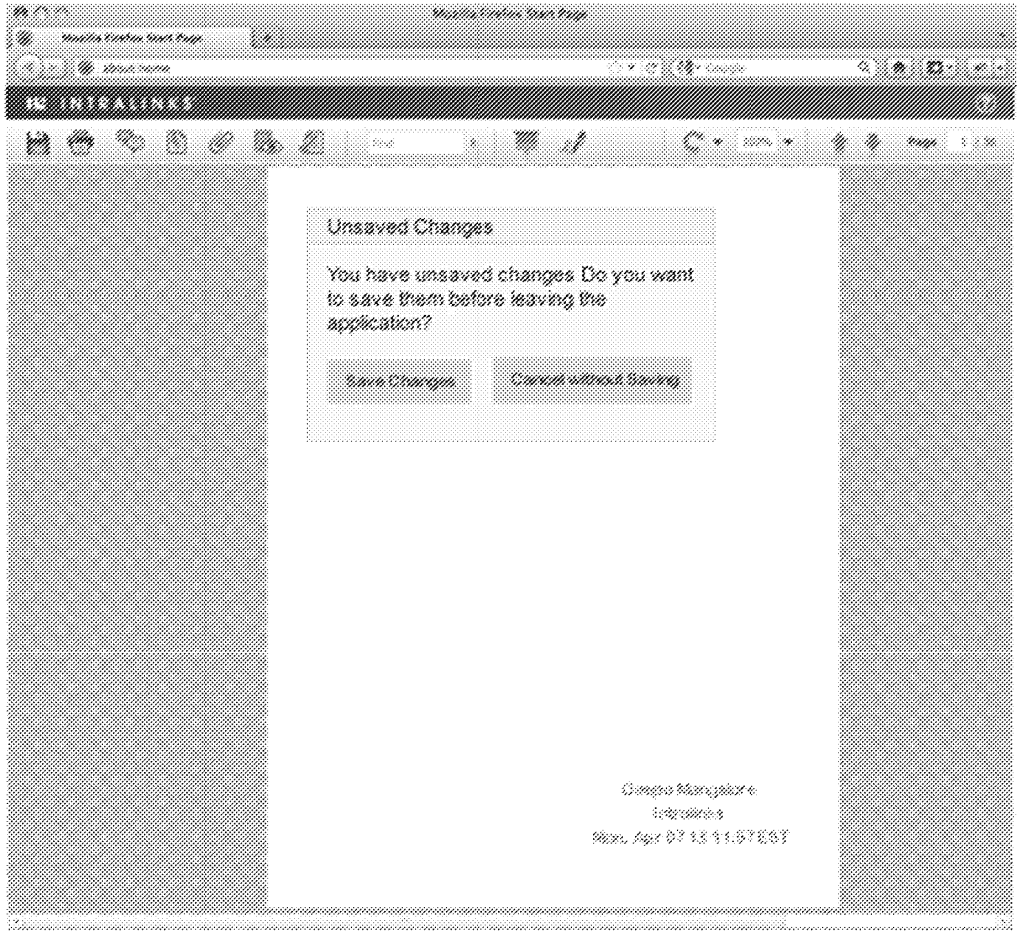
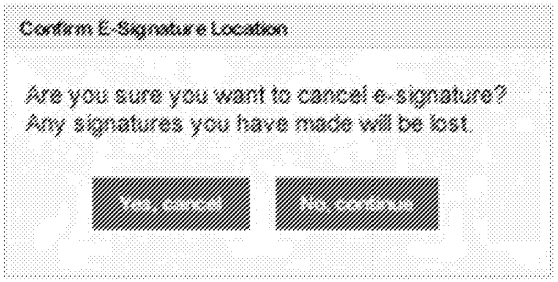


Fig. 5F

Cancelar la firma electrónica

Si el usuario intenta cancelar la firma electrónica, aparecerá la siguiente ventana emergente:



Al volver a hacer clic en el botón de firma electrónica, (cuando está activado).

Al hacer clic en cualquiera de los siguientes iconos de la barra de tareas: imprimir, comentario, marcador, informe sobe el acceso, rotar y ampliar, se desactivará.

Fig. 5G

ES 2 676 693 T3

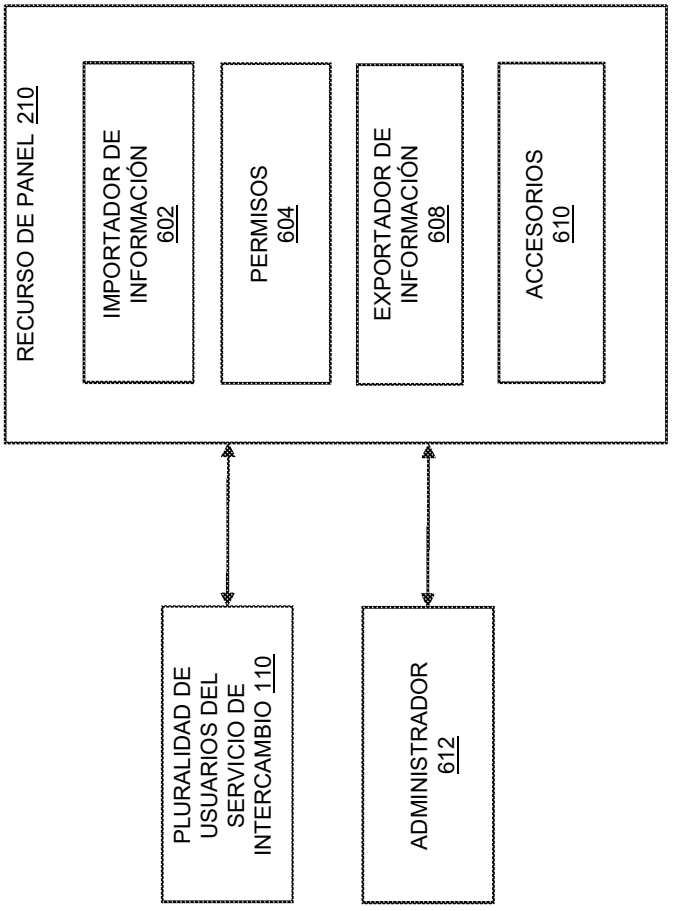

RECURSO DE PANEL 210
IMPORTADOR DE INFORMACIÓN 602
PERMISOS 604
EXPORTADOR DE INFORMACIÓN 608
ACCESORIOS 610
PLURALIDAD DE USUARIOS DEL SERVICIO DE INTERCAMBIO 110
ADMINISTRADOR 612

Fig. 6

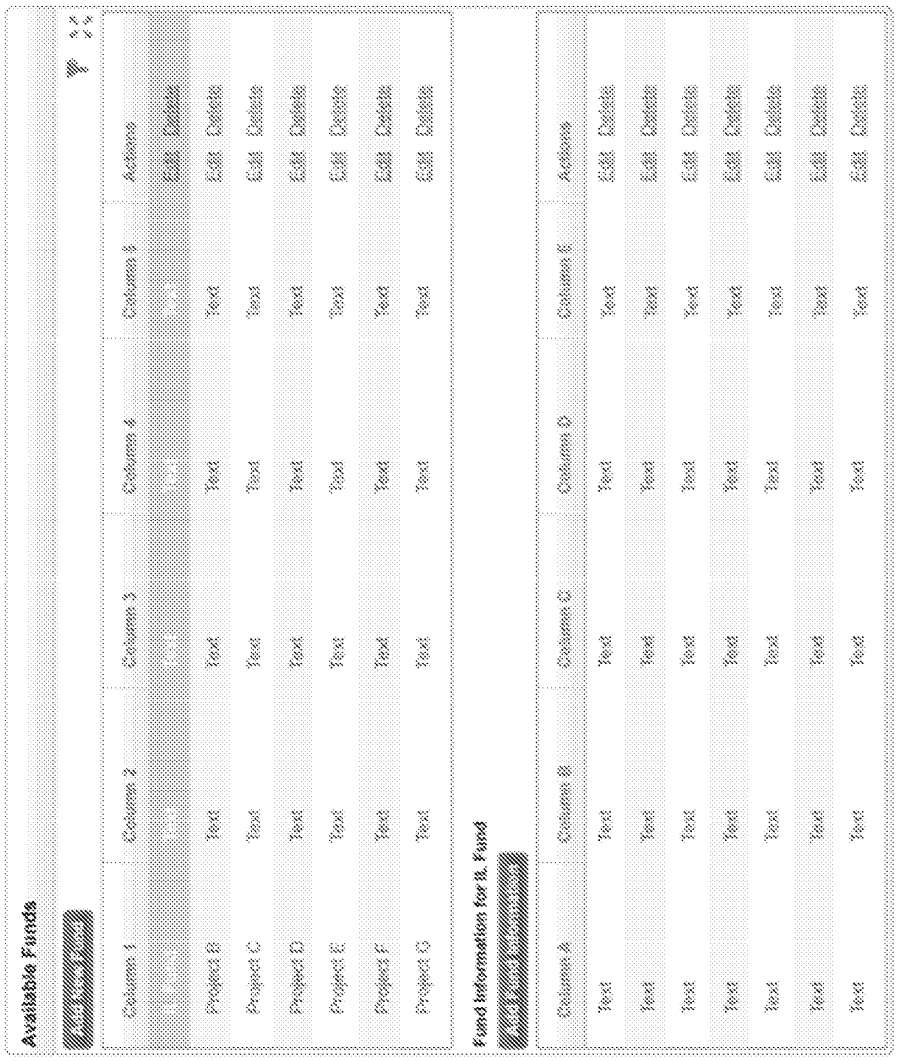

Available Funds
Column 1
Column 2
Column 3
Column 4
Column 5
Actions
Edit
Delete
Project B
Project C
Project D
Project E
Project F
Project G
Text
Fund Information for B. Fund
Column A
Column B
Column C
Column D
Column E
Column F

Fig. 6A

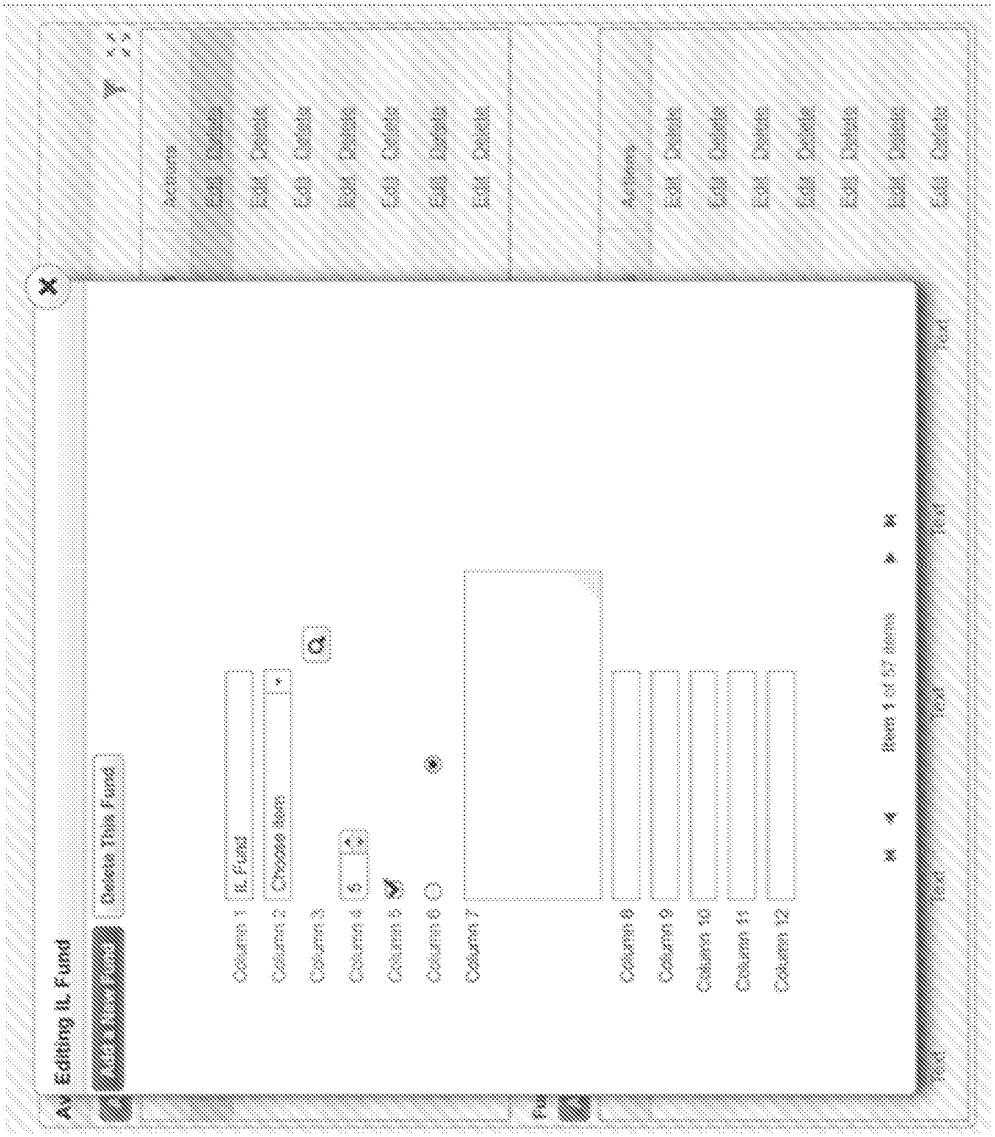

All Editing IL Fund
Delete This Fund
Actions
Edit Delete
IL Fund
Choose Item
Column 1
Column 2
Column 3
Column 4
Column 5
Column 6
Column 7
Column 8
Column 9
Column 10
Column 11
Column 12
Item 1 of 67 Items

Fig. 6B

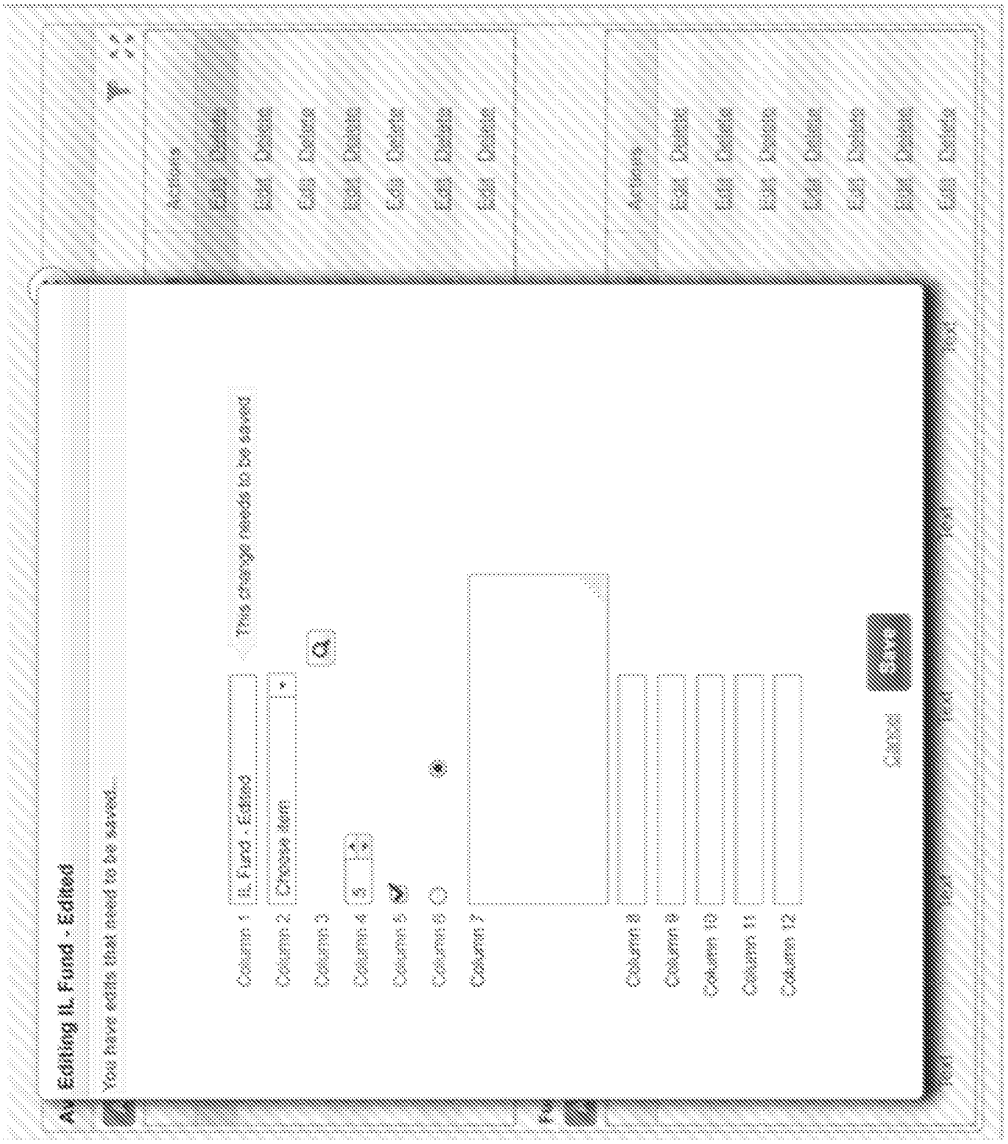

Editing IL Fund - Edited
You have edits that need to be saved...
Actions
Edit Delete
IL Fund - Edited
Choose item
You change needs to be saved
Column 1
Column 2
Column 3
Column 4
Column 5
Column 6
Column 7
Column 8
Column 9
Column 10
Column 11
Column 12
Cancel
Save

Fig. 6C

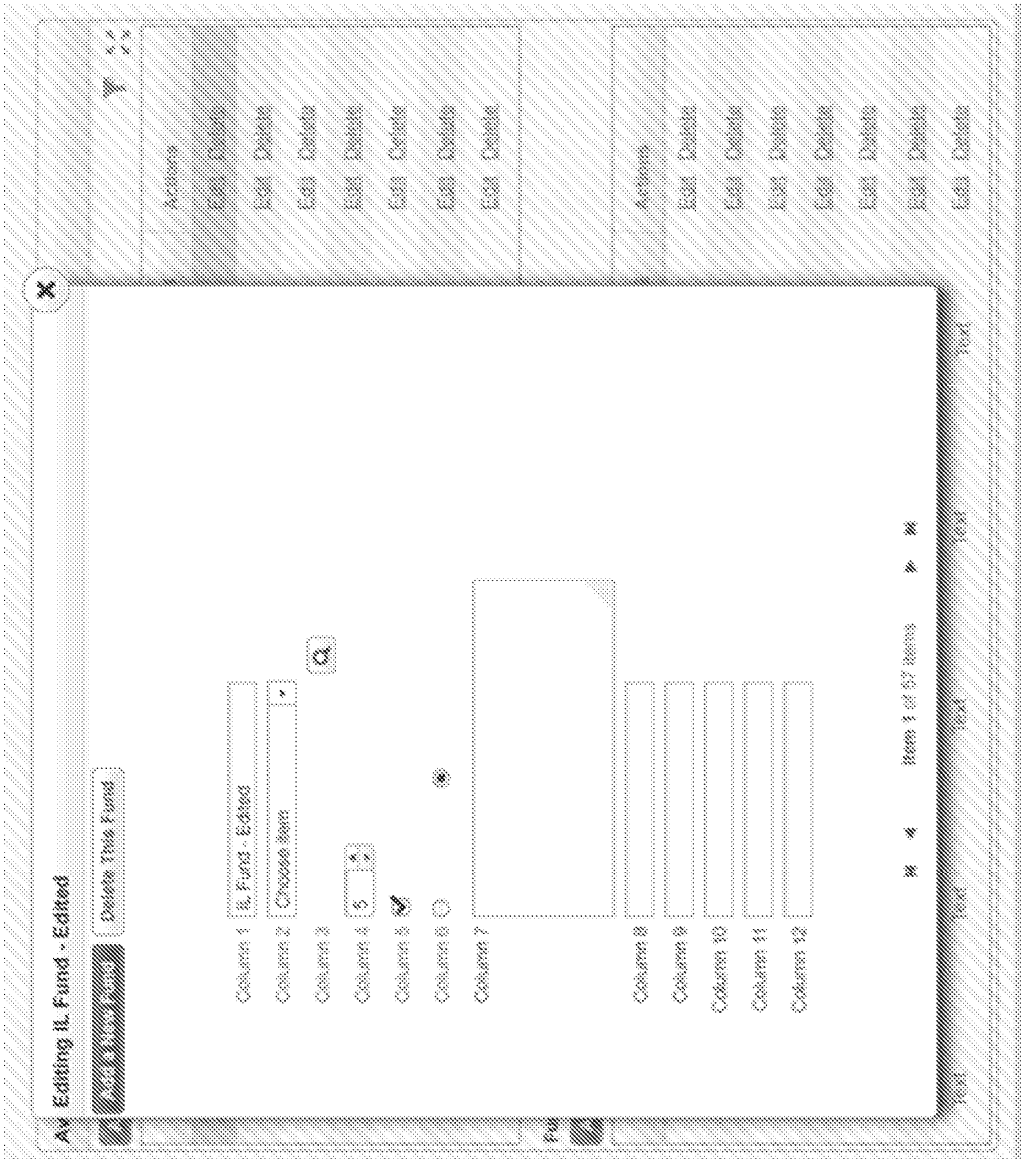

Editing IL Fund - Edited
Delete This Fund
Actions
Edit Delete
Column 1
IL Fund - Edited
Column 2
Choose Item
Column 3
Column 4
5
Column 5
Column 6
Column 7
Column 8
Column 9
Column 10
Column 11
Column 12
Item 1 of 67 Items

Fig. 6D

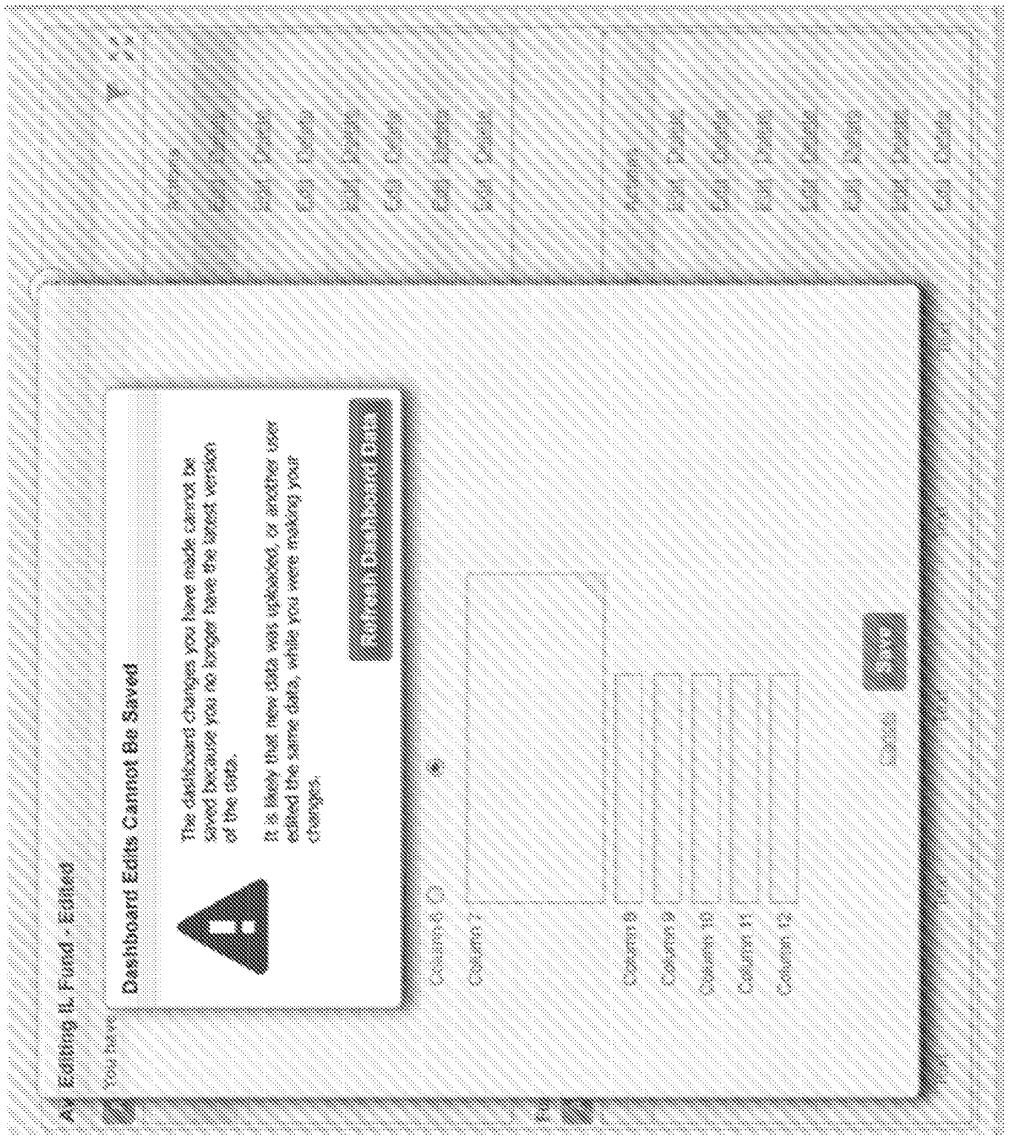

Editing IL Fund - Edited
You have
Dashboard Edits Cannot Be Saved
The dashboard changes you have made cannot be saved because you no longer have the latest version of the data.
It is likely that new data was uploaded, or another user edited the same data, while you were making your changes.
Column 0
Column 7
Column 8
Column 9
Column 10
Column 11
Column 12
Cancel
OK

Fig. 6E

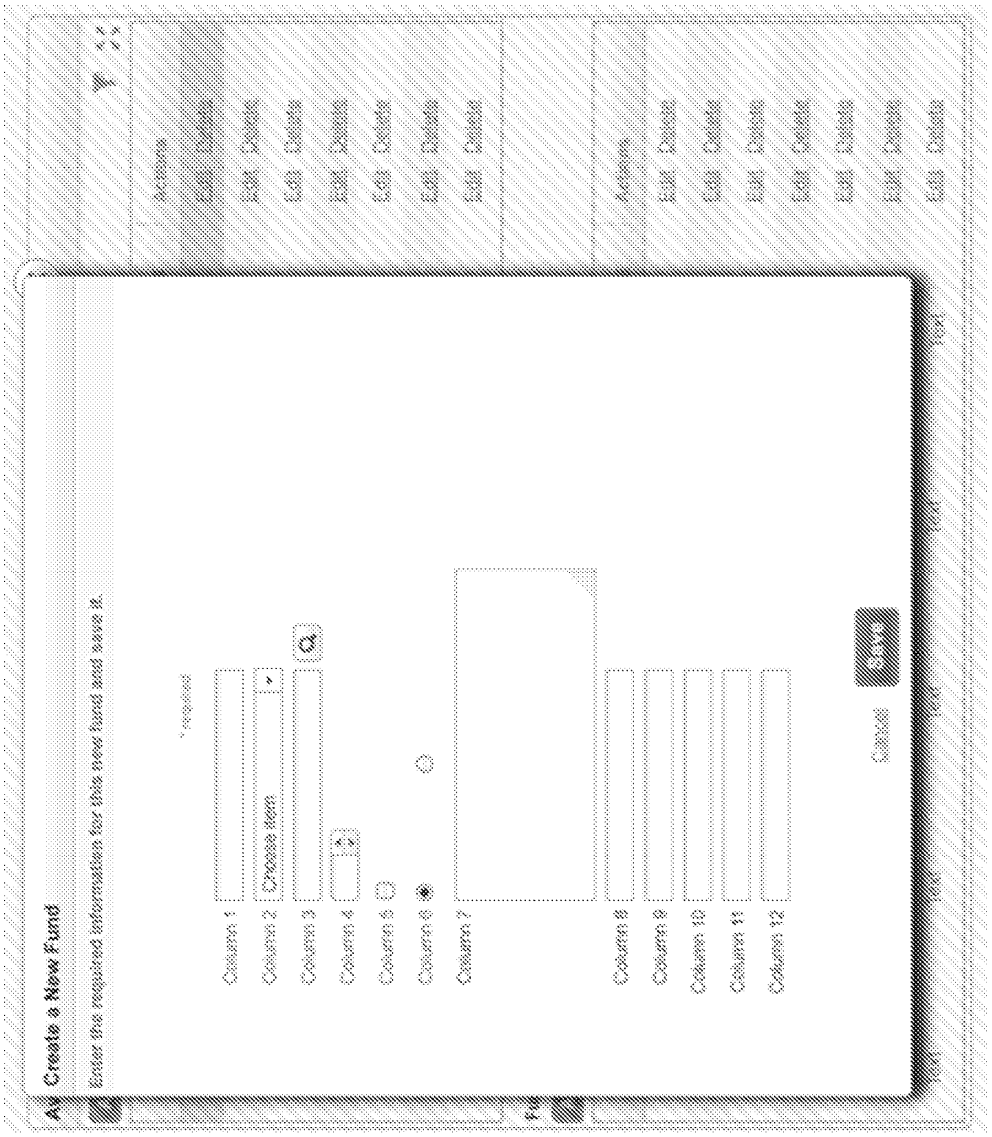

Create a New Fund
Enter the required information for this new fund and save it.
Column 1
Column 2
Choose item
Column 3
Column 4
Column 5
Column 6
Column 7
Column 8
Column 9
Column 10
Column 11
Column 12
Cancel
Save
Actions
Edit Details

Fig. 6F


Attach a Document to IL Fund > Financials
Browse for the file you want to attach to this record and click 'Select'
Exchange List
Search this list...
Search
Exchange Name
First
Phone
MG exchange 1
MG exchange 2
MG exchange 3
MG exchange 4
MG exchange 5
MG exchange 6
MG exchange 7
MG exchange 8
MG exchange 9
MG exchange 10
MG exchange 11
MG exchange 12
Actions
Edit Delete
Cancel
Select

Fig. 6G

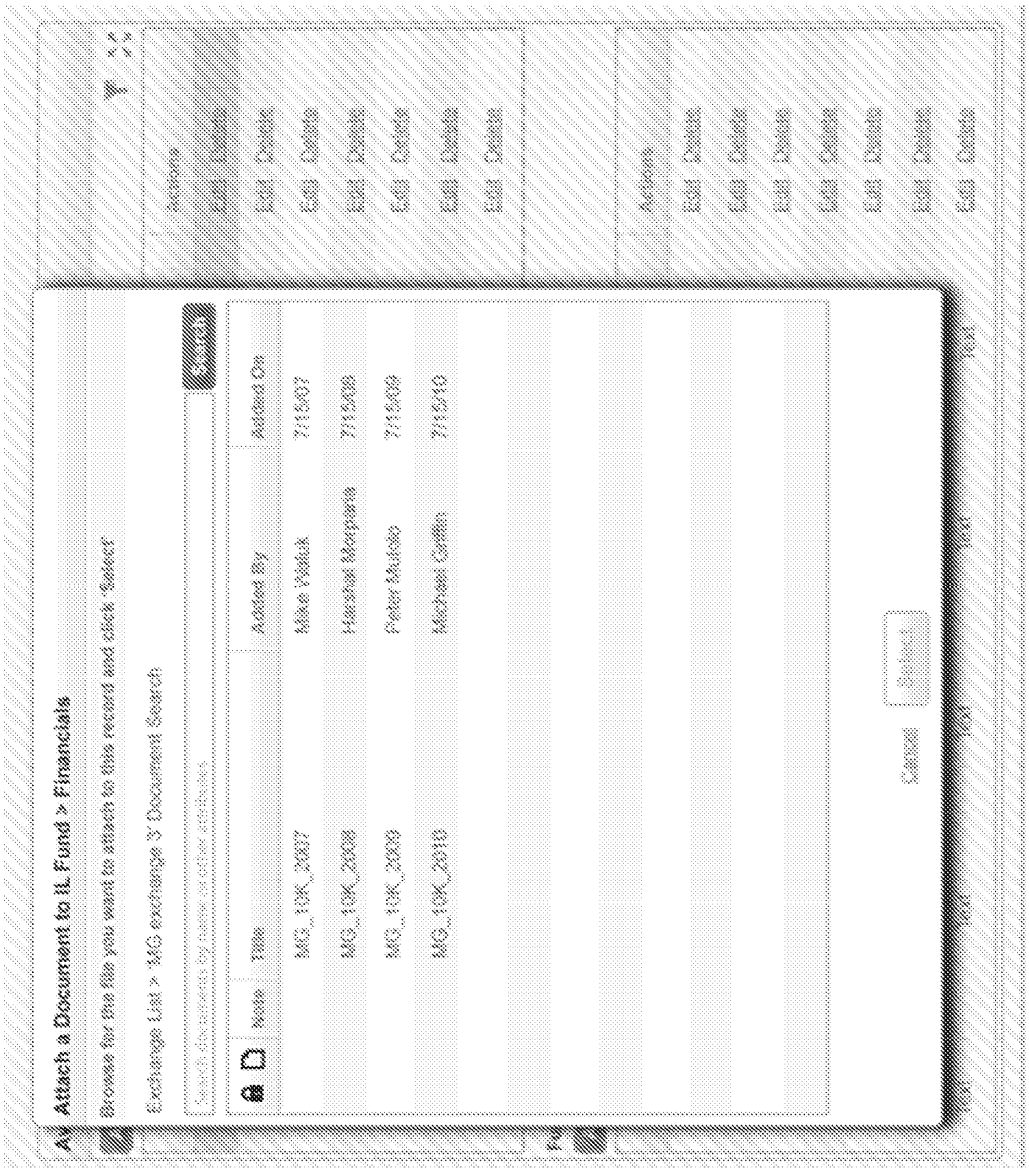

Attach a Document to IL Fund > Financials
Browse for the file you want to attach to this record and click 'Select'
Exchange List > MG exchange 3 Document Search
Search
Title
Added By
Added On
MG_10K_2007
Mike Wallak
7/15/07
MG_10K_2008
Harshal Manjrekar
7/15/08
MG_10K_2009
Peter Mullally
7/15/09
MG_10K_2010
Michael Griffin
7/15/10
Actions
Edit Delete
Cancel
Select

Fig. 6H

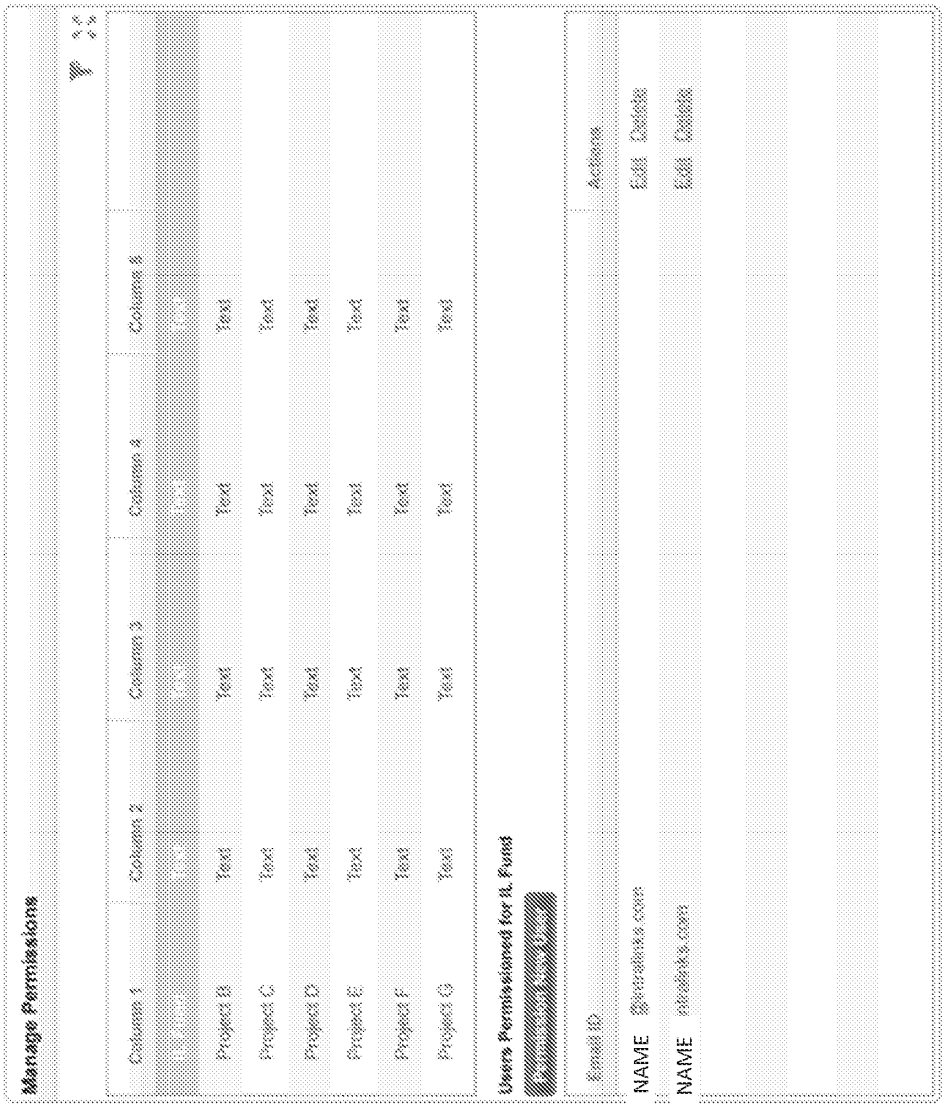

Manage Permissions
Column 1
Column 2
Column 3
Column 4
Column 5
Column 6
Project B
Project C
Project D
Project E
Project F
Project G
Text
Users Permissioned for it Fund
Email ID
Actions
NAME
Edit
Delete

Fig. 6l

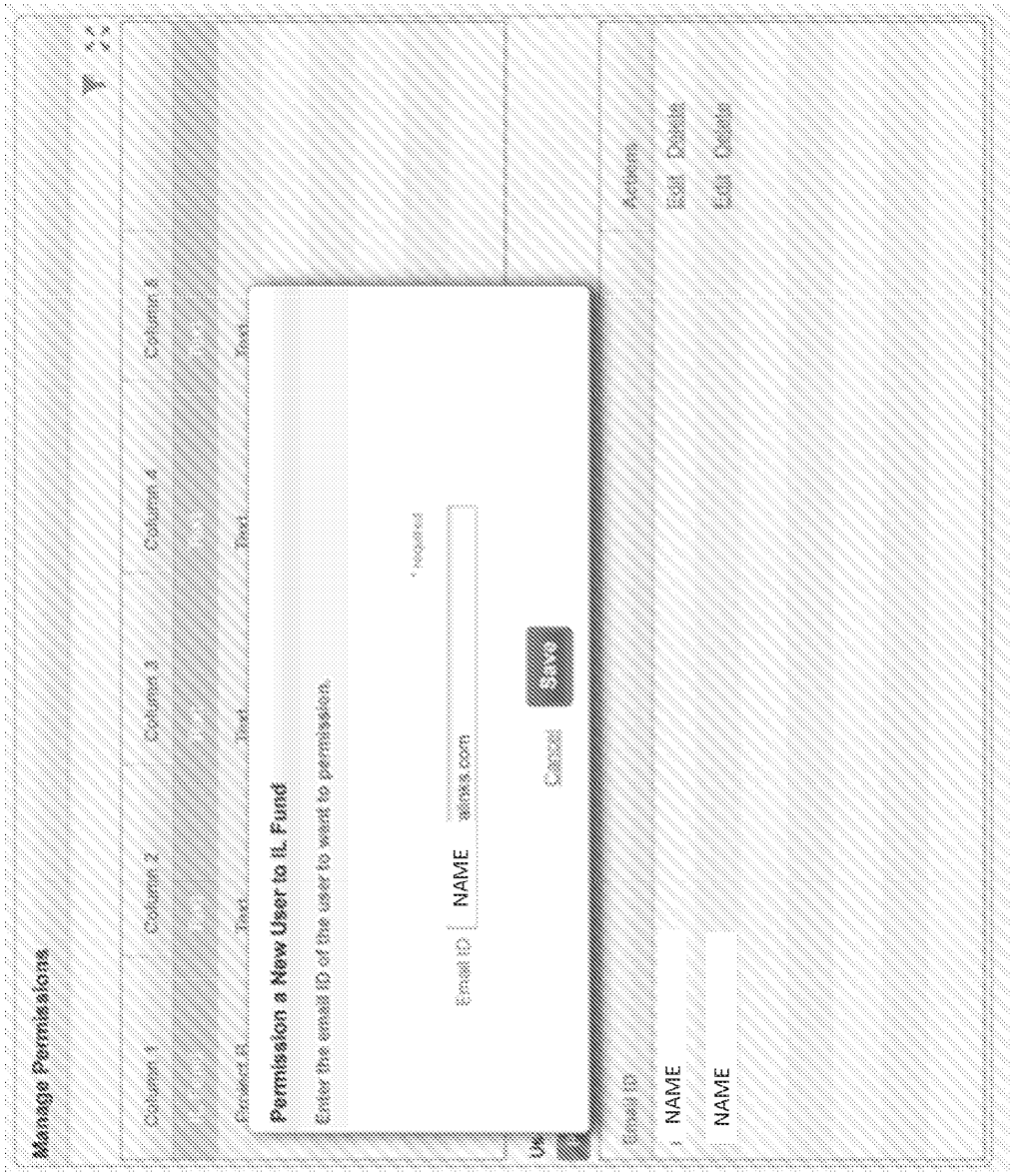

Manage Permissions
Permission a New User to IL Fund
Enter the email ID of the user to want to permission.
Email ID
NAME
Cancel
Submit
Actions
Edit Delete
Edit Delete
NAME
NAME

Fig. 6J

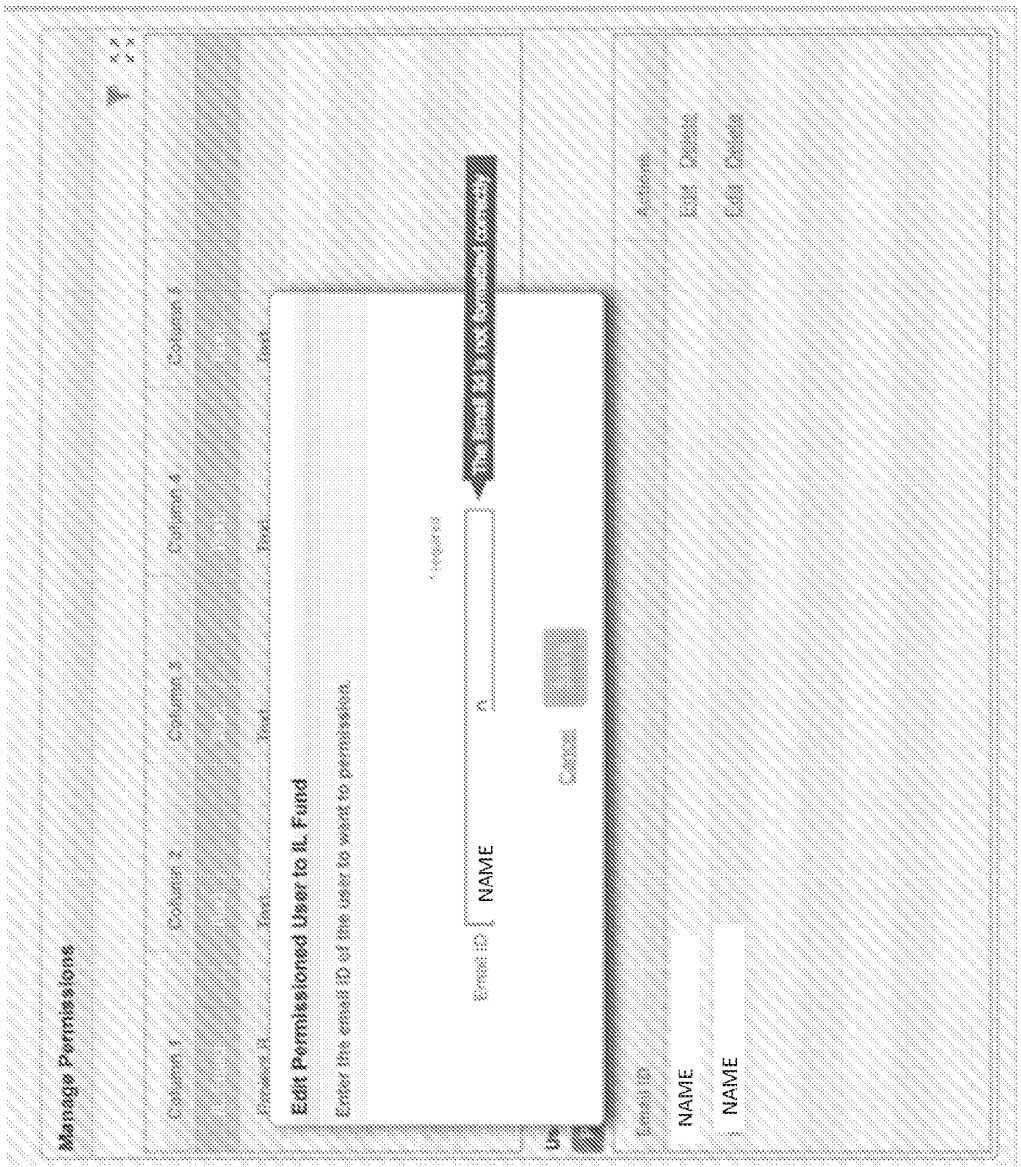

Manage Permissions
Edit Permissioned User to IL Fund
Enter the email ID of the user to want to permission.
Email ID
NAME
Cancel
NAME
NAME

Fig. 6K

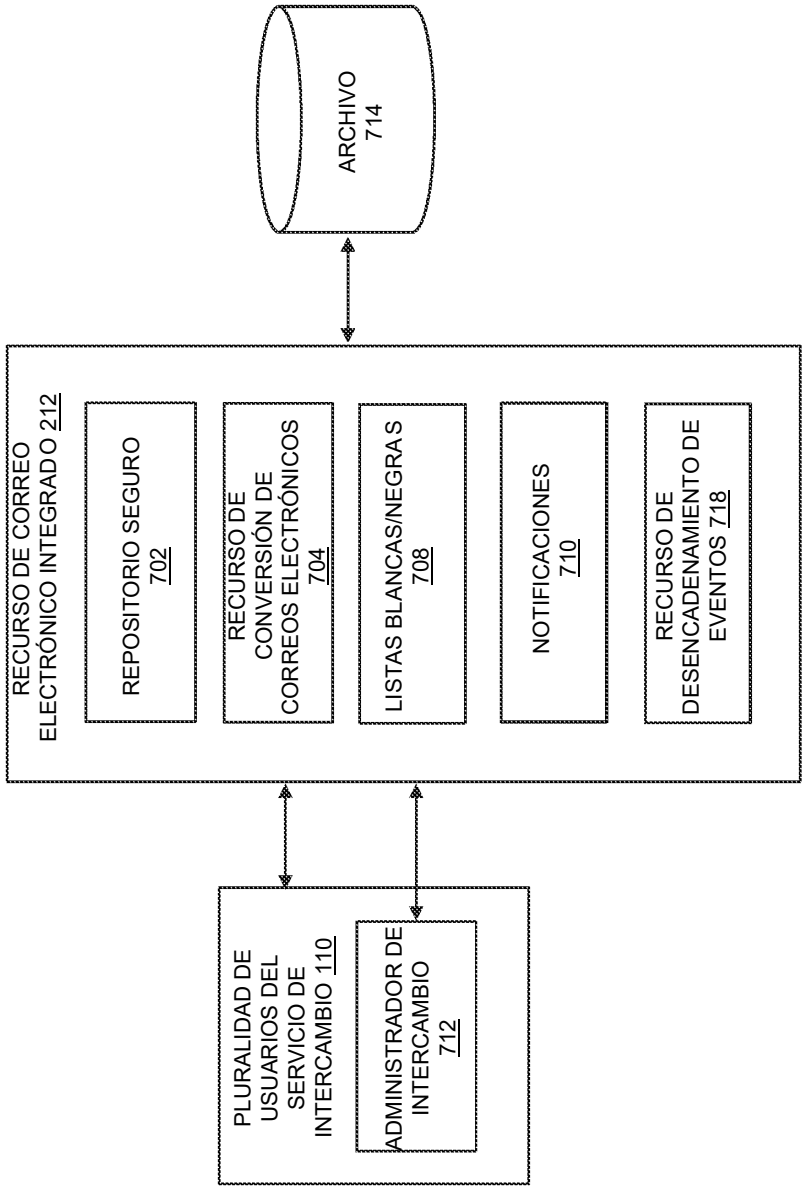

ARCHIVO
714
RECURSO DE CORREO ELECTRÓNICO INTEGRADO 212
REPOSITORIO SEGURO
702
RECURSO DE CONVERSIÓN DE CORREOS ELECTRÓNICOS
704
LISTAS BLANCAS/NEGRAS
708
NOTIFICACIONES
710
RECURSO DE DESENCADENAMIENTO DE EVENTOS 718
PLURALIDAD DE USUARIOS DEL SERVICIO DE INTERCAMBIO 110
ADMINISTRADOR DE INTERCAMBIO
712

Fig. 7

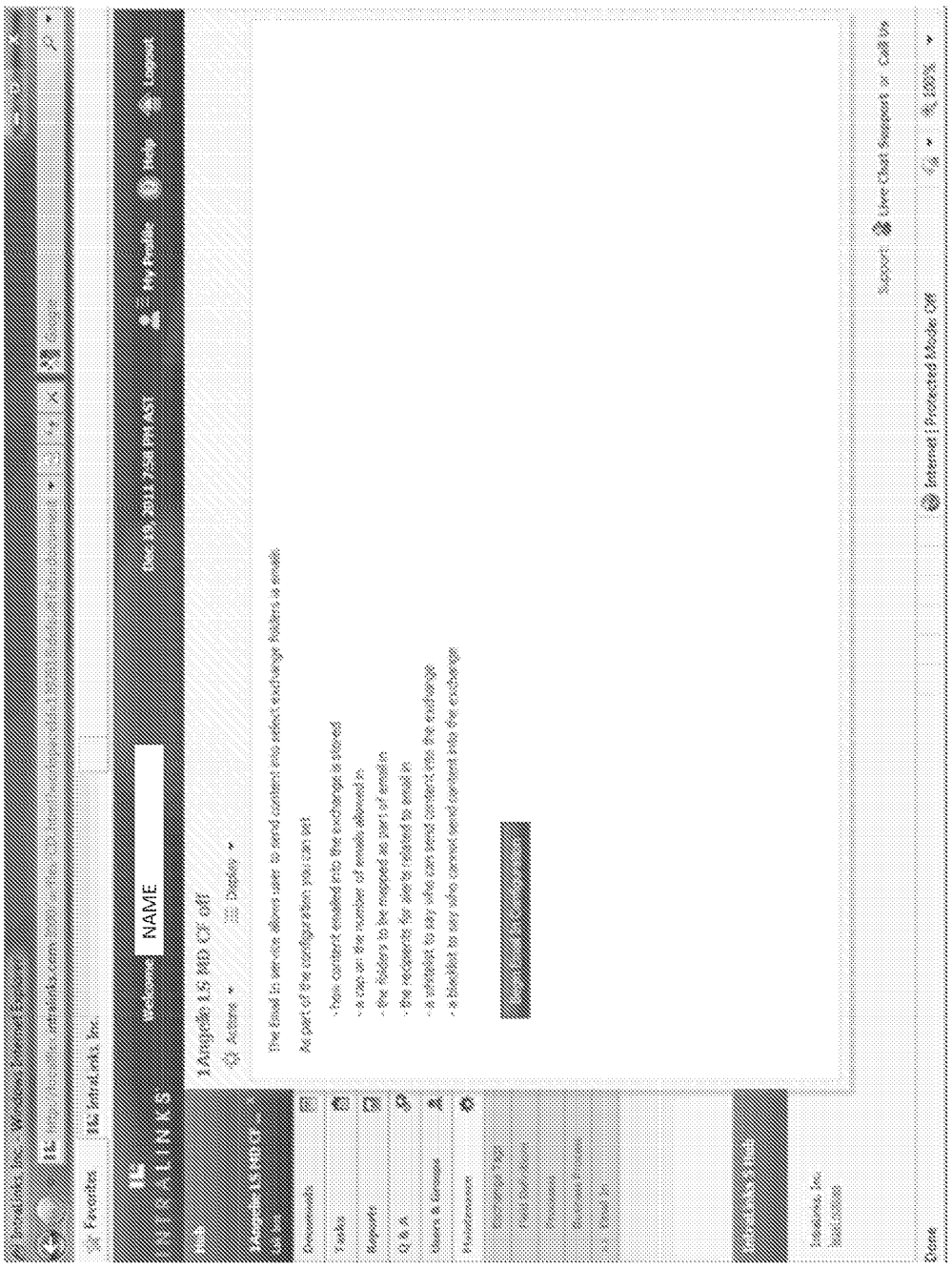


Fig. 7A

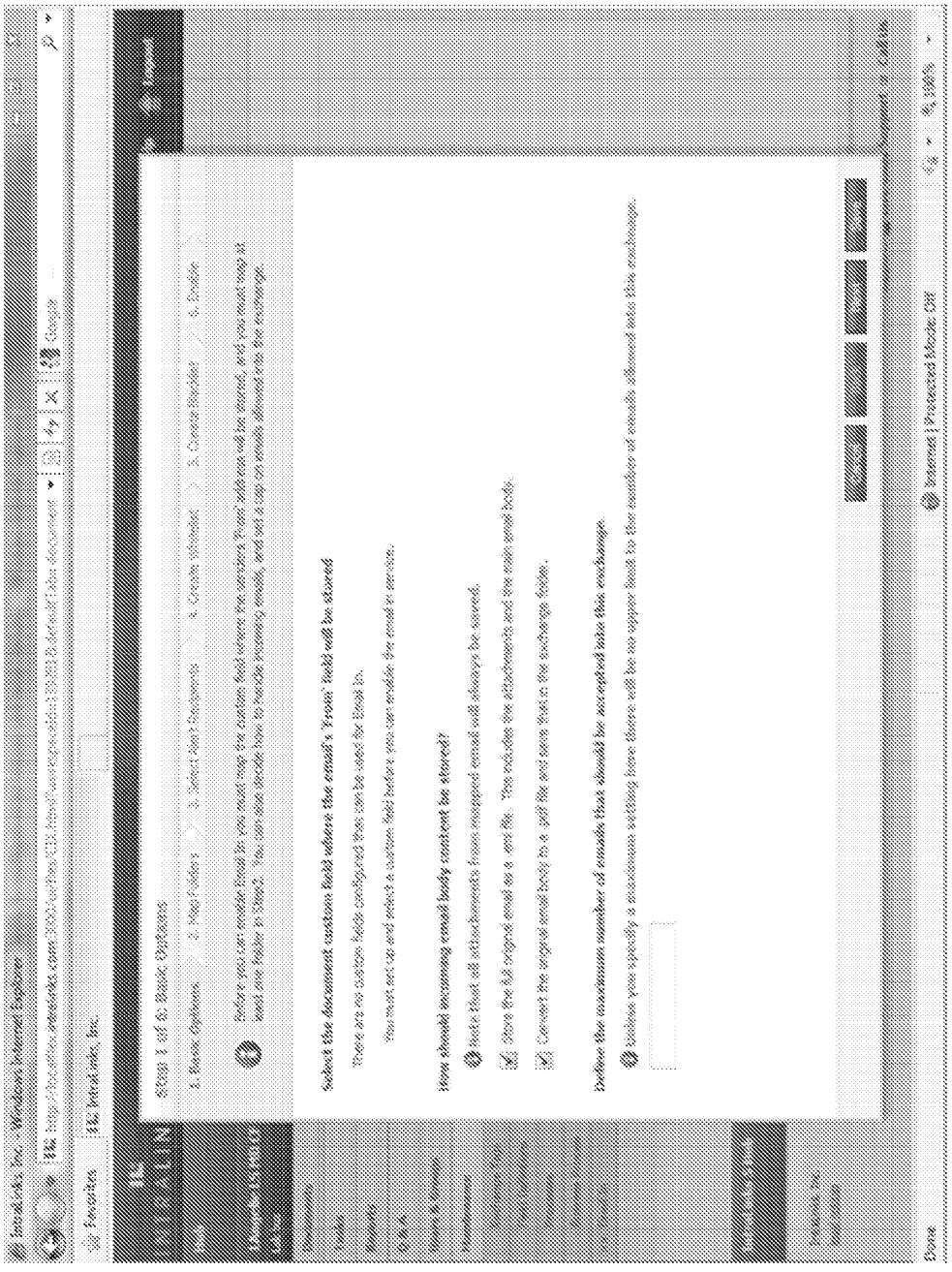


Fig. 7B

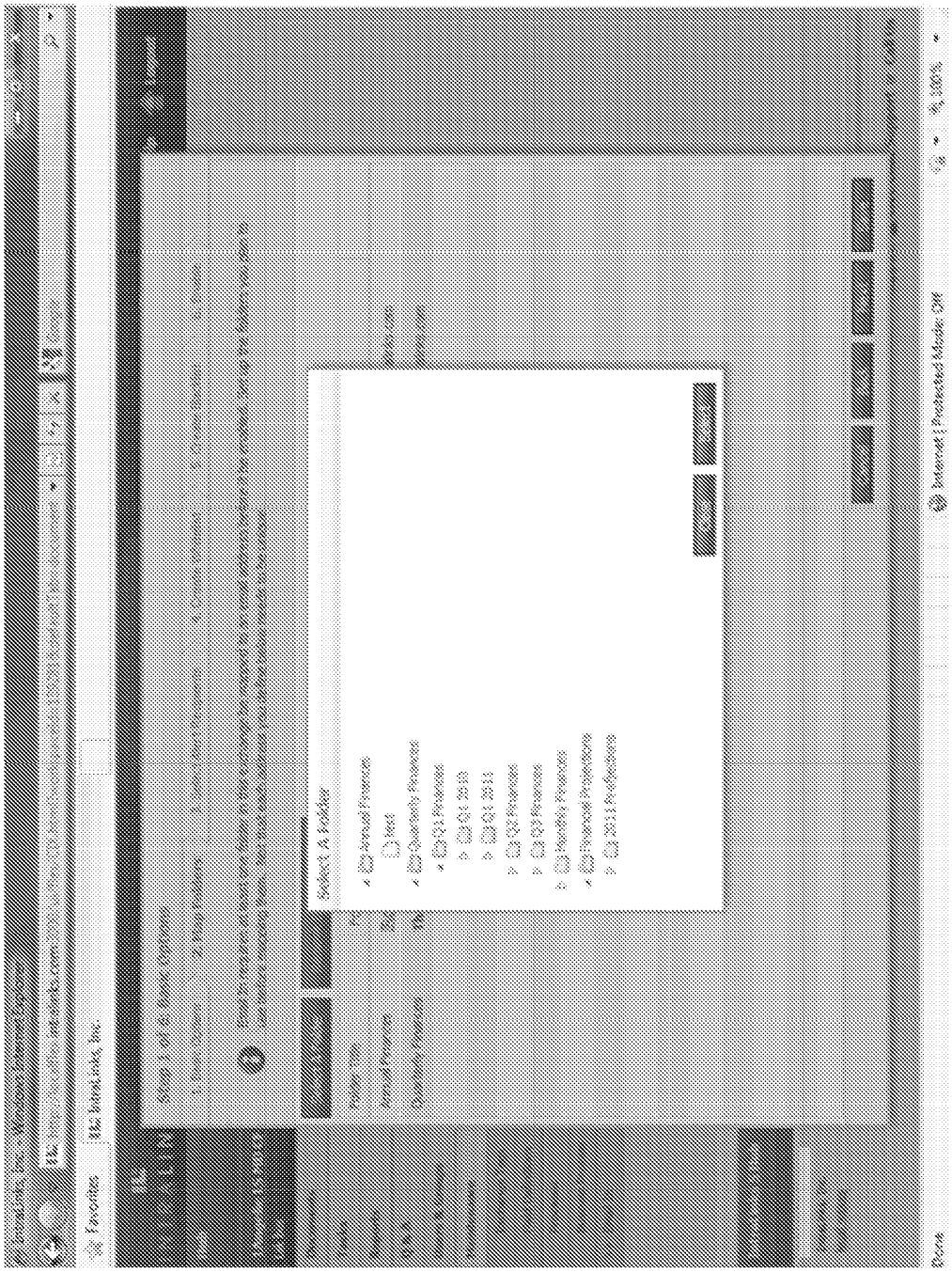


Fig. 7C

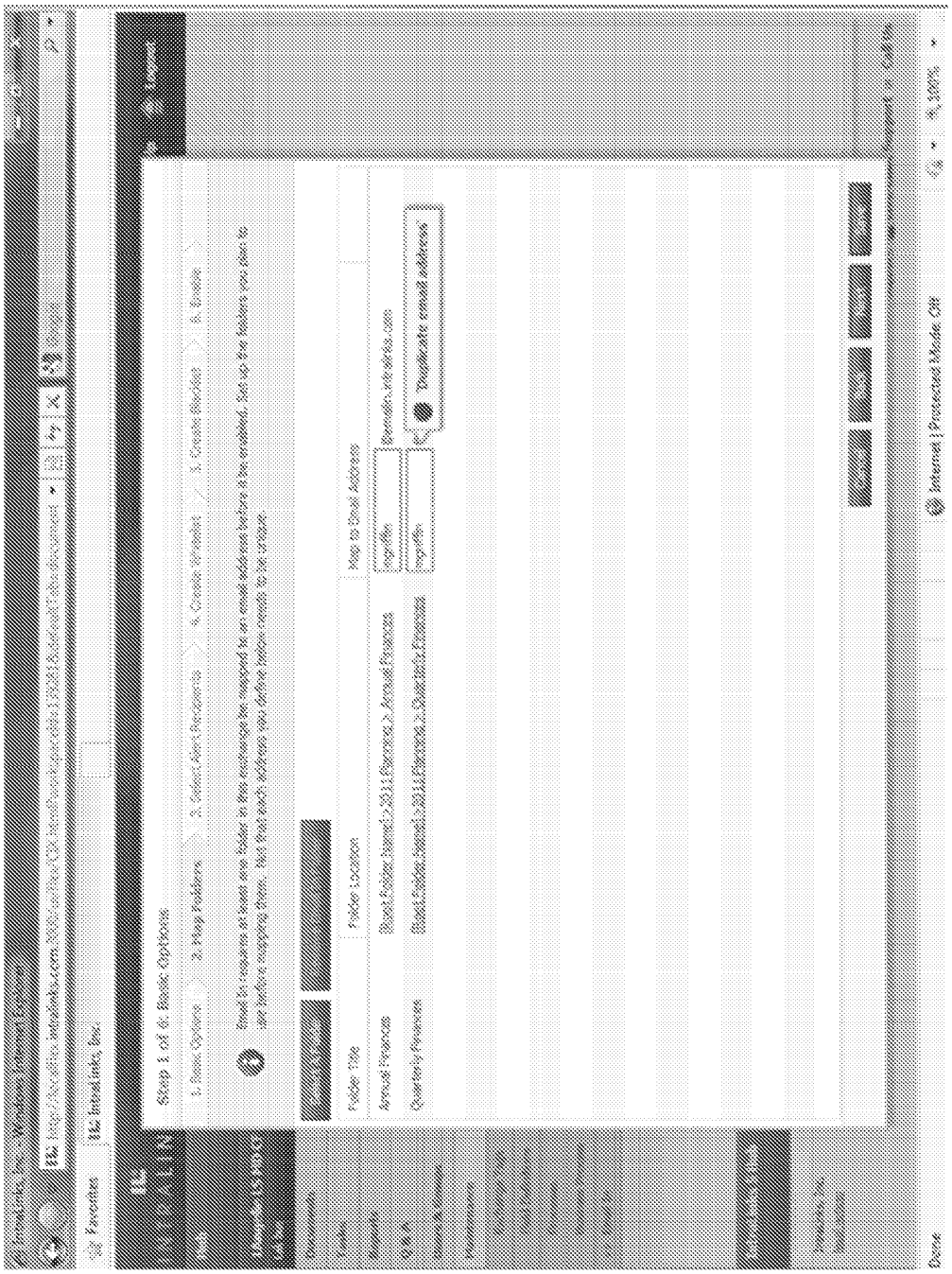


Fig. 7D

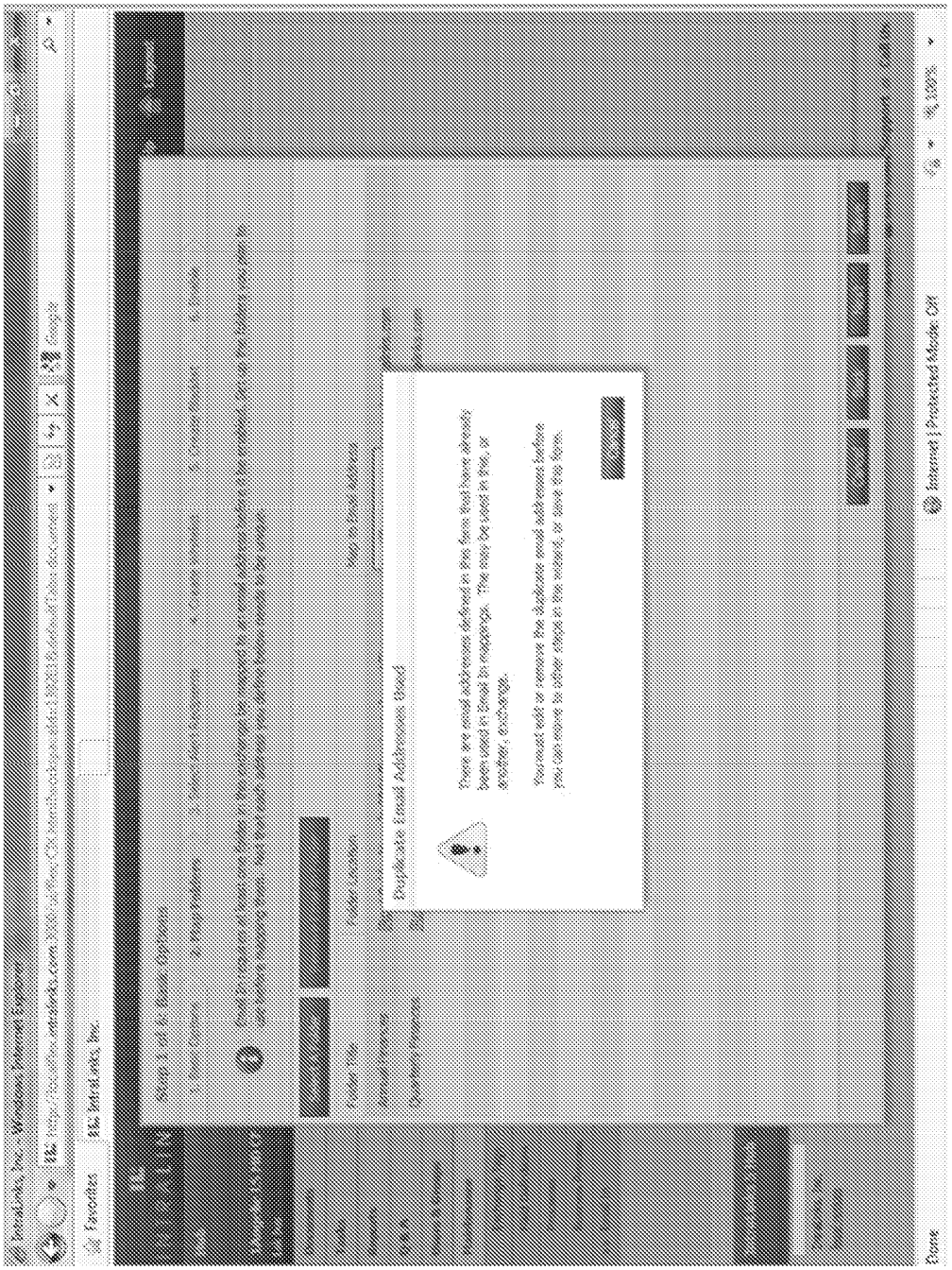


Fig. 7E

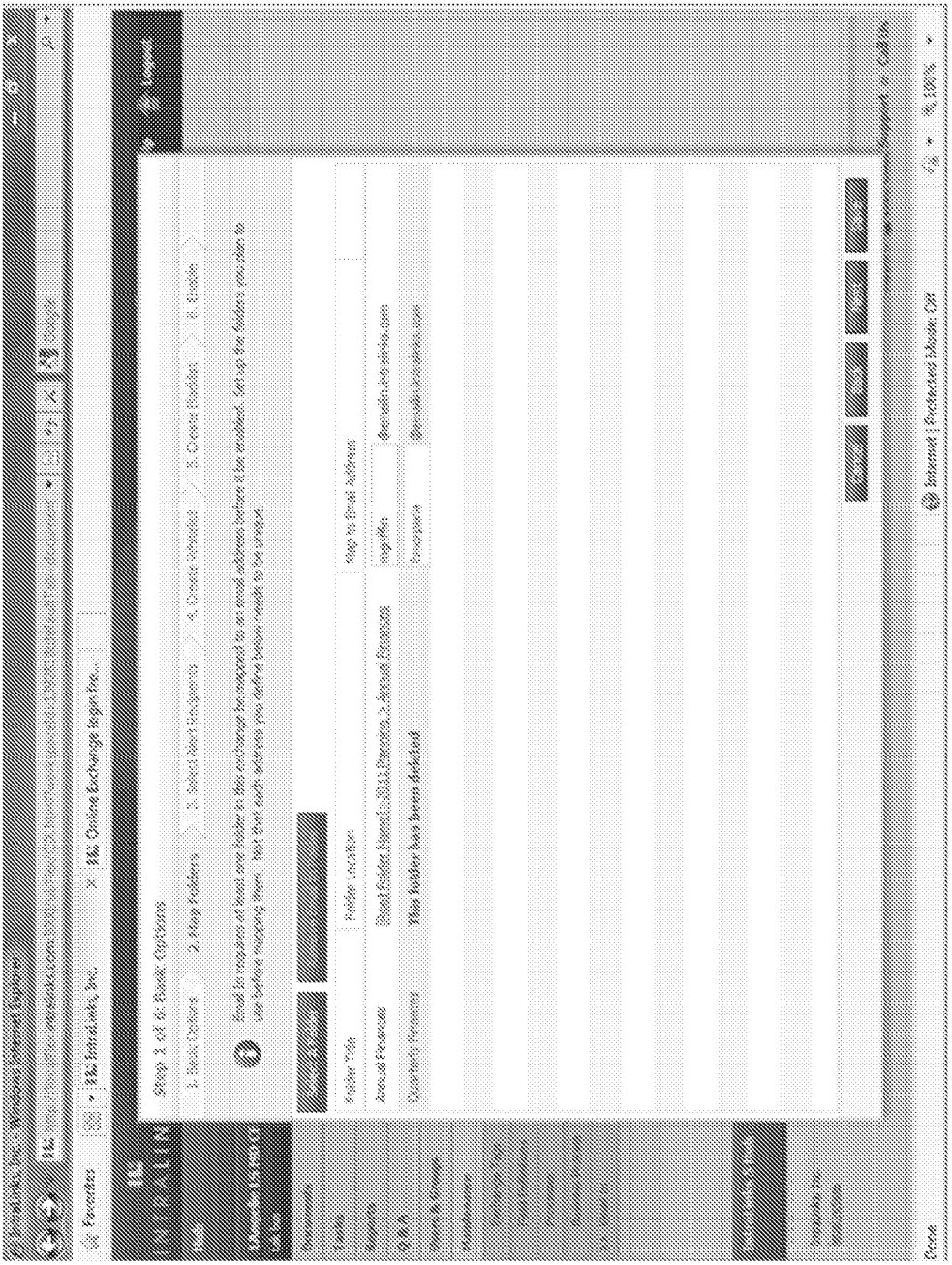


Fig. 7F


Step 1 of 3: Basic Options
Selected Users and User Alert Settings
Email
Name
Organization
NAME
NAME
NAME
NAME

Fig. 7G

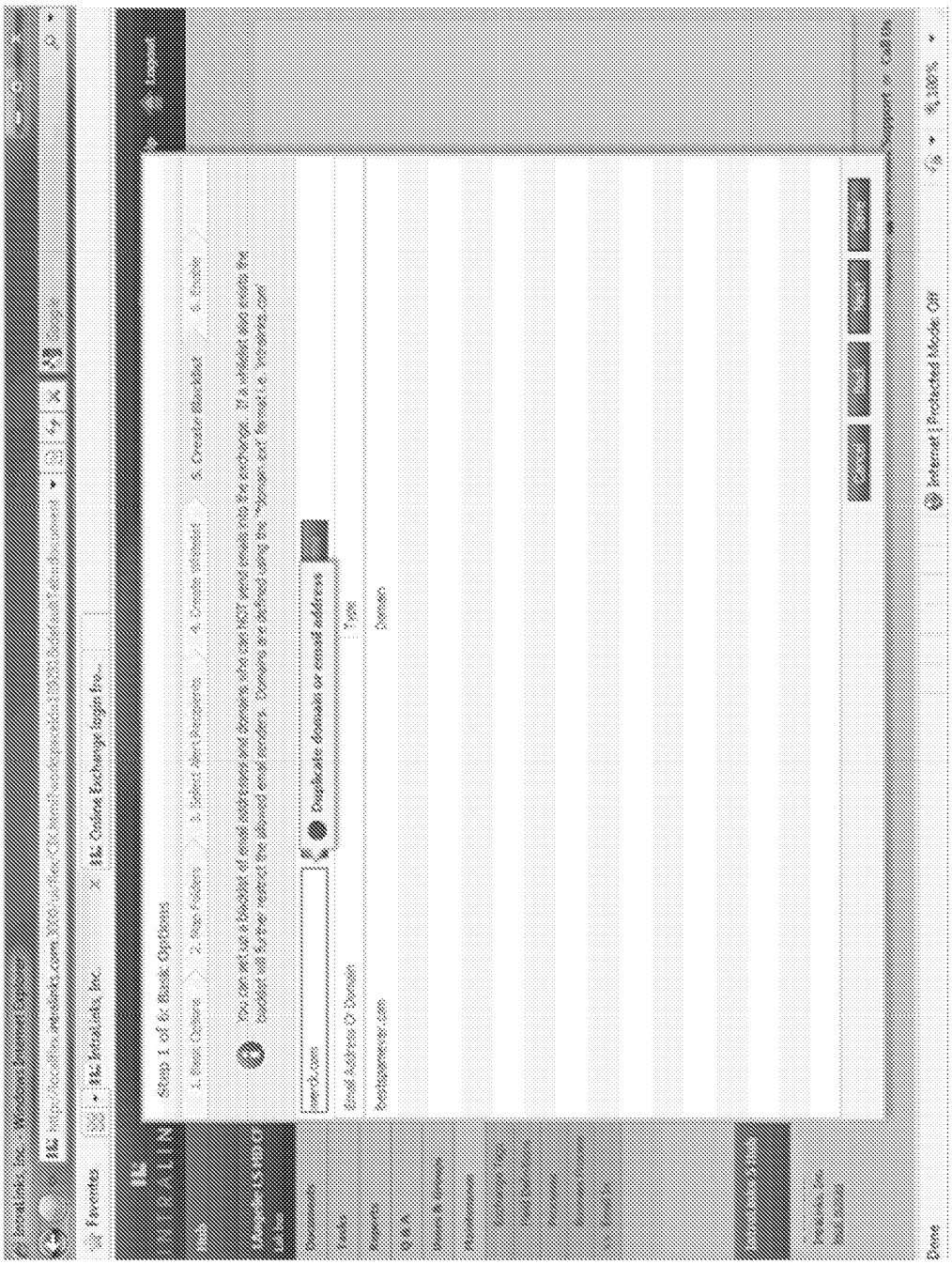


Fig. 7H

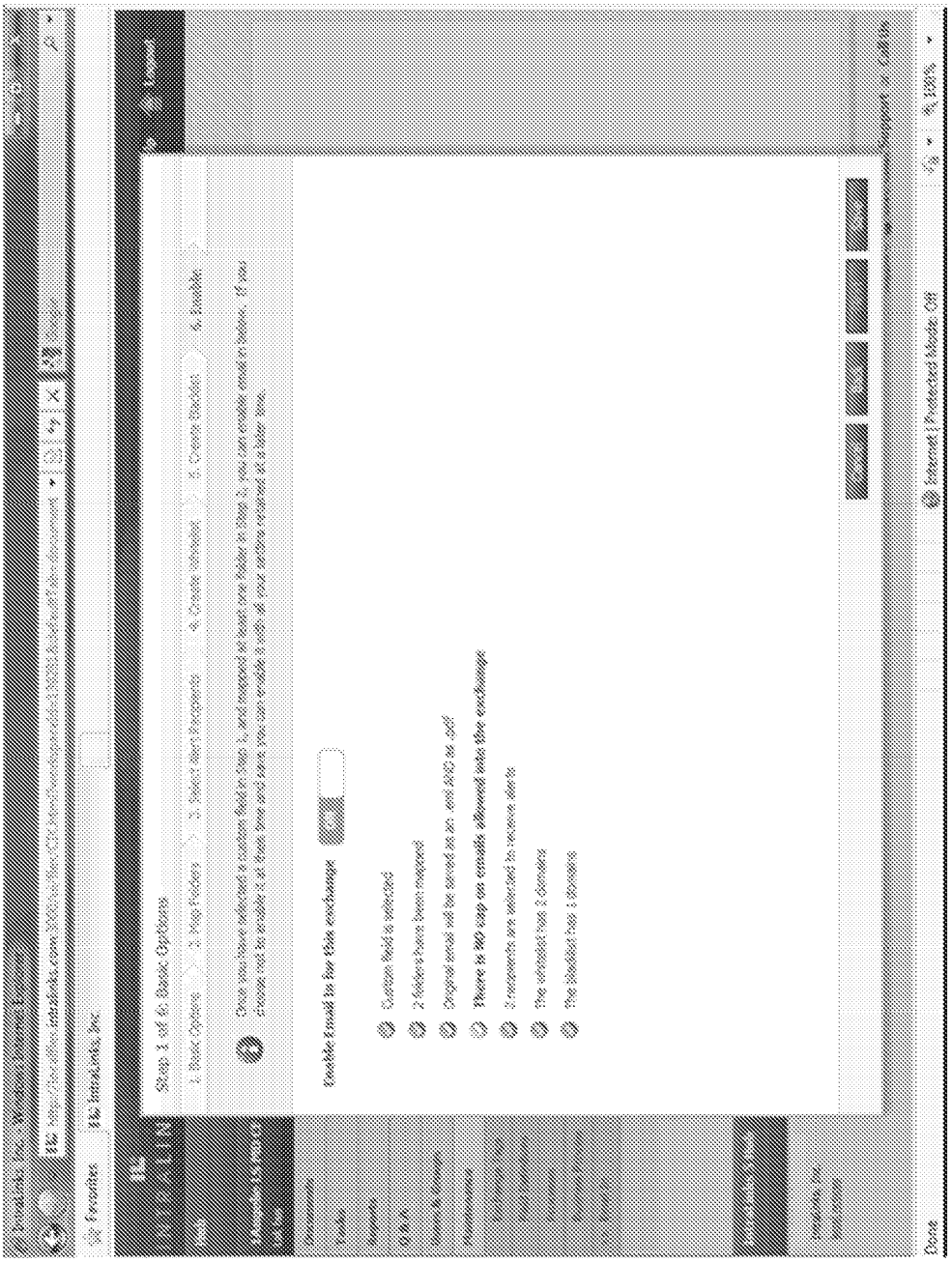


Fig. 7I

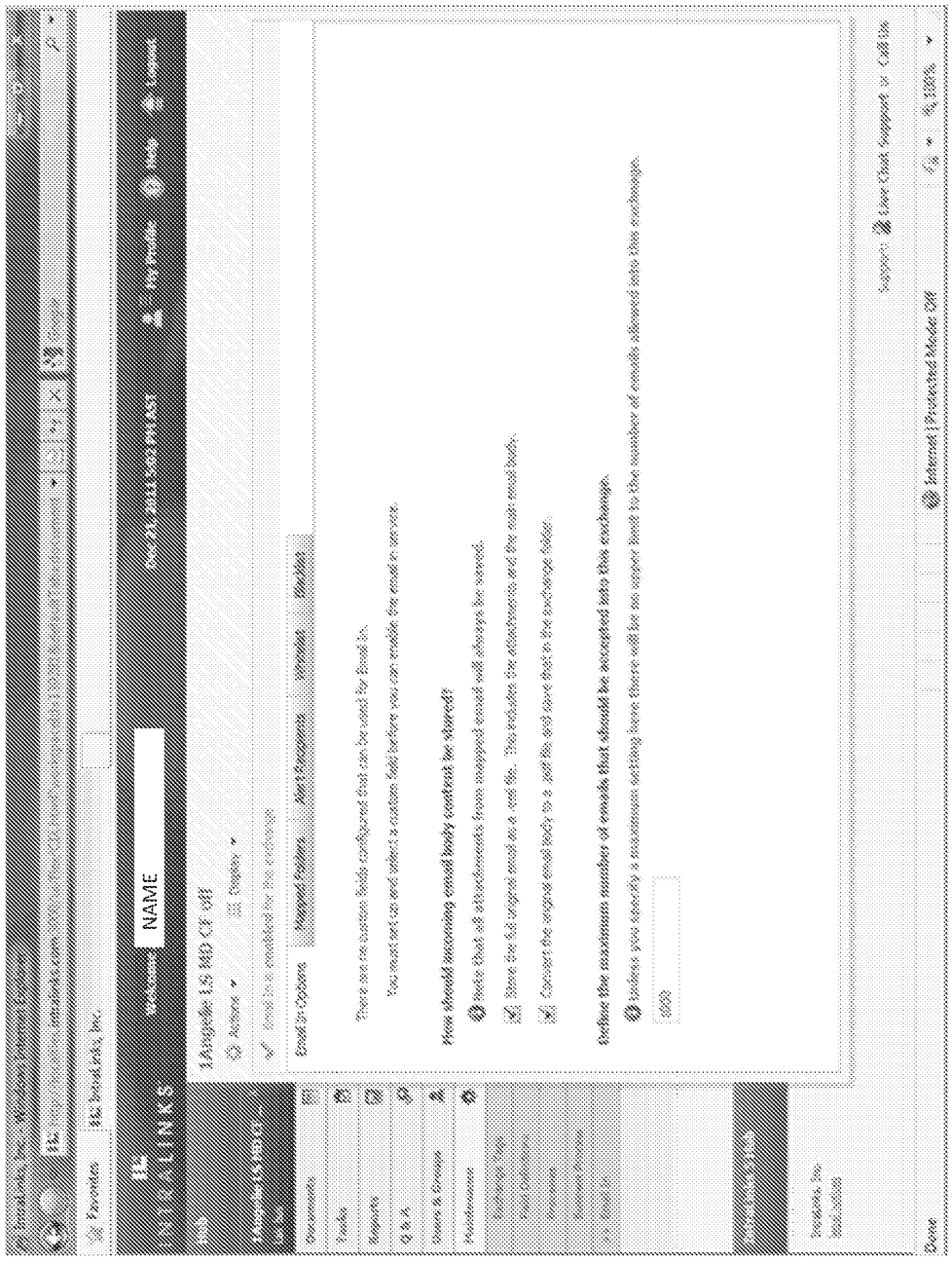


Fig. 7J

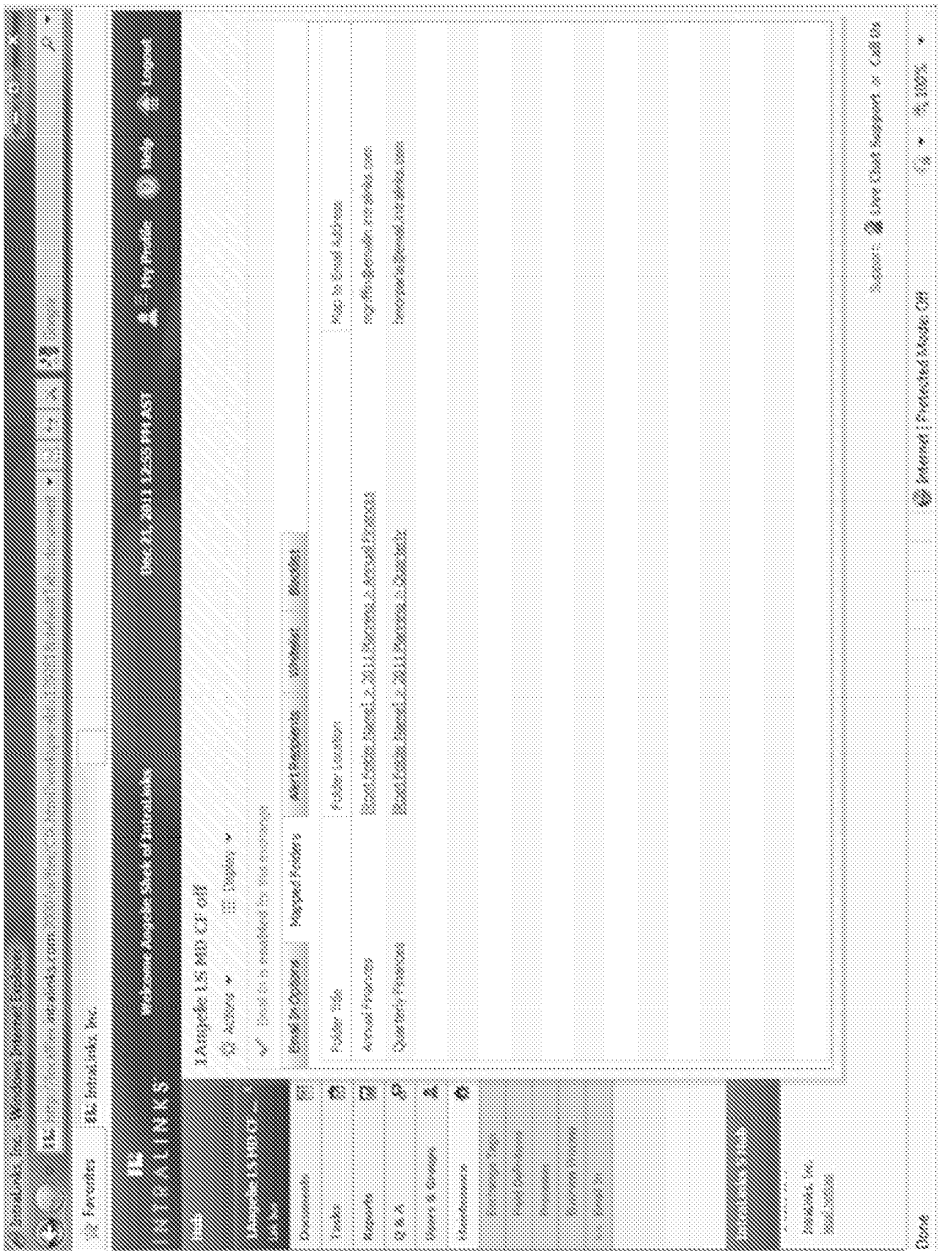


Fig. 7K

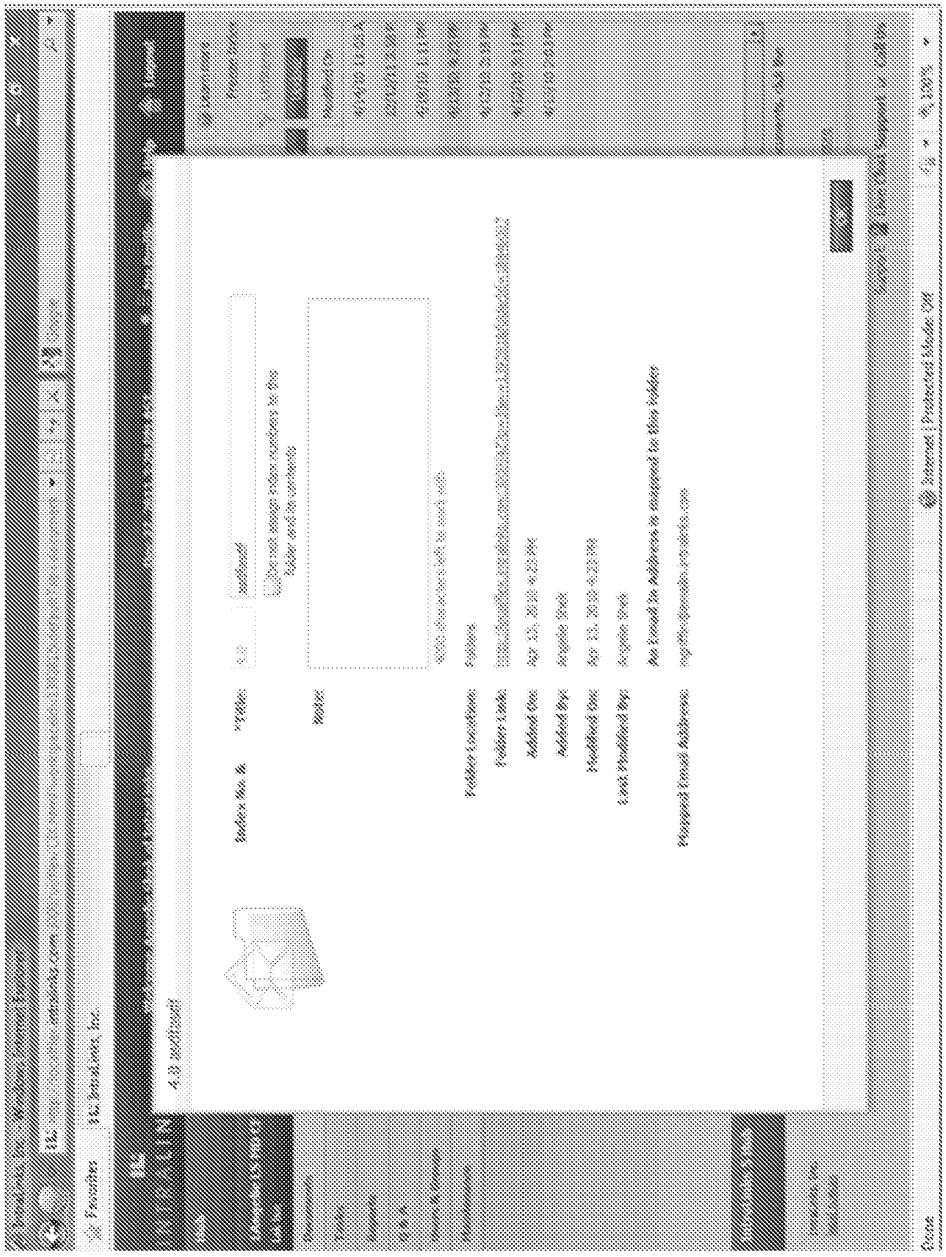


Fig. 7L

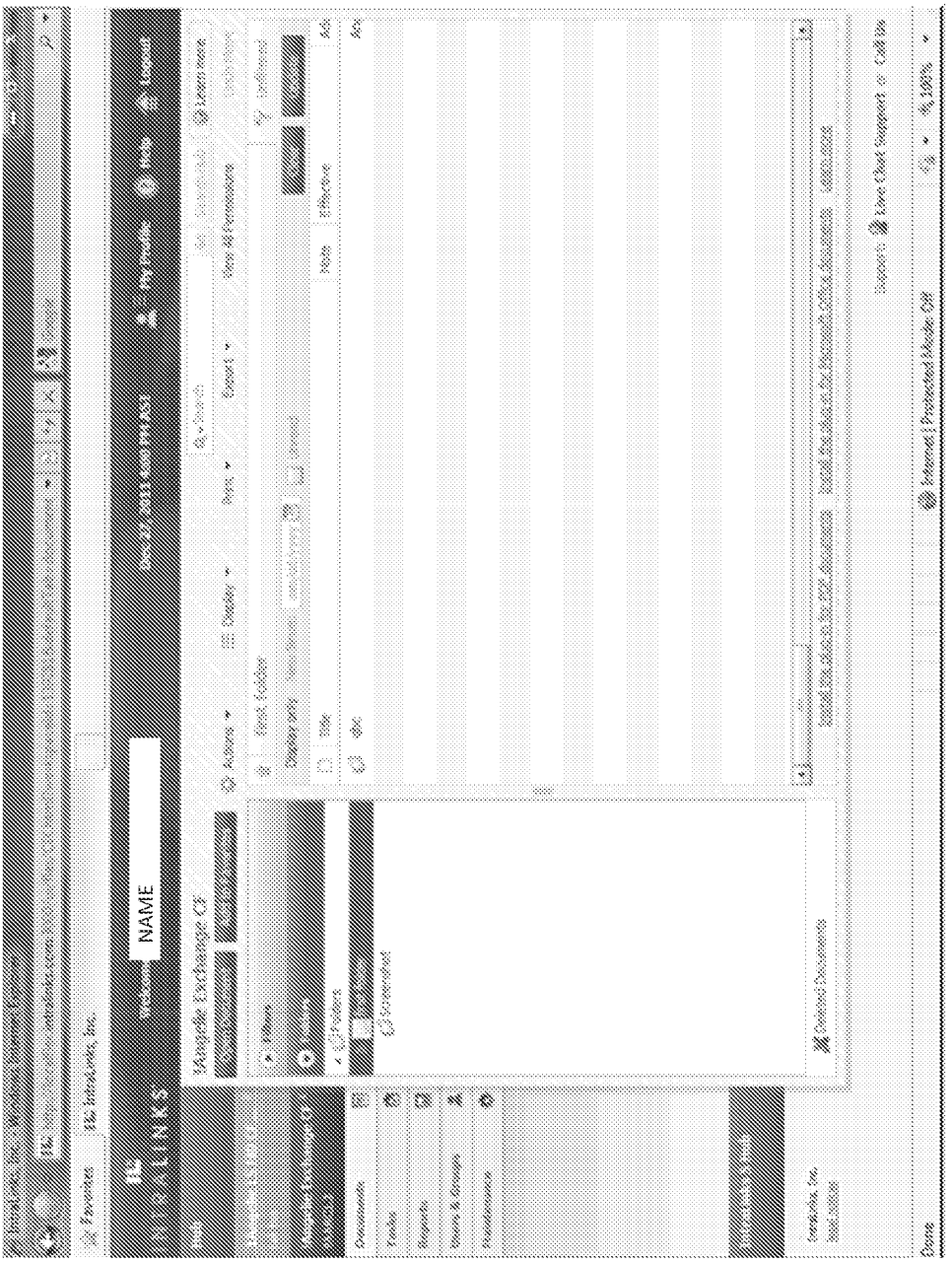


Fig. 7M

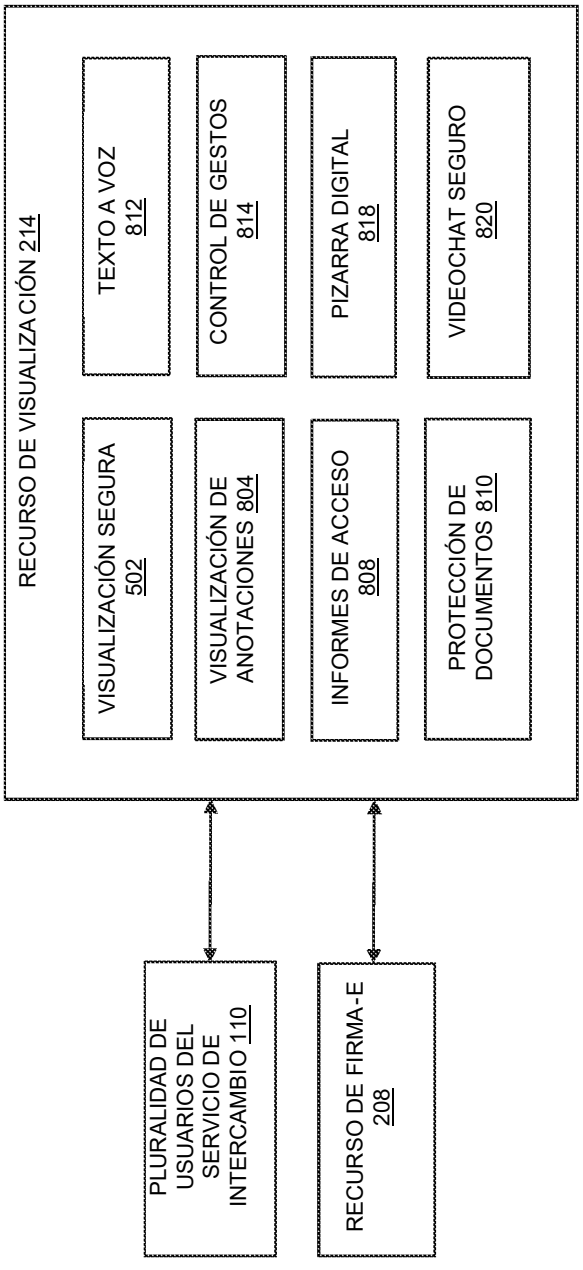
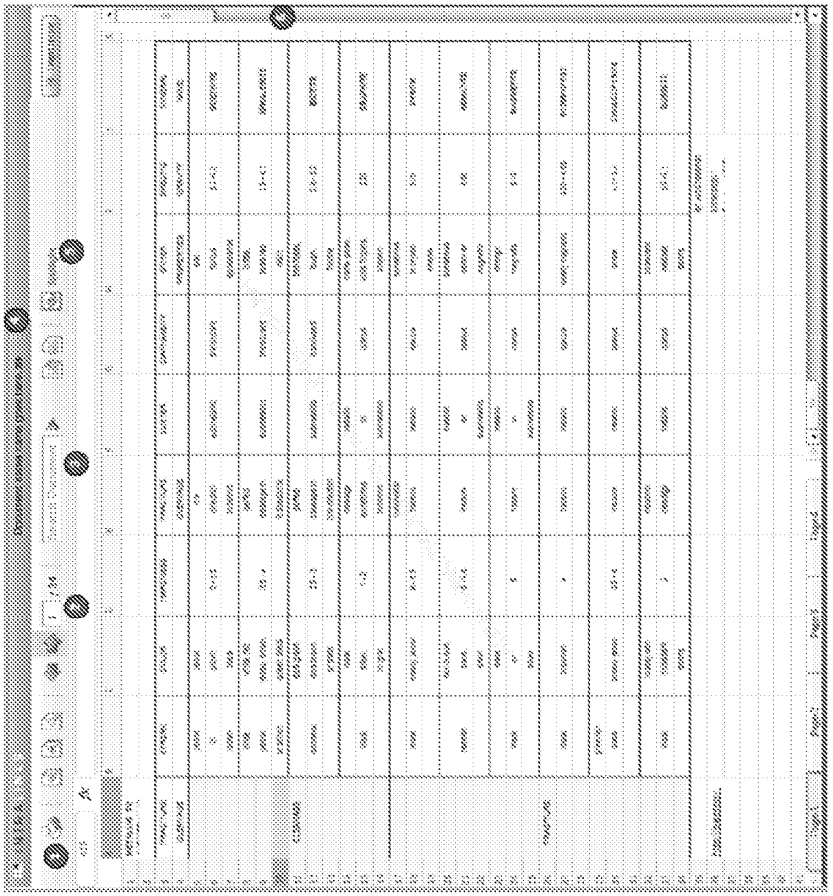

RECURSO DE VISUALIZACIÓN 214
VISUALIZACIÓN SEGURA 502
VISUALIZACIÓN DE ANOTACIONES 804
INFORMES DE ACCESO 808
PROTECCIÓN DE DOCUMENTOS 810
TEXTO A VOZ 812
CONTROL DE GESTOS 814
PIZARRA DIGITAL 818
VIDEOCHAT SEGURO 820
PLURALIDAD DE USUARIOS DEL SERVICIO DE INTERCAMBIO 110
RECURSO DE FIRMA-E 208

Fig. 8



1. No muestra los iconos de adjunto, marcador o comentarios (que se muestran en el visor de PDF).
2. Número de páginas (hojas).
3. Búsqueda en el documento.
4. La extensión del fichero se muestra como parte del nombre del fichero (también se aplica para un visor de PDF).
5. La barra de desplazamiento muestra que el documento tiene múltiples páginas. Véanse los requisitos específicos (también se aplica para un visor de PDF).

Fig. 8A

1. La búsqueda puede incluir caracteres especiales (también se aplica para un visor de PDF).
2. Área de resultados de búsqueda
3. Los resultados se agrupan por número de Página (hoja de cálculo).
4. El término buscado está subrayado. Se muestran los caracteres especiales (también se aplica para un visor de PDF).
5. Se muestra el mensaje si algunos resultados de búsqueda se muestran antes de que se complete toda la búsqueda en el documento (también se aplica para un visor de PDF).

Fig. 8B

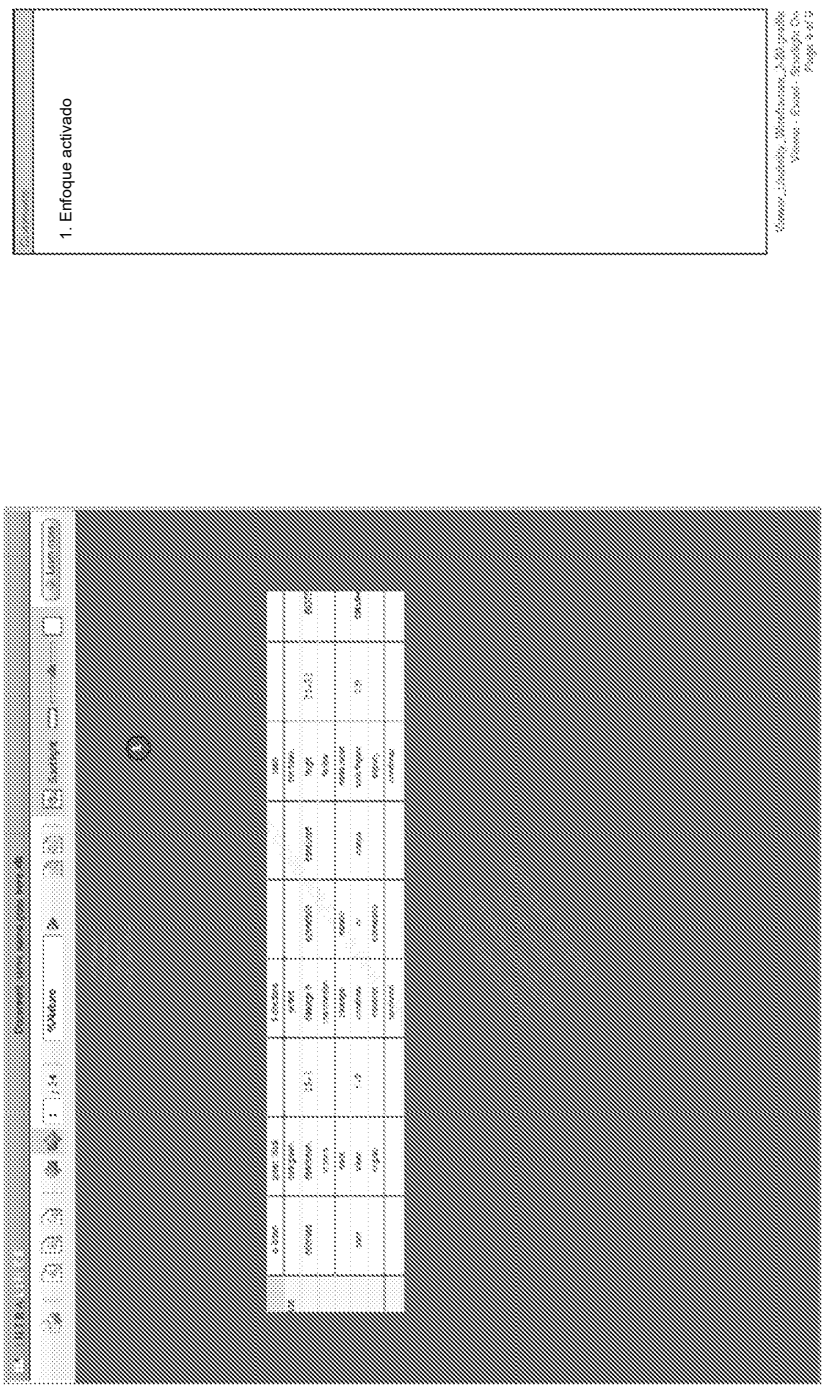


Fig. 8C

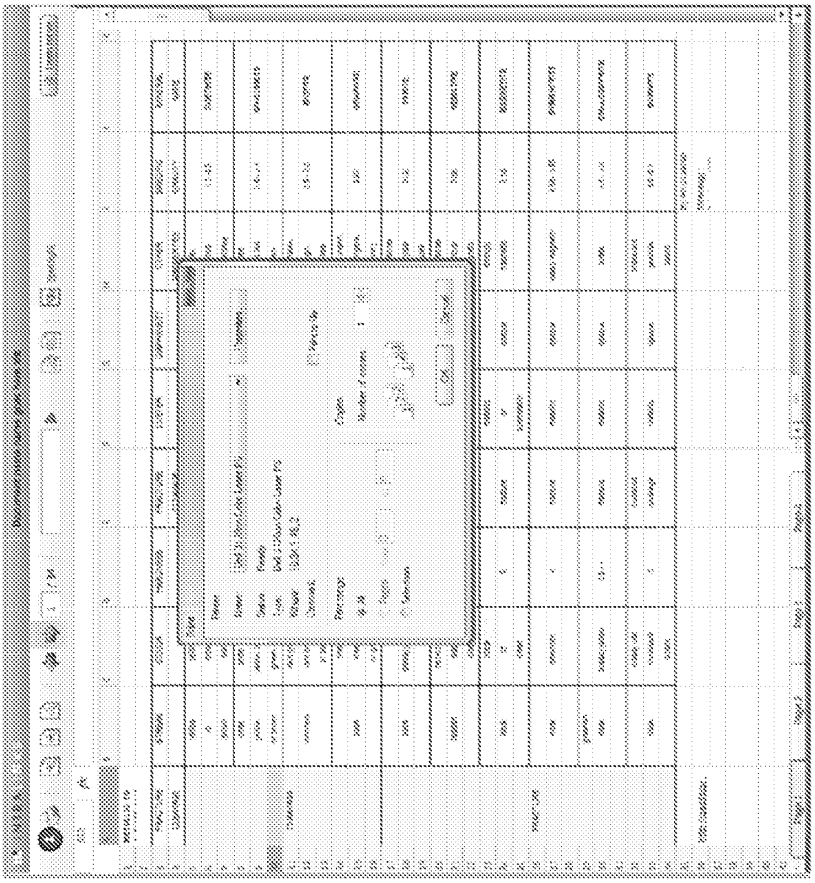
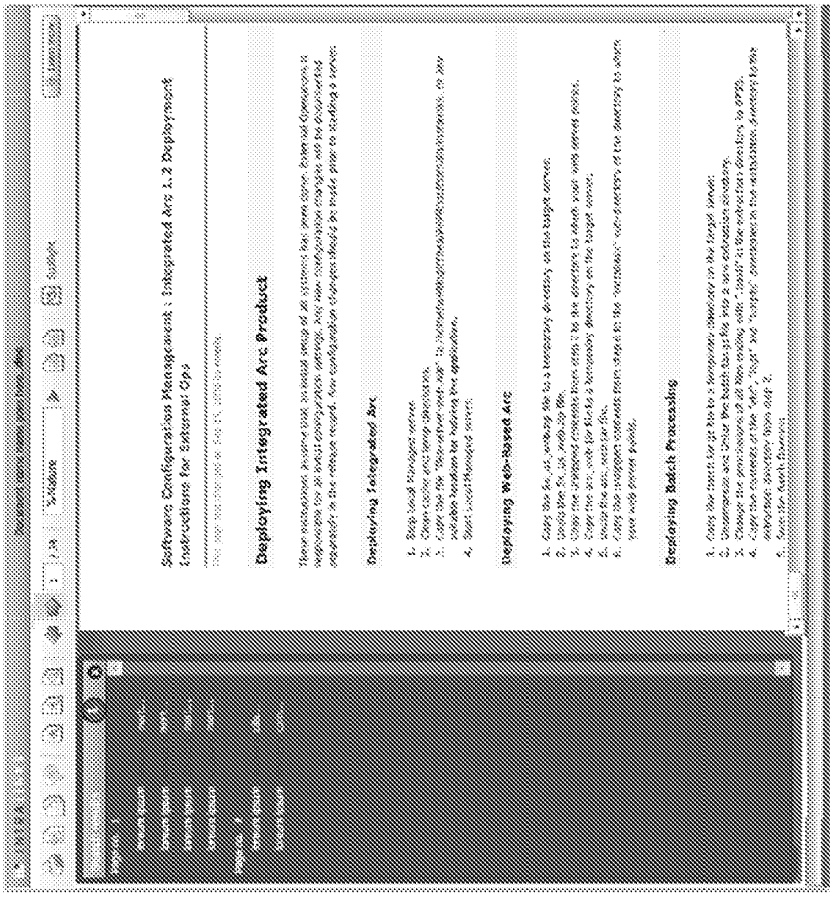

1. Cuando el usuario hace clic en el icono de Imprimir, se abre el diálogo de impresión del sistema (también se aplica en un visor de PDF).

Fig. 8D

1. Iconos de imprimir, adjunto, marcador, o comentarios (que se muestran en el visor de PDF).
2. Número de páginas.
3. Búsqueda en el documento.
4. La extensión del fichero se muestra como parte del nombre del fichero.
5. Interfaz de enfoque.
6. La barra de desplazamiento muestra que el documento tiene múltiples páginas.

INTRALINKS
Reports
User Coverage Report (From Users and Groups)
Group Coverage Report (From Users and Groups)
Activity Summary Report

Fig. 8E


Software Configuration Management : Integrated Arc 1.2 Deployment Instructions for External Ops
Deploying Integrated Arc Product
Deploying Web-Based Arc
Deploying Batch Processing

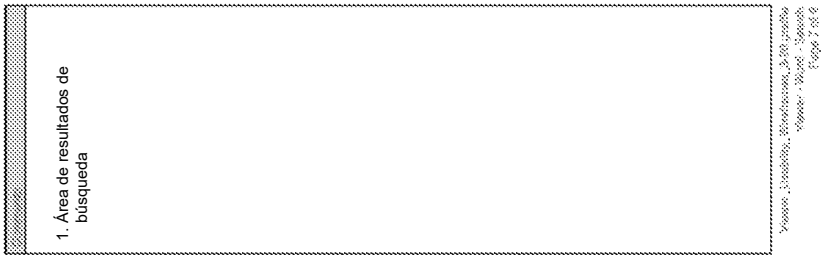

1. Área de resultados de búsqueda

Fig. 8F

1. El usuario ha hecho clic en el icono de Imprimir.
2. La ventana del documento se vuelve gris.
3. Aparece la pantalla previa a la impresión.
4. El usuario puede seleccionar:
Todas las páginas
La página actual que está viendo
Un intervalo de páginas.
5. Si el usuario hace clic en el cuadro de texto, se selecciona automáticamente el botón de radio «Intervalo de Páginas».
6. «Cancelar» cierra la ventana. La pantalla vuelve a la normalidad.
7. «Siguiente» cierra la ventana previa a la impresión y abre el diálogo de impresión del SO.

Fig. 8G

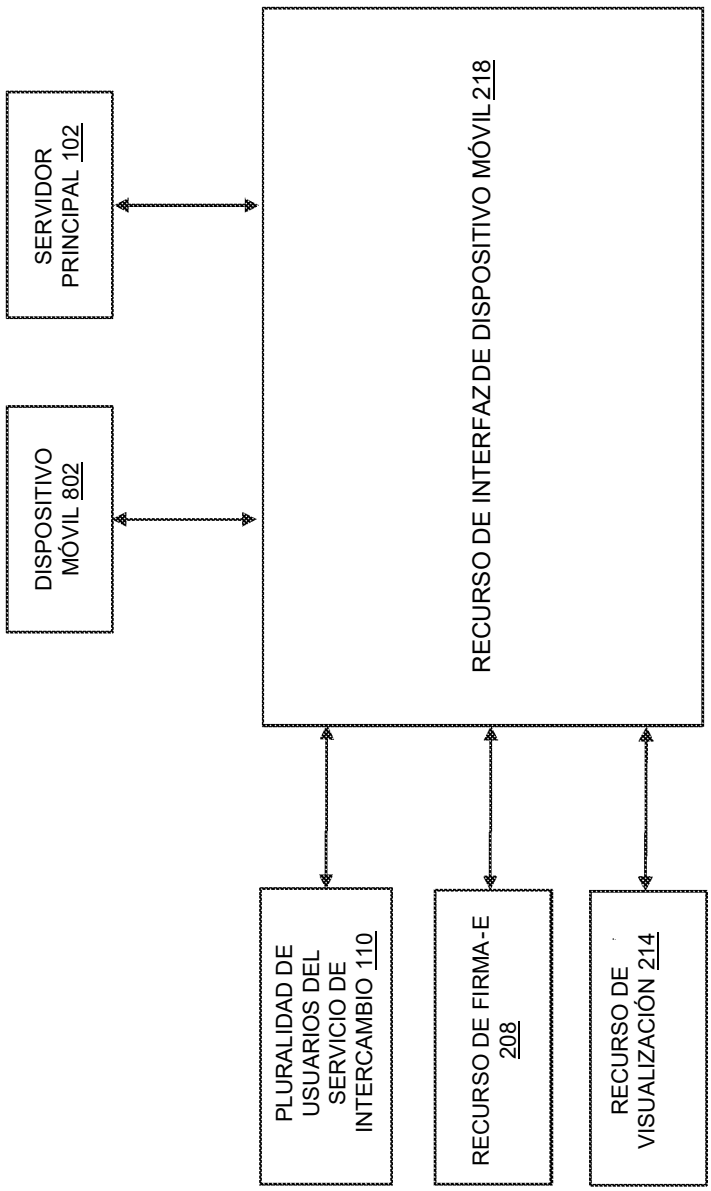

SERVIDOR PRINCIPAL 102
DISPOSITIVO MÓVIL 802
RECURSO DE INTERFAZ DE DISPOSITIVO MÓVIL 218
PLURALIDAD DE USUARIOS DEL SERVICIO DE INTERCAMBIO 110
RECURSO DE FIRMA-E 208
RECURSO DE VISUALIZACIÓN 214

Fig. 9

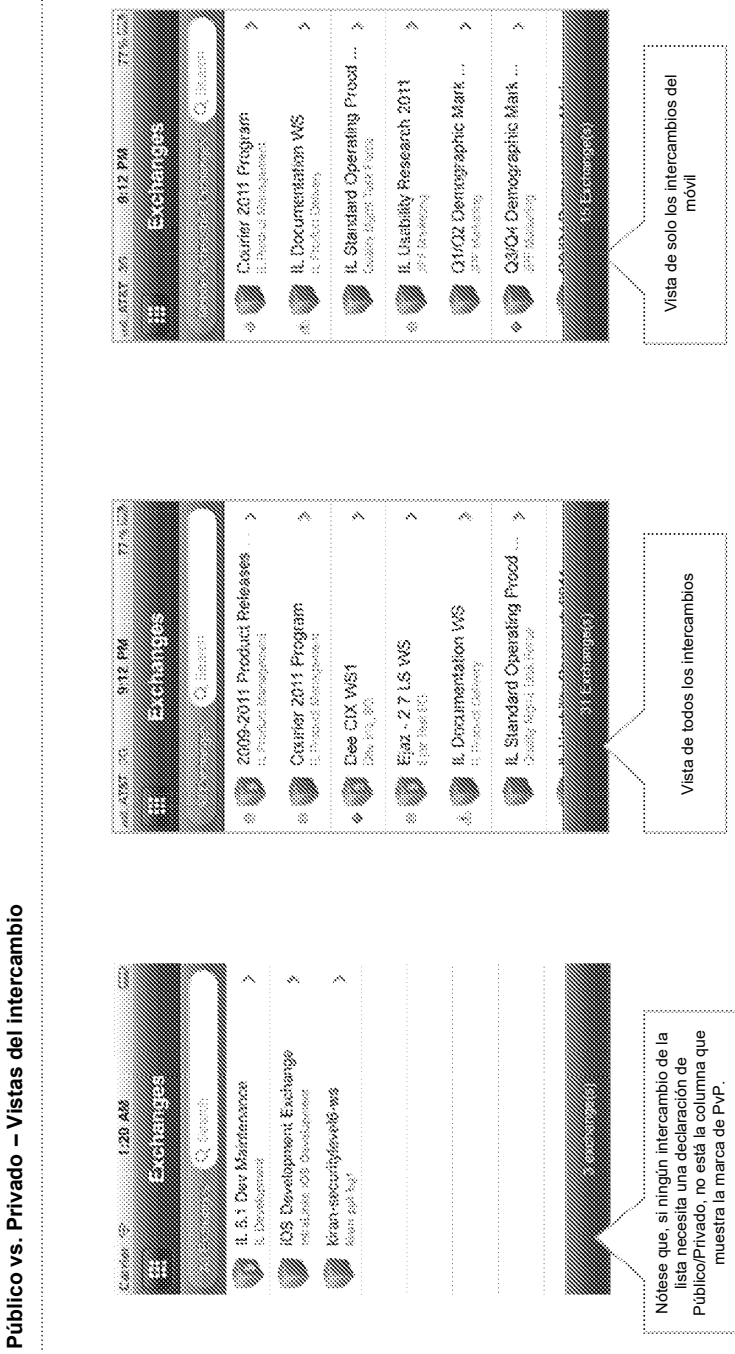

Público vs. Privado – Vistas del intercambio
Exchanges
Nótese que, si ningún intercambio de la lista necesita una declaración de Público/Privado, no está la columna que muestra la marca de PvP.
Vista de todos los intercambios
Vista de solo los intercambios del móvil

Fig. 9A

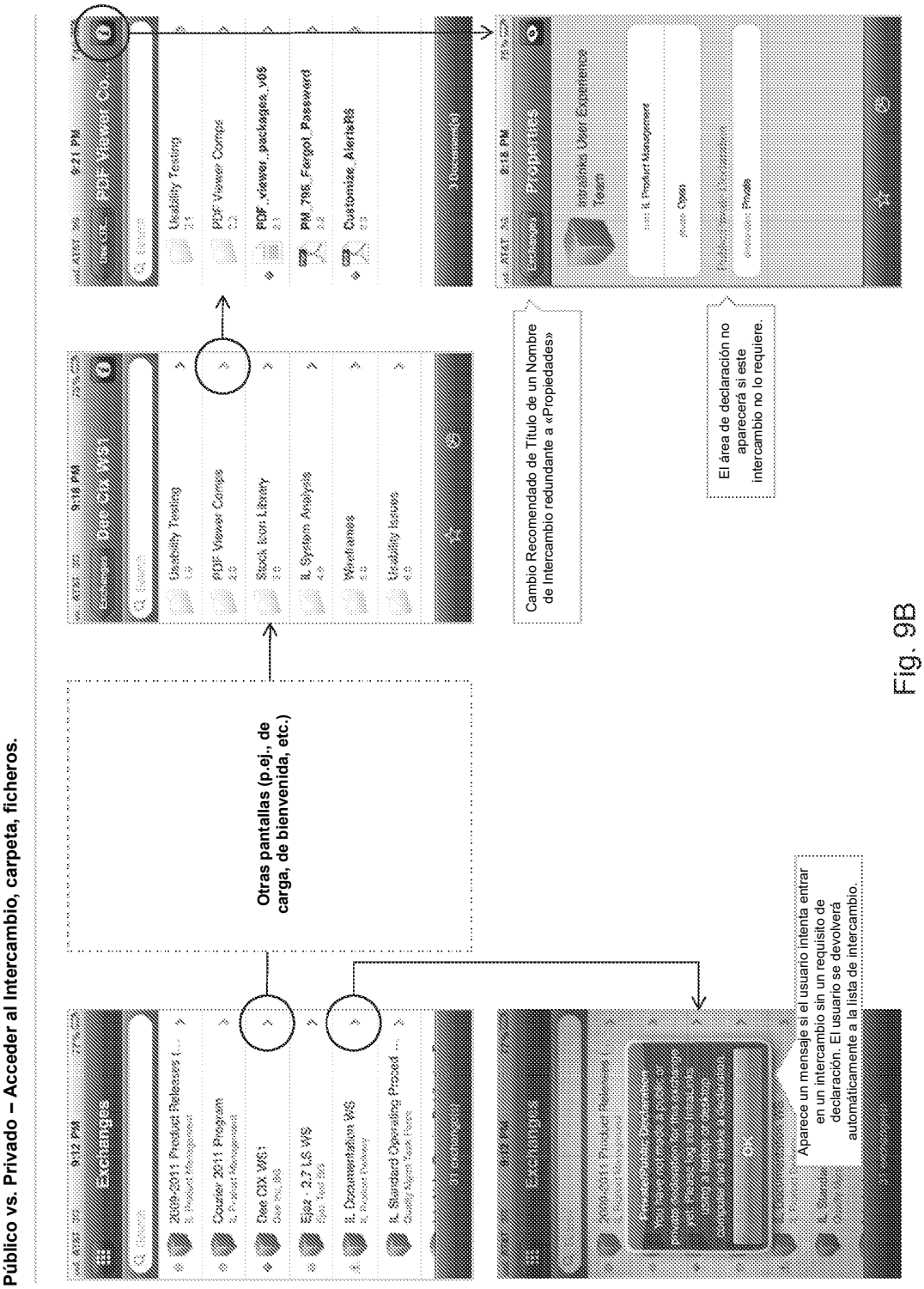

Público vs. Privado – Acceder al Intercambio, carpeta, ficheros.
Otras pantallas (p.ej., de carga, de bienvenida, etc.)
Cambio Recomendado de Título de un Nombre de Intercambio redundante a «Propiedades»
El área de declaración no aparecerá si este intercambio no lo requiere.
Aparece un mensaje si el usuario intenta entrar en un intercambio sin un requisito de declaración. El usuario se devolverá automáticamente a la lista de intercambio.

Fig. 9B

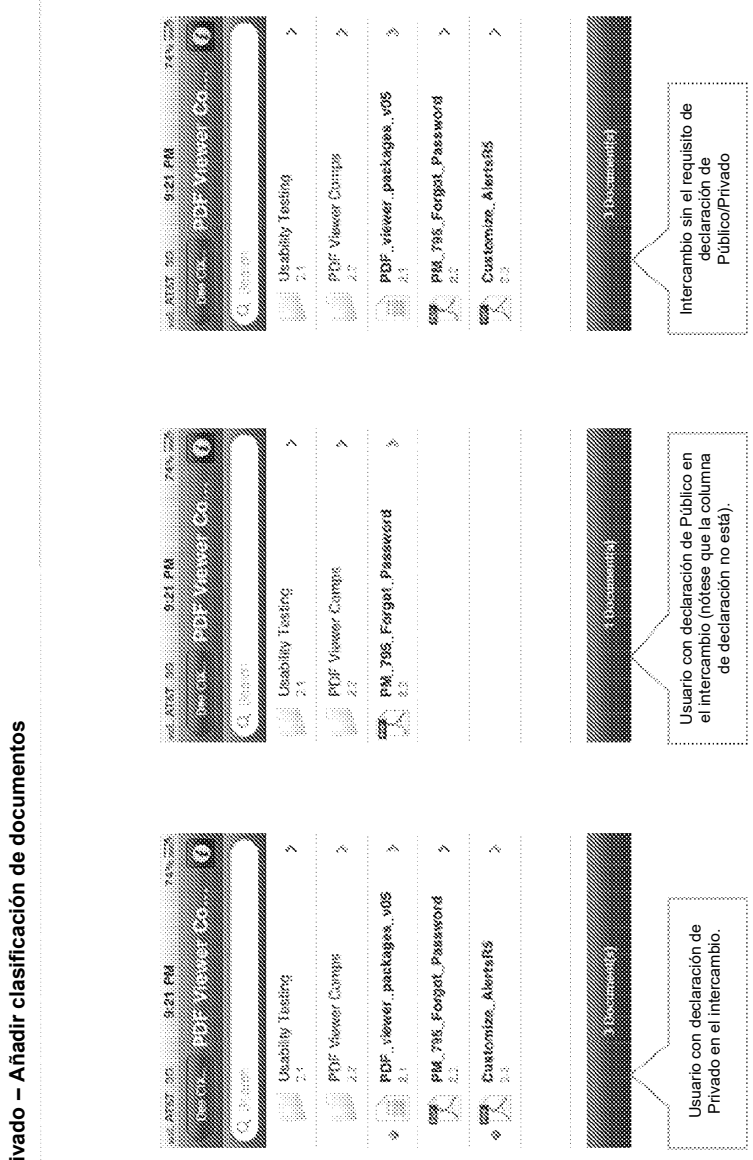

Público vs. Privado – Añadir clasificación de documentos
Usuario con declaración de Privado en el intercambio.
Usuario con declaración de Público en el intercambio (nótese que la columna de declaración no está).
Intercambio sin el requisito de declaración de Público/Privado

Fig. 9C

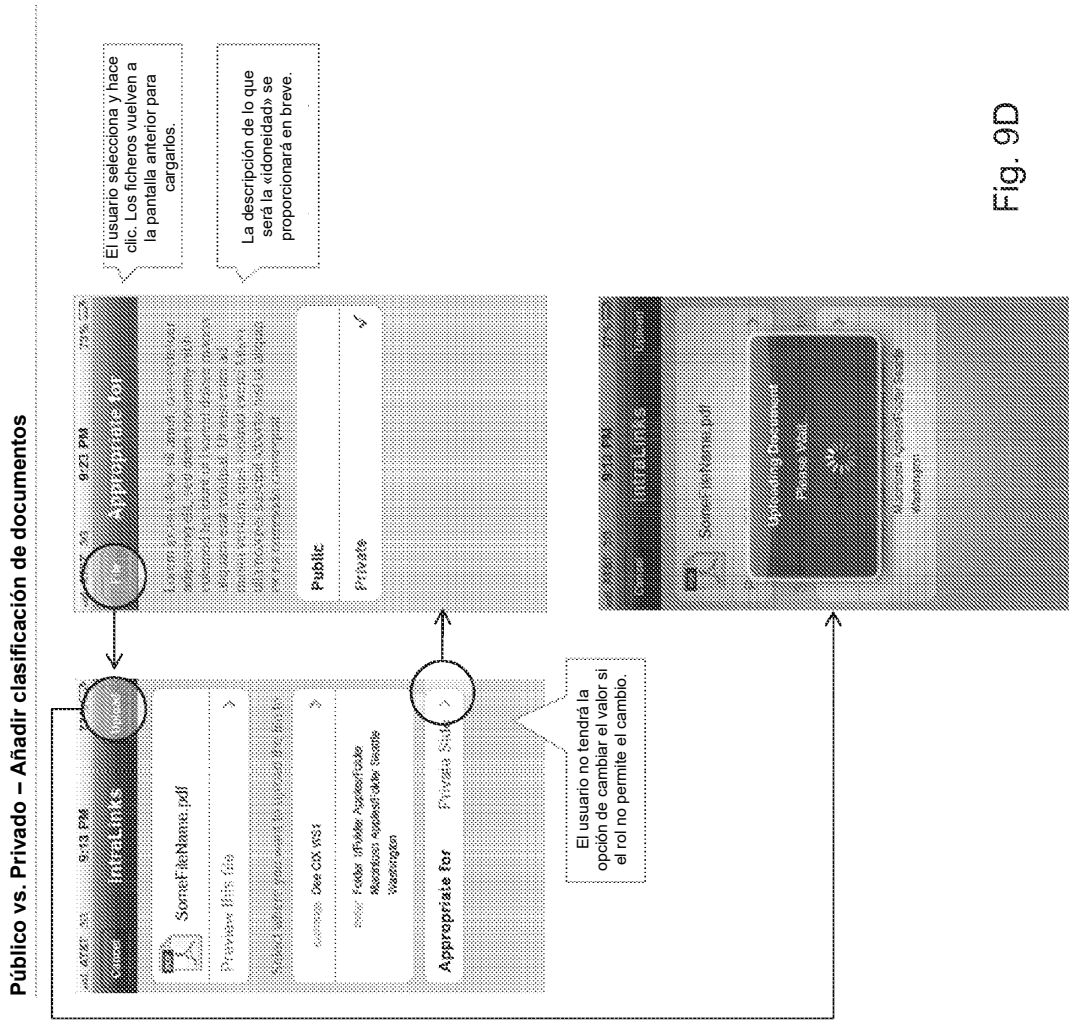

Público vs. Privado – Añadir clasificación de documentos
El usuario selecciona y hace clic. Los ficheros vuelven a la pantalla anterior para cargarlos.
La descripción de lo que será la «idoneidad» se proporcionará en breve.
El usuario no tendrá la opción de cambiar el valor si el rol no permite el cambio.
Public
Private
Appropriate for
Cancel
Upload
SomeFileName.pdf

Fig. 9D

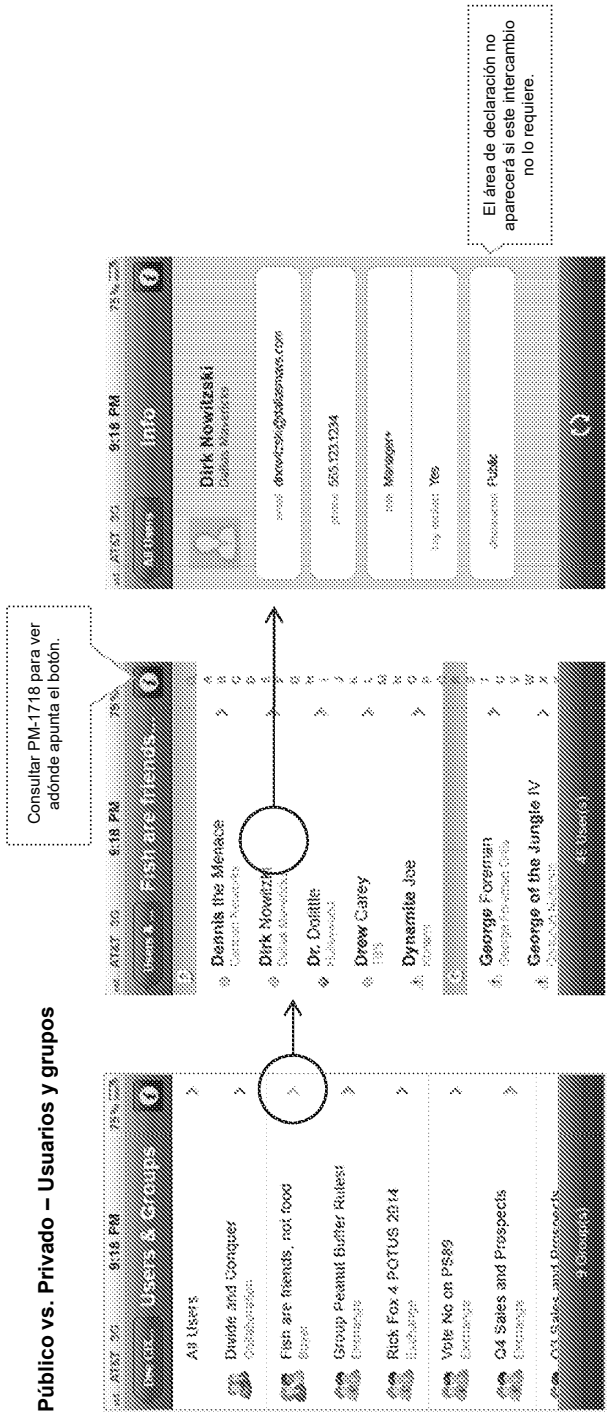

Público vs. Privado – Usuarios y grupos
Consultar PM-1718 para ver adónde apunta el botón.
El área de declaración no aparecerá si este intercambio no lo requiere.

Fig. 9E

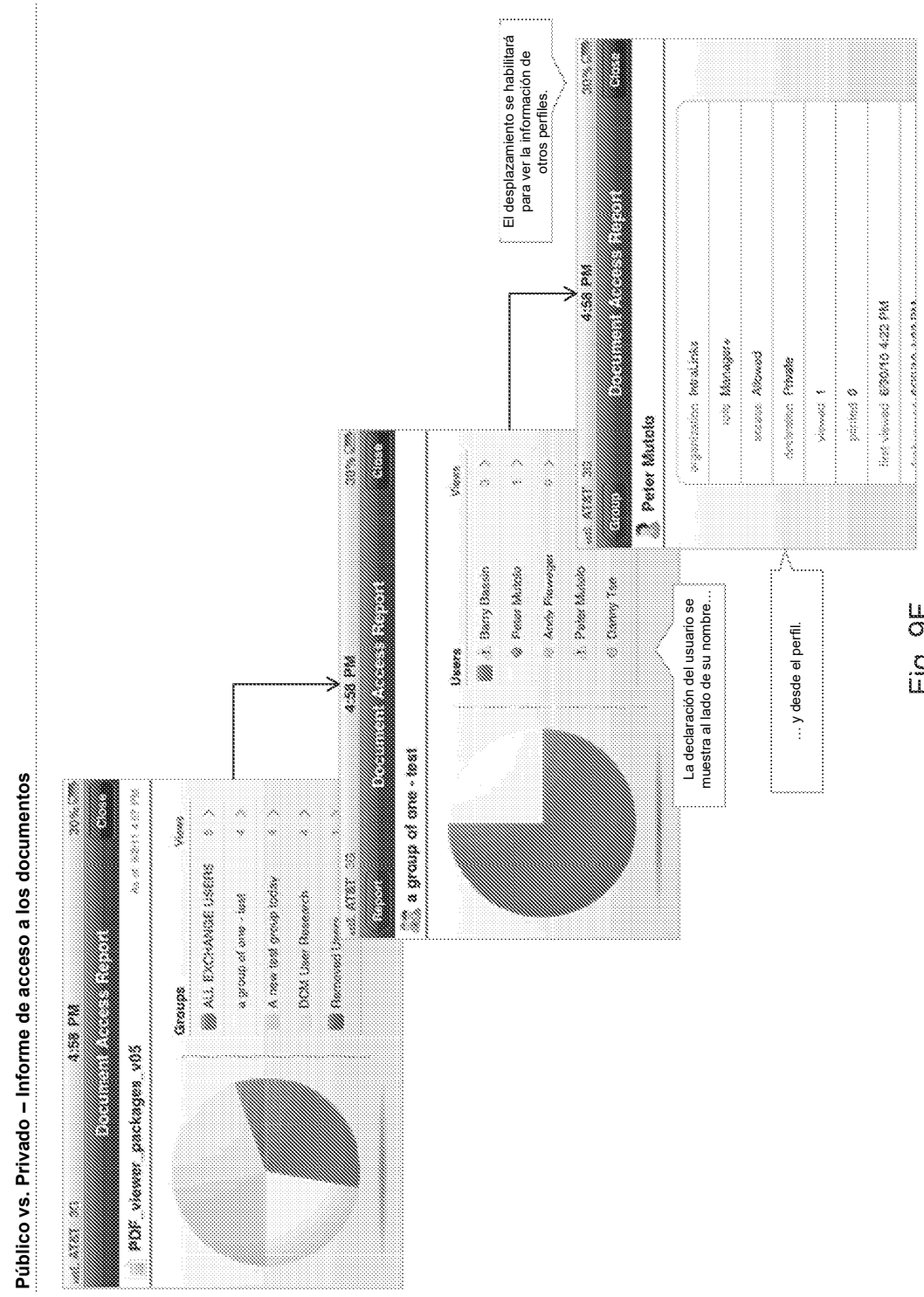

Público vs. Privado – Informe de acceso a los documentos
Document Access Report
4:58 PM
POF_viewer_packages_v03
Groups
ALL EXCHANGE USERS
a group of one - test
A new test group today
DCM User Research
Removed Users
Views
Users
a group of one - test
Barry Bassin
Peter Mutola
Andy Finnegan
Peter Mutola
Danny Tan
Close
El desplazamiento se habilitará para ver la información de otros perfiles.
Peter Mutola
La declaración del usuario se muestra al lado de su nombre...
... y desde el perfil.

Fig. 9F

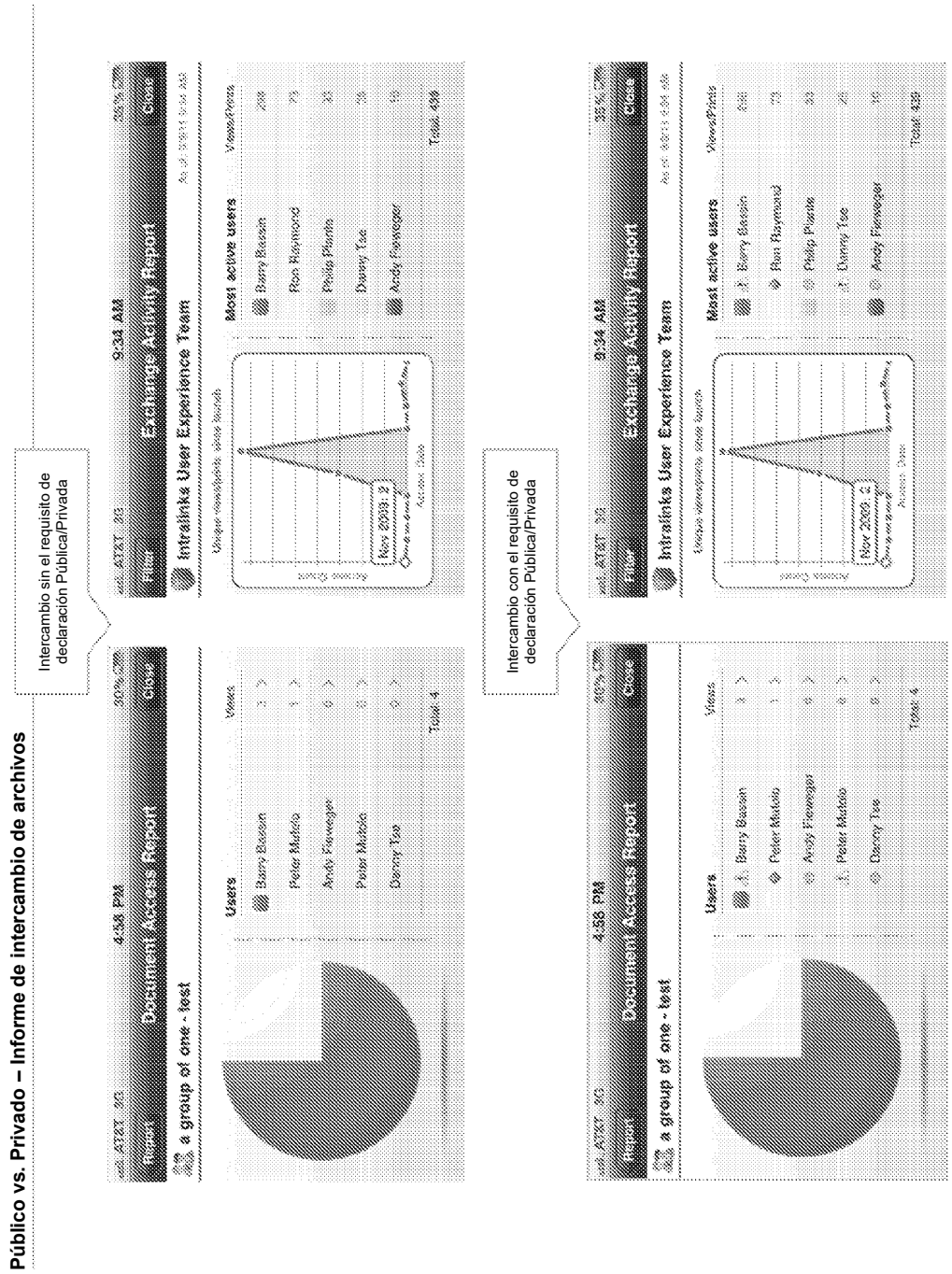

Público vs. Privado – Informe de intercambio de archivos
Intercambio sin el requisito de declaración Pública/Privada
Intercambio con el requisito de declaración Pública/Privada
Document Access Report
Intralinks User Experience Team
Most active users
Users
Views
Total: 4
Total: 439

Fig. 9G

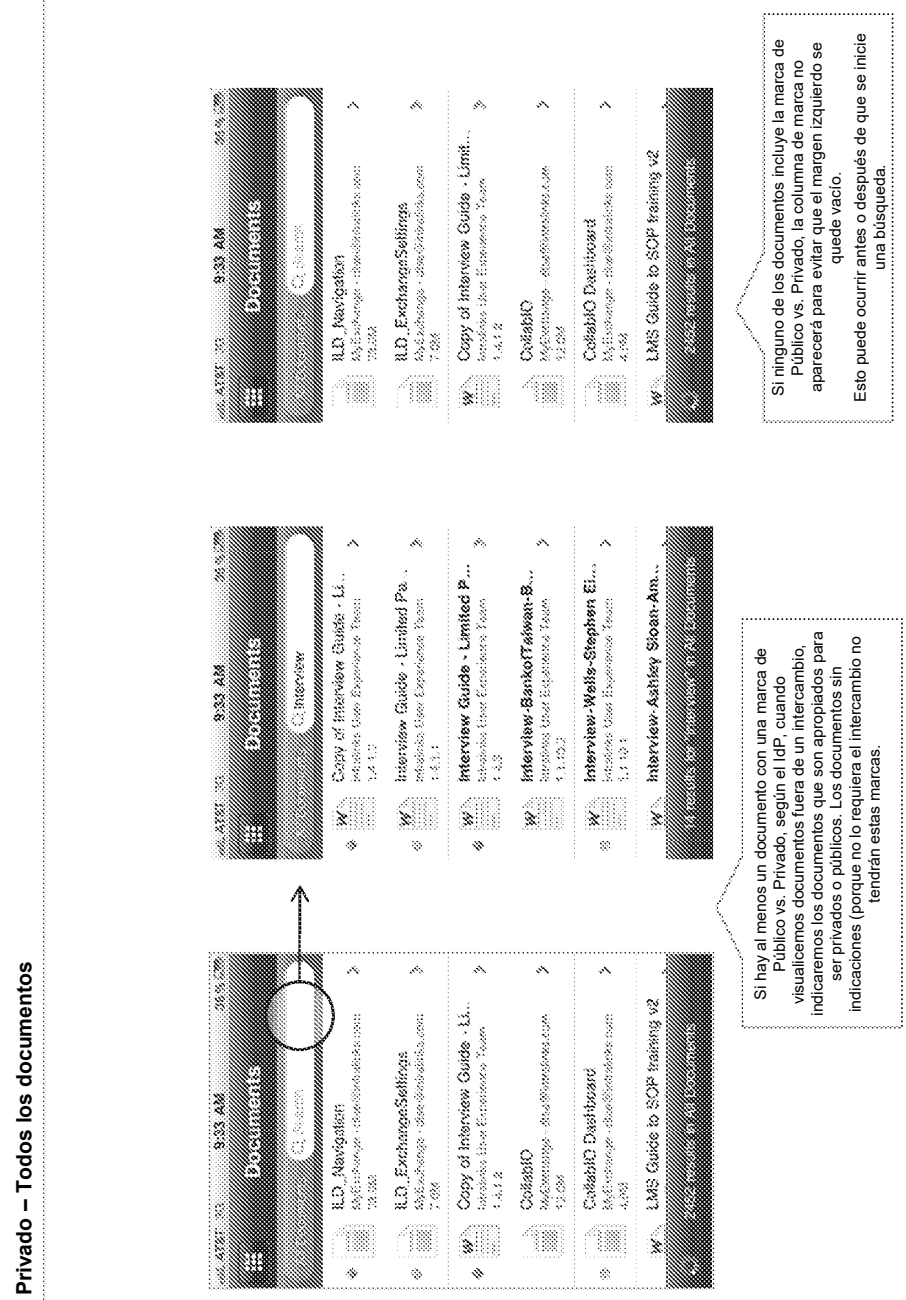

Público vs. Privado – Todos los documentos
Documents
Q Search
Si hay al menos un documento con una marca de Público vs. Privado, según el IdP, cuando visualicemos documentos fuera de un intercambio, indicaremos los documentos que son apropiados para ser privados o públicos. Los documentos sin indicaciones (porque no lo requiera el intercambio no tendrán estas marcas.
Si ninguno de los documentos incluye la marca de Público vs. Privado, la columna de marca no aparecerá para evitar que el margen izquierdo se quede vacío.
Esto puede ocurrir antes o después de que se inicie una búsqueda.

Fig. 9H

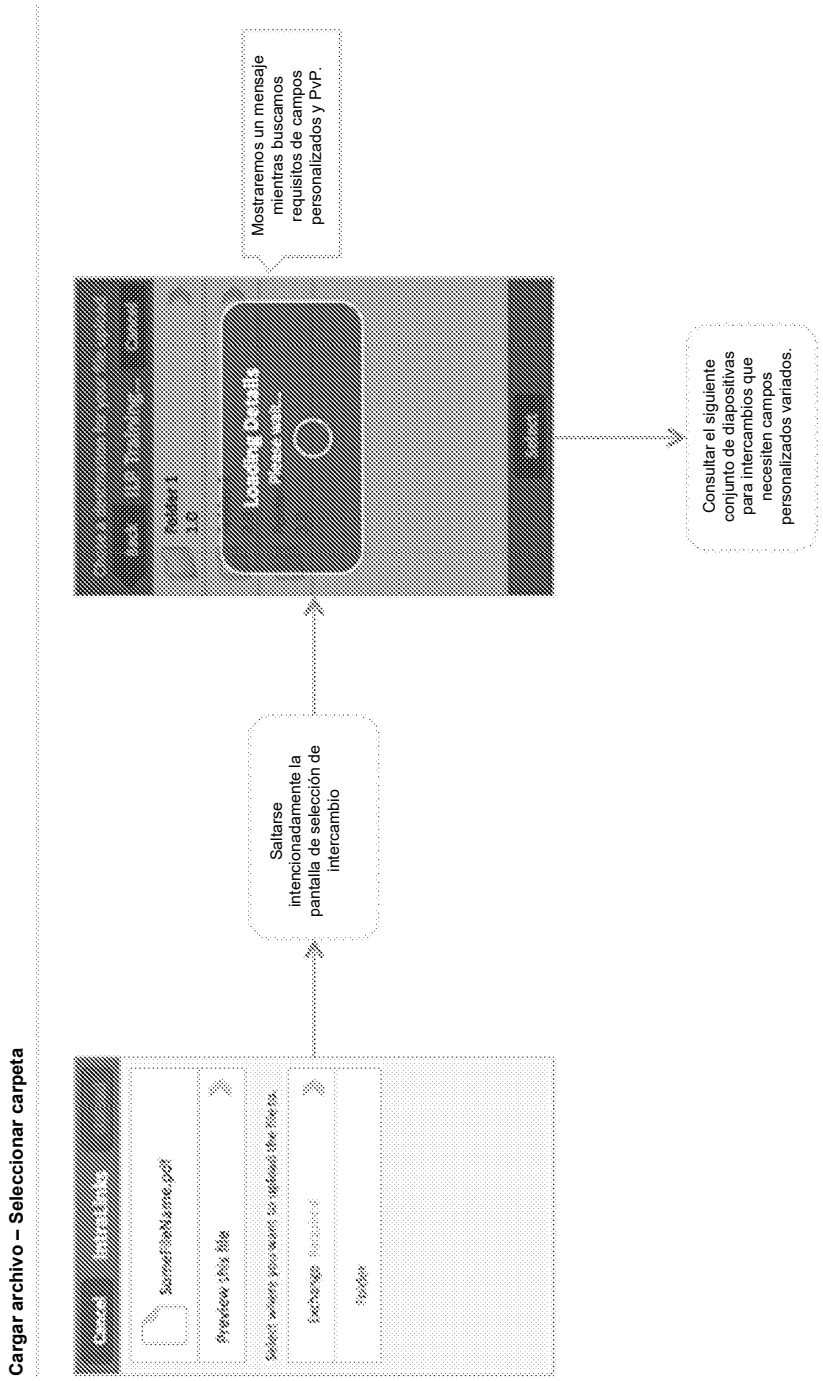

Cargar archivo – Seleccionar carpeta
Saltarse intencionadamente la pantalla de selección de intercambio
Mostraremos un mensaje mientras buscamos requisitos de campos personalizados y PvP.
Consultar el siguiente conjunto de diapositivas para intercambios que necesiten campos personalizados variados.

Fig. 9I

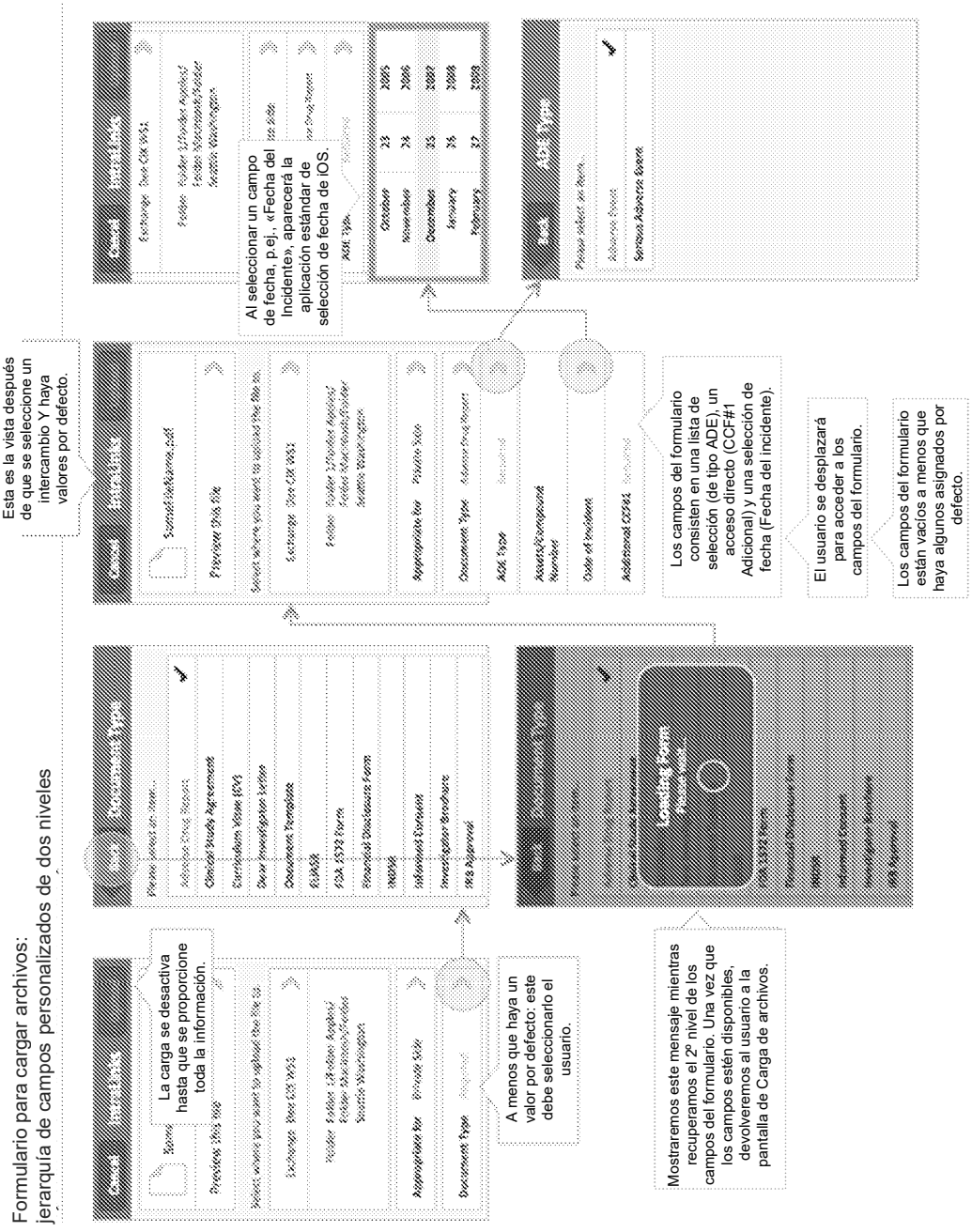

Formulario para cargar archivos:
jerarquía de campos personalizados de dos niveles
Esta es la vista después de que se seleccione un intercambio Y haya valores por defecto.
La carga se desactiva hasta que se proporcione toda la información.
A menos que haya un valor por defecto: este debe seleccionarlo el usuario.
Al seleccionar un campo de fecha, p.ej., «Fecha del Incidente», aparecerá la aplicación estándar de selección de fecha de iOS.
Los campos del formulario consisten en una lista de selección (de tipo ADE), un acceso directo (CCF#1 Adicional) y una selección de fecha (Fecha del incidente).
El usuario se desplazará para acceder a los campos del formulario.
Los campos del formulario están vacíos a menos que haya algunos asignados por defecto.
Mostraremos este mensaje mientras recuperamos el 2º nivel de los campos del formulario. Una vez que los campos estén disponibles, devolveremos al usuario a la pantalla de Carga de archivos.

Fig. 9J

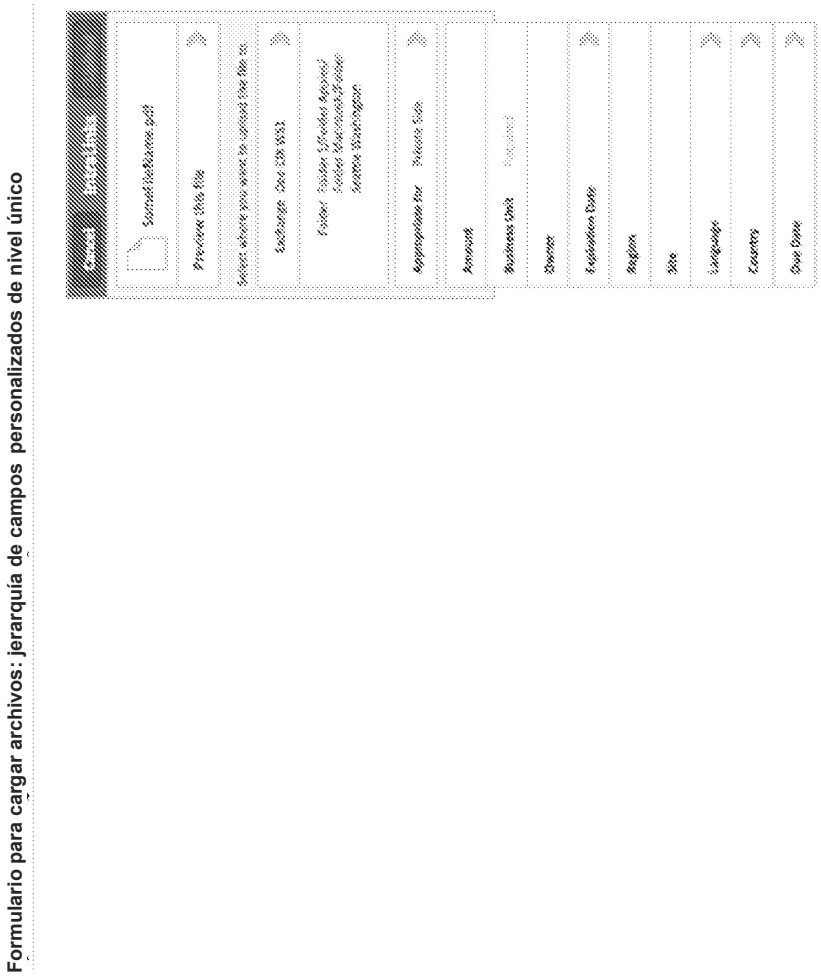

Formulario para cargar archivos: jerarquía de campos personalizados de nivel único

Fig. 9K

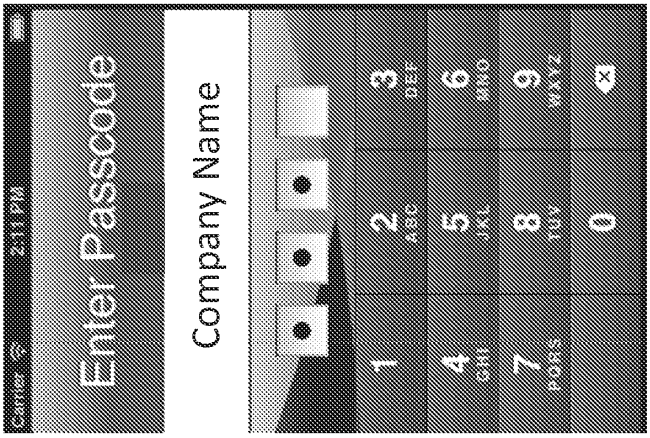

Enter Passcode
Company Name
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

Fig. 9M

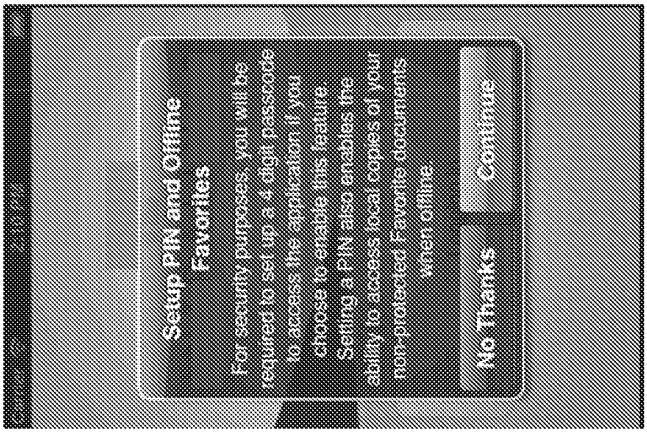

Setup PIN and Offline Favorites
for security purposes, you will be required to set up a 4 digit passcode to access the application. If you choose to enable this feature. Setting a PIN also enables the ability to access local copies of your non-protected Favorite documents when offline.
No Thanks
Continue

Fig. 9L

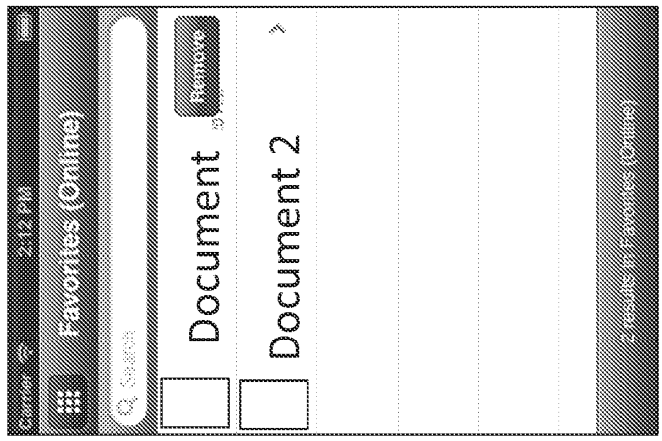


Fig. 9O

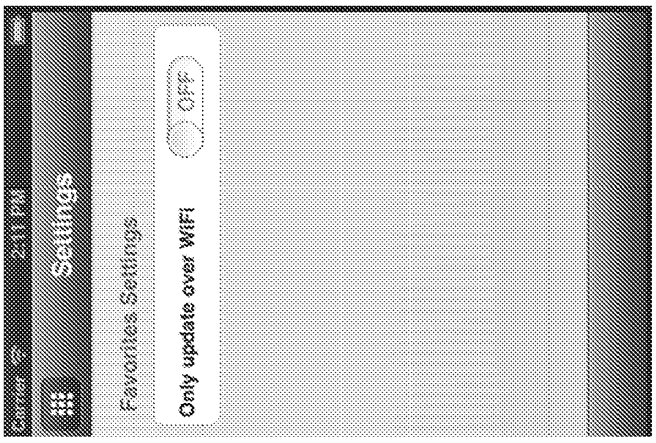


Fig. 9N

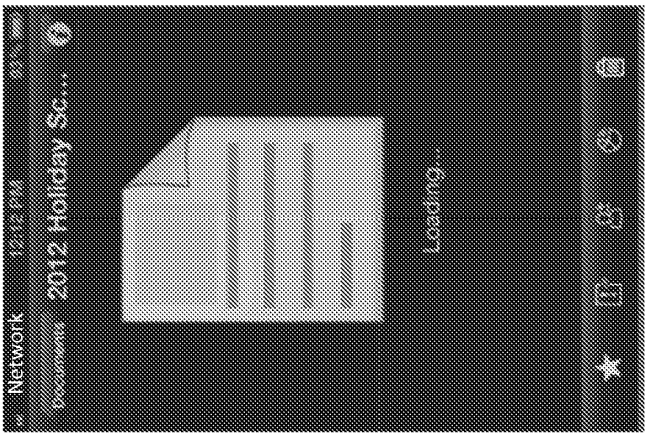


Fig. 9P

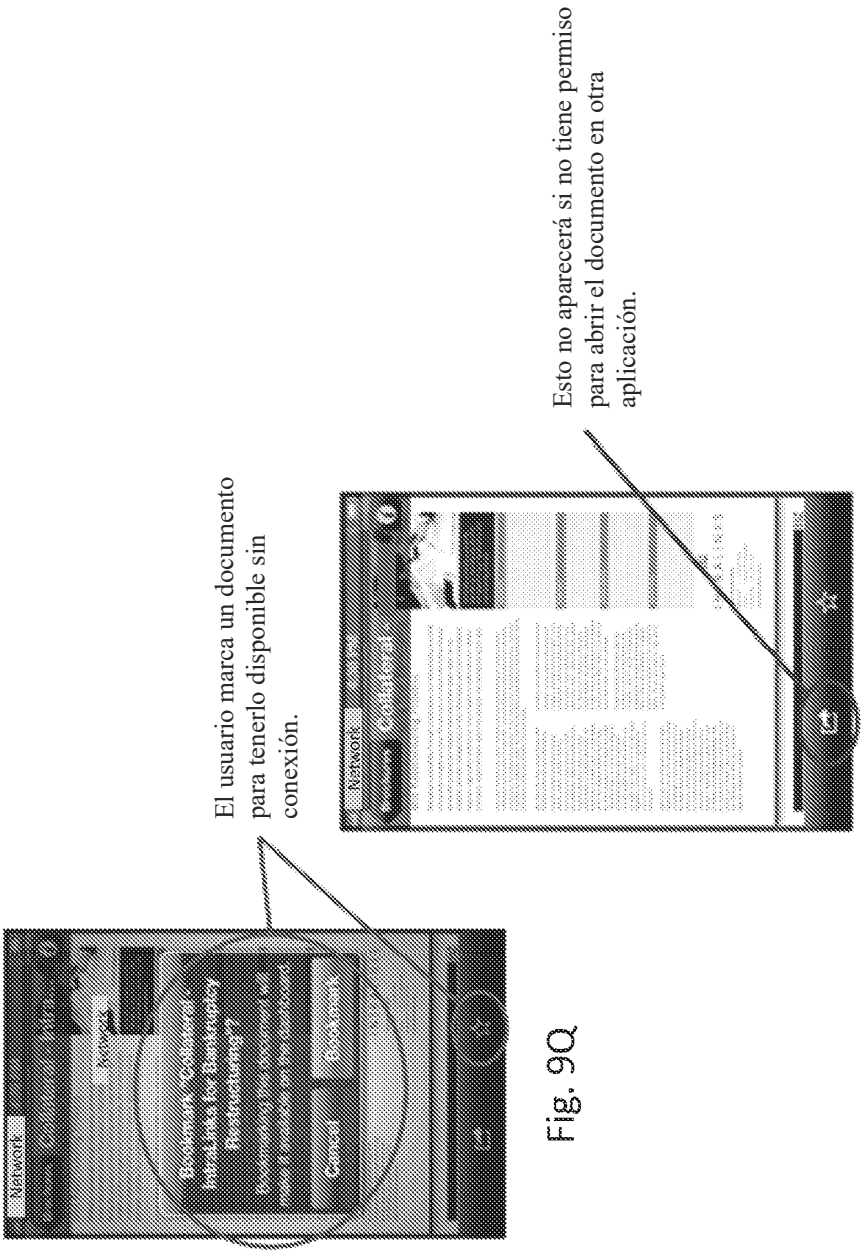


Fig. 9Q

Fig. 9R

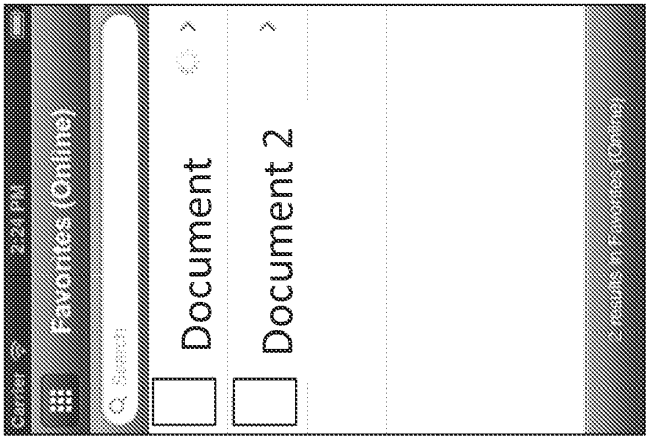


Fig. 9S

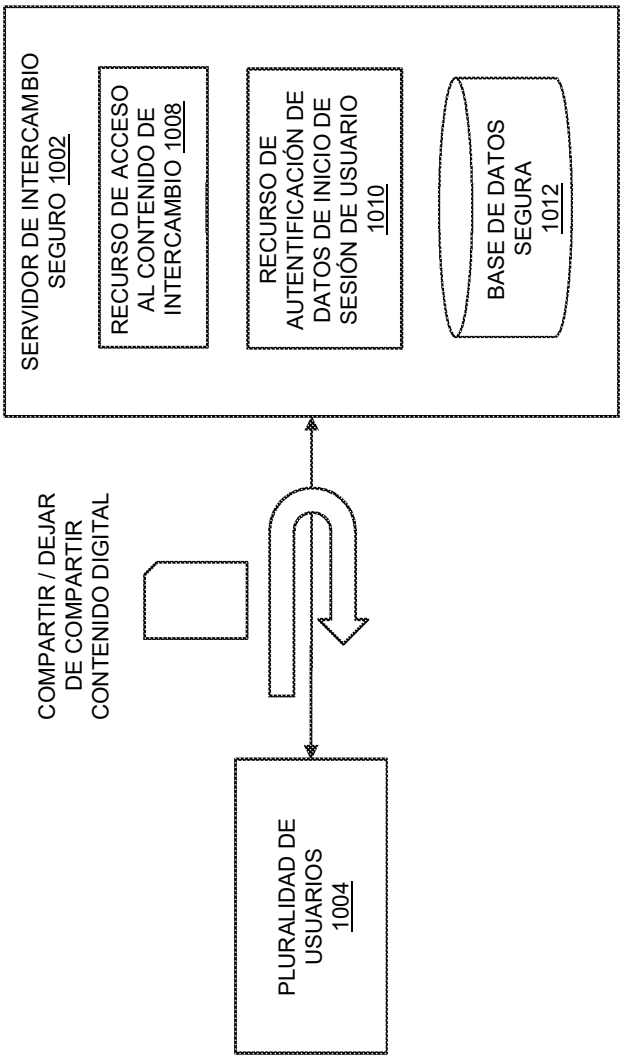

SERVIDOR DE INTERCAMBIO SEGURO 1002
RECURSO DE ACCESO AL CONTENIDO DE INTERCAMBIO 1008
RECURSO DE AUTENTIFICACIÓN DE DATOS DE INICIO DE SESIÓN DE USUARIO 1010
BASE DE DATOS SEGURA 1012
COMPARTIR / DEJAR DE COMPARTIR CONTENIDO DIGITAL
PLURALIDAD DE USUARIOS 1004
T

Fig. 10

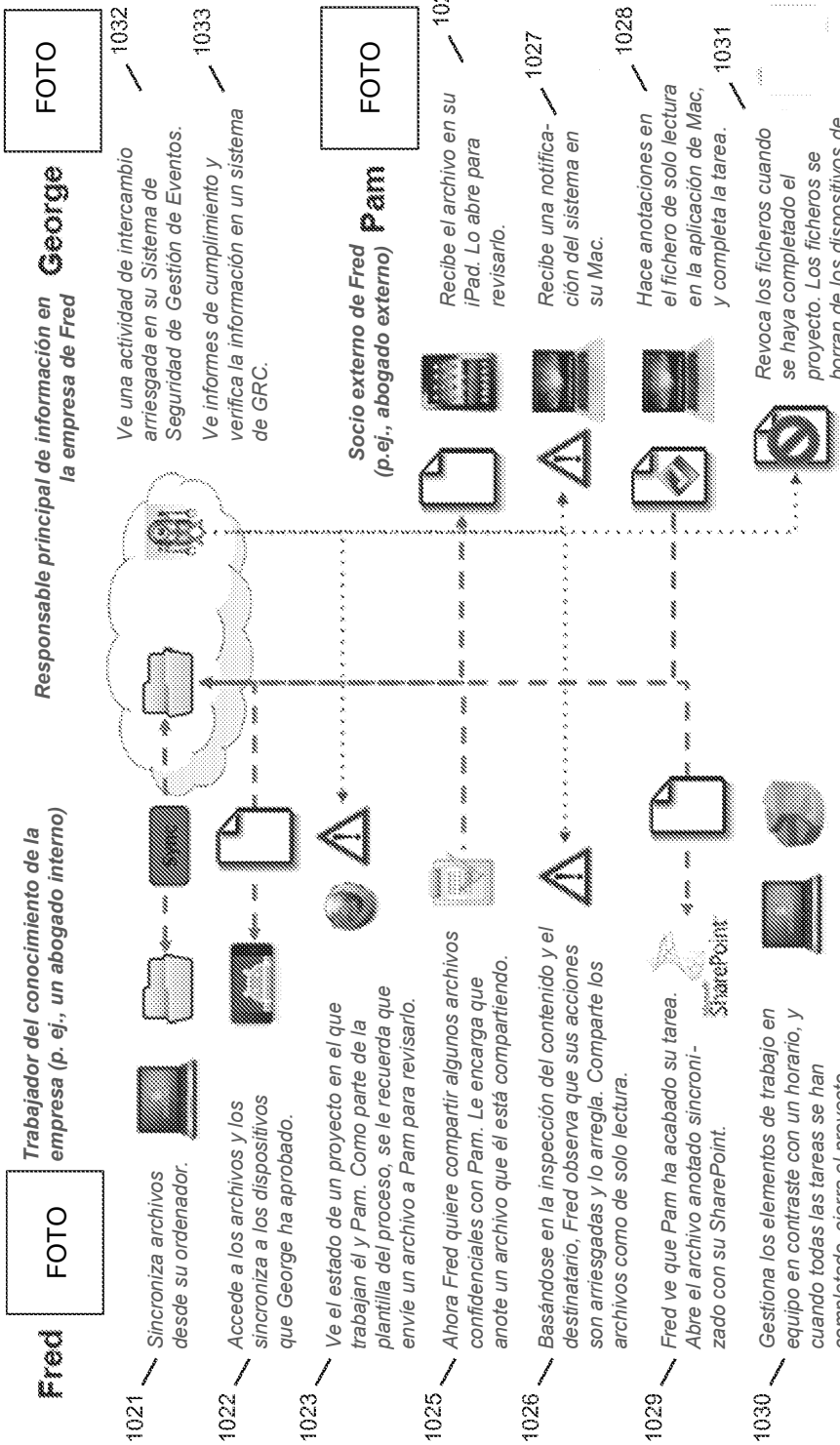

Fred
FOTO
Trabajador del conocimiento de la empresa (p. ej., un abogado interno)
Responsable principal de información en la empresa de Fred
George
FOTO
Socio externo de Fred (p.ej., abogado externo)
Pam
FOTO
1021
Sincroniza archivos desde su ordenador.
1022
Accede a los archivos y los sincroniza a los dispositivos que George ha aprobado.
1023
Ve el estado de un proyecto en el que trabajan él y Pam. Como parte de la plantilla del proceso, se le recuerda que envíe un archivo a Pam para revisarlo.
1025
Ahora Fred quiere compartir algunos archivos confidenciales con Pam. Le encarga que anote un archivo que él está compartiendo.
1026
Basándose en la inspección del contenido y el destinatario, Fred observa que sus acciones son arriesgadas y lo arregla. Comparte los archivos como de solo lectura.
1029
Fred ve que Pam ha acabado su tarea. Abre el archivo anotado sincronizado con su SharePoint.
SharePoint
1030
Gestiona los elementos de trabajo en equipo en contraste con un horario, y cuando todas las tareas se han completado, cierra el proyecto.
1032
Ve una actividad de intercambio arriesgada en su Sistema de Seguridad de Gestión de Eventos.
1033
Ve informes de cumplimiento y verifica la información en un sistema de GRC.
1024
Recibe el archivo en su iPad. Lo abre para revisarlo.
1027
Recibe una notificación del sistema en su Mac.
1028
Hace anotaciones en el fichero de solo lectura en la aplicación de Mac, y completa la tarea.
1031
Revoca los ficheros cuando se haya completado el proyecto. Los ficheros se borran de los dispositivos de Pam.

Fig. 10A

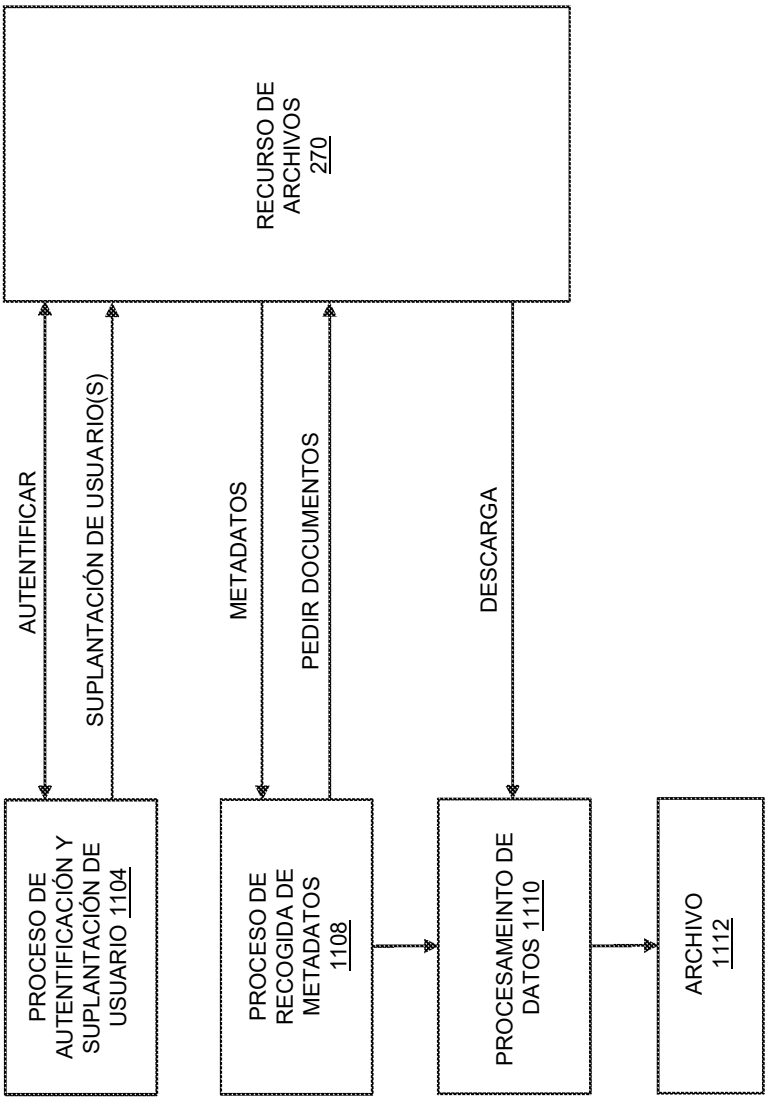

RECURSO DE ARCHIVOS 270
AUTENTIFICAR
SUPLANTACIÓN DE USUARIO(S)
METADATOS
PEDIR DOCUMENTOS
DESCARGA
PROCESO DE AUTENTIFICACIÓN Y SUPLANTACIÓN DE USUARIO 1104
PROCESO DE RECOGIDA DE METADATOS 1108
PROCESAMEINTO DE DATOS 1110
ARCHIVO 1112

Fig. 11