Sage XRT Communication & Signature

Versión 4.0.500

Datos personales

Índice

Objeto del documento **4**

Principales obligaciones europeas **5**

Seguridad de los datos **6**

Seguridad de acceso a la base de datos 6

Asignación de permisos 6

Selección del nivel de autenticación 6

Definición de una política de seguridad mediante Sage XRT Common Services 7

Gestión de perfiles, roles y usuarios 8

Funcionalidades de auditoría en la gestión de las identidades y de los accesos 8

Reporting de seguridad 10

Cumplimiento de la Ley Sarbanes Oxley 10

Datos personales y tratamientos asociados **12**

Lista de datos personales 12

Gestión de los usuarios 13

Opciones de seguridad por contrato bancario 13

Configuración 13

Reporting 14

Firmantes 15
Finalidad de los tratamientos 15
Gestión: creación, modificación, eliminación 15
Reporting sobre la base 15
Derecho a la rectificación y supresión de los datos: tiempo de conservación de los datos personales 15
Medidas de seguridad adicionales 17
Medidas generales 17
Uso de HTTPS 17
Contraseñas sólidas 17
Seguridad de los servidores por derechos de acceso 18
Protección de los servidores 18
Cifrado de los datos en tránsito 19
Seguridad del sistema de archivos 19
Medidas de aplicaciones 19
Firma de la aplicación 19
Autenticaciones 19
Autorizaciones 19
Un paso más allá 20
Advertencia 21

Objeto del documento

El Reglamento General de Protección de Datos (RGPD) se aplica desde el 25 de mayo de 2018 en los 28 países miembros de la Unión Europea.

El objetivo de este documento es identificar las funcionalidades existentes en **Sage XRT Communication & Signature** que pueden facilitar a las empresas el cumplimiento de este reglamento europeo.

©Sage 2018

Principales obligaciones europeas

Principales obligaciones sobre la protección de datos personales	Sage XRT Communication & Signature
Garantizar una seguridad apropiada	
Para garantizar la seguridad de los datos, la empresa deberá adoptar las medidas técnicas y organizativas necesarias, como la seguridad de los puestos de trabajo, de los servidores y de las unidades de almacenamiento, así como políticas o cláusulas de confidencialidad.	
Refuerzo de las contraseñas y de la protección de ciertos datos almacenados o intercambiados. (Véanse las funcionalidades existentes por lo que se refiere a la seguridad)	✔
Gestión de los derechos del interesado (derecho a la portabilidad, derecho al olvido/supresión, derecho a oponerse al tratamiento de los datos/consentimiento, derecho a la rectificación, etc.).	
En dicha gestión se preverán funcionalidades de rectificación de datos personales, de importación/exportación de datos personales y funciones de selección de personas a las que atañen los tratamientos.	
Uso de funciones de modificación/eliminación disponibles en cada aplicación y a las que se puede acceder según los permisos concedidos al usuario. (Véanse las funcionalidades existentes por lo que se refiere a los datos personales)	✔
Contribución para demostrar el cumplimiento con la normativa	
La empresa tendrá que hacer una lista de todos los documentos que demuestren las acciones llevadas a cabo para cumplir con las obligaciones referentes al RGPD europeo. Deberá poder presentar dichos documentos en caso de controles, como los documentos que describen las medidas técnicas y organizativas que ha adoptado para garantizar la seguridad del tratamiento de datos de carácter personal y el registro de tratamientos.	
Sage pone a disposición del usuario un mapa de datos personales y de tratamientos asociados para **Sage XRT Communication & Signature.** (Véase la lista de datos personales y de tratamientos asociados)	✔

©Sage 2018

Seguridad de los datos

Seguridad de acceso a la base de datos

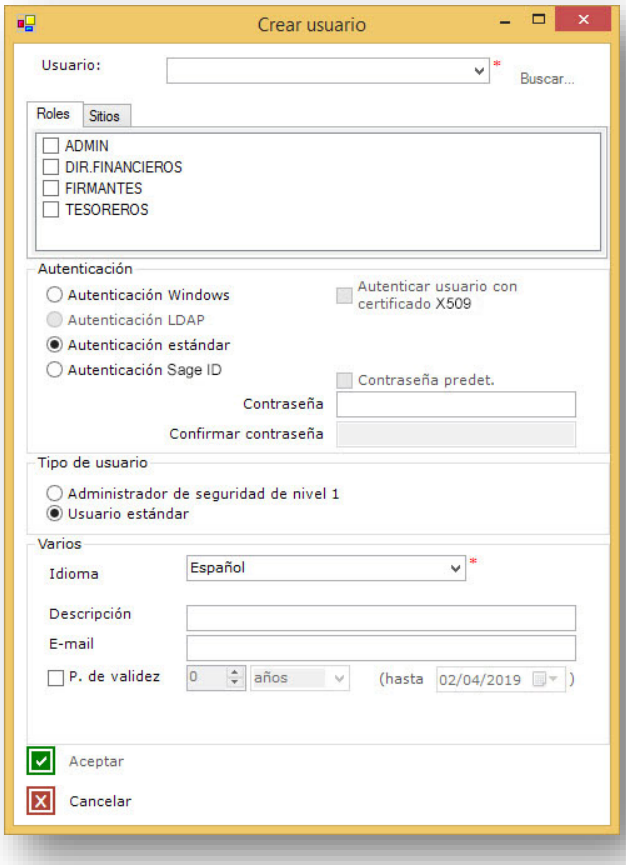
Desde la consola de administración **Sage XRT Common Services,** puede definir el tipo de gestión de los derechos de acceso de los usuarios a las aplicaciones **Sage XRT.**

Asignación de permisos

Los permisos pueden asignarse de dos formas diferentes:

- Si desea aplicar una gestión simple de los derechos de acceso a las aplicaciones, en la que solo intervendrá un único administrador de seguridad, seleccione **[Los derechos de acceso los concede un administrador de seguridad].**
- Si desea aplicar una gestión de los derechos de acceso a las aplicaciones en la que cualquier operación que realice un administrador de seguridad tenga que validarla un segundo administrador de seguridad, seleccione **[Los derechos de acceso los concede un administrador de seguridad de nivel 1 y los valida un administrador de seguridad de nivel 2].**

Selección del nivel de autenticación

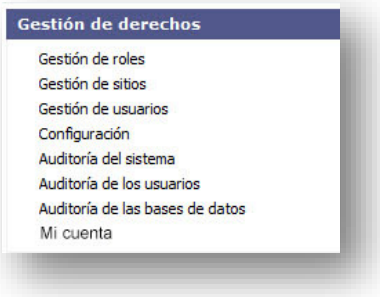


©Sage 2018

Según el tipo de autenticación decidido por el administrador para conectarse a las aplicaciones, seleccione una de las siguientes opciones:

- **Utilizar seguridad integrada de Windows:** el usuario se autentica por su cuenta de Active Directory (recomendado).
- **Utilizar un nombre de usuario y una contraseña:** el usuario se autentica mediante un nombre de usuario y una contraseña.
- **Autenticación del usuario por certificado X509:** para el cliente web, la autenticación fuerte consiste en un sistema de autenticación en dos fases:
    - Comprobación del certificado en el directorio **Active Directory** de la empresa.
    - Desafío/Respuesta entre el cliente y el componente de autenticación que permite comprobar la identidad del cliente.
- **Doble autenticación:** Se utiliza un segundo elemento para la autenticación de los usuarios con el fin de generar una contraseña de uso exclusivo.

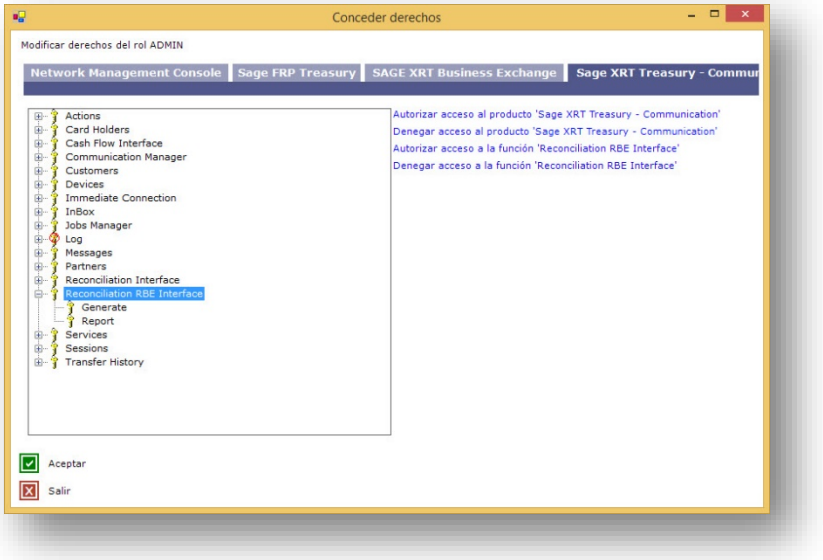
Definición de una política de seguridad mediante Sage XRT Common Services



©Sage 2018

Gestión de perfiles, roles y usuarios

Los perfiles permiten crear roles de usuarios y administradores para determinar las autorizaciones de acceso a las aplicaciones.



Funcionalidades de auditoría en la gestión de las identidades y de los accesos

Además de las distintas funcionalidades que propone, la gestión de las identidades y de los accesos debe proporcionar la prueba de su correcto funcionamiento.

Estas pruebas deberán enviarse, cuando así se solicite, a un auditor en forma de traza escrita para archivarlas.

Las pruebas proporcionadas deben abarcar los ámbitos que por lo general cubren las auditorías, entre otros:

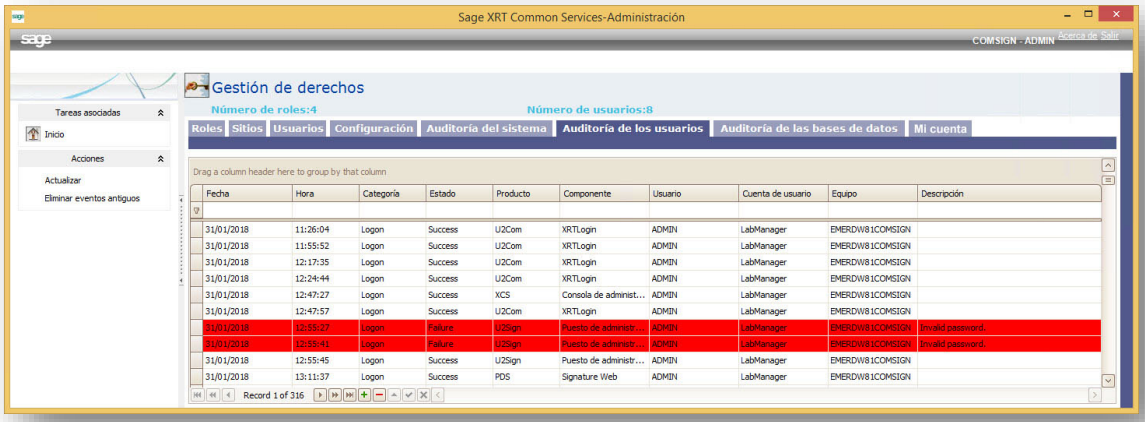
- Actividad de los administradores:
  - Crear usuarios
  - Eliminar usuarios
  - Cambiar la contraseña de un usuario
  - Cambiar la estrategia de gestión de las contraseñas
  - Cambiar la configuración de acceso al directorio LDAP
  - Conceder el acceso a una función o a un producto
  - Denegar el acceso a una función o a un producto

©Sage 2018

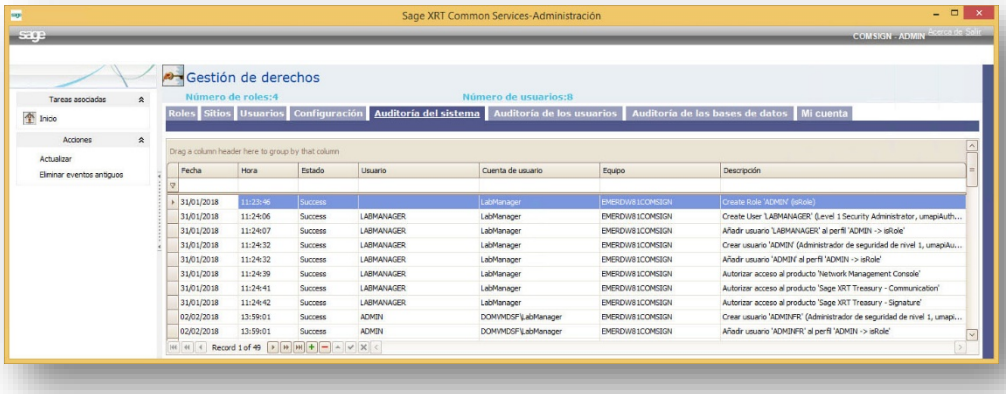
Seguridad de los datos

- Actividad de los usuarios finales:
  - Conexión de un usuario (*login*)
  - Desconexión de un usuario (*logoff*)
  - Mensajes específicos de la aplicación
- Pruebas de conformidad con la política de seguridad:
  - Cuenta de usuario bloqueada tras N intentos fallidos de conexión

En la tabla **Auditoría de los usuarios** figuran las acciones realizadas por los usuarios.



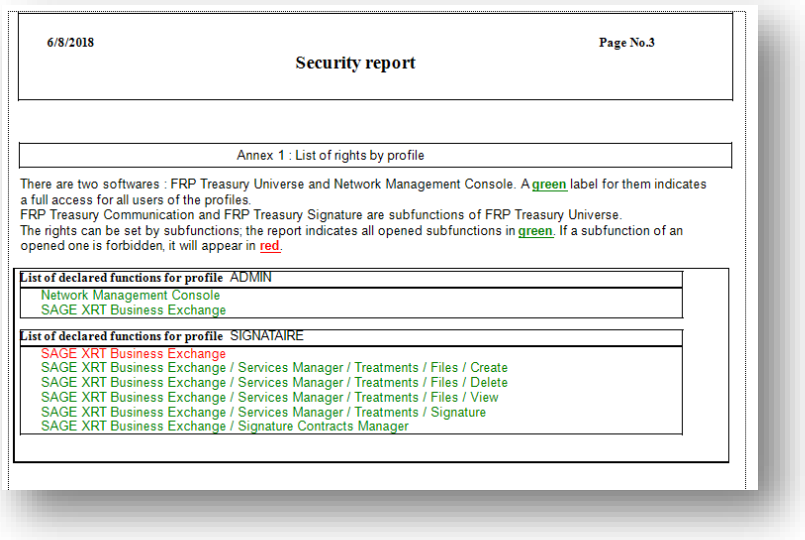
En la tabla **Auditoría del sistema** figuran todas las acciones ejecutadas en un instante T por cada usuario.



©Sage 2018

Reporting de seguridad

La consola de administración **Sage XRT Common Services** permite editar un informe en el que se detallan las funcionalidades permitidas o no permitidas para cada perfil, en cada una de las aplicaciones de la plataforma.



6/8/2018 Page No.3

Security report

Annex 1 : List of rights by profile

There are two softwares : FRP Treasury Universe and Network Management Console. A green label for them indicates a full access for all users of the profiles.
FRP Treasury Communication and FRP Treasury Signature are subfunctions of FRP Treasury Universe.
The rights can be set by subfunctions; the report indicates all opened subfunctions in green. If a subfunction of an opened one is forbidden, it will appear in red.

List of declared functions for profile ADMIN
- Network Management Console
- SAGE XRT Business Exchange

List of declared functions for profile SIGNATAIRE
- SAGE XRT Business Exchange
- SAGE XRT Business Exchange / Services Manager / Treatments / Files / Create
- SAGE XRT Business Exchange / Services Manager / Treatments / Files / Delete
- SAGE XRT Business Exchange / Services Manager / Treatments / Files / View
- SAGE XRT Business Exchange / Services Manager / Treatments / Signature
- SAGE XRT Business Exchange / Signature Contracts Manager

Cumplimiento de la Ley Sarbanes-Oxley

La Ley Sarbanes-Oxley obliga a cumplir con una serie de normas de seguridad de acceso a las aplicaciones.

En este apartado se repasan varios temas importantes asociados a la seguridad de acceso y al uso de las aplicaciones **Sage XRT** para un usuario común.

En las aplicaciones **Sage XRT,** la gestión de las contraseñas cumple las normas de la Ley Sarbanes-Oxley.

Tema de seguridad	Sage XRT Communication & Signature (cliente pesado)	Sage XRT Communication & Signature (módulo web)
El sistema debe gestionar los perfiles.	✔	✔
La contraseña es obligatoria.	✔	✔
Al crear la cuenta, se proporciona una contraseña estándar a todos o a un grupo.	✔	✔
Al conectarse por primera vez, se pedirá el cambio de contraseña.	✔ configurable	✔ configurable

©Sage 2018

Seguridad de los datos

Tema de seguridad	Sage XRT Communication & Signature (cliente pesado)	Sage XRT Communication & Signature (módulo web)
La contraseña tiene que tener seis caracteres como mínimo, entre los cuales habrá una mayúscula y una cifra.	✓ configurable	✓ configurable
La contraseña debe cambiarse cada 42 días.	✓ configurable	✓ configurable
El sistema guarda el registro de las contraseñas (histórico). Las cuatro últimas no pueden volverse a utilizar.	✓ configurable	✓ configurable
La contraseña no puede guardarse, para que no se solicite más en otras conexiones posteriores.	✓ De conformidad con una seguridad Windows completa, la contraseña que se utilizará es la de Windows. configurable ✓ De conformidad con la seguridad estándar de XRT, la contraseña de aplicación no se guarda.	✓
Si la contraseña se introduce tres veces de forma errónea, esta se bloqueará. Volverá a activarse pasados 10 minutos.	✓ configurable	✓ configurable
La cuenta no se bloqueará si no se utiliza durante varios días.	✓	✓
La sesión se bloqueará transcurridos 10 minutos de inactividad.	✗	✓ Tiempo configurable
Las normas de seguridad no pueden modificarse desde el puesto de trabajo del usuario.	✓	✓
Para acceder a la aplicación hay que iniciar sesión.	✓	✓
Para los contratos que no sean de duración indefinida, es obligatorio introducir una fecha final de validez, que coincidirá con la fecha final del contrato.	✓ configurable	✓ configurable

©Sage 2018

Datos personales y tratamientos asociados

Lista de datos personales

Los datos personales se utilizan para:

- identificar a los usuarios y controlar los accesos y las autorizaciones en la aplicación;
- realizar controles, validaciones y firmas electrónicas para los intercambios bancarios;
- recuperar archivos de datos bancarios.

Los datos financieros de los terceros permiten ejecutar las órdenes de pago resultantes de un contrato entre las partes implicadas.

Datos de carácter personal	Categoría	Finalidad
Alias del usuario	Datos del cliente	Identificación del usuario
Apellidos del usuario	Datos del cliente	Identificación del usuario: firmante
Nombre del usuario	Datos del cliente	Identificación del usuario: firmante
Correo electrónico del usuario	Datos del cliente	Identificación del usuario: firmante
Certificados del usuario	Datos del cliente	Identificación del firmante
Nombre de contacto del interlocutor financiero	Datos del cliente	Contacto del banco
Apellidos del tercero beneficiario	Datos de estado civil	Pago a proveedores, nóminas
Nombre del tercero beneficiario	Datos de estado civil	Pago a proveedores, nóminas
Dirección del tercero beneficiario	Datos de estado civil	Pago a proveedores, nóminas
Código país del tercero beneficiario	Datos del cliente	Pago a proveedores, nóminas
Teléfono del tercero beneficiario	Datos del cliente	Pago a proveedores, nóminas
Correo electrónico del tercero beneficiario	Datos del cliente	Pago a proveedores, nóminas
Fax del tercero beneficiario	Datos del cliente	Pago a proveedores, nóminas

©Sage 2018

Datos personales y tratamientos asociados

Datos de carácter personal	Categoría	Finalidad
Nombre del banco del tercero beneficiario	Datos bancarios	Pago a proveedores, nóminas
BIC del banco del tercero beneficiario	Datos bancarios	Pago a proveedores, nóminas
IBAN: Identificador de la cuenta del tercero beneficiario	Datos bancarios	Pago a proveedores, nóminas
IBAN: Identificador de la cuenta de gastos del tercero beneficiario	Datos bancarios	Pago a proveedores, nóminas
Apellidos del deudor	Datos de estado civil	Adeudos de clientes
Nombre del deudor	Datos de estado civil	Adeudos de clientes
IBAN del deudor	Datos bancarios	Adeudos de clientes
Divisa de la cuenta del deudor	Datos bancarios	Adeudos de clientes
BIC del banco del deudor	Datos bancarios	Adeudos de clientes
Referencia única del mandato	Datos del contrato	Adeudos de clientes

Gestión de los usuarios

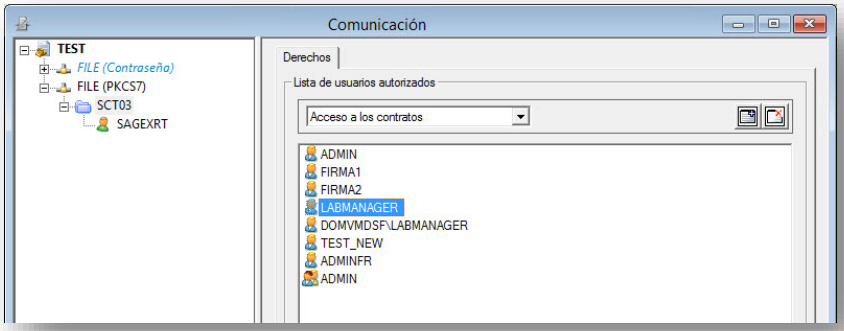
Un administrador habilitado crea los usuarios de la aplicación **Sage XRT Communication & Signature** (véase: **Definición de una política de seguridad mediante Sage XRT Common Services**).

Opciones de seguridad por contrato bancario

Configuración

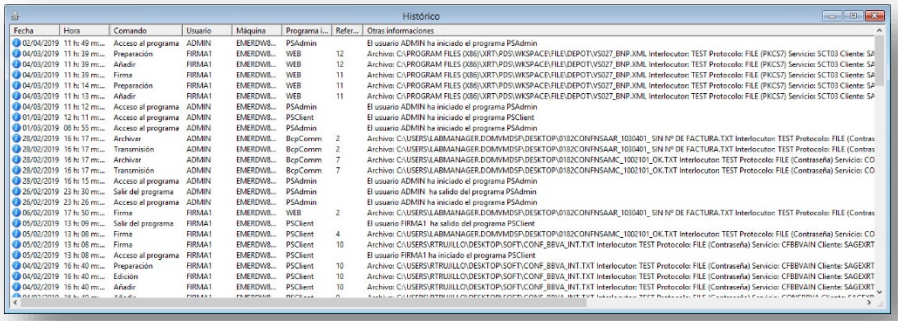
Los derechos de acceso, edición, extracción y eliminación de usuarios se configuran en los contratos de comunicación para la firma.

©Sage 2018



Reporting

Todas las acciones sobre los usuarios quedan registradas en los diarios de auditoría para el sitio **Firma Web** (creación, cambio, eliminación), o en la auditoría de administración (véase **Funcionalidades de auditoría en la gestión de las identidades y de los accesos**).



Firmantes

Finalidad de los tratamientos

Los firmantes realizan controles, validaciones y firmas electrónicas personales en los intercambios de datos financieros electrónicos entre una empresa y su interlocutor bancario.

El intercambio de datos electrónicos consiste en ejecutar las órdenes de pago resultantes de un contrato entre dos partes (pago de nóminas, facturas de proveedores, recibos bancarios...).

Gestión: creación, modificación, eliminación

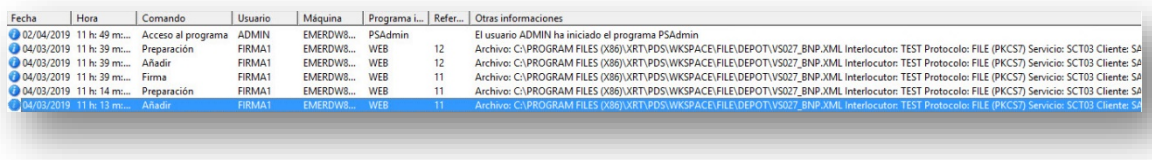
Un administrador habilitado puede crear firmantes siempre y cuando:

- el usuario se haya creado en la consola de administración Sage XRT Common Services (véase Funcionalidades de auditoría en la gestión de las identidades y de los accesos);
- el firmante se haya creado en la aplicación **Sage XRT Communication & Signature.**

Un usuario habilitado podrá modificar y eliminar un firmante.

Reporting sobre la base

Todas las acciones de los firmantes quedan registradas en el registro de eventos del servicio de transacciones.



Fecha	Hora	Comando	Usuario	Máquina	Programa i...	Refer...	Otras informaciones
02/04/2019	11 h: 49 m:...	Acceso al programa	ADMIN	EMERDW8...	PSAdmin		El usuario ADMIN ha iniciado el programa PSAdmin
04/03/2019	11 h: 39 m:...	Preparación	FIRMA1	EMERDW8...	WEB	12	Archivo: C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VS027_BNP.XML Interlocutor: TEST Protocolo: FILE (PKCS7) Servicio: SCT03 Cliente: SA
04/03/2019	11 h: 39 m:...	Añadir	FIRMA1	EMERDW8...	WEB	12	Archivo: C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VS027_BNP.XML Interlocutor: TEST Protocolo: FILE (PKCS7) Servicio: SCT03 Cliente: SA
04/03/2019	11 h: 39 m:...	Firma	FIRMA1	EMERDW8...	WEB	11	Archivo: C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VS027_BNP.XML Interlocutor: TEST Protocolo: FILE (PKCS7) Servicio: SCT03 Cliente: SA
04/03/2019	11 h: 14 m:...	Preparación	FIRMA1	EMERDW8...	WEB	11	Archivo: C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VS027_BNP.XML Interlocutor: TEST Protocolo: FILE (PKCS7) Servicio: SCT03 Cliente: SA
04/03/2019	11 h: 13 m:...	Añadir	FIRMA1	EMERDW8...	WEB	11	Archivo: C:\PROGRAM FILES (X86)\XRT\PDS\WKSPACE\FILE\DEPOT\VS027_BNP.XML Interlocutor: TEST Protocolo: FILE (PKCS7) Servicio: SCT03 Cliente: SA

Derecho a la rectificación y supresión de los datos: tiempo de conservación de los datos personales

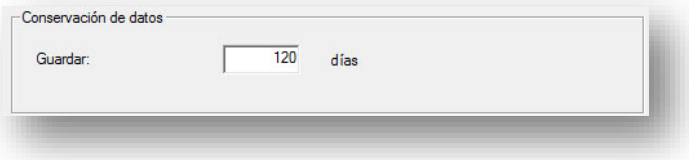
Puede modificar o eliminar cualquier dato de carácter personal de su aplicación si el interesado así lo solicita.

En todo caso, las aplicaciones proponen algunos controles técnicos que conviene respetar para llevar a cabo, con total garantía, la modificación o la supresión.

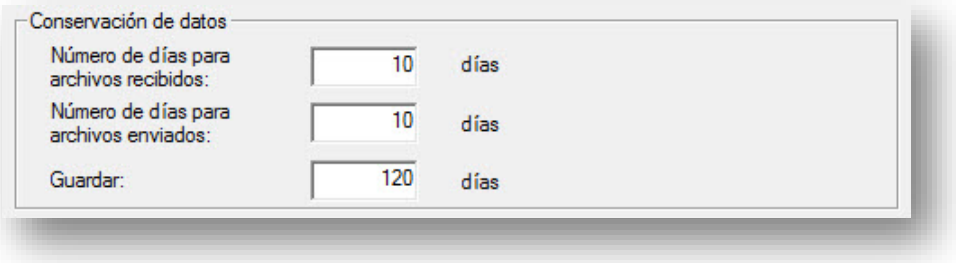
Importante: Todas las legislaciones locales imponen periodos mínimos de conservación de los datos.

Configuración del tiempo de conservación de los archivos que incluyen datos personales en Firma:

©Sage 2018



Configuración del tiempo de conservación de los archivos que incluyen datos personales en Comunicación:



©Sage 2018

Medidas de seguridad adicionales

Para minimizar el riesgo de violación de datos y de las sanciones correspondientes, es necesario seguir unos principios básicos de seguridad.

Aunque la seguridad del sistema y de la red queda bajo su responsabilidad, la plataforma de la aplicación le ofrece algunas herramientas:

- Se utilizan los navegadores web estándar y los protocolos HTTP o HTTPS. La tecnología web garantiza un aislamiento de primer nivel entre el servidor web y el puesto de trabajo.
- Las contraseñas no se transmiten a la red. El sistema de autenticación se basa en unas normas. Puede consistir en una conexión Windows controlada en un directorio LDAP o en una autenticación por certificado. Para que todo resulte más sencillo, hay disponible una solución basada en los usuarios y las contraseñas cifradas almacenadas en el servidor web. Puede añadir una doble autenticación.
- En las entidades se lleva a cabo la gestión de los derechos. Esta se basa en los perfiles de funciones asociados al usuario. También se pueden gestionar, para cada entidad, los permisos de acceso a los contratos en los servicios.

Medidas generales

Uso de HTTPS

Sage XRT Communication & Signature es una aplicación web a la que se puede acceder vía una conexión HTTP o HTTPS. Aunque HTTP esté disponible, le recomendamos que utilice siempre HTTPS para las instancias de producción, sobre todo si accede a la aplicación desde una red pública.

Contraseñas sólidas

Si utiliza este tipo de autenticación, acuérdese de establecer una política de gestión de las contraseñas, de forma que los usuarios definan una contraseña fuerte.

Para optimizar la seguridad, una contraseña fuerte tiene que cumplir con los siguientes criterios:

- Constar de 6 caracteres como mínimo (cuantos más caracteres haya, más fuerte será la contraseña).
- Combinar cifras, letras mayúsculas y minúsculas y símbolos del tipo @ # $%!? &, etc.
- No incluir un modelo de teclado del tipo Azerty.
- No incluir la fecha de nacimiento del usuario.
- No utilizar la misma contraseña en varias aplicaciones.

©Sage 2018

Seguridad de los servidores por derechos de acceso

En los servidores que alojan los componentes de la aplicación, figuran unos archivos de configuración y otros datos vulnerables a amenazas internas.

Los administradores deben ser los únicos que puedan conectarse a los servidores.

Concédales los derechos necesarios para administrar la aplicación en las carpetas correspondientes.

Importante: Los administradores de los servidores tienen que ser diferentes de los de la aplicación.

Protección de los servidores

Los servidores de la aplicación tienen que diseñarse siguiendo los estándares del sector.

Uso de cortafuegos locales

Utilice cortafuegos locales en sus servidores para bloquear cualquier puerto IP que no sea necesario para el funcionamiento de la aplicación o el acceso de los usuarios.

Por lo general, si todos los componentes de la aplicación están instalados en un mismo servidor, esta solo necesitará puertos HTTP o HTTPS para funcionar.

Para instalaciones en diferentes servidores, tendrá que abrir los puertos (o intervalos de puertos) necesarios para la comunicación entre los distintos componentes.

Seguridad de la arquitectura Internet

La arquitectura que implemente es la clave de su seguridad, sobre todo si su sistema es accesible desde una red pública.

Para conectar sus sistemas y acceder a ellos desde internet, tiene que decidir:

- qué servidores y puertos deberían verse desde el exterior;
- cómo se interceptan, traducen y dirigen esas solicitudes externas a los servidores y puertos, en su caso.

Ello implica disponer de:

- un cortafuegos, situado entre su red interna e internet para interceptar las consultas entrantes y transmitirlas a los servidores apropiados de su red;
- una DMZ o «zona desmilitarizada», es decir, una zona de red física o lógica que aísla su red local de internet.

El cortafuegos es el guardián de los puntos de control de su DMZ.

Nota: Estas recomendaciones solo se aplican si su aplicación es visible en internet. Si utiliza su propia red local, no necesitará configurar ni DMZ ni cortafuegos.

©Sage 2018

Cifrado de los datos en tránsito

La comunicación entre su capa de aplicación y su base de datos puede realizarse a través de la norma TLS (Transport Layer Security, o Seguridad de la capa de transporte).

La opción **ForceEncryption** de **SQL Server** fuerza el cifrado del protocolo y le permite preservar la confidencialidad de la información codificando los datos.

Seguridad del sistema de archivos

La seguridad del sistema de archivos de los diferentes servidores debe implementarse con las herramientas apropiadas (antivirus, seguridad de acceso a la red, etc.).

Asegúrese de que dichas herramientas no provoquen ningún problema de rendimiento.

Por ejemplo, evite ejecutar un análisis antivirus continuo en un servidor de base de datos

Medidas de aplicaciones

Firma de la aplicación

El código de su aplicación está firmado. Dicha firma certifica que el programa es legítimo y cumple con su desarrollo inicial.

Autenticaciones

La aplicación admite varios tipos de autenticación:

- **Seguridad integrada de Windows:** el usuario se autentica mediante su cuenta Active Directory. Este es el tipo de autenticación recomendable.
- **Nombre de usuario y contraseña:** el usuario se autentica mediante un nombre de usuario y una contraseña.
- **Autenticación del usuario por certificado X509:** para el cliente web, la autenticación fuerte consiste en un sistema de autenticación en dos fases:
    - Comprobación del certificado en el directorio *Active Directory* de la empresa.
    - Desafío/Respuesta entre el cliente y el componente de autenticación que permite comprobar la identidad del cliente.
- **Doble autenticación:** un segundo elemento se utiliza para la autenticación de los usuarios con el fin de generar una contraseña de uso exclusivo.

Autorizaciones

Un usuario tiene acceso a uno o varios contratos bancarios. Este se asocia a un perfil que determina sus derechos de acceso a las funciones de la aplicación y sus privilegios (acceso, creación, modificación y eliminación).

©Sage 2018

En cada contrato bancario, se pueden configurar unas autorizaciones específicas para los usuarios y los firmantes (acceso a los contratos y a las ediciones, derechos de archivado y de extracción de datos).

Gracias a estas funcionalidades, puede definir, de otra forma, el acceso a los datos críticos en cada entidad para un usuario determinado.

Importante: Asegúrese de mantener estas reglas en el tiempo. Simplifíquelas al máximo, sin que por ello se vea comprometida su política de seguridad.

Un paso más allá

La aplicación de estas medidas de seguridad adicionales requiere algunas competencias, así como el asesoramiento que nuestros equipos de consultoría pueden ofrecerle.

Nos comprometemos a ponernos en contacto con usted si desea aplicar estas recomendaciones.

©Sage 2018

Advertencia

La información referente al Reglamento General de Protección de Datos (en adelante «RGPD») que proporciona Sage es general y meramente informativa. En ningún caso constituye asesoramiento legal o profesional. Sage no puede garantizar que una información dada reproduzca con exactitud una normativa o una ley adoptada oficialmente. En caso de discrepancia, prevalecerá el texto publicado en el Diario Oficial.

Aunque hayamos hecho todo lo posible por asegurarnos de que la información proporcionada sea exacta y esté actualizada, esta se facilita «tal cual», sin garantía de ninguna clase, ni explícita ni implícita. Sage no se responsabiliza de ningún error u omisión, ni de ningún daño (entre los que se incluyen, entre otros, los daños en relación con la pérdida de clientes o de beneficios) que se pudieran desprender del uso de la información facilitada o de cualquier medida o decisión que se tome atendiendo a dicha información.

Nuestros programas integran funciones cuyo objetivo es ayudar al usuario en sus procesos de cumplimiento con el RGPD. No obstante, queremos recalcar a los usuarios que el solo uso de las aplicaciones no garantiza su conformidad con el RGPD.

Recuerde que la información facilitada no significa que los usuarios de las aplicaciones de Sage se abstengan de consultar a un asesor legal para obtener toda información concerniente al RGPD y poder cumplir con él.

©Sage 2018