



# Sage XRT Business Exchange

Versión 12.3

Configuración de la seguridad



# Índice

<b>Descripción .....</b>	<b>4</b>
<b>Integridad y seguridad .....</b>	<b>5</b>
Configuración de la pestaña Integridad del sitio Master .....	5
Activación de la integridad por primera vez .....	5
Configuración de las opciones de integridad .....	7
Modificación de la configuración de la integridad .....	9
Modificación de la contraseña .....	10
Utilidades de cálculo y de comprobación de las firmas .....	11
Errores de conexión.....	13
Elementos afectados .....	15
Datos firmados .....	15
Tablas afectadas .....	15
Importación y exportación de la configuración .....	16
Notificaciones.....	16
Descripción de las alertas.....	16
Auditorías .....	17
Auditoría de los usuarios de Sage XRT Common Services.....	17

Auditoría de la integridad de los datos .....	18
Auditoría de los errores de conexión .....	20
Derechos de Sage XRT Common Services en la pestaña Integridad .....	20
<b>Integridad de las herramientas DMZ .....</b>	<b>21</b>
<b>Notificaciones de detección de ataques .....</b>	<b>23</b>
<b>Workspace .....</b>	<b>24</b>
<b>Anexo .....</b>	<b>25</b>
<b>Advertencia.....</b>	<b>27</b>

# Descripción

Para aumentar la seguridad de la aplicación, desde la pestaña **Integridad** de **Administración de sistemas**, puede configurar diferentes opciones:

- La integridad calcula una firma en los campos de los contratos bancarios (**Integridad Base de datos**), en las claves del Registro de Windows (**Integridad Registro de Windows**), en los archivos de la aplicación Online Banking (**Integridad Sitio Online Banking**), en los *scripts* (**Integridad Script**) y en los archivos del VFS (**Integridad VFS**).
- Las anomalías en los contratos permiten detectar errores de integridad debido a intrusiones.
- Las anomalías de conexión de los contratos bancarios permiten detectar fallos en las conexiones y suspender los contratos bancarios solicitantes.
- El contrato de notificación permite definir la entidad y el alias de notificación para todas las anomalías de integridad, conexión y ataques SQL Injection, XSS (Cross-Site Scripting) y CSRF (Cross-Site Request Forgery).

Acceptar Cancelar

Base de datos Parámetros Internet Permisos Parámetros del PMP Integridad

Integridad

☒ Base de datos

☒ Sitio Online Banking

☒ VFS

☒ Script

☒ Registro de Windows

Anomalías en los contratos

☒ Detección de errores de conexión

☒ Suspender el contrato

Contrato de notificación

Entidad: SAGEXRT

Alias: INTEG

Suspender el acceso

No iniciar la transferencia

Ninguna acción

Ninguna acción

Opciones...

**Importante:** En modo multisitio, los sitios derivados heredan la configuración del sitio «Master». Desde los sitios derivados no se puede acceder a la pestaña **Integridad**.

## Integridad y seguridad

### Configuración de la pestaña Integridad del sitio Master

Esta configuración permite calcular y comprobar la firma:

- de la Base de datos (de los contratos solicitantes);
- del sitio Online Banking;
- del VFS (de los archivos de lectura (receptor) y escritura (emisor));
- de los scripts;
- del Registro de Windows.

Al activar la integridad, un agente Watch comprueba en tiempo real:

- Las acciones **Crear**, **Cambiar**, **Renombrar** y **Eliminar** en todos los archivos de la carpeta de la aplicación **Online Banking**.
- Cualquier intervención en el **Registro de Windows**.


El agente Watch identifica las intrusiones no autorizadas y se lo notifica a los administradores.

### Activación de la integridad por primera vez

Se deben detener todos los servicios de **Sage XRT Business Exchange**.

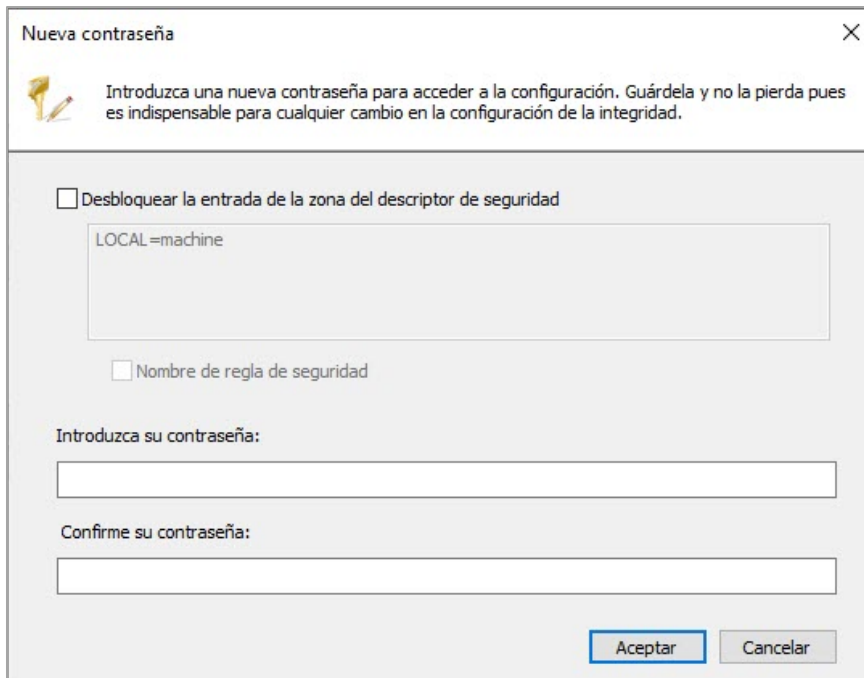
Para activar las opciones de configuración, es necesario introducir una contraseña.

**Importante:** Guarde dicha contraseña de forma segura. Tendrá que utilizarla cada vez que quiera modificar la integridad. Si la pierde, deberá reinstalar la aplicación por completo.

Haga clic en el icono de **bloqueo**  para acceder a la ventana de creación de la contraseña.



## Integridad y seguridad



**Desbloquear la entrada de la zona del descriptor de seguridad:** esta opción permite garantizar la seguridad de acceso a la clave de la contraseña. Por defecto, la configuración se define en **LOCAL=MACHINE**.

**Nota:** Para obtener información sobre la sintaxis de los descriptores de seguridad autorizados para este campo, consulte la documentación de Microsoft (versión en inglés):  
<https://msdn.microsoft.com/en-us/library/cc230368.aspx>  
[https://msdn.microsoft.com/en-us/library/windows/desktop/hh769091\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/hh769091(v=vs.85).aspx)  
[https://msdn.microsoft.com/en-us/library/windows/desktop/hh870248\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/hh870248(v=vs.85).aspx)

En la parte Anexo de este documento, figuran algunos ejemplos de configuración.

Complete los campos Introduzca su contraseña y Confirme su contraseña.

**Importante:** Para proteger la caja de seguridad de las contraseñas con más de **dos SID**, hay que utilizar un servicio Active Directory (AD) con un modo de compatibilidad del bosque (*forest*) igual a 2012 como mínimo.








Comando en PowerShell para obtener la versión:  
`[system.directoryservices.activedirectory.Forest]::GetCurrentForest().ForestMode`

**Importante:** Para activar la configuración de las opciones **Integridad** de la base de datos, del sitio **Online Banking** y del registro SXBE del Registro de Windows, hay que introducir la contraseña.

### Configuración de las opciones de integridad

El control de la integridad puede activarse en los elementos siguientes:

- Base de datos
- Sitio Online Banking
- VFS
- Script
- Registro de Windows

Integridad	
<input checked="" type="checkbox"/> Base de datos	
<input checked="" type="checkbox"/> Sitio Online Banking	  
<input checked="" type="checkbox"/> VFS	
<input checked="" type="checkbox"/> Script	
<input checked="" type="checkbox"/> Registro de Windows	

Suspender el acceso	▼
No iniciar la transferencia	▼
Ninguna acción	▼
Ninguna acción	▼

Los botones de **cálculo** (primera columna de iconos) permiten iniciar el cálculo de la firma.

Los botones de **comprobación** (segunda columna de iconos) se utilizan para comprobar la firma.

**Nota:** Hay que detener los servicios para poder habilitar los botones y poder acceder a las opciones.

Si marca la opción **Sitio Online Banking**, seleccione, en la lista desplegable correspondiente, la acción que se realizará si se detecta algún problema de integridad:

- **Ninguna acción**

Si se ha realizado la configuración de las notificaciones, se enviará un correo electrónico al administrador para advertirle de que uno o varios archivos están dañados. La actividad en el sitio **Online Banking** sigue su curso.

- **Suspender el acceso**

Aunque un único archivo de la aplicación esté dañado, el sitio **Online Banking** se suspende y aparece un mensaje de error: «*La integridad del sitio ya no está garantizada. Póngase en contacto con su administrador urgentemente*». Si se ha realizado la configuración de las notificaciones, se enviará un correo electrónico al administrador para advertirle de que uno o varios archivos están dañados.

**Importante:** Si se ha activado la integridad del sitio **Online Banking** y si el descriptor de seguridad es diferente de LOCAL=MACHINE, la identidad del grupo de aplicaciones de IIS debe ser una cuenta AD o una cuenta local (una cuenta que no sea virtual).

## Integridad y seguridad

Si marca la opción **Script**, seleccione, en la lista desplegable correspondiente, la acción que se realizará si se detecta algún problema de integridad.

- **Ninguna acción**

Si se ha realizado la configuración de las notificaciones, se enviará un correo electrónico al administrador para advertirle de que uno o varios archivos están dañados. La actividad sigue su curso.

- **No autorizar la ejecución**

El script dañado no se ejecuta.

**Importante:** Los scripts se firman y comprueban si están almacenados en la carpeta \scripts de la aplicación SXBE.

Existe la posibilidad de cambiar de carpeta vía la variable INSTALLSCRIPTS: // RUTA DE DESTINO DE LOS SCRIPTS

Los scripts se supervisan durante la ejecución.

Si marca la opción **VFS**, seleccione, en la lista desplegable correspondiente, la acción que se realizará si se detecta algún problema de integridad:

- **Ninguna acción**

Si se ha realizado la configuración de las notificaciones, se enviará un correo electrónico al administrador para advertirle de que el archivo de lectura (receptor) o de escritura (emisor) se ha dañado en la transmisión. La actividad sigue su curso.

- **No iniciar la transferencia**

El archivo se retiene y la transferencia no se realiza. El administrador recibe una notificación por correo electrónico para advertirle de que el archivo que se va a transferir está dañado.

Si marca la opción **Registro de Windows**, seleccione, en la lista desplegable correspondiente, la acción que se realizará si se detecta algún problema de integridad:

- **Ninguna acción**

Si se ha realizado la configuración de las notificaciones, se enviará un correo electrónico al administrador para advertirle de que uno o varios archivos están dañados. La actividad sigue su curso.

- **Detener el servicio**

La actividad se detiene por completo. Si se ha realizado la configuración de las notificaciones, se enviará un correo electrónico al administrador para advertirle de que uno o varios archivos están dañados.

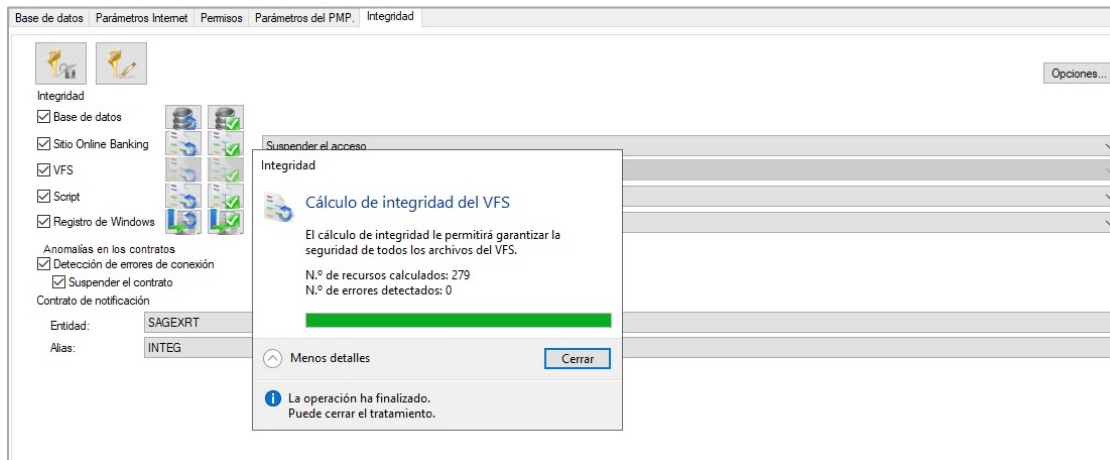
- **Suspender el acceso**

La actividad del servicio se suspende. Si se ha realizado la configuración de las notificaciones, se enviará un correo electrónico al administrador para advertirle de que uno o varios archivos están dañados.

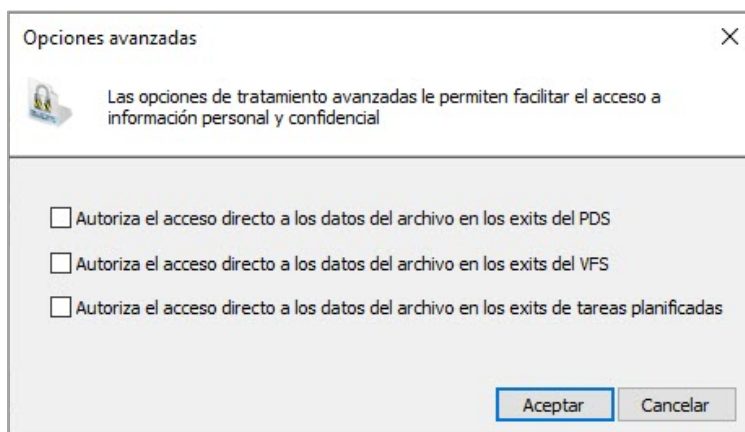


## Integridad y seguridad

En el momento en que se marca una de las opciones (**Base de datos**, **Sitio Online Banking**, **Script**, **VFS** o **Registro de Windows**), el cálculo de la firma se inicia de forma automática.



Las opciones avanzadas le permiten conceder los permisos necesarios para los tratamientos de datos de carácter confidencial y personal.




## Modificación de la configuración de la integridad

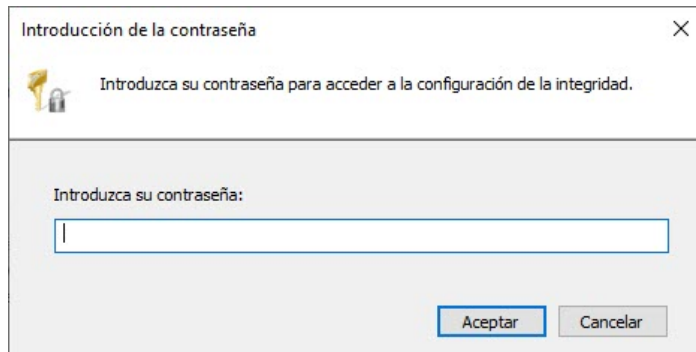
**Importante:** Hay que detener todos los servicios para modificar la configuración.

Puede realizar los siguientes cambios en la configuración del control de la integridad:

- Desactivar el control de las firmas
- Recalcular las firmas: **Cálculo** (/COMPUTE)
- Comprobar las firmas: **Comprobación** (/CHECK)

Para modificar la configuración, haga clic en el icono de **bloqueo**  e introduzca la contraseña en el cuadro de diálogo que aparece en pantalla.

## Integridad y seguridad

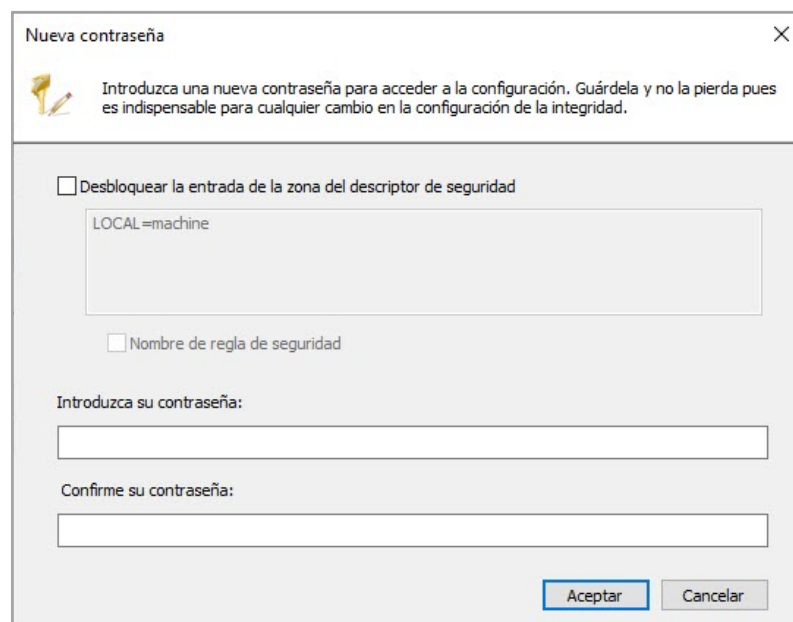
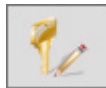


**Nota:** Si la opción **Integridad** está desactivada, no se realizará ningún recálculo.

## Modificación de la contraseña

**Importante:** Hay que detener todos los servicios para modificar la contraseña.

Haga clic en el botón **Cambiar**



En el cuadro de diálogo **Nueva contraseña**, introduzca la contraseña, confírmela y haga clic en **Aceptar**.

**Nota:** Si los servicios se están ejecutando, solo estarán disponibles las acciones de **comprobación**.

### Utilidades de cálculo y de comprobación de las firmas

#### Integridad en la base de datos de los contratos solicitantes (P5SECDB)

La utilidad **P5SECDB** permite calcular y comprobar el estado de integridad de la base de datos para los contratos solicitantes.

Por defecto, la utilidad activa el comando **CHECK** si no se ha indicado ninguna otra configuración.

Uso: P5SECDB {/CHECK   /COMPUTE} [/P: /S: /C: /T: /LOG: /SERVER:]	
<i>/CHECK</i>	Comprobación de la firma de la base de datos
<i>/COMPUTE</i>	Cálculo de la firma de la base de datos
<i>/LOG</i>	Nombre del archivo de LOG
<i>/P:</i>	Filtro entidad
<i>/S:</i>	Filtro servicio
<i>/C:</i>	Filtro cliente
<i>/T:</i>	Filtro protocolo
<i>/SERVER:</i>	Nombre del sitio (permite encontrar los recursos asociados al sitio (ejemplo: SRV_Test))

**Importante:** Aunque solo haya un único elemento incorrecto en el contrato solicitante, este no se podrá utilizar. La información se serializa en el registro de auditoría cada vez que se intenta utilizar el contrato.

La utilidad se puede programar para la acción */CHECK*. En caso de error de integridad, los errores se compilan en un archivo XML que se envía por correo electrónico.

#### Integridad del sitio Online Banking y de los scripts (P5SECFILE)

La utilidad **P5SECFILE** permite calcular y comprobar la firma:

- de los archivos del sitio **Online Banking**;
- de los scripts;
- de los archivos del **VFS**.

Se realiza un control de integridad en todos los archivos del sitio, en los scripts y en los archivos de lectura (receptor) y escritura (emisor) del VFS.

Uso: P5SECFILE {/CHECK   /COMPUTE} [/LOG:]	
/CHECKOLB	Comprobación de la firma de los archivos de Online Banking
/CHECKSCR	Comprobación de la firma de los scripts
/CHECKBIN	Comprobación de la firma de archivos binarios de la aplicación
/CHECKVFS	Comprobación de la firma de los archivos del VFS
/COMPUTEOLB	Cálculo de la firma de los archivos de Online Banking
/COMPUTESCR	Cálculo de la firma de los scripts
/COMPUTEVFS	Cálculo de la firma de los archivos del VFS
/LOG	Nombre del archivo de LOG

**Importante:** El control se realiza en todo el sitio **Online Banking** antes de que se inicie. Si se detecta alguna intrusión, puede que no se inicie. El control también puede llevarse a cabo en los archivos binarios de la aplicación (/CHECKBIN). La utilidad se puede programar para la acción /CHECK. En caso de error de integridad, los errores se compilan en un archivo XML que se envía por correo electrónico.

### Integridad del Registro de Windows (P5SECREG)

La utilidad **P5SECREG** permite calcular y comprobar la firma del Registro de Windows.

Las claves firmadas y comprobadas en el Registro son las siguientes:

- SMP-P5 (y su versión multisitio)
- AUTO
- COM
- ISAPI
- NTF
- PDS
- RCP
- WEB

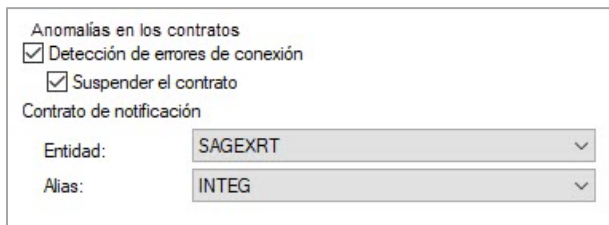
Uso: P5SECREG {/CHECK   /COMPUTE} [/LOG: /SERVER:]	
/CHECK	Comprobación de la firma del Registro de Windows
/COMPUTE	Cálculo de la firma del Registro de Windows
/COMPUTER:	Comprobación del Registro de Windows en otra máquina (Nombre de la máquina)
/LOG	Nombre del archivo de LOG
/SERVER:	Nombre del sitio

**Importante:** La utilidad se puede programar para la acción **/CHECK**. En caso de error de integridad, los errores se compilan en un archivo XML que se envía por correo electrónico.

## Errores de conexión

En el apartado **Anomalías en los contratos**, marque la opción **Detección de errores de conexión** para guardar en el archivo de Log las fases de conexión lógica o física con errores para los contratos bancarios solicitantes. A continuación, se enviará una notificación sobre dichos errores.

Si se selecciona dicha opción, se podrá acceder también a la opción **Suspender el contrato**.



Anomalías en los contratos

☒ Detección de errores de conexión

☒ Suspender el contrato

Contrato de notificación

Entidad: SAGEXRT

Alias: INTEG

En caso de que se supere el número de intentos indicado en la configuración de enlace del contrato solicitante, se suspenderá el contrato bancario.

## Integridad y seguridad

Gestión de enlaces

Este cuadro de diálogo le permite realizar la gestión de sus conexiones de red.

EXT

EXT

Configurar enlaces

Dispositivo

Identidad

Código: EXT

Información

Descripción:

Configurar reintentos

Número total de reintentos: 5

Intervalo de reintentos: 2 minutos

Número de reintentos enlace principal: 3

En caso de fallo

☐ Enviar un aviso

☐ Iniciar el exit de conexión

Añadir Cambiar Eliminar Salir

Después de suspender el contrato, no se podrá realizar ninguna conexión sin que intervenga el administrador.

La opción **Deshabilitado** se activa en el contrato solicitante.

General Conexión Escritura Lectura Puesto de firma

Información

Descripción: Propiedades avanzadas:

Política de seguridad

Periodo de validez

Fecha inicio: 03/12/2019 Fecha fin: 03/12/2029

Estado

☒ Deshabilitado

Enlace

EXT

Si no se indica ningún reintento, el contrato no se suspenderá.



## Elementos afectados

### Datos firmados

Todos los datos del contrato solicitante se firman (incluidos los **Datos del enlace Protocolo** y la configuración **Red** de la pestaña **Dispositivo**), salvo **Descripción y propiedades avanzadas**.

### Tablas afectadas

Tabla	Descripción	Comentario
HTTPMD	Contrato HTTP	Adición de la columna HASHSIGNATURE varchar (255) NULL
OFTPMD	Contrato Odette FTP	
SWIFTFTIMD	Contrato Swift	
EXTMD	Contrato External	
CPFMD	Contrato CopyFile	
MOMMD	Contrato MsMQ	
SMTPOP3MD	Contrato eMail	
X400MD	Contrato X400	
AS2MD	Contrato AS2	
SOAPMD	Contrato Soap	
PADEFMD	Contrato PaDeF	
SFTPMMD	Contrato SFTP	
EB3MD	Contrato EDI3	
PTDMD	Contrato PeSIT D	
PTEMD	Contrato PeSIT E	
FTPMMD	Contrato FTP	
EBICSMD	Contrato EBICS	
EBICSUSERS_DEM	Parámetro de identificación EBICS	
LIEN_NTW	Enlace	

## Integridad y seguridad

X25	Enlace / dispositivo de red X25	
TCPIP	Enlace / dispositivo de red TCPIP	
RDSI	Enlace / dispositivo de red RDSI	
RTC	Enlace / dispositivo de red RTC	

## Importación y exportación de la configuración

Si la opción **Integridad Base de datos** está marcada, la importación de la configuración, realizada desde la interfaz gráfica, calcula de forma automática el *hash* de firma.

La importación vía *IMPVIR* requiere la introducción de la contraseña.

En cambio, la contraseña no se solicita durante la exportación de la configuración. El tratamiento es idéntico al de la utilidad *EXPVPS*.

**Importante:** Los datos de enlace o de parámetros de identificación no asociados a un contrato bancario no se firman (datos de pruebas, por ejemplo). Estos datos se integrarán durante la exportación.

## Notificaciones

La configuración de las notificaciones se realiza en el apartado **Contrato de notificación** de la pestaña **Integridad** del sitio Master.

Debe introducir una **Entidad** y un **Alias**.

Contrato de notificación	
Entidad:	SAGEXRT
Alias:	INTEG

## Descripción de las alertas

Sitio Online Banking

- Asunto del email: Alerta de seguridad del sitio Online Banking [Nombre de la máquina, tenant físico (sitio, servidor)]
- Contenido: El sitio Online Banking se ha suspendido debido a la detección de una intrusión. Consulte el LOG para obtener más información.

## Integridad y seguridad

### Script

- Asunto del email: Alerta de control de integridad de los archivos
- Contenido: X/X archivo(s) no es (son) válido(s). Consulte el detalle del (de los) archivo(s) incorrecto(s) disponible en el archivo adjunto.

### Datos del contrato bancario

- Asunto del email: Alerta de control de integridad de la base de datos
- Contenido: X/X registro(s) no es(son) válido(s). Consulte el detalle del (de los) registro(s) incorrecto(s) en el archivo adjunto.

### Registro de Windows

- Asunto del email: Alerta de integridad del Registro de Windows [Nombre de la máquina, tenant físico (sitio, servidor)]
- Contenido: El Registro de Windows ha sufrido una acción que ha modificado su integridad. Consulte el LOG para obtener más información.

### Detección de fallos de conexión

- Asunto del email: Alerta de fallo de conexión [Nombre de la máquina, tenant físico (sitio, servidor)]
- Contenido: Se ha superado el número de intentos de conexión en el contrato ENTIDAD, PROTOCOLO, SERVICIO, CLIENTE. El contrato se ha suspendido.

## Auditorías

### Auditoría de los usuarios de Sage XRT Common Services

La configuración de la pestaña **Seguridad** queda registrada en la **Auditoría de los usuarios de Sage XRT Common Services**.

Environnement

Correspondencias

Derechos

Auditorías

Gestión de auditorías

Auditorías

Logs

Configuración

Tipo de auditoría

Usuarios

Periodo

Ninguno

Buscar

Purgar

Criterios de búsqueda aplicados

Categoría que contiene application

Usuario que contiene ADMIN

Limpiar

Fecha/Hora	Categoría	Estado	Producto	Componente	Usuario	Cuenta de usuario	Máquina	Descripción
15/03/2019 10:26:50	Application	Realizado	SXBE	SXBE Administration	ADMIN	Demo\test	EMERDW10TEST2	ADMIN solicita consultar la información de los contratos de firma de los servidores
15/03/2019 10:25:50	Application	Realizado	SXBE	SXBE Administration	ADMIN	Demo\test	EMERDW10TEST2	ADMIN solicita consultar la información de los contratos de firma de los servidores
15/03/2019 10:25:13	Application	Realizado	SXBE	SXBE Administration	ADMIN	Demo\test	EMERDW10TEST2	ADMIN solicita consultar la información de los firmantes de los servidores
14/03/2019 10:57:22	Application	Realizado	SXBE	SXBE Administration	ADMIN	Demo\test	EMERDW10TEST2	ADMIN solicita consultar el monitor de firma del servidor

### Auditoría de la integridad de los datos

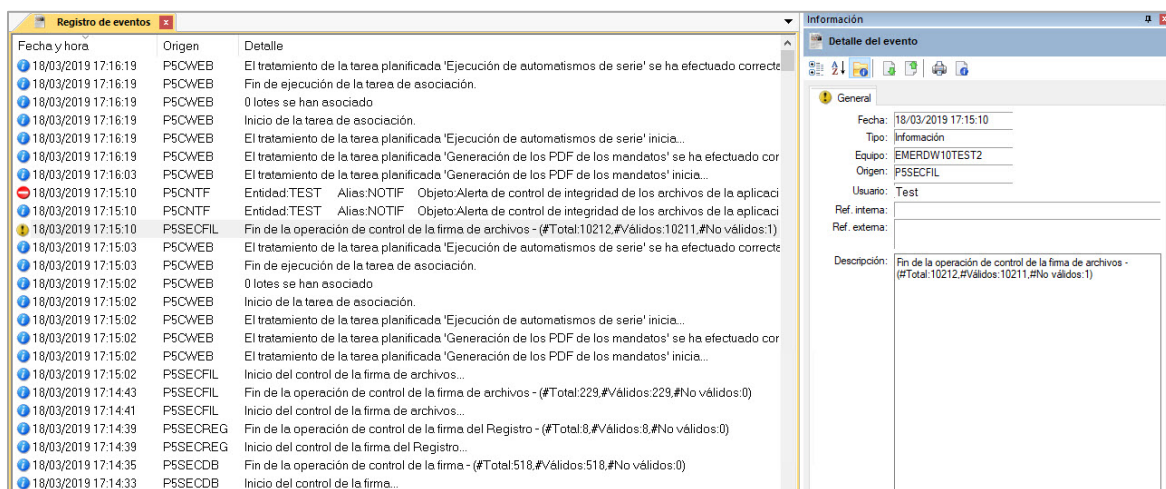
El cálculo (/COMPUTE) y la comprobación (/CHECK) de la firma de las utilidades quedan registrados en el Registro de eventos de las utilidades *P5SECDB*, *P5SECFIL* y *P5SECREG*.

**Cálculo (/COMPUTE):** número total de registros firmados.

**Comprobación (/CHECK):** número Total, número Válidos, número No Válidos.

Cuando se detecta un error, como mínimo, mediante las utilidades *P5SECFIL*, *P5SECDB* y *P5SECREG*, se crea y envía un archivo XML por correo electrónico.

Asimismo, dicho archivo XML está disponible en el LOG de la aplicación.



El agente Watch notifica en el acto las firmas incorrectas del **Registro de Windows** y del sitio **Online Banking**.

### Estructura del archivo XML

Recursos	Estructura
Cabecera	<pre>&lt;?xml version="1.0" encoding="UTF-8"?&gt;  &lt;signature datetime=" " user=" " computer="" server=""&gt;</pre>
P5SECFIL Comprobación de los binarios	<pre>&lt;binarypath&gt;      &lt;invalid&gt;          &lt;line&gt;&lt;filename&gt;apifmt.exe&lt;/filename&gt;&lt;/line&gt;          &lt;line&gt;&lt;filename&gt;audit.exe&lt;/filename&gt;&lt;/line&gt;      &lt;/invalid&gt;  &lt;/binarypath&gt;</pre>

Recursos	Estructura
<p>P5SECFILE</p> <p>Comprobación del sitio <b>Online Banking</b> y de los scripts</p>	<pre> &lt;onlinebankingpath&gt;      &lt;invalid&gt;          &lt;line&gt;&lt;filename&gt;apifmt.exe&lt;/filename&gt;&lt;/line&gt;          &lt;line&gt;&lt;filename&gt;audit.exe&lt;/filename&gt;&lt;/line&gt;      &lt;/invalid&gt;  &lt;/onlinebankingpath&gt; </pre>
<p>P5SECDB</p> <p>Comprobación de los contratos solicitantes</p>	<pre> &lt;invalid&gt;      &lt;line&gt;&lt;protocole&gt;&lt;/protocole&gt;&lt;entity&gt;&lt;/entity&gt;&lt;service&gt; &lt;/service&gt;&lt;client&gt; &lt;/client&gt;&lt;description&gt; &lt;/description&gt;&lt;/line&gt;      &lt;line&gt;&lt;protocole&gt;FTP&lt;/protocole&gt;&lt;entity&gt;SAGE&lt;/entity&gt;&lt;service&gt;AFB 160&lt;/service&gt;&lt;client&gt;SAG&lt;/client&gt;&lt;description&gt;Paielement&lt;/description&gt;&lt;/line&gt;  &lt;/invalid&gt; </pre>
<p>P5SECREG</p> <p>Comprobación del Registro de Windows</p>	<pre> &lt;SMP_P5   COM   ISAPI   NTF   PDS   RCP   WEB &gt;      &lt;invalid&gt;          &lt;line&gt;&lt;keyname&gt;[Keyname]&lt;/keyname&gt;&lt;/line&gt;          &lt;line&gt;&lt;keyname&gt;[Keyname]&lt;/keyname&gt;&lt;/line&gt;      &lt;/invalid&gt;  &lt;/SMP_P5   COM   ISAPI   NTF   PDS   RCP   WEB &gt; </pre>
Fin	</signature>

Ejemplo:

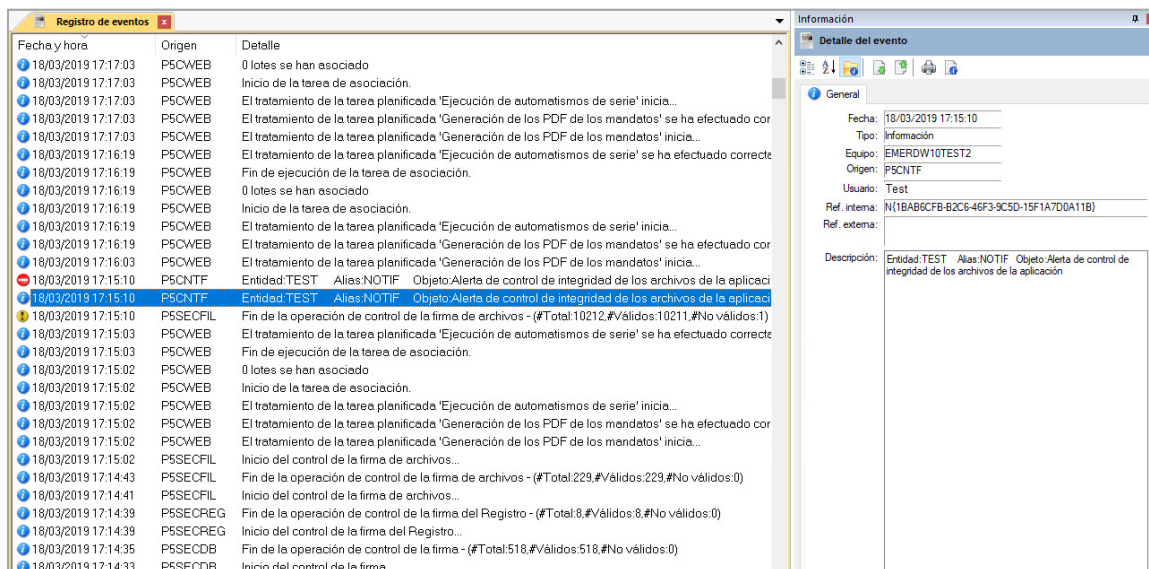
```

LOG.XML* x
<?xml version="1.0" encoding="UTF-8"?>
<signature datetime="03/04/2018 14:44:37" user="Paraph" server="" computer="">
  <invalid>
    <line>
      <protocole>EBICS</protocole>
      <entity>SG</entity>
      <service>AFB120</service>
      <client>SOCIETE</client>
      <description></description>
    </line>
    <line>
      <protocole>EBICS</protocole>
      <entity>SG</entity>
      <service>SCT</service>
      <client>SOCIETE</client>
      <description></description>
    </line>
  </invalid>
</signature>

```

### Auditoría de los errores de conexión

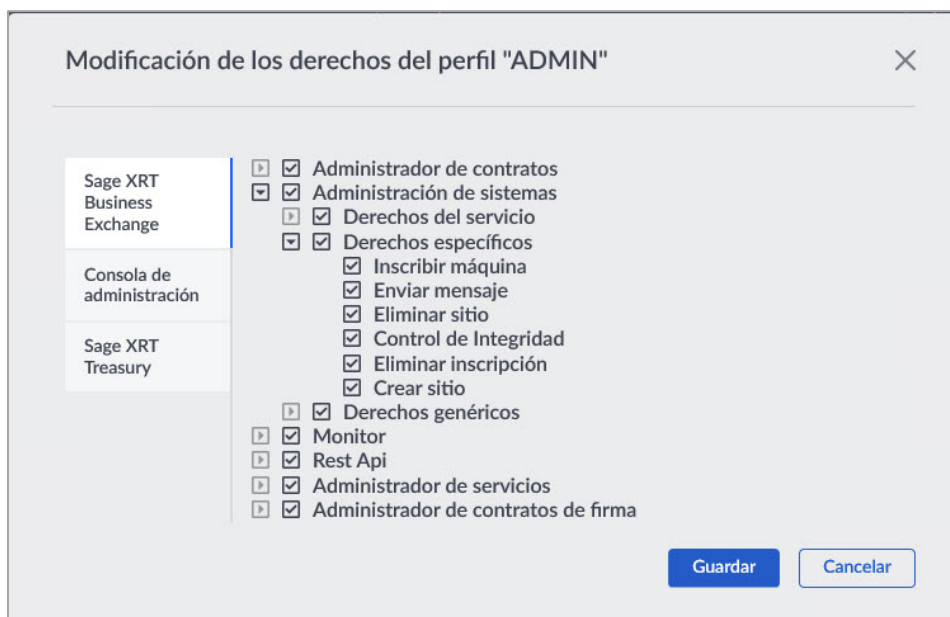
Todos los errores de conexión quedan registrados en el **Registro de eventos**.



### Derechos de Sage XRT Common Services en la pestaña Integridad

El derecho de acceso a la pestaña **Integridad** del sitio Master se puede configurar en **Sage XRT Common Services**, en los perfiles.

En la pestaña Sage XRT Business Exchange, despliegue la estructura en árbol hasta el nivel Administración de sistemas>Derechos específicos>Control de integridad.



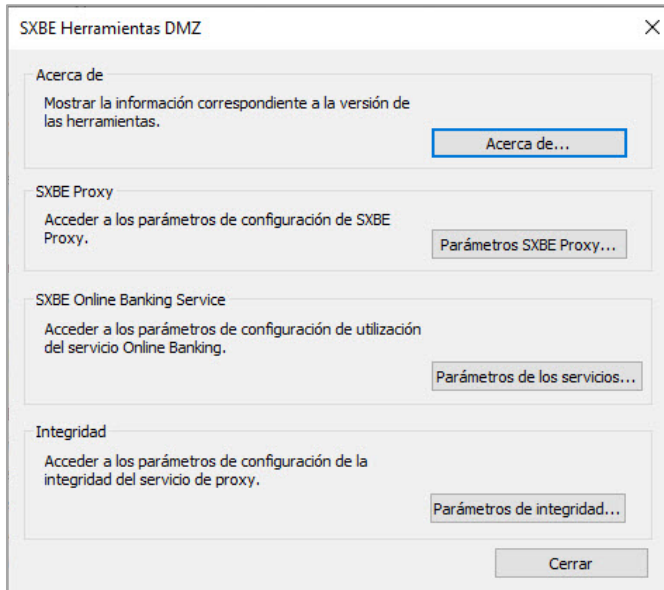


## Integridad de las herramientas DMZ

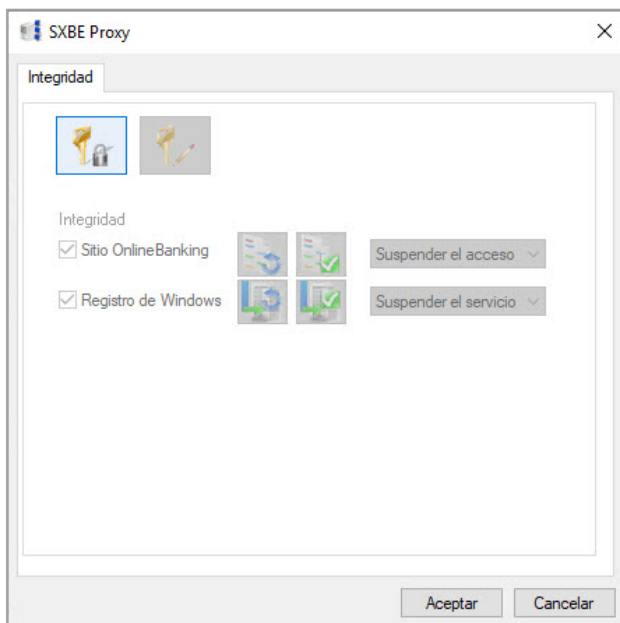
El control de la integridad permite calcular y comprobar la firma:

- del sitio Online Banking;
- del Registro de Windows.

La configuración del sitio **Online Banking** y del **Registro de Windows** para las herramientas DMZ se puede realizar en la interfaz del componente *dmztoolspanel.cpl*.



1. En el cuadro de diálogo **SXBE Herramientas DMZ**, haga clic en **Parámetros de integridad...** para abrir el cuadro de diálogo **SXBE Proxy**.



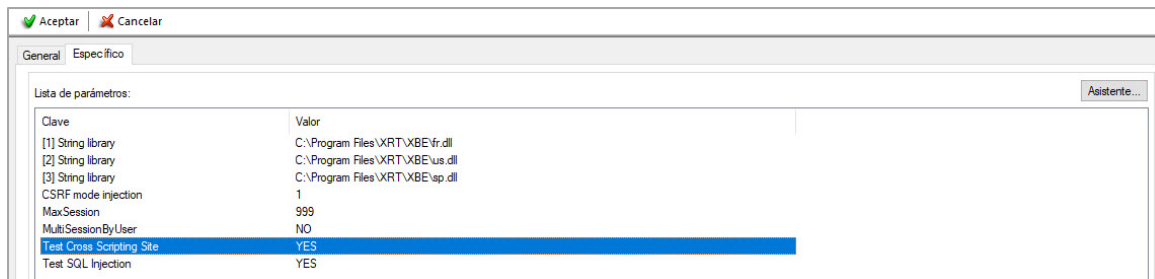
## Integridad de las herramientas DMZ

La información relativa a la integridad queda registrada en el LOG del sistema de Windows (Visor de eventos).

2. Al acceder por primera vez, defina una contraseña.
3. En el apartado **Integridad**, marque la opción **Sitio Online Banking** para ejecutar, de forma automática, el cálculo de la firma en el sitio. A continuación, seleccione una acción en la lista desplegable:
  - **Suspender el acceso:** si no se cumplen los requisitos de integridad, el sitio se suspende.
  - **Ninguna acción:** aunque los requisitos de integridad no se cumplan, los usuarios pueden continuar realizando sus operaciones. El evento queda registrado en el LOG de Windows.
4. Marque la opción **Registro de Windows** para ejecutar, de forma automática, el cálculo de la firma en el Registro de Windows. A continuación, seleccione una acción en la lista desplegable:
  - **Suspender el acceso:** si no se cumplen los requisitos de integridad del Registro de Windows, el sitio se suspende.
  - **Ninguna acción:** aunque los requisitos de integridad del Registro de Windows no se cumplan, los usuarios pueden continuar realizando sus operaciones. El evento queda registrado en el LOG de Windows.
  - **Detener el servicio:** si no se cumplen los requisitos de integridad del Registro de Windows, se detendrá el servicio Proxy. El evento queda registrado en el LOG de Windows.

# Notificaciones de detección de ataques

Existen algunas opciones para activar la detección de ataques SQL Injection, XSS y CSRF en el servicio de transacción.



Para activar la notificación de un ataque por correo electrónico, hay que indicar un contrato de notificación en la pestaña **Integridad** del sitio Master.

En el correo electrónico enviado figurará la información registrada:

- **SQL Injection y XSS:** Entidad, Usuario, Variable y contenido de los datos insertados.
- **CSRF:** Entidad, Usuario.

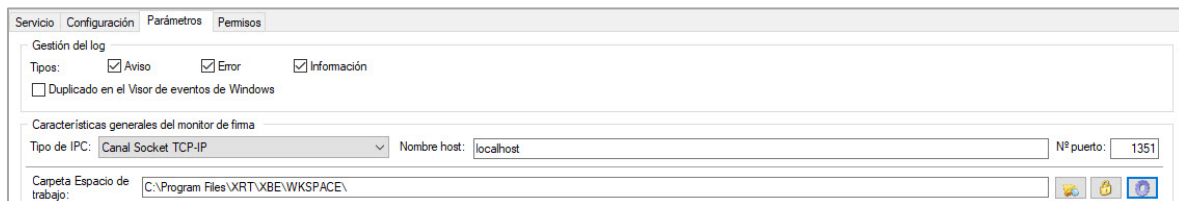
Asunto del email: Alerta de seguridad [Nombre de la máquina, tenant físico (sitio, servidor)]

Contenido: Detección de un posible ataque por **[Nombre del ataque]** mediante la variable del formulario **[Nombre del formulario]**, descripción de los datos insertados para el contrato **[Entidad, Usuario, Servicio]** (Online Banking), **[Función]** (Online Banking).

## Workspace

Los datos de la carpeta **Workspace** se sellan con el algoritmo SHA-256 y se cifran con AES 256.

Los derechos de acceso a esta carpeta se pueden configurar en el servicio de firma.



Existe la posibilidad de descifrar los datos de la carpeta Workspace con ayuda del comando PDSCRYPT.

Uso: PDSCRYPT {/D   /C   /S} [/SERVER:]	
/D	Descifrado del Workspace
/C	Cifrado del Workspace
/S	Eliminación de las secuencias ( <i>streams</i> ) del Workspace (caché de los archivos)
/SERVER	Nombre del sitio

**Importante:** Hay que definir una contraseña en la pestaña **Integridad** para descifrar o cifrar los datos de la carpeta **Workspace**.

Todas las operaciones quedan registradas en el **Registro de eventos**.



## Anexo

Ejemplo de configuración de una política de seguridad para el campo del **Descriptor de seguridad**.

Nueva contraseña

Introduzca una nueva contraseña para acceder a la configuración. Guárdela y no la pierda pues es indispensable para cualquier cambio en la configuración de la integridad.

☒ Desbloquear la entrada de la zona del descriptor de seguridad

SID=S-1-5-21-1004336348-162531612-4444556-43637 OR SID=S-1-5-21-1004336348-2531612-454566

☐ Nombre de regla de seguridad

Introduzca su contraseña:

Confirme su contraseña:

Aceptar Cancelar

Política de seguridad	Ejemplos
«LOCAL»	<p>LOCAL=logon</p> <p>LOCAL=user</p> <p>LOCAL=machine</p> <p><b>logon:</b> protects to the current logon session, user will not be able to unprotect after logoff or reboot ;</p> <p><b>user:</b> protects to the user on local machine, only this caller on the local machine will be able to unprotect;</p> <p><b>Machine:</b> protects to Local Machine, all users on the local machine will be able to unprotect;</p>
«SID»	<p>Permite acceder al objeto para el usuario 1 o el usuario 2</p> <p><b>Usuario 1</b> SID=S-1-5-21-1004336348-162531612-XXXXXXX-43637</p> <p><b>Usuario 2</b> SID=S-1-5-21-1004336348-162531612-XXXXXXX-</p> <p>Valor: SID= SID=S-1-5-21-1004336348-162531612-XXXXXXX-43637</p> <p>OR SID=S-1-5-21-1004336348-162531612-XXXXXXX-</p>

Política de seguridad	Ejemplos
«SDDL»	<p>SDDL es un lenguaje que permite proteger un recurso mediante un descriptor de seguridad de Windows.</p> <p><b>Policy: Allow Execute to Everyone if both of the following conditions are met:</b></p> <p>Title = PM</p> <p>Division = Finance or Division = Sales</p> <p>Valor: SDDL=D:(XA; ;FX;;;S-1-1-0; (@User.Title=="PM" &amp;&amp; (@User.Division=="Finance"    @User.Division == " Sales")))</p> <p><b>Policy: Allow execute if any of the user's projects intersect with the file's projects.</b></p> <p>Valor: SDDL=D:(XA; ;FX;;;S-1-1-0; (@User.Project Any_of @Resource.Project))</p> <p><b>Policy: Allow read access if the user has logged in with a smart card, is a backup operator, and is connecting from a machine with Bitlocker enabled.</b></p> <p>Valor: SDDL=D:(XA; ;FR;;;S-1-1-0; (Member_of {SID(Smartcard_SID), SID(BO)} &amp;&amp; @Device.Bitlocker))</p>
«CERTIFICATE»	<p>CERTIFICATE=HashId:4DA11316E5943B27454001515BB0C8DC1BFDC347</p> <p>CERTIFICATE=HashId:%HexValue%</p> <ul style="list-style-type: none"> <li>o %HexValue% is hex-encoded SHA1 thumbprint of the certificate</li> </ul> <p>CERTIFICATE=CertBlob:%Base64String%</p> <ul style="list-style-type: none"> <li>o %Base64String% is base64-encoded certificate blob</li> </ul>



## 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 de la Unión Europea.

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.