



# Sage XRT Business Exchange

Versión 12.1

## 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 .....       | 8        |
| Modificación de la contraseña .....                           | 9        |
| Utilidades de cálculo y de comprobación de las firmas .....   | 10       |
| Errores de conexión.....                                      | 12       |
| Elementos afectados .....                                     | 14       |
| Datos firmados .....  | 14       |
| Tablas afectadas .....  | 14       |
| Exportación/Importación de la configuración.....              | 15       |
| Notificaciones.....   | 15       |
| Descripción de las alertas.....                               | 15       |
| Auditorías .....  | 16       |
| Auditoría de los usuarios de Sage XRT Common Services.....    | 16       |

|   |           |
|---|-----------|
| Auditoría de la integridad de los datos .....                       | 17        |
| Auditoría de los errores de conexión .....                          | 19        |
| Derechos de Sage XRT Common Services en la pestaña Integridad ..... | 19        |
| <b>Integridad de las herramientas DMZ .....</b>                     | <b>20</b> |
| <b>Notificaciones de las detecciones de ataques .....</b>           | <b>22</b> |
| <b>Anexo .....</b>  | <b>23</b> |

# Descripción

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

- La integridad calcula una firma en los campos de los contratos bancarios (Integridad de la base de datos), en las claves del **Registro de Windows** (Integridad del Registro de Windows) y en los archivos de la aplicación **Online Banking** (Integridad del sitio Online Banking).
- Las anomalías en los contratos le 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 le permite definir la entidad y alias de notificación para todas las anomalías de integridad, conexión y ataques *SQL Injection*, *Cross Scripting* y *CSRF (Cross-Site Request Forgery)*.

Integridad

☐ Base de datos

☐ Sitio OnlineBanking

☐ Registro de Windows

Anomalías en los contratos

☐ Detección de errores de conexión

☐ Suspender el contrato

Contrato de notificación

Entidad:

Alias:

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

## Integridad y seguridad

### Configuración de la pestaña Integridad del sitio Master

Esta configuración permite calcular y/o comprobar la firma:

- de la **Base de datos** (de los contratos solicitantes);
- del sitio **Online Banking**;
- 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 la base del **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

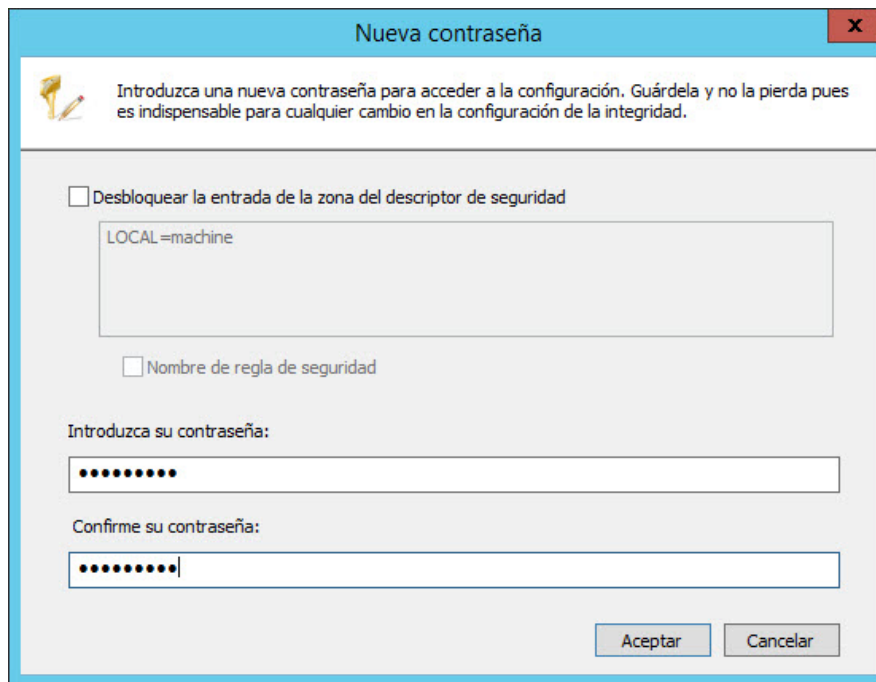
Se deben detener todos los servicios **Sage XRT Business Exchange**.

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 completamente la aplicación.

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





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

**Nota:** Para encontrar 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/es-es/library/windows/desktop/hh769091\(v=vs.85\).aspx](https://msdn.microsoft.com/es-es/library/windows/desktop/hh769091(v=vs.85).aspx)  
[https://msdn.microsoft.com/es-es/library/windows/desktop/hh870248\(v=vs.85\).aspx](https://msdn.microsoft.com/es-es/library/windows/desktop/hh870248(v=vs.85).aspx)

En la parte **Anexo** de este documento, hay disponibles algunos ejemplos de configuración.

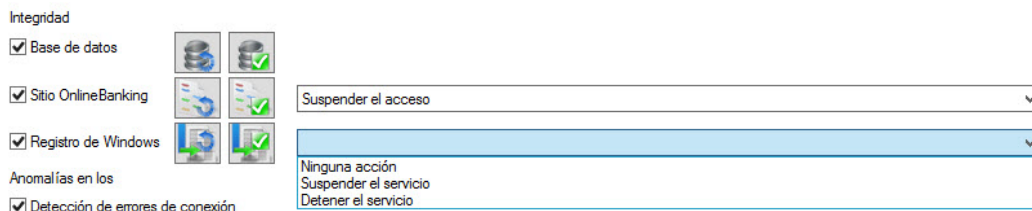
Complete los campos **Introduzca su contraseña** y **Confirme su contraseña**.

**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**
- **Registro**



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 un problema de integridad:

- **Ninguna acción**

Si se ha realizado la configuración de las notificaciones, se envía un correo electrónico al administrador para advertirle si 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 envía un correo electrónico al administrador para advertirle si uno o varios archivos están dañados.

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

- **Ninguna acción**

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

## Integridad y seguridad

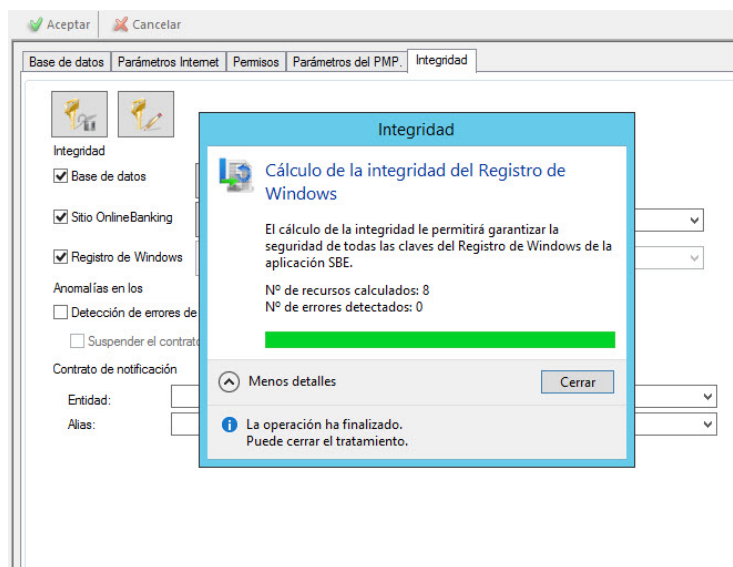
- **Detener el servicio**

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

Si se marca **Base de datos** o **Sitio OnlineBanking** o **Registro de Windows**, el cálculo de la firma se inicia de forma automática.



## Modificación de la configuración de la integridad


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

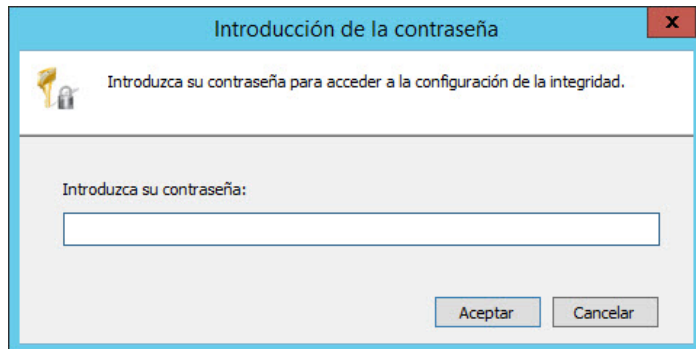
Puede realizar los siguientes cambios en la configuración del control de la integridad:

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



## Integridad y seguridad

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



Introducción de la contraseña

Introduzca su contraseña para acceder a la configuración de la integridad.

Introduzca su contraseña:

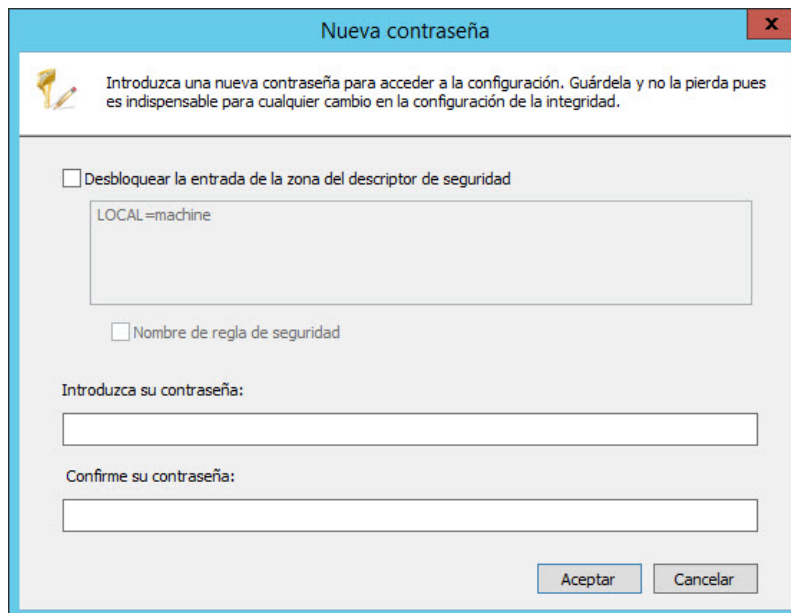
Aceptar Cancelar

**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** .



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

LOCAL=machine

☐ Nombre de regla de seguridad

Introduzca su contraseña:

Confirme su contraseña:

Aceptar Cancelar

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  |
| <i>/COMPUTE</i>   | Cálculo de la firma   |
| <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<br>(ejemplo: SRV_Test)) |

**Importante:** Aunque solo haya un único elemento en el contrato solicitante incorrecto, el contrato no se podrá utilizar.

La información se codifica en el registro de auditoría cada vez que se intenta utilizar el contrato.

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

## Integridad y seguridad

### Integridad del sitio Online Banking (P5SECFILE)

La utilidad **P5SECFILE** permite calcular y comprobar la firma de todos los archivos del sitio **Online Banking**.

Se realiza un control de integridad en todos los archivos que conforman el sitio.

| Uso: P5SECFILE {/CHECK   /COMPUTE} [/LOG:] |  |
|--|--|
| <i>/CHECK</i>                              | Comprobación de la firma de los archivos OnlineBanking         |
| <i>/CHECKBIN</i>                           | Comprobación de la firma de archivos binarios de la aplicación |
| <i>/COMPUTE</i>                            | Cálculo de la firma de los archivos OnlineBanking              |
| <i>/LOG</i>                                | Nombre del archivo de LOG                                      |

**Importante:** El control se realiza en todo el sitio **OnlineBanking** antes de que se inicie. Si se detecta alguna intrusión, puede que no se inicie el servicio. El control también puede llevarse a cabo en los archivos binarios de la aplicación (*/CHECKBIN*). La utilidad se puede planificar para la acción */CHECK*. En caso de error de integridad, los errores se reúnen 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 planificar para la acción **/CHECK**. En caso de error de integridad, los errores se reúnen 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

☒ Detección de errores de conexión

☒ Suspender el contrato

Contrato de notificación

Entidad: BANCO1 ▼

Alias: MAILTESO ▼

## Integridad y seguridad

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

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.

Si no se indica ninguna reclamación, 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<br>HASHSIGNATURE varchar (255)<br>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<br>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   |  |

## Exportación/Importación 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 del *hash* de firma.

La importación mediante **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: | <input type="text" value="BANCO1"/>   |
| Alias:   | <input type="text" value="MAILTESO"/> |

## Descripción de las alertas

### Sitio Online Banking

- Asunto del email: *Alerta de seguridad del sitio OnlineBanking [Nombre de la máquina, poseedor 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

### Datos del contrato bancario

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

### Registro

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

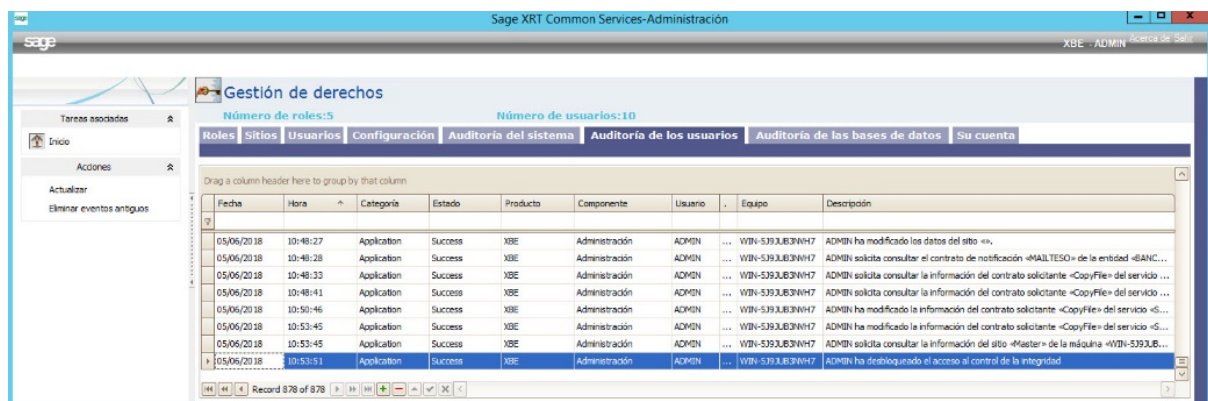
### Detección de fallos de conexión

- Asunto del email: Alerta de fallo de conexión [Nombre de la máquina, poseedor 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** se registra en la **Auditoría de los usuarios de Sage XRT Common Services**.



| Fecha      | Hora     | Categoría   | Estado  | Producto | Componente     | Usuario | Equipo         | Descripción   |
|------------|----------|-------------|---------|----------|----------------|---------|----------------|---|
| 05/06/2018 | 10:48:27 | Application | Success | XBE      | Administración | ADMIN   | WIN-5393UB3NH7 | ADMIN ha modificado los datos del sitio «».   |
| 05/06/2018 | 10:48:28 | Application | Success | XBE      | Administración | ADMIN   | WIN-5393UB3NH7 | ADMIN solicita consultar el contrato de notificación «NAILTESO» de la entidad «BANC...        |
| 05/06/2018 | 10:48:33 | Application | Success | XBE      | Administración | ADMIN   | WIN-5393UB3NH7 | ADMIN solicita consultar la información del contrato solicitante «CopyFile» del servicio «... |
| 05/06/2018 | 10:48:41 | Application | Success | XBE      | Administración | ADMIN   | WIN-5393UB3NH7 | ADMIN solicita consultar la información del contrato solicitante «CopyFile» del servicio «... |
| 05/06/2018 | 10:50:46 | Application | Success | XBE      | Administración | ADMIN   | WIN-5393UB3NH7 | ADMIN ha modificado la información del contrato solicitante «CopyFile» del servicio «S...     |
| 05/06/2018 | 10:53:45 | Application | Success | XBE      | Administración | ADMIN   | WIN-5393UB3NH7 | ADMIN ha modificado la información del contrato solicitante «CopyFile» del servicio «S...     |
| 05/06/2018 | 10:53:45 | Application | Success | XBE      | Administración | ADMIN   | WIN-5393UB3NH7 | ADMIN solicita consultar la información del sitio «Master» de la máquina «WIN-5393UB...       |
| 05/06/2018 | 10:53:51 | Application | Success | XBE      | Administración | ADMIN   | WIN-5393UB3NH7 | ADMIN ha desbloqueado el acceso al control de la integridad                                   |

## Auditoría de la integridad de los datos

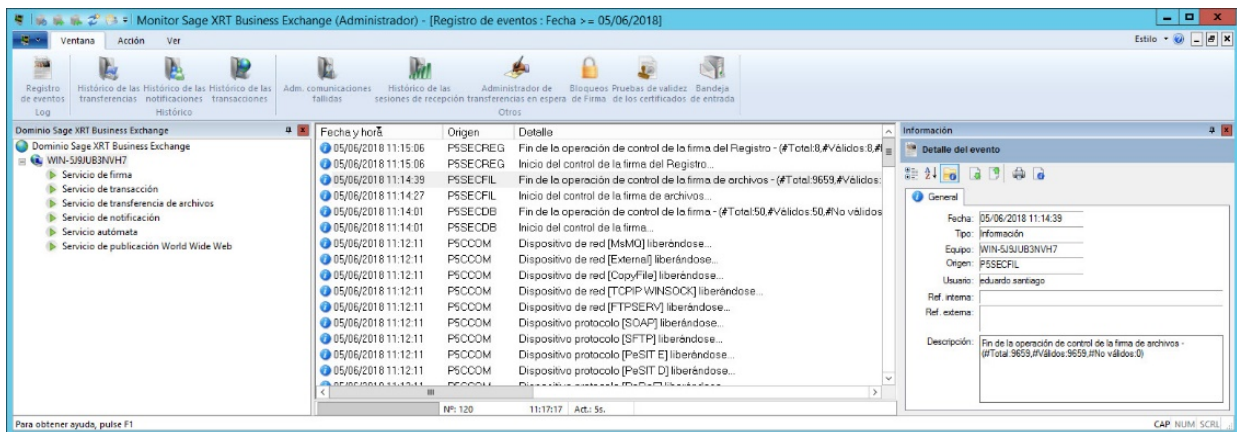
El cálculo (/COMPUTE) y la comprobación (/CHECK) de la firma de las utilidades se registran en el registro de eventos de las utilidades **P5SECDB**, **P5SECFIL** y **P5SECREG**.

**Cálculo (/COMPUTE):** Número total de registros firmados

**Comprobación (/CHECK):** Número total, número OK, número NOK

Quando se detecta como mínimo un error mediante las utilidades **P5SECFILE**, **P5SECDB** y **P5SECREG**, se crea y envía por correo electrónico un archivo XML.

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



El agente Watch notifica en tiempo real 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>  |
| P5SECFILE | <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> |
| P5SECFILE | <pre>&lt;onlinebankingpath&gt;</pre>  |

| Recursos  | Estructura   |
|---|--|
| Comprobación del sitio Online Banking                 | <pre> &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>  |
| P5SECDB<br>Comprobación de los contratos solicitantes | <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;Palement&lt;/description&gt;&lt;/line&gt;  &lt;/invalid&gt; </pre> |
| P5SECREG<br>Comprobación del Registro de Windows      | <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:

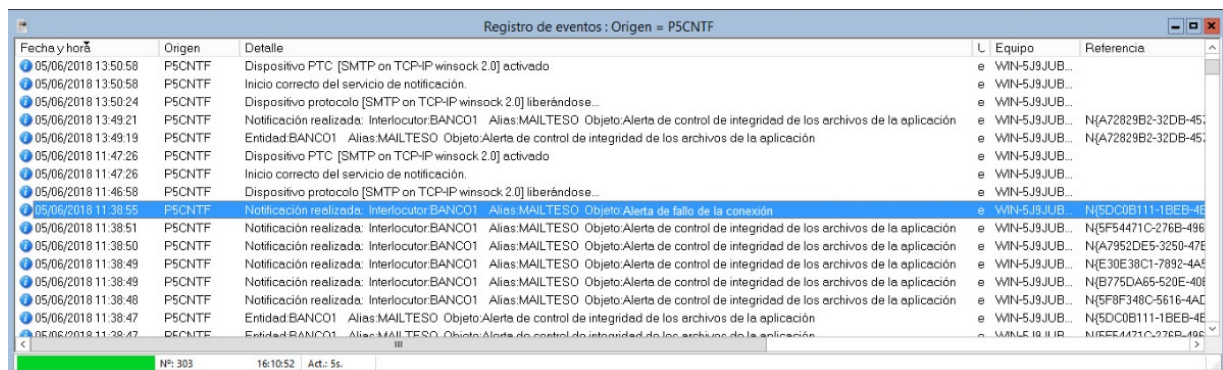
```

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 se registran en el registro de eventos.



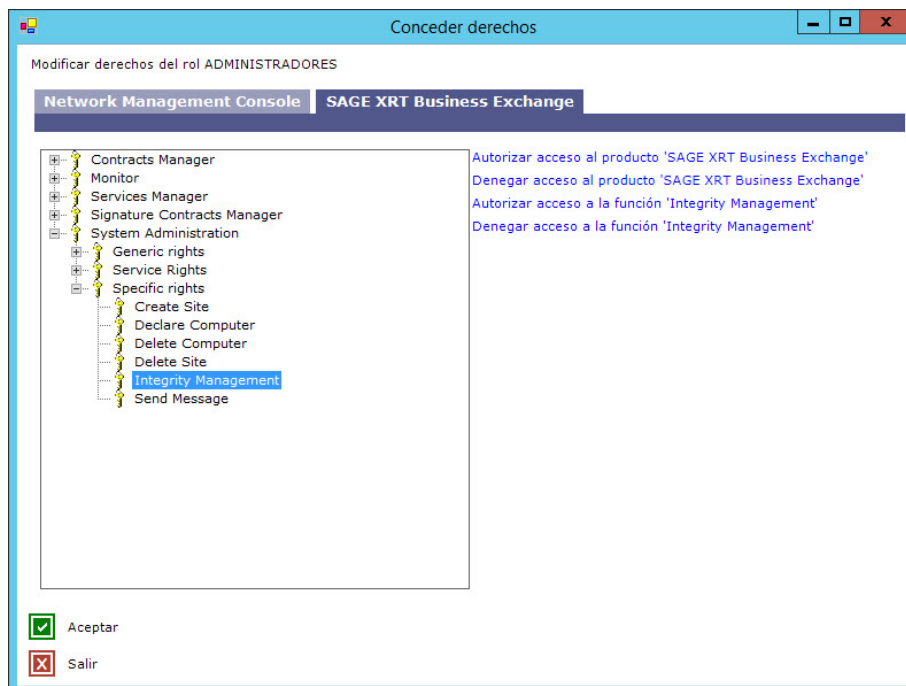
| Fecha y hora        | Origen | Detalle   | Equipo          | Referencia             |
|---------------------|--------|---|-----------------|------------------------|
| 05/06/2018 13:50:58 | P5CNTF | Dispositivo PTC [SMTP on TCP/IP winsock 2.0] activado   | e WIN-5J9JUB... |                        |
| 05/06/2018 13:50:58 | P5CNTF | Inicio correcto del servicio de notificación.   | e WIN-5J9JUB... |                        |
| 05/06/2018 13:50:24 | P5CNTF | Dispositivo protocolo [SMTP on TCP/IP winsock 2.0] liberándose...   | e WIN-5J9JUB... |                        |
| 05/06/2018 13:49:21 | P5CNTF | Notificación realizada: Interlocutor: BANCO1 Alias: MAILTESO Objeto: Alerta de control de integridad de los archivos de la aplicación | e WIN-5J9JUB... | N(A72829B2-32DB-45...  |
| 05/06/2018 13:49:19 | P5CNTF | Entidad: BANCO1 Alias: MAILTESO Objeto: Alerta de control de integridad de los archivos de la aplicación                              | e WIN-5J9JUB... | N(A72829B2-32DB-45...  |
| 05/06/2018 11:47:26 | P5CNTF | Dispositivo PTC [SMTP on TCP/IP winsock 2.0] activado   | e WIN-5J9JUB... |                        |
| 05/06/2018 11:47:26 | P5CNTF | Inicio correcto del servicio de notificación.   | e WIN-5J9JUB... |                        |
| 05/06/2018 11:46:58 | P5CNTF | Dispositivo protocolo [SMTP on TCP/IP winsock 2.0] liberándose...   | e WIN-5J9JUB... |                        |
| 05/06/2018 11:38:55 | P5CNTF | Notificación realizada: Interlocutor: BANCO1 Alias: MAILTESO Objeto: Alerta de fallo de la conexión                                   | e WIN-5J9JUB... | N(5DC0B111-1BEB-4E...  |
| 05/06/2018 11:38:51 | P5CNTF | Notificación realizada: Interlocutor: BANCO1 Alias: MAILTESO Objeto: Alerta de control de integridad de los archivos de la aplicación | e WIN-5J9JUB... | N(5F54471C-276B-496... |
| 05/06/2018 11:38:50 | P5CNTF | Notificación realizada: Interlocutor: BANCO1 Alias: MAILTESO Objeto: Alerta de control de integridad de los archivos de la aplicación | e WIN-5J9JUB... | N(A7952DE5-3250-47E... |
| 05/06/2018 11:38:49 | P5CNTF | Notificación realizada: Interlocutor: BANCO1 Alias: MAILTESO Objeto: Alerta de control de integridad de los archivos de la aplicación | e WIN-5J9JUB... | N(E30E38C1-7892-4A5... |
| 05/06/2018 11:38:49 | P5CNTF | Notificación realizada: Interlocutor: BANCO1 Alias: MAILTESO Objeto: Alerta de control de integridad de los archivos de la aplicación | e WIN-5J9JUB... | N(B775DA65-520E-408... |
| 05/06/2018 11:38:48 | P5CNTF | Notificación realizada: Interlocutor: BANCO1 Alias: MAILTESO Objeto: Alerta de control de integridad de los archivos de la aplicación | e WIN-5J9JUB... | N(5F8F348C-5616-4AC... |
| 05/06/2018 11:38:47 | P5CNTF | Entidad: BANCO1 Alias: MAILTESO Objeto: Alerta de control de integridad de los archivos de la aplicación                              | e WIN-5J9JUB... | N(5DC0B111-1BEB-4E...  |
| 05/06/2018 11:38:47 | P5CNTF | Entidad: BANCO1 Alias: MAILTESO Objeto: Alerta de control de integridad de los archivos de la aplicación                              | e WIN-5J9JUB... | N(5F54471C-276B-496... |

### 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 la pestaña **Sage XRT Business Exchange** de la ventana **Asignación de los derechos**, desarrolle la estructura en árbol hasta el nivel **Administración de sistema/Derechos específicos/Gestión de la integridad**.

A continuación, haga clic en los enlaces **Autorizar** o **Denegar** el acceso a la función **Gestión de la integridad**.



## Integridad de las herramientas DMZ

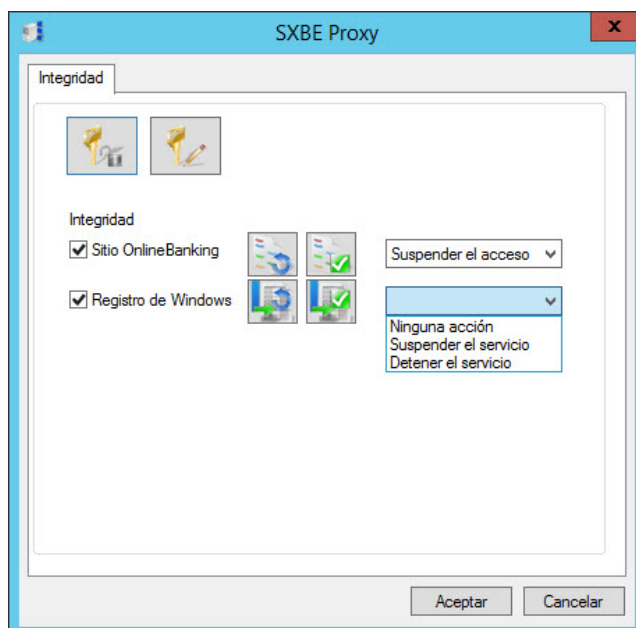
El control de la integridad permite calcular y/o comprobar la firma:

- 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 se guarda 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 OnlineBanking** 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 sitio. 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 las detecciones de ataques

Existen algunas opciones para activar la detección de ataques *SQL Injection*, por *Cross Scripting Site* y *CSRF* en el servicio de transacción.

General Especifico Asistente...

Lista de parámetros:

| Clave                        | Valor                           |
|------------------------------|---------------------------------|
| MaxSession                   | 999                             |
| MultiSessionByUser           | NO                              |
| Test Cross Scripting Site    | YES                             |
| Test SQL Injection           | YES                             |
| [1] String library           | C:\Program Files\XRT\XBE\vr.dll |
| [2] String library           | C:\Program Files\XRT\XBE\us.dll |
| [3] String library           | C:\Program Files\XRT\XBE\sp.dll |
| No Acl on static objects     | NO                              |
| Authentication Mode Standard | NO                              |
| Authentication Type          | BASE64                          |
| Allow Strong Authentication  | NO                              |
| Authentication SageID        | NO                              |
| CSRF mode injection          | 1                               |

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

Se envía un email con la información que se ha registrado:

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


Asunto del email: *Alerta de seguridad [Nombre de la máquina, poseedor 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).*

# 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 realizar cualquier cambio en la configuración de la integridad.

☒ Desbloquear la entrada de la zona del descriptor de seguridad

SID=S-1-5-21-2953480623-492028556-2955111087-1001 OR SID=S-1-5-21-2953480623-52

☐ Nombre de regla de seguridad

Introduzca su contraseña:

.....

Confirme su contraseña:

.....

Aceptar

Cancelar

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

| Política de seguridad | Ejemplos   |
|-----------------------|--|
| «SDDL"                | <p>SDDL es un lenguaje que permite proteger un recursos mediante un descriptor de seguridad 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:<br/>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:<br/>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:<br/>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> <p>o %HexValue% is hex-encoded SHA1 thumbprint of the certificate</p> <p>CERTIFICATE=CertBlob:%Base64String%</p> <p>o %Base64String% is base64-encoded certificate blob</p>  |