Sage XRT Business Exchange

Seguridad y medidas de protección

Versión 14

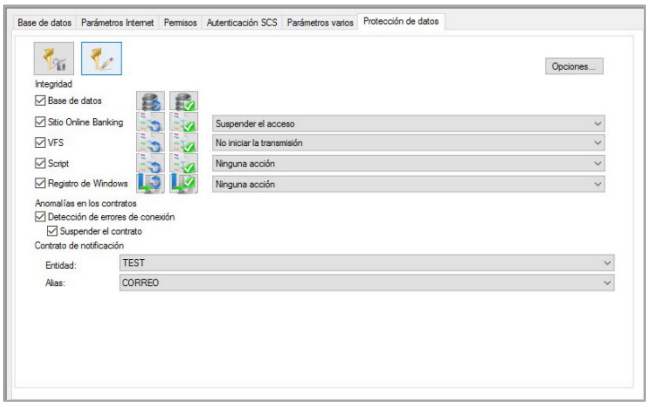
Sage

Índice

Descripción

Para aumentar la seguridad de la aplicación, desde la pestaña **Integridad** de **Administración de sistema,** se pueden configurar diferentes opciones:

- **Integridad** calcula una firma en los campos de los contratos bancarios para **Integridad Base de datos**, en las claves del Registro de Windows para **Integridad Registro de Windows**, en los archivos de la aplicación **Online Banking** para **Integridad Sitio Online Banking**, en los *scripts* para **Integridad Script** y en los archivos del VFS para **Integridad VFS**.
- **Anomalías en los contratos** permiten detectar errores de integridad debido a intrusiones.
- **Detección de errores de conexión** y **Suspender el contrato** para los contratos bancarios en modo solicitante.
- **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).



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.**

Asimismo, se han aplicado otras políticas de seguridad.

Protección de datos

Configuración de la Integridad

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 la base del **Registro de Windows.**

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

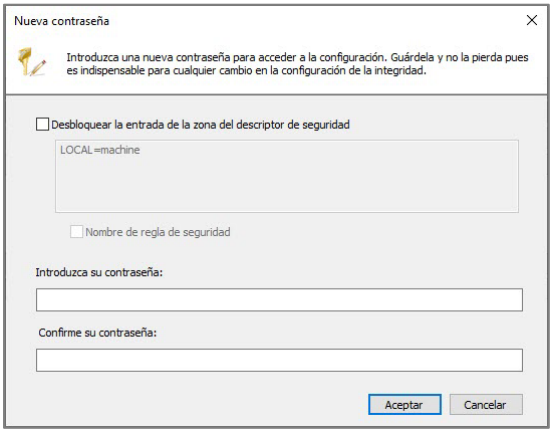
Activación por primera vez

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

Para activar las opciones de configuración, es necesario introducir una *contraseña* (*passphrase*).

Importante: Hay que guardar dicha *contraseña* de forma segura. Habrá que utilizarla cada vez que se necesite modificar la integridad. Si se pierde, se deberá reinstalar la aplicación por completo.

Hay que hacer clic en el icono de **bloqueo**  para acceder a la pantalla de creación de la *contraseña*.



Desbloquear la entrada de la zona del descriptor de seguridad: en este campo se puede proteger el acceso a la clave de la contraseña. La configuración definida de forma predeterminada es **LOCAL=machine**.

Nota: Para obtener información sobre la sintaxis de los descriptores de seguridad autorizados para este campo, se puede consultar la documentación de **Microsoft** (versión en inglés):

https://msdn.microsoft.com/en-us/library/cc230368.aspx
https://msdn.microsoft.com/fr-fr/library/windows/desktop/hh769091(v=vs.85).aspx
https://msdn.microsoft.com/fr-fr/library/windows/desktop/hh870248(v=vs.85).aspx

En el anexo de este documento, figuran algunos ejemplos de configuración.

Hay que completar los campos **Introduzca su contraseña** y **Confirme su contraseña.**

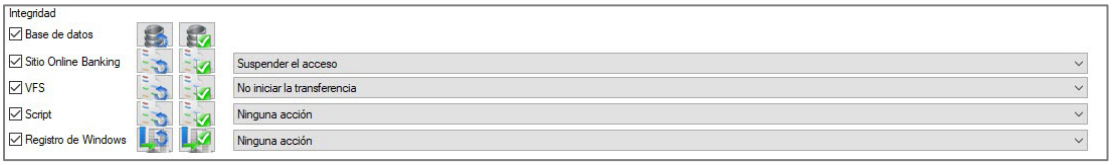
Importante: Para proteger la caja de seguridad de las contraseñas con más de **dos SID,** hay que utilizar un servicio Active Directory (AD) con un modo de compatibilidad del bosque (*forest*) igual a 2012 como mínimo.
Comando **PowerShell** para obtener la versión:
[system.directoryservices.activedirectory.Forest]::GetCurrentForest().ForestMode

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

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

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



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 se marca la opción **Sitio Online Banking,** hay que seleccionar, 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).

Si se marca la opción **Script,** hay que seleccionar, 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 scripts 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 **Sage XRT Business Exchange**.

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 se marca la opción **VFS,** hay que seleccionar, 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 transmisión**

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

Si se marca la opción **Registro de Windows,** hay que seleccionar, 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.

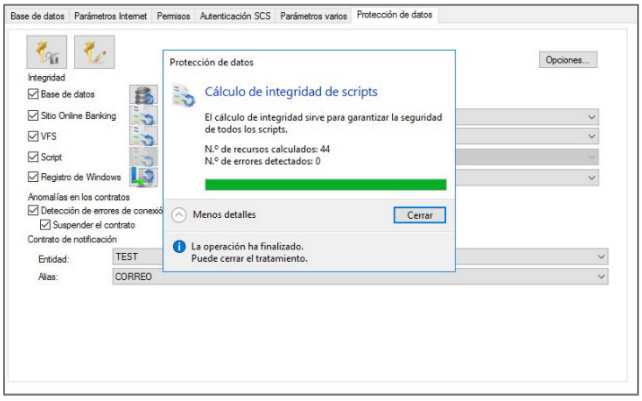
- **Detener el servicio**

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.

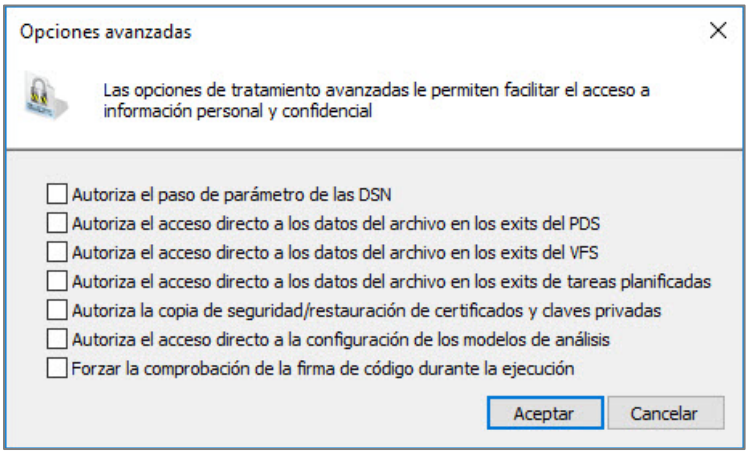
- **Suspender el acceso**

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.

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 inicia de forma automática.



Las opciones de tratamiento avanzadas sirven para autorizar el acceso a datos confidenciales y personales en determinados casos.



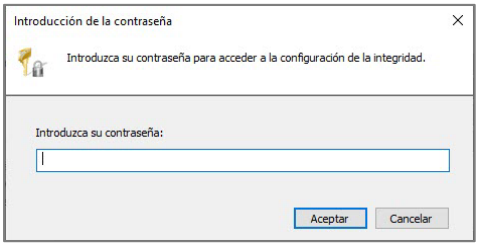
Modificación de la configuración

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

Se pueden 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, hay que hacer clic en el icono de **bloqueo**  e introducir la *contraseña* en el cuadro de diálogo que aparece en pantalla.

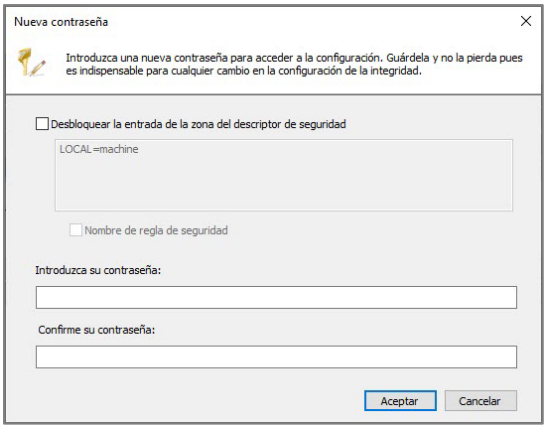


Nota: Si la opción **Integridad** está desactivada, no se realizará ningún recálculo.

Modificación de la contraseña

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

Hay que hacer en el botón **Cambiar**  .



En el cuadro de diálogo **Nueva contraseña,** hay que introducir la contraseña, confirmarla y hacer 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

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:]	
/CHECK	Comprobación de la firma de la base de datos
/COMPUTE	Cálculo de la firma de la base de datos
/LOG	Nombre del archivo de LOG
/P:	Filtro entidad
/S:	Filtro servicio
/C:	Filtro cliente
/T:	Filtro protocolo
/SERVER:	**Nombre del sitio** permite buscar los recursos asociados al sitio, por ejemplo: BDD

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

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

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

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

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

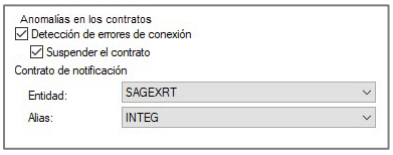
Uso: P5SECREG {/CHECK | /COMPUTE} [/LOG: /SERVER:]	
/CHECK	Comprobación de la firma del Registro de Windows
/COMPUTE	Cálculo de la firma del Registro de Windows
/COMPUTER:	Comprobación del Registro de Windows en otra máquina (Nombre de la máquina)
/LOG	Nombre del archivo de LOG
/SERVER:	Nombre del sitio

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.

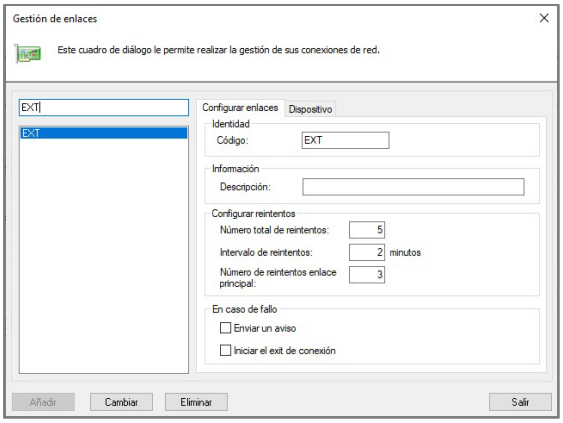
Errores de conexión

En el apartado **Anomalías en los contratos,** hay que marcar 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.

Asimismo, se podrá acceder a la opción **Suspender el contrato.**



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 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	Integración de la columna HASHSIGNATURE varchar (255) NULL
OFTPMD	Contrato Odette FTP	
SWIFTFTIMD	Contrato Swift	
EXTMD	Contrato External	
CPFMD	Contrato CopyFile	
MOMMD	Contrato MsMQ	
SMTPPOP3MD	Contrato eMail	
X400MD	Contrato X400	
AS2MD	Contrato AS2	
SOAPMD	Contrato Soap	

PADEFMD	Contrato PaDeF	
SFTPMD	Contrato SFTP	
EB3MD	Contrato EDI3	
PTDMD	Contrato PeSIT D	
PTEMD	Contrato PeSIT E	
FTPMD	Contrato FTP	
EBICSMD	Contrato EBICS	
EBICSUSERS_DEM	Parámetro de identificación EBICS	
LIEN_NTW	Enlace	
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*.

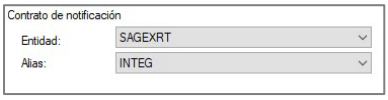
En cambio, la contraseña no se solicita durante la exportación de la configuración. El tratamiento es idéntico al de la utilidad EXPVPS.

Importante: Los datos de enlace o de parámetros de identificación no asociados a un contrato bancario no se firman (datos de pruebas, por ejemplo). Dichos 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.

Se debe introducir una **Entidad** y un **Alias.**



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.*

- **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 de los archivos incorrectos 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 de los registros incorrectos 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**

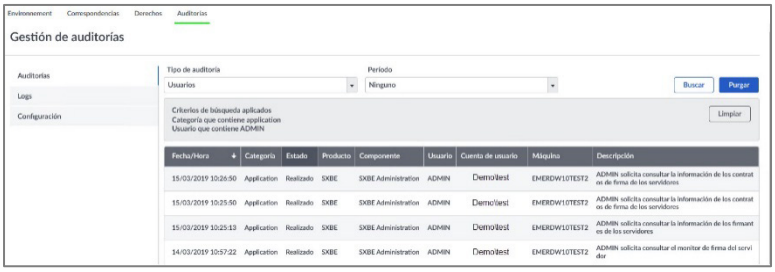
Asunto del email: *Alerta de error de conexión [Nombre de la máquina,* tenant *físico (sitio, servidor)]*

Contenido: *Se ha superado el número de intentos de conexión en el contrato ENTIDAD, PROTOCOLO, SERVICIO, CLIENTE. El contrato se ha suspendido.*

Auditoría

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.**



Auditoría de la integridad de los datos

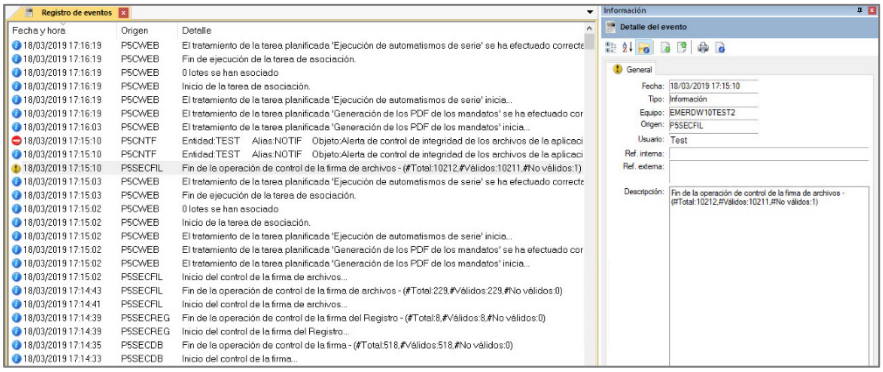
El cálculo (*/COMPUTE*) y la comprobación (*/CHECK*) de la firma de las utilidades quedan registrados en el registro de eventos de las utilidades **P5SECDB**, **P5SECFILE** y **P5SECREG**.

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 **P5SECFILE**, **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.

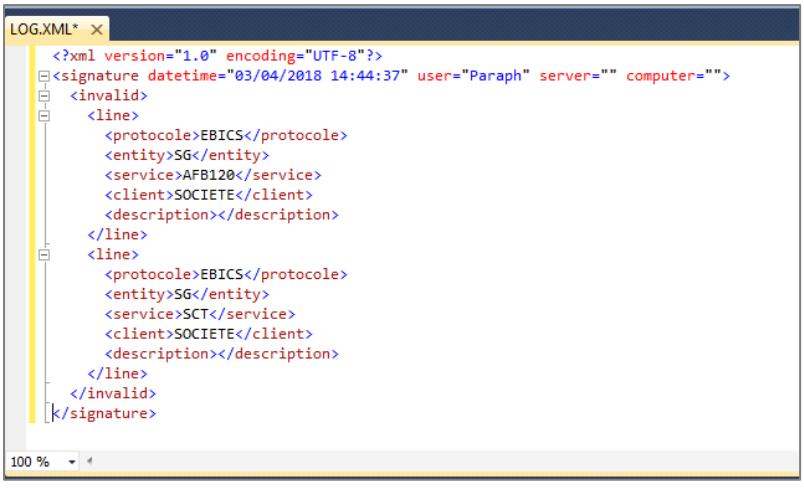


El agente Watch notifica en el acto las firmas incorrectas del **Registro de Windows** y del sitio **Online Banking.**

Estructura del archivo XML

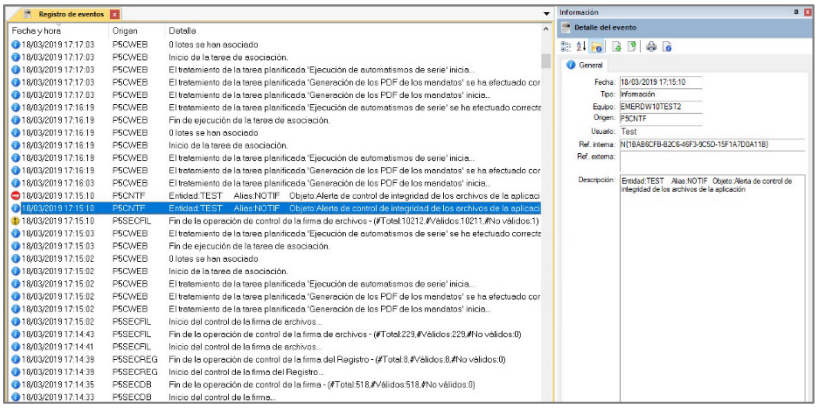
Recursos	Estructura
Cabecera	<?xml version="1.0" encoding="UTF-8"?> <signature datetime=" " user=" " computer="" server="">
P5SECFILE Comprobación de los binarios	<binarypath> <invalid> <line><filename>apifmt.exe</filename></line> <line><filename>audit.exe</filename></line> </invalid> </binarypath>
P5SECFILE Comprobación del sitio Online Banking y de los scripts	<onlinebankingpath> <invalid> <line><filename>apifmt.exe</filename></line> <line><filename>audit.exe</filename></line> </invalid> </onlinebankingpath>
P5SECDB Comprobación de los contratos solicitantes	<invalid> <line><protocole></protocole><entity></entity><service></service><client> </client><description> </description></line> <line><protocole>FTP</protocole><entity>SAGE</entity><service>AFB160</service><client>SAG</client><description>Paiement</description></line> </invalid>
P5SECREG Comprobación del Registro de Windows	<SMP_P5 | COM | ISAPI | NTF| PDS| RCP| WEB > <invalid> <line><keyname>[Keyname]</keyname></line> <line><keyname>[Keyname]</keyname></line> </invalid> </SMP_P5 | COM | ISAPI | NTF| PDS| RCP| WEB >
Fin	</signature>

Ejemplo:



Auditoría de los errores de conexión

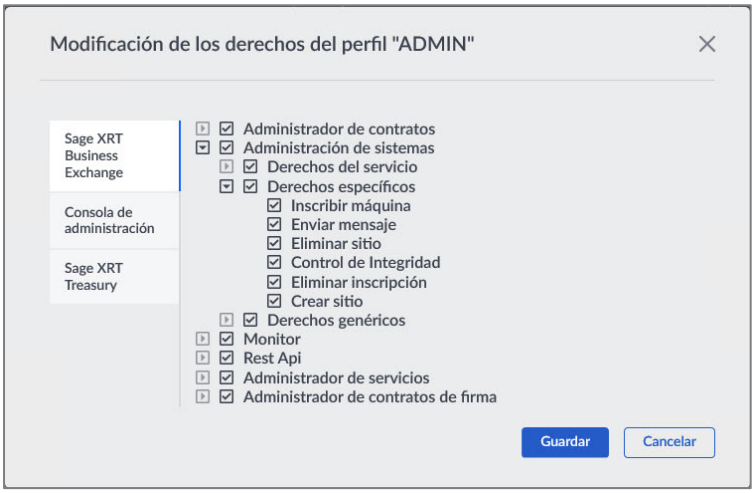
Todos los errores de conexión quedan registrados en el registro de eventos.



Derechos de acceso 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.

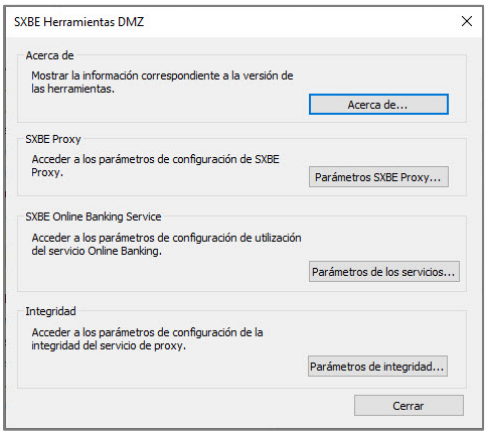
En la pestaña **Sage XRT Business Exchange,** hay que desplegar la estructura en árbol hasta el nivel **Administración de sistema>Derechos específicos>Control de integridad.**



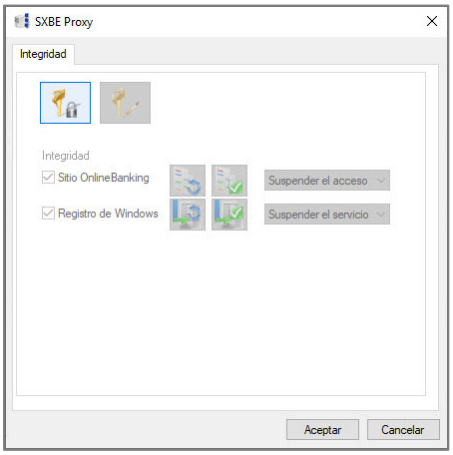
Integridad de las herramientas DMZ

El control de la integridad permite calcular y comprobar la firma del sitio **Online Banking** y 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**, hay que hacer clic en **Parámetros de integridad...** para abrir el cuadro de diálogo **SXBE Proxy**.



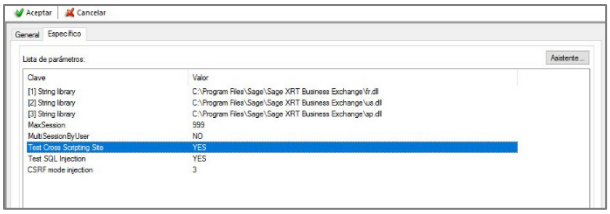
   La información relativa a la integridad queda registrada en el LOG del sistema de Windows (Visor de eventos).

2. Al acceder por primera vez, hay que definir una *contraseña*.

3. En el apartado **Integridad,** hay que marcar la opción **Sitio Online Banking** para ejecutar, de forma automática, el cálculo de la firma en el sitio. A continuación, hay que seleccionar 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. Hay que marcar la opción **Registro de Windows** para ejecutar, de forma automática, el cálculo de la firma en el Registro de Windows. A continuación, hay que seleccionar 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, Cross Scripting (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 Cross Scripting: 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)].*

Política de seguridad de las cabeceras HTTP

Online Banking

Para prevenir los posibles ataques en **Online Banking**, se ha establecido una política de seguridad en el archivo **web.config**, en la raíz del sitio.

Retirada de información de identificación del servidor IIS

<remove name="X-AspNet-Version" />

<remove name="X-Powered-By" />

<remove name="Server" />

Conservación de las anteriores políticas para asegurarla compatibilidad con anteriores navegadores

Valores	Información
<add name="X-XSS-Protection" value="1; mode=block" />	Esta cabedera protege la página contra ataques *XSS* calculados. Se ha reemplazado por la directiva *Content-Security-Policy* y ya no se utiliza en las versiones más recientes de los navegadores.
<add name="X-Frame-Options" value="SAMEORIGIN" />	Esta página protege los datos contra su inclusión en *frames* o *iframes*. Se ha reemplazado por la directiva *Content-Security-Policy* (equivalente a *frame-ancestors 'self'*) y ya no se utiliza en las versiones más recientes de los navegadores.
<add name="X-Content-Type-Options" value="nosniff" />	Esta cabecera protege contra la vulnerabilidad de tipo *Mime Sniffing*.

Integración de nuevas políticas

Valores	Información
<**add name="Strict-Transport-Security"** value="max-age=31536000; includeSubDomains; preload" />	Esta cabecera sirve para indicar al navegador que solo se puede acceder al conjunto de recursos del dominio por HTTPS y que cualquier intento de acceso por HTTP se convertirá en HTTPS. Para obtener más información sobre esta cabecera, se puede consultar la siguiente página: **https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security**
<**add name="Content-Security-Policy"** value="default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; connect-src 'self' https://127.0.0.1:48080; frame-src 'self'; font-src 'self' data:; img-src 'self' data:; object-src 'self'; frame-ancestors 'self'; base-uri 'self'; form-action 'self' https://id.sage.com" />	Esta cabedera sirve para la protección contra los ataques *XSS* (*Cross Scripting Site*) y sus variantes. Mediante las directivas de origen **-src*, permite lo siguiente: • especificar los dominios de donde pueden provenir los recursos (script, style, etc.); • prohibir o permitir, vía la directiva *frame-ancestors*, la integración de una página en otro sitio, autorizar la directiva *base-uri* y su posible localización; • controlar, vía la directiva *form-action*, dónde se pueden enviar los datos de los formularios. Según la implementación que necesite el cliente (utilización de GED, Kibana, etc.), se pueden flexibilizar las directivas predeterminadas. Se pueden añadir excepciones a las anteriores directiva, pero es importante no eliminarlas. **default-src 'none'**: por defecto, no se cargará ningún recurso. **script-src 'self' 'unsafe-eval' 'unsafe-inline'**: los scripts solo se cargarán en relación a sí mismos, autoriza la instrucción *Eval*, autoriza la ejecución de script *inline*. **style-src 'self' 'unsafe-inline':** los styles solo se cargan en relación a sí mismos, autoriza la definición de style *inline* **connect-src 'self'** https://127.0.0.1:48080 : conexión a servicios REST u otro en relación a sí mismo, autoriza la conexión a **SageIDSign** (se puede eliminar si no se utiliza el servicio de firma). **frame-src 'self'**: solo se permite la inserción de los *frames/iframes* para las páginas en relación a sí mismas.

Valores	Información
	font-src 'self' data: solo se permite la descarga de los tipos de letra en relación a sí mismos y vía una directiva *data* (necesaria para **Carbon**) **img-src 'self' data**: solo se permite la descarga de imágenes en relación a sí mismas y vía una directiva *data* (necesaria para **Carbon**) **object-src 'self'**: solo se permite la utilización de las inclusiones <*OBJECT*>/<*EMBED*>/<*APPLET*> en relación a sí mismas (necesaria para los *widgets* de **SCS**, solamente). **frame-ancestors 'self'**: indica los posibles almacenes de las páginas, solamente en sí mismas. **base-uri 'self'**: la instrucción <*BASE*> solo puede apuntar a sí misma. **form-action 'self'** https://id.sage.com**"**: los datos de los formularios solo se pueden enviar a sí mismos, autorización de redirección en el sitio de producción de **SageID** (se puede eliminar si no se utiliza **SageID**). Para obtener más información sobre esta cabecera, se puede consultar la siguiente página: **https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP**
<add name="permissions-policy" value="accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()" />	Esta cabecera sirve para controlar la utilización de los dispositivos físicos que permiten obtener varios datos. Cualquier utilización de la cámara, de la ubicación, etc., se prohíbe en **Online Banking**. Para obtener más información sobre esta cabecera, se puede consultar la siguiente página: **https://developer.mozilla.org/en-US/docs/Web/HTTP/Feature_Policy**
<add name="referrer-policy" value="strict-origin-when-cross-origin" />	Esta cabecera sirve para controlar la cantidad de información del remitente que se incluirá en la consulta. *strict-origin-when-cross-origin*: envío del origen, la ruta y los parámetros de consulta para las consultas con el mismo origen. Para obtener más información sobre esta cabecera, se puede consultar la siguiente página: **https://developer.mozilla.org/fr/docs/Web/HTTP/Headers/Referrer-Policy**

Servicio REST de producción

Para prevenir cualquier posible ataque en el servicio **REST Rapi**, se ha establecido una política de seguridad en la variable *HKEY_LOCAL_MACHINE\SOFTWARE\XRT\SMP_P5<.site>\RAPI\Spec\CustomHeaders*.

Valores	Información
"Cache-Control no-cache,no-store,must-revalidate"	Esta cabecera sirve para indicar al proxy que no ponga en caché el resultado |*Content-Security-Policy default-src 'self' 'unsafe-inline'; object-src 'none'; frame-ancestors 'none'*
"Strict-Transport-Security max-age=31536000; includeSubDomains; preload"	Esta cabecera sirve para indicar al navegador que solo se puede acceder al conjunto de recursos del dominio por HTTPS y que cualquier intento de acceso por HTTP se convertirá en HTTPS. Para obtener más información sobre esta cabecera, se puede consultar la siguiente página: **https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security**
"Content-Security-Policy default-src 'self' 'unsafe-inline'; object-src 'none'; frame-ancestors 'none'"	Esta cabedera sirve para la protección contra los ataques *XSS* (*Cross Scripting Site*) y sus variantes. **default-src 'self' 'unsafe-inline'**: los recursos relativos a sí mismos se pueden cargar, más los *inlines* (si no se permite la documentación *SWAGGER*, el valor se puede establecer en *'none'*). **object-src 'none'**: no se permite la utilización de las inclusiones *<OBJECT>/<EMBED>/<APPLET>*. **frame-ancestors 'none'**: no se permiten inclusiones en los almacenes. Para obtener más información sobre esta cabecera, se puede consultar la siguiente página: **https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP**
Política Cross-Origin Resource Sharing (CORS)	Por defecto, el servicio *REST* de **SXBE** permite: • todos los orígenes: es posible cambiar este comportamiento modificando el contenido de la variable *"HKEY_LOCAL_MACHINE\SOFTWARE\XRT\SMP\P5<.site>\RAPI\Spec\corsAllowOrigins"* • todos los encabezados (headers) • sólo los métodos *GET*, *POST*, *OPTIONS* • el soporte de credenciales (credentials)

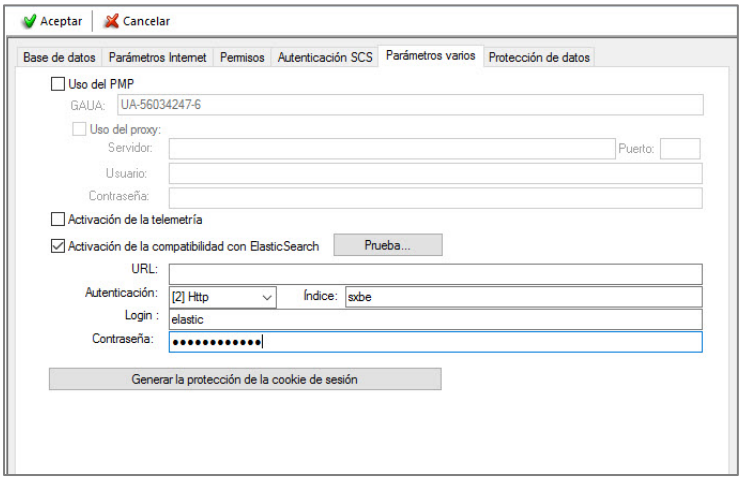
Otras políticas de seguridad

Compatibilidad de la seguridad SameSite

En **Online Banking,** la seguridad queda garantizada mediante la *cookie* de sesión gracias al atributo **SameSite.** Este atributo permite limitar los riesgos asociados a ataques de tipo *CSRF* (*Cross-Site Request Forgery*) y *XSSI* (*Cross-Site Script Inclusion*).

Protección de la cookie de sesión

Hay que activar el cifrado *AES 256* de la *cookie* de sesión haciendo clic en el botón **Generar la protección de la cookie de sesión** en la pestaña **Parámetros varios** del sitio *Master*. Para finalizar dicha activación, hay que reiniciar el servicio de transacción y el sitio IIS.



XML External Entity

Para protegerse contra ataques *XML External Entity (XXE)*, que consisten en el envío de un archivo malicioso dirigido a un intérprete de XML, la biblioteca **libxml2** se ha actualizado, y los diferentes *CVE (Common Vulnerabilities and Exposures)* registrados se han corregido.

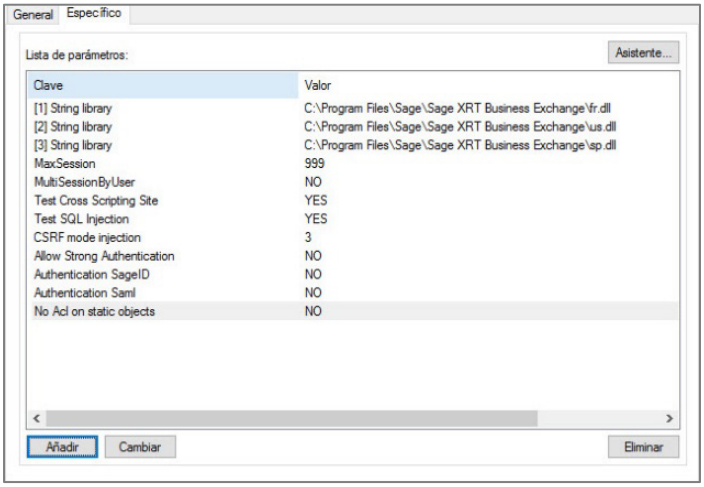
Protección contra ataques

Algunos ataques pueden llegar a comprometer la seguridad de los datos del usuario y de su dominio.

Los ataques que utilizan inyección de código SQL o *SQL injection* «inyectan» en una *consulta SQL* en curso una instrucción no prevista por el sistema, lo que puede comprometer la seguridad del sitio web.

La vulnerabilidad XSS (*Cross-Site Scripting*) es un tipo de vulnerabilidad informática, o agujero de seguridad, típico de las aplicaciones web que «inyecta» contenido en una página, lo que permite algunas acciones en los navegadores web que visitan la página.

Se pueden activar las opciones de detección de ataques en el servicio de transacción.



- El ataque CSRF (*Cross-Site Request Forgery*) consiste en transmitir a un usuario autenticado una consulta *http* falsificada que apunta a una acción interna del sitio para que la ejecute sin saberlo y utilizando sus propios derechos.
  Hay que activar la opción en los parámetros específicos del servicio.

- Los ataques *DTD* (Document Type Definition 'definición de tipo de documento') son agujeros de seguridad en los *parsers XML*.
  Dichos agujeros de seguridad ya se han utilizado para realizar ataques por denegación de servicio. También permiten obtener el contenido de un archivo al integrar una entidad externa.

- El código de la aplicación utiliza el compilador **XSL.NET** de última generación.

Periodicidad de acceso al sitio web

Se puede definir una periodicidad de acceso al sitio web para controlar la legitimidad de las conexiones.

Para ello, se puede definir un calendario de acceso a los datos.

Ejemplo: Se deniega el acceso de los usuarios al sitio web **Sage XRT Online Banking** los fines de semana.

Periodicidad de acceso de las conexiones

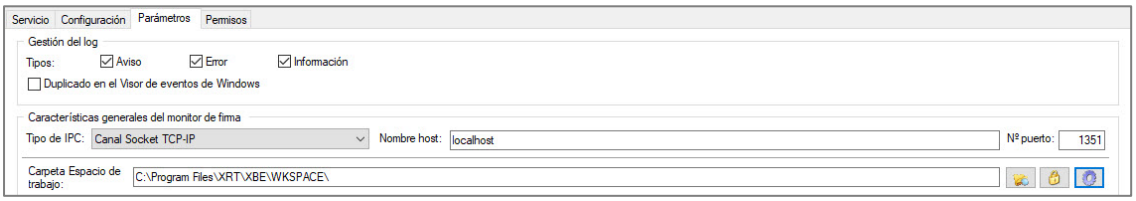
Se puede definir una periodicidad de acceso por protocolo para limitar las conexiones de los archivos.

Hay un calendario de acceso disponible para los protocolos.

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 (*streams*) del Workspace (caché de los archivos)
/SERVER	Nombre del sitio

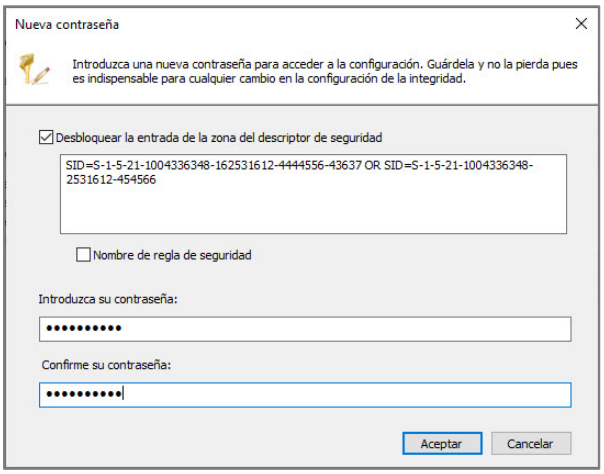
Importante: Hay que definir una contraseña en la pestaña **Integridad** para descifrar o cifrar los datos de la carpeta **Workspace.**

Todas las operaciones quedan registradas en el registro de eventos.

Date & Heure	Source	Détail	Utilisateur	Ordinateur
08/08/2018 15:43:59	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	POXXXX
08/08/2018 15:43:59	PDSCRYPT	- Accès refusé.	HATOU	POXXXX
08/08/2018 15:43:56	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	POXXXX
08/08/2018 15:21:45	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	POXXXX
08/08/2018 15:21:39	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	POXXXX
08/08/2018 15:20:29	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	POXXXX
08/08/2018 15:20:23	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	POXXXX
08/08/2018 15:19:31	PDSCRYPT	Fin de l'opération de suppression des streams du Wor...	HATOU	POXXXX
08/08/2018 15:19:31	PDSCRYPT	Début de l'opération de suppression des streams du ...	HATOU	POXXXX
08/08/2018 15:17:21	PDSCRYPT	Fin de l'opération de chiffrement du Workspace du ser...	HATOU	POXXXX
08/08/2018 15:17:21	PDSCRYPT	- Accès refusé.	HATOU	POXXXX
08/08/2018 15:17:14	PDSCRYPT	Début de l'opération de chiffrement du WorkSpace du ...	HATOU	POXXXX
08/08/2018 15:15:20	PDSCRYPT	Fin de l'opération de déchiffrement du Workspace du s...	HATOU	POXXXX
08/08/2018 15:15:07	PDSCRYPT	Début de l'opération de déchiffrement du WorkSpace ...	HATOU	POXXXX

Anexo

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



Política de seguridad	Ejemplos
«LOCAL»	*LOCAL=logon* *LOCAL=user* *LOCAL=machine* ***logon**: protects to the current logon session, user will not be able to unprotect after logoff or reboot ;* ***user** : protects to the user on local machine, only this caller on the local machine will be able to unprotect;* ***Machine** : protects to Local Machine, all users on the local machine will be able to unprotect;*
«SID»	Permite acceder al objeto para el usuario 1 o el usuario 2 **Usuario 1** SID=S-1-5-21-1004336348-162531612-XXXXXXX-43637 **Usuario 2** SID=S-1-5-21-1004336348-162531612-XXXXXXXX- Valor: SID= SID=S-1-5-21-1004336348-162531612-XXXXXXX-43637 OR SID=S-1-5-21-1004336348-162531612-XXXXXXXX-
«SDDL»	*SDDL* es un lenguaje que permite proteger un recurso mediante un descriptor de seguridad de Windows. ***Policy: Allow Execute to Everyone if both of the following conditions are met:*** *Title = PM* *Division = Finance or Division = Sales* Valor: SDDL=D:(XA; ;FX;;;S-1-1-0; (@User.Title=="PM" && (@User.Division=="Finance" || @User.Division ==" Sales")))

Política de seguridad	Ejemplos
	Policy: Allow execute if any of the user's projects intersect with the file's projects. Valor: SDDL=D:(XA; ;FX;;;S-1-1-0; (@User.Project Any_of @Resource.Project)) ***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.*** Valor: SDDL=D:(XA; ;FR;;;S-1-1-0; (Member_of {SID(Smartcard_SID), SID(BO)} && @Device.Bitlocker))
«CERTIFICATE»	CERTIFICATE=HashId:4DA11316E5943B27454001515BB0C8DC1BFDC347 CERTIFICATE=HashId:%HexValue% o %HexValue% is hex-encoded SHA1 thumbprint of the certificate CERTIFICATE=CertBlob:%Base64String% o %Base64String% is base64-encoded certificate blob

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 garantiza 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 producir por el 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.

Hay que recordar 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.