



# Sage Business Exchange

Versión 12.3

Directrices de seguridad



# Índice

<b>Medidas de seguridad .....</b>	<b>4</b>
Medidas generales .....	4
Uso de HTTPS.....	4
Contraseñas seguras.....	4
Seguridad de los servidores por derechos de acceso.....	5
Protección de los servidores .....	5
Transparent Data Encryption (TDE).....	6
Cifrado de los datos en tránsito .....	6
Cifrado de las copias de seguridad de la base de datos .....	6
Seguridad del sistema de archivos .....	6
Configuración SSL/TLS segura en un servidor Windows .....	6
Medidas de aplicaciones .....	7
Firma de la aplicación del sitio web y de los archivos.....	7
Varios modos de autenticación en la aplicación .....	7
Autorizaciones .....	8
Protección contra ataques .....	8
Prevención de ataques XML External Entity (XXE) .....	9
Compatibilidad con SameSite para crear cookies de sesión más seguras en Online Banking .....	9

## Medidas de seguridad

Cabecera HTTP Strict-Transport-Security .....	9
Periodicidad de acceso al sitio web.....	10
Para ir más allá... ..	10

## Medidas de seguridad

Para mitigar el riesgo de vulneración de datos y de las sanciones correspondientes, es necesario seguir unas pautas básicas de seguridad.

Aunque la seguridad del sistema y de la red queda bajo la responsabilidad del usuario final, la plataforma de la aplicación ofrece algunas medidas de seguridad, como las que siguen:

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

## Medidas generales

### Uso de HTTPS

**Sage XRT Business Exchange** es una aplicación web a la que se puede acceder vía una conexión HTTP o HTTPS. Aunque sea posible la conexión vía HTTP, le recomendamos que utilice siempre HTTPS para las instancias de producción, sobre todo si accede a la aplicación desde una red pública.

### Contraseñas seguras

Si utiliza el modo de autenticación fuerte, acuérdesse de establecer una política de gestión de las contraseñas, de forma que los usuarios definan una contraseña segura.

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

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

## Seguridad de los servidores por derechos de acceso

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

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

Hay que concederles los permisos necesarios en las carpetas correspondientes para que puedan administrar la aplicación.

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

## Protección de los servidores

Los servidores de la aplicación tienen que estar diseñados según los estándares del sector.

### Uso de cortafuegos locales

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

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

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

## Seguridad de la arquitectura web

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

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

- Qué servidores y puertos deberían verse desde el exterior.
- Cómo se interceptan y traducen las consultas externas para dirigirlas a los servidores y puertos correspondientes, en su caso.

Ello implica disponer de lo siguiente:

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

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

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



## Transparent Data Encryption (TDE)

Para garantizar al máximo la seguridad de su base de datos, puede aplicar el cifrado TDE (Transparent Data Encryption 'cifrado de datos transparente').

El cifrado TDE le permite cifrar su base de datos.

**Sage XRT Business Exchange 12.1** se ha validado con los siguientes entornos:

- SQL Server 2016 TDE
- Oracle 12c TDE

## Cifrado de los datos en tránsito

La comunicación entre su capa de aplicación y su base de datos puede realizarse a través del protocolo TLS (Transport Layer Security 'seguridad de la capa de transporte').

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

## Cifrado de las copias de seguridad de la base de datos

Se recomienda cifrar las copias de seguridad de la base de datos para proteger los datos.

El cifrado TDE protege *de facto* las copias de seguridad, pues es imposible restaurar o adjuntar archivos sin el certificado.

**Importante:** Es fundamental guardar el certificado en un lugar seguro y no en el mismo lugar que las copias de seguridad de las bases y la del certificado. Para *Oracle*, puede utilizar el cifrado de la red nativa.

## Seguridad del sistema de archivos

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

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

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

## Configuración SSL/TLS segura en un servidor Windows

Puede configurar el servidor IIS para restringir el uso de protocolos en los que no se garantiza la seguridad.

Consulte la siguiente documentación referente a entornos Windows de Microsoft (en inglés):

<https://medium.com/@rootsecdev/configuring-secure-cipher-suites-in-windows-server-2019-iis-7d1ff1ffe5ea>

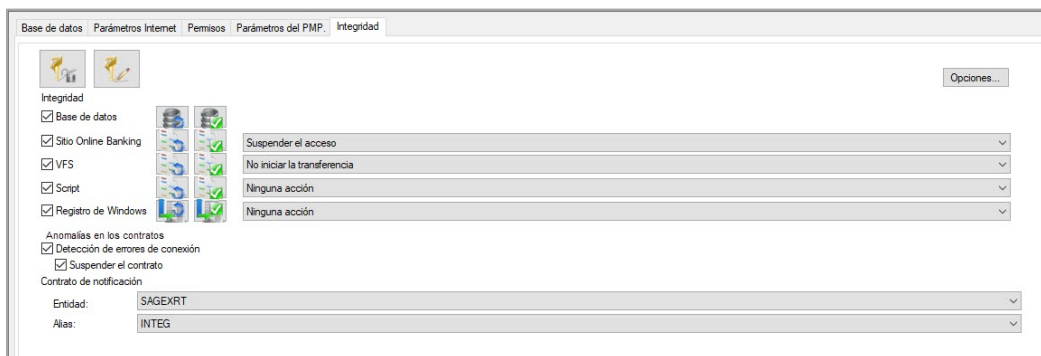
## Medidas de aplicaciones

### Firma de la aplicación del sitio web y de los archivos

El código de su aplicación está firmado. Dicha firma certifica que la aplicación es legítima y en conformidad con el desarrollo inicial, además de quedar garantizada la integridad de los archivos binarios.

Para garantizar la integridad del sitio web **Online Banking**, de los scripts y de los archivos del VFS, puede calcular una firma.

Un administrador habilitado se encargará de gestionar el cálculo y el control de la firma en el sitio Master de **Sage XRT Business Exchange**.



**Importante:** Para activar la integridad del sitio web puede definir una contraseña (*passphrase*). Esta debe guardarse en un lugar seguro.

### Varios modos de autenticación en la aplicación

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

## Autorizaciones

Un usuario tiene acceso a una o varias entidades. Este se asocia a un perfil que determina sus derechos de acceso a las funciones de la aplicación y sus privilegios: consulta de las listas, entrada de información, entidad validadora, entidad autorizadora, entidad de administración y firmante.

Los privilegios quedan determinados por los paquetes de importación.

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

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

**Importante:** Asegúrese de mantener dichas reglas. Simplifíquelas al máximo, sin que por ello se vea comprometida su política de seguridad.

## Protección contra ataques

Algunos ataques pueden llegar a comprometer la seguridad de sus datos 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.

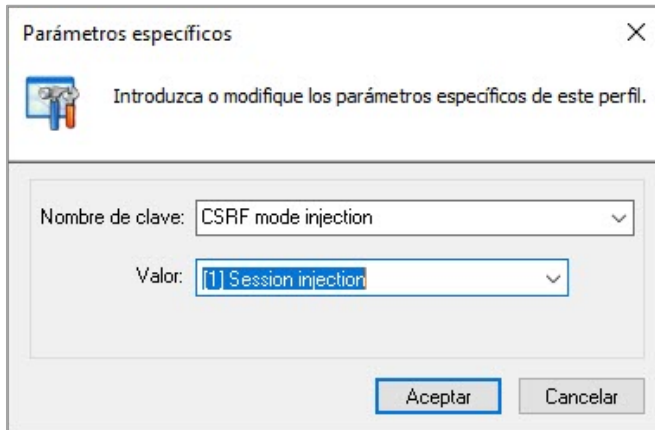
Puede activar las opciones de detección de ataques en el servicio de transacción.

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.



## Medidas de seguridad

Active 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.

### Prevención de ataques XML External Entity (XXE)

Los ataques XXE consisten en el envío de un archivo malicioso a un intérprete de XML.

Compatibilidad para la prevención de ataques XXE.

### Compatibilidad con SameSite para crear cookies de sesión más seguras en Online Banking

El atributo SameSite permite mitigar los riesgos asociados a los ataques de tipo CSRF (Cross-Site Request Forgery) y XSS (Cross-Site Script Inclusion).

Compatibilidad con el atributo SameSite.

### Cabecera HTTP Strict-Transport-Security

**HSTS** (HTTP Strict Transport Security 'HTTP con seguridad de transporte estricta') es un mecanismo de seguridad por el que un sitio web declara que los navegadores solo pueden comunicar con él mediante conexiones HTTP seguras, es decir, con el protocolo HTTPS, en lugar de HTTP.

La cabecera de las consultas del servidor es compatible con el protocolo HSTS.

## Periodicidad de acceso al sitio web

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 **Online Banking** los fines de semana.

## Para ir más allá...

Para aplicar estas medidas de seguridad adicionales se requieren ciertos conocimientos técnicos, así como el asesoramiento que nuestros equipos de consultoría pueden ofrecerle.

Nos comprometemos a ponernos en contacto con usted si desea aplicar dichas medidas.