

# Homologación Sistemas de Back office fyo

Versión: 1.1

Fecha: 09/01/2015

## Contenido

1.	Introducción.....	4
2.	Control de versiones.....	4
3.	Ventajas.....	4
4.	Versión del documento, vigencia y control de cambios.....	6
5.	Alcance.....	6
5.1	Requerimientos funcionales de negocio.....	6
5.2	Proceso de desarrollo.....	6
5.3	Seguridad.....	6
5.4	Documentación.....	7
5.5	Soporte funcional.....	7
6.	Procedimiento de Homologación.....	7
7.	Tipos de verificación.....	8
7.1	Homologación inicial.....	8
7.2	Revalidación cada dos años.....	8
7.3	Nuevas versiones.....	8
7.4	Períodos de Validez.....	8
8.	Roles y Responsabilidades.....	8
8.1	ISV/Participantes.....	8
8.2	Argentina Clearing.....	8
8.3	Auditor Asignado.....	9
9.	Anexo I: Requerimientos de validación.....	10
9.1	Requisitos funcionales del negocio.....	10
9.1.1	Generales.....	10
9.1.2	Producto.....	10
9.1.3	Operaciones.....	11
9.1.4	Contabilidad.....	12
9.1.5	Segregación de Fondos.....	12
9.1.6	Personas.....	13
9.1.7	Rendición de cuentas.....	14
9.2	Proceso de desarrollo.....	14
9.2.1	Funciones.....	14
9.2.2	Documentación.....	14
9.2.3	Versiones.....	14

9.2.4.	Respaldo .....	14
9.3	Seguridad .....	15
9.3.1.	Autenticación y Autorización.....	15
9.3.2.	Autorización.....	15
9.3.3.	Protección de la información .....	15
9.3.4.	Auditoría.....	17
9.3.5.	Tests de seguridad .....	17
9.3.6.	Resguardo de datos.....	17
9.4	Documentación.....	18
9.4.1.	Información para clientes .....	18
9.5	Soporte funcional .....	18
9.5.1.	Recursos de Soporte.....	18
9.5.2.	Información de contacto para soporte.....	18
10.	Anexo II: Versionado comodín.....	19
11.	Anexo III: Requisitos optativos.....	21

# Homologación sistemas de *backoffice*

## 1. Introducción

El procedimiento de homologación de sistemas de *backoffice* tiene como objetivo supervisar la calidad de los servicios prestados por los Participantes del Mercado; alineándolos con las mejores prácticas a criterio de ROFEX/Argentina Clearing y de esa forma, reforzar y fortalecer la calidad del sistema.

La iniciativa atiende a las exigencias de un mercado con gran potencial de crecimiento cuyos clientes son cada vez más selectivos. En los últimos tiempos se ha sumado una cantidad considerable de Participantes y clientes finales, los cuales necesitan ser nivelados para cumplir un estándar aceptable en la operatoria diaria.

Con el fin de establecer una línea de base, se definieron categorías de requisitos obligatorios que deben cumplir los sistemas utilizados por los Participantes, ya sean de desarrollo interno (In-House Development) o sistemas estandarizados desarrollados por empresas de software que realicen desarrollos empaquetados para terceros (Independent Software Vendors o ISV).

La aplicabilidad de la homologación alcanza únicamente a los módulos de futuros y opciones (FyO).

## 2. Control de versiones

Fecha	Versión	Comentarios
09/01/2015	1.1	<ul style="list-style-type: none"><li>Se agregó el punto 2. "Control de versiones".</li><li>Se hicieron agregados al punto 7.3 "Nuevas versiones".</li><li>Se agregó el punto 10. Anexo II "Versionado Comodín".</li><li>Se agregó el punto 11. Anexo III "Requisitos optativos".</li></ul>

## 3. Ventajas

Entendemos que la optimización del negocio que se persigue, traerá aparejados beneficios tanto para los Participantes como para ROFEX/Argentina Clearing, reflejados en mejoras operativas, ahorros de recursos significativos y por lo tanto aumento de la operatoria.

A continuación enumeramos las ventajas más importantes:

**Automatización de procesos:** Cuando un sistema de *backoffice* importa datos directamente desde Argentina Clearing a través de la interfaz de servicios web, **AnywherePortfolio Business Services** (APBS), suceden dos cosas positivas si la comparamos con una carga manual. La primera es la celeridad en la obtención de la información y la segunda, la mitigación de la posibilidad de errores potenciales asociados a cargas manuales.

**Segregación de garantías:** Argentina Clearing lleva un control global de las garantías depositadas por los Participantes, y estos últimos tienen la obligación de llevar un control segregado por cliente en sus propios sistemas. Un buen módulo de manejo de garantías asegurará al cliente final conocer exactamente el estado y destino de sus activos.

**Controles cruzados:** Los sistemas deben realizar por sí mismos ciertos cálculos, como por ejemplo el de diferencias y resultados, para luego comparar con los datos generados por la Cámara Compensadora. Cualquier discrepancia puede ser revisada en el momento y así evitar cobros o pagos indebidos que pueden ser difíciles de rastrear.

**Rendición a clientes:** Los clientes finales tienen el derecho a requerir información a los Participantes con los cuales operan. Si los sistemas ofrecen la posibilidad de mostrar o enviar dicha información de manera automática, se obtendrá una optimización y ahorro de recursos importante, que beneficiará también al Participante.

**Requisitos operativos:** Argentina Clearing establece requisitos mínimos relacionados con los Procedimientos Operativos que el Participante debe cumplir, un sistema homologado prevé la posibilidad de poder cumplirlos fácilmente.

**Armonización contable:** Un sistema homologado, mediante el uso de asientos modelos, permite la rápida comparabilidad de la información entre Argentina Clearing y el Participante.

**Prevención de incumplimientos:** Un sistema homologado brinda herramientas para administrar correctamente las carteras y garantías de los clientes y de esta forma prevenir incumplimientos.

**Análisis de procesos:** Las homologaciones conllevan a un repaso de los procesos realizados o a realizar por los sistemas. Generalmente, esto genera conocimientos nuevos o se detallan diferentes formas para realizar un mismo cálculo, encontrando de esta manera la mejor forma de hacerlo.

**Buenas prácticas:** Existen buenas prácticas que se incorporan en los requisitos de homologación. Muchas de ellas suelen ser no funcionales, pero tan importantes como las que lo son debido a que pueden detener el servicio o la operatividad por parte del Participante. Un repaso sobre estos puntos resulta saludable para evaluar riesgos relacionados con los sistemas.

**Retroalimentación:** ROFEX/Argentina Clearing se nutren también de los comentarios y planteos realizados por los Participantes/ISV, que pueden derivar en cambios en los sistemas de información para mostrar información que necesiten los sistemas de backoffice y que hoy no estén contemplados.

**Optimización de auditorías:** Cuando los Participantes son auditados, generalmente hay una dedicación importante de personas claves en el negocio, las cuales deben dejar de realizar tareas operativas para atender a los auditores. Un sistema homologado permite generar los reportes que necesitan los auditores en forma instantánea.

**Visibilidad:** Aquellos sistemas empaquetados que se encuentren homologados tendrán visibilidad en el sitio web institucional de Argentina Clearing, lo que simplificará el contacto por parte de nuevos Participantes que necesiten sistemas de backoffice y los posicionarán mejor que los sistemas no homologados.

**Cumplimiento Normativo:** Aquellos Participantes que cuenten con un sistema homologado podrán satisfacer el requerimiento de Auditoría Anual de Sistemas previsto en las Normas 2013 de la Comisión Nacional de Valores (CNV) mediante la simple presentación de una copia del Informe de Homologación del sistema de back office.

#### 4. Versión del documento, vigencia y control de cambios

ROFEX/Argentina Clearing se reservan el derecho de cambiar los requisitos en base a nuevos requerimientos de negocio, previa conformidad de la Comisión Nacional de Valores, sin afectar la vigencia de las homologaciones ya realizadas.

#### 5. Alcance

A continuación se detallan las categorías de requisitos que se van a revisar para la homologación.

En las Tablas Anexas “Requerimientos de Validación”, se desarrolla cada categoría en forma detallada.

##### 5.1 Requerimientos funcionales de negocio

Para favorecer el back office de la negociación de un mercado fyo, se establecieron las siguientes categorías:

- Generales
- Productos
- Operaciones
- Contabilidad
- Segregación de Fondos
- Personas
- Rendición de cuentas

##### 5.2 Proceso de desarrollo

La empresa debe contar con un procedimiento de desarrollo alineado con las buenas prácticas de la industria, que incluya al menos los siguientes puntos:

- Roles dentro del equipo de desarrollo.
- Documentación interna del sistema.
- Criterio de versionado de productos.
- Resguardo del código fuente.

##### 5.3 Seguridad

Con la finalidad de proteger la información utilizada por la aplicación y de mitigar inconvenientes relacionados con la divulgación o modificación indebida de la misma, se incluyen en esta categoría los siguientes ítems:

- Características de administración y autenticación de usuarios.
- Protección criptográfica de la información.
- Registros de auditoría.
- Verificación de vulnerabilidades.
- Facilidades de backup y Restore.

#### 5.4 Documentación

La aplicación deberá contar con una documentación mínima razonable hacia el usuario:

- Guía de instalación.
- Manual del Usuario.
- Notas de Versión.

#### 5.5 Soporte funcional

La empresa desarrolladora deberá contar con un servicio de soporte representado en uno o más consultores funcionales que conozcan los detalles de la aplicación y supervisen los requerimientos de los usuarios.

### 6. Procedimiento de Homologación

Tanto en el caso de Participantes que posean un sistema de *backoffice* desarrollado en forma interna, como en el caso de la homologación de sistemas para los fabricantes independientes de software (ISV), se realizará un proceso que constará de reuniones con equipos interdisciplinarios tanto del Participante o ISV como de ROFEX/Argentina Clearing, con el fin de validar que se cumplan los requisitos mínimos.

El entregable de la homologación será un **Informe de Homologación de sistema de backoffice** que contendrá el detalle, requisito por requisito, del estatus de cada uno (cumplido/no cumplido) más comentarios del auditor sobre lo que relevó.

Resulta conveniente aclarar que:

- Para los ISV la homologación aplica a una versión puntual de un sistema designado, y no al proveedor en sí mismo.
- El Procedimiento de homologación no implica soporte técnico y/o de negocios, salvo pruebas puntuales para Demos.

Para la homologación, los Participantes/ISV deberán preparar una Demo que cumpla con todos los requerimientos exigidos. Sólo serán homologados aquellos sistemas que satisfagan cada uno de los requisitos exigidos.

Los Sistemas de los ISV homologados se publicarán en el sitio web de Argentina Clearing.

## 7. Tipos de verificación

### 7.1 Homologación inicial

Los Participantes/ISV que se sometan al procedimiento de homologación de sus sistemas de back office contarán con una homologación inicial (HI).

La HI posee costo. Dicho valor deberá consultarse a ROFEX/Argentina Clearing S.A. y dar aceptación del mismo, antes de iniciar el proceso.

### 7.2 Revalidación cada dos años

Cada dos años los Participantes/ISV deberán someter sus sistemas a un proceso de revalidación periódico obligatorio (RPO), para certificar que cumplen con todos los requisitos, los cuales podrían surgir o variar tanto por la incorporación de nuevos estándares establecidos por CNV, ROFEX, Argentina Clearing, u otra institución pertinente.

La RPO posee costo. Dicho valor deberá consultarse a ROFEX/Argentina Clearing S.A. y dar aceptación del mismo, antes de iniciar el proceso.

### 7.3 Nuevas versiones

Los updates (cambios de funcionalidades) o upgrades (cambios de versiones del sistema), en caso de existir, también podrán contar con revalidación funcional (RF).

Es responsabilidad del Participante/ISV solicitar a ROFEX/Argentina Clearing las RF ante posibles liberaciones de actualizaciones o nuevas versiones del producto.

El Participante que solicite RF posee, para ejecutar el proceso, hasta 10 horas anuales sin costo (incluidas en las HI y RPO que posea).

De exceder las 10 horas anuales mencionadas, el ISV/Participante debe aceptar el costo por valor hora adicional antes de continuar el proceso.

En el caso de que el ISV/Participante adopte el criterio opcional de versionado comodín según lo especificado en el requerimiento "Versiones" de la Categoría "Proceso de Desarrollo", la RPO no será obligatoria. Para ello deberán informar a ROFEX/Argentina Clearing S.A. cada vez que saque una nueva versión con cambios menores, adjuntando el documento de "Notas de Versión" con el detalle de dichos cambios a fin de que se aprueben dichos cambios como menores y proceda a listar la nueva versión como homologada.

Ver Anexo II: Versionado Comodín.

### 7.4 Períodos de Validez

La validez de la HI será por 24 meses.

Cumplido el plazo, deberá efectuarse una RPO, y sucesivas RPOs cada 24 meses, independientemente de que hayan existido previamente una o más RF.

## 8. Roles y Responsabilidades

A continuación se definen roles y responsabilidades:

### 8.1 ISV/Participantes

Al ISV/Participante le corresponde desarrollar la App conforme las buenas prácticas, proveer documentación, preparar la Demo para la homologación.

### 8.2 Argentina Clearing



A Argentina Clearing le corresponde mantener y actualizar el procedimiento de homologación, designar a los auditores, emitir el Informe de Homologación y publicar los sistemas homologados.

### **8.3 Auditor Asignado**

A los auditores asignados les corresponderá realizar las verificaciones técnicas, funcionales y documentales de la aplicación.

## 9. Anexo I: Requerimientos de validación

A continuación se detallan los **requerimientos obligatorios** hacia la aplicación.

### 9.1 Requisitos funcionales del negocio

Categoría	Requisito		Detalle	
<b>9.1.1 Generales</b>	1. El sistema permite realizar el back office de un mercado.			
	2. El sistema permite administrar carteras de:	a) Futuros.		
		b) Opciones.		
	3. El sistema permite administrar más de una moneda.			
<b>9.1.2. Producto</b>	1. El sistema permite parametrizar los contratos compensados por ACSA:	a) Se cargan manualmente desde el sistema.	Ver Diccionario de Datos en Manual APBS: Método= ParametrosNuevo Consulta= ParametroCompleto (TipoConsulta = 2) Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>	
	2. Datos de los contratos que se guardan en el sistema:	a) ID Contrato		
		b) Subyacente (ID Producto)		
		c) Posición (descripción del contrato)		
		d) Tipo de Contrato (Futuro, Put o Call)		
		e) Precio de ejercicio (si es opción)		
		f) Fecha vencimiento del contrato.		
		g) Tamaño de Contrato (cantidad nominal)		

Categoría	Requisito		Detalle
		h) Unidad de Medida (en toneladas, dólares, onzas, barriles, etc.)	
<b>9.1.3. Operaciones</b>	3. En la operatoria diaria, la registración de las operaciones contempla:	a) Importación operaciones desde APBS.	
		b) Carga manual desde el Sistema.	
	4. En la importación de operaciones, se utilizan las siguientes consultas:	a) Todas las operaciones a una fecha dada.	Ver Diccionario de Datos en Manual APBS: Método= OperacionesNuevo Consulta= OperacionesOnLine (TipoConsulta = 1) Consulta= OperacionesAbiertas (TipoConsulta = 2) Consulta= OperacionesDiarias (TipoConsulta = 3) Consulta= OperacionesCanceladas (TipoConsulta = 4) Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>
		b) Operaciones canceladas luego del proceso diario.	
	5. En la importación de operaciones los datos que se guardan en el sistema son:	a) Boleta.	
		b) Fecha.	
		a) Hora.	
		b) Origen.	
		c) Cantidad.	
		d) Precio.	
		e) Comitente.	
		f) ID de Contrato.	
	g) Compra o Venta.		
h) Tipo de ejecución.			
6. En la importación de cancelaciones, los datos que se guardan en el sistema son:	a) Boleta Original.	Ver Diccionario de Datos en Manual APBS: Método= OperacionesNuevo Consulta= OperacionesCanceladas (TipoConsulta = 4) Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>	
	b) Boleta Cancelación.		
	c) Fecha Cancelación.		
	d) Cantidad.		
7. Con respecto a las carteras de los clientes, el proceso de cancelación se realiza (a ó b):	a) Importa cancelaciones desde APBS y cancela según ACSA.		
	b) Calcula las cancelaciones de operaciones con proceso propio y controla contra ACSA.		

Categoría	Requisito		Detalle	
	8. La administración de precios de ajuste diarios contempla:	a) Importación de precios de ajuste desde APBS.	Ver Diccionario de Datos en Manual APBS: Método= ParametrosNuevo Consulta= Parametros (TipoConsulta = 0) Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>	
		b) Carga manual desde el Sistema.		
	9. Con respecto al cálculo de diferencias de Futuros y Opciones, calcula las diferencias con proceso propio y controla contra ACSA.			Ver Diccionario de Datos en Manual APBS: Método= MovimientosContables Consulta= Movimientos Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>
	10. Con respecto al cálculo de resultados, calcula los resultados con proceso propio y controla contra ACSA.			
11. Con respecto al cálculo de márgenes, importa movimientos contables desde APBS.				
<b>9.1.4. Contabilidad</b>	1. En cuanto a la contabilidad del sistema, se generan asientos automáticos:	a) De márgenes		
		b) De diferencias		
		c) De primas		
d) De resultados				
2. En relación a comprobantes genera asientos automáticos a partir de recibos u órdenes de pago.				
3. Con respecto a la facturación de comisiones, calcula comisiones con proceso propio y se facturan.				
<b>9.1.5. Segregación de Fondos</b>	1. En relación a la cuenta corriente de comitentes:	a) Administra cuenta corriente a nivel comitente.		
		b) El sistema permite llevar la cuenta corriente en diferentes monedas.		

Categoría	Requisito	Detalle		
	2. En relación a la parametrización de los activos aceptados en garantía, se contempla:	Ver Diccionario de Datos en Manual APBS: Método= ParametrosNuevo Consulta= CotizacionesInstrumento (TipoConsulta = 4) Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>		
	b) Carga manual desde el Sistema.			
	3. Datos que se almacenan en el Sistema:	a) ID de Instrumento según ACSA.	Ver Diccionario de Datos en Manual APBS: Método= ParametrosNuevo Consulta= CotizacionesInstrumento (TipoConsulta = 4) Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>	
	b) Instrumento.	c) ID Moneda.		
	d) Cotización según ACSA.	a) Control de movimientos de instrumentos a nivel cliente brindando información vigente o histórica.		Ver Diccionario de Datos en Manual APBS: Método= ActivosGarantias Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>
	4. Con respecto a las garantías integradas, el sistema contempla:	b) Control contra el saldo global de ACSA.		
	5. Datos que se almacenan en el Sistema de las garantías integradas en Argentina Clearing:	a) Cuenta.	Ver Diccionario de Datos en Manual APBS: Método= ActivosGarantias Consulta= ActivosGarantias Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>	
	b) ID Instrumento.	c) Fideicomiso.		
	d) Tipo de Garantía.	e) Cantidad.		
	f) Fecha de Vencimiento.	g) Depositario.		
<b>9.1.6. Personas</b>	1. El sistema permite parametrizar las cuentas de los clientes, se cargan manualmente en el sistema y se asocia el ID de Comitente.	Ver Diccionario de Datos en Manual APBS: Método= Cuentas Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>		

Categoría	Requisito	Detalle
<b>9.1.7. Rendición de cuentas</b>	2. El sistema permite emitir los siguientes reportes para enviar a sus clientes:	a) Cuenta corriente.
		b) Garantías integradas.
		c) Cartera.
		d) Operaciones.
		e) Cancelaciones.
	3. El sistema permite enviar los reportes en forma manual.	

## 9.2 Proceso de desarrollo

Categoría	Requisito	Detalle
<b>9.2.1. Funciones</b>	1. Roles bien definidos dentro del equipo de desarrollo.	Debe existir una correcta y formal definición y separación de roles en el equipo de desarrollo. En particular, las personas encargadas de realizar pruebas o testing sobre la herramienta deben ser diferentes a las que realizan el desarrollo de la misma.
<b>9.2.2. Documentación</b>	1. Documentación interna del Sistema.	Debe existir documentación interna del sistema tal como casos de uso, diagramas de arquitectura, casos de prueba.
<b>9.2.3. Versiones</b>	1. Criterio de versionado de productos.	Se debe contar con un esquema de versionado de producto definido e implementado, a fin de poder identificar correctamente las distintas versiones de los productos y los cambios realizados en cada caso. Un sistema de versionado comodín que asegure que las correcciones de fallas se representarán en cambios de versión de baja jerarquía mientras que los cambios en funcionalidades existentes lo hagan en una jerarquía más alta, permitirá simplificar el proceso de RPO.
<b>9.2.4. Respaldo</b>	1. Resguardo del código fuente.	Se debe contar con un mecanismo de resguardo (Backup) del código fuente de la aplicación a homologar.

### 9.3 Seguridad

Categoría	Requisito	Detalle
<b>9.3.1. Autenticación y Autorización</b>	1. Existencia de un procedimiento de autenticación de usuarios.	<p>La aplicación debe requerir a todo aquel usuario, pasar satisfactoriamente un procedimiento de autenticación antes de la utilización de la misma. El procedimiento debe utilizar al menos uno de los 3 siguientes factores:</p> <ul style="list-style-type: none"> <li>• Secreto compartido (Ej: Contraseña / PIN)</li> <li>• Token (Tarjeta de coordenadas, Token de hardware, etc.)</li> <li>• Biometría</li> </ul> <p>El mecanismo de autenticación puede ser tanto propio (codificado en la aplicación) como integrado a un servicio externo (ej: Active Directory)</p>
	2. Administración de contraseñas.	<p>Si la aplicación administra las contraseñas de los usuarios (autenticación propia), debe contemplar los siguientes puntos:</p> <ul style="list-style-type: none"> <li>• El usuario debe poder cambiar su contraseña en cualquier momento.</li> <li>• Las contraseñas deben ser almacenadas en formato "HASH + SALT" con un algoritmo de HASH fuerte y un "SALT" aleatorio.</li> <li>• La aplicación no debe impedir al usuario la definición de contraseñas alfanuméricas.</li> <li>• La aplicación no debe impedir al usuario la definición de contraseñas "largas" (de 20 caracteres).</li> </ul>
	3. Utilización de IDs de usuarios únicos.	<p>La aplicación debe permitir la definición y utilización de IDs de usuario únicos por cada persona física que utilice la aplicación.</p>
<b>9.3.2. Autorización</b>	1. Funcionalidad de Autorización.	<p>Si la aplicación posee diferentes roles o permisos de acceso, debe implementar verificación de autorización en todas sus funcionalidades y accesos, de forma independiente al proceso inicial de autenticación. De esta forma, la aplicación debe validar entonces por cada invocación funcional o acceso a datos, si el usuario activo posee los roles o permisos necesarios para realizar dicha acción.</p> <p><b>Nota:</b> Una falla muy común en este aspecto, consiste en simplemente "ocultar" del menú funcional las opciones que no corresponden al rol o permisos del usuario activo.</p>
<b>9.3.3. Protección de la información</b>	1. Protección de los datos almacenados.	<p>La aplicación debe proteger criptográficamente los datos almacenados de carácter crítico o sensible, cuya confidencialidad sea un requisito.</p> <p>Aquellos datos que sólo requieran ser validados pero no leídos en su formato original (ej:</p>

Categoría	Requisito	Detalle
		<p>Contraseñas), se deben proteger con un algoritmo de HASH, fortalecido con un SALT aleatorio. Aquellos datos críticos o sensibles que por razones de negocio necesiten ser recuperados (ej: activos en garantía, saldos de cuentas, cartera) deben almacenarse encriptados, con un algoritmo considerado fuerte.</p> <p>A continuación se incluyen ejemplos de algoritmos criptográficos considerados “fuertes”:</p> <ul style="list-style-type: none"> <li>• <b>HASH:</b> SHA-256, RIPEMD-160, Whirlpool</li> <li>• <b>Encriptación simétrica:</b> AES, Serpent, Twofish (con claves de 256 bits o más)</li> <li>• <b>Encriptación asimétrica:</b> RSA, DSA (con claves de 2048 bits o más)</li> </ul> <p><b>Nota:</b> En todos los casos, se debe utilizar un algoritmo Standard de la industria, reconocido y testado.</p>
	2. Administración de claves de encriptación.	<p>Si la aplicación utiliza encriptación (simétrica o asimétrica), debe permitir el cambio periódico de la clave de encriptación.</p> <p>Dicha clave, debe ser accesible únicamente por un usuario con privilegios de administrador del sistema o aplicación.</p>
	3. Protección de los datos transmitidos.	<p>La aplicación debe proteger criptográficamente la transmisión de todos aquellos datos considerados críticos o sensibles, tanto entre diferentes componentes de la misma (ej: cliente/Servidor) como en la comunicación con terceras partes (ej: Integración o consultas con sistemas externos).</p> <p>La encriptación puede realizarse a nivel “dato puntual”, o bien a nivel capa de transporte (ej: TLS/SSL/IPsec). En ambos casos, deben utilizarse algoritmos de encriptación standard de la industria considerados “fuertes”.</p>



Categoría	Requisito	Detalle
<b>9.3.4. Auditoría</b>	1. Registros de Auditoría (Logs).	<p>La aplicación debe generar registros de auditoría que sirvan tanto para diagnosticar eventuales fallas funcionales u operativas (troubleshooting), como así también para el seguimiento y análisis de las actividades de los usuarios en caso de ser necesario. Dichos registros deben registrar la fecha y hora de ocurrencia del evento. Adicionalmente deben registrar por lo menos las siguientes actividades:</p> <ul style="list-style-type: none"> <li>• Log-In exitoso</li> <li>• Intento de log-In fallido</li> <li>• Cambio de contraseña</li> <li>• Inicio o detención del servicio o aplicación</li> <li>• Acciones críticas desde el punto de vista funcional y del negocio (ej: operaciones, órdenes, etc.)</li> </ul> <p>Los registros deben almacenarse de forma tal que no puedan ser eliminados, borrados o modificados por los usuarios normales de la aplicación, quedando esta función limitada al administrador del sistema.</p>
<b>9.3.5. Tests de seguridad</b>	1. Realización de pruebas de seguridad y verificación de vulnerabilidades.	<p>La versión a homologar de la aplicación, debe haber sido sometida a una prueba de seguridad del tipo “Test de Intrusión”, realizada por una empresa o profesional capacitado a tal fin. Dicha prueba de seguridad debe incluir como mínimo la verificación de vulnerabilidades tipificadas o conocidas en la industria del software (ej: Owasp Top 10)</p> <p>Se debe contar con evidencia de la realización de dicha prueba, como así también de la solución de los inconvenientes o vulnerabilidades eventualmente detectados en la misma.</p>
<b>9.3.6. Resguardo de datos</b>	1. Facilidades de copia de resguardo (Backup) y Restauración de datos.	<p>La aplicación debe poseer facilidades de copia de resguardo (backup) y restauración de los datos, con la finalidad de permitir la recuperación del sistema ante fallas graves, como la falla de un componente de hardware, o el borrado accidental de información. Dicha facilidad puede ser una funcionalidad propia de la aplicación, como un proceso externo a la misma (ej: volcado o “Dump” a nivel Base de Datos).</p> <p>El primer caso (funcionalidad propia) es preferido al segundo, ya que permite abstraer al usuario de la necesidad de acceder al Sistema Operativo o a las capas de software de base (ej: Base de Datos)</p> <p>En cualquiera de los casos, se debe contar con documentación que indique al usuario con claridad las instrucciones a seguir para la realización de una copia de resguardo de información y la eventual restauración de una copia de resguardo en el sistema.</p> <p>La información resguardada debe incluir como mínimo:</p>

Categoría	Requisito	Detalle
		<ul style="list-style-type: none"> <li>Datos críticos de negocio (ej: saldos de cuentas, activos en garantía, cartera)</li> <li>Cuentas de usuario y sus contraseñas</li> <li>Registros de auditoría</li> </ul> <p>Adicionalmente, la facilidad de copia de resguardo debe permitir la encriptación de la información al almacenarse en medios removibles (ej: Cinta, CD, DVD).</p>

#### 9.4 Documentación

Categoría	Requisito	Detalle
<b>9.4.1. Información para clientes</b>	1. Guía de Instalación.	El sistema debe contar con una guía de instalación que además incluya detalles de configuración y mantenimiento.
	2. Manual del Usuario.	El usuario deberá contar con un manual que detalle las cuestiones funcionales dentro del sistema.
	3. Notas de Versión.	Cada vez que se implemente una nueva versión es necesario un documento que detalle las mejoras y/o nuevas funcionalidades que incluye.

#### 9.5 Soporte funcional

Categoría	Requisito	Detalle
<b>9.5.1. Recursos de Soporte</b>	1. Existencia de un consultor.	El consultor deberá mantenerse actualizado con la evolución de los procesos de negocio y conocer al detalle el funcionamiento de la plataforma, como así también relevar y evaluar las necesidades de los usuarios, detectar inconsistencias, validar y generar requerimientos.
<b>9.5.2. Información de contacto para soporte</b>	1. Informar al cliente final sobre las vías de contacto.	En el Manual del usuario deberá informarse cuál es el canal de consultas existente.

## 10. Anexo II: Versionado comodín

La magnitud de los cambios se miden según el impacto del mismo sobre los siguientes ítems:

1. Funcionalidad de negocio.
2. Tecnologías utilizadas por la aplicación.
3. Administración, transmisión y almacenamiento de datos.

Consideramos cambios de impacto "alto", "medio" y "bajo" (o menor), siendo estos últimos los que pueden mantener el estado de homologación de una aplicación siempre y cuando se demuestre contar con y seguir un criterio de versionado formalmente documentado y coherente a tal fin.

Se considera cambio "alto" a aquel que tiene un impacto significativo en dichos ítems, como por ejemplo:

- Cambios que impacten en el cálculo de Diferencias, Cancelaciones, Resultados, armado de Carteras.
- Cambios que impacten de manera sustancial en la determinación de la Cuenta Corriente o en las Garantías de los Comitentes.
- Cambios que modifiquen las consultas de web services utilizadas.
- Cambio del lenguaje o Framework de programación
- Cambios mayores de arquitectura de la solución
- Incorporación de un nuevo tipo de interfaz o medio de comunicación con terceros

Se considera un cambio de magnitud "media" a aquel en donde el impacto sobre los ítems antes mencionado no es alto pero podría incurrir en un incumplimiento con los requisitos de homologación. Por ejemplo:

- Modificación en las interfaces de administración de usuarios
- Modificación del algoritmo criptográfico utilizado para la protección de datos sensibles, o del modo de administración de la clave de encriptación.

Por último, se considera un cambio de magnitud "baja" o "cambio menor" a aquel en el que el impacto sobre los ítems antes mencionado es mínimo y no permite incurrir en un incumplimiento con los requisitos de homologación. Por ejemplo:

- Correcciones o agregados que no modifican cálculos de Diferencias, Cancelaciones, cálculo de Resultados, armado de carteras.
- Correcciones o agregados inmateriales en la determinación de la Cuenta Corriente y Garantías del Comitente.

- Otras correcciones que no modifican la toma de datos de web services.
- Modificaciones de cálculos que están por fuera del alcance de la homologación.
- El agregado de un nuevo reporte.
- La solución de un bug en la visualización o ingreso de datos.
- El soporte para nuevos motores de bases de datos o versiones de Sistema Operativo o Software de base.

ROFEX/Argentina Clearing se reservan el derecho de considerar “de magnitud alta” otras modificaciones realizadas al Sistema.

## 11. Anexo III: Requisitos optativos

A continuación detallamos **requisitos optativos**.

Categoría	Requisito	Detalle
<b>Productos</b>	1. Importa <b>contratos</b> desde APBS.	Ver Diccionario de Datos en Manual APBS: Método= ParametrosNuevo Consulta= ParametroCompleto (TipoConsulta = 2) Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>
<b>Operaciones</b>	1. Importación de <b>Operaciones abiertas (Cartera)</b> a una fecha dada.	Ver Diccionario de Datos en Manual APBS: Método= OperacionesNuevo Consulta= OperacionesOnLine (TipoConsulta = 1) Consulta= OperacionesAbiertas (TipoConsulta = 2) Consulta= OperacionesDiarias (TipoConsulta = 3) Consulta= OperacionesCanceladas (TipoConsulta = 4) Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>
<b>Controles</b>	2. Con respecto al armado de las <b>Carteras</b> , calcula con proceso propio y controla contra ACSA.	
<b>Cálculo de Márgenes</b>	4. A los <b>márgenes</b> importados o calculados, aplica un <b>factor multiplicador</b> .	
<b>Tasas de mercado</b>	5. Con respecto al cálculo de <b>tasas de mercado</b> , importa movimientos contables desde APBS.	Ver Diccionario de Datos en Manual APBS: Método= MovimientosContables Consulta= Movimientos Link: <a href="http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx">http://www.argentinaclearing.com.ar/tecnologia/web_services.aspx</a>