GARA – Márgenes y Aforos

Aforos y Márgenes Iniciales – Caución y Pase Bursátil

Introducción

BYMA ha solicitado tener acceso a la información de Aforos y Márgenes Iniciales para la Operativa de Caución y Pase Bursátil de una manera más ágil a la que existe actualmente.

Cambios destinados a Agentes

Introducción

Se ha desarrollado un Web Service (WS) que está disponible para los Agentes que quieran obtener la información de aforos y márgenes iniciales de los distintos títulos habilitados en la operativa de Caución y Pase Bursátil. .

Descripción Funcional

El Servicio provee una lista de aforos y márgenes iniciales.
Para poder obtener estos los Agentes deben desarrollar el componente que invoque al Servicio ofrecido.

Se debe tener en cuenta que si la cantidad de registros a enviar supera los 5.000, el Web Service está preparado para paginar la consulta.

Este servicio solicita usuario y password, por lo que el Agente debe solicitar que se habilite un usuario especifico (puede ser genérico) con el rol para explotar Web Services desde GARA.

Por el mantenimiento de las passwords ver el ítem Manejo de Contraseñas

Invocación al Servicio - Request

La URL para descarga de los Aforos:

https://<url_gara>/garantias//service/api/v1/aforos

Por ejemplo:

https://posicionesygarantias.sba.com.ar/posicionesygarantias/service/api/v1/garantias/aforos

Invocación al Servicio - Response

La respuesta de tipo JSON y tiene el siguiente formato:

[
  {
    “codigo”: *valorNumérico*,
    “denominacion”: *“valorAlfanumerico”*,
    “codigoNegociacion”: *“valorAlfanumerico”*,
    “moneda”: *“valorString”*,
    “aforo”: *valorNumérico*,
    “margenIncial”: *valorNumérico o vacio*
  }
]

Ejemplo:


```
[
    {
        "codigo": 7,
        "denominacion": "ALUAR S.A. ORDS 1 VOTO ESCRITURALES",
        "codigoNegociacion": "ALUA",
        "moneda": "PESOS",
        "aforo": 70,
        "margenInicial": 30
    },
    {
        "codigo": 19,
        "denominacion": "AGROMETAL S.A. ORDS. 1 VOTO
ESCRITURALES",
        "codigoNegociacion": "AGRO",
        "moneda": "PESOS",
        "aforo": 50,
        "margenInicial": 50
    },
    {
        "codigo": 21,
        "denominacion": "ALPARGATAS S.A. ORD. 1 VOTO
ESCRITURALES",
        "codigoNegociacion": "ALPA",
        "moneda": "PESOS",
        "aforo": 60,
        "margenInicial": 20
    },
```


Informacion General del WS

Tecnologías utilizadas

Desde el punto de vista los protocolos y estándares utilizados, la implementación del Web-Service es la siguiente:

- GARA provee un *HTTPS Server* capaz de recibir un request por parte del cliente.

- Este server recibe los requests en una URL que será informada a los usuarios del servicio.
- Para realizar un requerimiento el cliente GARA cuenta una Interfaz REST: Se envía un GET indicando en los parámetros de la URL los filtros requeridos y se recibe una lista de Aforos y Márgenes Iniciales en formato JSON.
- Para autenticar al cliente se utiliza "HTTP Basic Authentication", es se autentica mediante usuario/password según el esquema de autenticación Basic

Manejo de Contraseñas

Para el manejo de la contraseña se provee una interfaz de tipo REST que permite al cliente actualizar la clave de acceso (utilizada en el esquema de autenticación BASIC).

Debemos notar que se usará el servicio actualmente expuesto para SDIB.

Este servicio sólo está disponible en la modalidad REST con autenticación BASIC.

La URL para invocar este servicio sería:

https://<url_sdib>/clave?anterior=<clave anterior>&nueva<nueva clave>

Donde

- <clave anterior> es la clave anterior del usuario autenticado
- <nueva clave> es la nueva clave que se quiere asignar al usuario autenticado

Atención: Esta URL debe invocarse con el método 'POST'

Por ejemplo:

https://sdib.sba.com.ar/sdib/service/basic/rest/clave?anterior=secreto1&nueva=secreto2

En caso de que SDIB haya procesado el pedido envía un HTTP Status Code = 200, caso contrario envía otro HTTP Status Code (ver sección "Manejo de Errores" para más detalles)

En cuanto al contenido de la respuesta (si el pedido se pudo procesar), ésta utiliza un formato JSON con los siguientes campos:

- **"resultado"** : Los valores posibles son "OK" (en caso de que se haya renovado la clave) O "ERROR" si hubo un problema (clave anterior inválida, clave nueva no cumple con los requisitos de seguridad, etc)

- **"detalle"**: Mensaje de error en caso de que el resultado haya sido "ERROR"

Ejemplos de respuesta:

```
{"resultado":"OK"}
```
→ El cambio de clave fue exitoso

```
{"resultado":"ERROR","detalle":"Fallo al autenticar el usuario ag00011"}
```

```
{"resultado":"ERROR","detalle":"La contraseña del usuario ag00011 no pudo ser modificada"}
```

```
{"resultado":"ERROR","detalle":"No se especifico el parametro 'anterior'"}
```

Manejo de Errores

GARA siempre envía como respuesta al cliente un HTTP Status Code [5] con valor 200 en caso de que pueda completar el requerimiento.

Cualquier otro valor significa que GARA no pudo completar el requerimiento y debe ser considerado un error.

En caso de que GARA complete el requerimiento detectando algún error (en la invocación o en el estado de la aplicación) envía una respuesta con un HTTP Status Code distinto de 200 y puede enviar además un texto describiendo el error.

Seguridad

En cuanto a la seguridad, la utilización de HTTPS para las comunicaciones entre GARA y el cliente garantiza la *privacidad* e *integridad* de toda la información que se intercambia.

Con respecto a la autenticación se utiliza Autenticación con HTTP Basic-Authentication (usuario/contraseña)

El cliente del servicio debe contar con un usuario/contraseña de aplicación similar o igual al que se utiliza para conectarse con GARA, hay que tener en cuenta que:

- Para poder utilizar este usuario, la Entidad Cliente deberá solicitar la asignación de un nivel de autorización especial a dicho usuario.

- La contraseña de este usuario debe ser definida y actualizada de acuerdo a las mismas políticas de seguridad de la aplicación que se aplican para todos los usuarios interactivos.

En cuanto al funcionamiento del mecanismo: cuando el Cliente intente acceder al Servicio este le solicitará un usuario y contraseña de acuerdo a lo establecido por el mecanismo BASIC [6]. Dado que la comunicación se realiza por HTTPS la privacidad del usuario y contraseña informado está garantizada.

Referencias

[1] REST: Representational state transfer

[2] HTTPS

[3] SSL

[5] HTTP Status Code

[6] HTTP Authentication: Basic and Digest Access Authentication