SERVICIOS SATELITALES

GUÍA DE USUARIO PARA ESQUEMA DE SEGURIDAD Y SERVICIOS SATELITALES

- **PERSONAS FÍSICAS**
- **PERSONAS MORALES**

MS-PF-SERV-SATEL / V.003
SEPTIEMBRE 2014

ÍNDICE

INTRODUCCIÓN

El esquema de seguridad establecido por Buró de Crédito llamado ***"Servicios Satelitales"*** permite que las consultas realizadas por los Usuarios a través de la conexión CPU –CPU manejen una contraseña cifrada de ocho posiciones. Este servicio se robustece además con políticas de rotación (expiración) y construcción e historial de contraseña, lo que ofrece mayor protección en el proceso de autenticación (login) de cada consulta.

En el esquema de seguridad considera los siguientes claves:

1) Claves para **Personas Físicas**, (*esquema de seguridad del Formato INTL11*)
2) Esquema para claves de **Personas Morales**
3) La creación de nuevos servicios adicionales al servicio de consulta de reporte de crédito

El formato INTL que soportará los cambios incluidos en el nuevo esquema de seguridad se conoce como **Formato INTL11**, y tiene un par de cambios específicos sobre su antecesor el Formato INTL 10.

Asimismo ***Servicios Satelitales*** permite a los Usuarios puedan obtener con una contraseña cifrada de 8 posiciones, así como conocer la fecha en que dicha contraseña expirará, es decir, dejará de ser válida para realizar consultas de reporte de crédito a través de la conexión CPU-CPU a la base de **Personas Físicas** y **Personas Morales**

El presente documento le brindará una guía detallada sobre el uso, construcción y operación de los servicios satelitales que conforman el nuevo Esquema de Seguridad de Buró de Crédito, así como un conjunto de preguntas frecuentes que muestran a través de ejemplos específicos y respuestas concretas algunas de las dudas más comunes por parte de nuestros Usuarios.

Histórico de Cambios

Historial de Cambio			
Fecha Liberación	**Tipo de Cambio**	**Resumen del Cambio con respecto a la Información Anterior**	**Página**
Septiembre '14	Reglas para la Construcción de Contraseñas	Se complemento la descripción de la cuarta viñeta.	11
Marzo '14	Cambio de codificación	Cambio en codificación del documento (Carátula). Actualización de Contactos BC	1 26

SERVICIOS SATELITALES

Los servicios satelitales aparecen como un soporte indispensable a los cambios que involucra las claves de Personas Físicas y Personas Morales, cubriendo fundamentalmente dos propósitos:

- Cifrar una contraseña proporcionada por el cliente para incorporarla al Sistema de Seguridad interno del Buró de Crédito
- Proveer la fecha en la que la contraseña en uso expirará

Los servicios satelitales cuentan con su propia especificación sintáctica y semántica, basada en mensajes tipo XML a través de los cuales es posible invocar los servicios que residen en Buró de Crédito; dicha especificación es descrita con mayor detalle en la siguiente sección.

ESTRUCTURA BÁSICA DE LOS SOBRES DE PETICIÓN Y RESPUESTA

La especificación para la invocación de los servicios satelitales se basa en mensajes tipo XML, los cuales son representados por *sobres* de petición y respuesta, cuya estructura está identificada con elementos bien definidos. A continuación se describe a detalle cada uno de los elementos que conforman los *sobres*.

SOBRE DE PETICIÓN

Un sobre de petición se usa para poder invocar cualquiera de los servicios satelitales disponibles. La estructura básica de un sobre de petición se compone de cinco elementos fundamentales, los cuales se listan a continuación.

1. bc-request-envelope

Establece el encabezado del sobre de petición. Este elemento cuenta con un atributo requerido de nombre "version", que identifica el propio *sobre*. Actualmente la versión 1.0 es la única soportada, por lo que cualquier otro valor generará un error. La manera correcta de construir el encabezado se muestra a continuación:

```
<bc-request-envelope version="1.0">
```

Es importante mencionar que al tratarse de mensajes tipo XML, cada elemento del sobre de petición y respuesta tiene su contraparte que "cierra". Por ejemplo, para el elemento "<bc-request-envelope>", existe su contraparte "</bc-request-envelope>" para cierre. Lo anterior permite delimitar y conocer cuál es el contenido del elemento.

2. bc-request

Establece el cuerpo de una petición dentro del sobre. El componente <bc-request> tiene otros elementos que dan información contextual de la propia petición: <credentials> y <service>. El primero provee información para autenticar al Otorgante que solicita alguno de los servicios satelitales. El segundo elemento, <service>, guarda información sobre el servicio que en particular se quiere invocar.

Los elementos <credentials> y <service> se describen con mayor detalle más adelante.

Se debe considerar que un sobre de petición (<bc-request-envelope>) puede contener "N" número de elementos <bc-request>. Esta funcionalidad permite incluir múltiples solicitudes dentro de un solo sobre de petición, evitando que el Usuario deba enviar un sobre por cada petición que quiera realizar.

A continuación se muestra cómo se construye la petición del servicio getExpirationDate para el member code BC24681012. Se asume que la clave tiene asignada la contraseña "tWi4p9us".

```
<bc-request>
      <credentials member="BC24681012" password="tWi4p9us" />
   <service name="getExpirationDate" />
</bc-request>
```

Más adelante se verán algunos ejemplos de cómo realizar peticiones con múltiples servicios dentro de un mismo elemento <bc-request>.

3. credentials

Este elemento contiene información para autenticar al Otorgante que hace la petición, por lo que reside dentro del elemento <bc-request>. Básicamente el elemento <credentials> tiene un par de atributos ("member" y "password"), a través de los cuales se establece la clave del Otorgante junto con la contraseña asociada; estos atributos son utilizados por los **Servicios Satelitales** para autenticar a la Institución solicitante del servicio.

A continuación un ejemplo de cómo construir el elemento <credentials> dentro de una petición:

```
<credentials member="BC24681012" password="tWi4p9us" />
```

4. service

Establece el nombre del servicio que se quiere invocar, así como los posibles parámetros que dicho servicio puede requerir. Este elemento cuenta con el atributo requerido "name", cuyo valor sólo puede ser changePassword o getExpirationDate, dependiendo del servicio que se quiera invocar. Cualquier otro nombre de servicio resultará en un error. También es importante mencionar que el nombre de los servicios debe ser escrito tal y como aparece en este documento. Es decir, respetando mayúsculas y minúsculas, de lo contrario se recibirá un error como respuesta a la petición.

No todos los servicios requieren de parámetros adicionales, sin embargo, para los servicios que así lo requieren se cuenta con el elemento <param>, que se describe a continuación.

5. param

Este elemento permite el paso de parámetros hacia un servicio, por lo que se encuentra dentro del elemento <service>. Básicamente, el elemento cuenta con un par de atributos: "name" y "value", a través de los cuales puede establecerse respectivamente nombre del parámetro y valor asociado al mismo.

A continuación un ejemplo de cómo se presenta el elemento <param>:

```
<param name="old-password" value="tWi4p9us" />
```

SOBRE DE RESPUESTA

La estructura básica de un sobre de respuesta se compone de 6 elementos y a continuación se detallan.

1. bc-response-envelope

Establece el encabezado de un sobre de respuesta. Este elemento cuenta con un par de atributos: "operation" y "versión". El primero provee información de estatus general del sobre y presenta tres diferentes valores: "ALL", "FAILURE, "PARTIAL", con el fin de determinar el éxito de la petición. El valor que se muestra en este atributo se encuentra íntimamente ligado con el código de retorno de la propia petición.

Más adelante se detallará el elemento <status> y ahí se retomará el significado de los diferentes valores que puede tener el atributo "operation".

El valor para el atributo "versión" es el mismo que se envió como parte del sobre de petición.

A continuación un ejemplo del encabezado de un sobre de respuesta:

```
<bc-response-envelope operation="ALL" version="1.0">
```

2. bc-response

Representa la respuesta a la petición hecha a través del elemento <bc-request> dentro del sobre de petición. Por cada elemento <bc-request> que se envía en el sobre de petición existe un <bc-response> relacionado, la forma en que se logra esta relación es a través del atributo "member".

Por ejemplo, suponga que dentro de un sobre de petición se envía lo siguiente:

```
<bc-request>
      <credentials member="BC24681012" password="tWi4p9us" />
   <service name="getExpirationDate" />
</bc-request>
```

Nótese que la petición hecha a través del elemento <bc-request> se ejecuta para el member BC24681012, por lo que el sobre de respuesta deberá identificar la respuesta con este mismo identificador, como se muestra a continuación:

```
<bc-response member="BC24681012">

      <!-- Cuerpo de la respuesta -->
      ...
</bc-response>
```

Esto permite establecer un vínculo entre cada una de las peticiones (<bc-request>) y su respuesta correspondiente (<bc-response>).

El elemento <bc-response> puede componerse de 1 o "N" número de elementos <service-response>, de acuerdo con el número de elementos <service> enviados en el sobre de petición.

3. service-response

Este elemento representa la respuesta generada por alguno de los servicios satelitales disponibles. El elemento <service-response> cuenta con el atributo "name", que contiene como valor el nombre del servicio satelital solicitado. Por ejemplo para la siguiente petición:

```
<bc-request>
      <credentials member="BC24681012" password="tWi4p9us" />
   <service name="getExpirationDate" />
</bc-request>
```

El elemento <service-response> contiene el nombre del servicio invocado, tal y como aparece a continuación:

```
<bc-response member="BC24681012">
   <service-response name="getExpirationDate">
      <!– Cuerpo de la respuesta -->
            ...
   </service-response>
</bc-response>
```

El elemento < service-response> se compone de elementos adicionales que brindan información sobre el estatus (<status>) y resultado (<result-set>) de la petición.

4. status

Este elemento contiene el código de retorno del servicio satelital invocado. Como parte de la especificación en los sobres de respuesta, se presentan códigos para conocer el estatus final del servicio solicitado y se acompañan de una breve descripción. La información se presenta en el elemento <status> y a continuación se muestra el significado de cada uno.

Código	Significado	Descripción
0	Exitoso	El servicio satelital invocado se ejecutó exitosamente.
1000	Error en autenticación	El atributo "member" o "password" proporcionado como parte del elemento <credentials> de la petición es incorrecto.
2000	Error en datos de entrada	Implica que el valor asignado en alguno de los parámetros de entrada es incorrecto.

A continuación un ejemplo de cómo se ve este elemento cuando la respuesta es exitosa.

```
<bc-response member="BC24681012">
   <service-response name="getExpirationDate">
   <status code="0">SUCCESS</status>
         <!– Cuerpo de la respuesta -->
            ...
   </service-response>
</bc-response>
```

La siguiente tabla muestra la relación entre los diferentes códigos de retorno y su afectación en el atributo "operation" del sobre de respuesta. (<bc-response-envelope>).

Operation	Status Code	Se presentará cuando
ALL	0	Todas las solicitudes (<bc-request>) enviadas en el sobre de petición (<bc-request-envelope>) regresaron con status code igual a "0".
FAILURE	---	El sobre de petición no cumple con la estructura básica descrita en este documento.
PARTIAL	N/A	El elemento <status> en al menos una de las solicitudes enviadas en el sobre de petición, es diferente a cero.
PARTIAL	1000	Se presenta cuando el "member code" o "password" enviado en la petición son incorrectos.
PARTIAL	2000	El nombre del servicio solicitado es inválido o alguno de los parámetros esperados por el servicio no está definido o no cuenta con un valor semánticamente válido.

5. result-set

Este elemento es sólo un contenedor de elementos <result> y son estos últimos los que guardan los valores de respuesta retornados por el servicio satelital. Este elemento sólo aparece cuando la respuesta fue exitosa, es decir: el atributo "code" del elemento <status> es igual a cero.

6. result

Este elemento contiene la respuesta del servicio satelital invocado. Se compone de un par de atributos: "key" y "value", donde "key" contiene un identificador definido en la propia especificación del servicio satelital y "value" es el valor que dicho identificador tiene.

El siguiente ejemplo muestra cómo el servicio satelital getExpirationDate retorna el identificador expiration-date como parte de su especificación y una fecha en el campo "value".

```
<service-response name="getExpirationDate">
      <status code="0">SUCCESS</status>
      <result-set>
         <result key="expiration-date" value="12/17/2004"/>
      </result-set>
</service-response>
```

NOTA IMPORTANTE:

Es importante destacar que como parte de la especificación de mensajes de petición y respuesta arriba descrita, el caracter de fin de cadena de envío será el valor **ASCII 19** (en decimal), por lo que, tanto el sobre de solicitud como el de respuesta terminarán con dicho caracter, con el objetivo de identificar el fin del sobre.

SERVICIO DE CAMBIO DE CONTRASEÑA ("CHANGE PASSWORD").

A partir de una contraseña definida por el Usuario, este servicio retorna una contraseña cifrada la cual es almacenada en el sistema de seguridad de Buró de Crédito, dicha contraseña deberá embeberse (respetando la composición y forma de la clave: minúsculas y mayúsculas) en el Registro de Consulta, para así acceder a la consulta del Reporte de Crédito. Periódicamente, y de acuerdo con la fecha de expiración indicada por el sistema, habrá de renovarse la clave. De no hacerlo, la Institución no podrá continuar realizando consultas de Reportes de Crédito. La siguiente tabla muestra los **parámetros de entrada y salida** de este servicio satelital:

Nombre de Servicio	Parámetros de Entrada	Parámetros de Salida	Notas
changePassword	old-password new-password	encrypted-password	Ambos parámetros de entrada son requeridos. El valor para el parámetro old-password deberá ser la contraseña actual del otorgante, mientras que el parámetro new-password deberá ser una cadena válida que cumpla con las **Reglas para la Construcción de Contraseñas (Passwords)**.

REGLAS PARA LA CONSTRUCCIÓN DE CONTRASEÑAS (PASSWORDS)

La contraseña que el Usuario envía a través del parámetro de entrada "**new-password"** deberá cumplir las siguientes reglas de construcción para ser considerado como válida:

- Ser clave alfanumérica.
- Tener una longitud de 8 caracteres.
- No debe iniciar o finalizar con número.
- No se permiten más de 2 caracteres consecutivos iguales (AAA o BBB son casos inválidos).
- Debe contener al menos un dígito.
- No deberán ser simétricos. Es decir, los primeros cuatro caracteres no podrán ser iguales a los últimos cuatro caracteres. Por ejemplo: **A32iA32i** es un password simétrico y por lo tanto inválido.
- Sólo cuando **solicite por primera vez** el servicio satelital "changePassword" se podrá y deberá utilizar dos veces consecutivas la contraseña actual de 4 posiciones relacionada con el member code. Por ejemplo, si la contraseña actual es "ABCD", al enviar la solicitud por primera ocasión deberá ser "ABCDABCD".
- Para la contraseña o password se podrán utilizar letras minúsculas y/o mayúsculas.

Cabe mencionar que las contraseñas que se registren en el Sistema de Seguridad Buró de Crédito contarán con las siguientes reglas de administración:

- **Tendrán una vigencia de 30 días.** Es necesario realizar el cambio de contraseña previo a la fecha de expiración.

- **Después de 3 intentos fallidos en la autenticación, la cuenta del usuario será bloqueada.** En caso de que su cuenta se encuentre en esta situación, será necesario comunicarse a Buró de Crédito, al área de Atención a Usuarios (5449 4949) para solicitar la reactivación de la contraseña actual.
  La nueva contraseña (asignada en automático por Buró de Crédito) sólo le servirá para poder invocar los Servicios Satelitales, por lo que usted no podrá realizar consultas INTL, hasta cambiar por una contraseña definida por usted a través del Servicio Satelital "**changePassword**".

A continuación se muestra un ejemplo con la construcción de un **sobre de petición solicitando el servicio satelital "changePassword"** para una claves de **Personas Físicas** al usuario BC24681012 cuyo password vigente es AcW24xxQ:

```
<bc-request-envelope version="1.0">
      <bc-request>
            <credentials member="BC24681012" password="AcW24xxQ" />
            <service name="changePassword">
                  <param name="old-password" value="AcW24xxQ" />
                  <param name="new-password" value="B5d2CRjD" />
            </service>
      </bc-request>
</bc-request-envelope>
```

La respuesta a la petición anterior es la siguiente:

```
<?xml version="1.0" encoding="UTF-16" standalone="yes"?>
<bc-response-envelope operation="ALL" version="1.0">
    <bc-response member="BC24681012">
        <service-response name="changePassword">
            <status code="0">SUCCESS</status>
            <result-set>
                <result key="encrypted-password" value="bQSt84:J"/>
            </result-set>
        </service-response>
    </bc-response>
</bc-response-envelope>
```

A continuación se muestra un ejemplo con la construcción de un sobre de petición solicitando el servicio satelital **"changePassword"** para una claves de **Personas Morales** al usuario **9999GONZALEZN** cuyo password vigente es **9999GONZALEZN**:

```
<?xml version="1.0" encoding="UTF-16" standalone="yes"?>
<bc-request-envelope lang="SP" version="1.0">
    <bc-request>
        <credentials member="9996GONZALEZN" password="9999GONZALEZN"/>
        <service name="changePassword">
            <param name="old-password" value="9999GONZALEZN"/>
            <param name="new-password" value="eal7am1r"/>
        </service>
    </bc-request>
</bc-request-envelope>
```

SOLICITUD DE CAMBIO DE CONTRASEÑA POR PRIMERA OCASIÓN

Es importante mencionar, que para los Usuario que cuentan con contraseñas de 4 posiciones, existe una regla para llevar a cabo el cambio de contraseña por primera vez:

La contraseña actual de cuatro posiciones debe duplicarse para formar una contraseña de ocho posiciones.

Por ejemplo, asumiendo que la contraseña del member code es "4H3S", para la primera solicitud debe usarse repetido: "4H3S4H3S". Esto aplica sólo la primera vez que se solicita contraseña y en caso de no considerar dicha regla, no se podrá obtener la contraseña cifrada.

Dada la especificación de envió de mensajes para el uso de servicios satelitales y asumiendo que existe una clave de otorgante ZZ995010001 y password 4H3S, la petición de contraseña se construirá de la siguiente manera:

```
<?xml version="1.0" encoding="UTF-16"?>
<bc-request-envelope version="1.0">
     <bc-request>
        <credentials member="ZZ99501001" password="4H3S4H3S"/>
        <service name="changePassword">
              <param name="old-password" value="4H3S4H3S"  />
              <param name="new-password" value="newPwd4u"  />
        </service>
    </bc-request>
</bc-request-envelope>
```

La respuesta regresará el nuevo password encriptado. A continuación el ejemplo de salida:

```
<?xml version="1.0" encoding="UTF-16" standalone="yes"?>
<bc-response-envelope operation="ALL" version="1.0">
      <bc-response member="ZZ99991001">
            <service-response name="changePassword">
                  <status code="0">SUCCESS</status>
                  <result-set>
                    <result key="encrypted-password" value="r|9w;H*E" />
                  </result-set>
            </service-response>
      </bc-response>
</bc-response-envelope>
```

Es justamente el valor en el parámetro "encrypted-password", que debe ser embebido (respetando la composición y forma de la clave: minúsculas y mayúsculas) en el encabezado del registro de consultas del Formato INTL para proceder a la obtención de Reportes de Crédito a través del medio de consulta CPU.

Es importante mencionar que la contraseña encriptada que regresa BC deberá ser utilizada como parte de las credenciales (elemento <credentials>) cada vez que se solicite alguno de los servicios satelitales.

SERVICIO "GETEXPIRATIONDATE"

Como parte de las políticas del ***Esquema de Seguridad del Buró de Crédito***, se requiere que la contraseña asociada al Usuario expire cada 30 días naturales, por lo que a través de este servicio se podrá solicitar la obtención de la fecha en que la contraseña vigente dejará de ser válida para realizar consultas de Reporte de Crédito de Personas Físicas y/o Personas Morales.

La siguiente tabla muestra los parámetros de entrada y salida para el servicio satelital **"getExpirationDate"**.

Nombre de Servicio	Parámetros de Entrada	Parámetros de Salida	Notas
getExpirationDate	N/A	expiration-date	El formato de la fecha de expiración que regresa este servicio es: **mm/dd/aaaa**.

A continuación se muestra un ejemplo con esquema de **Personas Morales** con la construcción de un sobre de petición para el servicio **"getExpirationDate"**:

```
<bc-request-envelope version="1.0">
      <bc-request>
            <credentials member="9999GONZALEZN" password="9999GONZALEZN" />
            <service name="getExpirationDate" />
      </bc-request>
</bc-request-envelope>
```

La respuesta de la petición presenta la siguiente información:

```
<?xml version="1.0" encoding="UTF-16" standalone="yes"?>
<bc-response-envelope operation="ALL" version="1.0">
    <bc-response member="9999GONZALEZN">
        <service-response name="getExpirationDate">
            <status code="0">SUCCESS</status>
            <result-set>
                <result key="expiration-date" value="08/30/2012"/>
            </result-set>
        </service-response>
    </bc-response>
</bc-response-envelope>
```

SOLICITUD DE SERVICIOS MÚLTIPLES

Es importante considerar que los Servicios Satelitales pueden trabajar de forma individual o en conjunto. Es decir, en los ejemplos descritos hasta ahora únicamente se hace referencia a los servicios de forma individual, sin embargo se puede crear una **Solicitud de Servicios Múltiples**. Por ejemplo en una misma petición se puede solicitar cambio de password y solicitud de fecha de expiración. A continuación se muestra el caso.

```
<bc-request-envelope version="1.0">
      <bc-request>
            <credentials member="ZM58002326" password="ab3hdweQ" />
      <service name="changePassword">
                  <param name="old-password" value="ab3hdweQ" />
                    <param name="new-password" value="secret04" />
            </service>
            <service name="getExpirationDate" />
      </bc-request>
</bc-request-envelope>
```

La respuesta de la petición anterior le devolverá la siguiente información:

```
<?xml version="1.0" encoding=" UTF-16" standalone="yes"?>
<bc-response-envelope operation="PARTIAL" version="1.0">

      <bc-response member="ZM58002326">

            <service-response name="changePassword">
                  <status code="200">INVALID DATA</status>
            </service-response>

            <service-response name="getExpirationDate">
                  <status code="0">SUCCESS</status>
                  <result-set>
                     <result key="expiration-date" value="15/09/2005" />
            </result-set>
            </service-response>

      </bc-response>

</bc-response-envelope>
```

Como puede observarse la respuesta de esta petición fue **"Partial"**, pues en una de las dos peticiones enviadas no se obtuvo la respuesta esperada.

La petición errónea fue **"changePassword"**, pues en la construcción de la nueva contraseña no se consideraron adecuadamente las reglas mencionadas en la sección referente a dicho servicio.

La petición **"getExpirationDate"** sí devolvió la Fecha de Expiración de la contraseña solicitada, pues el member code y password vigente están ligados mutuamente. Es decir, la información de entrada fue autenticada en el sistema de seguridad de Buró de Crédito.

MÚLTIPLES SOLICITUDES CON MÚLTIPLES SERVICIOS

Si usted requiere hacer una petición que contenga la solicitud de uno o ambos servicios, para diferentes members codes, bastará con que construya una petición llamada **múltiples solicitudes con múltiples servicios**, a continuación se muestra un ejemplo.

```
<bc-request-envelope version="1.0">

      <!-- A request with a single service -->
      <bc-request>
            <credentials member="ZZ53001005" password="fgwD3x9i" />
                  <service name="getExpirationDate" />
      </bc-request>

      <!-- Multiple services request -->
      <bc-request>
            <credentials member="ZM58002326" password="ab3hdweQ" />
                  <service name="changePassword">
                <param name="old-password" value="ab3hdweQ" />
                  <param name="new-password" value="secret04" />
            </service>
            <service name="getExpirationDate" />
      </bc-request>
</bc-request-envelope>
```

En esta petición, o ”sobre”, se observa la solicitud de los siguientes servicios:

- Para el Member Code ZZ53001005 únicamente se solicito el servicio **“getExpirationDate”**.
- Para el Member Code ZM58002326 se solicitaron ambos servicios.

```
<?xml version="1.0" encoding=" UTF-16" standalone="yes"?>
<bc-response-envelope operation="PARTIAL" version="1.0">
      <bc-response member="ZZ53001005">
            <service-response name="getExpirationDate">
                  <status code="0">SUCCESS</status>
                  <result-set>
                  <result key="expiration-date" value="15/09/2005" />
                  </result-set>
            </service-response>
      </bc-response>
      <bc-response member="ZM58002326">
                  <service-response name="changePassword">
                  <status code="200">INVALID DATA</status>
            </service-response>
                  <service-response name="getExpirationDate">
                  <status code="0">SUCCESS</status>
                  <result-set>
                  <result key="expiration-date" value="15/09/2005" />
                  </result-set>
            </service-response>
      </bc-response>
</bc-response-envelope>
```

La respuesta obtenida es parcial, pues en la segunda solicitud correspondiente al member code ZM58002326 en el servicio **"changePassword"** no se consideraron adecuadamente las reglas mencionadas en la sección correspondiente a este servicio.

EJEMPLOS DE PETICIONES INDIVIDUALES Y EN LOTE

1. Solicitud y Respuesta completamente exitosa.

```
<bc-request-envelope version="1.0">
      <!-- A request with a single service -->
      <bc-request>
            <credentials member="ZZ58002326" password="AX3EAX3E" />
            <service name="changePassword">
                  <param name="old-password" value="AX3EAX3E" />
                  <param name="new-password" value="B5R4D2CR" />
            </service>
      </bc-request>
</bc-request-envelope>
```

```
<?xml version="1.0" encoding="UTF-16" standalone="yes"?>
<bc-response-envelope operation="ALL" version="1.0">
    <bc-response member="ZZ58002326">
        <service-response name="changePassword">
            <status code="0">SUCCESS</status>
            <result-set>
                <result key="encrypted-password" value="fQ1w526n32>
            </result-set>
        </service-response>
    </bc-response>
</bc-response-envelope>
```

2. Solicitud y Respuesta parcialmente exitosa

```
<bc-request-envelope version="1.0">
      <bc-request>
            <credentials member="ZZ58002320" password="5p8256FJ1 />
            <service name="changePassword">
                  <param name="old-password" value="5p8256FJ1 />
                  <param name="new-password" value="1RR2ND1D" />
            </service>
            <service name="getExpirationDate" />
      </bc-request>
</bc-request-envelope>
```

La respuesta de esta petición, como se observa en el siguiente cuadro, fue **parcial** dado que en la primera petición el password enviado no cumple con las reglas mencionadas en la sección correspondiente a este servicio.

```
<?xml version="1.0" encoding="UTF-16" standalone="yes"?>
<bc-response-envelope operation="PARTIAL" version="1.0">
    <bc-response member="ZZ58002320">
        <service-response name="changePassword">
            <status code="2000">The new password you typed is not correct
        </status>
        </service-response>
        <service-response name="getExpirationDate">
            <status code="0">SUCCESS</status>
            <result-set>
                <result key="expiration-date" value="10/30/2004"/>
            </result-set>
        </service-response>
    </bc-response>
</bc-response-envelope>
```

3. Solicitud y Respuesta parcialmente exitosa para solicitudes múltiples con servicios múltiples

```
<bc-request-envelope version="1.0">
      <bc-request>
            <credentials member="ZZ58002322" password="W5PRW5PR" />
            <service name="changePassword">
                  <param name="old-password" value="W5PRW5PR" />
                  <param name="new-password" value="B1NC4M2R" />
            </service>
            <service name="getExpirationDate" />
      </bc-request>

<bc-request>
            <credentials member="ZZ58002340" password="PE8YPE8Y" />
            <service name="changePassword">
                  <param name="old-password" value="PE8YPE8Y" />
                  <param name="new-password" value="B1NS77BC" />
            </service>
            <service name="getExpirationDate" />
      </bc-request>
</bc-request-envelope>
```

```
<?xml version="1.0" encoding="UTF-16" standalone="yes"?>
<bc-response-envelope operation="PARTIAL" version="1.0">
    <bc-response member="ZZ58002322">
        <service-response name="changePassword">
            <status code="0">SUCCESS</status>
            <result-set>
                <result key="encrypted-password" value="Q-X+JYZ*"/>
            </result-set>
        </service-response>
        <service-response name="getExpirationDate">
            <status code="0">SUCCESS</status>
            <result-set>
                <result key="expiration-date" value="10/31/2004"/>
            </result-set>
        </service-response>
    </bc-response>
    <bc-response member="ZZ58002340">
        <service-response name="changePassword">
            <status code="1000">The membercode or password is incorrect. Recall
that letters must be typed using the correct case.
        </status>
        </service-response>
        <service-response name="getExpirationDate">
            <status code="1000">The membercode or password is incorrect. Recall
that letters must be typed using the correct case.
        </status>
        </service-response>
    </bc-response>
</bc-response-envelope>
```

Como se observa en la respuesta, el resultado es **parcial**, dado que el password enviado para el segundo member code no es correcto. Por lo tanto, no devolvió respuesta al segundo requerimiento.

Sin embargo, en la primera petición el member code y password enviados son correctos, por lo tanto los servicios solicitados respondieron correctamente.

4. Solicitud y Respuesta fallida.

```
<bc-request-envelope version="1.0">
      <credentials member="ZZ58002355" password="T7TQT7TQ" />
              <service name="changePassword">
                    <param name="old-password" value="T7TQT7TQ" />
                    <param name="new-password" value="qMYb5fYC" />
             </service>
</bc-request-envelope>
```

```
<?xml version="1.0" encoding="UTF-16" standalone="yes"?>
<bc-response-envelope operation="FAILURE" version="1.0">
    <failure-msg>tag name "credentials" is not allowed. Possible tag names are:
&lt;bc-request&gt;</failure-msg>
</bc-response-envelope>
```

Una vez utilizados los dos nuevos servicios del Esquema de Seguridad, usted podrá aplicar las consultas INTL que desee, considerando los cambios que a continuación se mencionan.

MODIFICACIONES AL FORMATO INTL

La habilitación del Esquema de Seguridad involucra realizar cambios al formato INTL para consultas del Reporte de crédito a través de la conexión CPU. A partir de ahora, las Instituciones que requieran hacer uso de estos servicios, deberán consultar el Formato **INTL11**, para construir correctamente la cadena de datos del Registro de Consulta y Respuesta.

CAMBIOS AL FORMATO EN LA LONGITUD DE LA CONTRASEÑA (PASSWORD).

Para el **Registro de Consulta** del Formato INTL, el **segmento de encabezado** cambia en el número de versión y la longitud en la etiqueta correspondiente a la contraseña de acceso, de 4 a 8 posiciones. Será requerido utilizar el password alfanumérico y codificado de acuerdo a las reglas establecidas por Buró de Crédito.

A continuación se detalla el alcance de la modificación en el segmento de encabezado del registro de consulta INTL.

Registro de Consulta*		INTL v. 10 (actual)	INTL v. 11
Etiqueta del Segmento		INTL	INTL
Versión		10	**11**
Nombre del Segmento		Encabezado	Encabezado
Criterios de Validación		Requerido	Requerido
Longitud Máxima del Segmento		80	**88**
Posición:			
41	**Clave del Usuario**	10	10
51	**Contraseña de Acceso**	4	**8**

* El registro se complementa con los segmentos: AU (Autenticación), PN (Nombre), PA (Dirección), PE (Empleo), PI (Cuenta del Cliente) y ES (Fin).

A continuación un ejemplo del registro de consulta INTL:

```
INTL11                                          001MX0000BC12345678XXXXXXXXIMIMX000000100SP01
0000000PN06PRUEBA0007EJEMPLO0109CONSULTAS0207NOMBRES0306NOMBRE040801011196305 10PUEC6301220602SR
0802MXPA25NICOLAS        SAN        JUAN        NUM        8794 0109DEL         VALLE0213BENITO
JUAREZ0306MEXICO0402DF0505 03100PE30SERVICIOS  ADMINISTRATIVOS  CASA0011NTE  20  25910223SAN
SALVADOR
XOCHIMANCA0312AZCAPOTZALCO0406MEXICO0502DF0605028701401MPI16555555017597XX90PI1655555502028345
XXPI1655555444058344XXPI075544XXXES0500473 0002**
```

En el registro INTL de respuesta retornado por Buró de Crédito únicamente se modificará el número de versión en la posición cinco del segmento de encabezado, que ahora será "**11**".

PREGUNTAS FRECUENTES

A continuación se proporciona una serie de las preguntas más frecuentes surgidas alrededor de los cambios por el nuevo Esquema de Seguridad establecido por Buró de Crédito.

¿Por dónde iniciar la nueva implementación de esquema de seguridad?
Antes de comenzar a modificar código alguno, es importante que la siguiente lista de prerequisitos sea verificada:

- **Conectividad con BC**
  El primer paso que debe seguir antes de comenzar a implementar los cambios involucrados con el nuevo esquema de seguridad es validar la conectividad entre el ambiente de pruebas provisto por BC y la(s) máquina(s) que el cliente utilizará para sus pruebas, dicho ambiente reside en la dirección IP 192.168.253.5 a través del puerto 25000 para el envío de peticiones a través del formato INTL y del 25100 para los servicios satelitales.

  NOTA: En caso de existir algún problema para establecer comunicación con la dirección IP y puertos arriba mencionados, favor de ponerse en contacto con el área de Soporte Técnico de Buró de Crédito al 5449 4978.

- **Envío de prueba**
  El Ambiente de Pruebas dispuesto por BC tiene la facultad de soportar la recepción de peticiones INTL tanto en versión 10 (i.e. versión actual) como en la nueva versión 11 (nuevo esquema de seguridad), por lo que con el fin de validar que la comunicación entre la máquina del cliente y dicho ambiente fluye sin problemas, se recomienda hacer una prueba enviando un INTL (versión 10) tal y como lo hace hoy en día.

- ***Guía de Usuario para Esquema de Seguridad y Servicios Satelitales***
  Es importante que antes de continuar tome un tiempo para entender con claridad la estructura de los mensajes de petición y respuesta de los que se habla en las secciones referentes a los servicios **"changePassword"** y **"getExpirationDate"** provistos por BC.

¿Cómo cambio mi contraseña actual?
Para este paso se requiere hacer uso del servicio satelital **"changePassword"**, el cual es provisto por BC.

Es importante mencionar que para los Usuarios que cuentan con contraseñas de 4 posiciones existe una regla para llevar a cabo el cambio de contraseña por primera vez la cual establece que: **La contraseña actual de cuatro posiciones, debe duplicarse para formar una contraseña de ocho posiciones.** Por ejemplo, asumiendo que la contraseña actual es "4H3S", el valor que debe asignarse tanto al atributo **"password"** dentro del elemento **"<credentials>"** del sobre de petición debe ser "4H3S4H3S". En caso de no considerar dicha regla, usted no podrá obtener la contraseña cifrada de ocho posiciones necesaria para llevar a cabo consultas INTL bajo la versión 11.

A continuación se muestra un ejemplo de un sobre de petición que hace uso del servicio satelital **"changePassword"** por primera vez para la clave de otorgante ZZ995010001 y contraseña actual R9ZT.

```
<?xml version="1.0" encoding="UTF-16"?>
<bc-request-envelope version="1.0">
     <bc-request>
        <credentials member="ZZ99501001" password="R9ZTR9ZT"/>
        <service name="changePassword">
              <param name="old-password" value=" R9ZTR9ZT"  />
              <param name="new-password" value="newPwd4u"  />
        </service>
    </bc-request>
</bc-request-envelope>
```

Como respuesta a la solicitud anterior, el servicio satelital **"changePassword"** regresará la nueva contraseña encriptada como se muestra a continuación:

```
<?xml version="1.0" encoding="UTF-16" standalone="yes"?>
<bc-response-envelope operation="ALL" version="1.0">
      <bc-response member="ZZ99991001">
            <service-response name="changePassword">
                  <status code="0">SUCCESS</status>
                  <result-set>
                    <result key="encrypted-password" value="r59w5H7E" />
                  </result-set>
            </service-response>
      </bc-response>
</bc-response-envelope>
```

Es justamente el valor que retorna este servicio en el parámetro **"encrypted-password"** y no la contraseña en texto plano definida originalmente por el usuario, el que debe:

- **Ser embebido en el INTL de consulta (respetando minúsculas y mayúsculas) para la obtención de Reportes de Crédito.**

  Antes

```
INTL10          07008330003666001MX0000ZZ99501001 4H3SICC          SP01
000000CPN06MICELI0009CARBONELL0206CARLOS0306ARTURO04000510MICC7108030802MXPA15M
ARIO BROWN 4240124TAMULTE DE LAS
BARRANCAS0312VILLAHERMOSA0403TAB0505861500710993351092 4PE16NOPROPORCIONADO0015M
ARIO BROWN 4240412VILLAHERMOSA0503TAB060586150PI046081ES05003370002**
```

  Ahora

```
INTL11          07008330003666001MX0000ZZ99501001r59w5H7EICC          SP01
000000CPN06MICELI0009CARBONELL0206CARLOS0306ARTURO04000510MICC7108030802MXPA15M
ARIO BROWN 4240124TAMULTE DE LAS
BARRANCAS0312VILLAHERMOSA0403TAB0505861500710993351092 4PE16NOPROPORCIONADO0015M
ARIO BROWN 4240412VILLAHERMOSA0503TAB060586150PI046081ES05003410002**
```

- **Ser usado como parte de las credenciales del sobre de petición (elemento `<credentials>`) cada vez que se solicite nuevamente alguno de los servicios satelitales.**

  Suponga que desea volver a cambiar su contraseña, lo único que se requiere es a generar la petición haciendo uso de su contraseña cifrada como se muestra a continuación:

```
<?xml version="1.0" encoding="UTF-16"?>
<bc-request-envelope version="1.0">

     <bc-request>
        <credentials member="ZZ99501001" password="r59w5H7E"/>
        <service name="changePassword">
              <param name="old-password" value="r59w5H7E"  />
              <param name="new-password" value="mysec2pw"  />
        </service>
    </bc-request>
</bc-request-envelope>
```

A continuación la respuesta generada por el servicio satelital **"changePassword"**:

```
<?xml version="1.0" encoding="UTF-16" standalone="yes"?>
<bc-response-envelope operation="ALL" version="1.0">
   <bc-response member="ZZ99501001">
      <service-response name="changePassword">
         <status code="0">SUCCESS</status>
         <result-set>
           <result key="encrypted-password" value="f1zM953D" />
         </result-set>
       </service-response>
   </bc-response>
</bc-response-envelope>
```

Suponga ahora que en una subsecuente petición se **quiere obtener la próxima fecha de expiración** para la clave de otorgante ZZ99501001. La solicitud de servicio debe construirse de la siguiente manera:

```
<?xml version="1.0" encoding="UTF-16"?>
<bc-request-envelope version="1.0">
     <bc-request>
        <credentials member="ZZ99501001" password="f1zM953D"/>
        <service name="getExpirationDate" />
    </bc-request>
</bc-request-envelope>
```

¿Cómo invocar el servicio de "getExpirationDate"?
El servicio **getExpirationDate** no recibe ningún parámetro de entrada, por lo que asumiendo que la clave de otorgante es ZZ99501001 y la contraseña encriptada es **f)zM;+3D**, el sobre se formaría de la siguiente manera:

```
<?xml version="1.0" encoding="UTF-16"?>
<bc-request-envelope version="1.0">
     <bc-request>
        <credentials member="ZZ99501001" password="r79w1H4E"/>
        <service name="getExpirationDate" />
    </bc-request>
</bc-request-envelope>
```

El servicio de **"getExpirationDate"** retorna la fecha en que la contraseña actual expirará. A continuación un ejemplo de la respuesta generada por este servicio.

```
<?xml version="1.0" encoding=" UTF-16" standalone="yes"?>
<bc-response-envelope operation="ALL" version="1.0">
   <bc-response member="ZZ99501001">
      <service-response name="getExpirationDate">
         <status code="0">SUCCESS</status>
          <result-set>
             <result key="expiration-date" value="15/09/2005" />
          </result-set>
      </service-response>
   </bc-response>
</bc-response-envelope>
```

¿Cómo hago una consulta de Reporte de Crédito bajo la nueva versión de INTL11?
Antes de que se intente enviar una consulta bajo la nueva versión de INTL 11, se deberá hacer uso del servicio **"changePassword"**

Actualmente la petición bajo el formato INTL versión 10 se ejecutaría de la siguiente manera:

```
INTL10          07008330003666001MX0000ZZ99501001 4H3S ICC          SP01
000000CPN06MICELI0009CARBONELL0206CARLOS0306ARTURO04000510MICC7108030802MXPA15MA
RIO BROWN 4240124TAMULTE DE LAS
BARRANCAS0312VILLAHERMOSA0403TAB0505861500710993351092 4PE16NOPROPORCIONADO0015MA
RIO BROWN 4240412VILLAHERMOSA0503TAB060586150PI046081ES05003370002**
```

Nótese que la versión del INTL es **10** y que la contraseña es de tan solo 4 posiciones.

El nuevo esquema de seguridad requiere que la versión de INTL sea declarada como **11** y la contraseña sea encriptada a través del servicio satelital **"changePassword"** el cual retorna contraseñas con una **longitud de ocho posiciones**.

Suponiendo que el servicio de **"changePassword"** invocado para el member code ZZ99501001 regresa el valor **r|9w;H*E**, la petición con el formato INTL versión 11 sería construida de la siguiente manera:

```
INTL11          07008330003666001MX0000ZZ99501001 r79w1H4E ICC          SP01
000000CPN06MICELI0009CARBONELL0206CARLOS0306ARTURO04000510MICC7108030802MXPA15MA
RIO BROWN 4240124TAMULTE DE LAS
BARRANCAS0312VILLAHERMOSA0403TAB0505861500710993351092 4PE16NOPROPORCIONADO0015MA
RIO BROWN 4240412VILLAHERMOSA0503TAB060586150PI046081ES05003410002**
```

¿Qué caracteres puedo usar para el cambio de mi contraseña?
Cuando el cliente realiza el cambio de contraseña a través del servicio **"changePassword"**, los únicos caracteres válidos que pueden ser utilizados en el atributo `new-password` son letras (mayúsculas o minúsculas) y números del 0 al 9.

¿Qué caracteres puede regresar el servicio "changePassword" en su parámetro de respuesta `encrypted-password`?
Los caracteres que pueden formar parte de la contraseña cifrada retornada por el servicio satelital de changePassword son los siguientes:

a-z	**Letras minúsculas de la 'a' a la 'z'**
A-Z	**Letras mayúsculas de la 'A' a la 'Z'**
0-9	**Números del 0 al 9**

¿Cuál es la dirección IP y puertos disponibles para tener acceso al ambiente de pruebas de Buró de Crédito?
La dirección IP del ambiente de Pruebas provisto por Buró de Crédito es la **192.168.253.5** y los puertos habilitados son el **25000** para consultas de Reporte de Crédito (formato INTL) y el **25100** para acceso a servicios satelitales.

NOTA: En caso de existir algún problema para establecer comunicación con la dirección IP y puertos arriba mencionados, favor de ponerse en contacto con el área de Soporte Técnico de Buró de Crédito al 5449 4978.

¿Cada cuándo debo cambiar mi contraseña para que esta no expire?
Buró de Crédito estableció como parte de su política de seguridad que el cambio de contraseña debe darse en un plazo no mayor a **30 días naturales**, por lo que antes que este período expire usted puede cambiar su contraseña cuantas veces quiera, recordando que **no podrá hacer uso de las últimas 5 contraseñas usadas recientemente**.

¿Requiero solicitar nuevos member codes (claves de otorgante) para realizar mis pruebas en el nuevo ambiente?

No, el ambiente de pruebas cuenta con las mismas claves de otorgante que el Usuario tiene en producción por lo que no es necesario que se soliciten nuevas claves para el ambiente de pruebas.

¿Tienen algún costo hacer uso de los servicios satelitales?

No, los servicios satelitales son gratuitos para nuestros Usuarios.

¿Puedo seguir enviando INTLs versión 10 una vez que Buró de Crédito comience a soportar el envío de INTLs versión 11 en el ambiente productivo?

Con el fin de que nuestros clientes vayan incorporándose a los cambios del nuevo Esquema de Seguridad, Buró de Crédito tiene contemplado seguir brindando soporte al formato INTL 10 durante un periodo determinado, sin embargo es muy importante que nuestros clientes tengan claro que eventualmente se dejará de soportar dicha versión del formato INTL, por lo que deberán tener listas las modificaciones pertinentes en sus sistemas.

CONTACTOS BURÓ DE CRÉDITO

AREA	TELÉFONO
Dirección Comercial	5449 4945
Gerencia de Ventas	5449 4917 5449 4942 5449 4930 5449 4972 5449 4900 ext. 5976 5449 4900 ext. 5914
Dirección Atención al Cliente	5449 4988
Dirección de Sistemas	5449 4973
Centro de Atención a Usuarios	5449 4949
Adquisición de Bases de Datos	5449 4923
Soporte Técnico	5449 4982 soportetecnico@burodecredito.com.mx

Propiedad y Confidencialidad