



## BANCO CENTRAL DEL URUGUAY

Montevideo, 30 de marzo de 2023

### COMUNICACION N°2023/070

**Ref: TODOS LOS MERCADOS - TERCERIZACIÓN DE PROCESAMIENTO DE DATOS EN O DESDE EN EL EXTERIOR - INFORMACIÓN DE UBICACIÓN DEL PUNTO UNIFICADO DE ACCESO.**

Se pone en conocimiento de las instituciones supervisadas que a los efectos de informar el punto unificado de acceso requerido en el artículo 35.3 de la RNRCSF, artículo 16.3 de la RNSR, artículos 58.3, 59.22, 67.3, 76.4, 106.3, 127.19 y 135.3 de la RNMV y artículo 30.1.4 de la RNCFP, deberán ceñirse a las siguientes instrucciones:

El envío se realizará en formato electrónico, a través del Sistema de Envío Centralizado (IDI), utilizando el tipo de dato aperiódico "541-Punto unificado acceso". Se requerirá el envío de un único archivo PDF con el formulario que se adjunta en el Anexo I, el que podrá descargarse en formato WORD en la opción "Descargas" , "Publicaciones" , "Archivos de trabajo" del sistema.

El envío de información deberá incluir la firma electrónica del autorizado a remitir información por parte de la entidad.

Se deberá informar dentro de los cinco días hábiles, tanto desde la fecha de su implementación como ante cualquier cambio que se produzca respecto de la información requerida (dirección, ubicación, responsable).

Las instrucciones para el acceso y uso del Sistema de Envío Centralizado y el aplicativo de firma del BCU pueden accederse en la siguiente dirección: <https://www.bcu.gub.uy/Servicios-Financieros-SSF/Documents/acceso-y-envio-info-ssf.pdf>

**Christian Salvarrey**

Gerente de Gestión Estratégica y Operativa

2022-50-1-02540



## BANCO CENTRAL DEL URUGUAY

## Anexo I

<b>SUPERINTENDENCIA DE SERVICIOS FINANCIEROS</b>			
<i>Comunicación de asignación de Punto Unificado de Acceso</i>			
<b>Institución solicitante</b>			
Razón Social*:		Código institución*:	
Dirección*:			
<b>Punto Unificado de Acceso</b>			
<p><b>El Punto Unificado de Acceso debe:</b></p> <ol style="list-style-type: none"> <li>1. Localizarse en el país, en la Casa Central de la Institución supervisada, o eventualmente en alguna de sus sucursales, pudiéndose cumplir el requisito mediante la asignación (en modalidad no exclusiva) de una o más oficinas, o un piso determinado.</li> <li>2. En caso de necesidad, ser accesible de forma inmediata y contar con espacio de uso exclusivo para su cometido (por ejemplo, una sala de reuniones), permitir el acceso a los funcionarios de la Superintendencia de Servicios Financieros y a todo el personal - propio y eventualmente de terceros - necesario para administración y operación de los servicios incluidos.</li> <li>3. Permitir el acceso y control a todos los servicios de procesamiento de datos, sus respectivos resguardos y las claves necesarias para el acceso y eventual descriptación de la información.</li> <li>4. Estar compuesto por las herramientas tecnológicas necesarias que en conjunto permitan el acceso, gestión continua y el control activo y total de los servicios y datos (hardware y software especializado, portales o consolas de administración, interfaces de líneas de comando, túneles VPN, mapeos de recursos u otros elementos), independientemente de la ubicación donde se realice su gestión operativa y de la naturaleza del servicio provisto.</li> <li>5. Contar con la infraestructura y acceso al personal y servicios (por ejemplo: equipamiento, personal con el conocimiento técnico, conexiones de red, niveles de acceso y servicio) necesarios para cumplir su propósito de forma autónoma, eficiente y eficaz.</li> <li>6. Ser formalmente probado al menos una vez por año. La prueba deberá documentarse y evidenciar el funcionamiento del punto y de cada uno de los accesos.</li> </ol>			
Dirección asignada al Punto Unificado precisando su ubicación (ej. oficina, piso, etc)*:			



## BANCO CENTRAL DEL URUGUAY

<b>Responsable Del Resguardo De Datos, Software Y Documentación</b>	
<p>Las instituciones deberán nombrar un responsable por la ejecución de los procedimientos de resguardo de datos, software y documentación. En particular, será responsable del resguardo de claves para el acceso y descryptación de los datos, así como de asegurar que la institución disponga de un procedimiento para dicho acceso y descryptación que no involucre requerir autorizaciones o acciones de personal que no esté bajo la dependencia de la institución supervisada. Cuando la institución opte por establecer un punto unificado de acceso, también será responsable por la determinación del espacio físico donde se ubicará, su implementación y prueba.</p>	
<p>Nombre del Responsable Del Resguardo De Datos, Software Y Documentación *:</p>	
<b>Observaciones:</b>	
<b>* Campo requerido</b>	
<p><i>Nota: La información del nombre del responsable del resguardo de datos, software y documentación no exime a las instituciones la obligación de reportar la información sobre personal superior en el módulo "Personal Superior" del Sistema de Envío Centralizado (SEC-IDI) de la Superintendencia conforme lo previsto por las Comunicaciones N° 2017/257, N° 2018/185, N° 2018/186, N° 2019/108 y N° 2019/109.</i></p>	