BANCO CENTRAL DEL URUGUAY

Montevideo, 10 de Marzo de 2015

C O M U N I C A C I Ó N N° 2015/034

Ref: **Instituciones Emisoras de Dinero Electrónico - Registro y documentación a presentar en BCU**

A efectos de cumplir con los requisitos establecidos en los artículos 83 y 109 del Libro VII de la Recopilación de Normas de Sistema de Pagos, la documentación a presentar para iniciar el trámite de autorización como emisor de dinero electrónico deberá observar las pautas que se indican a continuación.

Literal i: Copia certificada por escribano público de los estatutos de la entidad. En dichos estatutos deberá establecerse que el objeto social será la realización de actividades relacionadas con dinero electrónico, de acuerdo con los artículos 82 y 108 del Libro VII, y que las acciones serán nominativas en caso de tratarse de una Sociedad Anónima. En caso de encontrarse en trámite, deberán presentar un certificado del trámite iniciado ante la Auditoria Interna de la Nación.

Literal iv. La descripción de la estructura organizativa y dotación de personal prevista debe incluir el organigrama y la descripción de funciones (responsabilidades) asignadas a cada área, además de la dotación prevista al inicio y para los siguientes 3 años a los efectos de evaluar el plan de negocios.

Literal v.: La información que refiere a la descripción de la infraestructura tecnológica a utilizar por la Institución Emisora de Dinero Electrónico (en adelante, IEDE) debe presentarse en forma consolidada, incluyendo los sistemas propios así como los de las distintas empresas con las que se contrate la ejecución de procesos del negocio.

Dicha descripción deberá incluir:

- Diagrama de red, detallando segmentación de la red interna y principales componentes, así como las comunicaciones con redes externas.
- Equipo de soporte a las operaciones, ya sean servidores (físicos y virtuales), equipos de respaldo, etc.
- Dimensionamiento de la solución: cantidad de clientes y transacciones esperadas, pruebas de carga y de stress
- Mapa de aplicaciones propias y de terceros

- Arquitectura de TI

Literal vi.: La actividad de emisión de dinero electrónico tiene asociada riesgos que la institución asume. La evaluación de la capacidad para gestionar los riesgos que asume en forma prudente y rentable, se considera un factor clave para la autorización. En este sentido, la institución deberá implementar un sistema de gestión integral de riesgos, definido como el conjunto de políticas, procedimientos y mecanismos de control implementados para propiciar una adecuada identificación, medición, control y monitoreo de los riesgos a los que se encuentra expuesta.

Es responsabilidad del Directorio u organismo de decisión similar, aprobar la estrategia y las políticas significativas para los riesgos establecidos y revisarlas periódicamente. La estrategia debe reflejar la tolerancia al riesgo y el nivel de rentabilidad que espera obtener en el contexto de los distintos riesgos del negocio. Asimismo es responsable por promover una cultura interna de control y gestión de los riesgos, revisando periódicamente la efectividad de dicha gestión.

Es responsabilidad de la alta gerencia, implementar la estrategia y las políticas aprobadas por la Dirección y desarrollar los procedimientos para su identificación medición, monitoreo y control.

Se requerirá la evaluación de los riesgos inherentes al modelo de negocio de la institución y los mecanismos diseñados para gestionarlos. Para ello se presentará una matriz de riesgos que incluya los riesgos que identificados, el impacto y probabilidad de ocurrencia asignada, así como las medidas adoptadas para mitigarlos en cada caso y el personal a cargo de implementarlas.

Los principales riesgos considerados en este tipo de negocio son: Riesgo operativo, Riesgo de liquidez, Riesgo Tecnológico, Riesgo de fraude, Riesgo de reputación y Riesgo legal.

Para la presentación de la documentación se sugiere considerar como documentos de referencia, los manuales “Buenas prácticas para la gestión y supervisión del riesgo operativo” y “Principios para la adecuada gestión y supervisión del riesgo de liquidez” publicado por el Banco Internacional de Pagos (B.I.S), adecuándolos a la naturaleza, tamaño y complejidad de las actividades de la IEDE, así como a su perfil de riesgo.

Literal vii.: Las instituciones deberán disponer de Políticas de Seguridad de la Información y de Seguridad Física, debidamente definidas. Se deberá tomar como guía el estándar PCI DSS equiparando los elementos asociados al dinero electrónico con el concepto de tarjeta de crédito, a efectos de aplicar los requerimientos de seguridad de la información. Todas las vulnerabilidades y amenazas potenciales deben ser investigadas, evaluadas y documentadas, además de contar con un plan de mitigación.. Asimismo deberán disponer

de un Plan de Continuidad del Negocio, que incorpore el uso de un sitio secundario para desarrollar la actividad, garantizando que los sistemas críticos de tecnologías informáticas puedan retomar las actividades en un plazo razonable para no afectar la confianza de los usuarios en el instrumento. Dicho Plan de Recuperación de Desastres (DRP) y el Plan de Restablecimiento del Servicio, deberá indicar la localización del Data Center de Contingencia y del sitio de Contingencia Operativa. Para su elaboración se consideran documentos de referencia: la Norma UNIT-ISO/IEC 27002:2013, UNIT ISO/IEC 27031:2011, PU UNIT 22301:2012, BS 25999-2:2007, COBIT 5 y el documento denominado "High-Level Principles for Business Continuity", publicado en agosto del 2006 por el BIS (Bank for Internacional Settlements), adaptados a la naturaleza, tamaño y complejidad de las actividades de la IEDE, así como a su perfil de riesgo.

Se sugiere la revisión del documento Marco de divulgación y Metodología de evaluación – Banco de Pagos internacionales, Diciembre de 2012, que se utilizará a los efectos de la evaluación, exigiéndose únicamente la adopción de aquellas medidas que resulten adecuadas al volumen y tipo de operaciones realizadas para una Institución Emisora de Dinero Electrónico.

Entre otras cosas, se espera que las instituciones presenten la siguiente información:

- Mapa de procesos de la IEDE.
- Identificación de los procesos críticos del mapa presentado.
- Contingencias respecto a los procesos críticos.
- Mapa de aplicaciones que den soporte tecnológico a los procesos.
- Identificación de las aplicaciones críticas (todas aquellas aplicaciones que den soporte a los procesos críticos).
- Mapa de arquitectura de TI incluyendo servidores, equipos y líneas de comunicación – Indicando entre otras cosas la redundancia de las líneas de comunicación críticas.
- Identificación de hardware crítico
- Detalle del data center principal y del de contingencia – direcciones de ambos data centers, características de seguridad, equipamiento que existirá en el mismo, líneas de comunicación entre el data center principal y el de contingencia.
- Detalle del sitio de contingencia operativa – dirección, características, equipamiento con el que se va a contar, líneas de comunicación con el data center principal y el de contingencia, posibilidad de atención al público, justificación de ejecución de todos los procesos críticos.
- Estructura organizacional y roles del equipo de atención a desastres (DRT) junto al plan de comunicación ante eventos.
- Plan de recuperación de servicios informáticos – DRP de alto nivel indicando los tiempos de recuperación máximos para los procesos críticos.
- Plan de pruebas de continuidad de negocio con una frecuencia mínima de 1 vez al año.

- Plan de respaldos y recuperación de datos
- Plan de pruebas de seguridad de la información – Hackeos éticos, test de penetración.

Literal viii: La institución deberá presentar el Plan de Negocios y las proyecciones financieras para un período mínimo de tres años, acompañada de la documentación y evidencias que respaldan la elaboración de los planes (fuentes de información, justificación de supuestos, criterios utilizados, entre otros).

Se evaluará que el diseño de la operativa satisfaga razonablemente las necesidades de los usuarios así como la del sector en el que se desarrolla la actividad, en particular en relación a su estructura operativa, tipo de producto y servicio ofrecido, uso de tecnologías y procedimientos aplicados para la administración de los fondos, así como de su esquema de compensación y liquidación.

Literal ix: La información sobre la red de extracción está referida a los puntos en los cuales se puede efectuar operaciones de conversión y de reconversión. Se requiere adjuntar el contrato entre la IEDE y la red de extracción, cuando ésta haya sido subcontratada.

Literal x: Las instituciones deberán presentar todos los contratos en que se apoya la actividad. Se incluye el contrato con los usuarios, así como los contratos firmados con cada uno de los proveedores de servicios que realizan uno o varios procesos del negocio. En caso de no existir contratos firmados, se aceptará a los efectos de la evaluación la presentación del Modelo del contrato a firmar, y que la copia debidamente firmada sea presentada ante el BCU antes del inicio de las actividades.

Cuando la actividad tercerizada sea el procesamiento y/o autorización de las transacciones, las entidades deberán presentar la siguiente información:

- Descripción del tipo y alcance del procesamiento y de la información. Deberá incluirse el Acuerdo de Nivel de Servicio con los proveedores (SLA)
- Datos completos acerca del proveedor seleccionado, incluyendo su localización.
- Alcance de la tercerización.
- Localización del procesamiento, mantenimiento y de los respaldos, y planes de contingencia previstos en caso que se produzcan fallas en la comunicación, almacenamiento o procesamiento de datos.
- Si el procesamiento externo de la información se realiza en el extranjero, el contrato deberá consignar que la IEDE recibirá del proveedor, como parte del proceso de reanudación de actividades y del plan de contingencias, una copia con los resultados de las pruebas de simulación llevadas a cabo en relación con el recupero de información en caso de desastre informático o, en su defecto, un informe que confirme que las pruebas de simulación se completaron con éxito.
- Compromisos de confidencialidad.

- Nota firmada por la institución proveedora del servicio, en la que se acepte que el Banco Central del Uruguay tenga acceso total a los datos y documentación técnica relacionada y a la realización de auditorias periódicas en las instalaciones del proveedor, a efectos de evaluar los riesgos y verificar el cumplimiento de todos los aspectos contemplados en la normativa.
- Nota de aceptación de que los costos en que incurra el Banco Central del Uruguay por los traslados al exterior serán de cargo de la institución solicitante, y autorización para que la cancelación de las obligaciones resultantes de la liquidación de tales costos sea realizada a través de la cuenta corriente de éste en el Banco Central. Los costos estarán determinados sobre la base del régimen de viáticos y gastos de misiones al exterior de funcionarios del Banco Central del Uruguay, los que serán comunicados a la institución previo al traslado al exterior.
- Las instituciones emisoras de dinero electrónico deberán contar con políticas y procedimientos establecidos por escrito y la organización funcional necesarios que aseguren una efectiva identificación, medición, control y monitoreo de los riesgos –tanto presentes como futuros- asociados a los acuerdos de tercerización relativos al procesamiento externo de la información, sea en el país o en el exterior.

Literal xi: El procedimiento de registro de las transacciones refiere a la contabilización de las transacciones y los controles contables previstos de acuerdo a la normativa. El procedimiento financiero contable debe integrar el mapa de procesos solicitado en el literal v.

Asimismo, en lo que respecta los riesgos asumidos en materia de protección de datos de los usuarios, deberán presentar las medidas adoptadas o a adoptar tendientes a asegurar que la información se mantendrá con la reserva requerida por la legislación uruguaya.

Si la entidad a la que se contraten los servicios es extranjera, deberán prestar particular atención a los requerimientos legales y regulatorios existentes en la jurisdicción anfitriona así como a las potenciales condiciones políticas, económicas y sociales u otros eventos que puedan conspirar contra la habilidad del proveedor de cumplir satisfactoriamente con las obligaciones acordadas. La institución que solicita la autorización deberá proveer un informe jurídico detallando con las circunstancias en las que el ordenamiento jurídico de la jurisdicción de la entidad tercerizada habilita la revelación a terceros de la información procesada, sin el consentimiento expreso de la institución uruguaya. En el mismo se deberá hacer expresa referencia al marco legal aplicable y a los antecedentes jurisprudenciales y administrativos sobre relevamiento de secreto que pudiese existir en el Estado de radicación de la información.

Literal xiii: El Manual de Prevención de Lavado de Activos y Financiación del Terrorismo a presentar deberá incluir:

- Proceso para la prevención del Lavado de Activos y de la Financiación del Terrorismo, en sus diferentes etapas, al igual que las diferencias entre ambos.
- Marco regulatorio, Código de Conducta y estructura organizativa responsable de esta temática.
- Normas y procedimientos relativos al conocimiento del cliente (KYC).
- Políticas relativas a transacciones con el dinero electrónico: recargas, pagos, compras, retiros de efectivo.
- Funciones y responsabilidades del Oficial de Cumplimiento y del Directorio de la entidad.
- Reporte de actividades sospechosas.
- Políticas relativas a los empleados y régimen sancionatorio al personal.
- Políticas de archivo y conservación de la documentación.
- Revisión independiente del programa de prevención.

Se dará inicio al trámite de autorización cuando toda la documentación requerida haya sido presentada de acuerdo a las pautas que se establecen, indicando el tipo de dinero electrónico a emitir. Sin perjuicio del análisis documental, el proceso de autorización podrá requerir instancias presenciales de evaluación, a los efectos de la demostración del producto y/o explicación de los principales procesos, el funcionamiento y las particularidades del sistema, pudiendo incluirse una evaluación "in situ" para verificar el cumplimiento de políticas, relevar procedimientos y contar con una visión de los riesgos que asumen las instituciones.

Todos los documentos presentados a los efectos la solicitud de autorización, deberán estar acompañados de una copia en formato digital.

Las Instituciones interesadas en iniciar el trámite de autorización para emitir dinero electrónico, deberán proceder a su registro previo ante el Banco Central del Uruguay (Unidad de Gestión Documental), siguiendo las instrucciones establecidas en la página Web (http: //www.bcu.gub.uy/Acerca-de-BCU/Paginas/Default.aspx), en el enlace "Requisitos para el Registro de Firmas".

Cr. Jorge Xavier

Gerente Área de Sistema de Pagos