BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

COMUNICACIÓN "A" **8401**	**13/02/2026**

A LAS ENTIDADES FINANCIERAS,
A LAS CÁMARAS ELECTRÓNICAS DE COMPENSACIÓN,
A LAS REDES DE CAJEROS AUTOMÁTICOS,
A LOS PROVEEDORES DE SERVICIOS DE PAGO,
A LAS INFRAESTRUCTURAS DEL MERCADO FINANCIERO:

Ref.: Circular
RUNOR 1-1947,
CREFI 2-143:

Requisitos Mínimos para la Gestión y Control de los Riesgos de Tecnología y Seguridad de la Información. Expansión de Entidades Financieras. Actualización.

Nos dirigimos a Uds. para hacerles llegar en anexo las hojas que, en reemplazo de las oportunamente provistas, corresponde incorporar en los textos ordenados sobre Requisitos Mínimos para la Gestión y Control de los Riesgos de Tecnología y Seguridad de la Información y sobre Expansión de Entidades Financieras en función de las disposiciones divulgadas por la Comunicación A 8398.

Se recuerda que en la página de esta Institución www.bcra.gob.ar, accediendo a "Secciones - Sistema Financiero – MARCO LEGAL Y NORMATIVO – Ordenamientos y resúmenes – Textos ordenados de normativa general", se encontrarán las modificaciones realizadas con textos resaltados en caracteres especiales (tachado y negrita).

Saludamos a Uds. atentamente.

BANCO CENTRAL DE LA REPUBLICA ARGENTINA

Pablo D. Montero
Gerente de Emisión
de Normas a/c

Darío C. Stefanelli
Gerente Principal de Emisión y
Aplicaciones Normativas

ANEXO

-Índice-

1.1. Sujetos obligados

1.1.1. Entidades financieras.

1.1.2. Infraestructuras del Mercado Financiero conocidas como Sistemas de Pago de importancia sistémica: INTERBANKING, COELSA, LINK y NEWPAY.

1.1.3. Proveedores de servicios de pago (PSP) incluidos en el Registro de PSP del Banco Central de la República Argentina (BCRA).

1.2. Aspectos generales

Los sujetos obligados indicados en el punto 1.1., que a los efectos de esta norma denominaremos “entidades”, deberán asegurar la implementación de prácticas efectivas para el control interno y la gestión de riesgos de su entorno operativo de tecnología y seguridad de la información. Para ello, deberán demostrar comprensión de los riesgos y establecer un marco para su gestión acorde a la complejidad de los servicios financieros ofrecidos y de la tecnología que los soporta.

Las secciones siguientes establecen un conjunto de requisitos mínimos, aplicables a los procesos, estructuras y activos de información, que las entidades deberán implementar con el propósito de:

- Definir e implementar un marco de gestión de riesgos de la tecnología y la seguridad de la información como parte de la gestión integral de riesgos de la entidad.
- Definir marcos para el gobierno y la gestión de la tecnología y seguridad de la información, acordes con la gestión del riesgo.
- Alinearse con los objetivos de resiliencia operacional.
- Incluir procesos de mejora continua en los marcos de gestión.

Adicionalmente las entidades deberán promover:

- Una cultura de gestión de riesgos de tecnología y seguridad de la información que les permita identificar e implementar controles adicionales a estos requisitos mínimos.
- La adopción del “modelo de las tres líneas” en la definición de roles y responsabilidades.
- La adopción de marcos de referencia y estándares internacionales que permitan complementar los requisitos mínimos relacionados con riesgos, tecnología y seguridad de la información.

Las entidades podrán tercerizar procesos, servicios y/o actividades vinculados con los procesos de tecnología y seguridad de la información, dentro del país como en el exterior.

No se encuentran alcanzados por los requisitos de esta sección:

- Los servicios que brindan información de manera general sobre los mercados financieros.
- Los servicios de adopción obligatoria por regulación del sistema financiero.
- Los servicios brindados por organismos del Estado.
- Las actividades de corresponsalía bancaria.
- Los servicios de procesamiento de pago con tarjetas de crédito.

No se podrán tercerizar procesos, servicios y/o actividades en terceras partes que realicen funciones de auditoría interna y/o externa.

Las entidades que tercericen procesos, servicios y/o actividades vinculados a la tecnología y seguridad de la información no estarán liberadas de sus responsabilidades, presentes o futuras, que les correspondan conforme a las disposiciones legales y reglamentarias y a las normas dictadas por el BCRA.

En función de sus operaciones, procesos y estructura, las entidades deberán considerar el establecimiento de un sector o una función responsable de la gestión de la relación con las terceras partes.

La contratación o tercerización deberá contener disposiciones que aseguren que los procesos, servicios y actividades tercerizados cumplan con los requisitos exigidos en estas normas, de acuerdo con su evaluación de riesgos. La evaluación de los riesgos de todos los prestadores de servicio deberá estar documentada y aprobada por las máximas autoridades locales de la entidad.

10.1. Exigencia de notificación previa.

Las entidades deberán informar a la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias (SEFYC) las características de los servicios críticos a tercerizar**,** con una antelación no inferior a 60 días corridos del inicio de la tercerización.

La notificación previa de los servicios críticos a tercerizar deberá contener:

- La naturaleza de los servicios, conforme a la siguiente taxonomía:

  - Procesamiento de datos en infraestructuras tradicionales.
  - Infraestructura y procesamiento en modalidad *Infrastructure as a Service* (IaaS).
  - Soluciones en modalidad *Platform as a Service* (PaaS).
  - Soluciones en modalidad *Software as a Service* (SaaS).
  - Administración y gestión de datos.
  - Control de acceso a la infraestructura, a los sistemas y a los datos.
  - Operaciones de seguridad (incluye SOC).
  - Gestión de ciberincidentes (en cualquiera de sus etapas).

- Actividades de *back-office* con soporte tecnológico.
- Administración de pagos.
- Gestión de las comunicaciones y redes.
- Desarrollo, soporte y mantenimiento.
- Gestión de copias de respaldo.
- Otros servicios considerados críticos.

- Una descripción de los servicios y actividades alcanzados.

- Las ubicaciones geográficas (país, región, ciudad) donde se desarrollarán cada una de las actividades.

- Las ubicaciones geográficas (país, región, ciudad) donde se realizarán las tareas de control sobre las actividades.

- La fecha de puesta en funcionamiento de las actividades.

- Los datos del responsable de contacto directo en el tercero prestador de servicios (nombre, función, teléfono y correo electrónico).

- Cuando la actividad contemple subcontrataciones (“n-ésimas partes”), deberá identificarse cada uno de los prestadores, la actividad que realizará y las ubicaciones geográficas.

- Los instrumentos que formalicen la tercerización.

- Un plan de continuidad operativa que cumpla con los requisitos normativos vigentes.

- Contar con soluciones de continuidad alternativas conforme a lo previsto en las Secciones 3. y 6.

- En el caso de tercerización de servicios intra-grupo en el exterior, se deberá contar con una certificación escrita del ente supervisor del país de origen que indique que:

  - Se encuentra en conocimiento y no objeta la tercerización.
  - Los servicios tercerizados formarán parte de su programa normal de supervisión.
  - Se encuentra sujeta a principios, estándares o normas prevención del Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM) internacionalmente aceptados, entre otros los difundidos por el Grupo de Acción Financiera Internacional (FATF-GAFI) y el Comité de Supervisión Bancaria de Basilea.
  - Además, respecto de la forma de supervisión, que adhiere a los “Principios básicos para una supervisión bancaria eficaz”, divulgados por el Comité de Supervisión Bancaria de Basilea. Y también aplica supervisión consolidada asumiendo la vigilancia de la liquidez y solvencia, así como la evaluación y el control de los riesgos y situaciones patrimoniales considerados en forma consolidada.

10.2. Marco de gestión de la relación con terceras partes.

Las entidades deberán establecer una política y un marco para la gestión de procesos, servicios y/o actividades tercerizados que considere:

- La definición de roles y responsabilidades para las distintas actividades de la gestión.
- Las medidas de seguridad de acuerdo con los resultados de la gestión de riesgos de tecnología y seguridad; y los riesgos propios de la tercerización.
- Procedimientos para la selección y contratación de terceras partes.
- La identificación y documentación de los servicios y actividades tercerizados.
- La identificación de los puntos de contacto para los aspectos legales y los relacionados con tecnología, seguridad de la información y gestión de ciberincidentes.
- La elaboración y mantenimiento de un catálogo con la información de los servicios y actividades tercerizados.
- La continuidad de los servicios de acuerdo con los resultados de los análisis de riesgos.
- La evaluación continua del nivel de exposición a los riesgos durante todo el ciclo de vida de la tercerización.
- Mecanismos para la gestión de los conflictos de intereses.
- Mecanismos para la gestión de ciberincidentes.
- La elaboración de procedimientos para la supervisión del cumplimiento de los acuerdos formalizados.
- La implementación de auditorías independientes sobre los servicios y actividades gestionados por terceras partes que permitan evaluar la gestión de riesgos y la alineación con los procesos de tecnología y seguridad de la información de la entidad.

Por otra parte, las entidades deberán evaluar posibles escenarios de finalización planificada o forzada de los procesos, servicios o actividades provistos por terceras partes, y establecer planes de finalización que les permitan mitigar los riesgos de interrupción, incumplimiento de los requisitos legales y regulatorios, o degradación de la calidad. Los planes de finalización deberán considerar la obtención de los datos, los programas fuentes, y la documentación de los sistemas y aplicaciones.

Durante todo el ciclo de vida de la tercerización, cualquier cambio vinculado con la naturaleza de la actividad, la ubicación geográfica donde se realizan las actividades o las tareas de control, así como también la incorporación y/o modificaciones de las subcontrataciones (“n-ésimas partes”), deberá interpretarse como un nuevo proceso de tercerización y deberá cumplir con todos los requisitos contemplados en el punto 10.1.

Los cambios relevantes en la tercerización en el exterior de servicios críticos intra-grupo deberán contar con una nueva certificación escrita del supervisor del país de origen prevista en el punto 10.1.

10.3. Formalización de la relación.

10.3.1. Las entidades deberán formalizar en todos los casos las relaciones con terceras partes que brinden procesos, servicios y/o actividades tercerizados de acuerdo con los procedimientos establecidos. Se deberán fijar como mínimo:

- La naturaleza, el alcance de los procesos, servicios y/o actividades a tercerizar y las responsabilidades de las partes.
- La duración de la contratación o tercerización y cláusulas específicas que regulen la renovación automática.
- Los niveles mínimos de prestación y métricas de desempeño.
- La existencia de planes de continuidad.
- Los derechos a realizar auditorías por parte de la entidad.
- Los mecanismos de comunicación sobre los cambios que puedan afectar las condiciones en la prestación del servicio.
- Los acuerdos sobre confidencialidad.
- Los mecanismos para la resolución de disputas.
- Los procedimientos coordinados para la gestión de ciberincidentes.
- El cumplimiento del marco legal y regulatorio aplicables.
- Disposiciones que permitan a la entidad y a la SEFYC, en todos sus niveles de contratación, a requerir información precisa, completa y oportuna relacionada con los servicios tercerizados cuando lo estimen conveniente y el acceso irrestricto para auditar y obtener información relevante en las instalaciones, áreas de control y documentación sobre todos los prestadores de servicios.
- Los mecanismos de notificación sobre cambios en el control accionario y en los cambios de niveles gerenciales de las terceras partes.
- Las responsabilidades en los circuitos de reclamos de clientes o usuarios de servicios financieros de la entidad.
- Procedimientos y protocolos de comunicación que permitan el cumplimiento efectivo de los controles sobre los procesos, servicios y actividades tercerizados.
- La designación formal de un responsable en representación de la tercera parte para el tratamiento de aspectos vinculados con la tercerización, de acuerdo con las características del servicio y los resultados de los análisis de riesgo.
- Los mecanismos para la eliminación de los datos de la entidad gestionados por terceras partes, una vez extinguida la relación.
- Los procedimientos para la finalización de los servicios de acuerdo con la evaluación de riesgos.

Los servicios de mensajería financiera serán evaluados teniendo en cuenta sus condiciones particulares de contratación como por ejemplo SWIFT.

10.3.2. Subcontrataciones de las terceras partes.

Los documentos que instrumenten la contratación o tercerización deberán establecer formalmente la responsabilidad del prestador primario respecto de:

- Todos los procesos, servicios y/o actividades prestados por sí mismo o por medio de subcontratistas, con independencia de la ubicación geográfica.

- La notificación a la entidad de todas las subcontrataciones con la identificación de los servicios y actividades involucrados.

Además, todos los subcontratistas deberán asumir formalmente:

- La responsabilidad de cumplir con el marco legal y regulatorio aplicable.

- La asignación de derechos de acceso y auditoría, tanto para la entidad, como a la SEFYC.

10.4. Control y monitoreo.

Las entidades deberán definir un proceso de control de acuerdo con la evaluación de riesgos que les permita realizar un seguimiento y evaluación de los procesos, servicios y actividades de tecnología y seguridad de la información tercerizados.

Deberán existir procedimientos para la ejecución de controles sobre las terceras partes, la evaluación del cumplimiento de los requisitos regulatorios y los niveles de servicio acordados, y el seguimiento de las solicitudes de adecuación, en caso de incumplimientos.

La periodicidad de las actividades de control y monitoreo deberá definirse de acuerdo con el nivel de riesgo y la criticidad de los procesos, servicios o actividades tercerizados.

10.4.1. Informes de terceros independientes

Los informes de las evaluaciones realizadas por terceros independientes sobre los procesos, servicios y actividades tercerizados serán considerados complementarios a las actividades de control y monitoreo de la entidad, siempre que:

- Estén elaborados de acuerdo con procesos aceptados internacionalmente.

- Los alcances y los resultados permitan verificar los controles implementados.

- Se realicen auditorías o actividades de revisión adicionales cuando el alcance no cubra la totalidad de los requisitos normativos y los riesgos identificados.

10.5. Informes de auditoría interna y externa.

Se deberán realizar auditorías internas sobre los procesos, servicios y actividades tercerizados que incluyan revisiones del cumplimiento de los requisitos legales y regulatorios.

La periodicidad de los informes de auditoría deberá definirse de acuerdo con el nivel de riesgo y la criticidad de los servicios o actividades tercerizados evaluando su impacto en el sistema de control interno de la entidad.

Conjuntamente con los informes de auditoría interna, se deberán remitir a la Gerencia de Auditoría Externa de Sistemas los informes de los auditores externos efectuados con motivo de sus revisiones sobre los servicios y actividades tercerizados.

Deberán encontrarse disponibles para la SEFYC, en todo momento:

- Los informes de los auditores internos y externos corporativos sobre los servicios tercerizados intra-grupo.

- Los informes de auditoría sobre los distintos prestadores de servicios tercerizados extra-grupo.

En todos los casos, la auditoría interna de la entidad local deberá analizar los informes de las auditorias recibidos y evaluar la razonabilidad, consistencia e integridad respecto del cumplimiento de las normativas locales vigentes para determinar, en todo momento, el mantenimiento de las condiciones iniciales tenidas en cuenta al contratar dichos servicios.

10.6. Consideraciones adicionales.

10.6.1. Los gastos en que incurra la SEFYC para realizar las inspecciones de la actividad tercerizada en el exterior del país (pasajes, alojamiento, viáticos, traslados, otros) deberán ser cubiertos en su totalidad por la entidad.

10.6.2. La tercera parte del exterior en la que se tercerice deberá estar constituida en países que estén sujetos a principios, estándares o normas sobre prevención del Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM) internacionalmente aceptados, entre otros los difundidos por el Grupo de Acción Financiera Internacional (FATF-GAFI).

Seguridad de la información: la preservación de la integridad, disponibilidad y confidencialidad de la información. Además, podría incluir la autenticidad, la trazabilidad, la rendición de cuentas, el no repudio y la confiabilidad.

Servicios críticos: aquellos que resulten esenciales para el funcionamiento continuo del sistema financiero y de la entidad, y para el cumplimiento de las obligaciones legales y regulatorias.

***Shadow IT*:** se refiere a *software*, *hardware*, servicios y dispositivos no autorizados por la organización que operan en el entorno de TI.

Subcontratación: práctica en virtud de la cual una tercera parte encarga a un subcontratista (n-ésima parte) parte de lo que se le ha encomendado.

Tercera parte: quien brinda procesos, servicios y/o actividades tercerizados por la entidad.

Tolerancia al riesgo: nivel aceptable de variación respecto del apetito de riesgo definido en el logro de los objetivos de la entidad.

Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas.

A partir del 04/08/26, los Proveedores de servicios de pago (PSP) incluidos en el Registro de PSP del Banco Central de la República Argentina deberán implementar esta normativa.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

B.C.R.A.	ORIGEN DE LAS DISPOSICIONES CONTENIDAS EN EL TEXTO ORDENADO SOBRE REQUISITOS MÍNIMOS PARA LA GESTIÓN Y CONTROL DE LOS RIESGOS DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

TEXTO ORDENADO			NORMA DE ORIGEN				OBSERVACIONES
Sección	Punto	Párrafo	Com.	Cap.	Punto	Párrafo	
1.	1.1.		“A” 7724		2.		Según Com. “A” 7783 y 8398.
	1.2.		“A” 7724		2.		
2.	2.1.		“A” 7724		2.		
	2.2.		“A” 7724		2.		
	2.3.		“A” 7724		2.		
3.			“A” 7724		2.		
4.	4.1.		“A” 7724		2.		
	4.2.		“A” 7724		2.		
	4.3.		“A” 7724		2.		
	4.4		“A” 7724		2.		
	4.5.		“A” 7724		2.		
	4.6.		“A” 7724		2.		
	4.7.		“A” 7724		2.		
5.	5.1.		“A” 7724		2.		
	5.2.		“A” 7724		2.		
	5.3.		“A” 7724		2.		
	5.4.		“A” 7724		2.		
	5.5.		“A” 7724		2.		
	5.6.		“A” 7724		2.		
	5.7.		“A” 7724		2.		
	5.8.		“A” 7724		2.		
6.	6.1.		“A” 7724		2.		
	6.2.		“A” 7724		2.		
	6.3.		“A” 7724		2.		
	6.4.		“A” 7724		2.		
	6.5.		“A” 7724		2.		
	6.6.		“A” 7724		2.		
	6.7.		“A” 7724		2.		
	6.8.		“A” 7724		2.		
7.	7.1.		“A” 7724		2.		
	7.2.		“A” 7724		2.		
	7.3.		“A” 7724		2.		
	7.4.		“A” 7724		2.		
	7.5.		“A” 7724		2.		
	7.6.		“A” 7724		2.		
	7.7.		“A” 7724		2.		
8.	8.1.		“A” 7724		2.		
	8.2.		“A” 7724		2.		
	8.3.		“A” 7724		2.		
9.	9.1.		“A” 7724		2.		
	9.2.		“A” 7724		2.		
10.	10.1.		“A” 8398		3.		
	10.2.		“A” 7724		2.		Según Com. “A” 8398.
	10.3.		“A” 7724		2.		Según Com. “A” 8398.
	10.4.		“A” 7724		2.		Según Com. “A” 8398.
	10.5.		“A” 7724		2.		Según Com. “A” 8398.
	10.6.		“A” 8398		3.		

REQUISITOS MÍNIMOS PARA LA GESTIÓN Y CONTROL DE LOS RIESGOS DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN							
TEXTO ORDENADO			NORMA DE ORIGEN				OBSERVACIONES
Sección	Punto	Párrafo	Com.	Cap.	Punto	Párrafo	
11.			“A” 7724		2.		Según Com. “A” 8398.
12.			“A” 8398		1.		

-Índice-

2.1. Exigencia de comunicación previa.

Las entidades financieras podrán tercerizar –en instalaciones y/o infraestructuras de terceros con recursos técnicos y/o humanos de los terceros– procesos, servicios y/o actividades que no consistan en la atención de clientes y/o público general (administración, servicios vinculados con los procesos de tecnología y seguridad de la información, archivo, imprenta, etc.) previa comunicación cursada a la Superintendencia de Entidades Financieras y Cambiarias (SEFYC) con una antelación no inferior a 60 días corridos a la fecha de inicio de esas actividades.

En los casos de actividades que involucren la atención de sus clientes y público en general aplica lo previsto en la Sección 9.

2.2. Condiciones.

2.2.1. Los procesos, servicios y/o actividades tercerizados estarán sujetos a las regulaciones técnicas correspondientes a su naturaleza y tipo.

2.2.2. Para la tercerización de procesos, servicios y/o actividades vinculados con los procesos de tecnología y seguridad de la información deberá cumplirse lo previsto en los textos ordenados sobre Requisitos Mínimos para la Gestión y Control de los Riesgos de Tecnología y Seguridad de la Información y Requisitos Mínimos para la Gestión y Control de los Riesgos de Tecnología y Seguridad de la Información Asociados a los Servicios Financieros Digitales.

2.2.3. Para el resto de los servicios y/o actividades.

En la comunicación de tercerización se deberá consignar:

2.2.3.1. La naturaleza de cada proceso, servicio y/o actividad comprendida.

2.2.3.2. El domicilio donde se desarrollarán los procesos, servicios y/o actividades.

2.2.3.3. La fecha de comienzo de la tercerización de los procesos, servicios y/o actividades.

2.2.3.4. Adjuntarse copia del contrato.

2.2.3.5. Agregarse las informaciones, compromisos y documentación indicados en los puntos 2.2.1. y 2.2.4., firmados por una persona que acredite facultades suficientes para ello.

La documentación requerida deberá ser enviada a través de la modalidad que la SEFYC establezca en archivo con formato pdf, siendo conservados los originales en la entidad financiera a disposición de la SEFYC. El representante legal de la entidad deberá manifestar mediante nota con carácter de declaración jurada que la totalidad de la documentación remitida por medios electrónicos es copia fiel de la documentación que conserva la entidad y se encuentra a disposición de la SEFYC, detallando el lugar donde se encuentra.

2.2.4. En el contrato de tercerización deberá estar expresamente estipulado lo siguiente:

2.2.4.1. La aceptación y el compromiso de cumplimiento de las condiciones a que se refiere el punto 2.2.1., por todas las partes intervinientes.

2.2.4.2. La facultad de la SEFYC para auditar periódicamente el cumplimiento de dichas condiciones.

2.2.5. De acuerdo con lo establecido en el punto 2.2.4.2., las entidades financieras y los terceros que estas contraten deberán comprometerse a permitir que los agentes que designe la SEFYC puedan acceder a las instalaciones y/o infraestructuras donde se desarrolla el proceso, servicio y/o actividad, cuando ello resulte necesario para cumplir sus funciones de supervisión.

2.2.6. Deberán mantenerse en la República Argentina:

2.2.6.1. Los libros y registros contables originales establecidos por las disposiciones legales vigentes, que permitan tanto a la entidad local como a la SEFYC reconstruir y verificar las operaciones y negocios en cualquier momento.

2.2.6.2. El archivo de la información entregada y los documentos firmados por los clientes, que respalden las operaciones activas y pasivas.

2.2.6.3. Los legajos de los deudores, conforme al TO sobre Gestión Crediticia.

2.2.6.4. Los documentos y garantías que respalden las financiaciones vigentes otorgadas por la entidad o adquiridas, cuando la entidad compradora tenga a su cargo la administración de la cartera, y la documentación original demostrativa de la propiedad de los restantes activos.

2.2.6.5. Todo resguardo de documentación original, cuando normas legales, reglamentarias y/o disposiciones del Banco Central de la República Argentina (BCRA) determinen cursos de acción específicos.

2.3. Responsabilidades.

Las entidades financieras que tercericen procesos, servicios y/o actividades no estarán liberadas de sus responsabilidades, presentes o futuras, que les correspondan conforme a las disposiciones legales y reglamentarias y a las normas dictadas por el BCRA.

EXPANSIÓN DE ENTIDADES FINANCIERAS									
TEXTO ORDENADO			NORMA DE ORIGEN						OBSERVACIONES
Secc.	Punto	Párr.	Com.	Anexo	Cap.	Secc.	Punto	Párr.	
1.	1.7.		"A" 2241		II	5.	5.2. a 5.4.		Según Com. "A" 4382, 4771, 5355, 5983 y 6275.
	1.8.		"A" 2241		II	5.	5.1.		Según Com. "A" 4382, 5983 y 6275.
	1.9.		"A" 5983	único		1.	13.		Según Com. "A" 6275.
2.	2.1.		"A" 3149	I	II	6.	6.1.	1°	Según Com. "A" 5983, 6126, 6354, 7948 y 8398.
	2.2.1.		"A" 3149	I	II	6.	6.1.	3°	Según Com. "A" 6354 y 7948.
	2.2.2.		"A" 6354	I					Según Com. "A" 7948.
	2.2.3.		"A" 3149	I					Según Com. "A" 5983, 6126, 6354, 7948 y 8398.
	2.2.4.		"A" 3149	I	II	6.	6.1.2.	1°	Según Com. "A" 6354 y 8398.
	2.2.5.		"A" 6354	I					Según Com. "A" 7948 y 8398.
	2.2.6.		"A" 3149	I	II	6.	6.1.2.3.		Según Com. "A" 6354.
	2.3.		"A" 3149	I	II	6.	6.2.		Según Com. "A" 7948 y 8398.
3.	3.1.		"A" 3149	I	II	6.	6.3.	1°	Según Com. "A" 5983.
	3.2.		"A" 3149	I	II	6.	6.3.	1°	Según Com. "A" 5983.
	3.3.		"A" 3149	I	II	6.	6.3.	2° y último	Según Com. "A" 5983.
4.	4.		"A" 2241		II	9.			Según Com. "A" 6271.
	4.1.		"A" 2241		II	9.	9.2.		Según Com. "A" 5082 y 5983.
	4.1.1.		"A" 2241		II	9.	9.1.1.		Según Com. "A" 5082.
	4.1.2.		"A" 2241		II	9.	9.1.2.		Según Com. "A" 5082.
	4.2.		"A" 5082				9.2.		Según Com. "A" 5983.
	4.3.		"A" 5082				9.3.		
	4.3.1.		"A" 2241		II	9.	9.2. y 9.3.		Según Com. "A" 2512 y 5082.
	4.3.2.		"A" 2241		II	9.	9.3.2.		Según Com. "A" 5082.
	4.3.3.		"A" 2241		II	9.	9.4.		Según Com. "A" 5082.
	4.3.4.		"A" 5082			9.	9.3.4.		
	4.4.		"A" 5082			9.	9.4.		Según Com. "A" 7948.
	4.5.		"A" 5983	único		2.			
	4.5.1.		"A" 5983	único		2.	2.4.1.		Según Com. "A" 6457 y 6644.