ANEXO 00 - VERIFICACIÓN DE REQUISITOS EXIGIDOS POR LA SUPERINTENDENCIA DE BANCOS - SERVICIOS PROVISTOS POR TERCEROS

ARTÍCULO	REQUERIMIENTO NORMATIVO RESOLUCIÓN SB-2023-01901	APLICA / NO APLICA	CUMPLIMIENTO / JUSTIFICACIÓN	INSTRUCCIONES
23	Para mantener el control de los servicios provistos por terceros, incluidas las empresas de servicios auxiliares del sistema financiero, las entidades controladas deben implementar un proceso integral para la administración de proveedores de servicios que incluya las actividades previas a la contratación, suscripción, cumplimiento y renovación del contrato; para lo cual, deben cumplir, por lo menos, con lo siguiente, pero sin limitarse a:			
23.1	Para las actividades previas a la contratación, las entidades controladas deben establecer e implementar políticas, procesos y procedimientos que aseguren la evaluación, calificación y selección de los proveedores, relacionados con y sin limitarse a:			
23.1.a	a) Evaluación de la experiencia de la empresa y de su personal;	*APLICA*	*Incorporado en las bases del concurso*	**L**as áreas requirentes establecerán como parámetro de calificación en las Bases del Concurso, la experiencia del proveedor de manera obligatoria; y del personal de ser el caso.
23.1.b	b) Evaluación financiera para asegurar la viabilidad de la empresa durante todo el período de contratación previsto;	APLICA	Incorporado en las bases del concurso	**L**as áreas requirentes establecerán como parámetro de calificación en las Bases del Concurso, los índices financieros aplicables a la contratación de manera obligatoria; y el informe de auditoría externa si lo tuvieren.
23.1.c	c) Análisis de informes de auditoría externa, si los tuviere;			
23.1.d	d) Evaluación de la capacidad del servicio, instalación y soporte e historial del desempeño con base en los requisitos de la entidad controlada;	APLICA	Se incorporará en las bases del concurso	**L**as áreas requirentes establecerán en los parámetros de experiencia del proveedor, la capacidad del servicio, instalación y soporte e historal de desempeño, para su calificación, de acuerdo al servicio a ser contratado.
23.1.e	e) Evaluación de la capacidad logística de la empresa, incluyendo la infraestructura física y tecnológica y recursos humanos;			**L**as áreas requirentes establecerán como parámetro de calificación en las Bases del Concurso, la capacidad logística de los participantes, incluyendo la infraestructura física y tecnológica y recursos humanos, de acuerdo al servicio a ser contratado.
23.1.f	f) Análisis del riesgo reputacional de la empresa; y,	NO APLICA	Las Bolsa de Valores del país son los que establecen parámetro de calificación	Las áreas requirentes establecerán el parámetro de calificación en las Bases del Concurso relacionado con el riesgo reputacional de los participantes, de acuerdo al servicio a ser contratado.
23.1.g	g) Gestión de riesgos asociados a los servicios críticos provistos por terceros, que garanticen la gestión de seguridad de la información incluyendo ciberseguridad y la gestión de la continuidad del negocio, en función a la naturaleza del servicio contratado.	NO APLICA	No constituye un servicio crítico para el BIESS	Para garantizar la gestión de riesgos asociados a los servicios críticos provistos por terceros, las áreas requirentes, en función a la naturaleza del servicio a contratar, establecerán como requisitos mínimos en las Bases del Concurso, las condiciones que deberán cumplir los participantes, en gestión de seguridad de la información incluyendo ciberseguridad y la gestión de la continuidad del negocio.
23.2	Establecer políticas, procesos y procedimientos que aseguren la contratación de servicios en función de los requerimientos de la entidad controlada, y garanticen que los contratos incluyan, como mínimo, las siguientes cláusulas:			

23.2.a	a) Niveles mínimos de calidad del servicio acordado.	NO APLICA	No requiere Acuerdo de Nivel de Servicio, debido a que la Bolsa de Valores del país son las que establecen los niveles mínimos	Las áreas requirentes establecerán en las Bases del Concurso, los Acuerdos de Niveles del Servicio, de acuerdo al servicio a ser contratado; que serán incluidos en las cláusulas contractuales.
23.2.b	b) Garantías financieras y técnicas, tales como: buen uso del anticipo, fiel cumplimiento del contrato, buen funcionamiento y disponibilidad del servicio, entre otros.	NO APLICA	No aplica porque, el servicio se constitute en un riesgo bajo, el pago está condicionado a la prestación	Con base al Reglamento para contrataciones de Giro Específico del Negocio del Biess, las áreas requirentes establecerán en las Bases del Concurso, las garantías pertinentes, de acuerdo a la natrualeza y monto de la contratación; que serán incluidas en las cláusulas contractuales.
23.2.c	c) Multas y penalizaciones por incumplimiento.	APLICA	Se incorporará en las bases del concurso	Las áreas requirentes deberán establecer en las Bases del Concurso, las multas y penalizaciones; que serán incluidas en las cláusulas contractuales.
23.2.d	d) Personal suficiente y calificado para brindar el servicio en los niveles acordados.	APLICA	Se incorporará en las bases del concurso	Las áreas requirentes deberán establecer en las Bases del Concurso, en la metodología del trabajo, el personal suficiente y calificado para brindar el servicio en los niveles acordados; que serán incluidos en las cláusulas contractuales.
23.2.e	e) Capacitación, en los casos que aplique, del servicio contratado y entrega de toda la documentación que soporta el proceso o servicio asociado a los procesos críticos.	NO APLICA	Las Bolsa de Valores del país son las encargadas de brindar la capacitación respectiva	Las áreas requirentes, en los casos que aplique, deberán establecer en las Bases del Concurso, la capacitación del servicio contratado y entrega de toda la documentación que soporta el proceso o servicio asociado a los procesos críticos; que será incluido en las cláusulas contractuales.
23.2.f	f) Seguridad de la información incluyendo Ciberseguridad y protección de datos personales sobre la gestión de información usada de la entidad controlada en la provisión del servicio proporcionado por el proveedor.	APLICA	Se incorporará en las bases del concurso	Las áreas requirentes, en los casos que aplique, deberán establecer en las Bases del Concurso, como obligaciones del contratista, la suscripción del "Acuerdo de Confidencialidad y No Divulgación" por parte del representante legal y de todo el personal que prestará el servicio, en el formato establecido por la Dirección de Seguridades de la Información del Biess; que será incluido en las
23.2.g	g) Derechos de propiedad intelectual, cuando aplique.	NO APLICA	El objeto contractual corresponde a la prestación de un servicio que no contempla producto susceptible de protección por derechos de propiedad intelectual	Las áreas requirentes, en los casos que aplique, deberán establecer en las Bases del Concurso, los derechos de propiedad intectual; que será incluido en las cláusulas contractuales.

23.2.h	h) Definición del equipo de contraparte y administrador del contrato tanto de la entidad controlada como del proveedor.	NO APLICA	La prestación será ejecutada directamente por el proveedor designado, bajo los términos y condiciones establecidos, sin que resulte necesario formalizar la designación de un equipo de contraparte o administrador contractual	Las áreas requirentes deberán establecer en las Bases del Concurso, en la metodología del trabajo, el equipo de contraparte para la correcta ejecucion del servicio, así como en obligaciones del contratista, la definición de su equipo de contraparte también; y, en la respectiva clausula contractual se definirá el administrador del contrato.
23.2.j	i) Definición detallada de los productos y servicios a ser entregados por el proveedor.	APLICA	Se incorporará en las bases del concurso	Las áreas requirentes deberán establecer en las Bases del Concurso, los productos y servicios a ser entregados por el proveedor; que serán incluidos en las cláusulas contractuales.
23.2.j	j) Cumplimiento por parte del proveedor de las políticas que establezca la entidad controlada, las cuales deben incluir, al menos, la norma expedida por la Superintendencia de Bancos, aplicable en función del servicio a ser contratado.	NO APLICA	El contrato no implica la ejecución de funciones reguladas por normativa bancaria ni actividades sujetas a supervisión de la	Las áreas requirentes deberán establecer en las Bases del Concurso, como obligaciones del contratista, el cumplimiento de las políticas internas y la norma expedida por la Superintendencia de Bancos, aplicable en función del servicio a ser contratado; que será incluido en las cláusulas contractuales.
23.2.k	k) Facilidades para la revisión y seguimiento del servicio prestado a las entidades controladas, por parte de la unidad de auditoría interna u otra área que estas designen, así como de los auditores externos y la Superintendencia de Bancos, en aquellos procesos definidos como críticos.	NO APLICA	La prestación del servicio no genera riesgos operativos o financieros que requieran seguimiento por parte de la unidad de auditoría interna, auditores externos o la Superintendencia	Para la contratación de servicios que soportan los procesos críticos, las áreas requirentes deberán establecer en las Bases del Concurso, como obligaciones del contratista, prestar las facilidades para la revisión y seguimiento del servicio prestado, por parte de la unidad de auditoría interna u otra área que estas designen, así como de los auditores externos y la Superintendencia de Bancos; que será incluido en las cláusulas contractuales.

23.2.l	l) Informes de auditoría externa sobre el cumplimiento de los aspectos relacionados con la seguridad de la información y continuidad del negocio referidos en la presente norma, practicados por personal o empresas independientes con experiencia acreditada en el ramo emitidos en el último año; o, certificaciones en temas de Seguridad de la Información incluida ciberseguridad y continuidad del negocio, vigentes obtenidas ante certificadoras acreditadas, el alcance de los informes o certificaciones debe ser aplicable al servicio contratado.	NO APLICA	Dado que el servicio no afecta sistemas críticos ni datos sensibles regulados, no resulta pertinente exigir informes de auditoría externa ni certificaciones especializadas en seguridad de la información, ciberseguridad o continuidad del negocio.	Las áreas requirentes, en los casos que aplique, deberán establecer en las Bases del Concurso, como requisitos mínimos de los participantes, la presentación de estos informes o certificaciones, aplicables al servicio contratado, y en obligaciones del contratista, que deberán mantener vigentes estos informes o certificados, durante la vigencia del contrato; que será incluido en las cláusulas contractuales.
23.3	Administrar los riesgos a los que se exponen al contratar servicios provistos por terceros, particularmente de aquellos que soportan los procesos críticos.	NO APLICA	El servicio contratado no forma parte de los procesos críticos de la entidad, por lo que la gestión formal de riesgos asociados a terceros no resulta	Las áreas requirentes identificarán en la Matriz de Riesgo Operativo, los riesgos a los que se exponen al contratar servicios provistos por terceros, particularmente de aquellos que soportan los procesos críticos; e incluirán en las bases del concurso los mitigantes generales, identificados en dicha matriz, y los mitigantes específicos que deberá identificar cada área requirente de acuerdo a la naturaleza del servicio a ser contratado, asociados a los riesgos identificados.
23.4	Establecer políticas, procesos y procedimientos que aseguren el control y monitoreo de los servicios contratados, mediante la evaluación, gestión y vigilancia de éstos, a fin de garantizar que se cumplan en todo momento con los niveles mínimos de servicio acordados y demás cláusulas establecidas en el contrato. La información utilizada para el monitoreo de los servicios contratados debe ser obtenida por la entidad controlada de manera independiente de aquella que proporcione el proveedor, para lo cual podrá utilizar los mecanismos técnicos que considere pertinentes, que le permita confirmar el cumplimiento de las condiciones contractuales.	NO APLICA	La prestación del servicio no genera riesgos operativos, financieros o de cumplimiento que justifiquen la adopción de políticas o procedimientos especializados de monitoreo.	Las áreas requirentes deberán establecer en las Bases del Concurso, metodologia de trabajo, los procedimientos de evaluación, gestión y vigilancia de los servicios a recibir, para asegurar el control y monitoreo de los mismos, a fin de garantizar que se cumpla el SLA y demás cláusulas contractuales; la información utilizada en el monitoreo y control debe ser obtenida por el Biess de manera independiente de aquella que proporcione el proveedor, para lo cual podrá utilizar los mecanismos técnicos que considere pertinentes, que le permita confirmar el cumplimiento de las condiciones técnicas y contractuales; metodología que será incluida en la respectiva cláusula contractual.
23.5	Contar con proveedores alternos de los servicios que soportan a los procesos críticos, que tengan la capacidad de prestar el servicio para mitigar el riesgo de dependencia en un solo proveedor; en los casos de proveedor único, la entidad controlada debe asegurarse de que el proveedor cuenta con planes de contingencia y continuidad de negocio, que han sido probados y se encuentran actualizados, al menos, anualmente y sincronizados con los tiempos definidos por el banco.	NO APLICA	La prestación del servicio no genera riesgo significativo de interrupción de operaciones, por lo que no resulta pertinente implementar	Para la contratación de servicios que soportan los procesos críticos, las áreas requirentes deberán establecer en las Bases del Concurso, como obligaciones del contratista, la prestación de los planes de contingencia y continuidad de negocio, que deberán ser validados y aprobados por las áreas técnicas pertinentes; condición que será incluida en la respectiva cláusula contractual.

23.6	Para el caso de contratación de servicios de infraestructura, plataforma y/o software, en la nube tanto con proveedores nacionales o extranjeros; las entidades controladas deberán disponer conforme el servicio contratado: Un informe técnico, uno de seguridad de la información y uno legal, emitido por el personal de la entidad controlada en función de sus competencias, en los cuales, se haya identificado los riesgos operativos asociados al servicio y la gestión respectiva. Además, de identificar y gestionar los riesgos asociados a estos servicios la entidad debe:	NO APLICA	El servicio se ejecuta mediante procesos convencionales de la entidad, sin depender de infraestructura tecnológica crítica, por lo que no corresponde aplicar los requerimientos propios de servicios en la nube	Las áreas requirentes conjuntamente con la Coordinación de Tecnología determinarán si el objeto contractual contempla computación en la nube (servicios de infraestructura, plataforma y/o software); y al ser una contratación con componente tecnológico, la Coordinación de Tecnología también revisará y suscribirá las bases del concurso conjuntamente con las áreas requirentes. Para el caso de contratación de servicios de infraestructura, plataforma y/o software, en la nube tanto con proveedores nacionales o extranjeros; las áreas requirentes deberán gestionar conforme el servicio contratado: Un informe técnico, uno de seguridad de la información y uno legal, emitido por las unidades competentes, en función de sus competencias, en los cuales, se haya identificado los riesgos operativos asociados al servicio y la gestión respectiva. Además, deberán identificar y gestionar los riesgos asociados a
23.6.a	a) Informar a la Superintendencia de Bancos sobre el detalle de los servicios asociados a los procesos críticos a ser contratados que incluya entre otros: el tipo de servicio contratado, el detalle del servicio alojado, la arquitectura tecnológica contratada, según aplique; el análisis de los riesgos operativos, legales, tecnológicos, de seguridad de la información incluida la ciberseguridad y continuidad de operaciones a los que se exponen al adoptar este servicio; así como los controles para mitigarlos;	NO APLICA	Dado que el servicio no involucra infraestructura tecnológica crítica, servicios financieros ni datos sensibles,	Para el caso de contratación de servicios de infraestructura, plataforma y/o software, en la nube tanto con proveedores nacionales o extranjeros, las áreas requirentes deberán elaborar el respectivo informe dirigido a la Superintendencia de Bancos, con el detalle de los servicios asociados a los procesos críticos a ser contratados, que incluya la información mínima requerida en este punto de la norma.
23.6.b	b) Los centros de procesamiento de datos principal y/o alterno, contratados en la nube tanto con proveedores nacionales o extranjeros, deben haber sido implementados siguiendo el estándar ANSI-TIA-942 o superior y contar como mínimo con la certificación TIER III o su equivalente para diseño, implementación y operación y así garantizar la disponibilidad de los servicios brindados;	NO APLICA	La prestación del servicio no requiere la utilización de centros de procesamiento de datos ni afecta la disponibilidad de sistemas críticos	Para el caso de los centros de procesamiento de datos principal y/o alterno, contratados en la nube tanto con proveedores nacionales o extranjeros, las áreas requirentes solicitará a la Coordinación de Tecnología que en las bases del concurso se incluya las especificaciones técnicas determinadas en este punto de la norma.
23.6.c	c) El proveedor de servicios en la nube tanto con proveedores nacionales o extranjeros, debe contar, para los servicios ofertados, como mínimo, con certificación ISO 27001 en seguridad de la información, así como, la implementación de los controles establecidos en los estándares ISO 27017 (controles de seguridad para servicios en la nube), ISO 27018 (protección de información personal en la nube) u otras similares que aplique conforme el servicio ofertado;	NO APLICA	El servicio se ejecuta mediante procesos convencionales de la entidad, sin depender de infraestructura tecnológica crítica	Para el caso de contratación de servicios en la nube tanto con proveedores nacionales o extranjeros, las áreas requirentes deberán inlcuir en las bases del concurso, como requisito mínimo para los participantes / proveedores, la presentación de las certificaciones señaladas en este punto de la norma, u otras similares que aplique conforme el servicio ofertado.
23.7	Si los servicios provistos por terceros son de carácter financiero, estos están sujetos al cumplimiento de la normativa que emita la Junta de Política y Regulación Financiera y la Superintendencia de Bancos, en lo que corresponda.	NO APLICA	El contrato no es es un servicio financiero	Para la contratación de servicios de carácter financiero, las áreas requirentes deberán incluir en las bases del concurso, lo que corresponda para dar cumplimiento de la normativa que emita la Junta de Política y Regulación Financiera y la Superintendencia de
23.8	Para los casos en que las entidades financieras contraten la adquisición o acceso a bases de datos con información de personas naturales o jurídicas o de otra naturaleza, deberán aplicar procedimientos para asegurarse que el origen de la información es lícito; y se encuentra acorde con las leyes vigentes en el país.	NO APLICA	La prestación del servicio se realiza mediante procesos administrativos o profesionales convencionales, sin necesidad de controles sobre información	Para la contratación de adquisición o acceso a bases de datos con información de personas naturales o jurídicas o de otra naturaleza, las áreas requirentes deberán incluir en las bases del concurso, como obligación del contratista, la entrega de una declaración juramentada, u otro instrumento legal, que garantice el origen lícito de la información, y que se encuentra acorde con las leyes vigentes en el país.

23.9	Para la contratación total o parcial de servicios para ejecución de los procesos críticos, en el exterior, las entidades controladas deben notificar a la Superintendencia de Bancos, adjuntando la documentación de respaldo que asegure el cumplimiento de esta sección conforme la naturaleza del servicio contratado.	NO APLICA	Al no formar parte de los procesos críticos de la entidad, no existe obligación de notificación ni de remisión de documentación a la Superintendencia	Para la contratación total o parcial de servicios para ejecución de los procesos críticos, en el exterior, las áreas requirentes deben elaborar la notificación a la Superintendencia de Bancos, adjuntando la documentación de respaldo que asegure el cumplimiento de esta sección conforme la naturaleza del servicio contratado.
23.10	Para los casos en que las entidades financieras contraten servicios con las sociedades especializadas de depósitos y pagos electrónicos (SEDPES); y, con las administradoras de Sistemas Auxiliares de Pago (ASAP); deben garantizar que estas den cumplimiento según corresponda de la presente Norma.	NO APLICA	Al no formar parte de los procesos críticos de la entidad, no existe obligación de notificación ni de remisión de documentación a la Superintendencia	Para la contratación de servicios con las sociedades especializadas de depósitos y pagos electrónicos (SEDPES); y, con las administradoras de Sistemas Auxiliares de Pago (ASAP); las áreas requirentes deberán garantizar que estas den cumplimiento según corresponda de la Norma que rija para el efecto.
23.11	La Superintendencia de Bancos definirá los proveedores sistémicos en función de los servicios que ofrezcan y la cobertura que mantengan en las entidades controladas. El detalle de los proveedores sistémicos será puesto en conocimiento de las entidades controladas a fin de que esta característica sea considerada dentro de la gestión integral de sus proveedores.	NO APLICA	Al no formar parte de los procesos críticos de la entidad, no existe obligación de notificación ni de remisión de documentación a la Superintendencia	Cuando la Superintendencia de Bancos defina e informe al Biess cuales son los proveedores sistémicos, la Dirección de Servicios Generales, Contratación y Compras Públicas, verificará si coinciden con algún proveedor de servicio critico del Banco e informará a los Administradores de los Contratos correspondientes, para que levanten los riesgos que correspondan según esta condición, e implementen los controles para mitigarlos.

FIRMAS DE RESPONSABILIDAD

	CARGO	FIRMA
Aprobado por: Mgs. Andrés Urbina	Subgerente de Banca de Inversión	Firmado electrónicamente por: ANDRES JULIAN URBINA POSO. Validar únicamente con FirmaEC
Revisado por:Ing. Andrea Rodriguez	Directora de Valores y Estructuración	Firmado electrónicamente por: ANDREA YADIRA RODRIGUEZ TORRES. Validar únicamente con FirmaEC
Elaborado por: Ing. Roberto Montenegro	Analista de Valores y Estructuración	Firmado electrónicamente por: ROBERTO JAVIER MONTENEGRO TORRES. Validar únicamente con FirmaEC