Buenos Aires, 01 de enero de 2022

Banco Supervielle S.A.

Bartolomé Mitre 434 – CABA

At.: Gerencia de Abastecimiento Estratégico

Presente

De nuestra mayor consideración:

GLOBALLOGIC ARGENTINA S.R.L, con domicilio en Av. Corrientes 485, piso 6, CABA, representada en este acto por el Sr. Hernán Javier Pelimene (DNI: 25.850.280), en su calidad de Presidente, (en adelante, el Prestador), tiene el agrado de dirigirse a Banco Supervielle S.A., (en adelante, el Cliente y en su conjunto Las Partes), a fin de hacerles llegar la siguiente propuesta para adecuar los Servicios de Perfiles (en adelante, los "Servicios"), que nuestra entidad les presta con motivo de la Carta Oferta (en adelante, la "Carta Oferta"), que le cursáramos el 01/02/2019, y que fuera aceptada por el Cliente, y cuyo plazo y precio fueran modificados en virtud de la adenda que le cursáramos el 10/10/2019, 01/09/2020 y 03/09/2021, y que fuera aceptada por el cliente, en relación por los servicios, conforme los términos y condiciones que se establecen a continuación (en adelante, la "Oferta"):

PRIMERO: Prorrogar el plazo de la Carta Oferta, por el plazo de 12 (doce) meses, venciendo en consecuencia el 31/12/2022.

SEGUNDO: Establecer el costo del Servicio a partir del mes de enero, según el siguiente detalle de precios:

Perfil	Tarifario Actual por hora*	Incremento Tarifario 15% Enero-Marzo	Incremento Excepcional Febrero 35%	Incremento Tarifario 12% Abril-Junio	Incremento Excepcional Abril 15%
Jr Dev, UX, QA Aut, BA.	$3,046.72	$3,504.00	-NA-	$3,924.00	-NA-
Lead Dev, UX, QA Aut, ScrumMaster, BA	$4,698.14	$5,403.00	-NA-	$6,051.00	-NA-
Devops**	$5,242.37	$6,029.00	$8,139.00	-NA-	$9,360.00
Project Manager, Architect	$5,242.37	$6,029.00	-NA-	$6,752.00	-NA-
Senior PM, Senior Architect	$5,332.16	$6,132.00	-NA-	$6,868.00	-NA-
Jr Manual QA	$2,758.53	$3,172.00	-NA-	$3,553.00	-NA-
SSr Manual QA	$3,046.72	$3,504.00	-NA-	$3,924.00	-NA-
Sr Manual QA	$3,499.28	$4,024.00	-NA-	$4,507.00	-NA-
Lead Manual QA	$4,304.78	$4,950.00	-NA-	$5,545.00	-NA-

Perfil	Tarifario Actual por hora*	Incremento Tarifario 16% Enero-Marzo	Incremento Excepcional Febrero 35%	Incremento Tarifario 14% Abril-Junio	Incremento Excepcional Abril 15%
SSr Dev, UX, QA Aut, BA	$3,273.16	$3,797.00	-NA-	$4,328.00	-NA-
Sr Developer, Sr UX, Sr QA Automation, BA	$4,105.51	$4,762.00	-NA-	$5,429.00	-NA-

DocuSigned by:
975A2E6755FC4E4...

Estructura de Incrementos:

- Incrementos de Enero: 15% y 16% según tabla anterior diferenciado por roles.
- Incremento excepcional Febrero: 35% sólo para el rol de Devops (**)
- Incrementos Abril: 12%, 14% y 15% según tabla anterior diferenciado por roles.

Incrementos Julio y Octubre

- Estarán sujetos al movimiento acumulado del IPC informado por el Instituto Nacional de Estadística y Censos (INDEC) de la República Argentina. Y se aplicarán uniformemente a todos los roles.
- Períodos a considerar: Julio (Meses: Abril-Mayo-Junio). Octubre (Meses: Julio-Agosto-Septiembre).

Banco Supervielle NO compromete volumen de adjudicación

Los presentes precios no incluyen I.V.A.

TERCERO: A continuación, se enumeran los requisitos técnicos-operativos de la Comunicación 6375 de BCRA, para el caso que alguno de ellos resulte de aplicación a la contratación objeto de esta adenda:

Requisito Exigido BCRA	# Req.	Descripción Requisito
1	RGS001	Las entidades/prestadores deberán establecer y notificar al BCRA el detalle completo, exhaustivo y actualizado de las responsabilidades compartidas y/o exclusivas sobre los roles y funciones para la administración y gestión operativa de seguridad de la información asociadas al STI.
1	RGS004	La entidad y prestador deberán establecer y documentar los protocolos de intercambio de información entre los participantes del acuerdo de STI, incluyendo terceros subcontratados, así como las técnicas y medidas operativas (formatos, límites de tiempo, responsables, etc.) que garanticen información útil, oportuna y completa a las partes involucradas y al BCRA.
1	RGS005	En el caso de prestador o subcontratistas participantes de un STI que procesen, almacenen o transporten datos o procesos de la entidad en locaciones en el **exterior**, la entidad, los prestadores y los terceros involucrados deberán proveer los mecanismos necesarios para verificar si las locaciones satisfacen las disposiciones legales, normativas y contractuales establecidas en el acuerdo de STI, incluyendo lo establecido en las normas sobre "Expansión de entidades financieras".
1	RGS007	Las entidades/prestadores deben documentar y asignar la propiedad de todos los activos de información en el STI, determinando el nivel de responsabilidad administrativa y operativa de cada parte en el ciclo de vida de la información.
1	RCC001	Los contenidos del programa de CC deben formularse y mantenerse actualizados en base a un análisis de las vulnerabilidades y los resultados de la Gestión de Incidentes, e incluir, pero no limitarse a incidentes: reportados, detectados y conocidos.
1	RCC005	Mantener informado al personal interno, personal responsable por la gestión del STI, personal de terceros involucrado en las tareas operativas y clientes sobre las vías de comunicación para la recepción de denuncias o problemas en el circuito asociado al escenario descripto.
1	RCC006	Respecto de la audiencia del programa de CC, deben aplicarse los siguientes criterios: **a.** Características y segmentación de la audiencia, de acuerdo con el nivel de intervención en el proceso y naturaleza de la función o rol que ocupa cada participante. **b.** Deben encontrarse alcanzados todos los participantes necesarios en el flujo completo de la actividad indicada en el escenario.

DocuSigned by:
975A2E6755FC4E4...

		c. Orientado pero no limitado a: personal interno, personal responsable por la gestión del STI, proveedores y clientes.
1	RCC007	Con una periodicidad mínima anual, debe efectuarse un análisis del programa de CC ejecutado que mida la evolución de los incidentes, respecto de las actividades de CC realizadas incluyendo como mínimo: **a.** Un reporte de la cantidad y segmentación de destinatarios y contenidos del programa de CC. **b.** Una comparación entre los contenidos cubiertos por el programa de CC y la cantidad y tipo de incidentes de seguridad reportados/detectados/conocidos.
1	RCC010	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre las prácticas de seguridad en la plataforma de soporte de STI.
1	RCC012	Los contenidos del programa de CC deben incluir técnicas específicas para el desarrollo/ adquisición/fabricación, implementación, homologación y prueba de características de seguridad de los recursos informáticos del STI, asegurando que el personal involucrado interno/externo se encuentra debidamente capacitado para disminuir las fallas de implementación de las características de seguridad.
1	RCC013	Las entidades/prestadores deben contar con un mecanismo de comunicación de los contenidos de su programa de concientización y capacitación del STI que asegure: **a.** Que los destinatarios se encuentran informados de forma continua. **b.** Que los destinatarios pueden efectuar consultas y evacuar dudas.
1	RCA050	Las entidades/prestadores deben garantizar el acceso irrestricto a la entidad y al BCRA, a toda documentación e información relativa al procesamiento, operaciones y procedimientos del STI cuando sea requerida.
1	RCA051	La entidad debe asegurar que el prestador del STI documente y respalde el nivel de controles implementados para la protección de los servicios provistos, por medio de mediciones independientes, auditorías externas y certificaciones de estándares internacionales.
1	RCA052	Las entidades/prestadores deben contar e implementar con una política homogénea de administración de credenciales, basada en la necesidad de uso/conocimiento, la separación de roles incompatibles y la prevención de colusiones, para el acceso a, pero sin limitarse a: · Mecanismos de encripción de datos y canales de comunicación. · Usuarios privilegiados de la plataforma operativa/aplicativa. · Usuarios de emergencia/contingencia. · Usuarios comunes. Asimismo, deberán asegurar un ciclo de vida de las credenciales, cuyos parámetros, reglas, algoritmos, piezas de software involucradas deberán ser actualizadas y debidamente comunicadas a las partes.
1	RIR003	Los registros colectados por los servicios provistos por el prestador, deben asegurar la trazabilidad de las acciones realizadas en la totalidad de las actividades, identificando quien (cuenta, origen, destino), qué (actividad, función, transacción), dónde (servicio, ubicación), cuando (tiempo), cómo (patrón, relación de eventos).
1	RIR010	Los dispositivos/equipamiento y/o piezas de software dispuestas por la entidad/ prestador para el STI, deben asegurar que satisfacen un ciclo de vida y de desarrollo, basado en las siguientes etapas conceptuales: **a.** Análisis de requerimientos. **b.** Adquisición/fabricación/desarrollo. **c.** Prueba y homologación. **d.** Implementación. **e.** Operación y mantenimiento. **f.** Descarte y reemplazo. Asimismo, este ciclo debe proveer los elementos de seguridad relacionados con, pero no limitados, a: **g.** Requisitos funcionales de seguridad. **h.** Tipos y características de validación de los datos de entrada. **i.** Granularidad de las funciones y los registros. **j.** Niveles de acceso.

DocuSigned by:
975A2E6755FC4E4...

		k. Control de cambios. **l.** Actualización y parches.
1	RIR011	Las entidades/prestadores deben ejecutar un proceso de homologación de dispositivos/ equipamientos y/o piezas de software para interactuar con el STI, garantizando la verificación de todos los aspectos de diseño, funcionalidad, interoperabilidad y características de seguridad definidos en las etapas de adquisición/fabricación/desarrollo e implementación.
1	RIR021	Las entidades/prestadores deben garantizar y establecer los mecanismos de recupero de los activos de información ante rescisión/terminación y/o interrupción indefinida de los servicios y/o relocalización, respetando las condiciones de seguridad de la información y continuidad de las operaciones.
1	RIR022	Los recursos e información que se utilicen en el STI deben estar inventariados con su correspondiente identificación del propietario e indicando los parámetros de eliminación segura y sus parámetros de validación en el ciclo de vida del dato.
1	RIR023	Las entidades/prestadores deben establecer un ciclo de vida de los datos de registro de las actividades, según lo establece el requisito RIR003, cumpliendo con los requerimientos legales y las previsiones de seguridad para su almacenamiento, inalterabilidad por el tiempo legal de conservación y su accesibilidad a los responsables del control para soporte de investigaciones forenses en casos de incidentes de seguridad y detección de brechas de seguridad.
1	RIR025	Las entidades/prestadores deben asegurar una separación lógica de los ambientes de procesamiento, almacenamiento, transporte y recuperación de datos de la entidad respecto del prestador, otras entidades y terceros. Asimismo, deben asegurar que los dispositivos/equipamientos y piezas de software que se empleen o accedan a los entornos de la entidad, deben restringirse a los necesarios y homologados según lo indicado en el requisito RIR011.
1	RMC003	Las entidades/prestadores deben realizar un seguimiento en los STI de los cambios de configuración de seguridad y verificar los niveles de actualización de: sistemas operativos, bases de datos, vínculos de comunicación, herramientas de prevención y detección de códigos maliciosos, equipamientos de seguridad de red, controladores de tráfico y cualquier otra herramienta de seguridad. Deben incluir, pero no limitarse a: **a)** Seguimiento de privilegio y derechos de acceso; **b)** Procesos de copia, resguardo y recuperación de información; **c)** Disponibilidad de los dispositivos/equipamiento; **d)** Alarmas, alertas y problemas detectados por los sistemas de registro de eventos.
1	RMC006	A partir de los registros colectados por los recursos del STI asociados al escenario, las entidades/prestadores deben realizar una clasificación y determinación de los eventos de seguridad, una definición de los límites y umbrales de compromiso, niveles de comportamiento normal/inesperado y establecer las acciones de acuerdo con cada clasificación y límite determinados.
1	RMC014	Las entidades/prestadores deben determinar, documentar y procedimentar los recursos, dispositivos/equipamientos y piezas de software para monitorear las actividades de los STI.
1	RMC015	Las entidades/prestadores deben establecer formalmente y ejecutar periódicamente tareas de prueba y análisis de vulnerabilidades de los recursos asociados al STI en todos sus procesos críticos.
1	RGI001	Las entidades/prestadores deben realizar con una periodicidad mínima anual y con base en el análisis de riesgo de los activos informáticos asociados al escenario, un análisis de los incidentes ocurridos y un reporte que sirva para establecer medidas de protección, contenidos del programa de capacitación y concientización, modificaciones a la registración y control de eventos, y una redefinición de las alertas, límites y umbrales.
1	RGI002	La identificación de incidentes debe estar basada al menos en alertas tempranas, estadísticas de tipo/frecuencia/patrón de incidentes y recomendaciones de seguridad informática.
1	RGI003	La gestión de incidentes de seguridad puede ejecutarse en forma tercerizada pero debe ser coordinada con personal de la entidad financiera.
1	RGI005	Los incidentes detectados deben recibir un tratamiento regular con un escalamiento definido formalmente.

DocuSigned by:
975A2E6755FC4E4...

1	RCO001	Se debe contar con la provisión de los recursos necesarios para la creación, mantenimiento, actualización y prueba de un plan de continuidad del procesamiento de datos. El mismo debe ser operable y funcional, en base a los requerimientos acordados en el STI, propios de la entidad y regulados por el BCRA.
1	RCO002	Las entidades/prestadores deben definir, acordar, documentar y poner en ejecución los métodos para determinar el impacto de un evento que interrumpa las actividades de la organización tanto de la entidad, el prestador o terceros subcontratados contemplando, pero no limitándose, a: **i)** Identificación de recursos críticos, incluyendo usuarios operativos y de control; **ii)** Identificación de todas las dependencias, incluyendo procesos aplicaciones, pares, y terceros subcontratados; **iii)** Detección de las amenazas de los recursos críticos; **iv)** Determinación del impacto de las interrupciones planeadas o no, y su variación en el tiempo; **v)** Establecimiento de un periodo máximo tolerable de interrupción; **vi)** Establecimiento de periodos de recuperación parciales y totales; **vii)** Establecimiento del tiempo máximo tolerable de interrupción para la recuperación de recursos críticos; **viii)** Estimación de los recursos requeridos para la continuidad y eventual restauración de la operatoria y locaciones alternativas. Debe asimismo, darse participación activa a los responsables primarios de los procesos y recursos críticos, garantizando una cobertura completa de los asociados al STI.
1	RCO003	El plan de continuidad de procesamiento de datos debe considerar pero no limitarse a la incorporación de los siguientes contenidos: **a)** Procedimientos operativos manuales, logísticos y automatizados de emergencia según cada proceso/recurso identificado y acción determinada; **b)** Ubicación/locación, traslado y transporte de responsables, proveedores y servicios de emergencia y recursos físicos y lógicos; **c)** Procedimientos de recuperación/restauración de los recursos comprometidos.
1	RCO004	El plan de continuidad de procesamiento de datos debe ser probado periódicamente, como mínimo una vez al año. Las pruebas deben ser consistentes y coherentes con los criterios del requisito RCO002. Las pruebas también deben garantizar que todos los responsables y participantes de los procesos de continuidad y recuperación se encuentren informados de manera regular, continua y formal.

CUARTO: Convenir que las restantes cláusulas de la Carta Oferta que no hubieran sido modificadas por el presente acuerdo seguirán vigentes, sin alteración alguna.

QUINTO: Manifestar que, si la presente Oferta se encontrara alcanzada por cualquier gravamen, impuesto o sellado, el mismo será soportado en igual proporción por las Partes.

SEXTO: La presente Oferta se entenderá aceptada por el Cliente si en el plazo de 1 (un) día hábil de recibida la misma, no nos notificaran lo contrario.

Sin otro particular, los saludamos atentamente.

DocuSigned by:
975A2E6755FC4E4...

GlobalLogic
A Hitachi Group Company

Señores
Banco Supervielle S.A.
Bartolomé Mitre 434, CABA, Argentina.

De nuestra mayor consideración:

Quien suscribe, en nombre y representación de GlobalLogic Argentina S.R.L., CUIT 30-70731490-3 con domicilio en Av. Corrientes 485 piso 6° de la Ciudad Autónoma de Buenos Aires, tengo el agrado de dirigirme a usted, Banco Supervielle S.A., CUIT 33-50000517-9 con domicilio en Bartolomé Mitre 434, a los fines de poner en conocimiento que prestamos servicios de Desarrollo de Software Ágil.

El equipo interno del Banco Supervielle “Gestión Operativa y Administración de Inmuebles”, es quien nos contrata y con quien establecemos todos los acuerdos contractuales.

DocuSigned by:
975A2E6755FC4E4...

Hernan Pelimene
VP | Latam Delivery Head
Av. Corrientes 485, CABA
hernan.pelimene@globallogic.com

GlobalLogic
A Hitachi Group Company

Señores
Banco Supervielle S.A.
Bartolomé Mitre 434, CABA, Argentina.

De nuestra mayor consideración:

Quien suscribe, en nombre y representación de GlobalLogic Argentina S.R.L., CUIT 30-70731490-3 con domicilio en Av. Corrientes 485 piso 6° de la Ciudad Autónoma de Buenos Aires, tengo el agrado de dirigirme a usted, Banco Supervielle S.A., CUIT 33-50000517-9 con domicilio en Bartolomé Mitre 434, a los fines de poner en conocimiento que prestamos servicios de Desarrollo de Software Ágil.

El equipo interno del Banco Supervielle “Gestión Operativa y Administración de Inmuebles”, es quien nos contrata y con quien establecemos todos los acuerdos contractuales.

DocuSigned by:
975A2E6755FC4E4...

Hernan Pelimene
VP | Latam Delivery Head
Av. Corrientes 485, CABA
hernan.pelimene@globallogic.com