MEMORÁNDUM N° 0074-2022-AGROBANCO/DRT

Para	**:**	Enrique Orezzoli Moreno Gerente General (e)
Cc	:	María Elena Palacios Quiroz Gerente de Legal y Cumplimiento
De	**:**	Juan Carlos Miraya Anamaria Gerente de Riesgos
Asunto	**:**	Informe de Riesgos – Servicio de Outsourcing del Data Center
Fecha	**:**	17 de junio del 2022

Con motivo de presentar el informe de riesgos del Servicio de Outsourcing del Data Center en la sesión de Directorio extraordinaria, se adjunta el Informe N° 074-2022-AGROBANCO/ROP de fecha 17.06.2022.

Sin otro particular, quedo de usted.

Atentamente,

MIRAYA ANAMARIA Juan Carlos FAU 20504565794 soft

Firmado digitalmente por MIRAYA ANAMARIA Juan Carlos FAU 20504565794 soft
Fecha: 2022.06.17 20:37:10 -05'00'

Juan Carlos Miraya Anamaria
Gerente de Riesgos

Informe N° 074-2022-AGROBANCO/ROP de Riesgos por Servicio Significativo Provistos por Terceros: Servicio de Outsourcing del Data Center

GERENCIA DE RIESGOS

BANCO AGROPECUARIO

CONTENIDO:

I. OBJETIVO

Efectuar la evaluación de los riesgos a los que está expuesto el Banco y recomendar las medidas de tratamiento correspondientes, para el servicio de Outsourcing de Data Center.

II. BASE LEGAL

- Resolución S.B.S. N° 272 - 2017, Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos.
- Resolución S.B.S. N° 2116 - 2009, Reglamento para la Gestión del Riesgo Operacional
- Resolución S.B.S. N° 504 – 2021, Reglamento para la Gestión de Seguridad de la Información y la Ciberseguridad
- MDP-033-04 Manual de procedimientos de Riesgo Operacional
- REG-027-03 Reglamento de Contrataciones
- MDP-073-03 Manual de Procedimientos de Contrataciones
- REG – 026 – 05 Reglamento de Seguridad de Información

III. ANTECEDENTES

Dentro del Plan Anual de Contrataciones 2022, la División de Tecnología de la Información ha solicitado la contratación del servicio de Outsourcing de Data Center por 10 meses, esto con el fin de darle continuidad al servicio de Outsourcing del Centro de Datos Principal que viene siendo prestado por la empresa Kyndryl Perú SAC de acuerdo a la Adenda al Contrato N° 190000018-AGROBANCO firmada con fecha 24 de agosto 2021 entre AGROBANCO y KINDRYL PERU SAC.

El servicio de Outsourcing de Data Center que ha venido recibiendo el Banco, originalmente fue suscrito con la compañía IBM DEL PERU SAC, que mediante una reorganización societaria por escisión para separar la unidad de Servicios de Gestión de Infraestructura (MIS, por sus siglas en inglés) de su división de Servicios de Tecnología Global (GTS, por sus siglas en inglés) pasó a denominarse IBM OCEAN PERU S.R.L. y posteriormente por actualización de la razón social IBM, OCEAN PERU SRL pasó a denominarse KYNDRYL PERU SAC.

A la fecha el Banco viene recibiendo el servicio de Outsourcing de Data Center mencionado, habiéndose iniciado un proceso para la contratación del servicio por un período de 10 meses con la misma empresa KYNDRYL PERU SAC, de acuerdo a lo establecido en el Informe Técnico N° 00016-2022-AGROBANCO/DSS emitido por la división de Tecnología de Información.

Con fecha 09 de junio 2022 la división de Logística solicitó a la Gerencia de Riesgos la evaluación de los términos de referencia para la Contratación del Servicio de Outsourcing de Datacenter, solicitado por la División de Tecnología de la Información, para definir si se trata de un servicio significativo de acuerdo a lo establecido en el MDP-073-03 Manual de Procedimientos de Contrataciones.

Asimismo, se nos ha alcanzado toda la documentación referida al proceso de contratación, entre las que se encuentra la propuesta de Contrato, el mismo que estamos tomando como base para determinar los controles previstos para mitigar los riesgos identificados, en adelante lo denominaremos: El Contrato.

De la evaluación efectuada para determinar si se trata de un servicio significativo mediante requerimiento N° 2200000427, se ha determinado que el servicio de Outsourcing de Data Center corresponde a un Servicio Significativo Provisto por Terceros.

IV. ALCANCE

El presente informe corresponde a la evaluación de riesgos establecida en la Resolución SBS N° 272 – 2017 Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, Capítulo IV, Art. 35° numeral 36.3, que establece que:

> "*La empresa debe realizar una evaluación de los riesgos asociados a los servicios significativos provistos por terceros, ya sea que se encuentren o no bajo la modalidad de subcontratación. Dicha evaluación debe ser presentada al directorio para su aprobación.*"

El alcance de la evaluación de riesgos considera a los riesgos a los que está expuesto el Banco por: la contratación de un tercero para la ejecución de un servicio significativo.

V. ANÁLISIS

5.1 Información del servicio

5.1.1 Descripción del servicio

La descripción del servicio se ha obtenido de los términos de referencia del servicio enviado por la División de Logística, en el que se indica lo siguiente:

a. Referidas a las condiciones que debe cumplir el Centro de Datos Principal del proveedor

   El Banco, requiere que la infraestructura física dentro del Centro de Datos (Principal y Alterno), que proponga el proveedor, cumpla con los requerimientos técnicos mínimos establecidos en los términos de referencia.

b. Referidas a las condiciones que debe cumplir el Centro de Datos (Alterno) del proveedor

   Como parte de los servicios ofrecidos por el proveedor, este debe ofrecer un centro de datos alterno, el cual estará situado, fuera de las instalaciones del Centro de Datos principal, siendo necesario que exista una separación física entre ambos de por lo menos 5

km, el mismo que contará con las características técnicas descritas en los términos de referencia.

c. Referido al respaldo de información en el Centro de Datos Principal y Alterno (Backups)

El proveedor es responsable de ejecutar los respaldos de información (Backup), en coordinación con el Banco, para lo cual se utilizará tecnología de última generación que será propuesta por el proveedor y aprobada por el Banco, de corresponder, fijando además los horarios para la ejecución de los respaldos y las políticas, las mismas que serán fijadas durante la etapa de implementación.

d. Referido a la operación de la plataforma

El proveedor, debe brindar el servicio de operación de la plataforma propuesta, las 24 horas al día, los 7 días de la semana debiendo considerar algunas responsabilidades descritas en los términos de referencia.

e. Referido a la comunicación entre Oficina Principal y proveedor

Con la finalidad de asegurar las comunicaciones entre el Centro de Datos del proveedor y la oficina principal del Banco, se establece un segundo enlace (contingencia), con una velocidad mínima de un (1) Mbps, siendo necesario que este sea de un proveedor distinto al considerado para el enlace principal.

f. Referido a la comunicación LAN y seguridad de información

El proveedor, configurar una red LAN física o virtual (VLAN) que será de uso exclusivo para el Banco, en el Centro de Datos. Así mismo, como parte del servicio a brindar, deberá configurar un sistema de detección y prevención de intrusos (IPS), siendo necesario que se incluya además un sistema de detección y eliminación de virus informáticos.

g. Referido al Hardware requerido para el ambiente de producción, contingencia, proyectos, pruebas y desarrollo

El Banco, con la finalidad de mantener sus operaciones a nivel nacional requiere que el hardware propuesto por el proveedor cumpla los requerimientos técnicos mínimos que están descritos en los términos de referencia.

h. Referido a las condiciones de flexibilidad (aumento de la capacidad de procesamiento) del Hardware durante la ejecución del servicio por un determinado periodo

Como parte del servicio a brindar, el proveedor, facilita al Banco, la posibilidad de flexibilizar el incremento o decrecimiento de la capacidad de procesamiento del servidor de producción, en la oportunidad que el Banco, lo requiera.

i. Referido al software requerido para el ambiente de producción, contingencia, proyectos, pruebas y desarrollo

El Banco, con la finalidad de mantener sus operaciones a nivel nacional requiere que el software propuesto por el proveedor sea el que se detalla en los términos de referencia.

j. Otros puntos a considerar

- Con la finalidad de garantizar el proceso de implementación del servicio objeto de la contratación, el proveedor, debe asignar personal técnico experimentado y todos los materiales e insumos necesarios que permitan una adecuada implementación e integración a los sistemas del Banco.
- El proveedor, debe proveer al Banco, de un Servicio de Soporte Técnico, la cual garantice la operatividad del mismo durante la vigencia del contrato, siendo necesario que se incluya soporte vía telefónica, asesoría técnica para la mejora y optimización de los recursos implementados, sin que esto genere un costo adicional al Banco.
- El proveedor, debe proponer dentro de los diez (10) días siguientes a la firma del Contrato, a un profesional técnico que será líder del proyecto (responsable), que lo represente ante el Banco, quien coordinará, administrará, supervisará, y controlará los recursos asignados al proceso de implementación servicio objeto de la contratación.
- En caso cualquiera de los enlaces, deje de operar o exista una interrupción del servicio, el proveedor, dispondrá de un máximo de dos (2) horas, desde el momento en que se reportó la incidencia para la resolución del mismo, en caso se exceda el tiempo indicado, se aplicara la penalidad correspondiente.
- Existen operaciones que debe ejecutar el proveedor, en caso exista una mala práctica por parte del operador asignado, y esto devengue en una pérdida de información, mala carga de datos o cualquier análogo, se aplicaran las penalidades correspondientes.
- En caso el proveedor, ejecute un proceso de restauración de información a solicitud del Banco, este se deberá ejecutar en el servidor de desarrollo, caso contrario y esta se ejecute en el ambiente de producción sin la solicitud expresa del Banco, se estaría incurriendo un perjuicio, por tanto, se aplicarían las penalidades correspondientes, según el grado de perjuicio.

5.2 Evaluación de riesgos del servicio

5.2.1 Criterios de bienes o servicios por terceros

De los criterios evaluados en el "Requerimiento de bienes o servicios", se define que el servicio de Outsourcing del Data Center es un servicio significativo ya que, en caso de falla o suspensión del servicio, existe un Riesgo Importante que puede afectar a los Ingresos, Solvencia, Continuidad Operativa y a la Reputación del Banco.

De lo descrito anteriormente y teniendo en cuenta la Resolución SBS N° 2116-2009, en el que indica en su artículo 14: "*En los casos de **servicios significativos**, se encuentren o no bajo la modalidad de subcontratación, y de servicios subcontratados la empresa debe considerar los siguientes aspectos: (…) c) Gestionar y monitorear los riesgos asociados a estos servicios."*

Por lo que, al tratarse de un servicio significativo, se gestionará y monitoreará los riesgos asociados al servicio.

5.2.2 Riesgos identificados

A continuación, se presenta el análisis de los tipos de riesgos a los que se podría exponer el Banco debido a la contratación del Servicio de Outsourcing del Data Center:

5.2.2.1 Riesgo de Reputación

La interrupción del servicio podría generar una paralización de la operativa, lo cual podría generar que no se brinde atención a los clientes de manera oportuna, lo cual podría generar un daño en la imagen del Banco. Por otro lado, el Banco debe asegurarse de que se mantenga reserva y confidencialidad sobre la información que pudiera proporcionar al proveedor.

5.2.2.2 Riesgo Operacional

- **Análisis por Riesgo Operacional:**

  Se han identificado los siguientes riesgos operacionales:

  - Posibilidad de pérdida económica por incumplimiento de los compromisos y/o acuerdos de servicios definidos en el contrato con el proveedor.
  - Posibilidad de pérdida económica por la inoperatividad y/o interrupción de los servicios del Banco por una inadecuada gestión por parte del proveedor.
  - Posibilidad de pérdida económica por el incumplimiento de las políticas y procedimientos de Seguridad de Información y Protección de Datos Personales por parte del personal de proveedor.

Evaluación y control del riesgo operacional

N°	Riesgo	Causa	Consecuencia	Riesgo Inherente	Controles	Riesgo Residual
1	Posibilidad de pérdida económica por incumplimiento de los compromisos y/o acuerdos de servicios definidos en el contrato con el proveedor.	> Inadecuada definición de las cláusulas comerciales con el proveedor. > Inadecuada definición de los niveles de servicio - SLA/SLO (no personalizados a la realidad del Banco). > Falta de penalidades por incumplimiento de los acuerdos con el proveedor. > Falta de seguimiento de los acuerdos de niveles de servicio - SLA/SLO.	> Costos adicionales por proyecto inconcluso o no deseado asumido por el banco. > Multas de los entes reguladores (SBS, INDECOPI) por no cumplir con los requerimientos regulatorios.	Alto	**C1**. Se encuentra establecido en el contrato en "Penalidades" que el Banco aplicará penalidades por el incumplimiento de cualquiera de las obligaciones contraídas por el proveedor, las mismas que serán aplicadas en caso el tiempo objetivo señalado en las Condiciones Especificas no fuera alcanzado debido a razones atribuibles a el proveedor.	Moderado
2	Posibilidad de pérdida económica por la inoperatividad y/o interrupción de los servicios del Banco por una inadecuada gestión por parte del proveedor.	> Personal técnico no capacitado (En temas Técnicos, Normativas, sistemas del banco, entre otros). > Falta de capacidad instalada en producción y tecnología del personal del proveedor. > Inadecuada definición de los niveles de servicio - SLA/SLO con el proveedor.	> Indemnizaciones por reclamo de clientes > Multas de los entes reguladores (SBS, INDECOPI) por no cumplir con los requerimientos regulatorios.	Alto	**C1.** Se encuentra establecido en el contrato que el proveedor tiene conocimiento que en caso cualquiera de los enlaces, deje de operar o exista una interrupción del servicio, el proveedor, dispondrá de un máximo de dos (2) horas, desde el momento en que se reportó la incidencia para la resolución del mismo, en caso se exceda el tiempo indicado, se aplicara la penalidad correspondiente.	Moderado
3	Posibilidad de pérdida económica por el incumplimiento de las políticas y procedimientos de Seguridad de Información y Protección de Datos Personales por parte del personal de proveedor.	> Falta de comunicación entre el Banco y el proveedor, relacionado a los cambios de normativos (políticas, definiciones, entre otros). > Mal uso de la información confidencial. > Falta de seguimiento de las políticas de Seguridad de Información y Protección de Datos Personales al personal del proveedor. > Falta de niveles de servicio relacionados a Seguridad de Información.	> Indemnizaciones por reclamo de clientes. > Multas de los entes reguladores (SBS, INDECOPI) por no cumplir con los requerimientos regulatorios.	Alto	**C1.** Se encuentra establecido en el contrato que en caso el proveedor, ejecute un proceso de restauración de información a solicitud del Banco, este debe ejecutar en el servidor de desarrollo, caso contrario y esta se ejecute en el ambiente de producción sin la solicitud expresa del BANCO, se estaría incurriendo un perjuicio, por tanto, se aplicarían las penalidades correspondientes, según el grado de perjuicio. **C2.** Se encuentra establecido en el contrato que el proveedor debe tener conocimiento que existen operaciones que debe ejecutar, en caso exista una mala práctica por parte del operador asignado, y esto devengue en una pérdida de información, mala carga de datos o cualquier análogo, se aplicaran las penalidades correspondientes. **C3.** Dentro del contrato se establece la claúsula de Seguridad de Información o procesamiento de datos, en el que se indica que las partes serán responsables por los reclamos, denuncias, procesos judiciales, procedimientos administrativos y/o cualquier otro iniciado en contra de la otra parte; así como por los daños y perjuicios derivados del incumplimiento de las obligaciones establecidas en la presente cláusula, en tanto le resulten imputables. En ese sentido, las partes se harán cargo de las costas, costos, gastos, multas, indemnizaciones, así como cualquier otro gasto en que se incurra.	Bajo

Seguimiento de planes de acción y monitoreo

Dentro de la evaluación y control del riesgo, se hará seguimiento a los riesgos con niveles moderados en coordinación con la división de TI y el Oficial de Continuidad del Negocios y Seguridad de Información, con la finalidad de mitigar cualquier vulnerabilidad que podría generar alguna contingencia dentro del Banco. Asímismo, al mantenerse los riesgos en niveles moderados y bajo no será necesario la propuesta de planes de acción, pero como parte del monitoreo se hará seguimiento de los eventos que se puedan presentar en el servicio, analizando su frecuencia e impacto dentro del Banco.

5.2.2.3 Riesgo de seguridad de información y continuidad de negocio

Antecedentes

La evaluación de los riesgos de seguridad de información y continuidad de negocio están en función de los activos de información involucrados en el alcance del *servicio de outsourcing de data center*. Estos activos, de acuerdo con el inventario vigente son:

- A009 Servicio de outsourcing de Centro de Datos principal
- A010 Sistema IBS
- A001 Base de Datos DB2 - AS400 de producción

En función a estos se activos se han analizado los riesgos en el proceso de contratación de servicio de outsourcing de data center, aplicando la metodología contenida en el MDP-033-04 MANUAL DE PROCEDIMIENTOS DE RIESGO OPERACIONAL y en conjunto con la División de Tecnología. La matriz de evaluación de riesgos se encuentra adjunta a la presente (anexo 01) seguida del plan de tratamiento correspondiente (anexo 02). A continuación, se resume los principales aspectos de la evaluación de riesgos a los activos señalados:

Riesgos identificados

Este activo de información considera el servicio de terciarización del hardware y software base, principalmente para la operatividad del Sistema Core IBS y la base de datos de producción. Los riesgos que aplican en este contexto son:

[R01] Sanciones por incumplimiento regulatorio (SBS) por servicios significativos

Activos de información comprometidos:

- A009 Servicio de outsourcing de Centro de Datos principal

El servicio de outsourcing calza dentro de la definición de SBS para los servicios significativos. Por ende, es necesario aplicar los requerimientos regulatorios que son de responsabilidad del proveedor en los términos de referencia – TdR, bases y contrato.

El riesgo inherente o riesgo sin controles para este activo es 'extremo', lo cual indica la importancia y criticidad que tiene su gestión para el Banco.

Luego se analizaron los controles existentes: TdR, Bases del proceso y el Contrato del servicio outsourcing los cuales, de acuerdo con la metodología, logran una calificación de 'aceptables'.

Sin embargo, al calcular el nivel de riesgo residual, es decir luego de aplicar controles se obtiene un nivel de riesgo 'alto', lo cual significa que es necesario mejorar los controles o aumentarlos para lo cual se debe diseñar un plan de tratamiento.

En este caso, el plan de tratamiento considera como primera actividad el perfeccionamiento de los TdR (que son prácticamente los mismos que los del contrato ya vencido) a través del desarrollo de procedimientos o especificaciones anexas, dado que los TdR en el estado actual del proceso de contratación, no se pueden modificar sin que esto genere una nueva negociación de precios, presupuesto y revisiones con el proveedor. Esta actividad estará a cargo de la División de TI.

La segunda actividad ha sido la elaboración de una propuesta de bases y contrato elaborada por la Unidad de Seguridad de Información, en la que se ha incluido elementos que permitan sustentar el cumplimiento regulatorio de la Resolución SBS N° 504-2021. Esta propuesta, ha sido discutida con el proveedor y no va a generar cambios de presupuesto, por lo que ha sido entregada al área de Logística-As. Legal para su validación y continuar con el proceso.

[R02] Pérdida o divulgación de información de propiedad del Banco

Activos de información comprometidos:

- A009 Servicio de outsourcing de Centro de Datos principal

Sin controles, la posibilidad de que el proveedor pueda voluntaria o involuntariamente compartir o publicar información es un riesgo en nivel 'extremo' como se puede apreciar en la matriz de evaluación adjunta.

Al aplicar los controles para este riesgo: Certificaciones en seguridad de información del prov., y el Contrato del servicio outsourcing, el riesgo se mueve a la zona de nivel 'alto'. Esto significa que, si bien los controles son calificados como 'buenos'

es necesario reforzarlos o ampliarlos para bajar aún más el nivel de riesgo donde sea aceptable.
Por ello se considera la actividad de *Perfeccionamiento de los términos de referencia* del plan de tratamiento como el medio por el cual reducir dicho nivel.

[R03] Interrupción de los procesos de negocio por finalización no planificada del servicio de outsourcing

Activos de información comprometidos:

- A009 Servicio de outsourcing de Centro de Datos principal
- A010 Sistema IBS

Este riesgo está relacionado con la continuidad de los procesos del Banco, en especial del proceso crediticio, analizándose la posibilidad e impacto de una terminación unilateral de contrato. El nivel de riesgo inherente obtenido es 'extremo', lo cual denota la importancia y criticidad de su tratamiento. Al aplicar controles, se obtiene un nivel 'alto' lo cual requiere de actividades de tratamiento que son el perfeccionamiento de los términos de referencia, la inclusión de requerimientos de normatividad en bases y contrato y la elaboración de la estrategia de migración, esta última a cargo de la División de TI.

[R04] Interrupción de los procesos de negocio por no contar con contrato suscrito de outsourcing

Activos de información comprometidos:

- A009 Servicio de outsourcing de Centro de Datos principal
- A010 Sistema IBS

Otro riesgo para la continuidad operativa está relacionado con la interrupción del servicio de outsourcing al no contar con un contrato suscrito desde enero a la fecha de presente con el proveedor actual Kyndryl. Como es de esperarse, tanto el riesgo inherente como el riesgo residual en este caso resultan 'extremos' debido a que no existen controles formales que puedan reducir la probabilidad de este escenario.
En tal sentido, como plan de tratamiento se menciona: la suscripción del contrato con el proveedor, y el perfeccionamiento de los TdR. Ambas actividades a cargo de la División de TI.

[R05] Falta de disponibilidad o corrupción de datos por sobrepasar u operar muy cerca del límite de almacenamiento asignado según términos de referencia

Activos de información comprometidos:

- A001 Base de Datos DB2 - AS400 de producción

Con los nuevos términos de referencia, debido a la urgencia de firmar un contrato y las restricciones presupuestales, no es posible solicitar mayor espacio de almacenamiento del que se viene utilizado actualmente para el ambiente de producción: 2.64TB, el cual no se incrementa desde el año 2012. Esto representa un riesgo para las aplicaciones y procesos que tienen que ejecutarse en este entorno y que demandan espacio de disco en tiempo de ejecución. El riesgo inherente para este caso ha sido ubicado en la zona de 'extremo'.

Los controles que mitigan este riesgo son los TdR del servicio de outsourcing, aunque no resulta muy eficiente, y el procedimiento diario de descarga de backups que ejecuta la División de TI a fin de liberar espacio en los discos del ambiente de producción. A pesar de que, como resultado de la aplicación de estos controles, el riesgo se ubica en el nivel medio, esta restricción se convierte en un impedimento para el crecimiento de transacciones, la ejecución de procesos de revisión y el desarrollo de nuevos proyectos orientados por ejemplo a la monitoreo y auditoría de transacciones, inteligencia de negocios, transformación digital, digitalización, entre otros

VI. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- El servicio de Outsourcing del Data Center solicitado por la división de Tecnología de la Información se encuentra dentro del Plan Anual de Contrataciones presupuestado para este año.
- La división de Riesgo Operacional ha definido al servicio de Outsourcing del Data Center como Significativo. Dicho servicio es significativo ya que, en caso de falla o suspensión del servicio, existe un Riesgo Importante que pudiera afectar a los Ingresos, Solvencia, Continuidad Operativa y a la Reputación del Banco.
- El Banco podría verse afectado reputacionalmente ante una interrupción del servicio que paralice la operativa, lo cual podría generar no se brinde atención a los clientes de manera oportuna.
- Dentro de los riesgos operacionales que se pueden generar por el servicio, están los relacionados a las pérdidas económicas por incumplimiento de los compromisos definidos en el contrato con el proveedor, por la inoperatividad y/o interrupción de los servicios del Banco y por el incumplimiento de las políticas de seguridad de información y protección de datos personales por parte de personal del proveedor.
- De la evaluación y control del riesgo operacional, se realizará el seguimiento respectivo en coordinación con la división de Tecnología de Información y el Oficial de Continuidad del Negocio y Seguridad de Información para mitigar cualquier vulnerabilidad. Asímismo, al tener niveles de riesgo moderados y bajo no es necesario la propuesta de planes de acción, pero se realizará el monitoreo respectivo de los eventos que se puedan presentar en el servicio.

- Desde la perspectiva de seguridad de información y continuidad de negocio:
    - Todos los riesgos identificados tienen un plan de tratamiento (anexo 02) orientado a reforzar los controles existentes o crear nuevos con la finalidad de disminuir los niveles de exposición.
    - En el plan de tratamiento, la principal área involucrada es la División de Tecnología de Información, sobre todo para el perfeccionamiento de los TdR, lo cual va a requerir también un aumento del presupuesto asignado.

6.2 Recomendaciones

- La división de Logística debe tener en cuenta que, al tratarse de un servicio significativo, dicho servicio debe contar con un contrato, el cual debe incluir acuerdos de niveles de servicio; establecer claramente las responsabilidades del proveedor y del Banco; establecer la jurisdicción que prevalecerá en caso de conflicto entre las partes; e incorporar los niveles de seguridad de información requeridos.
- El comité de selección debe evaluar adecuadamente que el proveedor cumpla con los requisitos y condiciones mínimas para el adecuado cumplimiento del servicio, esto de la mano con los controles a considerar para mantener un nivel de riesgo bajo.
- La división de Logística en coordinación con el área usuaria (división de Tecnología de Información) debe verificar que se cumplan con los controles descritos en la “Evaluación y Control de Riesgo Operacional” del presente informe y que están considerados en los términos de referencia, los mismos que deberán de ser de cumplimiento para el proveedor. Así mismo, deberá informar si el área usuaria solicitante, proveedor o área Legal, realiza alguna modificación de los términos del contrato.
- El área usuaria solicitante debe comunicar oportunamente los eventos que se pudieran presentar en el servicio, a la división de Riesgo Operacional, para que en conjunto se hagan las gestiones para mitigar los riesgos relacionados. Asímismo, la división de Logística debe mantener el registro del incumplimiento del servicio o contrato por parte del proveedor.
- La división de Logística debe incluir al proveedor dentro del Registro de Proveedores de Servicios Significativos, de acuerdo a lo establecido en el literal d del Art. 14 de la Resolución SBS N° 2116 – 2009 Reglamento para la Gestión del Riesgo Operacional.
    - Desde la perspectiva de seguridad de información y continuidad de negocio:
        - A la División de Tecnología de Información, por intermedio de la GAOF y la Gerencia General, la ejecución de las actividades descritas en el Plan de Tratamiento (anexo 02), y se solicite el presupuesto que requieran las actividades de perfeccionamiento de los TdR principalmente.
        - A la División de Tecnología de Información y Logística, por intermedio de la GAOF, la suscripción del contrato del servicio de outsourcing (con las consideraciones regulatorias comunicadas al área de Logística) de manera que este servicio se encuentre formalmente respaldado y se brinde seguridad acerca de la disponibilidad del sistema core.

- A la División de Tecnología de Información por intermedio de la GAOF y la Gerencia General, efectuar la evaluación de los riesgos y los escenarios posibles respecto al sistema core de Banco para el mediano plazo, aprobándose un plan de acción que considere los presupuestos correspondientes.

- En la medida que el contrato a ser firmado tendrá una vigencia de 10 meses, la división de Tecnología de Información en coordinación con la división de Logística, deberán realizar las gestiones necesarias con la debida anticipación, a fin de mantener la continuidad del servicio.

AGROBANCO
BANCO AGROPECUARIO
César Caballero Samamé
Jefe de Riesgo Operacional

AGROBANCO
BANCO AGROPECUARIO
Luis Alberto Palza Ticona
Oficial de Seguridad de la Información y Continuidad de Negocio

ANEXO 01: MATRIZ DE EVALUACIÓN DE RIESGOS DEL SERVICIO DE OUTSOURCING POR SEGURIDAD DE INFORMACIÓN Y CONTINUIDAD DE NEGOCIO

SUB-PROCESO	ACTIVO DE INFORMACIÓN	COD. AMENAZA	AMENZA	COD. VULNERABILIDAD	VULNERABILIDAD	COD. RIESGO	RIESGOS	PROBABILIDAD	IMPACTO	RIESGO INHERENTE	CONTROLES	OC1	OC2	OC3	OC4	OC5	CDCi	CDC	Calificación del control	Mitiga Probabilidad	Mitiga Impacto	MITT_P	MITT_I	PR	IR	NIVEL DE RIESGO RESIDUAL	NO. PLAN DE TRATAMIENTO (ANX. 02)
Macroproceso principal Macroproceso de apoyo	A009 Servicio de outsourcing de Centro de Datos principal	AM68	Incumplimiento regulatorio del proveedor	VU23	Tablas de claves no protegidas	R01	Sanciones por incumplimiento regulatorio (SBS) por servicios significativos	4	5	Extremo	Términos de referencia del servicio outsourcing	0.9	0.1	0.5	0.5	0.7	**0.54**	**0.527**	**Aceptable**	1	0	0.527	0.17	1.89	4.13	**Alto**	01
		AM43	Acceso no autorizado al sistema	VU24	Mala administración de claves						Bases del proceso	0.9	0.1	0.5	0.4	0.7	**0.52**			1	0						02
		AM69	Pérdida de confidencialidad de datos	VU43	Procedimientos inadecuados de reclutamiento						Contrato del servicio outsourcing	0.9	0.1	0.5	0.4	0.7	**0.52**			1	1						
				VU46	Falta de concientización de seguridad de inf.	R02	Pérdida o divulgación de información de propiedad del Banco	4	4	Extremo	Certificaciones en seguridad de información del prov.	0.9	0.7	0.9	0.9	0.9	**0.86**	**0.620**	**Bueno**	1	0	0.620	0.00	1.52	4.00	**Alto**	01
				VU56	Dispo. inexistentes o insuficientes en contratos						Contrato del servicio outsourcing	0.2	0.1	0.5	0.4	0.7	**0.38**			1	0						
				VU58	Falta de auditorías regulares (supervisión)	R03	Interrupción del proceso de negocio por finalización no planificada del servicio de outsourcing	3	5	Extremo	Términos de referencia del servicio outsourcing	0.9	0.1	0.5	0.5	0.7	**0.54**	**0.440**	**Aceptable**	1	0	0.395	0.18	1.82	4.13	**Alto**	01
				VU62	Inexistencia o incumplimiento de SLA's						Bases del proceso outsourcing	0.9	0.1	0.5	0.4	0.7	**0.52**			1	0						02
				VU68	Falta de planes de continuidad						Contrato del servicio outsourcing	0.9	0.1	0.5	0.4	0.7	**0.52**			1	1						03
											Estrategia de migración	0.2	0.0	0.5	0.0	0.2	**0.18**			0	1						
						R04	Interrupción del proceso de negocio por no contar con contrato suscrito de outsourcing	4	5	Extremo	Términos de referencia del servicio outsourcing	0.0	0.1	0.5	0.5	0.7	**0.36**	**0.295**	**Insatisfactorio**	1	0	0.260	0.12	2.96	4.40	**Extremo**	01
											Bases del proceso outsourcing	0.0	0.1	0.5	0.4	0.7	**0.34**			1	0						02
											Contrato del servicio outsourcing	0.0	0.1	0.5	0.4	0.7	**0.34**			1	1						03
											Estrategia de migración	0.0	0.0	0.5	0.0	0.2	**0.14**			0	1						
Macroproceso principal Macroproceso de apoyo	A010 Sistema IBS	AM70	Interrupción del servicio	VU24	Mala administración de claves	R03	Interrupción del proceso de negocio por finalización no planificada del servicio de outsourcing	3	5	Extremo	Términos de referencia del servicio outsourcing	0.9	0.1	0.5	0.5	0.7	**0.54**	**0.440**	**Aceptable**	1	0	0.395	0.18	1.82	4.13	**Alto**	01
		AM43	Acceso no autorizado al sistema	VU31	No producir informes de gestión						Bases del proceso outsourcing	0.9	0.1	0.5	0.4	0.7	**0.52**			1	0						02
		AM29	Mal funcionamiento del software	VU60	Falta de informes de fallas registradas x adm./ope						Contrato del servicio outsourcing	0.9	0.1	0.5	0.4	0.7	**0.52**			1	1						03
											Estrategia de migración	0.2	0.0	0.5	0.0	0.2	**0.18**			0	1						
						R04	Interrupción del proceso de negocio por no contar con contrato suscrito de outsourcing	4	5	Extremo	Términos de referencia del servicio outsourcing	0.0	0.1	0.5	0.5	0.7	**0.36**	**0.295**	**Insatisfactorio**	1	0	0.260	0.12	2.96	4.40	**Extremo**	01
											Bases del proceso outsourcing	0.0	0.1	0.5	0.4	0.7	**0.34**			1	0						05
											Contrato del servicio outsourcing	0.0	0.1	0.5	0.4	0.7	**0.34**			1	1						
											Estrategia de migración	0.0	0.0	0.5	0.0	0.2	**0.14**			0	1						
Macroproceso principal Macroproceso de apoyo	A001 Base de Datos DB2 - AS400 de producción	AM69	Pérdida de confidencialidad de datos	VU31	No producir informes de gestión	R05	Falta de disponibilidad o corrupción de datos por sobrepasar u operar muy cerca del límite de almacenamiento asignado según términos de referencia	3	4	Extremo	Términos de referencia del servicio outsourcing	0.0	0.1	0.5	0.5	0.7	**0.36**	**0.490**	**Aceptable**	0	1	0.310	0.18	2.07	3.28	**Medio**	04
		AM40	Hacking	VU62	Inexistencia o incumplimiento de SLA's						Procedimiento de descarga de backups	0.9	0.7	0.0	0.8	0.7	**0.62**			1	0						
		AM67	Degradación parcial o total del servicio	VU101	Ausencia o incumplimiento de proc. de backup																							
				VU110	Ausencia de un análisis de Ethical Hacking																							

Participantes

Rafael Coronado Leon – Jefe de Tecnologías de Información
Eduardo Orihuela Paredes – Coordinador de Infraestructura y Comunicaciones
Luis Alberto Palza Ticona – Oficial de Seguridad de Información y Continuidad de Negocio

Fecha

15/06/2022

ANEXO 02: EVALUACIÓN DE RIESGOS DEL SERVICIO DE OUTSOURCING

PLAN DE TRATAMIENTO

NO	Descripción	Responsable	Fecha inicio	Fecha fin
01	Perfeccionamiento de los términos de referencia El objetivo es desta actividad es mejorar los términos de referencia mediante el establecimiento de procedimientos y especificaciones detalladas mediante adendas al contrato a los puntos específicos, como por ejemplo: 3.19.5, 3.28, 3.41, 3.56 entre otros. Esto permitirá evicendiar un mejor nivel de cumplimiento regulatorio sobre todo ante SBS.	T.I.	Fecha de inicio del contrato	Fecha de fin del contrato
02	Inclusión de requerimientos de la normatividad de servicios significativos a bases y contrato A fin de incorporar en las bases y contrato los aspectos regulatorios requeridos por las resoluciones SBS al respecto, el Oficial de SI y CN alcanzará una propuesta al área de Logística la misma que debe ser corroborada tanto por el proveedor(es) como por As. Jurídica.	Riesgos - Seg. De Inf.	--	--
03	Elaborar la estrategia de migración Por cumplimiento regulatorio y los riesgos de continuidad de negocio, es necesario que el área de TI prepare una estrategia en caso ocurra una interrupción del servicio lo cual obligue a analizar posibles cursos de acción ante esta contingencia.	T.I.	Fecha de inicio del contrato	31/07/2022
04	Ampliar el espacio de almacenamiento contratado en el outsourcing El espacio de almacenamiento para el ambiente de producción no ha aumentado desde el 2012 (2.64TB), por lo que la División de TI debe solicitar una vez iniciado el contrato la ampliación del espacio en producción principalmente a fin de asegurar que no se van a presentar errores de procesamiento y se pueda dar viabilidad a otros proyectos de crecimiento y nuevos productos.	T.I.	Fecha de inicio del contrato	Fecha de fin del contrato
05	Formalización del contrato se outosurcing La falta de un contrato y soporte al data center, como se vio en la matriz de riesgos, requiere de atención urgente por el nivel de riesgo extremo en que se encuentra. El área responsable es la División de TI.	T.I.	15/06/2022	30/06/2022