MODELO DE AUDITORÍA A LOS ACUERDOS DE NIVELES DE SERVICIO – ANS QUE SOPORTAN LOS CONTRATOS DE GESTIÓN DE TECNOLOGÍA EN LAS ENTIDADES BANCARIAS COLOMBIANAS

Autores: Elisa Fernanda Ríos Verdugo[1]
Cristian Eduardo Oviedo Rodríguez[2]

Resumen

El presente artículo tiene como finalidad conocer cómo son los ANS pactados entre los proveedores de servicios tecnológicos y las entidades pertenecientes al sector bancario en Colombia, con el fin de definir y establecer los riesgos asociados a la gestión servicios y tecnologías contratada con terceros. Proceso que conformará la base principal para el diseño de un modelo de seguimiento y control del cumplimiento de los contratos establecidos entre las diversas entidades bancarias colombianas y sus proveedores.

Palabras Claves ANS, tercerización, gestión de riesgos, acuerdos, cláusulas contractuales.

Abstract

The purpose of this article is to learn about the ANS agreed between technological service providers and entities belonging to the banking sector in Colombia, in order to define and establish the risks associated with the management of services and technologies contracted with third parties. Process that will form the main basis for the design of a model for monitoring and controlling compliance with the contracts established between the various Colombian banking entities and their suppliers.

Key words: SLA, outsourcing, risk management, agreements, contractual clauses.

Introducción

Actualmente, se está evidenciando en los diferentes medios de comunicación fallas o incidentes materializados en las entidades colombianas en especial en el tipo de entidades bancarias. Una de

[1] Elisa Fernanda Ríos Verdugo, Contadora Pública, estudiante de Especialización en Auditoría de Sistemas de la Universidad Antonio Nariño - erios95@uan.edu.co
[2] Cristian Eduardo Oviedo Rodríguez, Ingeniero de sistemas, estudiante de Especialización en Auditoría de Sistemas de la Universidad Antonio Nariño - coviedo08@uan.edu.co

las causas con mayor impacto se debe al incumplimiento por parte de los terceros que apoyan, soportan y brindan mantenimiento en la operación desarrollada en la gestión tecnológica de las entidades colombianas. De acuerdo con lo anterior, se hace necesario definir unos requerimientos mínimos que permitan validar y dar seguimiento a los acuerdos requeridos para prestar un mejor servicio por parte del tercero y en caso contrarios aplicar lo acordado con el mismo a través de los Acuerdos de Niveles de Servicio – (ANS), eliminando los agujeros legales que puedan permitir incumplimientos por alguna de las partes. Para el análisis y gestión de la información. A continuación, se relacionan el listado de las entidades bancarias:

Tabla 1. Lista de Entidades Bancarias.[3]

ENTIDADES BANCARIAS			
1	Banco de Bogotá S.A.	**15**	Banco Bancamía S.A.
2	Banco Popular S.A.	**16**	Banco W S.A.
3	Banco Itaú CorpBanca S.A.	**17**	Banco Coomeva S.A.
4	Bancolombia S.A.	**18**	Banco Finandina S.A.
5	Citibank Colombia S.A.	**19**	Banco Falabella S.A.
6	Banco GNB Sudameris S.A.	**20**	Banco Pichincha S.A.
7	Banco BBVA Colombia S.A.	**21**	Banco Coopcentral S.A.
8	Banco de Occidente S.A.	**22**	Banco Santander S.A.
9	Banco Caja Social S.A.	**23**	Banco Mundo Mujer S.A.
10	Banco Davivienda S.A.	**24**	Mibanco S.A.
11	Scotiabank Colpatria S.A.	**25**	Banco Serfinanza S.A.
12	Banco Agrario de Colombia S.A.	**26**	Banco J.P. Morgan Colombia S.A.
13	Banco Comercial AV Villas S.A.	**27**	Lulo Bank S.A.
14	Banco Credifinanciera S.A.	**28**	Banco BTG Pactual Colombia S.A.

Fuente: Superintendencia Financiera de Colombia SFC.

Metodología

La Universidad Antonio Nariño, Desde el programa de Especialización en Auditoría de Sistemas solicitará a 28 entidades bancarias una "AUTOEVALUACIÓN PARA LA GESTIÓN DE RIESGOS DE TERCERIZACIÓN" con el propósito de medir el nivel de madurez en gestión de servicios de tercerización para el tipo de entidades mencionadas. La autoevaluación como insumo de información para el Modelo de Auditoría a los ANS debe facilitar el análisis de brechas frente a los requerimientos mínimos establecidos en el marco integral del sistema de administración de

[3] Listado emitido por la Superintendencia Financiera de Colombia - SFC.

riesgos operacional SARO estipulado en la Circular Externa 025 de 2020, la norma ISO/IEC 20000-1 de diciembre de 2018 y normativa Ley 80 de 1993 del Congreso de Colombia 1993.

CAPÍTULO I

ACUERDOS DE NIVELES DE SERVICIO

Los ANS, se pueden describir como un conjunto de parámetros, tiempos y requisitos establecidos a través de un documento similar a un contrato formal entre el proveedor y el adquirente, para la entrega de productos o servicios de un proceso a los usuarios internos y externos, con los cuales se medirá la oportunidad en el cumplimiento de los términos pactados entre las partes.

Los ANS debido a su naturaleza pueden ser generados de formas distintas, dependiendo del sector al cual pertenece la entidad, así como, el servicio o producto obtenido. Algunas características pueden ser más relevantes que otras, aun así, los componentes generales que deben contener son:

Figura 1. Componentes generales de los ANS.

Fuente: Ley 80 de 1993 Congreso de Colombia.[4]

Como un valor agregado los proveedores pueden deben incluir información complementaria relevante como:

I. Compromiso con los usuarios.
II. Niveles de calidad del servicio.
III. Proyectos y servicios.
IV. Planes de innovación constante.
V. Aplicación de la vanguardia tecnológica.

[4] Ley 80 de 1993 del Congreso de Colombia: La ley tiene por objeto disponer las reglas y principios que rigen los contratos de las entidades estatales.

VI. Colaboraciones y alianzas actuales y presupuestadas a futuro.

A pesar de haber establecido como base la información anterior, durante el establecimiento de los ANS es importante establecer la dificultad de prever todas las posibles situaciones que se pueden dar, en la creación del contrato y la posterior puesta en marcha, por lo cual, es normal que surjan poco tiempo después de haber acordado los ANS. También puede ser que la empresa esté atravesando cambios que influyen en el ANS, así mismo, es posible que surja la necesidad de crear nuevas leyes relacionadas con la seguridad de datos, generando la dependencia de modificar algunas de las condiciones establecidas inicialmente, para lo que se requiere realizar una solicitud de cambio. Dependiendo de la naturaleza del cambio, pueden modificarse los ANS, incluso si la duración del contrato aún no se ha establecido. Dentro de los ANS, existen 3 tipos que son implementados por las organizaciones según sus necesidades, reflejados a continuación:

I. ANS de Servicio: Se establecen de forma concreta para determinados servicios, en diferentes niveles de calidad.

II. ANS de Cliente: Son aplicable a cualquier servicio contratado de forma específica por el mismo cliente.

III. ANS Multinivel: Se pueden combinar ANS de cliente y servicio en uno solo, estableciendo a cabalidad las necesidades de las 2 partes.

1.1. Participación de los proveedores de las entidades bancarias colombianas en los ANS.

Las entidades bancarias en Colombia, antes de poder establecer las formas de selección y la contratación de sus proveedores, requieren establecer y cumplir con unas obligaciones mínimas para garantizar mayores niveles de seguridad; igualmente deben determinar la clase de proveedores que están buscando, los requisitos mínimos que deben cumplir y las responsabilidades generales que les serán asignadas.

1.1.1. Requisitos mínimos de las entidades bancarias para la contratación de terceros.

Al interior de las entidades bancarias colombianas se deben determinar de forma anticipada, cuáles son las condiciones que deben cumplir los proveedores según el servicio y los productos que van a ofrecer, para esto es necesario que se cumplan con los siguientes apartados:

Figura 2. Requisitos mínimos de las entidades bancarias para la contratación de terceros.

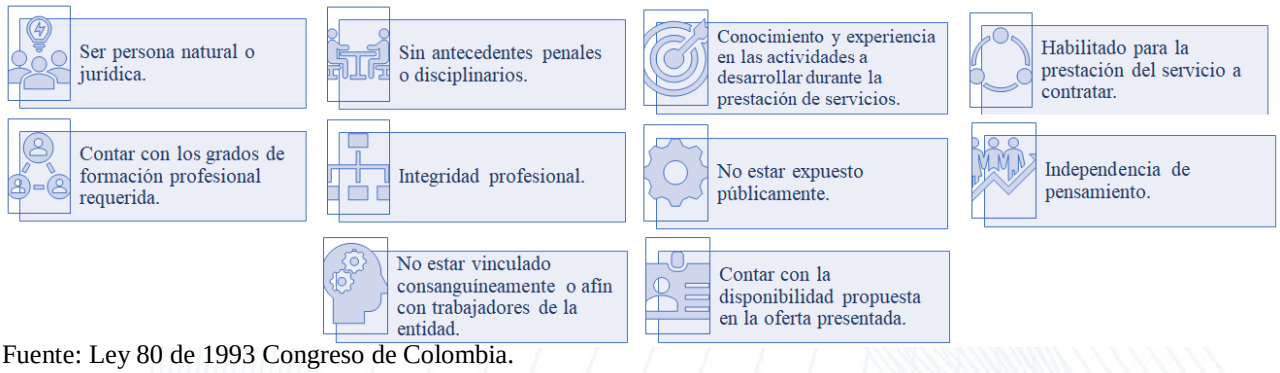
REQUISITOS MÍNIMOS DE LAS ENTIDADES BANCARIAS PARA LA CONTRATACIÓN DE TERCEROS		
Establecimiento de criterios y procesos de selección.	Acordar términos de confidencialidad de la información y establecer parámetros de cifrados.	Controles para documentación, respaldo y/o destrucción de la información con relación a los servicios adquiridos.
Determinar las obligaciones y compromisos entre las partes.	Analizar la vulnerabilidad.	Exigir a terceros planes de contingencia y continuidad debidamente documentados.
Contar con manuales y políticas de seguridad informática.	Fijar límites sobre la propiedad de la información.	Realizar análisis comparativos de vulnerabilidad con servicios pactados previamente.
Realizar un análisis de riesgos.	Restringir el acceso y uso de la información con base a las necesidades de la misma.	Contar con procedimientos establecidos para verificar el cumplimiento de las obligaciones por parte del proveedor.
Pactar los niveles de servicios.	Documentación de los procesos a implementar en caso de fallas, manipulación o alteración de dispositivos computacionales.	Establecimiento de las formas y periodos de pago.

Fuente: ISO 20000-1: 2018 - Sistema de gestión de servicios TI - ICONTEC.[5]

1.1.2. Perfiles de los Oferentes.

Para asegurar que los oferentes dispuestos a presentar propuestas cubran las necesidades mínimas requeridas por las entidades bancarias, se debe solicitar que los proveedores interesados en prestar un servicio específico cumplan con el siguiente perfil:

Figura 3. Perfiles de los Oferentes.



Fuente: Ley 80 de 1993 Congreso de Colombia.

1.1.3. Exigencias mínimas para los oferentes.

Para complementar el cumplimiento de los perfiles de los proveedores es importante poder verificar la legalidad de su constitución y del desarrollo de sus labores, así como, la experiencia y la confianza de los clientes que ya han adquirido sus servicios o productos. Por lo cual entre la

[5] ISO 20000-1: 2018 - Sistema de gestión de servicios TI - ICONTEC.: Especificar los requisitos para el establecimiento, la implementación,
el mantenimiento y la mejora continua de un sistema de gestión de servicios (SGS).

documentación solicitada para la postulación como proveedor de las entidades bancarias debe presentarse:

Tabla 2. Requisitos mínimos para la postulación de terceros.

REQUISITOS MÍNIMOS PARA LA POSTULACIÓN DE TERCEROS	
Carta de postulación de la propuesta con los requisitos mínimos establecidos por el oferente.	Certificación Bancaria cuya expedición no puede ser mayor a treinta (30) días.
Hoja de vida de sus colaboradores.	Copia del Registro Único Tributario RUT.
Documentos que certifiquen su experiencia previa en la prestación de servicios a fin.	Formato de la autorización para la notificación electrónica de las comunicaciones por parte del contratante.
Documento de identidad representante legal.	Composición accionaria.
Presentación y suscripción al Compromiso Anticorrupción	Autorización de tratamiento de datos personales.
Registro del revisor fiscal en caso de estar obligado.	Antecedentes de la Contraloría, Procuraduría y Policía Nacional.
Certificado de Existencia y Representación Legal: Expedido por la Cámara de Comercio respectiva no mayor a 30 días.	Que tenga dentro de su objeto social el desarrollo de actividades iguales o similares a las del objeto de contratación.
El oferente debe formular una oferta económica coherente al servicio que será prestado y sus respectivas características.	Obligación de realizar todas las actividades encaminadas a asegurar que todos sus socios, administradores, clientes, contratistas, empleados, etc., y los recursos de estos, no se encuentren relacionados o provengan de actividades ilícitas.
Certificado de Aportes a seguridad Social, Salud y Pensiones.	

Fuente: DANE.[6]

1.1.4 Obligaciones generales de los oferentes.

Por último, se deben establecer y comunicar mediante un documento formal de cuáles son los deberes básicos de obligatorio cumplimiento dirigidos a los diversos proveedores de los bancos colombianos, dicho documento debe contener las siguientes cualidades:

Tabla 3. Lineamientos de obligaciones generales de los oferentes.

LINEAMIENTOS DE OBLIGACIONES GENERALES DE LOS OFERENTES	
Prestación oportuna del servicio.	Ejecutar a cabalidad los procesos establecidos.
Establecimiento de contactos y medios de comunicación.	Dar cumplimiento a las políticas y requerimientos de la entidad contratante.
Asesorar y proponer las estrategias asociadas al alcance del objeto del contrato.	Garantizar la buena calidad de los bienes o servicios objeto del contrato.
Cumplimiento total de los acuerdos de confidencialidad de la información.	Informar sobre los actos irregulares de los cuales tenga conocimiento, que sean realizados por cualquier persona relacionada con las actividades de la organización.
Información oportuna en los periodos establecidos.	Entregar los informes pactados que cumplan con los requisitos y periodos pactados.
Informar oportunamente la presentación de hechos que dificulten la ejecución del contrato.	Garantizar que el proceso o servicio contratado cuente con los controles necesarios para mitigar los riesgos operacionales asociados al mismo.

[6] DANE: Requisitos para la contratación.

LINEAMIENTOS DE OBLIGACIONES GENERALES DE LOS OFERENTES	
Atender requerimientos de forma oportuna.	Cumplir al Manual de Políticas de Seguridad de la información establecido al interior de la organización.
Realizar el pago correspondiente al sistema de seguridad social.	Disponer de planes de contingencia y continuidad debidamente documentados y aprobados.
Causar, presentar y pagar los tributos resultantes de la relación profesional.	Comprometerse a implementar los planes de mejora que le sean requeridos por el contratante.
Presentar el documento legal correspondiente al cobro de sus servicios según su responsabilidad tributaria.	

Fuente: ISO 20000-1: 2018 - Sistema de gestión de servicios TI - ICONTEC.

CAPÍTULO II

CONTEXTO DE RIESGOS PARA FIJAR ANS EN LAS ENTIDADES BANCARIAS COLOMBIANAS

Las entidades tienen a su cargo el control completo sobre las responsabilidades y los requisitos relacionados con la prestación del servicio por parte de los proveedores, como apoyo del ciclo de vida de los servicios, para ello se deben establecer una serie de criterios para la selección y evaluación adecuada de los terceros oferentes para la prestación de los bienes o servicios requeridos por la entidad. Por lo cual, es necesario que, para cada uno de los servicios externos e internos contratados por la entidad, se establezcan estándares básicos sobre: los procesos, los objetivos, el volumen de trabajo, los límites de acceso y las excepciones que se pueden presentar por alguna de las partes.

En este capítulo se plasmarán los riesgos que presentan en común todas las entidades bancarias colombianas, con el fin de establecer un contexto que permita diseñar un modelo de auditoría a los ANS, adaptable para cada una de las entidades bancarias que tomen la decisión de adoptarlo dentro de su organización. Igualmente, se presentarán los requisitos mínimos que deben ser exigidos a los proveedores oferentes de productos y/o servicios tecnológicos, los perfiles que deben tener y las obligaciones a las cuales se comprometen legalmente al momento de desarrollar su actividad económica al interior de la entidad bancaria que los ha contratado.

2.1. Establecimiento de los riesgos que se pueden presentar en los ANS entre las entidades bancarias colombianas y sus proveedores.

Es importante comprender que no todas las empresas colombianas cuentan con los mismos riesgos, debido a que los procesos, los recursos, los conocimientos, el personal y los proveedores que requieren varían según la actividad económica que desarrollan y el sector al cual pertenecen. Por lo cual, los riesgos que se presentan en los ANS entre las entidades bancarias y los proveedores

se encuentran enfocados en las necesidades que requieren cubrir los bancos, para poder prestar sus servicios de forma continua, asegurando la privacidad de la información, manteniendo la confianza de sus clientes. Teniendo en cuenta lo anterior, se puede establecer que los riesgos que se pueden presentar a nivel de los ANS entre las entidades bancarias y sus proveedores son:

Tabla 4. Contexto de Riesgos.

CONTEXTO DE RIESGOS		
Retraso en el establecimiento del contrato final.	Demora en la iniciación del contrato establecido.	Pérdida de personal calificado o experimentado.
Riesgo de liquidez para obtener recursos para cumplir con el objeto del contrato.	Estimación errada o inadecuada de la propuesta económica realizada por el oferente.	Baja calidad o veracidad de la información suministrada por parte del contratista hacia la entidad.
Incremento no presupuestado de los costos y gastos a incurrir.	Demoras en la entrega de información por parte del contratista.	Revelación de información confidencial del proyecto a un tercero no autorizado.
Indisponibilidad del contratista por pérdida de liquidez o por encontrarse en proceso de insolvencia.	Deterioro de las condiciones de seguridad y orden público que interrumpan la prestación del servicio presencial.	Errores o fallas en la construcción de respuestas y soluciones a fallas de la herramienta para prevención de fuga de información.
Eventos derivados de accidentes laborales, enfermedad profesional, muerte, ausentismo, del personal.	Cambios en la normativa que modifique o impone nuevas obligaciones al contratista.	Falta de idoneidad del personal profesional asignado por el contratista.
Renuncia de uno o varios miembros del equipo profesional dispuesto por el contratista para la prestación de servicio objeto del contrato.	Errores o fallas en la construcción de respuestas y soluciones a fallas de la herramienta para prevención de fuga de información.	Nivel de precisión y confiabilidad de los productos o resultados del contrato.
Daños y perjuicios derivados de fallas del software o errores en la configuración.	Fallas en la ejecución del contrato por inseguridad en zona de ejecución del contrato.	Demora en el tiempo de ejecución del contrato.
Posibilidad que el personal que apoya la ejecución del contrato y que está a cargo del contratista sufra accidentes.	Escasez de la oferta de profesionales que puedan desarrollar las actividades del proyecto	

Fuente: ISO 30001: 2018 - Sistema de Gestión de Riesgos ICONTEC.[7]

CAPÍTULO III

MODELO DE AUDITORÍA A LOS ANS

La Universidad Antonio Nariño, Desde el programa de Especialización en Auditoría de Sistemas solicitará a 28 entidades bancarias una "*AUTOEVALUACIÓN PARA LA GESTIÓN DE RIESGOS DE TERCERIZACIÓN*" con el propósito de medir el nivel de madurez en gestión de servicios de tercerización para el tipo de entidades mencionadas. La autoevaluación como insumo de información para el Modelo de Auditoría a los ANS debe facilitar el análisis de brechas frente a los requerimientos mínimos establecidos en el marco integral del sistema de administración de riesgos

[7] ISO 30001: 2018 - Sistema de Gestión de Riesgos ICONTEC: Emite directrices para gestionar el riesgo al que se enfrentan las organizaciones.

operacional SARO estipulado en la Circular Externa 025 de 2020[8], la norma ISO/IEC 20000-1 de diciembre de 2018 y normativa Ley 80 de 1993 del Congreso de Colombia 1993.

La autoevaluación solicita información de los 1) componentes generales de gestión de riesgos tecnológicos, 2) plan de continuidad del negocio (PCN) y seguridad de la información y ciberseguridad temas orientados desde la perspectiva de gestión de servicios con terceros. Permitiendo, consolidar datos que ayudan a percibir la calidad y mejora continua de los ciclos de gestión de servicios tercerizados entre las entidades y tercero permitiendo evaluar las aristas de documentación, flujo de aprobación entre las partes, capacitación y sensibilización del personal, definición y ejecución de pruebas, estrategias de comunicación, así como, la evaluación a los ANS acordados entre las partes, logrando prepararse y soportar las posibles situaciones de alto impacto que afecten la operación normal de los servicios acordados entre las partes.

3.1. Estructura del modelo de auditoría a los ANS.

La estructura del modelo tiene por objeto proporcionar una evaluación y análisis coherente de los requisitos mínimos exigidos entre las entidades y los terceros que soportan los servicios. A continuación, se detalla la estructura del modelo.

Figura 4. Estructura del Modelo de Auditoría de Niveles de Servicio-ANS

Fuente: Elaboración propia.

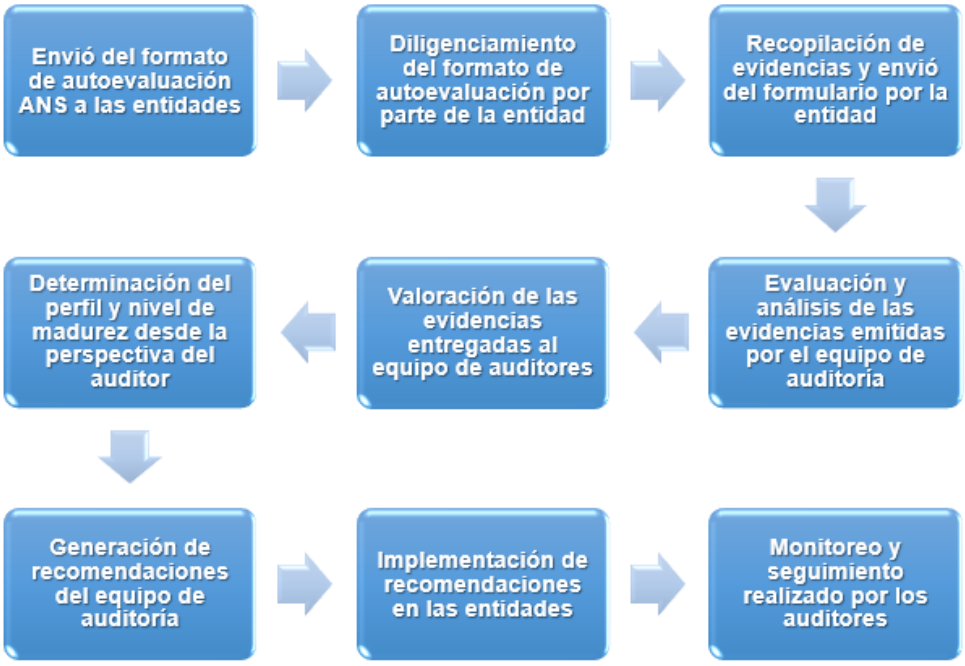
[8] REGLAS RELATIVAS A LA ADMINISTRACIÓN DEL RIESGO OPERACIONAL: En desarrollo de sus operaciones, las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC) se exponen al Riesgo Operacional (RO).

- Antecedentes y necesidades: Se realizó un análisis sobre el contexto actual de las fallas o incidentes materializados en las entidades colombianas en especial en el tipo de entidades bancarias a través de noticias y experiencias de usuario con las plataformas que soportan a los clientes. Evidenciando que en los factores principales se evidencian fallas con los terceros que soportan los servicios con las entidades bancarias.
- Contexto de la organización: Permite evaluar la gestión de riesgos, tecnología y servicios contratados con los terceros que apoyan los procesos críticos de la entidad.
- Insumos del modelo: Diseño de una autoevaluación que permite medir el nivel de madurez de las entidades bancarias alineado a la normativa aplicable y los servicios que prestan los terceros a las entidades bancarias.
- Evaluación y análisis: Validar y medir cualitativamente la posible materialización de los riesgos en la operación de la entidad en relación al incumplimiento de los ANS e indisponibilidades que afectan los intereses de la entidad.
- Valoración y recomendaciones: Asignar una calificación a cada uno de los Ítems evaluados según su nivel, bajo las directrices establecidas, para posteriormente realizar la emisión de recomendaciones orientadas al fortalecimiento de controles y estrategias que debe implementar las entidades con el propósito de mitigar posibles escenarios de indisponibilidad de servicio frente a los consumidores financieros.
- Monitoreo y Seguimiento: La entidad debe implementar y remitir un cronograma en el cual relacione la implementación de las recomendaciones en un periodo a corto, mediano y largo plazo, el cual será verificado periódicamente.
- Mejora continua: Una vez implementadas las recomendaciones se debe mantener un comportamiento cíclico sobre el monitoreo y seguimiento de las directrices emitidas.

3.2. Fases de implementación del modelo de auditoría a los ANS.

Las entidades deben mejorar continuamente en la conveniencia, adecuación y eficacia de los servicios contratados con los terceros. Para determinar los criterios de evaluación a aplicar a las oportunidades de mejora del modelo este debe cumplir con las siguientes fases:

Figura 5: Fases de implementación del modelo de auditoría a los ANS.



Fuente: Elaboración propia

- Envió del formato de autoevaluación ANS a las entidades: Se pondrá a disposición de las entidades bancarias el formato "*Autoevaluación para la gestión de riesgos de tercerización.xlsx*" (anexo 1) A través de correo electrónico adjuntando la comunicación *"Proforma comunicación de envió autoevaluación"* (anexo 2) el cual, se ha sido diseñado para recolectar toda la información relacionada con los ANS. Esta autoevaluación, será remitida a todas las entidades por parte de la Universidad Antonio Nariño en la primera semana de junio de 2022. Las entidades bancarias tendrán (30) días calendario, para atender la autoevaluación.
- Diligenciamiento del formato de autoevaluación por parte de la entidad: Se deben reportar, las generalidades y pasos a seguir para el diligenciamiento de la autoevaluación:
    a. **Pasos a seguir:** Validar el nivel de madurez sobre la gestión de riesgos con los servicios de terceros:
        I. El orden de diligenciamiento del formulario no afecta la valoración. Debe ser contestado en su totalidad y solo se deben diligenciar las casillas en color azul.

II. Para el diligenciamiento se debe tener en cuenta la información contenida en las siguientes tablas:

Tabla 5. Calificación preguntas dicotómicas.

Valor	Nombre	(%)
0	No	0
1	Si	100

Fuente: Elaboración propia.

Tabla 6. Calificación preguntas múltiples.

Valor	Nombre	(%)
1	Débil (D)	25
2	Necesita Mejorar (NM)	50
3	Adecuado (A)	75
4	Fuerte (F)	100

Fuente: Elaboración propia.

Tabla 7. Perfil del nivel de madurez.

Débil:	Las actividades no se ajustan a la normatividad o al perfil de riesgo de la entidad.
Necesita Mejora:	Se tiene un nivel bajo de cumplimiento de las normas y del perfil de riesgo de la entidad; se necesita realizar ajustes para su cumplimiento.
Adecuado:	Se tiene un nivel adecuado de cumplimiento de la normatividad y del perfil de riesgo de la entidad.
Fuerte:	Las actividades exceden el cumplimiento normativo y el perfil de riesgo de la entidad.

Fuente: Elaboración propia.

III. Para cada pregunta se debe seleccionar solo una de las opciones de respuesta.

IV. Al finalizar el diligenciamiento de la información se obtiene automáticamente el porcentaje y calificación. Para las calificaciones Débil y Necesita Mejora, deben implementar planes de tratamiento y fortalecer los controles para adecuar el nivel de madurez.

b. **Glosario de términos**: Detalla los términos generales del léxico de la autoevaluación.

c. **Autoevaluación**: Relación de las inquietudes planteadas para el diligenciamiento de la autoevaluación por parte de las entidades.

- Recopilación de evidencias y envió del formulario por parte de la Entidad: Las entidades deben recolectar las evidencias que soportan cada una de los interrogantes del soporte remitido. con el apoyo de las áreas que respaldan el proceso de contratación de terceros. Este soporte debe ser diligenciado en su totalidad con la mayor honestidad.
- Evaluación y Análisis de las evidencias emitidas por el equipo de auditoría: Una vez recolectada la información remitida, se realiza la evaluación y análisis para cada una de las entidades. Se realiza una dispersión por pregunta y se parametriza una recomendación asociada a cada interrogante, este aplica para las inquietudes atributos dicotómicos con calificación (0%) y las preguntas con múltiples respuestas con calificación (Débil) y (Necesita Mejora) aplica recomendación.

Del total de inquietudes se obtiene el perfil del nivel de madurez para cada entidad con el ánimo de perfilar a cada una. Se comparten las distribuciones de calificación para cada criterio de nivel de madurez:

Tabla 7. Criterios del perfil del nivel de madurez.

Débil:	0% a <30%
Necesita Mejora:	>=30% a <80%
Adecuado:	>=80% a <90%
Fuerte:	>=90% a 100%

Fuente: Elaboración propia.

Una vez realizada la evaluación y análisis a cada una de las entidades bancarias se realiza una compilación del total de entidades evaluadas para cada una de las inquietudes y realizando segmentaciones de los tres principales componentes 1) generales de gestión de riesgos tecnológicos, 2) plan de continuidad del negocio y 3) seguridad de la información y ciberseguridad estas orientadas a la gestión de servicios de tercerización y captar el nivel de madurez por entidad y tipo de sector financiero.

- Valoración de las evidencias entregadas al equipo de auditores: Tomando como base la información proporcionada por la entidad, se convierte en una actividad indispensable validar y analizar la veracidad y los niveles de importancia de las evidencias que han sido recopiladas.
- Determinación del perfil y nivel de madurez desde la perspectiva del auditor: Según las calificaciones asignadas, se debe establecer el nivel de madurez de la entidad, con

base a la información y los soportes recolectados, estableciendo las necesidades y los procesos que se deben implementar.

- Generación de recomendaciones del equipo de auditoría: Se remiten el soporte *"Formulario Recomendaciones entidades Bancarias.xlsx*" (anexo 3). A través de correo electrónico anexando la "*Proforma comunicación de envió recomendaciones*" (anexo 4). a las entidades bancarias, con el fin de presentar acciones de mejora que se ajustan a las necesidades actuales de la entidad.
- Implementación de recomendaciones en las entidades: La entidad bancaria debe establecer un cronograma, en el cual relacione los periodos de tiempo que utilizaran para la implementación de las recomendaciones que les han sido asignadas.
- Monitoreo y Seguimiento realizado por los auditores: *"Formulario Recomendaciones Entidades Bancarias.xlsx*" (anexo 3). Se realiza el seguimiento a cada entidad sobre la implementación de las recomendaciones, para robustecer el perfil del nivel de madurez obtenido para cada entidad.

Conclusiones

- Con el fin de controlar y asegurar la selección adecuada de los proveedores demandados por las entidades bancarias se deben determinar, aplicar y actualizar periódicamente los requisitos mínimos correspondientes para la contratación y renovación de cada uno de los servicios adquiridos a través de segregación de funciones con proveedores externos; convirtiéndose en una acción necesaria la determinación de los servicios específicos operados en cada una de las relaciones establecidas con los terceros, así como decretar: los objetivos a cumplir, los procesos que serán llevados a cabo, los límites que han sido establecidos por los oferentes y ofertantes y los compromisos de cumplimiento que han sido realizadas por cada una de las partes.
- La aplicación del modelo de auditoría para los ANS propuesto en este artículo, les permitirá a las entidades bancarias evaluar la gestión desarrollada, a través del establecimiento de calificaciones a componentes específicos relacionados con los riesgos de tercerización, para posteriormente seleccionar y aplicar las recomendaciones de mejora adecuadas con base en los resultados obtenidos.

Referencias

- Circular externa 025 de 2020, Superintendencia Financiera de Colombia.
- ISO 20000-1: 2018 - Sistema de gestión de servicios TI - ICONTEC.
- Listado de entidades bancarias SFC: https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/13070/f/0/c/0#Lista%20de%20Entidades
- Secretaría Jurídica de la Alcaldía Mayor de Bogotá D.C. (1993). Ley 80 de 1993 Nivel Nacional. Diario Oficial. http://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=304
- DANE: https://www.dane.gov.co/index.php/convocatorias-y-contratacion/informacion-laboral/requisitos-para-la-contratacion
- ISO 30001: 2018 - Sistema de Gestión de Riesgos ICONTEC

Anexos

1. Autoevaluación para la gestión de riesgos de tercerización.

COMPONENTES GENERALES DE GESTIÓN DE RIESGOS TECNOLÓGICOS	
1	¿La Entidad cuenta con procedimientos y criterios idóneos en el proceso de selección de los Terceros y servicios que serán atendidos por estos?
2	¿En la Entidad se realizan estudios previos sobre las necesidades de servicios contratadas con terceros?
3	¿Dentro del presupuesto de la Entidad, se encuentra establecido algún rubro para el establecimiento de ANS con Terceros?
4	¿La alta gerencia se mantiene informada de los ANS establecidos con los Terceros?
5	¿Cómo considera los canales de difusión para emitir las propuestas a los oferentes?
6	¿La Entidad cuenta con un comité en el cual evalúen las propuestas de los oferentes?
7	¿Qué tan activa es la participación de la Junta Directiva al momento de seleccionar los Terceros a contratar?
8	Califique la gestión del comité a cargo de negociar y establecer los ANS
9	¿Considera que existen vacíos legales en alguno de los ANS establecidos actualmente al interior de la Entidad?
10	¿Qué tan adecuada es la identificación de los riesgos tecnológicos y de tercerización?
11	¿Son adecuados los esquemas existentes actualmente para la creación y establecimiento de los ANS?
12	¿Qué tan apropiado es el seguimiento y monitoreo a los servicios prestados por los Terceros?
13	¿La Entidad realiza monitoreo de los riesgos y controles frente a los servicios prestados por los Terceros?
14	¿Los Terceros conocen las actividades y procedimientos para efectuar cambios en la operación?
15	¿Los Terceros cuentan con canales para reportar eventos de riesgo?
16	¿Qué tan adecuadas son las herramientas tecnológicas para monitorear los principales ANS acordados con los Terceros?
17	¿Qué tan adecuados son los indicadores definidos por la Entidad para medir la gestión del tercero? (tenga en cuenta si los resultados de los indicadores se consideran para mejorar el cumplimiento de los ANS)
18	¿Qué tan adecuados son los procedimientos, guías, instructivos, etc.… generados por los Terceros orientados a la entrega que compone la infraestructura tecnológica?
19	¿Qué tan adecuados son los procedimientos para realizar el monitoreo del cumplimiento de los ANS por parte de los Terceros?
20	¿Qué tan calificado y capacitado se encuentra el personal de la Entidad en la creación y establecimiento de ANS?
21	¿Qué tan adecuada es la gestión del personal encargado de establecer los ANS con los Terceros?
22	¿Qué tan adecuada es la gestión del personal encargado de la supervisión de los contratos pactados con los Terceros de tecnología?
23	¿El personal que supervisa los contratos de tecnología cuenta con conocimientos orientados a la gestión tecnológica?
24	¿La Entidad cuenta con un GAP de incumplimientos de los ANS reiterativos?

PLAN DE CONTINUIDAD DEL NEGOCIO (PCN)	
25	¿Los ANS establecidos en la Entidad tienen alguna relación con el PCN?
26	¿Se cuenta con grupos de trabajo que apoyan efectivamente la gestión del PCN?
27	¿El BIA tiene contemplado dentro de sus ítems el papel de los ANS con relación al bienestar de la organización?
28	¿Qué tan adecuada es la definición de los roles del tercero para la gestión del PCN?
29	¿Los contratos acordados con los Terceros cuentan con cláusulas asociadas a la gestión del PCN?
30	¿Los Terceros cuentan con procedimientos efectivos para la respuesta a eventos que puedan afectar la Entidad?
31	¿Qué tan adecuadas son las pruebas realizadas con el tercero para probar la efectividad del PCN? (tenga en cuenta si en las pruebas realizadas se incluyen, entre otros, ataques cibernéticos y eventos catastróficos)
32	¿Los cambios de infraestructura tecnológica son reportados a los Terceros que apoyan los procesos críticos de tecnología?
33	¿La Entidad cuenta con un comité de gestión de cambios que involucre los Terceros?
34	¿Qué tan adecuado es el reporte por parte de los Terceros en los escenarios en que realizan cambios en la infraestructura tecnológica?
35	¿En los escenarios en que se presentan indisponibilidades los Terceros reportan los eventos a la Entidad?

PLAN DE CONTINUIDAD DEL NEGOCIO (PCN)	
36	¿Cómo ha sido la prestación del servicio durante los eventos que afectaron a la Entidad por más de una hora, en el último año?
37	¿Qué tan ajustado se encuentra el RTO de los procesos críticos frente a las promesas de servicio de los Terceros que soportan la operación en la Entidad?
38	¿Los Terceros que soportan servicios críticos cuentan con un CPD y CAPD?
39	¿El CPD y CAPD del tercero está certificado en estándares reconocidos internacionalmente, tales como ANSI/TIA 942 TIER 3 o superior, ICREA u otro, que confirme, al menos, un nivel de disponibilidad del 99.95%?
40	¿Qué tan apropiadas son las evaluaciones que se realizan a los Terceros involucrados en los procesos críticos de la Entidad respecto de la gestión del PCN? (tenga en cuenta la periodicidad con la que se realizan dichas evaluaciones)

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	
41	¿Dentro de los ANS establecidos con Terceros de servicios tecnológicos se han establecido cláusulas directamente relacionadas con la ciberseguridad?
42	¿El personal calificado en temas relacionados con la ciberseguridad, se involucra en el establecimiento de los ANS con Terceros tecnológicos?
43	¿Qué tan adecuados son los procedimientos para la identificación de amenazas y vulnerabilidades por parte de los Terceros que apoyan la operación?
44	¿Los Terceros que apoyan la operación cuentan con herramientas actualizadas para la prevención, protección, detección y recuperación de ataques cibernéticos?
45	¿Qué tan apropiadas son las evaluaciones que se realizan a los Terceros involucrados en los procesos críticos de la Entidad respecto de la gestión de la seguridad y la ciberseguridad? (tenga en cuenta la periodicidad con la que se realizan dichas evaluaciones)
46	¿Qué tan adecuados son los procedimientos para la gestión de incidentes cibernéticos con Terceros tecnológicos en la Entidad?
47	¿Los terceros reportan los incidentes de seguridad de la información y ciberseguridad a la Entidad?

2. Proforma comunicación de envió autoevaluación.

Doctor
Juan Carlos Mora Uribe
Presidente
Bancolombia S.A
Carrera 48 No. 26 - 85 Avenida Los Industriales
Medellín

Número de Radicación: xxxxxxxxx-xxxx-xxx
Trámite: Comunicación Oficial
Actividad: Requerimiento a la entidad

Asunto: Autoevaluación de Gestión de Tercerización.

Respetado doctor Mora:

Con el propósito de compilar la información de los riesgos y gestión que pueda afectar los servicios de tecnología prestados por los terceros, la universidad Antonio Nariño solicita a las entidades bancarias con el propósito de validar el nivel de madurez en la gestión de tercerización.

Por esta razón, se remite el documento *"Autoevaluación para la gestión de riesgos de tercerización*" esta deberá ser remitida en 30 días hábiles a esta Universidad.

Finalmente, cualquier inquietud que se genere por la presente comunicación será resuelta por Fernanda Ríos Verdugo o Cristian Eduardo Oviedo Rodríguez, en los correos: erios95@uan.edu.co y coviedo08@uan.edu.co respectivamente.

Cordialmente,

Especialistas de Auditoría de Sistemas
Universidad UAN

3. Formulario Recomendaciones Entidades Bancarias.

COMPONENTES GENERALES DE GESTIÓN DE RIESGOS TECNOLÓGICOS	
1	Se deben establecer criterios y procedimientos idóneos para la selección de los servicios que deben ser suplidos por Terceros y los requerimientos para los Terceros seleccionados.
2	Implementar estudios previos sobre las necesidades de la Entidad para posterior contratación de Terceros.
3	Adecuar el presupuesto anual de la Entidad, incluyendo los costos y gastos que genera la Entidad de acuerdo a los nuevos servicios a contratar con terceros o renovación de los mismos.
4	Informar periódicamente a la alta gerencia el establecimiento o modificación de los ANS con los Terceros.
5	Ampliar los medios de comunicación de las ofertas de tercerización, para asegurar que se presente una mayor cantidad de oferentes para la selección del proveedor más adecuado según las necesidades de la Entidad.
6	Crear un comité dirigido a la revisión, análisis, aprobación y selección de la propuesta que más se adapte a las necesidades de la Entidad.
7	Realizar una sensibilización a la Junta Directiva en relación al proceso de contratación de Terceros que prestan servicios tecnológicos. Con el ánimo de validar el cumplimiento y seguimiento a estos.
8	Realizar capacitaciones a los miembros del comité a cargo de los ANS para mantener actualizados sus conocimientos y criterios establecidos en los procedimientos de la Entidad.
9	Verificar y analizar los ANS actualmente estipulados en la Entidad y actualizarlos según se genere la necesidad o cambios en la operación.
10	Actualizar y aplicar periódicamente los criterios de identificación de los riesgos y tecnológicos. Por lo menos una vez al año.
11	Actualizar los modelos existentes en la Entidad para el establecimiento y actualización de los ANS con terceros.
12	Realizar adecuaciones al proceso de seguimiento y monitoreo de la Entidad con relación al cumplimiento de los ANS.
13	Establecer la periodicidad para aplicar procedimientos de seguimiento y control de posibles riesgos emergentes relacionados con el servicio prestado por el tercero.
14	Mantener informados a los Terceros sobre los cambios de los procedimientos establecidos con relación a las actividades en las que el tercero se ve involucrado.
15	Establecer los canales oficiales a través de los cuales las Entidades desean establecer comunicación y recibir actualizaciones sobre los riesgos que se presentan con la presentan con la prestación del servicio.
16	Verificar, analizar y adecuar las herramientas tecnológicas que tiene la Entidad para monitorear los ANS existentes.
17	Implementar mecanismos de gestión de Terceros y establecer umbrales aplicables al incumplimiento de los mismos.
18	Actualizar la documentación referente a los ANS existentes al interior de la Entidad y enfocarlos a las necesidades reales.
19	Actualizar los procedimientos existentes orientados hacia el monitoreo ANS existentes en la Entidad.
20	Capacitar mínimo una vez al año al personal a cargo del establecimiento de los ANS y programas de contratación.
21	Realizar evaluaciones periódicas sobre el desempeño y criterios emitidos sobre los contratos establecidos con los Terceros.
22	Realizar evaluaciones periódicas sobre los procesos y evidencias establecidas en los ANS con el propósito de establecer alineación de los procesos.
23	Implementar programas de sensibilización orientados a los procesos de la Gestión Tecnológica y metodologías de servicios de tercerización.
24	Implementar herramientas o técnicas orientadas al monitoreo sobre los incumplimientos de los ANS.

PLAN DE CONTINUIDAD DEL NEGOCIO (PCN)	
25	El PCN debe alinearse a los ANS vigentes en la Entidad.
26	Implementar grupos de trabajo que evalúen la efectividad de las estrategias contingentes con los Terceros.
27	Actualizar e integrar el BIA a los ANS establecidos con los Terceros.

PLAN DE CONTINUIDAD DEL NEGOCIO (PCN)	
28	Verificar los perfiles de los recursos contratados por el Terceros en relación a los servicios a ejecutar en la Entidad.
29	Implementar cláusulas orientadas al sistema PCN en los contratos acordados para la prestación de servicios.
30	Evaluar los procedimientos establecidos por el tercero para atender eventos que puedan afectar los intereses de la Entidad.
31	Robustecer las pruebas de efectividad del PCN acordadas con los Terceros.
32	Establecer los mecanismos de información con los Terceros, en relación a los cambios de infraestructura tecnológica. En los escenarios que afecte los servicios prestados.
33	Involucrar a los Terceros en los comités de evaluación de cambios sobre la infraestructura tecnológica.
34	Establecer mecanismos de comunicación efectiva con los Terceros. En los cuales notifique cambios de la infraestructura tecnológica de este.
35	Robustecer los mecanismos de comunicación efectiva con los Terceros.
36	Levantar estrategias contingentes eficientes frente a las fallas críticas y parciales presentadas en la Entidad.
37	Realizar una evaluación mínima anual al RTO establecido con los Terceros críticos que apoyan la gestión tecnológica.
38	Los Terceros que prestan los servicios tecnológicos a la Entidad deben contar con un CPD y CAPD.
39	Validar a los Terceros críticos que prestan servicios tecnológicos en la Entidad cuenten con estándares reconocidos internacionalmente.
40	Ajustar la periodicidad de evaluación a las estrategias contingentes con los Terceros.

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	
41	Actualizar las cláusulas existentes en los ANS y estipular los requerimientos necesarios con relación a la gestión de ciberseguridad
42	Involucrar a los expertos de la Entidad sobre ciberseguridad y contar con su apoyo durante el diseño de los ANS.
43	Evaluar y modificar los procedimientos actuales sobre la identificación de vulnerabilidades y amenazas por parte de los Terceros relacionados directamente con la operación.
44	Exigir previa contratación de Terceros críticos que estos cuenten con herramientas actualizadas para la prevención, protección, detección y recuperación de ataques cibernéticos.
45	Robustecer la periodicidad, los criterios y el enfoque con los cuales se debe evaluar la gestión de la seguridad y la ciberseguridad por parte de los terceros.
46	Fortalecer los procedimientos establecidos para la gestión de incidentes cibernéticos con terceros tecnológicos.
47	Evaluar los mecanismos de reporte y los tiempos de servicio referente al reporte de incidentes de ciberseguridad y seguridad de la información.

4. Proforma comunicación de envió recomendaciones.

Doctor
Juan Carlos Mora Uribe
Presidente
Bancolombia S.A
Carrera 48 No. 26 - 85 Avenida Los Industriales
Medellín

Número de Radicación: xxxxxxxxx-xxxx-xxx
Trámite: Comunicación Oficial
Actividad: Requerimiento a la entidad

Asunto: Recomendaciones Gestión de Tercerización.

Respetado doctor Mora:

Me refiero a su comunicación radicada en esta Universidad, con el número de la referencia, mediante la cual Bancolombia S.A, remitió la respuesta al requerimiento relacionado con gestión de riesgos de servicios de tercerización.

Al respecto, una vez analizada la información aportada, solicitamos su acostumbrada colaboración para que su administración atienda las recomendaciones descritas en el archivo adjunto, las cuales están fundamentadas en las mejores prácticas y estándares internacionales relacionados con el tema.

Para efectos de seguimiento que debe realizar esta Universidad. La entidad deberá suministrar trimestralmente el archivo denominado *"Formulario Recomendaciones entidades Bancarias.xlsx*", debidamente diligenciado, iniciando con el reporte a corte septiembre de 2022, dentro de los 10 primeros días calendario del mes siguiente, hasta finalizar las actividades. Los documentos soporte a las medidas implementadas se deben remitir junto con el formulario señalado, indicando a qué recomendación corresponden.

De otra parte, la Auditoría Interna deberá remitir un informe con la evaluación de las acciones implementadas al culminar la adopción de todas las medidas.

Finalmente, cualquier inquietud que se genere por la presente comunicación será resuelta por Elisa Fernanda Ríos Verdugo o Cristian Eduardo Oviedo Rodríguez, en los correos: erios95@uan.edu.co y coviedo08@uan.edu.co respectivamente.

Cordialmente,

Especialistas de Auditoría de Sistemas
Universidad Antonio Nariño