BancoAgrícola
¡Cosechando esperanza!

RNC-401007665

SB ENTIDAD AUTORIZADA REGISTRO # II-050-1-00-0101

INFORME TÉCNICO PERICIAL QUE JUSTIFICA EL USO DEL PROCEDIMIENTO EXCEPCIÓN DE PROVEEDOR ÚNICO PARA LA RENOVACIÓN SERVICIO DE MONITOREO Y RESPUESTA DE CIBERSEGURIDAD (SOC) EN HORARIO 24*7.

Al : Comité de Compras y Contrataciones.

Fecha : 09 de mayo de 2025

Asunto : Informe pericial de justificación de uso del procedimiento Excepción de Proveedor Único para LA RENOVACIÓN DEL SERVICIO DE MONITOREO Y RESPUESTA DE CIBERSEGURIDAD (SOC) EN HORARIO 24*7.

Resumen: El Banco Agrícola de la República Dominicana (BAGRICOLA) actualmente cuenta con un Centro de Operaciones de Seguridad (SOC) externo para Banco Agrícola Dominicano, con el fin de mejorar la gestión y respuesta ante incidentes de ciberseguridad. En el contexto actual de amenazas digitales en constante evolución, la protección de la infraestructura tecnológica de las instituciones financieras necesarios para la mantener la continuidad de las operaciones del negocio y toda nuestra plataforma bancaria. Esta plataforma está centralizada en nuestro SOC la mejora de la capacidad de respuesta ante incidentes, así como los entregables y el personal técnico requerido para su operación exitosa ante protección de amenazas.

En la actualidad, las entidades financieras están expuestas a un número creciente de riesgos asociados a la ciberseguridad debido a la digitalización de sus operaciones y servicios. La protección de la información sensible, así como de los activos y transacciones de los clientes, se ha convertido en un desafío prioritario para el sector. Ante esta realidad, la adopción de tecnologías avanzadas de monitoreo y protección, como los **SOCs (Centros de Operaciones de Seguridad)**, resulta fundamental para asegurar la continuidad operativa y la integridad de los sistemas financieros.

Actualmente, el Banco Agrícola Dominicano cuenta con un área interna de SOC, conformada un personal técnico especializado lo cual, es una base fundamental para el monitoreo en horario laboral. Sin embargo, con el aumento de las amenazas cibernéticas externas, los servicios digitales del Banco y el aumento en su exposición digital, se amerita continuar con un servicio de SOC externo que apoye la Sección de SOC interna del Banco Agrícola. Dicho SOC Externo está monitoreando 24*7, los 365 días al año.

Un SOC externo ofrece una solución robusta y eficiente para enfrentar las amenazas de seguridad, permitiendo a las instituciones financieras enfocarse en su core business sin comprometer la seguridad de sus sistemas. A través de un SOC, se puede mejorar la visibilidad y control sobre los sistemas de la organización, gestionar riesgos de manera proactiva y asegurar el cumplimiento con normativas nacionales e internacionales.

Preámbulo: Dada la situación de la necesidad de un soporte licenciamiento y uso de la plataforma Fortinet y UTM se adquirió mediante el proceso de compras Ref.: BAGRICOLA-CCC-CP-2024-0011, LA CONTRATACIÓN SERVICIO DE MONITOREO Y RESPUESTA DE CIBERSEGURIDAD (SOC) EN HORARIO 24*7. En este proceso anterior fueron seleccionados los servicios de SOC, BIGFIVE a través del proveedor de servicios en República Dominicana seleccionado, IP EXPERT IPX, SRL, por factor de resultar ganancioso del proceso, de ser proveedor y representante en el país y además de reunir las características necesarias para lograr el objetivo.

Para la institución es de sumo interés continuar con el servicio de soporte del proveedor adquirido, ya que el Banco se encuentra trabajando de manera activa y continua en procesos de actualización, incluyendo nuestra plataforma bancaria y nuevos productos, como es el Internet Banking. Nuestro enfoque también incluye plataformas de centralización y de administración de hardware, configuraciones previas y existentes, por lo que cambiar de marca implicaría retrasos significativos sobre los avances logrados y rehacer todo el trabajo hecho.

En vista de lo anterior, se solicita continuar con servicio de SOC Externo BIGFIVE para protección de amenazas a través del representante local autorizado, la empresa IP EXPERT IPX, SRL, la cual actualmente maneja la cuenta de Banco Agrícola. Este servicio solución ya se encuentra implementada con soluciones integradas de nuestra plataforma en producción además de que se encuentra integrada con las 64 localidades a nivel nacional. Esto nos permitirá mantener la configuración actual e integración de los servicios de monitoreos actuales y de esta forma no interrumpir el proceso de los de monitoreo ante una nueva implementación con otro proveedor u otras soluciones.

Base Legal y Técnica para justificación de proceso de excepción.

Las razones legales y técnicas debidamente motivadas que demuestran porque no resulta eficiente ni conveniente realizar un proceso ordinario y que incluya los fundamentos jurídicos de que esta contratación se reconoce como una excepción:

El decreto 416-23, de fecha catorce (14) del mes de septiembre del año dos mil doce (2023) contentivo del reglamento de aplicación de compras y contrataciones de bienes, Servicios y Obras, indica a su vez en los procedimientos especiales / caso de excepción, en su artículo cincuenta y siete (57) establece que serán considerados casos de excepción y no una violación a la ley, las (situaciones) que se detallan a continuación, siempre y cuando se realicen de conformidad con los procedimientos que se establecen en el presente Reglamento:

Artículo 57. Procedimiento de excepción por proveedor único. Establece que el Procedimiento de excepción por proveedor único. Se utilizará este procedimiento para obtener bienes o servicios insustituibles, que solo pueden ser suministrados por una persona natural o jurídica, que es la única opción en el mercado o **que posee la titularidad o derecho del objeto contractual**. Este procedimiento aplica para entregas adicionales del proveedor original que serán utilizadas como repuestos, ampliaciones **o servicios continuos para equipos existentes, programas de cómputos, servicios o instalaciones**. Cuando el cambio de un proveedor obligue a la institución contratante a adquirir bienes o servicios que no sean compatibles con equipos, programas de cómputos, **servicios o instalaciones existentes, utilización de patentes, marcas exclusivas** y tecnologías que no admitan otras alternativas técnicas

Justificaciones de importancia y aspectos técnicos:

Actualmente, el Banco Agrícola Dominicano, es regulado por la Superintendencia de Bancos de la República Dominicana y el Banco Central República Dominicana, dichos reguladores poseen un reglamento de seguridad cibernética y de la información con la resolución: RESOLUCION JM 151101-02, el cual, estipula y exige controles y lineamientos de seguridad cibernética y de la información a las entidades de intermediación financieras, donde se incluye al Banco Agrícola Dominicano. Dicho reglamento dentro de sus artículos exige los siguientes controles relacionados al monitoreo, gestión y respuesta a incidentes de ciberseguridad:

Artículo 30. Gestión de Vulnerabilidades y Amenazas Tecnológicas. Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben establecer un proceso de análisis, monitoreo y evaluación integral de las vulnerabilidades y amenazas tecnológicas a sus sistemas, infraestructuras y procesos tecnológicos, para minimizar la ocurrencia de incidentes

e) **Monitoreo de los Sistemas y la Infraestructura Tecnológica:** Los sistemas y la Infraestructura Tecnológica deben ser monitoreados y revisados continuamente para asegurar el rendimiento de los mismos, reducir la ocurrencia de sobrecargas, identificar vulnerabilidades y detectar posibles intrusiones maliciosas;

Adicional al reglamento de seguridad cibernética y de la información de la Superintendencia de Bancos de la República Dominicana y el Banco Central República Dominicana, el Banco Agrícola Dominicano, es regido por la entidad internacional SWIFT (*Society for Worldwide Interbank Financial Telecommunication*), la misma, es la plataforma que soporta las transferencias de tipo LBRT o de pagos al instante, dicho servicio de transferencias, el Banco Agrícola Dominicano lo ofrece a sus clientes vía el canal digital Internet Banking.

SWIFT, posee un programa de requisitos de seguridad (The Swift Customer Security Controls Framework (CSCF)), que las entidades financieras deben poseer, dentro de esos requisitos, esta el siguiente que se relaciona al servicio de SOC:

Control 5: Monitoreo de eventos de seguridad

- ***Descripción: Este control exige que las entidades implementen la capacidad de monitorear y registrar todos los eventos relevantes relacionados con la seguridad para detectar actividades sospechosas y de riesgo, y para tomar medidas correctivas cuando sea necesario.***

Este servicio SOC está sustentado y es exigido por normativa, tanto por regulaciones locales o nacionales, como internacionales por la naturaleza de los servicios digitales que ofrece una entidad financiera a sus clientes.

Considerandos:

- Que cambiar de proveedor implicaría reconstruir toda la configuración actualmente existente de integraciones entre ambos SOC,
- Que Banco Agrícola tiene establecido un contrato de mantenimiento, soporte y servicios con el SOC EXTERNO ACTUAL BIGFIVE, a través de su representante IP EXPERT IPX, SRL
- Que este representante local IP EXPERT IPX, SRL posee actualmente todos los derechos de SOC Externo actual, BIGFIVE para administrar la cuenta de Banco Agrícola en el contrato existente,
- Que nuestra institución posee actualmente usa el software para la administración SOC externo BIGFIVE como servicio, como único medio para gestionar, monitorear las alertas en tiempo real de todas las conexiones con todas las sucursales y oficinas de servicios,
- Que sin el soporte o servicio adecuado el cual actualmente es gestionado por el SOC EXTERNO BIGFIVE ante un evento o ataque cibernético podría colapsar toda la plataforma convirtiéndola en vulnerable e imposibilitando la operación a nivel nacional,
- Que el uso de estas plataformas y servicios es exigido por los organismos regulatorios y no contar con ellas sería un riesgo inminente ante un atentado cibernético,

- Que cambiar de plataforma y proveedor implicaría meses de trabajo, configuración y pruebas para lograr la implementación y se perdería los avances y la estabilidad ya logradas,
- Que cambiar la integración de plataforma mediante el servicio actual implicaría una migración de todos los activos tecnológicos desde la plataforma actual a una nueva plataforma, lo que implicaría el riesgo de pérdida de visibilidad de los activos y el monitoreo,

Recomendación:

Dado que la actual infraestructura de soporte y mantenimiento de nuestra plataforma de conexión con las sucursales funciona de forma estable con el SOC BIGFIVE y que bajo el contrato existente solo posee los derechos de soporte el representante local IP EXPERT IPX, SRL, recomendamos el procedimiento Excepción de Proveedor Único para la contratación y continuidad de los servicios de la plataforma Fortinet de con el proveedor local IP EXPERT IPX, SRL.

Michael Grullon
Administrador de Base de datos, TIC

Ivan Tamariz
Encargado de Ciberseguridad

Jorge Aquino
Director de Desarrollo, TIC

Lucia Rosario
Técnico de Tesorería

Maria Fernanda Aquino
Abogado Perito, Jurídica.

Carlos Brown
Administrador de Redes, TIC

David Marte
Encargado SOC

Delis Ortiz
Analista de Proveedores, TIC

Jose Baez
Enc. De Infraestructura y Datacenter