Informe Técnico de Justificación
PROYECTO CIBERSEGURIDAD INTERNA Y PERIMETRAL
(Marcas FORTINET y CISCO)

25 de octubre de 2021

A: **Comité de Compras**
Banco Agrícola

Comisión de TIC

Asunto: Informe de justificación de *PROYECTO CIBERSEGURIDAD INTERNA Y PERIMETRAL* (Marcas FORTINET y CISCO)

Motivación del proyecto

Banco Agrícola persigue elevar la calidad del servicio brindado a los usuarios y clientes a través del uso de las tecnologías para el desarrollo del campo y la agricultura como eje principal de la institución. Todo esto alineado estrictamente a las regulaciones del sector financiero.

Como parte de los requerimientos establecidos por las normas y regulaciones internas (así como aplicables a las entidades de intermediación financiera) y orientados a mantener la ciberseguridad interna y perimetral, exigidos por el reglamento e instructivo de seguridad cibernética y de la información del Banco Central y la Superintendencia de Banco, se requiere la ejecución del PROYECTO DE CIBERSEGURIDAD INTERNA Y PERIMETRAL, con la finalidad de lograr aplicar los controles necesarios vía las soluciones y equipos de ciberseguridad a adquirir, logrando establecer un nivel de riesgo cibernético aceptable de cara a nuestros clientes y ante los reguladores.

Dada la actual infraestructura tecnológica que posee la institución, a nivel de equipos de telecomunicaciones, ciberseguridad y Datacenter, de las marcas FORTINET y CISCO, recomendamos orientar este PROYECTO DE CIBERSEGURIDAD INTERNA Y PERIMETRAL, para que se adquieran de manera exclusivas estas marcas FORTINET y CISCO.

Considerandos

Considerando: Que nuestra institución cuenta con 64 localidades (Sucursales y oficinas), las cuales cuentan con equipos de marca **FORTINET** (Modelo Fortinet 30E) y de la marca **CISCO** (Switch de acceso Cisco).

Considerando: Que nuestra institución cuenta con un Datacenter equipado predominantemente por infraestructura manufacturada por **FORTINET** y **CISCO**. Más aún, estos fabricantes proveen el 100% de las plataformas de

seguridad interna y perimetral (además de una participación importante en el resto de la infraestructura); equipos que a su vez generaran y gestionan la mayor parte del volumen de información que se procesa en la institución.

Considerando: Que nuestra institución cuenta con una red interna (IDF), compuesta por equipos de la marca **CISCO**.

Considerando: Que nuestra institución cuenta con equipos de protección de seguridad de la marca **CISCO** (modelo ASA y FirePower).

Considerando: Que nuestra institución cuenta con una solución de Antivirus de marca **CISCO** (modelo Cisco AMP).

Considerando: Que con la adquisición de las soluciones y equipos de ciberseguridad de las marcas **FORTINET** y **CISCO**, se garantiza 100% la integración, configuración y visibilidad con las demás soluciones y equipos de la infraestructura tecnológica interna de la institución.

Considerando: Que se ha evaluado el proyecto de ciberseguridad interna y perimetral, el cual, con las marcas **FORTINET** y **CISCO**, se cubre todo el alcance de este proyecto, en el logro de los objetivos a nivel interno y acorde a las regulaciones nacionales del Banco Central y la Superintendencia de Bancos.

DNS

Recomendación

En virtud de nuestra evaluación y comparación técnica, sugerimos la adquisición de una Solución Unificada que nos permita desplegar, como un solo esfuerzo, la adquisición, implementación y actualización de las soluciones y equipos de ciberseguridad de las marcas FORTINET y CISCO.

Esta estrategia nos permite aprovechar en su totalidad los equipos existentes de la infraestructura tecnológica FORTINET y CISCO (soluciones y equipos de telecomunicaciones y ciberseguridad) y a la vez reducir al mínimo el factor de riesgo ante problemas de incompatibilidad que puedan surgir por la integración de distintos fabricantes durante las fases de implementación y migración.

Esta recomendación se fundamenta en los siguientes factores clave:

- **Continuidad de negocio:** Para un proyecto de alta complejidad y envergadura como el que se plantea, reducir los riesgos en la implementación es uno de los factores críticos. Al extender nuestra plataforma sobre tecnologías de fabricantes existentes, la compatibilidad queda asegurada y por tanto se elimina la incertidumbre por posibles fallas en el proceso de integración.

  Esto además nos asegura los siguientes beneficios:

  - Evitar interrupciones y mantener el SLA en los servicios críticos que demanda la institución.
  - El proceso de resolución de problemas es más eficiente debido a que las herramientas de diagnóstico ofrecen mayor visibilidad.
  - La gestión de incidentes que se escalan a través del fabricante se manejan de forma integral con un único punto de responsabilidad que facilita la gestión del lado de nuestra institución.

- **Seguridad:** La integración que nos ofrecen los mismos fabricantes entre todos sus componentes permite que la gestión de vulnerabilidades y el tiempo de respuesta ante incidentes de seguridad sean más eficientes. Debido a que las remediaciones abarcan de forma integral cada uno de los elementos que conforman la solución.

- **Reducción del Costo Total de Adquisición:** La selección los mismos fabricantes para expandir la plataforma actual nos permite extender la vida útil de los equipos existentes, reduciendo así el costo total de adquisición para el proyecto en alrededor de un 15%. Otros factores adicionales son:
    - Reducción en los costos de servicios profesionales por implementación e integración de las nuevas soluciones
    - Reducción en los costos de licenciamiento de software para gestión y monitoreo de los servicios
    - Reducción en los costos de capacitación para el personal que ya maneja la infraestructura existente

- **Implementación simplificada:** Al mantener el mismo núcleo tecnológico tendremos la posibilidad de integrar los nuevos servicios en paralelo sin afectar la operatividad. A la vez se reduce el tiempo y esfuerzo de implementación y migración debido a que se podrá reutilizar la configuración existente.

- **Visibilidad:** La administración centralizada, a partir de la integración de los mismos fabricantes, nos asegura los siguientes beneficios:

    - Nos permite gestionar varias tecnologías desde una interfaz centralizada
    - Reduce el riesgo de que existan elementos fuera del alcance de monitoreo
    - El monitoreo simplificado permite prevenir o anticiparnos a incidentes
    - Facilita el despliegue de actualizaciones y parches críticos
    - Nos permite mantener la trazabilidad de eventos en las soluciones integradas

Referencias:

Los equipos y soluciones que conforman este proyecto, están sustentados y avalados por los siguientes marcos regulatorios y estándares, tanto nacionales, como internacionales:

A. REGULACIÓN NACIONAL

- **REGLAMENTO SEGURIDAD CIBERNETICA Y DE LA INFORMACION**
- **INSTRUCTIVO SEGURIDAD CIBERNETICA Y DE LA INFORMACION**
- **Reglamento Interno de Riesgo Operacional**

B. ESTÁNDARES INTERNACIONALES

- **ISO/IEC 27001**
- **NIST CYBERSECURITY FRAMEWORK**

Por la Comisión Técnica que produce este Informe de Justificación:

Engel Rivas
Director Ciberseguridad

Dirección de Tecnología de la Información y Comunicación (TIC) Bagrícola Más que un banco, un aliado

Dorby Saldedo
Director de Operaciones, TIC