PLIEGO DE CONDICIONES ESPECÍFICAS

SOLICITUD DE PROPUESTA PARA MODALIDAD DE EXCEPCIÓN
MEDIANTE CONTRATACIÓN DIRECTA

REF. BAGRICOLA-CCC-PEPU-2025-0003

CONTRATACION DE LA RENOVACION DE SERVICIOS DE **LICENCIAMIENTO, SUSCRIPCIONES Y/O SOPORTE** RELACIONADOS CON: ***1)*** **SOLUCIONES DE CIBERSEGURIDAD E INFRAESTRUCTURA** QUE SOPORTAN EL CORE BANCARIO, ***2)*** BASE DE DATOS **INFORMIX** Y EL SISTEMA OPERATIVO **REDHAT LINUX ENTERPRISE**, ***3)*** PLATAFORMA DE **MO**NITOREO CENTRALIZADO **MANAGE-ENGINE**, ***4)*** SISTEMAS **EASYBANK** Y **GESTIÓN DE CRÉDITO CARTERA DIGITAL**, ***5)*** SISTEMA DE **GESTIÓN DE COBROS VEOCRM,** Y **6)** ALMACENAMIENTO DE **COPIAS DE SEGURIDAD EN LA NUBE DE HUAWEI.**

Santo Domingo de Guzmán, República Dominicana
Mayo, 2025

23 de mayo del 2025

Señores
IP Expert IPX, SRL
Representante Legal: **Marino Castro González**
Dirección: Calle Francisco Prats Ramírez #810, equina Privada Santo Domingo, D.N.
Teléfono: (809) 532-4262
Email: mcastro@ipexdr.com; cjimenez@ipexdr.com; ps@ipexdr.com

Mediante el presente documento, el Banco Agrícola de la República Dominicana (BAGRICOLA) le notifica la solicitud de propuesta para modalidad de excepción mediante contratación directa del procedimiento de proveedor único el cual se realizará cumpliendo con el debido proceso administrativo reglado por la Ley núm. 340 y sus modificaciones, el Nuevo Reglamento de Aplicación dictado por el Decreto núm. 416-23 y el Manual general de procedimientos de contratación por excepción, con especial énfasis en las particularidades definidas en algunos procedimientos de excepción directos.

El objeto de este procedimiento de excepción por proveedor único Ref. No. BAGRICOLA-CCC-PEPU-2025-0003 para la "CONTRATACION DE LA RENOVACION DE SERVICIOS DE LICENCIAMIENTO, SUSCRIPCIONES Y/O SOPORTE RELACIONADOS CON: **1) SOLUCIONES DE CIBERSEGURIDAD E INFRAESTRUCTURA QUE SOPORTAN EL CORE BANCARIO,** 2) BASE DE DATOS INFORMIX Y EL SISTEMA OPERATIVO REDHAT LINUX ENTERPRISE, 3) PLATAFORMA DE MONITOREO CENTRALIZADO MANAGE-ENGINE, 4) SISTEMAS EASYBANK Y GESTIÓN DE CRÉDITO CARTERA DIGITAL, 5) SISTEMA DE GESTIÓN DE COBROS VEOCRM, Y 6) ALMACENAMIENTO DE COPIAS DE SEGURIDAD EN LA NUBE DE HUAWEI" y en lo adelante encontrará las especificaciones técnicas de los servicios para que pueda preparar su propuesta de forma apropiada, para el **LOTE NO. 1**, según se detalla a continuación:

LOTE No.	SOLUCIONES DE CIBERSEGURIDAD E INFRAESTRUCTURA QUE SOPORTAN EL CORE BANCARIO	UNIDAD DE MEDIDA	CANTIDAD SOLICITADA
1	Sistema MFA (CISCO)	Licencia	1
	Seguridad DNS y Filtrado Web (CISCO)	Licencia	1
	WAF y DNS (Cloudfare)	Licencia	1
	SOC Externo (SOC Externo BigFive)	Servicio	1
	Ciberseguridad interna y perimetral Cisco Fire Power	Licencia	1
	Central Telefónica Cisco (33 centrales en sucursales + 32 oficinas + 385 teléfonos + 2 centrales telefónicas en oficina principal)	Licencia	1
	Switch Fortinet y Forigaste UTM	Licencia	1

Además, en la siguiente ficha encontrará toda la información relacionada con la ejecución de la renovación de las SOLUCIONES DE CIBERSEGURIDAD E INFRAESTRUCTURA QUE SOPORTAN EL CORE BANCARIO. Su oferta deberá ser presentada a más tardar el día **28 de mayo del 2025 a las 4:10 P.M.** a través de cualquiera de los siguientes medios: mediante el Sistema Electrónico de Contratación Pública (SECP-Portal Transaccional), vía correo electrónico a compras@bagricola.gob.do, o de manera presencial en la Unidad Operativa de Compras y Contrataciones del BAGRICOLA, ubicada en la Av. George Washington #601, Santo Domingo de Guzmán, Distrito Nacional.

Atentamente,

Dionisio E Jiménez H.
Unidad Operativa de Compras y Contrataciones
BANCO AGRICOLA DE LA REPÚBLICA DOMINICANA

FICHA PARA SOLICITUD DE PROPUESTA PARA MODALIDAD DE EXCEPCIÓN MEDIANTE CONTRATACIÓN DIRECTA	
1. OBJETO DE LA CONTRATACIÓN	
1.1	**SOLUCIÓN CISCO DUO - MFA** Se requiere la renovación de licencia, soporte y garantía directo del fabricante de las diferentes herramientas de Ciberseguridad del fabricante **Cisco System** del Banco Agrícola de la Republica Dominicana. Por un periodo mínimos de renovación 1 **año.** - 200 licencias de Cisco Duo Essentials edition (formerly MFA) - 1 Cisco Duo Basic Support
1.2	**SOLUCIÓN CISCO UMBRELLA (CISCO SECURE ACCESS)** Se requiere la renovación de licencia, soporte y garantía directo del fabricante de las diferentes herramientas de Ciberseguridad del fabricante **Cisco System** del Banco Agrícola de la Republica Dominicana. Por un periodo mínimos de renovación 1 **año.** - 1 Enhanced Support for Cisco Secure Access - 850 licencias de Cisco Secure Internet Access Advantage - 100 licencias de Cisco Secure Private Access Advantage
1.3	**SOLUCIÓN WAF CLOUDFLARE** Se requiere la renovación de licencia, soporte y mantenimiento del fabricante de las diferentes herramientas de Ciberseguridad del fabricante **Cloudflare** del Banco Agrícola de la Republica Dominicana por un Periodo mínimo de renovación **1 año.** **Application Security Core Advanced** DNS queries 60(MM) / CDN 60(MM) Request WAF Advanced / Advanced DDoS 2 Domains / 2 Advanced Certificate Manager 0.5 TB Mensual Adv Rate Limiting Bot Management Argo API Shield Page Shield **Descripción:** 1. Customer Success Manager (CSM) para apoyo en el proceso y seguimiento puntual de la cuenta a través del pool de soporte premium. 2. Incluir soporte técnico 24x7x365, ticket/email,chat/bot, phone. 3. Prioridad de tráfico en la red de Cloudflare. 4. Incluir capacidad de logs que pueden ser usados para auditoría ISO, SOC, otros e integración con sistemas como SIEM, SOC, etc. 5. La consola debe ser multiusuarios con definición de roles en la misma. 6. Acceso a documentación en línea. 7. Acceso a talleres de capacitación en línea.
1.4	**SERVICIOS SOC EXTERNO**

	Se requiere la renovación del servicio de SOC externo del Banco Agrícola de la Republica Dominicana Periodo mínimo de renovación **12 meses.** ***Servicio de NG-SOC*** - Monitoreo activo 24/7 - Gestión de Alarmas y Alertas - Reportes - 10 Casos de Uso - Detección de Amenazas Internas y Externas - Soporte Multicanal ***Gestión de Vulnerabilidades y Amenazas*** • Pruebas de Penetración (1 Graybox cada 12 meses) ***Servicio Proactivo de Inteligencia de Amenazas*** • Identificación y análisis de ciberamenazas. ***Reportes*** • Informes Mensuales de Eventos Detectados y Operaciones Realizadas • Reuniones Semanales
1.5	**CIBERSEGURIDAD INTERNA Y PERIMETRAL CISCO FIRE POWER** Se requiere la renovación de licencia, soporte y garantía directo del fabricante de las diferentes herramientas de Ciberseguridad del fabricante **Cisco System** del Banco Agrícola de la Republica Dominicana Periodos mínimos de renovación **1 año**. ***Cisco Secure Firewall de Ultima Generación para perímetro Interno*** - 2 x Licencias Cisco FPR2110 Threat Defense Threat and Malware - 1 x Licencia Cisco Firepower Management Center - 2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades). - ***Cisco Secure Firewall de Ultima Generación para Centro de Datos*** - 2 x Licencias Cisco FPR2130 Threat Defense Threat and Malware - 2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
1.6	**CENTRAL TELEFÓNICA CISCO (33 CENTRALES EN SUCURSALES + 32 OFICINAS + 385 TELÉFONOS + 2 CENTRALES TELEFÓNICAS EN OFICINA PRINCIPAL)** Se requiere la renovación de licencia, soporte y garantía directo del fabricante de las diferentes herramientas de telecomunicación del fabricante **Cisco System** del Banco Agrícola de la Republica Dominicana Periodos mínimos de renovación **1 año**. ***Cisco Business Edition 6000M***

	- 385 x Licencias EntW On-Premises Calling - 2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades). - 72 x Licencias VMware vSphere Standard 8 o superior - Servicios Profesionales de Upgrade Licenciamiento de Collaboracion ***Cisco Unity Connection*** - 6 x Licencias On-Premises Unity Connection ***Cisco ISR 4331 Datacenter*** - 100 x Licencias CUBE Enhanced Trunk Session - 2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades). ***Cisco ISR 4321 Sucursales*** - 31 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
1.7	**LICENCIAMIENTO Y SOPORTE SWITCH FORTINET Y FORIGASTE UTM** Se requiere la renovación de licencia, soporte y garantía directo del fabricante de las diferentes herramientas de telecomunicación del fabricante **Fortinet** del Banco Agrícola de la Republica Dominicana Periodos mínimos de renovación **1 año**. ***Firewall FortiGate para Perimetro Externo*** - 2 x Licenciamiento UTP - 2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades). ***Firewall FortiGate para VPN Principal*** 2 x Licenciamiento UTP 2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades). ***Firewall FortiGate para VPN Remotas*** 65 x Licenciamiento UTP 65 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades). ***FortiManager para Gestión Centralizada*** 1 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades). ***FortiAnalyzer para Gestión y Almacenamiento de Logs de los NGFW*** 1 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).

	FortiSwitches para Acceso LAN 64 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).

FICHA TECNICA
RENOVACIÓN DE INFRAESTRUCTURA CISCO SYSTEM, CLOUDFLARE, SOC, FORTINET

	ESPECIFICACIONES TÉCNICAS
1	**Solución de Cisco DUO**
1.1	Solución SaaS.
1.2	Se requiere de la solución de autenticación multifactor para proteger a cada usuario y brindar controles básicos de acceso a datos, gestión administrativa avanzada, aprovisionamiento de usuarios, verificación confiable de dispositivos y una experiencia segura de inicio de sesión único.
1.3	Incluye capacidad de Single Sign-On para inicio de sesión federado en aplicaciones SSO con nuestro proveedor de identidad Microsoft
1.4	Proveer funcionalidades de Passwordless para una autenticación segura con un solo gesto en lugar de ingresar una contraseña seguida de MFA.
1.5	Capacidad de diferenciar entre dispositivos corporativos y personales y limitar el acceso a datos confidenciales a dispositivos administrados conocidos.
1.6	Capacidad de proveer verificación de dispositivos confiables, requisitos de aplicaciones y opciones de políticas de registro de dispositivos seguros, y uso de apliacion como método de autenticación
1.7	Funcionalidad de sincronización de directorios para importar usuarios y administradores a la solución requerida desde almacenes de identidad externos de Active Directory, Azure y OpenLDAP.
1.8	Incluir portal de autoservicio que permita la gestión por parte del usuario final de los dispositivos de autenticación de la solución.
1.10	Proporcionar una aplicación de autenticación móvil segura.
1.11	Proveer aprobación rápida y basada en notificaciones push para verificar la identidad de su usuario con soporte para teléfonos inteligentes, relojes inteligentes y tokens U2F.
1.12	Permitir una variedad de otros métodos de autenticación compatibles para satisfacer las necesidades de cada usuario.
1.13	Debe soportar los siguientes métodos de doble factor de autenticación: Push, U2F USB, Biometrico, Token y Passcodes.
1.14	Permitir diferentes opciones de aprovisionamiento de usuarios en la solución propuesta, tales como: sincronización de directorio avanzado, inscripción masiva y auto inscripción de usuarios.
1.15	Capacidad de utilizar API de administración en la solución que nos permita interactuar con los registros de seguridad de la solución para fines de informes y análisis personalizados.
1.16	Entregar un resumen de alto nivel del estado de seguridad de los dispositivos (endpoint) que cada vez que acceden a las aplicaciones.
1.17	Capacidad de limitar el acceso a las aplicaciones en función de las necesidades de seguridad.
1.18	Soportar integración con aplicaciones locales, basadas en la web y basadas en la nube para doble factor de autenticación.
1.19	La solución ofertada debe contar con una
	Entregables
1.20	200 licencias de Cisco Duo Essentials edition (formerly MFA).
1.21	Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus funcionalidades).
2	**Solución de Cisco Secure Access**
2.1	Solución SaaS.

2.11	Se requiere de la solución de seguridad SSE en la nube, basada en confianza cero, que proporcione acceso fluido, transparente y seguro desde cualquier lugar. Con capacidad de SSE (ZTNA, SWG, CASB y FWaaS), además de funciones ampliadas, como VPN como servicio (VPNaaS), DLP integrado en línea y en la nube, Asistente de IA para la creación de políticas y Acceso de IA para visibilidad, control y protección para aplicaciones de IA de terceros.
2.21	La solución debe incluye controles administrativos, estructuras de datos y gestión de políticas comunes que faciliten la interoperabilidad con otros productos de Cisco y de terceros. Tales como integración con una amplia variedad de proveedores de identidad (IDP) SAML, como AD, Azure AD, Okta, Ping, etc, otras soluciones de Cisco, como SD-WAN, XDR y Thousand Eyes (Experience Insights, basado en Thousand Eyes), así como con tecnologías de terceros como Menlo Remote Browser Isolation, Google Chrome Enterprise Browser y AppOmni para SSPM.
2.31	Proporciona acceso seguro granular y específico para aplicaciones privadas en centros de datos locales o en entornos de nube/IaaS. Incluir al menos 100 aplicaciones privadas.
2.41	Provee un diseño de proxy consciente de la identidad con utilización de principios de mínimo privilegio y conocimientos contextuales para denegar de forma granular el acceso de manera predeterminada y otorgar acceso a las aplicaciones cuando la política lo otorga explícitamente.
2.51	Acceso basado en cliente
2.61	Acceso sin cliente (a través del navegador) con capacidad de proteger el tráfico a aplicaciones web (http/https) y aplicaciones privadas con soporte para protocolos SSH y RDP basados en navegador.
2.71	Establece acceso seguro por sesión después de una verificación del estado del dispositivo.
2.10	Capacidad de autenticar a los usuarios a través de un túnel seguro y encriptado, de modo que los usuarios solo ven las aplicaciones a las que tienen permiso de acceso.
2.11	Proporciona acceso remoto transparente y seguro sin exponer las aplicaciones a Internet, ocultando la información de red a los clientes que las usan, evitando el reconocimiento de IP malicioso incluso si un dispositivo ha sido comprometido.
2.12	Implementa políticas de control de acceso específicas del dispositivo.
2.13	Para aquellas aplicaciones privadas que no pueden protegerse con ZTNA, la solución provee la opción VPNaaS, para proporcionar acceso seguro en la nube a todas las aplicaciones privadas, incluidas aquellas que no son compatibles con ZTNA.
2.14	Facilidad de uso para el usuario (siempre en VPN, iniciar antes de iniciar sesión).
2.15	Control de acceso basado en identidad utilizando múltiples métodos de autenticación, incluidos SAML, RADIUS y certificado.
2.16	Soporta integración con Identity Services Engine (ISE), para aprovechar el cambio de autorización (COA) de SGT y RADIUS.
2.17	Capacidad de registrar e inspeccionar todo el tráfico web (http/https) para mayor transparencia, control y protección. Se debera utilizar túneles IPsec, archivos PAC y encadenamiento de proxy para reenviar el tráfico y lograr visibilidad completa, controles a nivel de URL y aplicación, y protección avanzada contra amenazas.
2.18	Filtrado de contenido por categoría o URL específicas para bloquear destinos que violen políticas o regulaciones de cumplimiento.
2.19	Escanea archivos descargados en busca de malware y otras amenazas.
2.20	Incluye capaciad de Sandboxing para analizar archivos desconocidos
2.21	Bloquea tipo de archivo (por ejemplo, bloquear la descarga de archivos .exe).
2.22	Descifrado TLS completo o selectivo para protegerse de ataques e infecciones ocultos.
2.23	Controles de aplicaciones granulares para bloquear actividades específicas del usuario en aplicaciones seleccionadas (por ejemplo, cargas de archivos a Dropbox, archivos adjuntos a Gmail, publicaciones/compartir en Facebook).
2.24	Informes detallados con direcciones URL completas, identidad de red, acciones permitidas o bloqueadas, además de la dirección IP externa.
2.25	Protección multimodo de aplicaciones SaaS basadas en Internet con controles personalizables y opciones de ruta de tráfico.

2.26	Capacidad de detectar, informar y bloquear aplicaciones en la nube seleccionadas en uso, incluyendo IA generativa.
2.27	Bloquea el uso de aplicaciones ofensivas, improductivas, riesgosas o inapropiadas para reducir el riesgo.
2.28	Funciones multimodo para detectar, registrar y controlar las actividades de usuarios/grupos.
2.29	Capacidad de descubrir, bloquear y revocar la autorización de complementos y extensiones riesgosos desde la autorización basada en OAuth para los inquilinos de Microsoft 365 y Google.
2.30	Informar sobre la categoría del proveedor, el nombre de la aplicación y el volumen de actividad de cada aplicación descubierta.
2.31	Proveer detalles de la aplicación e información de riesgo, como puntuación de reputación web, viabilidad financiera y certificaciones de cumplimiento relevantes.
2.32	Proveer restricciones de inquilinos para controlar las instancias de aplicaciones SaaS a las que pueden acceder grupos o individuos.
2.33	Detectar y controlar el uso o intento de uso de más de 720 aplicaciones de IA generativa con capacidad de bloquear el uso o crear e implementar políticas para controlar cómo se usan estas aplicaciones.
2.34	Incluye funcionalidad de Prevención de Pérdida de Datos (DLP) Multimodo con capacidad de analizar datos en línea para proporcionar visibilidad y control sobre la información confidencial que sale de la organización.
2.35	Funcionalidad basada en API en la Prevención de Pérdida de Datos (DLP) para análisis fuera de banda de datos en reposo en la nube. Políticas e informes unificados para una administración más eficiente y el cumplimiento normativo.
2.36	Incluye al menos 1200 identificadores globales integrados para información de identificación personal (PII), que abarcan 77 países, para cumplir con la información de salud personal (PHI), GDPR, HIPAA, PCI y más.
2.37	Identificadores para tokens, claves y secretos de API y sesión de proveedores de servicios en la nube (AWS, GCP, Azure).
2.38	Detectar y eliminar malware de aplicaciones de almacenamiento de archivos en la nube.
2.39	Capacidad de inteligencia artificial generativa que ayude a los administradores de seguridad a ahorrar tiempo, mejorar la eficiencia operativa y reducir la complejidad.
2.40	El asistente de políticas debe es capaz de convertir automáticamente frases conversacionales en inglés en políticas de seguridad específicas.
2.41	Monitorea el estado y el rendimiento de los endpoints, las aplicaciones y la conectividad de red a medida que los usuarios acceden a los recursos.
2.42	Optimiza la productividad del usuario, simplificar la resolución de problemas y reducir el tiempo de resolución de incidentes capturando automáticamente detalles sobre la experiencia integral del usuario, con información integrada basada en IA que ayude a identificar y mitigar proactivamente posibles problemas de rendimiento, garantizando un entorno más resiliente.
2.43	Proporcionar visibilidad total y controles de seguridad integrales para el tráfico entre usuarios y destinos/aplicaciones, en Internet o en la infraestructura privada del Banco, en todos los puertos y protocolos. Incluyendo el acceso de usuarios remotos a Internet o a aplicaciones privadas mientras están en roaming o desde la red de una sucursal.
2.44	Reglas de control de acceso L3/4 para proteger a usuarios/grupos, redes o dispositivos para acceder a Internet, redes privadas y/o aplicaciones privadas.
2.45	Perfiles IPS personalizables compatibles con Snort 3.0 que permita implementar inspecciones IPS por regla en los patrones de tráfico que coincidan con una regla, tanto para acceso a Internet como privado.
2.46	Visibilidad y control sobre aplicaciones de capa 7, protocolos de aplicación y puertos/protocolos, con una base de aplicaciones identificadas en constante crecimiento.
2.47	Descifrar antes de las inspecciones, para el tráfico de Internet o de acceso privado.
2.48	Inspeccionar archivos bidireccional y controles de tipo de archivo para el tráfico entre usuarios y aplicaciones privadas.
2.49	Combinar sandboxing avanzado con inteligencia de amenazas para proteger al Banco del malware.
2.50	Capacidad de detectar métodos de ataque ocultos e informar sobre archivos maliciosos.
2.51	Soporta API para integrar con XDR y SIEM de uso común para enriquecer los datos de seguridad.

2.52	Incluye Aislamiento remoto del navegador (RBI) que permita: ● Aislamiento del tráfico web entre el dispositivo del usuario y las amenazas basadas en el navegador. ● Protección contra amenazas de día cero. ● Controles granulares para diferentes perfiles de riesgo. ● Implementación rápida sin cambiar la configuración del navegador existente. ● Escalabilidad bajo demanda para proteger fácilmente a usuarios adicionales. ● Proteja a los empleados que puedan necesitar acceder a sitios web de riesgo.
2.53	Filtrar en la capa DNS para bloquear solicitudes a destinos maliciosos y no deseados, a través de cualquier puerto o protocolo, antes de que se establezca una conexión a la red o los puntos finales.
2.54	Proteger el acceso a Internet en todos los dispositivos de red, ubicaciones de oficina y usuarios itinerantes y dispositivos móviles.
2.55	Proporcionar informes detallados de la actividad de DNS por tipo de amenaza de seguridad o contenido web y las medidas tomadas.
2.56	Incluir algoritmos de inteligencia artificial que brinden detección y protección en tiempo real contra la exfiltración de datos.
2.57	La solución ofertada debe contar con una garantía directa del fabricante por 12 meses (licencia o suscripción) y con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento en piezas y sus funcionalidades).
	Entregables
2.58	850 licencias Cisco Secure Internet Access Advantage para usuarios finales
2.59	100 licencias Cisco Secure Private Access Advantage para acceso a aplicaciones privadas.
2.60	Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus funcionalidades).
2.61	Servicios Migracion de Cisco Umbrella a Cisco Secure Access
3	**Solución de Cloudflare Application Security Core Advanced DNS**
3.01	Solución SaaS.
3.02	Procesamiento de hasta 60 millones de consultas DNS por mes.
3.03	Capacidad para gestionar hasta 60 millones de solicitudes CDN por mes.
3.04	Web Application Firewall (WAF) avanzado con reglas personalizables y protección contra amenazas de aplicaciones.
3.05	Protección avanzada contra ataques DDoS para dos dominios.
3.06	Soporte para Advanced Certificate Manager con hasta 2 dominios configurados.
3.07	Capacidad mensual de tráfico cifrado y seguro de 0.5 TB.
3.08	Implementación de Advanced Rate Limiting para gestionar y controlar el tráfico basado en umbrales personalizables.
3.09	Gestión avanzada de bots con detección y mitigación basada en aprendizaje automático.
3.1	Argo Smart Routing para mejorar la latencia y la conectividad a través de rutas óptimas.
3.11	API Shield para proteger las interacciones de API mediante autenticación de tokens y esquemas de validación.
3.12	Page Shield para monitorear y proteger contra ataques de tipo Magecart en scripts de terceros.
	Entregables
3.13	1 x Application Security Core Advanced DNS queries 60(MM)/ CDN 60(MM) Request WAF Advanced / Advanced DDoS 2 Domains / 2 Advanced Certificate Manager 0.5 TB Mensual Adv Rate Limiting Bot Management Argo API Shield Page Shield
3.14	Servicios profesionales de afinación de la solución
3.15	Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus funcionalidades).
4	**Cisco Secure Firewall de Ultima Generación para Perimetro Interno**
4.01	Dos (2) Firewalls de última generación o NGFW (ambos instalados en el perímetro de la red empresarial de Banco Agrícola) e instalados bajo el esquema de alta disponibilidad (HA).

4.02	El sistema operativo del equipo es de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Firewall.
4.03	Los Cisco Secure Firewall son un equipo dedicado solo para estos fines.
4.04	Los Cisco Secure Firewall entregan un rendimiento de Firewall de al menos 3 Gbps, NGFW de 2.3 Gbps y NGIPS 2.3 Gbps.
4.05	Los Cisco Secure Firewall cuentan con 12 interfaces de red Ethernet (RJ45) y 4 x SFP integrada.
4.06	Soporta un mínimo de sesiones simultáneas, con AVC de un (1) millón.
4.07	Soporta un mínimo de nuevas conexiones por segundo, con AVC de 14K.
4.08	Entrega un rendimiento de inspección de trafico cifrado (TLS) de 365 Mbps.
4.09	Cuenta con al menos una interfaz dedicada para la administración del hardware.
4.10	Cuenta con al menos un puerto serial o consola de administración.
4.11	1 Rack Unit.
4.12	Capacidad de administración local.
4.13	Capacidad de ser administrada de forma centralizada, que entregue una configuración, registro (Logging), la supervisión (monitoring) y los informes (report) de forma centralizado.
4.14	Incluye solución de administración centralizada Cisco Secure Firewall Management Center con la capacidad de administrar un mínimo de diez (10) equipo de seguridad (NGFW).
4.15	La solución Cisco Secure Firewall Management Center tiene la capacidad de correlacionar eventos de seguridad de los equipos de seguridad (NGFW) integrado a la plataforma.
4.16	Puede administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y otro) desde cualquier equipo conectado a la red que tenga un browser (Edge, Internet Explorer, Mozilla, Firefox, Chrome) instalado sin necesidad de instalación de ningún software adicional.
4.17	Capacidad de correlacionar todos los eventos de intrusión con un impacto del ataque, y entregar al operador qué necesita atención inmediata.
4.18	Entrega un perfilamiento de seguridad de los hosts (IP) de la red, a través del descubrimiento de dispositivos pasivos, incluido el sistema operativo, las aplicaciones de cliente y servidor, las vulnerabilidades, el procesamiento de archivos y los eventos de conexión, etc.
4.19	Habilidad de adaptación automática de las defensas a los cambios dinámicos en la red, en archivos o con hosts. Esto cubre ajuste de reglas de NGIPS y la política de firewall de red.
4.20	Habilidad de correlacionar las actividades de la red y de los hosts (dispositivos finales) mediante más de 1,000 indicadores de compromisos basado en comportamiento.
4.21	Proporciona análisis y protección de amenazas contextuales completos, con conocimiento de los usuarios, historial de usuarios en cada máquina, dispositivos móviles, aplicaciones del lado del cliente, sistemas operativos, vulnerabilidades y amenazas.
4.22	La funcionalidad de IPS de próxima generación cuenta con conciencia contextual en tiempo real y mapeo de red.
4.23	Capacidad de hacer recomendaciones de políticas de NGIPS para garantizar de forma correcta los ajustes de las reglas de detección y prevención de intruso.
4.24	Capacidad de realizar análisis continuo y retrospección de archivo o detección, más allá del horizonte de eventos (punto en el tiempo).
4.25	Habilidad de detectar, alertar, rastrear, analizar y remediar de manera retrospectiva el código malicioso (malware) avanzado que al principio puede parecer limpio o que evade las defensas iniciales y luego se identifica como malicioso.
4.26	Capacidad de mapear cómo los hosts transfieren archivos, incluidos los archivos de malware, a través de su red.
4.27	Habilidad para ver si se bloqueó la transferencia de un archivo o si el archivo se puso en cuarentena. Que permita proporcionar un medio para determinar el alcance, proporcionar controles de brotes e identificar al paciente cero.
4.28	Incluye sandboxing dinámicas integradas.
4.29	Habilidad de comprender, analizar y contener rápidamente un ataque activo incluso después de que suceda.

4.30	Debe ser posible obtener una visualización completa del alcance de una amenaza o ataque ya exitoso, como también contener, bloquear o poner en cuarentena.
4.31	Permita implementar políticas de seguridad de cumplimiento de acuerdo con criterios, como sistema operativo, aplicaciones (Web y Cliente) y protocolos de red.
4.32	Capacidad de realizar línea base (base line) de tráfico de la red de acuerdo con definición de la red, host, servicio, otros.
4.33	Permita tomar acciones de acuerdo con los eventos de violaciones de cumplimientos.
4.34	Cuenta con reportes predefinidos por el fabricante.
4.35	Permite crear o personalizar reporte de seguridad y red, de acuerdo con malware, aplicaciones, intrusión, etc.
4.36	Permite descargar o exportar los reportes de seguridad generado en la solución.
4.37	Permite enviar reportes de seguridad a un repositorio externo.
4.38	Permite almacenar reportes de seguridad de forma local.
4.39	Entrega los reportes en formato de archivo de al menos PDF, HTML y CSV.
4.40	El Threat Intelligence es Cisco Talos.
4.41	Cuenta con Inteligencia de amenazas e interdicción, Investigación de detección, Ingeniería y desarrollo, Investigación y descubrimiento de vulnerabilidades, Comunidades, Alcance global y Repuesta a Incidente directamente del Centro de Inteligencia de Amenazas de la solución propuesta.
4.42	Capacidad de enviar alerta vía SNMP, Syslog y correo electrónico.
4.43	Envia alertas de eventos de intrusión, tales como: - El host de origen o destino está potencialmente comprometido por un virus, un troyano u otra pieza de software malicioso. - El host de origen o destino está en la red y se establece una vulnerabilidad al host - Entre otros.
4.44	Envia alertas de acuerdo con parámetros de redes, tales como: cliente, host, puerto, protocolo, entre otros.
4.45	Capacidad de enviar alertas de eventos de malware.
4.46	Permite al operador especificar de forma granular las alertas de amenazas a recibir vía correo electrónico, es decir, especificar cuáles reglas de NGIPS desea recibir las alertas.
	Entregables
4.47	2 x Licencias Cisco FPR2110 Threat Defense Threat and Malware
4.48	1 x Licencia Cisco Firepower Management Center
4.49	2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
5	**Cisco Secure Firewall de Ultima Generación para Centro de Datos**
5.01	Dos (2) Firewalls de última generación e instalados bajo el esquema de alta disponibilidad (HA).
5.02	El sistema operativo de los Cisco Secure Firewall es de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de IPS.
5.03	Los Cisco Secure Firewall es de un equipo dedicado solo para estos fines.
5.04	Capacidad para crecer y escalar a una arquitectura de seguridad integral en el perímetro externo.
5.05	Entrega un rendimiento de firewall de 10 Gbps, NGFW de 5 Gbps y NGIPS 5 Gbps.
5.06	Cuenta con 12 x 10M/100M/ 1GBASE-T interfaces Ethernet (RJ- 45) y 4 x 10 Gigabit (SFP+) interfaces Ethernet integrada.
5.07	Soporta un mínimo de sesiones simultáneas, con AVC de dos (2) millones.
5.08	Soporta un mínimo de nuevas conexiones por segundo, con AVC de 27K.
5.09	Entrega un rendimiento de inspección de trafico cifrado (TLS) de 735 Mbps.
5.1	Fuente de corriente redundante.
5.11	Cuenta con al menos una interfaz dedicada para la administración del hardware.
5.12	Cuenta con al menos un puerto serial o consola de administración.
5.13	1 Rack Unit.
5.14	Funcionalidades de NGFW

5.15	Capacidad de administración local.
5.16	Capacidad de ser administrada de forma centralizada, que entregue una configuración, registro (Logging), la supervisión (monitoring) y los informes (report) de forma centralizado.
	Entregables
5.17	2 x Licencias Cisco FPR2130 Threat Defense Threat and Malware
5.18	2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
6	**Cisco Business Edition 6000M**
6.01	Cisco Business Edition 6000 en alta disponibilidad (2 nodos) para ofrecer a los empleados una gama completa de herramientas de colaboración: voz de primera calidad, video, mensajería, mensajería instantánea y presencia, conferencia, videoconferencia, servicios de contact center, capacidades de movilidad, y más.
6.02	Se incluye garantia 12 meses SNTC-24X7X4 Cisco Business Edition 6000M
6.03	Cisco UCS 770W AC Power Supply for Rack Server
6.04	Cisco 12G Modular RAID controller with 2GB cache
6.05	300GB 12G SAS 10K RPM SFF HDD
6.06	Enable RAID 5 Setting
6.07	16GB DDR4-2666-MHz RDIMM/PC4-21300/single rank/x4/1.2v
6.08	2.2 GHz 4114/85W 10C/13.75MB Cache/DDR4 2400MHz
6.09	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America
6.1	VMware vSphere Standard 8
	Entregables
6.11	2 x Licencias Cisco BE Embedded Virt. Basic 7x, BE6K
6.12	385 x Licencias EntW On-Premises Calling
6.13	2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
6.14	72 x Licencias VMware vSphere Standard 8
6.15	Servicios Profesionales de Upgrade Licenciamiento de Collaboracion
7	**Cisco Unity Connection**
7.01	Solución de Mensajería de Voz Cisco Unity Connection, la cual se integra de manera nativa con la solución Cisco Collaboration
7.02	Incluye Garantía, Servicios de Soporte y Mantenimiento, directamente del fabricante, con SLA 24x7x4; esto significa: respuesta ante incidentes y atención a la garantía durante 24 horas, 7 días de la semana, con tiempo de respuesta de 4 horas o menos para todos los casos prioritarios.
7.03	Incluye 6 unidades de Cisco Unity Connection
7.04	Cisco Unity Connection es una plataforma rica en funcionalidades de voz y de mensajería unificada basada en el mismo sistema operativo Linux y Cisco Unified Communications del Cisco Unified Communications Manager. Con Cisco Unity Connection, puede acceder y gestionar mensajes de voz en una variedad de formas, utilizando su buzón de correo electrónico, navegador web, teléfono IP de Cisco, teléfonos inteligentes, Cisco Jabber, y mucho más. Cisco Unity Connection proporciona también características de reconocimiento de voz robusto para cuando son móviles, por lo que puede manejar sus mensajes de voz con manos y ojos libres.
7.05	Capacidad de Mensajería Unificada.
7.06	Capacidad de Contestadora Automática.
7.07	Capacidad de búsqueda de usuarios por comando de voz en la contestadora automática o deletreando el nombre del empleado.
7.08	Capacidad de Recibir los mensajes de Voz en el Email.
7.09	Capacidad de leer los mensajes de correo para ser escuchado por el teléfono.
7.1	Comandos de control de voz (pausar, reanudar, repetir, avanzar, eliminar, guardar, oír la indicación de día o de fecha/hora, saltar hacia adelante o hacia atrás) para acceder a los mensajes o directorios.
7.11	Capacidad de controlar el volumen o la velocidad durante la reproducción del mensaje.

7.12	Marcar los mensajes como normales, urgentes, privados o protegidos.
7.13	Grabar conversaciones en vivo y enviar archivos de sonido a una casilla de correo.
7.14	Acceso a mensajes de correo electrónico a través del teléfono (necesita integración con Microsoft Exchange).
7.15	Conexiones de red opcionales con otras soluciones de correo de voz de Cisco para permitir la comunicación de los usuarios en varios sistemas.
7.16	Capacidad de configurar reglas para enrutar llamadas por hora del día, persona que llama o estado del calendario (basado en la integración con Microsoft Exchange).
7.17	Opciones personalizadas para notificación de mensajes y saludos personales.
7.18	Capacidad de grabar hasta cinco saludos personales (alternativo, teléfono ocupado, interno, fuera de horas de oficina o estándar).
7.19	Capacidad de cambiar el orden en el que se presentan los mensajes.
	Entregables
7.2	6 x Licencias On-Premises Unity Connection
8	**Cisco ISR 4331**
8.01	Cisco ISR 4000 Series provee capacidades de rendimiento superior, con vergencia en las empresas y sus sucursales y WAN Inteligente para creer una plataforma de servicios consolidada en una solución de última generación. Las nuevas plataformas han sido diseñadas para permitir a la siguiente fase de la evolución de media gateways, ofreciendo la colaboración de medios enriquecidos y la virtualización aumentando al máximo el ahorro de costos operativos.
8.02	Esquema en alta disponibilidad
8.03	Hardware encryption acceleration.
8.04	Los nuevos módulos de procesamiento de voz (DSP) 4 (PVDM4)
8.05	DSP con capacidad de procesar voz y video.
8.06	Firewall basado en IOS.
8.07	Procesamiento de llamadas, mensajería de voz, servicios, aplicaciones.
8.08	La plataforma soporta la más amplia gama de interfaces de la industria como son: T1/E1, T3/E3, FXS/FXO, xDSL, cobre y fibra, y SIP Trunk.
8.09	Maneja al menos 400 llamadas simultaneas.
8.1	Maneja al menos 1000 sesiones SIP Trunk simultaneas.
8.11	Soporta al menos 12 puertos BRI/Análogos.
8.12	Soporta al menos 16 GB de memoria RAM. Incluye 8GB mínimo.
8.13	Soporta al menos 16 GB de memoria flash. Incluir 8GB mínimo.
8.14	Módulos o Memoria para el procesamiento de sesiones y Transcode mínimo de 128 canales.
8.15	Amigable al medio ambiente con consumos (sin módulos) de hasta 45 watts o menor.
8.16	Capacidad de poder realizar de manera simultánea mínimo lo siguiente: Capacidad incluida de realizar sesiones de transcodificación seguras de mínimo 20 sesiones. Capacidad incluida de realizar sesiones de transcodificación no seguras de hasta 20 sesiones. Conferencias de audio mínimo 8 participantes: 5 en G711, 5 en G729, 5 en G722, 5 en iLBC.
8.17	Soporta los protocolos SIP y H.323.
8.18	Soporta los protocolos SNMP versión 1, 2 y 3.
8.19	Soporta el protocolo IPv6.
	Entregables
8.20	100 x Licencias CUBE Enhanced Trunk Session
8.21	2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
9	**Cisco ISR 4321**
9.01	Cisco ISR 4000 Series provee capacidades de rendimiento superior, con vergencia en las empresas y sus sucursales y WAN Inteligente para creer una plataforma de servicios consolidada en una solución de última generación. Las nuevas plataformas han sido diseñadas para permitir a la siguiente fase de la evolución de

	media gateways, ofreciendo la colaboración de medios enriquecidos y la virtualización aumentando al máximo el ahorro de costos operativos.
9.02	Incluye Garantía, Servicios de Soporte y Mantenimiento, directamente del fabricante, con SLA 24x7x4; esto significa: respuesta ante incidentes y atención a la garantía durante 24 horas, 7 días de la semana, con tiempo de respuesta de 4 horas o menos para todos los casos prioritarios.
9.03	Esquema en alta disponibilidad
9.04	Hardware encryption acceleration.
9.05	Los nuevos módulos de procesamiento de voz (DSP) 4 (PVDM4)
9.06	DSP con capacidad de procesar voz y video.
9.07	Firewall basado en IOS.
9.08	Procesamiento de llamadas, mensajería de voz, servicios, aplicaciones.
9.09	La plataforma soporta la más amplia gama de interfaces de la industria como son: T1/E1, T3/E3, FXS/FXO, xDSL, cobre y fibra, y SIP Trunk.
9.1	Maneja al menos 400 llamadas simultaneas.
9.11	Maneja al menos 1000 sesiones SIP Trunk simultaneas.
9.12	Soporta al menos 12 puertos BRI/Análogos.
9.13	Soporta al menos 16 GB de memoria RAM. Incluye 8GB mínimo.
9.14	Soporta al menos 16 GB de memoria flash. Incluir 8GB mínimo.
9.15	Módulos o Memoria para el procesamiento de sesiones y Transcode mínimo de 128 canales.
9.16	Amigable al medio ambiente con consumos (sin módulos) de hasta 45 watts o menor.
9.17	Capacidad de poder realizar de manera simultánea mínimo lo siguiente: Capacidad incluida de realizar sesiones de transcodificación seguras de mínimo 20 sesiones. Capacidad incluida de realizar sesiones de transcodificación no seguras de hasta 20 sesiones. Conferencias de audio mínimo 8 participantes: 5 en G711, 5 en G729, 5 en G722, 5 en iLBC.
9.18	Soporta los protocolos SIP y H.323.
9.19	Soporta los protocolos SNMP versión 1, 2 y 3.
9.20	Soporta el protocolo IPv6.
	Entregables
9.21	31 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
10	**Firewall FortiGate para Perimetro Externo**
10.01	Entrega un rendimiento de Firewall de al menos 32 Gbps, IPS 7.8 Gbps, NGFW 6 Gbps y Threat Protection 5 Gbps
10.02	Soporta 4 Millones de sesiones concurrentes (TCP)
10.03	Soporta nuevas sesiones / segundo (TCP) 450.000
10.04	Soporta sin necesidad de licenciamiento al menos 2,000 túneles VPN IPsec P2P
10.05	Soporta sin necesidad de licenciamiento al menos 50,000 túneles VPN IPsec de cliente a puerta de enlace
10.06	Plataforma de protección de red, basada en un dispositivo con funcionalidades de Firewall e IPS de Próxima Generación (NGIPS y NGFW), así como consola de gestión y monitoreo.
10.07	Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos
10.08	Plataforma optimizada para análisis de contenido de aplicaciones en capa 7
10.09	La gestión del equipo compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
10.1	Soporta Policy based routing y policy-based forwarding
10.11	Soporta la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente
10.12	Soporta la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3
10.13	Soporta integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios

10.14	Soporta la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD
10.15	Permite la creación de políticas de NGIPS, NGFW, antivirus y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL
10.16	Soporta la autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local
10.17	Permite la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL
10.18	1x USB Port
10.19	1x Console Port
10.2	16x GE RJ45 Ports
10.21	16x GE SFP Slot Ports
10.22	1 RU
10.23	NGIPS
10.24	NGFW
10.25	Protección avanzada contra virus
10.26	Firewall en esquema de alta disponibilidad
	Entregables
10.27	2 x Licenciamiento UTP
10.28	2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
11	**Firewall FortiGate para VPN Principal**
11.01	Rendimiento de Firewall de 27 Gbps, IPS 5 Gbps, NGFW 3.5 Gbps y Threat Protection 3 Gbps.
11.02	Soporta 3 millones de sesiones concurrentes (TCP)
11.03	Soporta Nuevas sesiones / segundo (TCP) 280.000
11.04	Soporta sin necesidad de licenciamiento al menos 2,500 túneles VPN IPsec puerta a puerta.
11.05	Soporta sin necesidad de licenciamiento al menos 16,000 túneles VPN IPsec de cliente a puerta de enlace.
11.06	Plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo
11.07	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos
11.08	Plataforma optimizada para análisis de contenido de aplicaciones en capa 7.
11.09	La gestión del equipo compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
11.1	Soporta Policy based routing y policy based forwarding.
11.11	Soporta la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
11.12	Soporta la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
11.13	Soporta integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios.
11.14	Soporta la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
11.15	Soporta VPN de sitio-a-sitio y cliente-a-sitio.
11.16	Soporta VPN IPSec.
11.17	Soporta VPN SSL.
11.18	Compatible con 3DES.
11.19	Compatible con la autenticación MD5 y SHA-4.
11.2	Compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
11.21	Compatible con Internet Key Exchange (IKEv1 y v2).
11.22	Compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
11.23	Compatible con la autenticación a través de certificados IKE PKI.
11.24	Permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting.
11.25	La VPN SSL soporta que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web.

11.26	Las características de VPN SSL cumplen con o sin el uso de agentes.
11.27	Soporta la asignación de DNS en la VPN de cliente remoto.
11.28	Permite la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL.
11.29	Soporta la autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
11.3	Permite la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
11.31	1x USB Port .
11.32	1x Console Port.
11.33	2x GE RJ45 MGMT/DMZ Ports .
11.34	2x GE RJ45 WAN Ports .
11.35	2x GE RJ45 HA Ports
11.36	14x GE RJ45 Ports SOC3 1U RPS / 480GB 7. 2x GE RJ45/SFP Shared Media Pairs
11.37	Incluye garantía directa del fabricante por 12 meses mínimo en piezas y funcionalidad de seguridad con un SLA mínimo de 24X7, lo cual garantice el reemplazo de piezas y partes, o del equipo completo en caso de presentar algún desperfecto o falla durante el funcionamiento. Los oferentes deberán entregar una carta de compromiso indicando que se comprometen a cumplir con este requerimiento y a entregar los contratos de garantía registrados en el fabricante a nombre de la empresa contratante.
11.38	1 RU.
11.39	IPS.
11.4	Protección avanzada contra virus.
11.41	Control de aplicaciones.
11.42	Filtrado web y video.
11.43	Anti-spam.
11.44	Alta disponibilidad.
	Entregables
11.45	2 x Licenciamiento UTP
11.46	2 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
12	**Firewall FortiGate para VPN Remotas**
12.01	Rendimiento de Firewall 5 Gbps, IPS 1 Gbps, NGFW 800 Mbps y Threat Protection 600 Mbps.
12.02	Soporta 700 mil sesiones concurrentes (TCP).
12.03	Soporta Nuevas sesiones / segundo (TCP) 35.000.
12.04	Soporta sin necesidad de licenciamiento al menos 200 túneles VPN IPsec puerta a puerta.
12.05	Soporta sin necesidad de licenciamiento al menos 250 túneles VPN IPsec de cliente a puerta de enlace.
12.06	Plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo
12.07	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos
12.08	Plataforma optimizada para análisis de contenido de aplicaciones en capa 7.
12.09	La gestión del equipo compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
12.1	Soporta Policy based routing y policy-based forwarding.
12.11	Soporta la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
12.12	Soporta la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
12.13	Soporta integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios.
12.14	Soporta la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
12.15	Soporta VPN de sitio-a-sitio y cliente-a-sitio.
12.16	Soporta VPN IPSec.
12.17	Soporta VPN SSL.

12.18	Compatible con 3DES.
12.19	Compatible con la autenticación MD5 y SHA-4.
12.2	Compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
12.21	Compatible con Internet Key Exchange (IKEv1 y v2).
12.22	Compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
12.23	Compatible con la autenticación a través de certificados IKE PKI.
12.24	Permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting.
12.25	La VPN SSL soporta que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web.
12.26	Las características de VPN SSL cumplen con o sin el uso de agentes.
12.27	Soporta la asignación de DNS en la VPN de cliente remoto.
12.28	Permite la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL.
12.29	Soporta la autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
12.3	Permite la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
12.31	1x USB Port .
12.32	1x Console Port.
12.33	1x GE RJ45 WAN.
12.34	3x GE Ethernet Ports.
12.35	Incluye garantía directa del fabricante por 12 meses mínimo en piezas y funcionalidad de seguridad con un SLA mínimo de 24X7, lo cual garantice el reemplazo de piezas y partes, o del equipo completo en caso de presentar algún desperfecto o falla durante el funcionamiento. Los oferentes deberán entregar una carta de compromiso indicando que se comprometen a cumplir con este requerimiento y a entregar los contratos de garantía registrados en el fabricante a nombre de la empresa contratante.
12.36	IPS.
12.37	Protección avanzada contra virus.
12.38	Control de aplicaciones.
12.39	Filtrado web y video.
12.4	Anti-spam.
	Entregables
12.41	65 x Licenciamiento UTP
12.42	65 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
13	**FortiManager para Gestión Centralizada**
13.01	Virtual y compatible con el ambiente Vmware, Microsoft Hyper-V, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM on Redhat 6.5+ y Ubuntu 17.04, Nutanix AHV (AOS 5.10.5), Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI) y Alibaba Coud (AliCloud).
13.02	Soporta acceso vía SSH, WEB (HTTPS) para la gestión de la solución.
13.03	Cuenta con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.
13.04	Permite acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
13.05	Soporta SNMP versión 2 y 3.
13.06	Permite virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
13.07	Permite la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
13.08	Permite activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH, API abierta.

13.09	Soporta autenticación de usuarios de acceso a la plataforma vía LOCAL, LDAP, Radius y TACACS+
13.1	Capacidades de Alta disponibilidad (HA).
13.11	Capacidad de permitir provisionar y monitorear configuración de SD-WAN de todos los dispositivos gestionados desde una sola consola.
13.12	Visibilidad SD-WAN de los dispositivos gestionados centralmente, visibilidad de estado de enlace, desempeño de aplicación, utilización de ancho de banda y cumplimiento de SLA objetivo.
13.13	Capacidad de automatizar flujos de trabajo y configuraciones para los dispositivos gestionados desde una sola consola.
13.14	Capacidad Multi-tenancy para separar los datos de gestión de infraestructura de manera lógica o geográfica y permitir despliegue zerotouch para un aprovisionamiento masivo rápido.
13.15	Capacidad de realizar respaldos automáticos de configuración hasta en 5 nodos , conteniendo updates de todos los dispositivos gestionados.
13.16	Capacidad de permitir provisionar comunidades VPN y monitorear conexiones VPN de todos los dispositivos gestionados desde una sola consola y mostrar su geolocalización en un mapa.
13.17	API RESTful para permitir interacción con portales personalizados en la configuración de objetos y políticas de seguridad.
13.18	Integración de intercambio y compartición de datos con terceros mediante pxGrid, OCI, Esxi .
13.19	Accesos concurrentes de administradores.
13.2	Interfaz basada en línea de comando para administración de la solución de gestión.
13.21	Mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos;
13.22	Bloquea cambios, en el caso de acceso simultaneo de dos o más administradores.
13.23	Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, acceso de lectura, creación de usuarios, cambio de configuraciones.
13.24	Alertas automáticas por Email.
13.25	Alertas automáticas por SNMP.
13.26	Alertas automáticas por Syslog.
13.27	Soporta backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horario.
13.28	Permite al administrador transferir los backups a un servidor FTP, SCP y SFTP.
13.29	Los cambios realizados en un servidor de gestión son automáticamente replicados al servidor redundante.
13.3	Permite a los administradores autenticarse en los servidores de gestión a través de Certificado Digital X.509 (PKI).
13.31	Soporta sincronización de reloj interno por protocolo NTP.
13.32	Registra las acciones efectuadas por cualquier usuario.
13.33	
13.34	Soporta SNMP versión 2 y la versión 3 en los equipos de gestión.
13.35	Permite habilitar o deshabilitar, para cada interfaz de red de la solución de gestión, permisos de acceso HTTP, HTTPS, SSH, SNMP y Web Services (API).
13.36	Permite virtualizar la solución de gestión, de manera que cada administrador pueda gerenciar, visualizar y editar solo los dispositivos autorizados y registrados en su ambiente virtualizado.
13.37	Permite crear administradores que tengan acceso a todas las instancias de virtualización.
13.38	Permite la creación y administración de políticas de firewall y control de aplicación.
13.39	Permite la creación y administración de políticas de IPS, Antivírus y Anti-Spyware.
13.4	Funcionalidades de Gestión de Firewalls.
13.41	Permite la creación y administración de políticas de Filtro de URL.
13.42	Permite buscar cuáles reglas un objeto está siendo utilizado.
13.43	Permite la creación de reglas que permanezcan activas en horario definido.
13.44	Permite ser repositorio de firmas de antivirus, IPS, Web Filtering, email filtering, para optimizar la velocidad y descarga centralizada a los dispositivos gestionados.
13.45	Capacidad de desplegar los resultados de auditoría de seguridad d elos dispositivos gestionados.
13.46	Permite backup de las configuraciones y rollback de configuración para la última configuración salva.

13.47	Mecanismos de validación de políticas avisando cuando hayan reglas que ofusquen o conflictúen con otras (shadowing).
13.48	Permite la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas.
13.49	Permite que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión.
13.5	Herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador actualizar licencias en los aparatos a través de esta herramienta.
13.51	Permite la distribución e instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos.
13.52	Capacidad de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados.
13.53	Permite crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador.
13.54	Tiene "wizard" de gestión para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de los mismos.
13.55	Permite que las políticas y los objetos ya presentes en los dispositivos sean importados a la solución de gestión cuando se agregan.
13.56	Permite la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horario de lo sistema y firmware.
13.57	Tiene "wizard" en la solución de gestión para instalación de políticas y configuraciones de los dispositivos.
13.58	Permite crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración.
13.59	Permite crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos.
13.6	Tiene histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión.
13.61	Permite configurar y visualizar el manejo de SD-WAN de los dispositivos gestionados de forma centralizada.
13.62	Permite crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos.
13.63	Permite crear reglas de NAT64 y NAT46 de forma centralizada.
13.64	Permite la creación de reglas anti DoS de forma centralizada.
13.65	Permite la creación de objetos que serán utilizados en las políticas de forma centralizada.
13.66	Permite crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topología (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía.
13.67	Permite el uso de DDNS en VPNs de manera centralizada.
13.68	Permite la gestión de Access Points propietarios de manera centralizada.
13.69	Permite la gestión de Switches propietarios de manera centralizada.
13.7	Permite la gestión de perfiles de seguridad de software endpoint propietario de manera centralizada.
	Entregables
13.71	1 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
14	**FortiAnalyzer para Gestión y Almacenamiento de Logs de los NGFW**
14.01	Virtualizada y compatible con el ambiente Vmware, Microsoft Hyper-V, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM on Redhat 6.5+ y Ubuntu 17.04, Nutanix AHV (AOS 5.10.5), Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI) y Alibaba Coud (AliCloud).
14.02	
14.03	Soporta acceso vía SSH, WEB (HTTPS) para la gestión de la solución.
14.04	Comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.

14.05	Permite acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
14.06	Soporta SNMP versión 2 y 3.
14.07	Permite virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
14.08	Permite la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
14.09	Permite activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH.
14.1	Soporta autenticación de usuarios de acceso a la plataforma vía LDAP, Radius y TACACS+
14.11	Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos, burbuja y tabla.
14.12	Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
14.13	Asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
14.14	Ver la cantidad de logs enviados desde cada dispositivo supervisado.
14.15	Mecanismos de borrado automático de logs antiguos.
14.16	Permite la importación y exportación de reportes.
14.17	Capacidad de crear informes en formato HTML, PDF, XML y CSV.
14.18	Permite exportar los logs en formato CSV.
14.19	Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
14.2	Los logs generados por los dispositivos administrados son centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
14.21	Reportes predefinidos.
14.22	Enviar automáticamente los logs a un servidor FTP externo a la solución.
14.23	Duplicación de reportes existentes para su posterior edición.
14.24	Capacidad de personalizar la portada de los reportes obtenidos.
14.25	Permite centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
14.26	Los logs de auditoría de cambios de configuración de reglas y objetos son visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
14.27	Capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas.
14.28	Mecanismo de “Drill-Down” para navegar en los reportes de tiempo real.
14.29	Permite descargar de la plataforma los archivos de logs para uso externo.
14.3	Capacidad de generar y enviar reportes periódicos automáticamente.
14.31	Permite la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
14.32	Permite el envío por email de manera automática de reportes.
14.33	Permite que el reporte a enviar por email sea al destinatario específico.
14.34	Permite la programación de la generación de reportes, conforme a un calendario definido por el administrador.
14.35	Visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
14.36	Permite el uso de filtros en los reportes.
14.37	Permite definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
14.38	Permite especificar el idioma de los reportes creados.
14.39	Alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
14.4	Permite el envío automático de reportes a un servidor externo SFTP o FTP.

14.41	Capacidad de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.
14.42	Capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
14.43	Herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de estos.
14.44	Capacidad de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
14.45	Define el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
14.46	Proporciona información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
14.47	Compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
14.48	Permite aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos.
14.49	Permite visualizar en tiempo real los logs recibidos.
14.5	Permite el reenvío de logs en formato syslog.
14.51	Permite el reenvío de logs en formato CEF (Common Event Format).
14.52	Dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red.
14.53	Dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
14.54	Dashboard para operaciones SOC que monitorea el tráfico en su red.
14.55	Dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red.
14.56	Dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
14.57	Dashboard para operaciones SOC que monitorea actividad de endpoints en su red.
14.58	Dashboard para operaciones SOC que monitorea actividad VPN ren su red.
14.59	Dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs..
14.6	Dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria).
14.61	Dashboards personalizados para monitoreo de operaciones SOC .
14.62	Permite configuración de alta disponibilidad Master/Slave en la capa 3..
14.63	Permite generar alertas de eventos a partir de logs recibidos.
14.64	Permite crear incidentes a partir de alertas de eventos para endpoint.
14.65	Permite la integración al sistema de tickets ServiceNow.
14.66	
14.67	Permite respaldar logs en nube publica de Amazon S3, Microsoft Azure y Google Cloud.
14.68	Permite estándar SAML para autenticación de usuarios administradores.
14.69	Reporte de cumplimiento de PCI DSS..
14.7	Reporte de utilización de aplicaciones SaaS.
14.71	Reporte de prevención de perdida de datos (DLP).
14.72	Reporte de VPN.
	Entregables
14.73	1 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
15	**FortiSwitches para Acceso LAN**
15.01	Administrable.
15.02	Velocidad 10/100/1000 (PoE+) 24 Ports.
15.03	Uplink interfaces 4 SFP.
15.04	PoE+ 370W.
15.05	Switching capacity 56Gbps.

15.06	Soporta al menos 4K VLANs.
15.07	Soporta conectividad segura para administración del equipo.
15.08	Soporta SSH, IPV6.
15.09	Soporta 8 Link Aggregation Groups.
15.10	Certificaciones de cumplimiento: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2.
	Entregables
15.11	64 x Garantía directa del fabricante por 12 meses (licencia o suscripción) con un SLA mínimo de 24X7 (servicio de soporte y mantenimiento de sus piezas y funcionalidades).
16	**Servicio SOC Externo BigFive**
16.01	Servicio integral que asegura la continuidad y seguridad de nuestras operaciones, en donde se incluye respuesta ante Incidentes para la detección, contención y recuperación de ataques cibernéticos, monitoreo activo, capacidad para gestión de soluciones y asistencia de ingenieros certificados con experiencia con los fabricantes Cisco, Fortinet y Cloudflare, etc.
16.02	Escaneo, detección y remediación de vulnerabilidades de los Activos TI del Banco.
16.03	Escaneo e Informe mensual de hallazgos en la detección y remediación de vulnerabilidades en los Servicios web especificados.
16.04	Man Power en sitio para el monitoreo y asistencia de incidentes que se pudieran concretar.
16.05	Recomendaciones basado en las mejores prácticas de la industria; mejoras en diseño de la arquitectura y recomendaciones basado en ISO 27001.
16.06	Informes mensuales de los eventos detectados y las operaciones realizadas.
16.07	Díez (10) Casos de Uso que se ajusten al ambiente actual y necesidad del Banco, respecto a la detección, contención y respuesta de incidentes.
16.08	Investigación de amenazas técnicas y tácticas que apoye a la operación, entregando información clave para la anticipación de potenciales ataques.
16.09	Búsqueda proactiva de amenazas avanzadas en los sistemas, redes e infraestructura.
16.1	Acciones para la detección, tales como: - Credenciales comprometidas - Movimiento lateral - Escalamiento de privilegios - Suplantación de identidad (correos electrónicos sospechosos, phishing) - Anomalías en el ingreso a los sistemas - Visibilidad de la red interna, nube y direcciones IP asociadas a incidente - Eliminación anómalas de logs - Cambios directos sobre las bases de datos - Malware
16.11	Ingenieros disponibles para hacer presencia en sitio de la Sede Central 24x7 de manera presencial, para la atención de incidentes en caso de que la situación lo amerite, además, del monitoreo activo de la plataforma de seguridad.
16.12	Gestión de Vulnerabilidades para realizar evaluación continua del estado de los sistemas operativos y aplicaciones. Esto involucra la identificación, clasificación y corrección de vulnerabilidades de seguridad de la información.
16.13	Monitoreo y correlación de eventos debe monitorear todos los eventos recolectados a través del SIEM y brindar respuesta a incidentes de seguridad de la información 24x7.
16.14	Monitoreo activo 24x7.
16.15	Hacer inteligencia de ataques y detección de nuevo malware y APTs y establecer procedimientos de contención y erradicación de estos.
16.16	Herramienta de tickets
16.17	Mecanismo que permita obtener inteligencia de amenazas tanto en el contexto externo como interno de la organización.
	Entregables

16.18	1 x Servicio SOC Externo, que incluya: Security Operations Center (SOC), Cyber Threat Intelligence (CTI) y un Pentesting GrayBox durantes 6 meses.

2. PROCEDIMIENTO DE EXCEPCIÓN POR CONTRATACIÓN DIRECTA APLICABLE

Excepción por Proveedor Único No. **BAGRICOLA-CCC-PEPU-2025-0003**

3. PLAZO EN QUE REQUIERE EL OBJETO DE LA CONTRATACIÓN

Estas renovaciones son requeridas en los siguientes plazos:

- **SOLUCIÓN CISCO DUO – MFA:** vigencia de 1 **año**
- **SOLUCIÓN CISCO UMBRELLA (CISCO SECURE ACCESS):** vigencia de **1 año**
- **SOLUCIÓN WAF CLOUDFLARE:** vigencia de **1 año**
- **SERVICIOS SOC Externo: 1 año**
- **CIBERSEGURIDAD INTERNA Y PERIMETRAL CISCO FIRE POWER:** vigencia de **1 año**
- **CENTRAL TELEFÓNICA CISCO:** vigencia de **1 año**
- **SWITCH FORTINET Y FORIGASTE UTM:** vigencia de **1 año**

4. CRONOGRAMA DEL PROCEDIMIENTO DE EXCEPCIÓN

ACTIVIDADES	PERIODO DE EJECUCION
1. Recepción Ofertas “Sobre A” y “Sobre B”	**28 de mayo del 2025 a las 4:10 P.M.**
2. Apertura de Ofertas “Sobre A” y “Sobre B”	**29 de mayo del 2025 a las 11:00 A.M.**
3. Verificación, validación y evaluación de Ofertas	**30 de mayo del 2025 a las 11:00 A.M.**
4. Adjudicación.	**Hasta el 13 de junio del 2025 a las 3:01 P.M**
5. Notificación de adjudicación	**Hasta el 20 de junio del 2025 a las 3:01 P.M**
6. Suscripción de contrato	**Hasta el 15 de julio del 2025 a las 3:01 P.M**

5. LUGAR Y FECHA PARA PRESENTAR PROPUESTA Y COTIZACIÓN EN SOPORTE PAPEL (FÍSICA).

La presentación de la propuesta y cotización en soporte papel debe ser entregada en la Unidad de Operativa Compras y Contrataciones de Banco Agrícola de la República Dominicana (BAGRICOLA) localizada en la Av. George Washington 601, Santo Domingo, Distrito Nacional, hasta **28 DE MAYO DEL 2025 a las 4:10 P.M.** y solo podrá postergarse por causas de Fuerza Mayor o Caso Fortuito definidos en la presente solicitud.

Los documentos contenidos en la **propuesta** deberán ser presentados tanto en original debidamente marcado como "**ORIGINAL**" en la primera página del ejemplar, junto con **DOS (2) fotocopias simples de la misma**, debidamente marcada en su primera página, como "**COPIA**" y en ella deberá constar en la primera página la firma original del oferente y de ser una persona jurídica la firma del representante legal y el sello social de la compañía.

6. IDENTIFICACIÓN DE LAS PROPUESTAS Y COTIZACIÓN

A través del SECP-Portal Transaccional de forma digital, Correo Electrónico, compras@bagricola.gob.do o de forma física, mediante un sobre cerrado identificado como: "Propuesta y cotización para la CONTRATACIÓN DE LOS SERVICIOS DE LICENCIAMIENTO, SUSCRIPCIONES Y/O SOPORTE RELACIONADOS CON: 1) SOLUCIONES DE CIBERSEGURIDAD E INFRAESTRUCTURA QUE SOPORTAN EL CORE BANCARIO, 2) BASE DE DATOS INFORMIX Y EL SISTEMA OPERATIVO REDHAT LINUX ENTERPRISE, 3) PLATAFORMA DE MONITOREO Y GESTIÓN DE SERVICIOS CENTRALIZADO MANAGE-ENGINE, **4) SERVICIO DE SOPORTE Y MANTENIMIENTO DEL CORE BANCARIO: SISTEMA EASYBANK (CB) Y SISTEMA GESTIÓN DE CRÉDITO CARTERA DIGITAL (CB),** 5) CONTRATO DE SERVICIO DE SOPORTE Y MANTENIMIENTO DEL SISTEMA DE GESTION DE COBROS VEOCRM Y VCTALK, Y 6) ALMACENAMIENTO BACKUP EN LA NUBE HUAWEI" del Procedimiento de excepción por Proveedor Único No. **BAGRICOLA-CCC-PEPU-2025-0003**. El oferente depositará su propuesta con la siguiente información legible en la parte frontal:

Nombre de la persona física/ jurídica
(Sello Social y RNC)
Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES

7. REQUERIMIENTOS TÉCNICOS QUE DEBE TENER LA PROPUESTA

Documentación legal y credenciales:

1) Formulario de Presentación de Oferta (SNCC.F.034).
2) Formulario de Información sobre el Oferente (SNCC.F.042).
3) Certificación que demuestre estar al día con sus obligaciones fiscales en la Dirección General de Impuestos Internos (**DGII**), lo cual será verificado en línea por la institución.
4) Certificación que demuestre estar al día con el pago de sus obligaciones de la Seguridad Social en la Tesorería de la Seguridad Social (**TSS**), lo cual será verificado en línea por la institución.
5) Copia de la **Cedula de Identidad y Electoral** del representante legal de la empresa, o en caso de ser extranjero, su pasaporte.
6) Copia del **Certificado de Registro Mercantil vigente**, o el documento homólogo en su país de origen emitido por un organismo estatal correspondiente o documento que acredite la incorporación de la empresa comercial y su actividad económica.

Documentación técnica:

7) **Oferta Técnica (Firmada y Sellada):** Conforme a las especificaciones técnicas suministradas y/o informe pericial adjunto en los documentos del proceso.

8. REQUERIMIENTOS QUE DEBE TENER LA COTIZACIÓN

Formulario de Presentación de Oferta Económica (SNCC.F.033)

La Oferta deberá presentarse en pesos dominicanos (RD$). Los precios deberán expresarse en dos decimales (XX.XX) que tendrán que incluir todas las tasas (divisas), impuestos y gastos que correspondan, transparentados e implícitos según corresponda.

Los precios no deberán presentar alteraciones ni correcciones y deberán ser dados por la unidad de medida establecida en los listados.

9. DISPOSICIONES GENERALES PARA EL CONTRATO

9.1 Plazo para la suscripción del contrato

El contrato entre Banco Agrícola de la República Dominicana y el(la) adjudicatario(a) deberá ser suscrito en la fecha que establece el cronograma de actividades del presente pliego de condiciones, el cual no deberá ser mayor a veinte (20) días hábiles, contados desde la fecha de notificación de la adjudicación, de conformidad con el artículo 164 del Reglamento 416-23.

9.2 Validez y perfeccionamiento del contrato

El contrato será válido cuando para su suscripción se haya cumplido con ordenamiento jurídico y cuando el acto definitivo de adjudicación y la constitución de la Garantía de Fiel Cumplimiento de contrato hayan sido satisfechas.

El contrato se considerará perfeccionado una vez se publique por el SECP-Portal Transaccional y en el portal institucional de Banco Agrícola de la República Dominicana, en un plazo no mayor de cinco (5) días hábiles luego de su suscripción y, además, en el caso de las instituciones sujetas a la Ley núm. 10-07 del Sistema Nacional de Control Interno, se haya registrado en la Contraloría General de la República.

9.3 Gastos legales del contrato

En este procedimiento de contratación los gastos de la legalización de firmas del contrato resultante por parte del notario serán asumidos por la institución contratante.

9.4 Vigencia del contrato

La vigencia del Contrato será por **UN (1) AÑO** a partir de la fecha de la suscripción de este y hasta su fiel cumplimiento y liquidación, de conformidad con el Cronograma de Ejecución, el cual formará parte integral y vinculante del mismo.

9.5 Supervisor o responsable del contrato

El Banco Agrícola de la República Dominicana ha designado como supervisor o responsable del contrato al Lic. **Felix Terrero**, Encargado de **Banca Digital,** dirección de Tecnología de la Información y Comunicación (TIC).

9.6 Entregas

El Banco Agrícola de la República Dominicana implementará los servicios conforme a las necesidades específicas del área requirente, sin que esto afecte o modifique el monto del contrato adjudicado. La ejecución

de la entrega se realizará de manera flexible, atendiendo los requerimientos puntuales de la dirección de Tecnología de la Información y Comunicación (TIC).

9.7 Suspensión del contrato

La Banco Agrícola de la República Dominicana podrá ordenar la suspensión temporal del contrato mediante acto administrativo motivado suscrito por la máxima autoridad y notificado al(la) contratista, por las causas que establece el artículo 31 numeral 5) de la Ley núm. 340-06 y sus modificaciones y el artículo 182 del Reglamento 416-23.

La Dirección General de Contrataciones Públicas (DGCP), también podrá ordenar la suspensión del contrato como resultado de una medida cautelar impuesta en el marco del conocimiento de un recurso, investigación o inhabilitación.

9.8 Modificación de los contratos

Toda modificación del contrato sea unilateral o prevista en el pliego de condiciones, se formalizará a través de una enmienda con el contenido previsto en el artículo 164 del Reglamento núm. 416-23 y previo a realizarse cualquier prestación sustentada en la modificación deberá ser publicada en el SECP.

9.9 Equilibrio económico y financiero del contrato

El Banco Agrícola de la República Dominicana adoptará todas las medidas necesarias para mantener las condiciones técnicas, económicas y financieras del contrato durante su ejecución. En el evento de que estas condiciones no se mantengan, puede dar paso a una ruptura del equilibrio económico y financiero del contrato, que afecte al contratista o a la institución, siempre que se origine por razones no imputables a la parte que reclama la afectación y que no tenía la obligación de soportar.

La afectación puede dar paso al derecho tanto al contratista como al Banco Agrícola de la República Dominicana a procurar el restablecimiento del equilibro económico y financiero del contrato con sus correspondientes ajustes. No obstante, el hecho de que una de las causas que provocan la ruptura del equilibrio económico se materialice, no significa que, automáticamente, se ha podido comprobar el daño económico para quien lo invoque.

En ese sentido, para el restablecimiento del equilibro económico y financiero del contrato, quien lo invoque deberá demostrarlo y solicitarlo, conforme a los criterios y el procedimiento previsto en el artículo 32 numeral 1) de la Ley núm. 340-06 y sus modificaciones y los artículos 176, 177 y 178 del Reglamento núm. 416-23.

9.10 Subcontratación

El(la) contratista podrá subcontratar la ejecución de hasta el 50% del monto de las tareas comprendidas en este pliego de condiciones, con la previa y expresa autorización de la institución contratante de acuerdo con el numeral 2) del artículo 32 de la Ley núm. 340-06 y sus modificaciones.

El(la) oferente, al momento de presentar su oferta, debe indicar los servicios que subcontrataría y las personas físicas o empresas que ejecutarían cada una de ellas, quienes no podrán estar en el régimen de inhabilidades previsto en el artículo 14 de la Ley y sus modificaciones; en el entendido, que el(la) contratista será solidariamente responsable de todos los actos, comisiones, defectos, negligencias, descuidos o incumplimientos de los(as) subcontratistas, de sus empleados(as) o trabajadores(as).

9.11 Recepción de servicio

Concluida la prestación del servicio, el personal designado por la institución como responsable del contrato procederá a completar un acta de recepción provisional donde determine, a partir de los términos de referencia, si el servicio cumplió o no con lo pactado.

Si la prestación del servicio fue acorde con los términos de referencia, la institución deberá formalizarla mediante la recepción conforme en un plazo de **cinco (5) días hábiles**, a partir del día siguiente de notificado la prestación del servicio. El proveedor tiene derecho de intimar a la institución contratante la emisión de la recepción conforme, sino lo realiza en el referido plazo.

De existir cualquier anomalía con la prestación, y se tenga tiempo suficiente para que el proveedor corrija las faltas antes de que se cumpla el período en que se necesita, la institución deberá notificar en un plazo de cinco (5) días hábiles, al proveedor para que subsane los defectos y proceda, en un plazo no superior **a cinco (5) días hábiles**, a la corrección de los errores detectados.

En los casos donde el proveedor no haya cumplido con el servicio y la corrección no fue posible antes del período en que la institución lo requería, la institución deberá notificar en un plazo de cinco (5) días hábiles, el acta de no conformidad con la prestación del servicio y, conforme con el debido proceso, puede iniciar las medidas administrativas correspondientes por la falta del proveedor.

9.12 Finalización del contrato

El contrato finalizará por una de las siguientes condiciones que acontezca en el tiempo: **a)** cumplimiento del objeto; **b)** por mutuo acuerdo entre las partes o; **c)** por las causas de resolución previstas en el artículo 190 del Reglamento núm. 416-23.

9.13 Incumplimiento de contrato y sus consecuencias

Se considerará incumplimiento del contrato las siguientes situaciones, sin perjuicio de aquellas contempladas en la normativa:

a) La mora del proveedor en la ejecución de servicio por causas imputables;
b) El incumplimiento de la calidad en relación con las especificaciones técnicas, prevista en el presente pliego de condiciones;
c) El suministro, prestación o ejecución de menos unidades solicitadas y/o adjudicadas.
d) Si el Proveedor viola cualquier término o condiciones del Contrato.

El incumplimiento del contrato por parte del(la) proveedor(a) podrá suponer una causa de resolución de este, de conformidad con el artículo 190 del Reglamento de Aplicación, y además el(la) contratista ser pasible de las sanciones previstas en el artículo 66 de la Ley núm. 340-06 y sus modificaciones, sin perjuicio de las acciones penales o civiles que correspondan.

9.14 Penalidades por retraso

Las penalidades serán de naturaleza pecuniaria y se aplicarán por incumplimiento de las obligaciones como se describen en las especificaciones técnicas indicadas, correspondiente al proceso número BAGRICOLA-CCC-PEPU-2025-0003. En este entendido, las penalidades aplicables durante la ejecución del contrato son las siguientes:

- El BAGRICOLA aplicará una penalidad equivalente a un por ciento (1%) del monto total del contrato pendiente de recepción por cada día o fracción de día en que LA ENTIDAD CONTRATADA incumpla con el plazo establecido para la entrega de los servicios. Para que se considere ejecutada la obligación de entrega la misma deberá ser satisfactoria conforme los términos y condiciones que se determinarán en el contrato a ser suscrito.

- En los casos en que los bienes, servicios u obras no se correspondan con las especificaciones técnicas contenidas en el presente documento o las especificaciones técnicas, planos y listados de partida, el BAGRICOLA procederá a no recibir los mismos y notificarle dicha situación a LA ENTIDAD CONTRATADA, ya sea por medios físicos o electrónicos, otorgándole un plazo de dos (2) días hábiles para que proceda a la sustitución de los bienes, servicios u obras correspondientes. En caso de que LA ENTIDAD CONTRATADA no obtempere con el requerimiento, transcurrido este plazo adicional otorgado, el BAGRICOLA aplicará una penalidad del dos por ciento (2%) del monto total del contrato por cada día hábil o fracción de día hábil en que no se hayan subsanado las faltas indicadas.

- El BAGRICOLA aplicará una penalidad equivalente a un diez por ciento (10%) del monto total del contrato en caso de que LA ENTIDAD CONTRATADA incumpla con los términos y condiciones sobre el funcionamiento esperado y satisfactorio de los bienes suministrados a través de los servicios recibidos, que serán establecidos en el contrato a ser suscrito.

- El BAGRICOLA aplicará una penalidad equivalente a cero puntos cinco por ciento (0.5%) del monto total del contrato por cada día o fracción de día en que LA ENTIDAD CONTRATADA incumpla con los términos y condiciones que serán establecidos en el contrato para los servicios entregados.

El Banco Agrícola de la Republica Dominicana actuará conforme al artículo 230 numeral 3) del Reglamento núm. 416-23.

9.15 Causas de inhabilitación del Registro de Proveedores del Estado

La institución contratante podrá solicitar a la Dirección General de Contrataciones Públicas el inicio de un procedimiento administrativo sancionador, contra el(la) oferente o contratista que ha cometido alguna de las infracciones regladas en el artículo 66 de la Ley núm. 340-06 y sus modificaciones.

El procedimiento administrativo sancionador por las infracciones administrativas referidas en los numerales 7) al 10) del indicado artículo, podrá ser iniciado de oficio por la Dirección General de Contrataciones, si en el cumplimiento de su función de verificar que se cumplan con las normas del Sistema Nacional de Compras y Contrataciones, identifica indicios de que han sido cometidas.

9.16 Garantías del fiel cumplimiento de contrato

Para poder suscribir el contrato el adjudicatario deberá constituir previamente una garantía de fiel cumplimiento de contrato en favor de **Banco Agrícola de la República Dominicana** para asegurar que cumplirá con las condiciones y cláusulas establecidas en el pliego de condiciones y en el contrato y que los servicios sean entregados de acuerdo con las condiciones y requisitos previstas en el pliego de condiciones, las especificaciones técnicas, la oferta adjudicada y el propio contrato.

En esos casos, corresponderá al adjudicatario presentar en un plazo no mayor de en el plazo de **cinco (5) días hábiles** una garantía, ya sea bancaria o póliza emitida por una compañía aseguradora autorizada por la Superintendencia de Seguros para operar en la República Dominicana, por el equivalente al **cuatro por ciento (4 %)** del monto de la adjudicación. En el caso de un adjudicatario certificado como MIPYME, el equivalente será de uno por ciento (1%) del monto de la adjudicación y solo se le exigirá la fianza de seguro.

La vigencia de la garantía será de **mínimo UN (1) AÑO**, contados a partir de la constitución de la misma y hasta el fiel cumplimiento y hasta la liquidación del contrato.

Si el adjudicatario no presenta la garantía de fiel cumplimiento de contrato en el plazo señalado, se considerará una renuncia a la adjudicación que dará paso a que la institución contratante ejecute su garantía de seriedad de la oferta.

La garantía de fiel cumplimiento será devuelta luego de la recepción conforme de los servicios contratados.

10. CONDICIONES DE PAGO Y RETENCIONES

El detalle de la forma de pago se presenta a continuación:

1- Se establece un pago único correspondiente al **100%** del monto total adjudicado, cubriendo las licencias de software por un periodo de UN (1) año**:**
- **SOLUCIÓN CISCO DUO – MFA:** vigencia de **1 AÑO.**
- **SOLUCIÓN CISCO UMBRELLA (CISCO SECURE ACCESS):** vigencia **de 1 AÑO**

2- Se establece un pago único correspondiente al **100%** del monto total adjudicado, cubriendo las licencias de software por un periodo de un (1) año:
- **SOLUCIÓN WAF CLOUDFLARE:** vigencia de **1 AÑO**

3- Se establece que el **100%** del monto total de este servicio o ítem adjudicado será pagado en 6 cuotas mensuales consecutivas, cubriendo las licencias de software por un periodo de **6 MESES**. Estos pagos se realizarán contra presentación de factura cada mes, una vez verificada la entrega y validación de los servicios mediante solicitud realizada por la Direccion de Tecnologia de la Información y Ciberseguridad:
- **SERVICIOS SOC EXTERNO: 6 MESES**

4- Se establece un pago único correspondiente al **100**% del monto total adjudicado, cubriendo las licencias de software por un periodo de un (1) año:
- **CIBERSEGURIDAD INTERNA Y PERIMETRAL CISCO FIRE POWER:** vigencia de **1 AÑO**

5- Se establece un pago único correspondiente al 100% del monto total adjudicado, cubriendo las licencias de software por un periodo de **un (1) año:**
- **CENTRAL TELEFÓNICA CISCO:** vigencia de **1 AÑO**

6- Se establece un pago único correspondiente al 100% del monto total adjudicado, cubriendo las licencias de software por un periodo de un (1) año:
- **SWITCH FORTINET Y FORIGASTE UTM:** vigencia de **1 AÑO**

Estos pagos se realizarán contra presentación de factura, una vez verificada la entrega y activación completa de los servicios requeridos por la Direcciones de Tecnología de la Información y Comunicación y de Ciberseguridad.

La Entidad Contratante no podrá comprometerse a entregar, por concepto de avance, un porcentaje mayor al veinte por ciento (20%) del valor del Contrato.

En caso de que el adjudicatario del contrato sea una Micro, Pequeña y Mediana empresa (MIPYME), la entidad contratante podrá entregar un avance inicial correspondiente al veinte por ciento (20%) del valor del contrato, para fortalecer su capacidad económica, contra la presentación de la garantía del buen uso del anticipo y firma del contrato, **en un plazo no mayor a 15 días.** El 80% restante se realizará con la presentación de los servicios entregados y con el recibido conforme por el área requirente y administrador del contrato en el BAGRICOLA, como parte de las condiciones de pago previstas.

Las facturas deberán presentarse con Número de Comprobante Gubernamental B15 y deberán ser entregadas en la unidad de correspondiente, ubicada en la Av. George Washington 601, Banco Agrícola de la República Dominicana.

El Proveedor no estará exento de ningún pago de impuestos y por tanto será el único responsable por el pago de los gravámenes sobre las sumas percibidas bajo el presente contrato.

La condición de pago es máxima **Treinta (30) días**, a realizarse con la entrega y recibo conforme por la **Direcciones de Tecnología de la información y Comunicación y/o de Ciberseguridad**, salvo común acuerdo entre las partes.

El pago será realizado máximo 30 días por transferencia, después de que sea presentada y aprobada la factura de los servicios entregados.

Las Facturas y documentos comerciales de nuestros proveedores deben contener los siguientes datos:

- Nombre Comercial.
- Razón Social.
- Registro Nacional del Contribuyente (RNC).
- Registro de Proveedor del Estado (RPE).
- Numero de Comprobante Gubernamental B15
- Domicilio, Teléfono y persona de Contacto.
- Numeración secuencial.

Se considerarán no recibidas todas aquellas facturas que no cumplan lo expuesto en los párrafos anteriores de este acápite.

11. DOCUMENTOS ANEXOS

a) Informe justificativo.
b) Formulario de oferta Económica (SNCC.F.033)
c) Formulario de Información del Oferente (SNCC.F.042)
d) Presentación de Oferta (SNCC.F.034)
e) Borrador contrato ejecución de servicios

12. CONTACTO

Para cualquier consulta o aclaración del procedimiento de referencia, los datos de contacto son los siguientes:

Unidad Operativa de Compras del Banco Agrícola de la Rep. Dom.
Dionisio E Jiménez
Teléfono: 809-535-8088 ext. 4316
Mail: compras@bagricola.gob.do