BANCO DE COMERCIO EXTERIOR DE COLOMBIA

BANCÓLDEX S.A.

Anexo técnico

Adquisición de solución de conectividad inalámbrica y control de acceso a redes

BOGOTÁ D.C.

Anexo Técnico

Adquisición de solución de conectividad inalámbrica y control de acceso a redes

OBJETO

Contratar la adquisición de solución de conectividad inalámbrica de las sucursales Bancoldex y solución de sistema de control de acceso a redes (NAC), incorporando los servicios de instalación, configuración, despliegue, soporte, mantenimiento y capacitación de las soluciones adquiridas para las sucursales Bogotá, Barranquilla, Bucaramanga, Medellín, Cali y Pereira de BANCOLDEX.

ALCANCE

El proponente debe proveer la infraestructura necesaria para la conectividad inalámbrica del banco en la sede principal y las sucursales de este, incluyendo el número de AP necesarios para generar un área de cobertura de la red inalámbrica para todos los funcionarios y visitantes de las sedes del banco.

La solución debe incluir una consola de administración para los AP y redes inalámbricas desplegadas centralizada en nube que además de permitir configurar las redes y los AP de manera independiente, debe entregar estadísticas de ubicación, uso y seguridad de cada uno de los AP (características en detalle en la descripción técnica de este documento).

La solución de conectividad inalámbrica a proveer debe ofrecer compatibilidad con la solución de infraestructura de networking actual del banco Cisco ACI y debe ser agnóstica a los switches de borde.

La solución debe contemplar los medios de alimentación de los AP ya sea por medio de inyectores PoE o switches con esta característica, actualmente la infraestructura del banco no tiene la capacidad de proveer energía por este medio.

El proponente debe proveer un sistema de control de acceso a redes (NAC), que tenga la capacidad de integrarse directamente al directorio activo del banco para realizar la autenticación de usuarios y dispositivos y conceder así mismo los accesos permitidos a la red del banco basado en políticas de roles gestionables desde la misma solución.

La solución NAC debe ser una solución libre de agentes instalados en los dispositivos y que permita la centralización de políticas basada en roles de acceso a redes en el mismo. Además de la gestión personalizable de acceso a visitantes y contratistas que ingresen a las instalaciones del banco.

La solución NAC debe estar en la capacidad de generar reportes personalizables sobre preferencias o tendencias de autenticación, dispositivos perfilados, datos de los invitados, dispositivos conectados y estado de salud de los end points e incluir la facilidad de creación de alertas y advertencias sobre fallas de autenticación y comportamientos sospechosos.

La solución de conectividad inalámbrica y la solución de acceso a redes deben ser instaladas, configuradas y desplegadas por el proveedor, el cual debe hacer entrega de las soluciones instaladas por medio de la transferencia de conocimiento al equipo de infraestructura del banco y debe entregar soporte para atención de incidentes de las soluciones 7x24 y atención a requerimientos 5x8 NBD para cambio de partes con una duración de al menos 3 años.

El proponente adicionalmente deberá realizar el mantenimiento físico y lógico de la solución wifi 1 vez al año y entregar un informe de los hallazgos y procedimientos que se deban ejecutar para el mismo.

Se debe realizar capacitación certificada de la solución inalámbrica y NAC a una persona del equipo de infraestructura de Bancoldex.

La cobertura de la solución de conectividad inalámbrica debe contemplar con AP para los pisos 37 a 42 de la sede Bogotá del banco, para la sede Bogotá se debe realizar una visita de estudio de sitio que se coordinará y será parte integral de la propuesta con el área de infraestructura con la cual podrán determinar el número de AP para la solución de manera que se garantice que no haya zonas grises de cobertura en la misma. Para las sucursales, se deben entregar la cantidad de AP que se relaciona a continuación:

1. Barranquilla (2AP)
2. Bucaramanga (1AP)
3. Medellín (2AP)
4. Cali (1AP)
5. Pereira (1AP)

CONDICIONES GENERALES

El proponente debe contar o acreditar:

1. Certificación del fabricante que lo acredite como canal autorizado en nivel gold o superior (o su equivalente) para el año fiscal 2022 (adjuntar certificado) para el territorio colombiano.
2. Dos certificaciones donde se relacione la experiencia en implementación de proyectos que cuenten con una cantidad igual o superior de Access points de tecnología WiFi 6 (802.11ax), e incluya el control de acceso a redes WLAN en los últimos dos años.
3. Personal certificado por el fabricante que lo acredite en nivel “Professional” o superior en el diseño de sus soluciones (adjuntar certificado/s).
4. Todos los equipos, software y licenciamiento de la/s solución/es son del mismo fabricante (MONOMARCA).
5. Todos los equipos, software y licenciamiento de la/s solución/es son nuevos de fábrica, no son remanufacturados, reparados y/o genéricos.
6. Todos los equipos, software y licenciamiento de la/s solución/es NO se encuentran en anuncio de fin de vida (end of life) y/o fin de venta (end of sale) por parte del fabricante.
7. Para garantizar la protección de inversión, alineación con las tendencias tecnológicas de la industria, soporte y vigencia tecnológica y estar preparados para

los requerimientos futuros, los equipos de la/s solución/es ofertada/s deben corresponder a una marca que se encuentre dentro del siguiente listado:

a. JUNIPER
b. EXTREME NETWORKS
c. HPE (ARUBA)
d. CISCO.

ESPECIFICACIONES TÉCNICAS

Especificaciones técnicas mínimas para los Access Point (AP)

Los Access Point (AP) a proveer por el proponente, deben tener las siguientes especificaciones técnicas mínimas.

Estándares y protocolos soportados	802.11ax con soporte OFMDA Y MU-MIMO
	La solución debe soportar configuración de un servidor Syslog y SNMP V3.
	La solución debe soportar el protocolo LLDP
	Debe soportar los protocolos IEEE 802.1Q IEEE 802.3af/at clase 4 o superior IEEE 802.1x
	Soporte protocolo IPv6
Certificaciones WIFI-ALLIANCE	Wi-Fi CERTIFICADO a, b, g, n, ac
	Wi-Fi CERTIFICADO 6 (ax)
	WPA, WPA2 and WPA3-Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE)
	WMM, WMM-PS, Wi-Fi Vantage, W-Fi Agile Multiband
	Passpoint
Número de antenas para los AP	Mínimo 2 antenas
Operación MIMO	MU-MIMO 4x4:4 (5GHz)
Densidad clientes	Deben soportar al menos 16 SSID
	Deben soportar al menos 500 clientes por radio o más
	Para salas de conferencia se puede usar un tipo de AP de alta densidad con capacidad de más clientes por antena
Asignación y selección de canales y potencia	Automática
Interfaces	Al menos dos interfaces con las siguientes características: Int1: RJ45 100/1000/2500 base-T con capacidad de alimentación eléctrica vía estándar PoE 802.3af/at clase 4 o superior.
	Int2: RJ45 100/1000 base-T
	Las interfaces deben soportar LACP entre ellas.
	Interfaz de administración serial.
Alimentación eléctrica	Debe incluir alimentación PoE basada en el standard IEEE 802.3 af/at/ y/o bt
	Debe incluir PoE injector para cada uno de los APs, de tal manera que se garantice la potencia necesaria para el correcto encendido de todas las antenas y funcionalidades del AP, estos PoE injector deben ser nuevos de fábrica, de la misma marca de los APs, no se admiten PoE Injectors remanufacturados, reparados ni genéricos

Migración clientes	Debe contar con mecanismos automáticos que migren a los clientes hacia el punto de acceso que puede prestar el mejor nivel de servicio en todo momento, basado en información de ubicación del cliente, capacidades del dispositivo cliente, condiciones del entorno RF y congestión de los puntos de acceso, sin que requiera intervención del usuario y que aplique a las distintas marcas y modelos de dispositivos end points presentes en el mercado. Esto para evitar problemas asociado a sticky clients.
Modos de operación	Los AP deben contar con modo de operación tanto stand-alone, como AP controlado al integrarse al Wireless Access Controller físico (appliance) o gestionado desde la nube.
	Modo monitor red inalámbrica
	Los APs deberán tener la capacidad de operar en modo controlado usando su propio sistema operativo, sin necesidad de una controladora física, ni licencias adicionales.
	Modo analizador de espectro
Seguridad	Debe ser integrable a la solución NAC ofertada y debe ser de la misma marca
	Debe contar con un statefull firewall en capa 7, con Deep packet inspector que facilite la visibilidad de más de 2000 aplicaciones de uso común, y permita aplicar políticas granulares de seguridad, QoS, control de ancho de banda y filtrado web.
Montaje de los AP	Cada AP debe incluir su respectivo kit de montaje para superficies sólidas, los mismos deben ser nuevos de fábrica, de la misma marca de los APs, no se admiten kit de montaje genéricos.
Medio implementación o provisionamiento	Debe contar con mecanismos que permitan zero touch provisioning para implementación automática al contar con una conexión a Internet sin intervención de servicio técnico especializado.
Cifrado	Debe incluir soporte para cifrado mínimo WPA2 Enterprise y WPA3

Especificaciones técnicas mínimas para la controladora inalámbrica

La controladora inalámbrica debe contar con mínimo las siguientes especificaciones técnicas o capacidades:

Consola de administración	Debe contar con un dashboard gráfico en el que se visualice el estado de salud de la red, cantidad de dispositivos registrados, y cuantos están en operación y cuantos fuera de operación.
	Debe proveer estadísticas y alarmas del sistema
	Debe proveer estadísticas de los usuarios conectados y el tráfico entrante y/o saliente del sistema inalámbrico.
	Debe proveer estadísticas de los clientes donde se pueda determinar la velocidad de acceso, calidad de la señal, tipo de dispositivo conectado y SO.
	Debe proveer estadísticas del tiempo de operación
	Debe proporcionar para cada AP, información de estatus, cantidad de usuarios conectados en función del tiempo, SSID manejados, estatus de las interfaces y de sus radios

	Debe brindar información de las cantidades de usuarios en cada uno de los radios y sus parámetros de transmisión
	Posibilidad de creación de al menos dos SSID desde la consola de administración independientes para funcionarios y visitantes
	La solución de administración en Nube debe estar en capacidad de indicar la salud de la conexión de los usuarios, con al menos los siguientes parámetros: Asociación de usuario. - Autenticación de usuario. - Asignación de direccionamiento vía DHCP. - Conexión al Portal Cautivo. - Información del DNS.
	Para los APs debe brindar información de cada uno donde muestre el estatus, la cantidad de usuarios conectados en función del tiempo, los SSID que maneja, el estado de sus interfaces de red y de sus radios.
Portal cautivo	Debe tener la capacidad de proveer el servicio de portal cautivo para usuarios invitados.
	El portal cautivo debe ser personalizable cómo mínimo en el logo y texto de bienvenida
	Permitir la creación de accesos temporales
Filtrado y seguridad	Servicios de seguridad para identificación, clasificación y bloqueo de IPs, archivos o URLs maliciosos
	La solución inalámbrica debe contar con un statefull firewall en capa 7, con inspeccionador de paquetes que facilite la visibilidad de aplicaciones de uso común, y permita aplicar políticas granulares de seguridad, QoS, control de ancho de banda y filtrado web.
	La solución WLAN debe soportar funcionalidades de “Wireless Intrusion Detection System” (WIDS) y de “Wireless Intrusion Prevention” (WIPS).
	Debe contar con la capacidad de manejar roles por usuario y políticas basadas en identidad.
	La red WLAN debe poder identificar APs tipo “rogue”. Estos se consideran APs ajenos al sistema que irradian señal en el área de cubrimiento de la red, pero no están conectados a la red cableada.
	Los APs de la red WLAN deben tener funcionalidades de monitoreo del aire, que permitan detección de interferencias, APs tipo “rogue” y detección de ataques inalámbricos.
	Debe incluir soporte para cifrado mínimo WPA2 Enterprise y WPA3
Quality of service	La solución debe permitir marcación de prioridad QoS
	La solución debe poder identificar llamadas de voz y video (estándares SIP y H.323) y darles un tratamiento especial para su buen funcionamiento.
	La solución debe ajustar automáticamente la potencia de los radios
	La solución debe hacer conmutación inteligente y en tiempo real del canal.
	La solución debe evaluar la calidad del canal.

	La solución debe soportar “Band steering”, para forzar que un nuevo dispositivo asociado que la soporte, se ubique en la banda de frecuencia óptima, considerando la cantidad de clientes trabajando en la misma y el porcentaje de utilización del medio
	La solución debe poder balancear los clientes asociados entre diferentes APs
Monitoreo	Al menos soporte para: - SNMP v2c y v3. - HTML con SSL. - Consola serial.
Gestión y administración	La solución debe tener una interface centralizada con conexión web segura accesible desde cualquier lugar
	La solución debe ser en modelo cloud.
	Debe contar con la capacidad de centralizar el proceso de configuración mediante roles de usuario usuario y políticas basadas en identidad.
	La solución debe soportar aprovisionamiento automático (zero touch).
	La solución debe tener un dashboard intuitivo, con visibilidad de las aplicaciones y con filtros personalizados.
	La solución debe generar reportes técnicos de consumo, capacidad y tendencias.
	La solución debe permitir la integración de funcionalidades con otras marcas.
	La solución debe permitir la configuración masiva de todos los Access Point.
	La solución debe soportar el inicio único de sesión (SSO)
	La solución debe permitir la actualización programada de firmware.
	Centralizar todo el proceso de configuración del sistema mediante la creación de perfiles o carpetas, para simplificar la configuración de nuevos dispositivos.
	Brindar todo el manejo de registro de nuevos dispositivos.
	Permitir el acceso a la consola de configuración CLI de los APs y switches registrados en la plataforma de gestión.
	Debe manejar respaldo de la configuración de los APs
	La solución debe soportar configuración de portal cautivo embebido en la solución. deberá de tener la flexibilidad de crear portales cautivos para la validación de los diferentes tipos de usuarios.
	La solución debe permitir ver la ubicación de los Access Point y de los clientes conectados.
	Aun cuando los dispositivos gestionados pierdan la conexión al plano de control hacia la plataforma de administración en Nube o física, la red con todos sus Access Points, deben continuar operando.
	La comunicación entre la plataforma de gestión y los dispositivos gestionados debe realizarse a través de HTTPS.
Licenciamiento	Se debe garantizar la entrega de todos los licenciamientos necesarios para el funcionamiento de la solución
	El licenciamiento no debe estar atado a una característica del equipo como dirección MAC, de manera que las licencias se puedan reasignar con facilidad.

	El licenciamiento debe ser gestionado de manera centralizada y permitir hacer transferencias de licenciamiento
Expiración de servicio	Si a futuro Bancoldex decide no renovar las licencias de servicio, al expirar la suscripción de las mismas toda la infraestructura de red debe seguir operando, y debe existir la opción para cambiar a un modo de operación y administración local.
Servicios para el SW	El servicio de gestión en Nube se debe brindar por un periodo no menor a 3 años
	Se deben brindar las actualizaciones de software durante el mismo periodo de servicio (3 años)

Especificaciones técnicas mínimas NAC

La controladora de acceso a redes (NAC) debe contar con las siguientes características o especificaciones técnicas mínimas:

Compatibilidad	Debe ser una solución libre de agentes instalados en los dispositivos
	debe ofrecer compatibilidad con la solución de infraestructura de networking actual del banco Cisco ACI y debe ser agnóstica a los switches de borde
Capacidad	La solución deberá manejar hasta 10.000 sesiones RADIUS activas recurrentes.
	Soporte para Assessment de postura, perfilamiento y autenticación web en ambientes de red multi-vendor y basado en protocolos estándar RADIUS y RADIUS CoA
	Debe ser capaz de controlar el acceso de usuarios y dispositivos a través de la red cableada (switches), inalámbrica (access points y controladores WiFi) y VPN (firewalls y concentradores VPN) de manera unificada
	La política de seguridad deberá permitir tomar en consideración elementos contextuales como: horario, ubicación, tipo de dispositivo, versión de SO y nombre del dispositivo, entre otros
Reportes y estadísticas	Debe incluir un módulo o componente de monitoreo y reportería con información en tiempo real e histórica sobre usuarios y dispositivos conectados, alertas, detalle de autenticación y autorización, consumo de anchos de banda.
Perfilamiento	Debe soportar métodos de perfilamiento activos (NMAP, WMI, SSH, SNMP)
	Debe soportar métodos de perfilamiento pasivos (MAC OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFLOW, Puerto 'SPAN', HTTP User-Agent, IF-MAP)
	Debe soportar métodos de perfilamiento Integrados y de terceros: Desde la solucion de BYOD y de chequeo de postura, EMM/MDM, Rapid7, Cisco device sensor.
Licenciamiento de Servicios	Debe incluir licenciamiento base para los siguientes servicios: 802.1X
	Autenticación por MAC Address
	TACACS+
	Enforcement a través de SNMP
	Perfilamiento de dispositivo
	Integraciones con terceros mediante REST APIs
Protocolos para los servicios AAA	RADIUS, RADIUS CoA, TACACS+, autenticación web, SAML 2.0

	PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS. EAP-PEAP-Public,EAP-PWD)
	TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5,PAP, CHAP)
	EAP-TLS
	PAP, CHAP, MSCHAPv1 y 2, EAP-MD5
	OAuth2
	Autenticación de Máquina en dominio Windows
	SMB v2/v3
	Autenticación vía MAC (para dispositivos que no soportan 802.1x)
	- Online Certificate Status Protocol (OCSP)
	SNMP generic MIB, SNMP private MIB
	Common Event Format (CEF), Log Event Extended Format (LEEF)
	EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
Fuentes de autenticación	Debe soportar la autenticación sin licenciamiento o plug-ins adicional de las siguientes fuentes: - Microsoft Active Directory - RADIUS - Cualquier directorio basado en LDAP - MySQL, Microsoft SQL, PosGRES, Oracle 11g y cualquier servidor SQL ODBC-compliant - Servidores de Token - Base de datos Interna - Kerberos - Microsoft Azure Active Directory (via SAML y OAuth2.0) - Google G Suite
Single Sign On	La solución deberá soportar SAML tanto como SP e IdP y el protocolo Oauth para habilitar Single Sign On con aplicaciones y portales externos
Licenciamiento	El licenciamiento deberá ser perpetuo y debe incluir al menos 600 usuarios.
Integración con soluciones de terceros	Deberá tener la capacidad de integración vía REST-based APIs, de manera nativa y sin costo adicional de licenciamiento, con soluciones de Seguridad Perimetral (Ej: CheckPoint, Palo Alto, Fortinet, etc.), MDM/EMM (Ej.: Citrix, MobileIron, AirWatch), sistemas de gestión de tickets (Ej.: Service Now, y multiples factores de autenticación (Ej.: DUO, RSA SecurID), UEBA (IntroSpect)
Segmentación dinámica	Se requiere que la solución aplique el control de acceso y segmentación dinámica basada en roles, para evitar el uso de múltiples VLANs para aplicar políticas de seguridad
Disponibilidad del servicio	La Alta disponibilidad debe permitir modo activo/activo Se requiere que el failover en caso de fallas sea automático, sin necesidad de realizar tareas manuales
Certificados digitales	La solución deberá ser capaz de actuar como entidad certificadora Root o Intermediaria

SOPORTE

El modelo de soporte debe ser 5x8 NBD para atención de incidentes, requerimientos, cambios y actualizaciones de firmware de todos los dispositivos por parte del canal y para sustitución de partes directamente con el fabricante.

GESTION DEL SERVICIO

EL CONTRATISTA realizará su gestión para cumplir los siguientes tiempos de atención para el servicio

Horario de prestación del servicio para la atención de requerimientos, incidentes y cambios	5x8 Atención 4 horas Solución 8 horas o de acuerdo con plan de trabajo

CONTRATACIÓN

El contrato de soporte, garantía y licenciamiento de la solución deberá ser a 3 años. Igualmente, el servicio de mantenimiento, actualizaciones, atención de incidentes y requerimientos asociados a la plataforma de Wireless se deberá proyectar a 3 años.

IMPLEMENTACIÓN

Los equipos no pueden ser entregados en más de 180 días.

La implementación se hará una vez recibidos los equipos y no puede durar más de 60 días.

Para recibir la solución a satisfacción después de implementación, se deben generar los siguientes entregables:

1. Documentación técnica de la solución implementada que incluya:
    - Distribución de los AP's instalados en su totalidad en planos de pisos y sucursales
    - Arquitectura implementada para solución de conectividad inalámbrica.
    - Arquitectura implementada para solución de control de acceso a redes.
    - Informe de certificación de cobertura de redes inalámbricas.

2. Manuales de usuario y configuración de la solución
3. Listas de participantes en las capacitaciones de transferencia de conocimiento.

CAPACITACIÓN Y TRANSFERENCIA DE CONOCIMIENTO

El proveedor debe realizar el número de sesiones necesarias de transferencia de conocimiento para el equipo de infraestructura, en las que se debe asegurar que el personal

del banco esté en la capacidad de administrar la plataforma en su totalidad para poder realizar configuraciones, diagnósticos de fallas y generar posibles soluciones. La duración mínima de esta transferencia de conocimiento es de 15 horas y se deben contemplar los costos para una audiencia mínima de 10 personas.

El proveedor deberá incluir en la propuesta capacitación certificada de fábrica para uno de los integrantes del equipo de infraestructura seleccionado por el banco de la solución implementada.