CONSULTAS Y OBSERVACIONES
ADQUISICION NIVEL II N° 023-2024-AGROBANCO
“Adquisición de Licencias NAC”

Proveedor: IMPERIA SOLUCIONES TECNOLOGICAS SAC

ormu	Formula	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se	Respuesta
1	Consulta	Capítulo III	3.8.1		26	Dice:"Un (01) Jefe de Proyecto Certificado ITIL vigente." Consulta: Teniendo en cuenta que el certificado ITILv3 no tiene fecha de fin de vigencia, sírvase confirmar que se aceptará la certificación ITIL v3, esto para permitir una mayor pluralidad de postores.		Se confirma aceptar la certificacion ITIL v3
2	Consulta	Capítulo III	3.8.2		27	Dice:"Un (01) especialista en redes para la solución NAC Mínimo bachiller ó profesional en Ingeniería de Sistemas e Informática, Ingeniería de Telecomunicaciones, Ingeniería de Electrónica, Ingeniería de Seguridad y Auditoría Informática, Técnico en seguridad informática, Técnico en Redes y Comunicaciones de Datos, o afines." Consulta: Para permitir una mayor pluralidad de postores sírvase confirmar, que con la mención de carreras "afines", la entidad aceptará a profesional técnico en computación e informática.		La entidad si aceptara a profesional tecnico en computacion e informatica
3	Consulta	Capítulo III	IV.2.1	d)	31	Dice: "IV.2.1. Instalación y Configuración El POSTOR dejará implementado los mecanismos necesarios para el despliegue de las licencias restantes en todos los equipos del BANCO, dado a que los equipos están tanto en Oficina Principal como en todas las oficinas que están en las distintas ubicaciones dentro del territorio peruano." Consulta: "Sírvase a la entidad confirmar si el despliegue de la solución para las oficinas remotas, estarán involucradas dentro del primer paquete de despliegue de 300 dispositivos finales"		Para el despliegue del primer paquete de 300 dispositivos finales se realizara en la Of. Principal y no en oficinas remotas
4	Consulta	Capítulo III	IV.2.1	d)	31	Dice: "IV.2.1. Instalación y Configuración El POSTOR dejará implementado los mecanismos necesarios para el despliegue de las licencias restantes en todos los equipos del BANCO, dado a que los equipos están tanto en Oficina Principal como en todas las oficinas que están en las distintas ubicaciones dentro del territorio peruano." Consulta: "Sírvase a la entidad confirmar cuál es la arquitectura de conexión entre la sede principal y sedes remotas que permitirán realizar la sincronización de los switches remotos hacia la solución NAC"		Mediante RPV (enlace de datos), Site to Site (Internet), Client to Site (internet)

5	Consulta	Capítulo III	IV.2.3	a)	32	Dice: "IV.2.3. Migración de Políticas y Reglas Migración de las políticas de acceso existentes a la nueva solución NAC." Consulta: "Sírvase a la entidad aclarar cuál es la solución actual con la que cuenta, en las que existen las políticas de acceso existentes que se tendrán que migrar a la nueva solución NAC"		No se cuenta con solucion NAC. La migracion seria mediante la politicas de acceso del AD
6	Consulta	Capítulo III	IV.3.3	a)	33	Dice: "IV.3.3. Garantía Presentar carta del fabricante que se indique que los componentes son nuevos y originales" Consulta: "Sírvase confirmar con la entidad que la carta requerida se presentará para la etapa de perfeccionamiento del contrato"		La carta de Garantia requerida se debera entregar al momento de la entrega de los equipos
7	Consulta	Capítulo III	IV.1.1		28	Dice: "Soporte de varias fuentes de autenticación Tales como RADIUS, LDAP, LDAPS, AD, HTTP, SQL, Kerberos u Okta" Consulta: "Se solicita confirmar que las fuentes de autenticación LDAPS, SQL u OKTA, se acepten de manera opcional con la finalidad de permitir mayor pluralidad de postores."		Aunque es opcional el uso de SQL u Okta, si es requerido LDAPS o la implementacion de alguna otra capa de seguridad(como StartTLS) que asegure que los datos no viajen en claro como lo hace al utilizar LDAP, siendo esta informacion critica y sensible por ser parte del proceso de autenticacion.
8	Consulta	Capítulo III	IV.1.1		28	Dice: "Los tipos de enforcements aplicados para cada uno de los servicios de autenticación podría ser cualquier de los siguientes: ▪ RADIUS enforcement permit / deny / CoA ▪ Policy assignment ▪ SNMP enforcement ▪ DACL ▪ TACACS+ ▪ HTTP ▪ Filter Id" Consulta: "Se solicita confirmar que los tipos de enforcements solicitados como DCAL, TACACS+, HTTP y Filter ID, se acepten de manera opcional con la finalidad de permitir mayor pluralidad de postores."		Pueden ser opcionales DACL, HTTP y Filter Id, mas no TACACS+ ya que es uno de los mas usados junto a RADIUS. Y TACACS+ sera implementado para mejorar la gestion y control de nuestra red.

9	Consulta	Capítulo III	IV.1.1		28	Dice: "Deberá permitir utilizar atributos de múltiples repositorios de identidad tales como Microsoft Active Directory, LDAP, base de datos SQL compatibles con OBDC, servidores de Token o base de datos interna, con el objetivo de utilizar estos atributos dentro de una política para un control granular." Consulta: "Se solicita confirmar que los atributos de base de datos SQL compatibles con ODBC, serán aceptados de manera opcional para permitir una mayor pluralidad de postores"		De acuerdo a la arquitectura actual del Banco, es opcional el uso de ODBC para base de datos, por lo que no se requiere
10	Consulta	Capítulo III	IV.1.1		29	Dice: "Identificación y clasificación (profiling) basada en datos contextuales tales como: ▪ MAC OUIs ▪ Nmap Scan ▪ DHCP fingerprints ▪ TCP fingerprints ▪ HTTP user agent ▪ SNMP traps ▪ LLDP ▪ Netflow / IPFIX ▪ WMI ▪ Span Port" Consulta: "Se solicita confirmar que la opción de identificación y clasificación mediante LLDP, serán aceptados de manera opcional para permitir una mayor pluralidad de postores"		La opcion de profiling LLDP es opcional ya que esta es una de las tecnologías utilizadas para descubrir información sobre los dispositivos conectados a la red y facilitar la clasificación y control de acceso, pero también existen otras opciones como SNMP, filtrado de direcciones MAC, DHCP, etc.
11	Consulta	Capítulo III	IV.1.1		29	Dice: "Deberá informar sobre la integridad del dispositivo final como el estado del antivirus, anti-spyware, firewall, aplicaciones peer-to-peer, a los cuales se les definirá la autorización de su uso." Consulta: "Se solicita confirmar que la opción de informar sobre el estado de anti-spyware, serán aceptados de manera opcional para permitir una mayor pluralidad de postores"		El estado del anti-spyware seria Opcional, ya que el BANCO cuenta con software especializado que adiciona una capa de seguridad mas.
12	Consulta	Capítulo III	IV.1.1		29	Dice: "El sistema proporcionará un agente ligero NAC (Network Access Control) que garantice la integridad de los dispositivos. Este agente comprobará el estado y actualización de anti-virus, anti-spyware, firewalls, etc., y proporcionará instrucciones de remediación en caso de que el dispositivo viole las políticas corporativas. El agente deberá ser compatible con, al menos: Windows, Linux y MacOS." Consulta: "Se solicita confirmar que la opción de informar sobre el estado de anti-spyware e instrucciones de remediación en caso de que el dispositivo viole las políticas corporativas, serán aceptados de manera opcional para permitir una mayor pluralidad de postores"		El estado del anti-spyware e instrucciones de remediacion en caso el dispositivo viole las potlicas corporativas, seria Opcional, ya que el BANCO cuenta con software especializado que adiciona una capa de seguridad mas.

13	Consulta	Capítulo III	IV.1.1		29	Dice: "Deberá soportar la auto-remediación para los dispositivos que no cumplen las políticas de salud." Consulta: "Se solicita confirmar que esta opción será aceptada de manera opcional para permitir una mayor pluralidad de postores"		La Autoremediacion sera considerada como Opcional, ya que al identificar el equipo y este no cumpla con las condiciones o politicas, no le permitira su acceso.
14	Consulta	Capítulo III	IV.1.1		30	Dice: "La plataforma debe permitir el uso de protocolos SNMP y SSH para realizar el enforcement de políticas" Consulta: "Se solicita confirmar que la opción de SSH será aceptada de manera opcional para permitir una mayor pluralidad de postores"		Para el SNMP debera de utilizar la v3 que es mas segura. La implementación de SSH es crucial para garantizar la seguridad en la administración remota y la transmisión de datos entre los dispositivos de red y el sistema NAC. Si no se implementa SSH, la red se expone a riesgos de interceptación y manipulación de datos. Sin embargo, existen alternativas para asegurar que la información se maneje de forma segura, como el uso de VPN, TLS/SSL, 802.1X, y autenticación multifactor, pero es requerido la implementacion de SSH.
15	Consulta	Capítulo III	IV.1.1		31	Dice: "Deberá soportar LDAP y LDAPS" Consulta: "Se solicita confirmar que la opción de LDAPS será aceptada de manera opcional para permitir una mayor pluralidad de postores"		Es requerido LDAPS o la implementacion de alguna otra capa de seguridad(como StartTLS) que asegure que los datos no viajen en claro como lo hace al utilizar LDAP, siendo esta informacion critica y sensible por ser parte del proceso de autenticacion.

CORONADO LEON Rafael FAU 20504565794 soft

Firmado digitalmente por CORONADO LEON Rafael FAU 20504565794 soft
Fecha: 2024.12.17 11:16:25 -05'00'

Rafael Coronado León

BLAS RIVERA Martin Felipe FAU 20504565794 soft

Firmado digitalmente por BLAS RIVERA Martin Felipe FAU 20504565794 soft
Fecha: 2024.12.17 17:53:39 -05'00'

Martín Blas Rivera

MORANTE MARIÑO Miguel Cristopher FAU 20504565794 soft

Firmado digitalmente por MORANTE MARIÑO Miguel Cristopher FAU 20504565794 soft
Fecha: 2024.12.17 11:27:18 -05'00'

Miguel Morante Mariño