RESPUESTAS A SOLICITUD DE ACLARACIONES

La Gerencia de Adquisiciones (GAD), del Banco Central de Nicaragua (BCN), informa a las personas proveedores, que se está procediendo a dar respuestas a consultas realizadas por medio de correo electrónico, relacionadas a la Invitación a Ofertar, correspondiente al proceso de **Contratación Ordinaria de Régimen Especial No. BCN-01-1-26-CORE, "Auditoría de cumplimiento de programa de seguridad (SWIFT)"**, que a continuación, se detallan:

Sobre Arquitectura y conectividad SWIFT

Pregunta No. 1

¿Cuántos servidores y estaciones de trabajo conforman el alcance de la "Secure Zone" de SWIFT? ¿Está esta zona segmentada lógica o físicamente del resto de la red?

Respuesta No. 1

El inventario de equipos que conforman la zona segura corresponde a: 1 servidor y 10 estaciones de trabajo. Esta segmentada lógicamente.

Pregunta No. 2

¿Cuántos centros de datos con información SWIFT tienen (incluyendo réplicas)?

Respuesta No. 2

No Aplica.

Pregunta No. 3

¿Cómo interactúan los operadores y los sistemas del banco con Alliance Lite2?

- ¿Es exclusivamente un acceso manual (flujo U2A) o tienen el Core Bancario integrado para transacciones automáticas (flujo A2A)?
- En caso de integración automática (A2A): ¿Qué tipo de software utilizan localmente para conectarse al servicio Lite2 (ej. Alliance Lite2 AutoClient, sFTP, MQ, o middleware comercial)?

Respuesta No. 3

Es acceso exclusivo al Alliance Lite 2 de SWIFT. No está integrado al Core Bancario. No se utiliza Middleware, por tanto, no hay flujo de intermedio adicional.

Pregunta No. 4

¿La gestión de la infraestructura local recae 100% en el personal interno o hay proveedores externos en el alcance?

Respuesta No. 4

La zona segura de SWIFT, es administrada por personal interno del BCN.

Sobre el Análisis de Vulnerabilidades (NVA):

Pregunta No. 5

¿Cuántas direcciones IP (hosts activos) o URLs conforman el alcance externo e interno para el análisis?

Respuesta No. 5

Son 94 segmentos de red privados/24 y 6 URL´s públicas.

Pregunta No. 6

¿Los escaneos internos deben ser autenticados (con credenciales) o no autenticados?

Respuesta No. 6

Se requiere que sea no autenticados.

Pregunta No. 7

¿El alcance incluye una fase de Re-test para validar la remediación de vulnerabilidades o el servicio finaliza con la entrega del primer informe?

Respuesta No. 7

El oferente adjudicado tendrá la obligación de entregar un informe detallado con las recomendaciones técnicas necesarias para la remediación de las vulnerabilidades identificadas en

el análisis. Dicho informe deberá incluir medidas concretas de mitigación, priorización de riesgos. No será requerido un re-test posterior; sin embargo, el oferente será responsable de asegurar que las recomendaciones propuestas sean suficientes y aplicables para reducir la exposición de los sistemas a los riesgos detectados.

Sobre las Pruebas de Penetración (Pentest):

Pregunta No. 8

¿Se realizará la prueba para los mismos activos que el NVA?

Respuesta No. 8

No, porque en el Pentest se incluyen los 3 segmentos de red público, 1 IP pública.

Pregunta No. 9

¿El alcance es de tipo Caja Negra, Caja Gris o Caja Blanca?

Respuesta No. 9

Caja gris.

Pregunta No. 10

¿Cuántos servidores, equipos o aplicaciones web específicas están dentro del alcance?

Respuesta No. 10

Aproximadamente 100 servidores, 200 PC y 30 App Web.

Pregunta No. 11

¿El Pentest está limitado exclusivamente a la zona segura de SWIFT o abarca la red corporativa general?

Respuesta No. 11

Red LAN en general y los segmentos de red públicos.

Pregunta No. 12

¿El alcance incluye una fase de Re-test para validar la remediación o finaliza con la entrega del primer informe?

Respuesta No. 12

El alcance definido para las pruebas de penetración es la entrega del informe inicial, en el cual se detallan las vulnerabilidades encontradas, su criticidad y las recomendaciones de mitigación. No está contemplada una fase de re-test dentro del alcance actual. Sin embargo, el oferente tiene la obligación de entregar las mejores recomendaciones técnicas y organizativas para fortalecer la seguridad de la infraestructura.

Especificaciones de Capacitación:

Pregunta No. 13

Sobre las dos (2) sesiones de concienciación de 2 horas: ¿Serán presenciales o virtuales?

Respuesta No. 13

Serán virtuales y presenciales en coordinación con la Gerencia de Servicios Tecnológicos.

Pregunta No. 14

¿Aproximadamente cuántos usuarios asistirán por sesión?

Respuesta No. 14

Al menos 200 colaboradores.

Dado en la ciudad de Managua, el día 25 de febrero de 2026.

Ericka del Carmen González Castillo
Especialistas en Adquisiciones I

Gerencia de Adquisiciones

cc: Expediente/KC