BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME N° 0064-2020-GTI230-N

ASUNTO : Informe técnico previo de evaluación de software -
Renovación de suscripciones de la solución de control de
acceso a red (NAC)

1. NOMBRE DEL ÁREA:

Dpto. de Redes, Telecomunicaciones y Bases de Datos

2. RESPONSABLE DE LA EVALUACIÓN:

Alexander Gamboa Inga

3. CARGO:

Especialista en Redes, Telecomunicaciones y Bases de Datos

4. JUSTIFICACIÓN:

El control de acceso a red ha llegado a ser esencial en las redes corporativas. La evolución de las prácticas empresariales, así como la necesidad del cumplimiento de regulaciones y el explosivo crecimiento de las vulnerabilidades están llevando a las empresas a la necesidad de controlar quien puede ser admitido en la red corporativa y que recursos (servidores, aplicaciones, datos almacenados) pueden accederse. De tal forma que las empresas han empezado a proactivamente asegurar la aplicación de las políticas corporativas porque los riesgos son demasiado altos si es que sólo se confía en que todos los usuarios se adherirán al cumplimiento de las políticas de seguridad y acceso, por si mismos.

La automatización de los procesos de negocio ha incrementado la dependencia corporativa en la información basada en red. Al mismo tiempo la comunidad de usuarios ha llegado a ser más diversa y los límites corporativos son más flexibles. Es común la presencia de personal externo (visitantes, contratistas, consultores, etc.) con necesidades diversas de acceso a la red y a las aplicaciones, y que conforman una fuerza de trabajo dinámica con diferentes requerimientos y que pueden operar desde diferentes ubicaciones.

Por otra parte, la adopción de nuevas tecnologías y la transformación de la red corporativa en una infraestructura de comunicaciones convergente, han llevado a la proliferación de nuevos dispositivos en la red, tales como teléfonos IP, cámaras de seguridad, lectores de código de barras, entre otros. En medio de esta nueva era de apertura, las empresas deben asegurar el cumplimiento de las regulaciones de la industria y el Gobierno, lo que implica que deben demostrar que tienen controles de acceso estrictos para proteger datos críticos y sensitivos tales como la información financiera, tarjetas de crédito y registros con información personal de empleados y clientes.

BANCO CENTRAL DE RESERVA DEL PERÚ

Ante esta situación se desarrolló la tecnología de protección denominada sistemas de control de acceso a red (NAC – Network Access Control), que proporcionan las siguientes funcionalidades:

- **Control de acceso a la red**
Proporciona acceso a la red en base a la identidad de los endpoints (nodos de red). De esta forma puede limitar la conectividad según el perfil de acceso (usuario estándar, visitante, etc.).
- **Verificación de cumplimiento y remediación**
Determinar si los endpoints cumplen con las políticas de configuración de dispositivos y en base al resultado obtenido tomar una acción (permitir/denegar/remediar).

Next Generation NAC

La primera generación de soluciones NAC se enfrentó a la siguiente problemática:

- ✓ **Nuevos dispositivos y aplicaciones**
El uso de dispositivos móviles en el entorno laboral ha complicado enormemente la seguridad. Hoy en día se realizan transacciones y acceso a información sensible a través de teléfonos móviles y tabletas con acceso a Internet, por lo que se requiere entregar servicios seguros a través de dichos dispositivos.
- ✓ **El incremento en la frecuencia y complejidad de las amenazas de seguridad**
Cada día se incrementa el número de amenazas, las mismas que se hacen cada vez más sofisticadas en sus estrategias, con lo cual la detección de las mismas es cada vez más compleja.

Ante la problemática mencionada surgió una nueva generación de soluciones NAC (Next Generation NAC), enfocadas en los siguientes procesos clave:

- ✓ **Visibilidad de toda la red**
Las soluciones NAC deben identificar, inspeccionar y controlar todos los dispositivos que se conectan a la red, incluyendo tanto a dispositivos que se conectan a redes cableadas, como a los que se conectan a través de redes inalámbricas y aquellos que acceden remotamente, garantizando en todos ellos el cumplimiento de políticas y la mitigación de amenazas. La continua visibilidad y control de la red permiten atender riesgos concernientes a varias tendencias actuales tales como la creciente demanda por acceso a recursos de red, el incremento en el número y tipos de dispositivos móviles y personales, y la adopción de servicios móviles, virtuales y en nube.
- ✓ **Monitoreo continuo y protección avanzada**
Las soluciones NAC deben permitir definir, implementar y hacer cumplir políticas de acceso granulares para la conexión de los dispositivos finales, basadas en la identidad del usuario, roles, tipo de dispositivos, postura de seguridad, ubicación y otros factores. Para lograr ello, la tecnología NAC debe ser capaz de identificar los dispositivos, independientemente del tipo de dispositivo y el método de conexión empleado. NAC actúa como un monitor centralizado de políticas de seguridad de red, las cuales también se encarga de hacer cumplir a través de su interacción con los sistemas de acceso, la infraestructura de red, el software de protección de nodos finales, sistemas de monitoreo, entre otros componentes de la infraestructura tecnológica. NAC reduce el riesgo de exposición a malware, APT (Advanced Persistent Threat) y

BANCO CENTRAL DE RESERVA DEL PERÚ

ataques, reduciendo el vector de amenaza que representan dispositivos inseguros, comprometidos, desconocidos, usuarios no autorizados y aplicaciones no seguras.

NTP-ISO/IEC 27001 : 2014 y NAC

Las soluciones Next Generation NAC nos permiten implementar controles requeridos en el Anexo A de la norma NTP-ISO/IEC 27001 : 2014, entre ellos:

Dominio	Objetivos de control	
Gestión de activos	8.1.1	Inventario de activos
Control de acceso	9.1.1	Política de control de acceso
	9.1.2	Acceso a redes y servicios de red
Seguridad de las operaciones	12.2.1	Controles contra códigos maliciosos
	12.4.1	Registro de eventos
	12.5.1	Instalación de software en sistemas operacionales
	12.6.1	Gestión de vulnerabilidades técnicas
	12.6.2	Restricciones sobre la instalación de software
Seguridad de las comunicaciones	13.1.1	Controles de la red
	13.1.3	Segregación de redes
Adquisición, desarrollo y mantenimiento de sistemas	14.2.4	Restricciones sobre cambios a los paquetes de software
	14.2.8	Pruebas de seguridad del sistema
Cumplimiento	18.2.3	Revisión del cumplimiento técnico

5. ALTERNATIVAS:

El BCRP cuenta con la solución de control de acceso a red (NAC), de la marca Forescout y modelo VCT-4000, adquirida el año 2016. Esta solución se encarga de brindar control en la conexión a la red informática institucional.

6. ANÁLISIS COMPARATIVO TÉCNICO:

Debido a que es una solución con la cual ya cuenta el BCRP desde el año 2016, y el cual ha sido solicitado sea estandarizado, lo que se desea es contratar el servicio de renovación de suscripciones.

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- Identificar, inspeccionar y controlar todos los dispositivos que se conectan a la red.
- Definir, implementar y hacer cumplir políticas de acceso granulares para la conexión de los dispositivos finales, basadas en la identidad del usuario, roles, tipo de dispositivos, postura de seguridad, ubicación y otros factores.
- Reducir el vector de amenaza que representan dispositivos inseguros, comprometidos, desconocidos, usuarios no autorizados y aplicaciones no seguras

BANCO CENTRAL DE RESERVA DEL PERÚ

Costos:

Las prestaciones requeridas corresponden al periodo de tres (03) años de servicio:

- Prestación principal: Suscripción a los servicios del fabricante Forescout
Actualizaciones de software (incluyendo el suministro de nuevas versiones y patches), soporte técnico del fabricante (escalamiento).
- Prestación accesoria: Servicios del partner (proveedor local)
Mesa de ayuda y soporte presencial, en el esquema 24x7x2 y mantenimiento técnico preventivo anual.

En lo que respecta a los costos asociados, la solución fue adquirida por S/ 600 000,00 (LP 0014-2016-BCRPLIM). Se estima que el costo de la renovación de suscripciones por el periodo de tres (03) años no debe exceder de S/ 225 000,00 incluido IGV, lo que representa el 37,5% del monto de adquisición.

8. CONCLUSIONES:

Por lo expuesto anteriormente, se considera conveniente la contratación de la renovación de suscripciones de la solución de control de acceso a red (NAC).

Lima, 21 de febrero de 2020

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

VISADO POR: