BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME N° 0057-2023-GTI230-N

ASUNTO : Informe técnico previo de evaluación de software –
Contratación de suscripciones para el sistema de control de
acceso a red (NAC - Network Access Control)

1. NOMBRE DEL ÁREA:

Dpto. de Ciberseguridad y Redes

2. RESPONSABLE DE LA EVALUACIÓN:

Alexander Gamboa Inga

3. CARGO:

Especialista en Ciberseguridad y Redes

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 proactivamente a asegurar la aplicación de las políticas corporativas pues 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 sí 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, permitiendo la aplicación de políticas (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

BANCO CENTRAL DE RESERVA DEL PERÚ

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

Implementación de la Norma ISO/IEC 27001: 2022 y NAC

Las soluciones Next Generation NAC nos permiten implementar controles requeridos en el Anexo A de la norma ISO/IEC 27001: 2022, entre ellos:

Group	Controls	
Organizational controls	5.9	Inventory of information and other associated assets
	5.15	Access control
	5.36	Compliance with policies, rules and standards for information security
Technological controls	8.7	Protection against malware
	8.8	Management of technical vulnerabilities
	8.15	Logging
	8.19	Installation of software in operational systems
	8.20	Networks security
	8.22	Segregation of networks

Implementar controles del NIST Cybersecurity Framework

Las soluciones Next Generation NAC nos permiten implementar controles requeridos del NIST Cybersecurity Framework, entre los que se encuentran:

Identificador de la función	Función	Identificador de la categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
PR	Proteger	PR.AC	Control de accesos
		PR.PT	Seguridad Tecnológica
DE	Detectar	DE.CM	Control continuo de seguridad
RS	Responder	RS.MI	Mitigación

Solución NAC y el modelo de Zero Trust

El modelo de Zero Trust es un enfoque de seguridad que se basa en la premisa de que ningún dispositivo o usuario se puede confiar automáticamente, independientemente de su ubicación física o lógica en la red. En lugar de confiar en las barreras perimetrales para proteger la red, el enfoque de Zero Trust se basa en la verificación continua de la identidad y la política de seguridad antes de permitir el acceso a recursos.

BANCO CENTRAL DE RESERVA DEL PERÚ

Se basa en cinco pilares:

- ✓ **Identidad:** Verificar la identidad de los usuarios y dispositivos antes de permitir el acceso a los recursos.
- ✓ **Acceso:** Controlar y limitar el acceso a los recursos de acuerdo con las políticas de seguridad.
- ✓ **Red:** Segmentar la red para limitar el impacto de un posible compromiso.
- ✓ **Dispositivo:** Verificar la configuración y el cumplimiento de los dispositivos antes de permitir el acceso a la red.
- ✓ **Servicios:** Proteger los servicios críticos mediante la implementación de medidas de seguridad adicionales.

El modelo de seguridad Zero Trust tiene como objetivo mejorar la seguridad de la red mediante la implementación de controles de seguridad adicionales que se aplican a todos los dispositivos y usuarios, independientemente de su ubicación en la red. Esto ayuda a garantizar que solo los dispositivos y usuarios autorizados tengan acceso a los recursos, lo que reduce el riesgo de ataques y compromisos de seguridad.

La solución NAC ayuda a implementar el enfoque de Zero Trust al controlar y restringir quién tiene acceso a la red. Al utilizar técnicas de autenticación, verificación de cumplimiento y políticas de acceso, una solución NAC ayuda a garantizar que solo los usuarios y dispositivos autorizados tengan acceso a la red. Esto es especialmente importante en un enfoque de Zero Trust, donde no se confía automáticamente en ningún dispositivo o usuario que intenta acceder a la red.

Además, una solución NAC también puede ayudar a implementar políticas de seguridad basadas en el contexto, como la ubicación geográfica del usuario, el tipo de dispositivo que está utilizando y el momento del día. Esto permite a los administradores de seguridad adaptar dinámicamente los niveles de acceso y las políticas de seguridad en función de las necesidades actuales de la red, lo que ayuda a reforzar el enfoque de Zero Trust.

Resumen del historial de contratación

En el año 2010, a través del ítem 02 del proceso ADP 0009-2010-BCRPLIM – Sistema de seguridad informática para el control de acceso a red (NAC), el BCRP adquirió dos appliances Juniper UAC IC 4500, incluyendo tres (03) años de los servicios de garantía de hardware, mantenimiento de software y soporte técnico.

Mediante el proceso AMC-0045-2014-BCRPLIM, fue renovado el servicio de mantenimiento de los equipos Juniper UAC en el año 2014. En el mismo año Juniper vendió la línea de productos UAC a la empresa Pulse Secure, completando la transferencia de servicios el 31 de julio de 2015.

En el año 2016 a través del proceso LP 0014-2016-BCRPLIM, el BCRP adquirió una nueva solución de control de acceso a red de la marca Forescout con modelo VCT-4000, basada en licenciamiento perpetuo.

BANCO CENTRAL DE RESERVA DEL PERÚ

En el año 2020, se realizó la contratación de la renovación de servicios para la solución NAC de la marca Forescout mediante la adjudicación simplificada N° AS 0014-2020-BCRPLIM, incluyendo tres (03) años de los servicios de mantenimiento de software y soporte técnico.

Para el presente año 2023, de acuerdo con lo comunicado por la marca Forescout, su línea de productos NAC utilizará en adelante el modelo de licenciamiento basado en suscripción, por lo cual ya no será posible realizar la contratación de la renovación de servicios para la solución con que cuenta el BCRP, pues esta utiliza licenciamiento perpetuo, siendo necesario realizar un proceso de contratación sin estandarización.

5. ALTERNATIVAS:

Consideramos los siguientes productos:

- ✓ Forescout NAC (eyeSight, eyeControl, eyeRecover)
- ✓ HPE Aruba ClearPass
- ✓ Cisco ISE

6. ANÁLISIS COMPARATIVO TÉCNICO:

El análisis técnico ha sido realizado de conformidad con la metodología establecida en el documento "Guía Técnica sobre evaluación de software en la administración pública" (Resolución Ministerial N° 139-2004-PCM), tal como se exige en el reglamento de la Ley N° 28612.

a. Propósito de evaluación

Comparar alternativas de productos existentes en el mercado.

b. Identificar el tipo de producto

Solución de control de acceso a red.

c. Identificación del modelo de calidad

Se aplicará el Modelo de Calidad de Software descrito en la Parte I de la Guía de evaluación de software aprobado por RM N° 139-2004-PCM.

d. Selección de métricas.

Las métricas fueron seleccionadas en base a las características técnicas descritas en el Anexo N° 1.

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

En el análisis costo beneficio se han tomado en cuenta los siguientes conceptos:

- ✓ Licenciamiento
Se requiere licenciamiento basado en suscripción por el periodo de tres (03) años.
- ✓ Hardware necesario para su funcionamiento

BANCO CENTRAL DE RESERVA DEL PERÚ

El BCRP proporcionará recursos de hardware virtual necesarios para el funcionamiento de la solución, hasta el siguiente límite:

- ✓ Soporte y mantenimiento externo
Se solicita incluir el soporte técnico del fabricante (brindado como parte de la suscripción a ser contratada), así como el soporte técnico del partner local.
Se solicita incluir el mantenimiento técnico preventivo periódico (al menos una vez al año) por parte del partner local.
- ✓ Personal y mantenimiento interno
Personal del Dpto. de Ciberseguridad y Redes será encargado de la administración de la solución, así como de brindar soporte técnico interno o gestionar el soporte técnico externo, ante incidentes que puedan presentarse.
- ✓ Capacitación
Se requiere incluir la capacitación oficial para seis (06) participantes.

Costos:

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

- Prestación principal: Suscripciones de software
Licenciamiento basado en suscripción, 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 técnico (incluido el soporte presencial), en el esquema 24x7x2 y mantenimiento técnico preventivo anual.
- Prestación accesoria: Capacitación
Capacitación oficial para seis (06) participantes.

8. CONCLUSIONES:

Considerando la necesidad de controlar el acceso a la red institucional del BCRP, se recomienda la Contratación de suscripciones para el sistema de control de acceso a red (NAC - Network Access Control), por el periodo de tres (03) años

BANCO CENTRAL DE RESERVA DEL PERÚ

ANEXO N° 1

ATRIBUTOS Y MÉTRICAS

N°	Atributos	Puntaje máximo	Forescout NAC	HPE Aruba ClearPass	Cisco ISE
1	Control de acceso a redes wired basado en 802.1x	8	8	8	8
2	Control de acceso a redes wired sin requerir 802.1x	10	10	9	9
3	Control de acceso a redes wireless basado en 802.1x	8	8	8	8
4	Integración con controladores VPN	6	4	4	4
5	Perfilamiento de dispositivos	10	10	8	8
6	Verificación de compliance	8	8	8	8
7	Gestión de usuarios invitados	8	8	8	8
8	Soporte de entornos virtuales	8	8	8	8
9	Flexibilidad de políticas	10	10	9	9
10	Integración con soluciones de terceros	8	8	7	7
11	Soporte de alta disponibilidad	8	8	8	8
12	Soporte técnico local	8	8	8	8
Puntaje Total		100	98	93	93

Lima, 21 de marzo de 2023

cc.

N° Sistema: INF-2023-001998

Firmado con certificados digitales emitidos por RENIEC. Los nombres de los firmantes figuran en la última página.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

VISADO POR: