PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA EL SUMINISTRO Y PUESTA EN MARCHA DE UNA SOLUCIÓN DE SEGURIDAD PARA EL CONTROL DE ACCESO A LA RED CORPORATIVA EN LA ADMINISTRACIÓN DEL PRINCIPADO DE ASTURIAS. (Expediente Nº 40/2017)

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

Contenido

1. Introducción 3
2. Objeto de la contratación 4
3. Descripción del suministro a realizar 5
3.1. Características técnicas 5
3.1.1. Operativa y funcionalidades 5
3.1.2. Modularidad y escalabilidad 8
3.1.3. Instalación 9
3.1.4. Consola de gestión 9
3.1.5. Integraciones 10
3.1.6. Políticas 11
3.1.7. Cuarentena y remediación 13
3.1.8. Protección 13
3.1.9. Gestión de vulnerabilidades 14
3.1.10. Continuidad del servicio 14
3.1.11. Inventarios 15
3.1.12. Informes 15
3.1.13. Manuales de la herramienta 16
3.1.14. Hardware de la solución 16
4. Servicios de instalación 17
5. Servicios de formación 18

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

1. Introducción

En los últimos años la Administración del Principado de Asturias ha hecho un importante esfuerzo en el ámbito de las tecnologías de la información, avanzando de forma importante en temas como la administración electrónica, los servicios electrónicos al ciudadano o la interconexión con otras administraciones y redes de terceros. La importancia y la criticidad de los sistemas informáticos y de las redes de la organización ha aumentado decisivamente y en igual medida la necesidad de aumentar los controles de seguridad sobre ellos.

Es vital que los sistemas informáticos cumplan con su finalidad en las mejores condiciones técnicas y operativas, y desde luego sin olvidar esa atención prioritaria a la seguridad y a la protección de la información; la actual coyuntura de virulencia de los ataques informáticos obliga a rediseñar los mecanismos de seguridad y a disponer de dispositivos de última generación, con el objetivo de garantizar el mayor nivel posible de protección proactiva frente a cualquier ataque malicioso que se ejecute contra las infraestructuras y datos de la Organización.

Es sabido que una importante amenaza surge por la conexión de un dispositivo que no cumple con una serie de normativas de seguridad, es decir, que no tiene los parches de seguridad instalados o actualizados o que contiene aplicaciones potencialmente peligrosas que pueden provocar graves problemas una vez que estos equipos entran en la red corporativa; igual preocupación debe generarnos que, usuarios invitados, o incluso desconocidos, pretendan conectarse a la red sin que se haya aplicado un mínimo control de acceso, de uso o de acceso a información sensible.

Se hace pues necesario el controlar el acceso a las redes, es decir, saber quién es el usuario que se está conectando, saber cómo y cuándo se está conectando, desde dónde se está conectando y qué tipo de dispositivo está usando.

El mercado de la seguridad TI desde hace unos años ha ido perfilando una tecnologías específica para dar respuesta a estos problemas, lo que conocemos como NAC (Network Access Control, del inglés). Dicha tecnología de seguridad NAC no sustituye a otros elementos activos de seguridad de la organización, sino que se complementa con ellos para dar una respuesta pro-activa a cualquier amenaza o sospecha, aislando los elementos peligrosos en "zonas de cuarentena" donde se limite sus movimientos y acciones, y se valore la conveniencia de proceder o continuar con un acceso en todo momento controlado.

Estos sistemas de seguridad NAC, permiten realizar cuatro acciones principales sobre nuestra red:

Ver. Permiten una visibilidad completa de la red, comprobando que dispositivos se están conectando y de qué tipo, de quién son, quién lo está usando, que aplicaciones está ejecutando o en qué estado se encuentra el dispositivo conectado en cuanto a antivirus, parches del sistema operativo, configuración o agentes de seguridad, entre otros.

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea
Fondo Europeo de Desarrollo Regional

Acceder. Según las reglas definidas en la política de seguridad, el sistema permitirá el acceso a aquellos dispositivos que cumplan en lo que respecta a dispositivos conocidos, antivirus actualizado, entre otros. Con los dispositivos no autorizados se puede realizar todo tipo de acciones como notificar al usuario y/o administrador, restringir o bloquear completamente el acceso a la red, entre otros.

Remediar. En aquellos dispositivos que no cumplen completamente nuestra política de seguridad, se puede modificar el sistema operativo, el antivirus, modificar configuraciones, entre otros.

Proteger. Cuando el sistema detecte comportamientos anómalos de equipos conectados a la red, podrá realizar el bloqueo

Se pretende, en definitiva, realizar un tratamiento completo sobre los innumerables dispositivos que se conectan a la red corporativa y para poder establecer un control de acceso a la red robusto, que permita controlar que sólo los usuarios autorizados y sus equipos, igualmente validados, y siempre que cumplan los requisitos de seguridad establecidos, tendrán acceso a la información y recursos que les corresponda.

2. Objeto de la contratación

El objeto de esta contratación es el suministro de una solución de seguridad para el control de acceso a la red corporativa en la Administración del Principado de Asturias (en adelante APA), producto denominado NAC (Network Access Control, Control de Acceso a la Red), con el fin de disponer de un control sobre la seguridad de los dispositivos que se conectan a la red, destinado a la mejor protección de la infraestructura informática y de telecomunicaciones.

El objeto del contrato, por lo tanto, contempla una parte de suministro y otra de servicios.

SUMINISTRO

- De un mínimo de dos equipos para garantizar la alta disponibilidad de la solución de seguridad NAC, y con las características que se indican en este pliego.
- Software de integración de todas las herramientas utilizadas en una única consola.
- Las licencias necesarias para su funcionamiento, si las precisa.
- Los correspondientes periféricos y latiguillos de fibra necesarios para su conexión.

SERVICIO

- Implantación del equipamiento adquirido que incluye:

- Diseño de la implantación, realizando un análisis detallado y documentado de la opción más óptima de instalación de la solución de seguridad NAC en la infraestructura tecnológica de la APA, proporcionando los documentos exigidos en las metodologías de la APA (documento de análisis y diseño de la arquitectura) junto con el documento de intervención detallado para la conexión a la red.

- Servicios de instalación, configuración, optimización y puesta en marcha de los equipos, según detalle de este pliego.

- Estudio de los dispositivos a securizar y comportamiento de la red, así como de las posibles vulnerabilidades existentes, para realizar un adecuado ajuste inicial personalizado de la solución ofertada y de todos sus componentes.

- Despliegue on-site de la solución NAC. Toda la solución de seguridad NAC debe ser desplegada y estar operativa en el Centro de Proceso de Datos (en adelante CPD) de la APA.

- Documentación de toda la infraestructura instalada y del proyecto siguiendo las metodologías del Principado de Asturias.

- Formación sobre la solución de seguridad NAC instalada, según detalle de este pliego.

3. Descripción del suministro a realizar

3.1. Características técnicas

La herramienta objeto del contrato es una solución integral para el control de acceso a la red corporativa del APA, con el fin de garantizar, limitar o impedir el acceso a los recursos de red a través de políticas que definan si los usuarios, o los dispositivos a conectar tienen permisos de accesos a los activos de la organización.

Las características técnicas solicitadas en este pliego para la solución de seguridad NAC (en adelante SNAC) se dividen en doce grupos (**Operativa y funcionalidades**, **modularidad y escalabilidad**, **instalación, consola de gestión**, **integraciones, políticas, cuarentena y remediación, protección, gestión de vulnerabilidades, continuidad del servicio, inventarios e informes**), las cuales están referidas a la solución de seguridad del suministro.

3.1.1. Operativa y funcionalidades

A continuación se indican las características mínimas de SNAC que se solicitan relativas a la operativa y funcionalidades de la solución:

- **Dispositivos a gestionar**. La solución deberá ser capaz de gestionar al menos 4.000 dispositivos IP conectados concurrentemente a la red corporativa tanto central como delegaciones.

- **Control de los dispositivos**. El control de los dispositivos se podrá realizar con o sin agente instalado.

- **Soporte de la solución**. SNAC deberá soportar, tanto con agente como sin agente, equipos Windows, Macintosh, Linux y sus diferentes distribuciones y cualquier dispositivo que soporte SNMP.

- **Dominio del APA**. Para aquellos dispositivos IP que pertenezcan al dominio de la APA, SNAC deberá analizar y remediar vulnerabilidades de sistema operativo y aplicaciones instaladas sin necesidad de tener un agente instalado.

- **Dominio no APA**. Para aquellos dispositivos considerados invitados que no pertenezcan al dominio de la APA, SNAC ofrecerá un agente volátil que deberá ser instalado vía Web mediante una pantalla de bienvenida y que se deberá desinstalar automáticamente.

- **Agente volátil**. El agente volátil deberá crear una conexión segura entre SNAC y los dispositivos.

- **Estándares del agente**. El agente deberá soportar como mínimo los siguientes estándares: SSL v2, SSL v3, TSL v1, TLS v1 (FIPS). Haciendo uso del estándar más seguro en el momento de la instalación de SNAC en la APA.

- **Inyección de ACLs**. SNAC tendrá la posibilidad de inyectar ACLs en equipos de comunicaciones (tanto de nivel 2 como nivel3) mediante línea de comandos.

- **Autenticación**. SNAC deberá permitir al menos autenticación por IP o por MAC.

- **Portal cautivo**. SNAC deberá permitir la redirección a un portal cautivo que ofrezca al usuario una interfaz de entrada de credenciales para la conexión, sin elementos o dispositivos adicionales.

- **Control y bloqueo de dispositivos externos/USB**. SNAC deberá permitir controlar y bloquear dispositivos externos/USB que no cumplan la política establecida en la organización, consiguiendo entre otros, evitar la fuga de información (DLP) y evitar posibles amenazas desde dispositivos externos.

- **Múltiples roles de usuarios**. SNAC deberá soportar múltiples roles de usuarios (incluyendo invitados y visitantes) y deberá permitir diferentes políticas de admisión aplicadas a cada rol.

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

- **Soporte a aplicaciones más comunes**. SNAC deberá identificar y proporcionar soporte para las aplicaciones más comunes (anti-virus, firewalls personales, parches del sistema operativo, mensajería instantánea, entre otros).

- **Chequeos personalizados**. SNAC deberá soportar chequeos personalizados en el registro de Windows, ficheros, servicios y aplicaciones.

- **Usuarios de red**. SNAC deberá soportar tanto usuarios de red con cable como sin cable (WIFI).

- **Usuarios VPN**. SNAC deberá soportar usuarios VPN (Virtual Private Network, Red Privada Virtual).

- **Ejecución de scripts**. SNAC deberá soportar la ejecución de scripts en equipos locales.

- **Personalización de mensajes**. SNAC deberá permitir la personalización de mensajes de usuarios y permite mostrar políticas de aceptación de uso por política, con registro de estas acciones en logs del sistema, que serán almacenados en el sistema de logs centralizado de la organización

- **Múltiples roles de administración**. SNAC deberá soportar múltiples roles de administración con diversos niveles de acceso administrativo (administrador de red, administrador de seguridad, helpdesk, entre otros); dichos roles se encuentran gestionados por el sistema de gestión de identidades corporativo de la APA, junto con las identidades de los usuarios que desempeñan cada rol.

- **Listas negras y blancas**. SNAC deberá permitir la creación de listas negras y blancas de procesos, aplicaciones, así como crear listas basadas en cualquier propiedad reconocible (procesos detectados, aplicaciones instaladas, servicios ejecutándose y puertos abiertos, entre otros) por el NAC, para su utilización en políticas.

- **Detección de NAT**. SNAC deberá permitir la detección de NAT sobre un puerto.

- **Dispositivos no autorizados**. SNAC deberá poder descubrir de manera rápida (en un máximo de 30 segundos) dispositivos no autorizados en la red.
- **Servicios no autorizados**. SNAC deberá poder detectar servicios no autorizados en la red, tales como servidores de correo distintos a los autorizados, servidores DHCP falsos, servidores web no autorizados, entre otros.

- **Envío de alarmas**. SNAC deberá poder enviar alarmas a los distintos administradores al menos a través de correo electrónico y SMS.

- **Despliegue**. SNAC deberá disponer de la posibilidad de desplegarse en capa 2 y capa 3.

- **Controles**. SNAC deberá disponer de controles para PDAs, iPad, Android, iPhone, Windows y Linux.

- **Detección de ataques**. SNAC deberá disponer de la capacidad de detección de ataques Man-in-the-Middle de sesiones SMB durante la autenticación.

- **Detección de múltiples IPs**. SNAC deberá permitir detectar múltiples IPs sobre un puerto de acceso.

- **Rollback**. SNAC deberá disponer de la posibilidad de realizar "Rollback" o marcha atrás en caso de actualización de los plugins/plataforma.

- **Firma de correos**. SNAC deberá disponer de la posibilidad de firmar correos enviados por la plataforma mediante certificado digital S/MIME.

- **Recolección de paquetes**. SNAC deberá disponer de la capacidad de recolección de paquetes transferidos en la detección de equipos maliciosos.

- **Dispositivos IoT**. SNAC deberá tener la capacidad de clasificar y aplicar las políticas de control de acceso a dispositivos IoT, debiendo disponer de la capacidad de crear políticas de clasificación de este tipo de dispositivos desde cero.

- **Limitar acceso**. SNAC deberá tener la posibilidad de limitar el acceso tanto a la consola de gestión como a los accesos SSH mediante filtrado por direccionamiento IP.

- **DHCP**. SNAC debe poder funcionar en un entorno sin DHCP

3.1.2. Modularidad y escalabilidad

A continuación se indican las características mínimas de SNAC que se solicitan relativas a la modularidad y escalabilidad de la solución:

- **Escalable**. SNAC deberá ser escalable, permitiendo pasar a un número mayor de dispositivos IP soportados con la agregación de dispositivos adicionales físicos o con la escalabilidad de manera virtual.

- **Funcionalidades adicionales**. SNAC deberá disponer de la posibilidad de añadir funcionalidades adicionales a través de "plugins" gratuitos. Estos plugins no afectarán al servicio de control de acceso en caso de fallo o de un mal funcionamiento.

- **Arquitectura con distintos formatos de appliances**. SNAC deberá disponer de appliances en formato físico y virtual que permiten ajustarse a las necesidades de gestión

de los dispositivos IP de la organización. La arquitectura permite utilizar en un mismo despliegue los diferentes formatos de appliances (físicos, virtuales o una mezcla de ambos), ofreciendo una arquitectura flexible y fácilmente adaptable a las necesidades del entorno.

3.1.3. Instalación

A continuación se indican las características mínimas de SNAC que se solicitan relativas a la instalación de la solución:

- **Instalación fuera de banda**. SNAC se deberá instalar fuera de banda, bien usando port mirroring o Networks TAP, los Networks Taps (dispositivos de escucha de red) son dispositivos que permiten examinar el tráfico de red sin intervenir en el flujo de datos. Trabajan a nivel 1 de OSI, por lo que no realizan ninguna función de redirección o encaminamiento del tráfico, mientras que el port mirroring o puerto espejo es utilizado con un switch de red para enviar copias de paquetes de red vistos en un puerto del switch (o una VLAN entera) a una conexión de red monitorizada en otro puerto del switch.

3.1.4. Consola de gestión

A continuación se indican las características mínimas de SNAC que se solicitan relativas a la interfaz o consola de gestión de la solución:

- **Consola única de gestión.** SNAC deberá disponer de una consola de gestión única para toda la solución que facilitará la gestión y administración de todas las funcionalidades.

- **Hardware de consola de gestión.** En caso de necesitar un servidor dedicado para la consola de gestión de SNAC, dicho hardware se considera incluido en el contrato, no siendo aportado por la APA en ningún caso.

- **Consola gráfica e intuitiva**. La consola o interfaz de gestión deberá ser gráfico e intuitivo, granular y personalizable, permitiendo además la creación de diferentes usuarios de administración de la solución con diferentes perfiles y privilegios.

- **Acceso a la consola**. El acceso a la consola de gestión centralizada se deberá realizar autenticándose mediante el sistema de autenticación corporativo de la APA.

- **Registros de logs y operaciones**. Se registran tanto los logs de acceso como los de operación de los administradores en dicha consola, los cuales serán enviados al sistema de logs centralizado de la organización.

- **Copia de seguridad y restauración**. La consola de gestión centralizada deberá disponer de mecanismos de copia de seguridad y restauración de los distintos componentes involucrados.

3.1.5. Integraciones

A continuación se indican las características mínimas de SNAC que se solicitan relativas a las integraciones de la solución:

- **Sistemas de autenticación**. SNAC se deberá integrar con el sistema de autenticación centralizado de la APA.
- **Sistema de Backup**. SNAC se deberá integrar con la plataforma de backup de la APA.
- **Infraestructuras heterogéneas**. SNAC estará basado en estándares, permitiendo la integración con infraestructuras de red heterogéneas, independientemente del fabricante de los componentes de estas infraestructuras.
- **Interacción con switches**. SNAC deberá poder integrarse con los switches y dispositivos usados actualmente en la APA. Al menos deberá soportar la integración con switches de Cisco, Enterasys, Juniper, HP, 3COM, Alcatel-Lucent, Aruba y con genéricos.
- **Compatibilidad e integración**. SNAC deberá ser compatible y deberá poder integrarse con el servicio de directorio LDAP de la organización.
- **SIEM**. SNAC deberá poder integrarse fácilmente con el sistema de gestión de la seguridad de la información y gestión de eventos (SIEM) de la organización.
- **Monitorización**. SNAC deberá poder integrarse con la plataforma corporativa de monitorización de la APA.
- **SDK**. SNAC deberá disponer de un kit de desarrollo de software para integración con aplicaciones y dispositivos de terceros.
- **Dispositivos Wireless**. SNAC deberá disponer de integración con dispositivos Wireless Cisco, Aruba, y Dlink.
- **SNMP**. SNAC deberá hacer uso del estándar SNMP v1,2,3 para la comunicación e integración con los distintos fabricantes, proporcionando información de los distintos dispositivos de red como dirección IP, dirección MAC, puerto, VLAN y poder interactuar con ellos para el cumplimiento de opciones como cambio de VLAN, deshabilitado de puertos, entre otros.

- **802.1x**. SNAC deberá disponer de la posibilidad de integración con 802.1x.

3.1.6. Políticas

A continuación se indican las características mínimas de SNAC que se solicitan relativas a la creación de políticas básicas de control de acceso y políticas de chequeo:

Políticas básicas de control de acceso:

SNAC deberá proporcionar plantillas sencillas predefinidas para la creación de políticas de control de acceso, a saber:

1. Clasificación de los dispositivos en la red (Dispositivos NAT, móviles, Desktop Windows, impresoras, dispositivos Linux/Unix, Dispositivos Mac, dispositivos VoIP, Dispositivos de electrónica, dispositivos desconocidos).
2. Clasificación de dispositivos externos (wireless, USB, Impresoras vía USB, PCMCIA, Módems, Dispositivos infrarrojos, Scanners, Lectores de DVD/CD, Dispositivos Bluetooht).
3. Clasificación de máquinas virtuales.
4. Clasificación de dispositivos móviles (Android, Apple, Windows Mobile, Blackberry, Kindle, Kindle Fire, Symbian, Palm, entre otros).
5. Clasificación de dispositivos corporativos e invitados.
6. Plantilla de cumplimiento de seguridad de antivirus.
7. Plantilla de cumplimiento de conexión de dispositivos USB externos para fuga de información.
8. Plantilla de cumplimiento de programas de P2P.
9. Plantilla de cumplimiento de instalación/ejecución de firewall en puesto.
10. Plantilla de cumplimiento de usos de mensajería instantánea.
11. Plantilla de cumplimiento de parches de seguridad de Windows.
12. Plantilla de cumplimiento de parches de seguridad de Macintosh.
13. Plantilla de avisos de propagación de malware.
14. Plantilla de suplantación de identidad.
15. Plantilla para evitar doble conexión a la red por WIF y Wired simultáneamente.

Políticas de chequeo:

SNAC deberá soportar al menos las siguientes políticas de chequeo:

1. Aplicación.
2. Software instalado.
3. Mensajería instantánea.
4. Aplicaciones P2P.

5. Información del dispositivo.
6. Nombre DNS.
7. Device is NAT.
8. Usuario del dominio.
9. Dirección y cambio de dirección IP.
10. Dirección MAC.
11. Fabricante de NIC.
12. Dominio y nombre NetBios.
13. Función de red.
14. Clase de sistema operativo.
15. Versión del servicio.
16. Puertos abiertos.
17. Comportamiento del tráfico.
18. Eventos.
19. ARP Spoofing.
20. Petición DHCP.
21. Evento de autenticación.
22. HTTP login.
23. Eventos maliciosos (Evento IPS).
24. Comportamiento de cliente y de servidor.
25. Atributos LDAP.
26. Información de usuario (Nombre, email, teléfono).
27. Pertenencia a grupo.
28. Pertenencia a comunidad (para autenticación).
29. Atributos SNMP.
30. SNMP MIB-II if Number.
31. SNMP MIB-II Sys Description.
32. SNMP MIB-II Sys Location.
33. SNMP MIB-II System Name.
34. SNMP MIB-II Sys Up Time.
35. SNMP OID Value.
36. Pertenencia a dominio.
37. Procesos en ejecución de Windows.
38. Procesos en ejecución en hosts inspeccionados.
39. Clave de registro.
40. Versión de sistema operativo.
41. Directorios compartidos.
42. Fecha de actualización de antivirus.
43. Hotfix instalados.
44. Vulnerabilidades Microsoft.

Proyecto financiado por la Unión Europea a través del Fondo Europeo de Desarrollo Regional en el marco del Programa Operativo FEDER de Asturias 2014-2020

Unión Europea

Fondo Europeo de Desarrollo Regional

3.1.7. Cuarentena y remediación

A continuación se indican las características o funcionalidades mínimas de SNAC que se solicitan relativas a la cuarentena y remediación de la solución:

- **Control de VLAN basado en SNMP**. SNAC deberá poder cambiar automáticamente a VLAN de cuarentena, invitado o producción.
- **Control de puerto en switch basado en SNMP**. SNAC debe ser capaz de deshabilitar automáticamente un puerto en el switch para poner en cuarentena un PC (por ejemplo infectado por un gusano) incluso aunque se cambie de puerto.
- **VLAN de cuarentena**. SNAC permitirá mover un dispositivo a una VLAN aislada mientras se realiza la actualización del mismo.
- **Actualizaciones de remediación**. SNAC debe proporcionar actualizaciones y funcionalidades de remediación para aquellos dispositivos que se encuentren en cuarentena.
- **Interfaz gráfico**. Durante el proceso de remediación, el agente de la solución deberá guiar al usuario mediante un interfaz gráfico.
- **Scripts personalizados**. SNAC deberá soportar scripts personalizados para la remediación.
- **Remediación basada en roles**. SNAC deberá permitir diferentes procesos de remediación basados en roles de usuarios.

3.1.8. Protección

A continuación se indican las características o funcionalidades mínimas de SNAC que se solicitan relativas a la protección:

- **Firewall virtual**. SNAC deberá permitir la creación de un firewall virtual que permita bloquear cualquier tráfico TCP, UDP e ICMP, permitiendo bloquear por lo tanto, cualquier tráfico hacia o desde cualquier dispositivo.
- **Redirección**. SNAC deberá permitir la redirección de cualquier consulta http desde un PC para informar al usuario sobre violación de políticas, basándose en hijack de sesión o redirección DNS.

- **Múltiples acciones**. SNAC deberá permitir desconectar usuarios, apagar PCs, cerrar o matar procesos y aplicaciones, bloquear acceso a la red, deshabilitar dispositivos USB o ejecutar comandos del sistema operativo.

- **Envío de correos electrónicos**. SNAC podrá enviar correos electrónicos a los usuarios, explicando la violación de políticas y/o presentar el portal del cumplimiento de políticas.

- **Acceso limitado**. SNAC permitirá a un PC tener acceso limitado mediante el firewall virtual mientras se realiza la actualización.

- **Actualizaciones en segundo plano**. SNAC deberá permitir que las actualizaciones no críticas se puedan realizar en segundo plano mientras el usuario está trabajando.

- **Actualización al desconectar**. SNAC deberá permitir realizar una actualización de un dispositivo cuando el usuario se desconecte.

- **Mensajes**. SNAC deberá permitir mostrar a los usuarios mensajes con las instrucciones y enlaces necesarios para actualizar el puesto él mismo.

- **Actualizar automáticamente**. SNAC deberá actualizar automáticamente nuevas versiones o ficheros de datos de las aplicaciones más comunes.

3.1.9. Gestión de vulnerabilidades

A continuación se indican las características o funcionalidades mínimas de la herramienta SNAC que se solicitan relativas a la gestión de vulnerabilidades:

- **Escaneo de vulnerabilidades**. SNAC deberá soportar escaneo de vulnerabilidades de sistemas tanto con agente como sin él, en tiempo real o en diferido.

- **NMAP**. SNAC deberá tener la posibilidad de inclusión de la herramienta de securización NMAP para el escaneo de redes completas y obtención de información acerca de los servicios, sistemas operativos y vulnerabilidades derivadas de la conjunción de éstos.

3.1.10. Continuidad del servicio

A continuación se indican las características o funcionalidades mínimas de SNAC que se solicitan relativas a la continuidad del servicio:

- **Redundancia y alta disponibilidad**. SNAC deberá soportar configuración de redundancia y alta disponibilidad.
- **Modo fuera de línea**. SNAC deberá soportar el modo fuera de línea, evitando así un punto de fallo en caso de caída del equipo.

3.1.11. Inventarios

A continuación se indican las características o funcionalidades mínimas de SNAC que se solicitan relativas a los inventarios, debiendo proporcionar al menos los siguientes:

- Inventario de todos los activos que haya descubierto, así como de sus características, tipo de conexión, etc.
- Inventarios en tiempo real.
- Inventarios de Linux, Mac y Windows.
- Inventario de aplicaciones en ejecución, servicios en ejecución y aplicaciones instaladas.
- Inventario Android, iOS, Windows, Firefox OS, entre otros.

3.1.12. Informes

A continuación se indican las características o funcionalidades mínimas de SNAC que se solicitan relativas a los informes:

- **Personalización de informes**. SNAC deberá tener la capacidad de generación, planificación y envío de informes personalizados.
- **Plantillas de informes**. SNAC deberá contar al menos con las siguientes plantillas de informes: Vulnerabilidades, Tendencia de las políticas, Estado de las políticas, Detalles de las Políticas, Cumplimiento, Detalle de los equipos, Análisis de invitados registrados, Invitados registrados.
- **Informes de seguridad**. SNAC deberá poder generar al menos los siguientes informes de seguridad: Host infectados (Origen del malware, host infectados por segmento, host infectados por servicio, equipos más infectados), Intentos de infección por malware en correo (equipos más infectados, hosts infectados por segmento), por estadística de actividades (métodos de escaneo, intentos de infección en el tiempo, detección de escaneos en el tiempo).

3.1.13. Manuales de la herramienta.

La herramienta SNAC deberá venir provista con los siguientes manuales en el idioma castellano:

- Manual de instalación.
- Manual de configuración.
- Manual de uso.

Todo ello se realizará atendiendo siempre a las demandas y criterios que emanen del Jefe/Responsable de Proyecto de la DGTIC y en general siguiendo las metodologías existentes en la Administración del Principado de Asturias.

3.1.14. Hardware de la solución.

El hardware proporcionado con la solución debe tener las siguientes características mínimas:

- El hardware aportado para la solución de seguridad NAC debe basarse en appliance/s dedicados.
- El diseño del a solución de control de acceso a red, deberá incluir al menos dos dispositivos en alta disponibilidad.
- Los equipos deben disponer de soporte para IPv6 con tecnología de doble pila.
- Los equipos deben contar con certificaciones de bajo consumo, protecciones de seguridad para su manipulación y compatibilidad electrónica.
- Cada equipo deberá disponer de al menos 4 puertos 100/1000BaseT–RJ45, 2 puertos 10Gbase-SR en SFP+.
- Cada equipo debe disponer además del puerto de red de gestión dedicado, de un puerto de consola.
- Los equipos deben ser enrackables en un armario rack estándar de 19'.
- Los equipos deberán tener alimentación eléctrica en corriente alterna de 220V a 50 Hz.
- Los equipos deben disponer de doble fuente de alimentación redundante, extraíble en caliente.

- Los equipos deben disponer de ventiladores "Front-to-back".
- Los equipos deben tener un tamaño máximo de 2U.
- El consumo eléctrico de los equipos debe ser inferior a 600 W, en cualquier condición de funcionamiento.

4. Servicios de instalación

El adjudicatario deberá prestar los servicios de instalación necesarios para la puesta operativa de la solución de seguridad NAC, teniendo especial relevancia las siguientes tareas:

- Suministro de los componentes, servidores y licencias.
- Estudio de los dispositivos a securizar y comportamiento de la red, así como de las posibles vulnerabilidades existentes, para realizar un adecuado ajuste inicial personalizado de la solución ofertada y de todos sus componentes.
- Análisis detallado y documentado de la opción más óptima de instalación de la solución de seguridad NAC en la infraestructura tecnológica de la APA, proporcionando los documentos exigidos en las metodologías de la APA (documento de análisis y diseño de la arquitectura) junto con el documento de intervención detallado para la conexión a la red.
- Despliegue on-site de la solución NAC. Toda la solución de seguridad NAC debe ser desplegada y estar operativa en el Centro de Proceso de Datos (CPD) de la APA.
- Instalación y configuración de todos los componentes de la solución de seguridad NAC.
- Configuración de informes de incidencias, de forma que desde la consola centralizada se pueden obtener informes de las incidencias graves (criticidad máxima, alta y media) que afecten al servicio y que permitan determinar el impacto y causas de las mismas. Un informe concreto dentro de este epígrafe será el "informe de fallos y trabajos sobre gestión de resolución de incidencias" que deberá estar disponible 24 horas tras la detección de la incidencia. Es caso de no dejar realizada la configuración indicada para estos informes de incidencias, el adjudicatario deberá enviar dicho informe mensualmente a la APA durante el tiempo que dure la garantía.
- Informes de riesgos, vulnerabilidades y fallos de seguridad. Se entregarán informes y enviarán alertas de los riesgos, vulnerabilidades y fallos de seguridad detectados, incluidos exploits de día cero, que afecten, directa o potencialmente, a los equipos objeto del contrato. Estos informes y alertas deberán entregarse de forma inmediata una vez

detectado el riesgo, vulnerabilidad o fallo de seguridad. El adjudicatario enviará dichos informes durante el tiempo que dure la garantía.

5. Servicios de formación

El adjudicatario deberá prestar los servicios de formación o transferencia del conocimiento durante al menos tres jornadas (15 horas) sobre la operación y mantenimiento del sistema implantado.

La formación se realizará en las instalaciones de la Administración del Principado de Asturias.

En el caso de que los equipos suministrados sean de un fabricante o tecnología diferente a los existentes en la APA, el adjudicatario deberá proporcionar formación oficial del fabricante. Esta formación será de al menos tres jornadas presenciales en las dependencias de la APA en Oviedo que designe la DGTIC, en idioma español, y para un mínimo de 12 personas, con el fin que el personal técnico de la APA pueda adquirir el conocimiento suficiente para gestionar y operar los equipos. La formación será impartida por un técnico con certificación oficial de fabricante en vigor que abarque los equipos suministrados. El coste integral de esta formación, incluido desplazamiento, dietas y material necesario, se considera incluido en el precio de adjudicación.

Oviedo, 5 de julio de 2017
EL RESPONSABLE DE PROYECTOS DE SEGURIDAD,

Fdo.: Luis Alberto Fernández Ardura