UNIVERSIDAD NACIONAL DE COLOMBIA

VICERRECTORÍA GENERAL
DIRECCIÓN NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - DNTIC

DIRECTRIZ TÉCNICA No. 9A

Para: **RECTOR**
VICERRECTOR GENERAL
VICERRECTORES DE SEDE
GERENCIA NACIONAL FINANCIERA Y ADMINISTRATIVA
DIRECTORES SEDES PRESENCIA NACIONAL
DIRECCIONES ADMINISTRATIVAS DE SEDE
JEFES DE OFICINAS DE PLANEACIÓN
JEFES DE OFICINAS DE TECNOLOGÍA
UNIVERSIDAD NACIONAL DE COLOMBIA

Consecutivo: **DNTIC-0156-16**

Referencia: **DIRECTRIZ TÉCNICA No. 9A POR LA CUAL SE MODIFICA LA DIRECTRIZ TÉCNICA No. 9 "IMPLANTACIÓN DE SOLUCIONES PARA LA GESTIÓN UNIFICADA DE AMENAZAS A LA SEGURIDAD DE LAS REDES DE DATOS"**

Fecha: **3 DE MARZO DE 2016**

El Acuerdo 46 de 2009 *"por el cual se definen y aprueban las políticas de Informática y Comunicaciones que se aplicarán en la Universidad Nacional de Colombia"*, establece en el numeral 2 del artículo 4: "*Dando aplicación a las políticas de informática y comunicaciones y con el fin de garantizar la estandarización, la integración y la interoperabilidad de la plataforma tecnológica de la Universidad, la Dirección Nacional de Informática y Comunicaciones emitirá las directrices técnicas de acuerdo con la normatividad vigente".*

La Dirección Nacional de Tecnologías de Información y Comunicaciones consciente de la necesidad de garantizar la integridad, confiabilidad, disponibilidad y la seguridad de los sistemas informáticos y de comunicaciones de la Universidad, contando con la activa participación de los profesionales que conforman los equipos de trabajo de las Oficinas de Tecnologías de las Sedes, teniendo en cuenta la renovación de la infraestructura de hardware, software y procesos de acuerdo con la vigencia tecnológica y con el objetivo de garantizar la estandarización e interoperabilidad de la plataforma tecnológica de la Universidad, establece la siguiente directriz técnica en relación con las herramientas para la gestión unificada de amenazas a la seguridad de las redes de datos (UTM, NGFW), en virtud de lo cual deberá tenerse en cuenta los siguientes aspectos:

1. En general, toda adquisición de este tipo de soluciones debe buscar que sea estandarizada en software, hardware y procedimientos (configuración, mantenimiento, copias de seguridad, etc.)

para todas las sedes de la Universidad. En este sentido, deberá tenerse en cuenta las soluciones que se encuentren implantadas en las sedes en el momento de iniciar la adquisición de la solución. En caso de considerar la necesidad de hacer un cambio, éste deberá justificarse adecuadamente.

Esta estandarización facilitará la puesta a punto, control y mantenimiento de los equipos, las personas relacionadas con la administración y operación de las soluciones unificarán conceptos y profundizaran en el conocimiento de la herramienta, facilitará las actualizaciones y aplicación de parches de seguridad (al igual que el proceso de adquisición y soporte por parte de los proveedores). Todo esto tendrá como consecuencia una significativa reducción de costos.

2. Se privilegiará en la selección las soluciones que simplifiquen la gestión de los diferentes componentes en tanto satisfagan los requerimientos de la Sede durante el tiempo de vida esperado de la solución y cumplan con los requerimientos de seguridad esperados para tipo de aplicaciones y las condiciones particulares de la Sede.

3. Se adelantarán y verificarán las actividades que se orienten a garantizar que la implantación de las herramientas adquiridas brinden estabilidad a los servicios prestados en cada una de las sedes. Como una guía, que no pretende ser completa, a continuación se listan algunos elementos que deben garantizar las Oficinas de Tecnologías de las sedes en la búsqueda de la estabilidad mencionada en las herramientas para fortalecer la seguridad de la red:
    a. La capacidad y vigencia tecnológica para satisfacer los requerimientos de seguridad de la sede durante un horizonte de tiempo establecido (permitiendo saber qué momento debe renovarse/cambiarse). La vigencia debe soportarse en actualizaciones permanentes en software y firmware, evitando cambiar de hardware.
    b. La compatibilidad con la infraestructura y topología de red existente en la sede y de la red WAN.
    c. Acompañamiento del proveedor en la instalación, configuración, puesta a punto, migración de la herramienta en uso, soporte y garantía de la solución.
    d. Capacitación adecuada del equipo de trabajo, especialmente cuando haya cambios de personal.
    e. La protección física y ambiental a los equipos que conformen la solución (tanto cableados como inalámbricos).
    f. Acceso seguro para administración de las herramientas (*método de autenticación más allá de usuario/password y uso de canal cifrado –SSH, SSL, VPN, etc.*)
    g. Documentación, respetando el sistema de gestión documental en uso en la universidad, de los componentes instalados y los procedimientos utilizados. Se espera que esta documentación incluya: manuales técnicos y funcionales y mejores prácticas, entre otros.
    h. Toda modificación que se planee realizar a este tipo de soluciones, debe acompañarse de un procedimiento de gestión de cambios junto con un registro que permita evidenciar las actividades realizadas y los responsables. Idealmente esta modificación debería recibir la aprobación de un Comité de Cambios que avale el procedimiento realizado.
    i. Creación de un esquema a de copias de seguridad (*backup*) para las configuraciones y log (bitácoras) de los componentes de la solución, verificando su correcta aplicación. Los log de los sistemas son requeridos para procesos de diagnóstico de problemas o de algún otro tipo de investigación.

j. Para los componentes del sistema que utilicen certificados digitales debe garantizarse la gestión correspondiente para que estos certificados tengan vigencia durante el tiempo de vida de uso de la solución.
k. Definir quién tendrá acceso a los reportes que se puedan generar y garantizar que dichas personas usen la información de forma correcta (respetando la privacidad y la confidencialidad).
l. Programar auditorias periódicas para revisar el estado de los sistemas y la valoración de vulnerabilidades (configuración de firewalls, IPS, SSL VPN, servidores web, parchado de equipos, vigencia de software antivirus, configuración en DNS, etc.)

NOTA: Las herramientas mencionadas aquí son aquellas que, entre otras cosas, previenen intrusiones en la red, buscan asegurar aplicaciones, servicios y servidores, brindan soporte de VPN con IPSec y SSL para conectar de forma segura los dispositivos móviles (tablets, smartphones, etc.) y equipos remotos a la red, permiten realizar rastreo de malware entrante y saliente, dan soporte a conexiones seguras (WPA2, en los accesos WIFi) y proveen esquemas de alta disponibilidad (especialmente para las funcionalidades de firewall e IPS).

Cordialmente,

HENRY ROBERTO UMAÑA ACOSTA
Director