DIRECTRIZ TÉCNICA No. 09

PARA: DEPENDENCIAS DE TODAS LAS SEDES DE LA UNIVERSIDAD NACIONAL DE COLOMBIA

DE: DIRECCIÓN NACIONAL DE ESTRATEGIA DIGITAL A TRAVÉS DE SUS DEPENDENCIAS ADSCRITAS EN EL NIVEL NACIONAL Y DE SEDE.

FECHA: 01 DE OCTUBRE DE 2024

ASUNTO: DIRECTRIZ TÉCNICA No. 09 "IMPLANTACIÓN DE SOLUCIONES PARA LA GESTIÓN UNIFICADA DE AMENAZAS A LA SEGURIDAD DE LAS REDES DE DATOS"

El Acuerdo No. 316 de 2019 del Consejo Superior Universitario, modificó la estructura interna académico - administrativa del Nivel Nacional de la Universidad Nacional de Colombia, creó la Dirección Nacional de Estrategia Digital, como Unidad Estratégica TI, estableció sus funciones y estructura conformada con las dependencias que se enuncian a continuación:

1. Oficina de Arquitectura Organizacional (Nivel Nacional)
2. Oficina de Gestión de la Información (Nivel Nacional)
3. Oficina de Gobierno y Gestión Administrativa (Nivel Nacional)
4. División Universidad Laboratorio (Nivel Nacional)
5. División de Gestión Tecnológica: (Nivel Nacional)

5.1. Sección de Seguridad de la Información (Ubicada en la Sede Manizales)
5.2. Sección de Aplicaciones (Ubicada en la Sede Medellín)
5.3. Sección de Infraestructura y Gestión de Servicios de TI (Ubicada en la Sede Bogotá)
5.4. Sección de Identidades Digitales (Ubicada en la Sede Palmira)

De acuerdo con la estrategia trazada para el fortalecimiento de la Gestión TI, específicamente para la gestión de las adquisiciones de soluciones tecnológicas con recursos de funcionamiento e inversión, buscando la estandarización, compatibilidad, integración y la interoperabilidad de la plataforma tecnológica de la Universidad, además de estar enmarcadas en acuerdos que proporcionen beneficios o valor agregado a la Institución, se emitió la Resolución de Rectoría No. 015 de 2023, la cual modificó los numerales 3, 4 y 5 del artículo 66 de la Resolución de Rectoría No. 1551 de 2014 "*Por medio de la cual se adopta el Manual de convenios y contratos de la Universidad Nacional de Colombia*".

Con fundamento en las facultades otorgadas a la Dirección Nacional de Estrategia Digital en la Resolución mencionada, se emitió la Circular No. 1 de 2024, la cual fijó los lineamientos para la emisión de las viabilidades técnicas previas, directrices técnicas y conceptos técnicos de la Dirección Nacional de Estrategia Digital a través de sus dependencias adscritas en el nivel nacional y de sede.

(+57 1) 3165087 – (+57 1) 3165000 EXT:18197
Bogotá D.C., Colombia
dned@unal.edu.co

Con el fin de garantizar la estandarización, integración e interoperabilidad de la plataforma tecnológica de la Universidad Nacional de Colombia, contando con la activa participación de los profesionales que conforman los equipos de trabajo de las dependencias adscritas, 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 brinde 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 secciones de tecnologías de la información (TI) en las sedes andinas y los profesionales responsables de TI en la sede de La Paz y en las sedes de presencia nacional 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).

(+57 1) 3165087 – (+57 1) 3165000 EXT:18197
Bogotá D.C., Colombia
dned@unal.edu.co

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 de copias de seguridad (backup) para las configuraciones y log (bitácoras) de los componentes de la solución, verificando su correcta aplicación. Los logs 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 auditorías 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).

DIRECCIÓN NACIONAL DE ESTRATEGIA DIGITAL Y DEPENDENCIAS ADSCRITAS
UNIVERSIDAD NACIONAL DE COLOMBIA

(+57 1) 3165087 – (+57 1) 3165000 EXT:18197
Bogotá D.C., Colombia
dned@unal.edu.co