GUÍA PARA CONEXIÓN A REDES SEGURAS MEDIANTE VPN-CLIENTE A SITIO

PROCESO GOBIERNO Y GESTIÓN DE SERVICIOS DE TI

Febrero de 2017

OBJETIVO DE LA GUÍA:
Facilitar la incorporación de controles de seguridad informática en desarrollo de la Política de Seguridad Informática y de la Información[1], cuando se requiera efectuar conexiones desde estaciones de trabajo o servidores de la red de datos de la Universidad a otras redes externas por motivos institucionales. En consecuencia, la presente guía, propende por que la conexión a redes de datos diferentes a la de la Universidad Nacional de Colombia, sea debidamente protegida contra accesos no autorizados a través de mecanismos de control.

ALCANCE
Esta guía aplica a todas las dependencias que componen la comunidad académica e institucional, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la Universidad a través de contratos, convenios o acuerdos con terceros y a todo el personal de la Universidad, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe dentro del alcance definido para el Sistema de Gestión de Seguridad Informática y de la Información y en general a todos los usuarios de la información o aquellos que sean beneficiados con el uso de la infraestructura y servicios de conexión a redes diferentes a las de la Universidad.

DEFINICIONES:
Se relacionan a continuación los elementos/conceptos que son usados en el desarrollo de la presente guía; específicamente en el Diagrama de conexión a redes mediante VPN Cliente.

a. Estación de trabajo: Son todos los equipos utilizados para gestionar la información y las comunicaciones. Ejemplo: computadores, teléfonos, impresoras. Para el caso de la presente guía, es el equipo de cómputo desde el cual el usuario realiza la conexión VPN.

b. Firewall: Un cortafuego (Firewall-Abreviatura **FW**)[2] es una parte de un sistema o red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo las comunicaciones autorizadas.

c. **LAN** (Sigla en inglés – Local Area Network)**[3]:** Es una red que se utiliza para conectar equipos de una compañía u organización (para el caso UNAL). Por lo general una red de área local conecta equipos (o recursos, como impresoras) a través de un medio de transmisión (cables o señales inalámbricas).

[1] Literal i del Capítulo 2 "Marco Regulatorio de la Seguridad (MRS)", establece: "En desarrollo del marco de cooperación científica y tecnológica realizado por la Universidad Nacional de Colombia en convenio con otras universidades nacionales o internacionales o entidades públicas o privadas, se hace necesario aprovechar entre otros, los recursos tecnológicos de redes e infraestructura de tecnología informática, así como de aplicaciones y sistemas de información institucional; para lo cual será de estricta aplicación, la presente política de seguridad informática y de la información y los mecanismos para tales fines.". http://dntic.unal.edu.co/images/seguridad/PolticadeSeguridadInformaticaydelaInformacion.pdf

[2] WIKIPEDIA. Cortafuegos (informática). [Última modificación 29 septiembre 2016]. [Online]. [2016]. https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)

[3] CCM Benchmark Group. ¿Qué es una red de área local?. [Sin fecha de publicación]. [Online]. [2016]. http://es.ccm.net/contents/295-redes-de-area-local

d. LDAP[4]: Son las siglas de Lightweight Directory Access Protocol (*en español Protocolo Ligero/Simplificado de Acceso a Directorios*) que hacen referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también se considera una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas. Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica.

e. Usuario: Es todo personal de la Universidad (funcionarios), el personal subcontratado (Contratista), los usuarios y en general todos aquellos que tengan acceso de una manera u otra a los activos de información de la Universidad.

f. **VPN[5]** (Sigla en inglés – Virtual Private Network): Redes privadas virtuales. Definido en el diagrama de conexión a redes mediante VPN Cliente como "*Túnel-VPN SSL-TLS*" Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar una VPN para que sus empleados desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían. Sin embargo, conectar la computadora de un empleado a los recursos corporativos es solo una función de una VPN.

g. **Matriz de la asignación de responsabilidades** (**RACI** por las iniciales de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo)). De esta manera se logra asegurar que cada uno de los componentes del alcance esté asignado a un individuo o a un equipo. R) responsable, A) Quien autoriza, C) Quien debe ser consultado y I) Quien debe ser informado.

h. **VLAN[6]:** Acrónimo de virtual LAN (Red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

CONDICIONES GENERALES

Es de obligatorio cumplimiento que las conexiones VPN-Cliente a Sitio desarrolladas en la presente guía, sean efectuadas desde equipos de cómputo (estaciones de trabajo o servidores) de y desde la red de la Universidad. No se permiten accesos remotos por conexiones diferentes o puentes o conexiones alternas para llegar a estos equipos y posteriormente desde ellos lograr el uso de las VPNs.

1. DESARROLLO DEL CONTENIDO

[4] WIKIPEDIA. Protocolo ligero de Acceso a Directorios. [Última modificación 23 sep. 2016]. [Online] https://es.wikipedia.org/wiki/Protocolo_Ligero_de_Acceso_a_Directorios

[5] WELIVESECURITY. ¿Qué es y cómo funciona una VPN para la privacidad de la información? [10 septiembre 2012] [Online] http://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

[6] WIKIPEDIA. VLAN. [Última modificación 23 sep. 2016]. [Online] https://es.wikipedia.org/wiki/VLAN

El diagrama que se muestra a continuación define los elementos requeridos para garantizar la conexión VPN-Cliente de forma segura. Los números indicados en el diagrama corresponden a las actividades que han de ser realizadas para que el usuario de la conexión mantenga condiciones de seguridad tanto para la red Institucional, cómo para el servidor o red a la que se desea conectar.

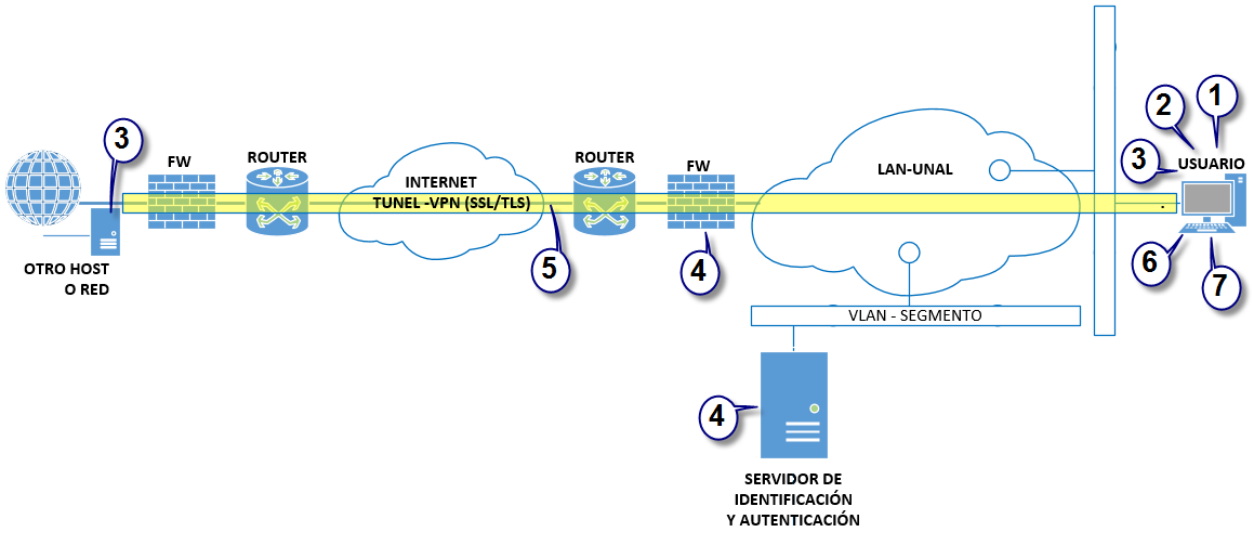

Diagrama de conexión a redes mediante VPN Cliente

Matriz de responsabilidades.

#	DEFINICIONES, ACTIVIDADES O ESTADOS	RESPONSABLES			
		R	A	C	I
1	**El usuario debe tener un rol y perfil definido**. La persona interesada en la conexión debe solicitar la autorización al dueño del proceso; se puede consultar a la OTIC sobre los perfiles que tiene el usuario. Una vez autorizado, la OTIC procede a implementar el rol y perfil y luego informa a la persona interesada y al dueño sobre la habilitación del rol.	a	d	c d	b c d
2	**Protecciones contra código malicioso**. La OTIC debe revisar que la estación de trabajo o servidor desde la cual se realizará la conexión, cuente con protección contra código malicioso (agente de antivirus) y que la máquina limpia. OTIC informará a la persona interesada y al dueño del proceso para continuar con las demás actividades. **NOTA**: OTIC podrá ejecutar la hoja de necesidades de seguridad a la estación de trabajo del interesado, a efectos de verificar los controles requeridos por ISO27001:2013. Esta hoja de necesidades de seguridad estará disponible en DNTIC en caso de requerirse.	c			a d
3	**Instalación del Software VPN (Servidor + Cliente).** OTIC confirmará con los responsables del servidor al que se desea conectar, que las protecciones de la estación o servidor han sido habilitadas. Se procederá a instalar el software de agente VPN en la estación e trabajo y se realizaran las pruebas de ña conexión segura. OTIC informará al interesado y al dueño cuando las pruebas sean realizadas.	b			a c
4	**Acceso autorizado para uso del servicio (LDAP) y Firewall**. OTIC	d	c		a

#	DEFINICIONES, ACTIVIDADES O ESTADOS	RESPONSABLES			
		R	A	C	I
	realizará los ajustes a las políticas (Puertos que usará la VPN, registro de la estación de trabajo, entre otras) en el Firewall y/o en el perfil del usuario en LDAP o en quien este prestando el servicio de autenticación. OTIC informará al interesado y al dueño cuando las actividades sean realizadas.		d		c
5	**Información de intercambio.** El interesado o dueño, efectúa los procedimientos de conexión al servidor mediante la activación del software de VPN. La información de intercambio es responsabilidad del interesado y del dueño.	a			d
6	**Equipo parchado y actualizado**. OTIC realizará de forma periódica la revisión del equipo del usuario interesado a efectos de actualizar el sistema operativo y el software de conexión de red, para garantizar el funcionamiento adecuado de la conexión. Se mantendrá una bitácora sobre el equipo, y se informará al dueño del proceso sobre las actividades realizadas	c			a d
7	**Plan de continuidad y restauración**. El usuario interesado y/o dueño del proceso realizarán las copias de seguridad de la información a intercambiar y efectuarán restauraciones de prueba para garantizar la presencia de eventos contingentes.	a	d		d

Actores de la tabla RACI

Código	ACTOR
a	Persona (usuario) que usa el servicio de conexión a otras redes
b	Host o red que ofrece el servicio de conexión
c	OTIC -Oficina de Tecnologías de Información y Comunicaciones
d	Dueño o responsable (Área funcional) de la conexión
e	DNTIC – Dirección Nacional de Tecnologías de información y comunicaciones

ELABORÓ	**Adriana María Jaramillo Pinzón** **Manuel Antonio Pérez Chaparro**	**REVISÓ**	**Johan Sebastián Eslava Garzón** **Mauricio León Guzmán Correa** **Alexis Miguel Taborda Salazar** **Jairo Andrés Londoño Jaramillo** **Francisco Naranjo Madero** **Edgar Sarmiento Coba** **Alexis Ernesto Parra Sales** **Robins Alex Landázuri Quiñones** **Adriana María Jaramillo Pinzón** **Manuel Antonio Pérez Chaparro**	**APROBÓ**	**Henry Roberto Umaña Acosta**

CARGO	Asesor DNTIC Consultor DNTIC (Contratista)	**CARGO**	Jefe Oficina de Tecnologías Sede Bogotá Jefe Oficina de Tecnologías Sede Medellín Jefe Oficina de Tecnologías Sede Manizales Jefe Oficina de Tecnologías Sede Palmira Coordinador Oficina de Tecnologías Sede Orinoquía Coordinador Oficina de Tecnologías Sede Caribe Coordinador Oficina de Tecnologías Sede Amazonía Coordinador Oficina de Tecnologías Sede Tumaco Asesor DNTIC Consultor DNTIC (Contratista)	**CARGO**	Director
FECHA	08 de Noviembre de 2016	**FECHA**	23 de Diciembre de 2016	**FECHA**	21 de Febrero de 2017