CONTROL DE CAMBIOS					
Versión	**Elaborado por**	**Revisado Por**	**Aprobado por**	**Fecha de aprobación**	**Descripción de las Modificaciones**
1	Andres Casallas **Cargo:** Administrador conectividad	Cesar Cardenas Cargo: Gerente TI	Cesar Cardenas Cargo: Gerente TI	13-12-2018	Elaboración inicial del documento

TABLA DE CONTENIDO

1. OBJETIVO 3

2. ALCANCE 3

3. GENERALIDADES 3

3.1 POLÍTICAS DE SEGURIDAD 4
3.2 POLÍTICAS GENERALES 4

4. PROCEDIMIENTOS 5

4.1 CREACIÓN VPN 5
4.2 RENOVACIÓN DE VPN 5
4.3 ELIMINACIÓN DE VPN 6
5. REGISTROS GENERADOS DEL PROCEDIMIENTO 7

1. Objetivo

Definir los lineamientos para la autorización, creación, renovación y eliminación de redes privadas virtuales VPN client to site para organismos de tránsito que permitan su interacción con la plataforma tecnológica HQ-RUNT.

2. Alcance

El procedimiento cubre los procesos de autorización, creación, renovación o eliminación de VPN client to site para organismos de tránsito que hagan o no parte de la línea base del RUNT definidos como “OT alcance RUNT” y “OT fuera alcance RUNT”. La VPN client to site será utilizada en dos casos específicos:

- Creación de un nuevo organismo de tránsito.
- Traslado de un organismo de tránsito.

En caso de que se presente un requerimiento particular que requiera la habilitación de VPN client to site para un organismo de transito deberá ser aprobado por el Ministerio de Transporte.

3. Generalidades

Para efectos de este procedimiento se entenderá como un “OT alcance RUNT”, a los organismos de tránsito que fueron creados y que se encontraban operativos a la fecha de la firma del contrato de Concesión 033 (07 de junio de 2007) y como un “OT fuera alcance RUNT”, a aquellos organismos de tránsito creados por el Ministerio de Transporte después de la fecha de la firma del contrato de Concesión 033.

De acuerdo con el numeral 7.2 del manual de condiciones técnicas y tecnológicas COTT, los organismos de tránsito únicamente pueden acceder a la plataforma RUNT a través de canales dedicados de datos o VPN.

La conectividad a través de VPN está definida en el numeral 7.3 del manual de condiciones técnicas y tecnológicas COTT donde se establece:

> *La comunicación entre los diferentes OT, las DT y el nodo central del RUNT, puede realizarse a través de Internet, siempre y cuando esta comunicación sea segura, es decir esté encriptada desde el origen hasta el destino. Por este motivo, los equipos de comunicaciones involucrados en el RUNT deben soportar el estándar VPN, de acuerdo con las siguientes características:*
>
> - *Estándares de encriptación DES y 3DES, IKE con certificados digitales (PKI X.509) o secreto compartido o negociación manual, deben estar como soportes.*
> - *Autenticación fuerte con SHA-1 y MD5.*
> - *Políticas basadas en NAT que permita operar con aplicaciones extranet para VPN.*
> - *Alta Disponibilidad de las VPN.*
>
> *La Concesión se reserva el derecho de utilizar Redes Privadas Virtuales cuando las condiciones de conectividad del OT así lo requieran.*

3.1 Políticas de seguridad

Las VPN client to site entregadas a los organismos de transito deberán cumplir las siguientes políticas de seguridad:

- Se entregará una VPN client to site para cada usuario asignado por el organismo de transito que deberá indicarse en la solicitud inicial del secretario de tránsito.
- El uso de la VPN es personal e intransferible.
- Se entregarán máximo 4 VPN client to site por organismo de tránsito.
- La VPN client to site solo permitirá el acceso a la plataforma HQ-RUNT.
- La VPN client to site solo funcionara de lunes a sábado de 7 am a 7pm teniendo en cuenta el horario habitual de operación de los organismos de tránsito a nivel nacional.
- El acceso a internet y sus condiciones de servicio y seguridad estarán bajo la responsabilidad del organismo de tránsito.
- Cada VPN client to site estará bajo la responsabilidad del organismo de tránsito, por tanto, los tramites efectuados con dicha conexión estarán bajo su gestión, control y competencia.
- No se habilitará el acceso por VPN de manera simultanea con el acceso a través de canal dedicado.

3.2 Políticas generales

Estas políticas definen los lineamientos para la habilitación de VPN client to site para organismos de transito:

- En los casos en que un organismo de transito nuevo esté listo para operar, pero que aún no tenga instalado el canal dedicado, se puede brindar acceso a través de VPN mientras se finalizan las actividades de instalación del canal.
- Para las actividades de traslado es viable habilitar VPN temporalmente mientras se ejecutan las actividades de instalación.
- El tiempo de aprobación y vigencia de la VPN client to site para organismos de transito estará definido por el Ministerio de Transporte.
- El usuario que solicita la VPN deberá tener las respectivas credenciales de acceso a la plataforma HQ-RUNT.
- El computador donde se utiliza la VPN deberá contar con las herramientas tecnológicas pertinentes para el funcionamiento de la VPN y su soporte y funcionamiento estará bajo responsabilidad del organismo de tránsito.

4. Procedimientos

4.1 Creación VPN

Actividades	Descripción	Responsables
1. Solicitud de aprobación para operación por VPN	Esta solicitud puede llegar en dos casos, nuevos organismos de tránsito y traslados de organismos de tránsito activos. El organismo de tránsito a través de su secretario de transito deberá solicitar al Ministerio de Transporte a la Coordinación Grupo RUNT la aprobación de la VPN con la respectiva justificación para cualquiera de los dos casos y la cantidad de usuarios respetando los lineamientos y políticas generales y de seguridad. El Ministerio de transporte evaluara la solicitud y aprobara o no la creación de la VPN. En caso de que la VPN sea aprobada, se deberá indicar el tiempo de vigencia. La aprobación podrá ser remitida a través de correo electrónico o través de oficio físico.	Organismo de transito Ministerio de transporte
2. Tramitar solicitud con RUNT	El organismo de Tránsito deberá solicitar a la Concesión RUNT al área de seguridad al correo seguridad@runt.com.co la creación de las VPN remitiendo la autorización del Ministerio de Transporte. La solicitud deberá contener los siguientes datos de los usuarios: ✓ Nombre completo del usuario. ✓ Cargo del funcionario en el organismo de tránsito. ✓ Cedula de ciudadanía. ✓ Correo electrónico personal. ✓ Teléfono personal. Es responsabilidad del organismo de transito tramitar la solicitud con 5 días hábiles de antelación a la fecha de inicio de operación por VPN con el fin de evitar afectación de servicios a los usuarios.	Organismo de transito
3. Gestionar la solicitud	✓ La concesión RUNT gestionara internamente la solicitud dentro de los tiempos definidos que corresponden a máximo 6 horas hábiles. ✓ Se enviarán por correo electrónico a los correos personales las credenciales de acceso de la VPN con el instructivo de utilización.	Concesión RUNT

4.2 Renovación de VPN

Actividades	Descripción	Responsables
1. Solicitud de aprobación para renovación de VPN	El organismo de Tránsito a través de su secretario de transito deberá solicitar al Ministerio de Transporte la aprobación de la renovación de la VPN con la respectiva justificación respetando los lineamientos y políticas generales y de seguridad. El Ministerio de transporte evaluara la solicitud y aprobara o no la	Organismo de transito Ministerio de transporte

Actividades	Descripción	Responsables
	renovación de la VPN. En caso de que la renovación de la VPN sea aprobada, se deberá indicar el tiempo de vigencia. La aprobación podrá ser remitida a través de correo electrónico o través de oficio físico.	
2. Tramitar solicitud con RUNT	El organismo de tránsito a través de su secretario de transito deberá solicitar al Ministerio de Transporte a la Coordinación Grupo RUNT la aprobación de la renovación de la VPN con la respectiva justificación para cualquiera de los dos casos y la cantidad de usuarios respetando los lineamientos y políticas generales y de seguridad: ✓ Nombre completo del usuario. ✓ Cargo del funcionario en el organismo de tránsito. ✓ Cedula de ciudadanía. ✓ Correo electrónico personal. ✓ Teléfono personal. Es responsabilidad del organismo de transito tramitar la solicitud con 5 días hábiles de antelación a la fecha de inicio de operación por VPN con el fin de evitar afectación de servicios a los usuarios.	Organismo de transito
3. Gestionar la solicitud	✓ La concesión RUNT gestionara internamente la solicitud dentro de los tiempos definidos internamente que corresponden a máximo 6 horas hábiles. ✓ Se enviarán por correo electrónico la notificación de renovación del acceso.	Concesión RUNT

4.3 Eliminación de VPN

La eliminación de las VPN cliente to site pertenecientes a un organismo de transito se efectuará por directriz del Ministerio de transporte. Teniendo en cuenta que las VPN tienen un tiempo de vigencia definido por políticas de seguridad, las VPN que pierden vigencia quedan completamente fuera de operación.

5. Registros Generados del Procedimiento

CONTROL DE REGISTROS										
Registro	**Soporte**		**Dónde Archiva**	**Retención**		**Disposición**		**Clasificación de la información**	**Acceso**	**Actividades de disposición final**
	P	**ME**		**Gestión**	**Central**	**E**	**CT**			
Correo solicitud de VPN organismo de transito		x	R:\SISTEMAS DE GESTION\00 SGC RUNT-REGISTROS\09 G Infraestructura Tecnológica\	Permanente	No aplica		X	Uso interno	Especialista de seguridad de la información	No aplica
P: Papel			**ME:** Medio electrónico			**E:** Eliminar		**CT:** Conservación total		