	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED



SECRETARÍA GENERAL

EQUIPO DE INFRAESTRUCTURA Y SOPORTE TECNOLÓGICO

BOGOTÁ, NOVIEMBRE DE 2021




	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

TABLA DE CONTENIDO

1. OBJETIVO.....	5
2. ALCANCE.....	5
3. DOCUMENTOS DE REFERENCIA Y RELACIONADOS.....	5
4. CONCEPTOS Y DEFINICIONES.....	6
5. POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	9
5.1 Generalidades	9
5.2 Ciclo de vida de la red	10
5.2.1 Fase de Adquisición	11
5.2.2 Fase de despliegue	11
5.2.3 Fase de operación	11
5.2.4 Fase de retiro	11
5.2.5 Fase de Mejora continua	12
5.3 Controles de seguridad de la red	12
5.3.1 Control de acceso.....	12
5.3.2 Autenticación	12
5.4 Seguridad de la red.....	13
5.4.1 Nombramiento Redes Vpn	14
5.4.2 Grupos de navegación en Internet	14
5.4.2.1 Nombramiento grupos de navegación en Internet	15
5.4.3 Topología de la red y servicios	15
5.4.4 Monitoreo de los dispositivos de red y seguridad	16
5.4.5 Herramientas para asegurar la red	17
5.4.6 Nombramiento de equipos de red	19
5.4.6.1 Nombramiento por capas	20
5.4.6.2 Nombramiento de dispositivos según el fabricante.....	20

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

5.4.7 Nombramiento de dispositivos según la Sede	20
5.4.8 Nombramiento para los Switches	21
5.4.9 Nombramiento de los puertos.....	21
5.4.9.1 Según sus conexiones.....	22
5.4.9.2 Según su tipo de puerto.....	22
5.4.9.3 Según su capacidad	22
5.4.10 Nombramiento de servidores.....	23
5.5 Seguridad de la comunicación	23
5.6 Ciframiento de los datos a través de la red	24
5.6.1 Cifrado de datos en tránsito.....	24
5.6.2 Cifrado de datos en reposo	24
5.6.3 Doble factor de autenticación	24
5.7 Protocolos autorizados	24
6. REVISIÓN Y CUMPLIMIENTO	25


	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

LISTADO DE TABLAS

Tabla 1. Tipos de Dispositivos de Red – ANT.....	17
Tabla 2. Protocolos Autorizados ANT	25

LISTADO DE ILUSTRACIONES

Ilustración 1. Modelo básico para el ciclo de vida de la red ANT	10
Ilustración 2. Diseño de Topología del servicio de internet.....	15
Ilustración 3. Diseño de topología del servicio de MPLS	16
Ilustración 4. Diseño físico del Datacenter.....	18
Ilustración 5. Diseño del Datacenter ANT	19

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

1. OBJETIVO


Establecer la política que brinde los lineamientos, directrices y recomendaciones mínimas sobre el aseguramiento e integridad de los servicios de red de la Agencia Nacional de Tierras (ANT) con el objetivo de garantizar la disponibilidad de las aplicaciones, elementos de comunicaciones y de seguridad.

2. ALCANCE

Esta política aplica para todos los funcionarios, contratistas, colaboradores y demás partes interesadas que se encarguen de administrar la plataforma tecnológica y dispositivos de red, comunicaciones y seguridad con el fin de garantizar el aseguramiento e integridad de los servicios de red de la ANT en pro de la confidencialidad, privacidad e integridad de la información.

3. DOCUMENTOS DE REFERENCIA Y RELACIONADOS

- ISO/IEC 27001:2013.
- Política de seguridad de la información INTI-Política -001.
- Lineamientos de seguridad de la información INTI - Política-008.
- Política de protección de datos personales INTI-Política-011.
- Decreto 1008 del 14 de junio de 2018.
- Resolución 00500 de marzo 10 de 2021.
- Guía 3 procedimientos de seguridad de la información – MinTic.
- INTI-P-006 Gestión de los Servicios Tecnológicos.
- ADMBS-P-014 administración de cuentas de usuario y acceso a los recursos tecnológicos.
- ADMBS-F-072- creación y/o novedad de usuarios.
- ADMBS-F-078 solicitud de VPN usuarios internos y externos
- GINFO-I-015 buenas prácticas en ITIL para la gestión de los servicios de TI
- GINFO-I-012 instructivo nombramiento equipos de cómputo
- Ficha técnica de salidas y productos – ABMDS-FT-001 BAJA DE BIENES

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

4. CONCEPTOS Y DEFINICIONES

Colaborador: persona que ejerce unas funciones u obligaciones dentro de la Agencia Nacional de Tierras como funcionario, contratista o tercero que apoyan el cumplimiento de la planeación estratégica de la entidad.

Contraseña: es una combinación de palabras, frases y signos que sirven de autenticación ante un sistema de información y por lo tanto debe mantenerse en secreto para evitar la suplantación de identidad, pérdidas y fugas de información.

Cifrado de datos: procedimiento que utiliza un algoritmo de cifrado con cierta clave para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta del algoritmo.

Confidencialidad: hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos. sólo las personas autorizadas pueden acceder a la información

Correo electrónico: también conocido como e-mail, es un servicio de red que permite mandar y recibir mensajes con múltiples destinatarios o receptores, situados en cualquier parte del mundo.


Disponibilidad: asegura la fiabilidad y el acceso oportuno a los datos y recursos por parte de los individuos o personas autorizadas.

Dispositivo de red: cualquier hardware que conecte diferentes recursos de red permitiendo la comunicación e interacción entre dos o más dispositivos.

Directorio Activo: base de datos y un conjunto de servicios que conectan a los usuarios con los recursos de red que se necesitan para ingresar a las diversas aplicaciones de la entidad a gestionar su trabajo.

DDos- Distributed Denial Of Service: es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

https: (HyperText Transfer Protocol Secure: protocolo seguro de transferencia de hipertexto) es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

Información: se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.¹

Integridad: los datos se mantienen intactos libre de modificaciones o alteraciones por terceros. Sólo se podrá modificar la información mediante autorización.

Interrupción: situación que impide a los usuarios y colaboradores de la entidad acceder a los datos y las aplicaciones corporativas.

MPLS - Multiprotocol Label Switching: conmutación de etiquetas multiprotocolo, es una técnica que unifica la transferencia de diferentes tipos de datos a través de una misma red, para superar las limitaciones de velocidad y mejorar el flujo de trabajo de internet.

NAC (NETWORK ACCESS CONTROL):

Red: interconexión de un número determinado de computadores (o de redes, a su vez) mediante dispositivos alámbricos o inalámbricos que, mediante impulsos eléctricos, ondas electromagnéticas u otros medios físicos, les permiten enviar y recibir información en paquetes de datos, compartir sus recursos y actuar como un conjunto organizado.

Red LAN - Local Area Network: red de Área Local, es un grupo de computadoras y dispositivos periféricos que comparten una línea de comunicaciones común o un enlace inalámbrico a un servidor dentro de un área geográfica específica.


RDP - Remote Desktop Protocol Protocolo: permite que el escritorio de un equipo informático sea controlado a distancia por un usuario remoto.

Router: es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función es la de establecer la ruta que destinará a cada paquete de datos dentro de una red informática

Sandbox: un entorno de prueba aislado dentro de un sistema informático. Este programa nos permite ejecutar otras aplicaciones o abrir archivos sin poner en riesgo la aplicación, el sistema o la plataforma en la que se ejecutan

Siem- Security Information and Event Management: es un sistema de seguridad que persigue proporcionar a las empresas una respuesta rápida y precisa para detectar y responder ante cualquier amenaza sobre sus sistemas informáticos,

¹ Ley 712 de 2014

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

SSL - Secure Sockets Layer: protocolo de cifrado utilizado para garantizar la seguridad de las comunicaciones a través de Internet.

SSH: es un protocolo que garantiza que tanto el cliente como el servidor remoto intercambien informaciones de manera segura y dinámica

Switch: es un dispositivo que sirve para conectar varios elementos dentro de una red. En casa, un switch puede conectar dispositivos como una impresora, un PC, una consola o una televisión.


TFTP - protocolo trivial de transferencia de archivos: es un protocolo simple que proporciona una función básica de transferencia de archivos sin autenticación de usuario.

VLAN - Virtual Local Area Network: red de área local virtual, es un segmento lógico más pequeño dentro de una gran red física cableada. Las diferentes estaciones se combinan en una solución de red independiente de su ubicación y siempre que estén conectadas entre sí en la misma LAN, es posible combinarlas mediante una VLAN.

VPN - Virtual Private Network: es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando internet.

Waf - Web application firewall: protege de múltiples ataques al servidor de aplicaciones web en el backend. La función del WAF es garantizar la seguridad del servidor web mediante el análisis de paquetes de petición HTTP / HTTPS y modelos de tráfico.

Usuario: Toda persona que tiene acceso a cualquier recurso tecnológico de la Agencia (correo electrónico, cuenta de dominio, bases de datos, aplicaciones corporativas, página web, entre otras).


	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

5. POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED

Establecer los lineamientos para el aseguramiento de los servicios disponibles en la red de la Agencia Nacional de Tierras con el fin de mantener la confidencialidad, disponibilidad, privacidad e integridad de la información minimizando los riesgos a los que se encuentra expuesta la información en el proceso de emisión, envío y recepción de esta.

5.1 Generalidades

- ❖ Todos los dispositivos que sean instalados en la red deben ser configurados, asegurados y monitoreados con el fin de evitar vulnerabilidades a los que se encuentran expuestos.
- ❖ Todos los dispositivos de red deben ser adquiridos al fabricante o distribuidor autorizado por el fabricante con un tiempo de garantía establecido sobre el mismo.
- ❖ El acceso de visitantes a la red de la ANT se encuentra establecida por una red WiFi abierta y limitada a temas educativos y páginas del gobierno.
- ❖ Los funcionarios, contratistas y partes interesadas que estén incluidos en el directorio activo podrán acceder desde sus computadores personales a las aplicaciones corporativas haciendo uso de la WiFi prevista para tal fin.
- ❖ Todas las redes WiFi deben tener un segmento específico.
- ❖ Los directivos de la entidad tienen acceso a la red WiFi con un perfil específico que les permite navegar por diversos sitios con una configuración especial.
- ❖ Los funcionarios, contratistas y colaboradores que poseen acceso VPN tendrán el acceso limitado a las redes de la entidad de acuerdo con el rol a desempeñar dentro de la Agencia y los grupos previamente establecidos dentro del concentrador VPN.
- ❖ Las claves de los accesos a los dispositivos de red deben cumplir con las políticas de seguridad de la información de la entidad y deben cambiarse frecuentemente.
- ❖ La autenticación para el acceso a los dispositivos de red se realiza a través del directorio activo.
- ❖ El tiempo de bloqueo de pantalla por inactividad de los equipos de cómputo es de 15 minutos.
- ❖ El tiempo de bloque para las conexiones a las redes VPN por inactividad es de 1 hora.
- ❖ Las contraseñas que se usan en la configuración de los dispositivos de red deben cumplir los lineamientos de la política de seguridad de la información.
- ❖ Todos los dispositivos de red deben tener asignada una dirección IP perteneciente a los segmentos establecidos por la entidad para cada elemento de red.
- ❖ Todos los dispositivos de red que sean críticos para la operación deben estar monitoreados para identificar los eventos.

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

- ❖ Todos los equipos de red deben tener configurado y habilitado los protocolos básicos de acceso (SSH, HTTPS, TFTP y RDP).
- ❖ Todas las conexiones exitosas o fallidas a los dispositivos de red están monitoreadas quedando su registro en el gestor de la aplicación.
- ❖ Se deben mantener actualizados los dispositivos de red, de acuerdo con las últimas versiones liberadas por el fabricante.
- ❖ Se deben restringir el uso de acceso al internet, contenido multimedia y redes sociales de acuerdo con el perfil, funciones u obligaciones del funcionario, contratista o colaborador.
- ❖ Mantener actualizados los diseños del centro de datos, diseño de las topologías del redes e internet.
- ❖ Mantener actualizados los inventarios que hacen parte de los dispositivos de red en la CMDB.
- ❖ Todos los dispositivos de red deben estar nombrados acorde con los lineamientos aquí mencionados.

5.2 Ciclo de vida de la red

Se establecen las siguientes fases mínimas como factor principal para gestionar el ciclo de vida la red:

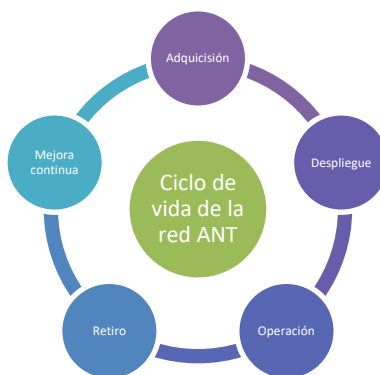



Ilustración 1. Modelo básico para el ciclo de vida de la red ANT

Fuente: Equipo de Infraestructura y Soporte Tecnológico

Teniendo en cuenta que se trata de un modelo cíclico e interactivo, los dispositivos podrán reusarse en cualquier momento permitiendo la optimización de recursos técnicos, tecnológicos y de inversión para maximizar y potencializar el gasto público.

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

A continuación, se describen cada una de las fases que hacen parte del modelo del ciclo de vida de la red para la ANT:

5.2.1 Fase de Adquisición

En esta fase se tiene en cuenta el manual de contratación de la Entidad para la adquisición de un bien o servicio en pro de fortalecer la infraestructura tecnológica permitiendo optimizar la productividad, el funcionamiento y la seguridad de la información de la Agencia, adicionalmente se realizara un estudio técnico en donde se definirá los requerimientos mínimos que debe cumplir el elemento a adquirir, así como también se validarán los adelantos tecnológicos del mercado con el fin de proponer mejoras que soporten los cambios de configuración a futuro.

5.2.2 Fase de despliegue


En esta fase se de tener en cuenta el instructivo de buenas prácticas en ITIL para la gestión de los servicios de TI (GINFO-I-015) donde se abordan temas como la gestión de cambios tecnológicos y gestión de entregas y despliegues. Previamente se debe realizar el alistamiento del dispositivo como son: actualización de firmware del elemento, migración o inclusión de configuraciones previas, registro de inventarios e inclusión de placa por parte de almacén general, solicitud del activo por parte del EIST, establecimiento de una clave robusta, y ejecución de plantilla base de configuración, si esta última no existe se debe crear de acuerdo con los requerimientos de la entidad, pruebas de funcionalidad y homologación de servicios en caso requerido, entre otros.

5.2.3 Fase de operación

Una vez el dispositivo se encuentre instalado y operando, se debe monitorear su desempeño, rendimiento, alertas y/o eventos generados, seguridad, ubicación y reubicación física para garantizar el correcto funcionamiento y disponibilidad.

5.2.4 Fase de retiro

El encargado de la infraestructura y soporte tecnológico de la entidad debe hacer un análisis de la vida útil del dispositivo que permita determinar si este ha cumplido con su objetivo para dar de baja siguiendo Política nacional para la gestión integral de los residuos de aparatos eléctricos y electrónicos (RAEE) y la ficha técnica de salidas y productos – ABMDS-FT-001 BAJA DE BIENES.

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

5.2.5 Fase de Mejora continua

La infraestructura tecnológica (hardware y software) deberá contar con las actualizaciones de sistema operativo y versionamiento de licenciamiento de acuerdo con las versiones liberadas por los fabricantes previo análisis de impacto sobre la operación. Esto permitirá garantizar la seguridad, mantenimiento y funcionamiento del elemento de configuración y reducir el riesgo ante fallos y/o daños. Adicionalmente se deberá validar si requiere reconfiguración que permita explotar el máximo provecho de sus funcionalidades y capacidades para soportar las necesidades de los usuarios.

5.3 Controles de seguridad de la red

5.3.1 Control de acceso


Todos los funcionario, contratista o parte interesada de la ANT pueda acceder a los diversos recursos de red y sistemas de información de la entidad, siempre y cuando se encuentren registrados en el directorio activo previo cumplimiento de los requisitos establecidos y mencionados en los siguientes documentos:

- ❖ INTI-P-006 Gestión de los Servicios Tecnológicos.
- ❖ ADMBS-P-014 administración de cuentas de usuario y acceso a los recursos tecnológicos.
- ❖ ADMBS-F-072- creación y/o novedad de usuarios.
- ❖ ADMBS-F-078 solicitud de VPN usuarios internos y externos
- ❖ GINFO-I-015 buenas prácticas en ITIL para la gestión de los servicios de TI

5.3.2 Autenticación

Todos los funcionario, contratista o colaborador de la ANT previo registro de sus datos en el directorio activo y aplicaciones de la entidad podrá hacer uso de los sistemas de información disponibles para el cumplimiento de sus obligaciones y/o funciones teniendo en cuenta que su uso estará regido por los lineamientos y políticas de seguridad de la información de la Entidad. Existen varias aplicaciones que contienen el doble factor de autenticación permitiendo una mayor seguridad en la gestión de la información.

Para el caso de los accesos a redes VPN los usuarios se deben autenticar y deben estar asociados a un grupo específico creado previamente en el directorio activo. Adicionalmente, dentro del firewall se establecen reglas de conexión que parametrizan las redes y/o servicios a los cuales podrá acceder el usuario.

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

Por otro lado, se establecen los siguientes criterios de autenticación que deberán ser acatados:


- ❖ Solo se mantendrá activa una (1) sesión por usuario y dispositivo.
- ❖ El tiempo de bloqueo de pantalla por inactividad de los equipos de cómputo es de 15 minutos.
- ❖ El tiempo de bloque para las conexiones a las redes VPN por inactividad es de 1 hora.
- ❖ Máximo 5 intentos erróneos para el bloqueo de la clave. Posteriormente será activada pasado los 15 minutos. Si persiste el error la clave se bloquea.
- ❖ La clave vence cada 45 días por política de seguridad de la información.
- ❖ Para la creación de los claves estas deben cumplir con los lineamientos establecidos en la política de seguridad de la información.
- ❖ Las características mínimas que debe tener una contraseña se encuentran configuradas en el directorio activo.
- ❖ Para el caso de los usuarios locales de los dispositivos de red, se debe asignar manualmente una contraseña con los requisitos de complejidad definidos en el directorio activo.
- ❖ Las contraseñas de las aplicaciones y dispositivos de red deben estar cifradas.

5.4 Seguridad de la red

Los dispositivos de seguridad de la red son de administración y uso exclusivo del Equipo de Infraestructura y Soporte Tecnológico adscrito a la Secretaría General, para la administración y gestión se deben tener usuarios locales diferentes al administrador, que corresponde al usuario con permisos y privilegios totales y es de uso exclusivo de la entidad.

Para el acceso a los servicios VPN de la ANT está definido por cuatro (4) grupos (Tecnología, SoporteTI, Proveedores, Operación), estos grupos delimitan el acceso a los segmentos de red, de tal manera que se garantiza que cada usuario ingrese solamente a los servicios que requiere para operar., Los administradores del Equipo de Infraestructura y Soporte Tecnológico deberán gestionar estos accesos con base en las siguientes características:

1. **GVPN_SOPORTETI:** en este grupo se encuentran los especialistas administradores de la plataforma tecnológica que tendrán acceso a las diferentes redes de servidores, administración y redes LAN.
2. **GVPN_OPERACIÓN:** aquí se encuentran los funcionarios, contratistas y partes interesadas que tendrán acceso a los escritorios remotos de la ubicación de su computador y algunos servidores específicos como las carpetas compartidas (File Server).
3. **GVPN_TECNOLOGÍA:** se relacionan todos los especialistas de la SSIT que se encargan del desarrollo de aplicaciones. Solo tienen acceso a los segmentos de los servidores y red LAN del piso 3 donde se ubica físicamente la oficina de TI.

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

4. **GVPN_PROVEEDORES:** usuarios locales que por alguna circunstancia deben ejecutar obligaciones contractuales con la entidad. Estos usuarios solo tendrán acceso a un servidor específico del segmento de la red de servidores de producción.

5.4.1 Nombramiento Redes Vpn

El estándar para la creación de nuevos grupos asociados a las redes VPN debe conservar la siguiente estructura:

- La primera letra corresponde a la palabra “GRUPO”:



- Los siguientes 3 caracteres corresponden a la sigla del tipo de red.




- El siguiente carácter corresponde al símbolo underscore (_) y
- La palabra final debe estar relacionada al tipo de grupo de usuarios que almacenará.

5.4.2 Grupos de navegación en Internet

La entidad cuenta con un directorio activo en donde se crean los siguientes grupos de navegación para la prestación del servicio de Internet con el fin de controlar los accesos de los usuarios a las diversas páginas y proteger la red de la entidad:

1. Grupo de Navegación VIP: en este grupo es uso exclusivo para los directivos de la entidad que ocupan los siguientes cargos: Director General, Secretario General, Asesores, Directores Misionales y Jefes de Oficina cuya navegación en Internet no tiene restricciones, para redes sociales, audio, voz y video.
Nota: Para el perfil VIP está restringido el contenido para adultos, armas, juegos y descargas entre otros.
2. Grupo de Navegación Básico: aquí se incluyen todos los usuarios de la operación los cuales tiene acceso a buscadores, páginas del gobierno, servicios de whatsapp, soluciones de colaboración como video conferencia
Nota: Para el perfil Básico está restringido el contenido para adultos, armas, juegos, youtube, redes sociales y descargas entre otros.

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

3. Grupo de Navegación Soporte: este grupo de es de uso exclusivo para el Equipo de Infraestructura y Soporte Tecnológico, tiene FULL permisos de navegación realizar toda y cada una de las pruebas que se requieran para la administración y gestión de los servicios.

Nota: Para el perfil de Soporte está restringido el contenido para adultos, armas, juegos, entre otros.

5.4.2.1 Nombramiento grupos de navegación en Internet

La estructura para la creación de nuevos grupos de navegación para internet debe seguir el siguiente nombramiento:

- Los primeros caracteres corresponden a G(Grupo) y deben ser en mayúscula.
- Los segundos caracteres identifican la palabra Navegación
- El siguiente carácter corresponde al símbolo underscore (_) y
- La palabra final debe estar relacionada al tipo de grupo de usuarios que almacenará.

5.4.3 Topología de la red y servicios

Se analizó, diseñó y estructuró la topología del servicio de internet el cual debe actualizarse si este llegará a presentar algún cambio:

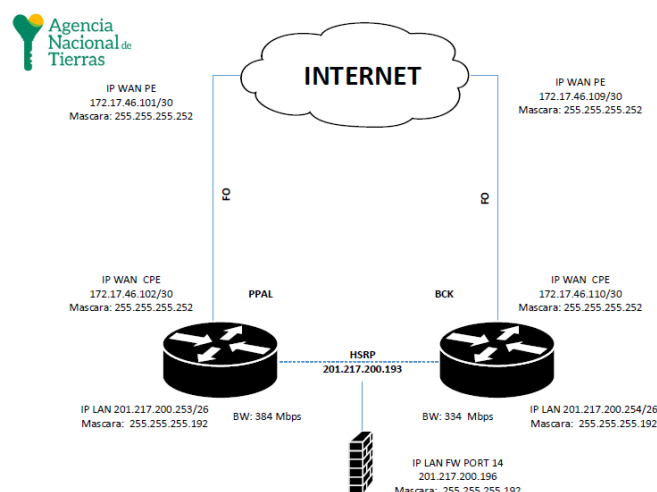



Ilustración 2. Diseño de Topología del servicio de internet

Fuente: Equipo de Infraestructura y Soporte Tecnológico

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

También se estableció la topología para el servicio MPLS quedando de la siguiente manera:

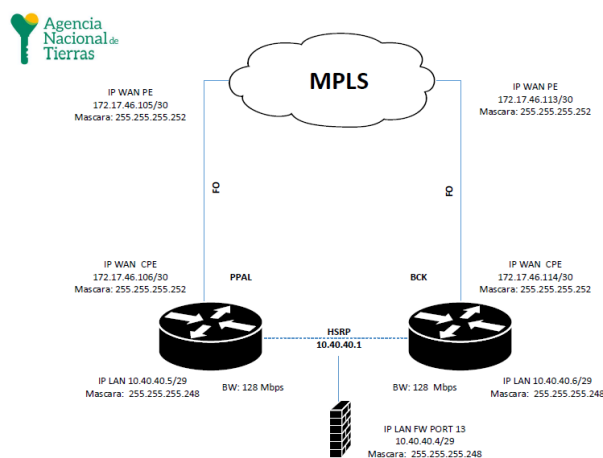



Ilustración 3. Diseño de topología del servicio de MPLS

Fuente: Equipo de Infraestructura y Soporte Tecnológico

5.4.4 Monitoreo de los dispositivos de red y seguridad

La entidad cuenta con una herramienta (correlacionador de eventos) enfocada en el monitoreo de alarmas y eventos que permiten integrar a la gestión los dispositivos por medio del protocolo SNMP y realizar reportes de los eventos recibidos de los servicios críticos de la entidad. A través de los análisis de los eventos recibidos se deben tomar las acciones correspondientes con el fin de mitigar o remediar la alerta presentada. Este monitoreo debe realizarse permanentemente para detectar las alertas tempranas y evitar interrupción en la prestación de los servicios.

Estos eventos deben gestionarse de acuerdo con el Instructivo de buenas prácticas en ITIL para la gestión de los servicios de TI (GINFO-I-015), numeral 5.6 Monitoreo y Gestión de Eventos Tecnológicos.

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

5.4.5 Herramientas para asegurar la red

Con el ánimo de respaldar la continuidad en los servicios, la entidad cuenta con diversos tipos de dispositivos de red que permiten compartir, centralizar, proteger, asegurar la información, monitorear los eventos, gestionar el soporte y garantizar el direccionamiento de paquetes de datos, voz, video, internet entre otros.


En la siguiente tabla se detallan los tipos de dispositivos que posee la entidad:

Tabla 1. Tipos de Dispositivos de Red – ANT

Fuente: Equipo de Infraestructura y Soporte Tecnológico

Dispositivo	Tipo de dispositivo
Dispositivos de red	Switches
	Router
	APs
Dispositivos de seguridad	
	FortiSiem
	FortiAnalyzer
	Firewall
	Sandbox
	WAF
	DDOS
Dispositivos de infraestructura	Servidores
	Almacenamiento
	Tape (herramienta para grabación en cinta)

Por otro lado, se cuenta con el diseño del centro de datos que permite localizar de manera rápida y sencilla los dispositivos de red ubicados dentro de los diversos racks para el acceso ante cualquier eventualidad. Este diseño debe ser actualizado cada vez que se requiera:

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

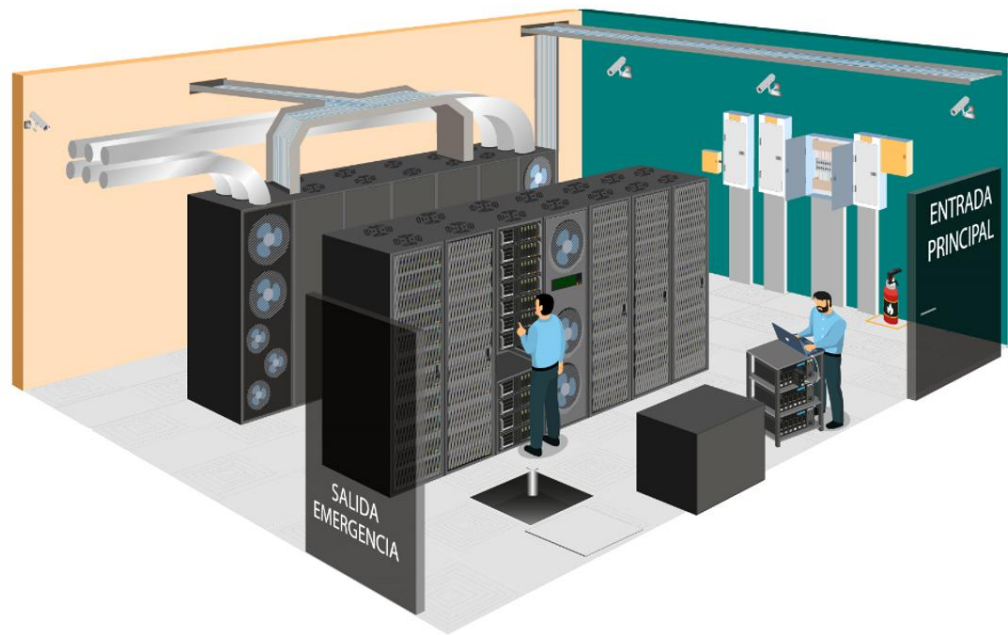

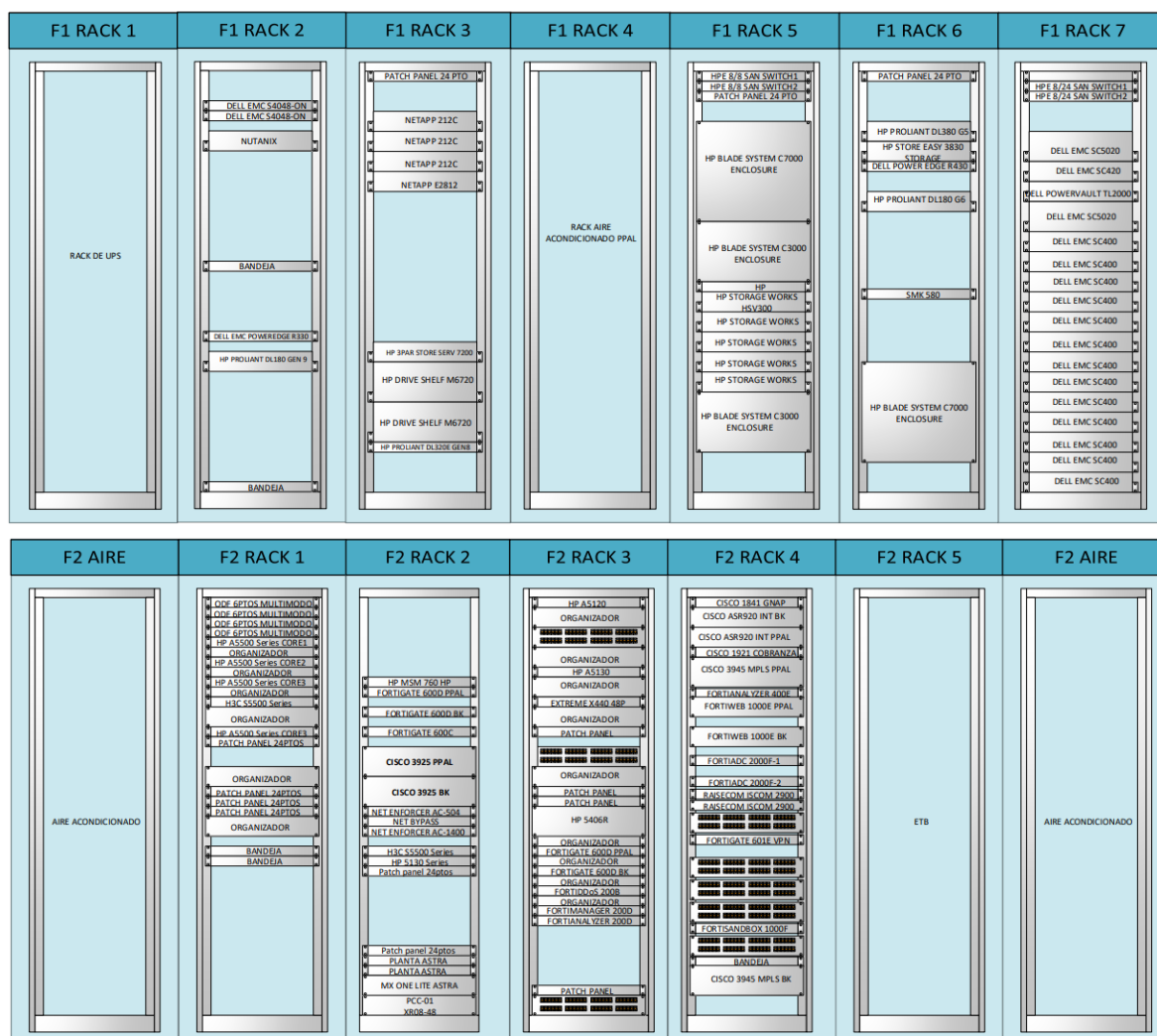



Ilustración 4. Diseño físico del Datacenter

Fuente: Equipo de Infraestructura y Soporte Tecnológico

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021



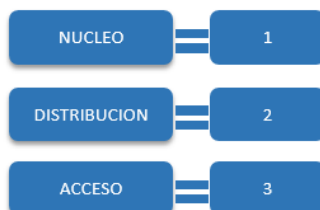
Fuente: Equipo de Infraestructura y Soporte Tecnológico

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

5.4.6.1 Nombramiento por capas

A nivel de red, la entidad ha definido el siguiente esquema que debe ser tenido en cuenta para la configuración de un dispositivo de red:

❖ Categorización de la red:



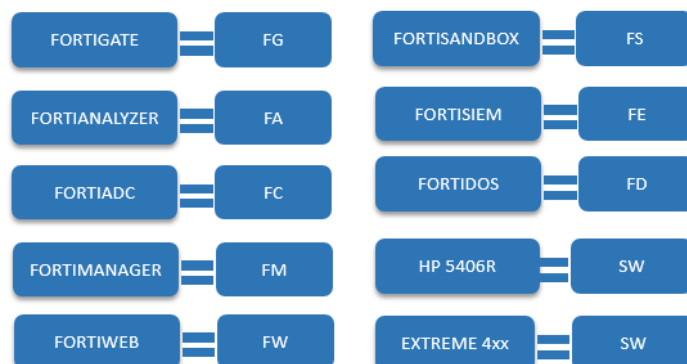
Cada uno de estos elementos (núcleo, distribución y acceso) cumplen la función principal de la red y soporta todo el tráfico de la entidad.

❖ Seguridad:

Todos los equipos de seguridad deben tener la nomenclatura iniciando con el consecutivo aquí mencionado:




5.4.6.2 Nombramiento de dispositivos según el fabricante



5.4.7 Nombramiento de dispositivos según la Sede

El identificador se construye de la siguiente manera:

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

- **Departamento:** uso de los primeros 3 caracteres en mayúscula
- **Municipio:** uso de los primeros 3 caracteres en mayúscula
- **Sitio o sede:** uso de los primeros 3 caracteres del nombre de la sede
- **Fabricante:** uso de 1 carácter
- **Producto:** uso de 2 caracteres
- **Capa/Seguridad Perimetral:** 1 dígito numérico
- **Orden:** 2 dígitos numéricos de acuerdo con el consecutivo de nombramiento del dispositivo.

Ejemplo:

CUN_BOG_CAN_FFG401

CUN_BOG_CAN_FFG402

5.4.8 Nombramiento para los Switches

El identificador se construye de la siguiente manera:

- **Departamento:** uso de los primeros 3 caracteres en mayúscula
- **Municipio:** uso de los primeros 3 caracteres en mayúscula
- **Sitio o sede:** uso de los primeros 3 caracteres del nombre de la sede
- **Fabricante:** uso de 1 carácter
- **Producto:** uso de 2 caracteres
- **Capa/Seguridad Perimetral:** 1 dígito numérico
- **Piso:** 1 dígitos numérico de acuerdo con la ubicación física del piso que cubre el dispositivo.
- **Equipo:** 2 dígitos correspondientes al consecutivo del dispositivo


Ejemplo:

CUN_BOG_CAN_ESW3301

CUN_BOG_CAN_ESW3302

5.4.9 Nombramiento de los puertos

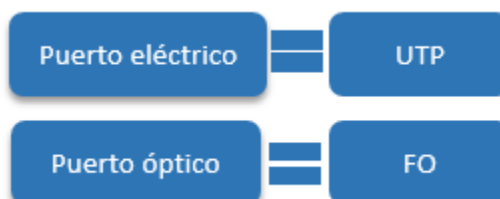
Los puertos se deben nombran de la siguiente manera para conservar el estándar definido:

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

5.4.9.1 Según sus conexiones



5.4.9.2 Según su tipo de puerto



5.4.9.3 Según su capacidad

De acuerdo con la capacidad que tienen los puertos que se manejan en la entidad, estos se identifican como troncales en megas (MB) y para el ancho de banda su nomenclatura corresponde a la capacidad del puerto conectado físicamente:




5.2.4.4 Descripción general nomenclatura de los puertos

<Conexiones>_TO_F<numero_fila>_R<numero_de_rack>_<"nombre_equipo_destino">_PTO-<pto_dest>_PTO<Tipo_puerto>_BW-<K,M,G>

Ejemplo: este ejemplo detalla el nombramiento de puertos tomando el firewall asignado al puerto 4.

TO_F2_R4_"CUN_BOG_CAN_HSW1101"_PTO-A7_FO_BW-1G

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

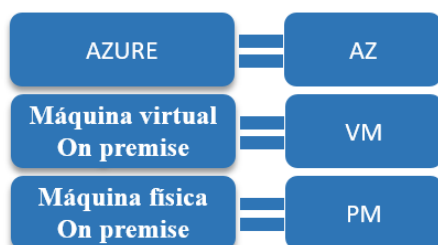
Cabe mencionar que, para el nombramiento de equipos de cómputo, este se encuentra relacionado en el instructivo GINFO-I-012 del mapa de procesos de la Entidad y se debe cumplir con su estructura para mantener un estándar.

5.4.10 Nombramiento de servidores

- Las primeras 3 letras identifica el tipo de elemento de configuración, que para este caso es un Servidor y debe nombrarse en letras mayúsculas (SRV).

SRV

- De acuerdo con la ubicación (física/nube) puede tener el siguiente estándar:




- El nombre del servidor debe tener una longitud máxima de 15 caracteres.
- En el nombre del servidor se deben identificar el ambiente al cual pertenece el servidor (PRO, PRU, DES).
- El restante del nombre debe asociarse al servicio o rol que provee este elemento.

Ejemplo:

SRVVMXROADPRU

5.5 Seguridad de la comunicación

La entidad posee diversos tipos de VLAN para cada servicio que se encuentran distribuidas en servidores, red LAN, administración de dispositivos de red, de seguridad, telefonía voz IP, Internet y MPLS con el fin de independizar y categorizar los servicios.

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

5.6 Ciframiento de los datos a través de la red

5.6.1 Cifrado de datos en tránsito

- ❖ Los datos que viajan a través de la MPLS van cifrados.
- ❖ Los servicios expuestos en Internet siempre deberán contar con un certificado SSL para garantizar la protección de este. Adicionalmente, deberá configurarse el WAF para que sea protegido.

5.6.2 Cifrado de datos en reposo

Para acceder a la información de las bases de datos que soportan en las aplicaciones, se debe contar con una autenticación que cumpla con los lineamientos mínimos de complejidad de contraseña. Para el caso de la información que se comparte con entidades externas se usa el acceso FTP mediante el cual las entidades deben acceder igualmente, con un usuario y contraseña.

5.6.3 Doble factor de autenticación

Se requiere que todas las aplicaciones de la Agencia posean como mínimo el doble factor de autenticación para garantizar la autenticidad del usuario que está realizando el acceso a los servicios expuestos en la red y así evitar el robo o pérdida de la información de valor para la entidad. Para este caso, los aplicativos de apoyo, como Orfeo y KLIC ya cuentan con un segundo factor de autenticación.

5.7 Protocolos autorizados

La Agencia Nacional de Tierras en pro de la seguridad de la información ha establecido los siguientes protocolos para la administración, configuración de dispositivos de red y aplicaciones e intercambio de información:


	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021


Tabla 2. Protocolos Autorizados ANT

Fuente: Equipo de Infraestructura y Soporte Tecnológico

Nombre del protocolo	Descripción
SSH Versión 2 o superior	Se utiliza para el ingreso y administración de dispositivos de red y seguridad por comando de línea (CLI)
HTTPS	Se utiliza para el ingreso y administración de dispositivos de red y seguridad por interfaz gráfica (GUI)
FTP	Protocolo de transferencia de archivos entre los diversos sistemas conectados a la red de la ANT.
SNMP Versión 2 o superior	Protocolo simple de administración para facilitar el intercambio de información de alarmas
NTP	Permite la sincronización del reloj de los dispositivos en la zona horaria.
IPSEC	Permite la conexión con entidades externas a través de un túnel seguro.
SMB Versión 3 o superior	Permite la conexión a las carpetas compartidas
RDP	Se utiliza para la conexión a escritorios remotos

6. REVISIÓN Y CUMPLIMIENTO

- ❖ Esta política será revisada una vez al año o cuando se considere necesario para asegurar su aplicabilidad, eficacia y efectividad. Igualmente será actualizada en cualquier momento y en caso requerido. Adicionalmente,
- ❖ EL Equipo de Infraestructura y Soporte Tecnológico de la Secretaría General, realizarán revisiones periódicas y aleatorias para verificar la implementación y aplicación de estos lineamientos y deberán realizar ajustes a los dispositivos de red en caso que sea necesario resguardando la integridad, confidencialidad y disponibilidad de la información que se encuentre respaldada por los dispositivos siguiendo las recomendaciones establecidas en el procedimiento de cambios tecnológicos de la entidad.

	POLÍTICA	POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED	CÓDIGO	GINFO-Política-019
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTIÓN DE LA INFORMACIÓN	FECHA	26/11/2021

HISTORIAL DE CAMBIOS		
Fecha	Versión	Descripción
26/11/2021	01	Primera versión del documento.

Elaboró: Alexandra Ruiz Bedoya	Revisó: Fabián Augusto Patarroyo Morales	Aprobó: Raul Alberto Badillo Espitia
Cargo: Contratista - Secretaría General	Cargo: Contratista - Secretaría General	Cargo: Secretario General
Firma: ORIGINAL FIRMADO	Firma: ORIGINAL FIRMADO	Firma: ORIGINAL FIRMADO