POLÍTICA PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE RED

SECRETARÍA GENERAL
EQUIPO DE INFRAESTRUCTURA Y SOPORTE TECNOLOGICO

ABRIL 2025

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.

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.

NORMATIVIDAD

- 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.
- 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.

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 autentificación 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 enviar 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 de red que permite gestionar las identidades (usuarios, equipos y recursos de red). Facilitando la autenticación de usuarios 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.

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.

[1] *Ley 712 de 2014*

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 que permite a un usuario acceder de manera remota al escritorio de un equipo informático.

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 herramienta 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,

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. 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).

EIST: Equipo de Infraestructura y Soporte Tecnológico.

1. DESCRIPCIÓN

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, recepción y almacenamiento de esta.

1.1. Generalidades

- Los dispositivos, protocolos y servicios de red que sean instalados y utilizados en las sedes de la entidad, en centros de datos y servicios de nube, y que hagan parte de la infraestructura de red de la agencia, deben ser configurados, asegurados y monitoreados siguiendo las buenas prácticas del fabricante o la industria, con el fin de mitigar la posibilidad de explotación de vulnerabilidades conocidas de estos o debidas a prácticas deficientes de configuración.
- Los dispositivos de red deben mantener vigente durante el tiempo que estén en servicio, la garantía y soporte del fabricante o distribuidor autorizado.
- El acceso de visitantes a la red de la ANT se realizará a través de una red wifi para invitados, con acceso exclusivo a Internet y sin conexión a ningún segmento de red en producción. Su habilitación y permisos se otorgarán únicamente en las sedes que determine la jefatura del Equipo de Infraestructura y Soporte Tecnológico.
- 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 red prevista para tal fin, sin embargo, al ser computadores personales, la entidad no será responsable por el software ni hardware del dispositivo personal, su licenciamiento o su uso, dicha responsabilidad quedará a cargo del usuario y/o propietario del dispositivo.
- La red de la entidad debe segmentarse de forma que se propenda por su buen rendimiento, seguridad y se cumplan las prácticas aceptadas y vigentes de la industria.
- El acceso a la infraestructura y servicios de red de la entidad sea por medio inalámbrico, cableado, o remoto con VPN.
- Se controlará el acceso a la red, Internet, contenido multimedia, redes sociales entre otros, de acuerdo con el perfil, funciones u obligaciones del funcionario, contratista o colaborador.
- Se propenderá, si el dispositivo lo permite, que la autenticación para el acceso a la gestión de la **infraestructura tecnológica institucional** (servidores, aplicaciones y dispositivos de red) se realice mediante la consulta a la base de datos centralizada en el Directorio Activo o equivalente, sin embargo, en todos los casos se debe contar con cuentas de autenticación locales y mecanismos de contingencia para que en caso de que la comunicación entre el dispositivo y el servidor de autenticación falle, sea válida la autenticación con las cuentas locales.

- Las contraseñas de gestión de los dispositivos y servicios TI de la entidad deben ser gestionadas por el equipo de infraestructura y Soporte Tecnológico o a quien esta delegue.
- La creación de cuentas en sitios del fabricante asociadas a la prestación de servicios, garantías, soporte técnico entre otros, debe ser realizada utilizando la cuenta de correo electrónico del Equipo de Infraestructura y Soporte Tecnológico creada para tal fin y en todos los casos se deberá incluir la cuenta de la jefatura del equipo y las que este autorice.
- El tiempo de bloqueo para las conexiones a las redes VPN por inactividad es de 1 hora.
- Todas las conexiones exitosas o fallidas para la gestión remota de dispositivos de red deben estar monitoreadas.
- Se deben mantener actualizados los dispositivos de red, de acuerdo con las últimas versiones liberadas por el fabricante.
- 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, equipos, servidores en la CMDB.

1.2. Ciclo de vida de la red

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

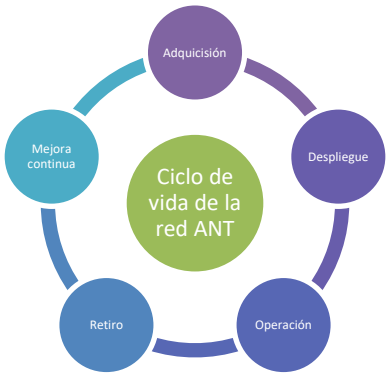


Ilustración 1. Modelo básico para el ciclo de vida de la red ANT
Fuente: Equipo de Infraestructura y Soporte Tecnológico

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

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

1.2.1. 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 realizará un estudio técnico en el cual se definirán 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.

1.2.2. Fase de despliegue

En esta fase se debe 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 la 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.

1.2.3. 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.

1.2.4. 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 la 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.

1.2.5. Fase de mejora continua

La infraestructura tecnológica (hardware y software) deberá contar con las actualizaciones de sistema operativo y 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.

1.3. Controles de seguridad de la red

1.3.1. Control de acceso

Los funcionarios, contratistas o partes interesadas de la ANT podrán 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

1.3.2. Autenticación

Todo 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 acceder a la red VPN, los usuarios deben autenticarse y ser miembros de 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.

Por otro lado, se establecen los siguientes criterios de autenticación, los cuales deberán ser cumplidos. Estos criterios aplican a los servicios integrados con el Directorio Activo.

- Solo se mantendrá activa una (1) sesión por usuario y dispositivo.
- Máximo 5 intentos erróneos para el bloqueo de la clave. Después se activará 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 las claves estas deben cumplir con los lineamientos y las características mínimas exigidas que se encuentran establecidas en la política de seguridad de la información. **INTI-Política-008 LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN V4.pdf**
- Para el caso de los usuarios locales de los servidores o dispositivos de red, se debe asignar manualmente una contraseña que cumpla con los mismos requisitos de complejidad stablecidas en la

política de seguridad de la información **INTI-Política-008 LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN V4.pdf**.

- Las contraseñas de las aplicaciones y dispositivos de red deben estar cifradas.

1.4. Seguridad de la red

Los dispositivos de seguridad de la red son de administración del Equipo de Infraestructura y Soporte Tecnológico adscrito a la Secretaría General y del equipo de seguridad de la información de la SSIT, 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.

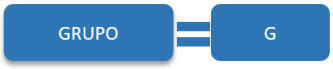
Para el acceso a los servicios VPN de la ANT está definido en, estos grupos delimitan el acceso a los segmentos de red, de tal manera que se garantiza que cada usuario ingrese solamente a los servicios que requiere para operar. Los administradores del Equipo de Infraestructura y Soporte Tecnológico deberán gestionar estos accesos

El acceso a los servicios VPN de la ANT se otorga con base en criterios de rol y necesidad de uso, asegurando que cada usuario disponga únicamente de los recursos indispensables para el cumplimiento de sus funciones. Los permisos son gestionados por el Equipo de Infraestructura y Soporte Tecnológico y se asignan de manera diferenciada, de modo que algunos usuarios cuenten con privilegios administrativos sobre redes y servidores, mientras que otros disponen de accesos operativos para escritorios remotos, carpetas compartidas u otros servicios autorizados. Asimismo, se contempla la habilitación de accesos específicos para labores de desarrollo de aplicaciones, así como la posibilidad de otorgar, bajo condiciones controladas, conectividad restringida a terceros o proveedores que lo requieran en el marco de sus obligaciones contractuales.

1.4.1. Nombramiento de 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.

1.4.2. 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 tienen acceso a buscadores, páginas del gobierno, servicios de WhatsApp, soluciones de colaboración como videoconferencia.
   Nota: Para el perfil Básico está restringido el contenido para adultos, armas, juegos, YouTube, redes sociales y descargas entre otros.

3. Grupo de Navegación Soporte: este grupo es de uso exclusivo para el Equipo de Infraestructura y Soporte Tecnológico, tiene permisos completos de navegación, con el objetivo de 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.

1.4.2.1 Nombramiento grupos de navegación en Internet

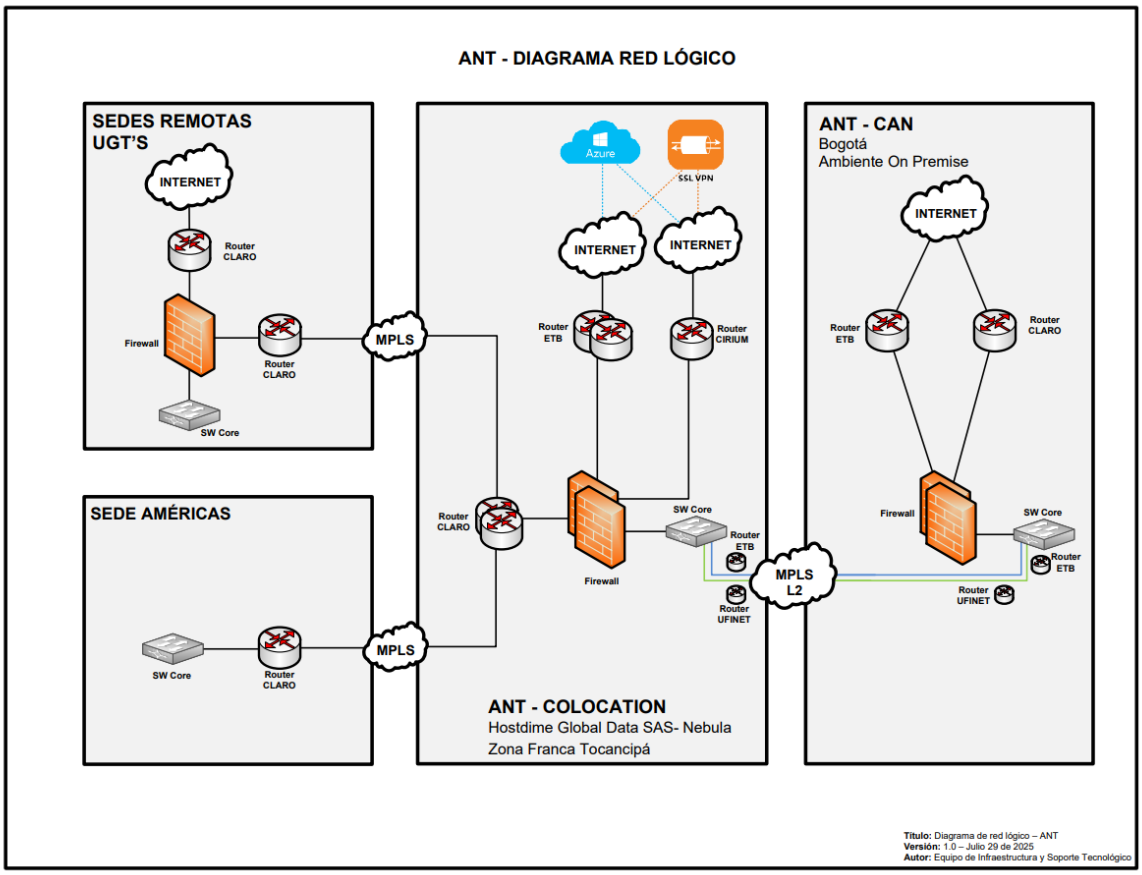
La estructura para la creación de nuevos grupos de navegación para Internet debe seguir el siguiente nombramiento:

- 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 "_"
- La palabra final debe estar relacionada al tipo de grupo de usuarios que almacenará.

1.4.3 Topología de la red y servicios

A continuación, se presenta la topología de los servicios de conectividad la cual debe actualizarse si este llegará a presentar algún cambio:

Ilustración 2. Diagrama de red lógico servicios de Internet y MPLS



Fuente: Equipo de Infraestructura y Soporte Tecnológico

1.4.4. Monitoreo de los dispositivos de red y seguridad

La entidad cuenta con herramientas enfocadas 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.

1.4.5. Herramientas para asegurar la red

Con el objetivo 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.

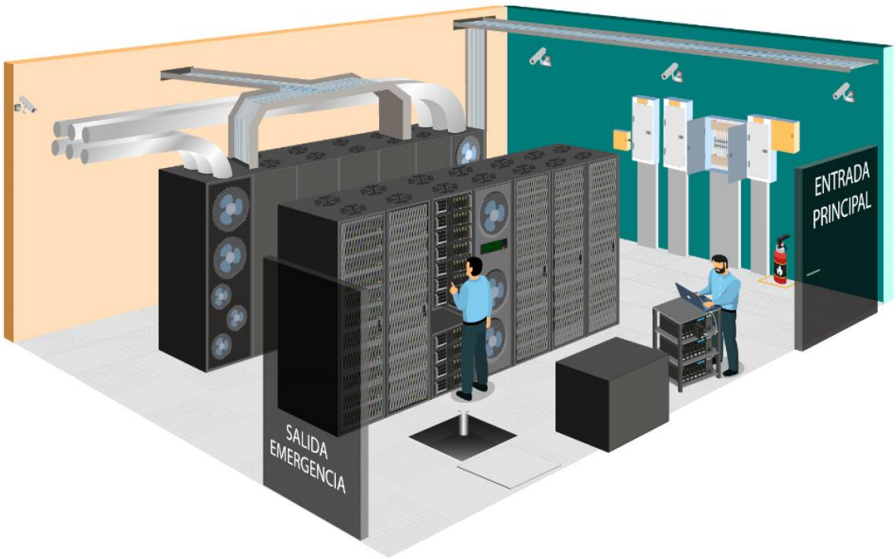
En la siguiente tabla se detallan los tipos de dispositivos que posee la entidad:

Tabla 1. Tipos de Dispositivos de Red – ANT

Dispositivo	Tipo de dispositivo
Dispositivos de red	Switches
	Router
	APs
Dispositivos de seguridad	Balanceadores
	Siem
	Analyzer
	Firewall
	Sandbox
	WAF
	DDoS
Dispositivos de infraestructura	Servidores
	Almacenamiento

Fuente: Equipo de Infraestructura y Soporte Tecnológico

Ilustración. Diseño físico del Datacenter



Fuente: Equipo de Infraestructura y Soporte Tecnológico

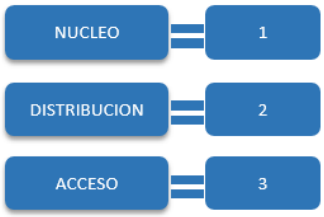
1.4.6 Nombramiento de equipos de red

Se estableció la siguiente política de nombrado de dispositivos de red y seguridad para estandarizar la nomenclatura de los elementos de Configuración (CI) de la red. Está conformada por una capa de red y seguridad, nombre del fabricante, demarcación de la ubicación física del dispositivo y un id consecutivo.

1.4.6.1 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:

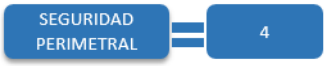
- **Categorización de la red:**



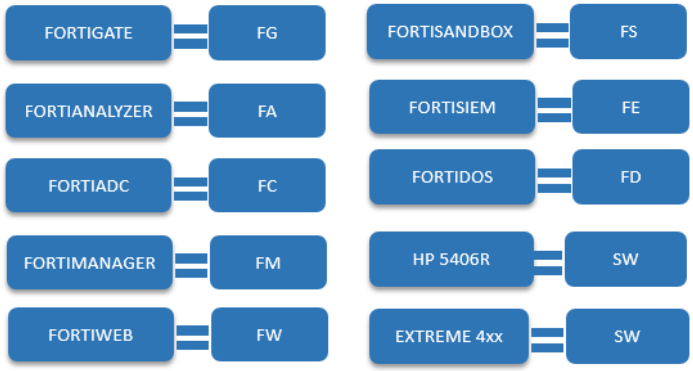
Cada uno de estos elementos (núcleo, distribución y acceso) cumplen la función principal de la red y soporta todo el tráfico de la entidad.

- **Seguridad:**

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



1.4.6.2 Nombramiento de dispositivos según el fabricante



1.4.7 Nombramiento de dispositivos según la Sede

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
- **Orden**: 2 dígitos numéricos de acuerdo con el consecutivo de nombramiento del dispositivo.

Ejemplo:

CUN_BOG_CAN_FFG401

CUN_BOG_CAN_FFG402

1.4.8 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 dígito 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

1.4.9 Nombramiento de los puertos

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

1.4.9.1 Según sus conexiones

MPLS	MP	SERVIDOR	SV
INTERCONEXION	IC	LAN	LA
INTERNET	IN	WAN	WA
GESTION	GT	VLAN	VL

1.4.9.2 Según su tipo de puerto

Puerto eléctrico	UTP
Puerto óptico	FO

1.4.9.3 Según su capacidad

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

1.4.9.4 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>

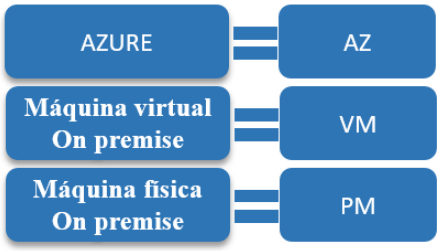
Ejemplo: este ejemplo detalla el nombramiento de puertos tomando el firewall asignado al puerto 4.

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.

1.4.10 Nombramiento de servidores

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

1.5 Seguridad de la comunicación

La entidad posee segmentación por VLAN para cada servicio distribuidos en servidores, red LAN, administración de dispositivos de red, de seguridad, telefonía voz IP, Internet y MPLS para independizar y clasificar los servicios.

1.6 Cifrado de los datos a través de la red

1.6.1 Cifrado de datos en tránsito

- ❖ 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.

1.6.2 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 la información compartida con entidades externas se usa el acceso FTP, con el que las entidades deben acceder igualmente, con un usuario y contraseña.

1.6.3 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.

1.7 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:

Tabla 2. Protocolos Autorizados ANT

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)
SFTP	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

Fuente: Equipo de Infraestructura y Soporte Tecnológico

REVISIÓN Y CUMPLIMIENTO

Esta política se revisará anualmente o cuando se considere necesario para asegurar su aplicabilidad, eficacia y efectividad. Se actualizará 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.

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
26/11/2021	1	Primera versión del documento.
15/08/2025	2	Segunda versión del documento
08/05/2026	3	Se actualiza contenido y lineamientos acordes al estado actual de la entidad, cambia formato y se actualiza versión.

APROBACIÓN				
	NOMBRE	**CARGO**	**FIRMA**	**FECHA**
ELABORÓ	Carlos Julián Calvete	Contratista – Subdirección de Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	10/12/2025
REVISÓ	Roberto Andrés Zabala Barrera	Contratista – Secretaría General	**ORIGINAL FIRMADO**	23/12/2025
APROBÓ	Angela Lorena Ortiz Rosero	Secretaría general	**ORIGINAL FIRMADO**	08/05/2026