1. JUSTIFICACIÓN

Los grandes volúmenes de información institucionales se originan desde diversas fuentes y con estándares tecnológicos heterogéneos en hardware, software, comunicaciones que requieren de una infraestructura de red adecuada, funcional y confiable para su transmisión y almacenamiento.

En el caso de la Agencia Nacional de Seguridad Vial, las soluciones de conectividad y servicios informáticos fueron diseñadas fundamentalmente para soportar aplicaciones de procesamiento de datos que funcionan en un servicio de transporte operativo pero que no han sido rigurosas en parámetros de QoS (calidad del servicio) y CyberSec (ciberseguridad).

El crecimiento que plantea la entidad en cuanto a nuevos servicios y aplicaciones para los cuales no se ha realizado una planeación adecuada puede desencadenar en dificultades en la operación de la red y en la gestión de la seguridad de la información, elementos que han estado en una baja y arriesgada prioridad en el dimensionamiento tecnológico institucional.

En el marco de las TI se hace necesaria la implementación de estrategias de seguridad para preservar los servicios disponibles y garantizar la confidencialidad e integridad de los datos en las aplicaciones.

Existen algunos estándares de seguridad informática que sugieren como primera medida realizar análisis de vulnerabilidades para responder corrigiendo posibles fallos y apuntando a modelos preventivos. Estos esfuerzos son inocuos, si en este mismo sentido, la alta dirección no está involucrada y comprometida con la implementación de un Sistema Integral de la Seguridad de la Información.

El presente documento pretende exponer una serie de lineamientos para implementar las mejores prácticas de Seguridad Informática en la Agencia Nacional de Seguridad Vial, con el fin de optimizar la disponibilidad, la integridad, la confidencialidad/privacidad, entre otros principios relevantes, teniendo en cuenta la infraestructura y limitaciones actuales.

Por otro lado, la Agencia Nacional de Seguridad Vial cuenta con lineamientos y políticas que mantienen la seguridad y privacidad de la información; de igual forma parte del presente documento es el cronograma de implementación del Sistema de Gestión y Seguridad de la Información que está planteado para las vigencias 2018 y 2019.

2. SEGURIDAD PERIMETRAL

En la Agencia Nacional de Seguridad Vial se encuentra implementada una solución que no cumple con las condiciones de alta disponibilidad de un Firewall que contribuya a la seguridad perimetral de los datos, aplicaciones, servicios, servidores y usuarios finales. La solución de Checkpoint fue configurada para controlar el tráfico unidireccional entre la red de la Agencia Nacional de Seguridad Vial e internet, además de evitar que los usuarios de Internet no

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

La movilidad es de todos Mintransporte

autorizados tengan acceso a redes privadas conectadas a internet, bloqueando aquellos que no cumplen los criterios de seguridad especificados.
El dispositivo encargado de esta tarea en la Agencia Nacional de Seguridad Vial es un Firewall de referencia Checkpoint 3000, con características de firewall, IPS (Sistemas de Prevención de Intrusos), Antivirus, AntiSpam, VPN, Filtrado Web y control de Aplicaciones. Adicionalmente se cuenta con un Sistema SmartConsole para el análisis de tráfico y la generación de reportes. El análisis de estos reportes lleva a la detección de fallas de seguridad e intrusiones frustradas, además de otros servicios de subscripción que proveen conexión y actualización a las bases de datos propietarias para Antivirus, Prevención de Intrusiones, Filtrado Web, Antispam y Control de aplicaciones.

En capa lógica, se cuenta con segmentación de dominios de broadcast a través de VLANs conectadas a los diferentes puertos del Firewall, procurando controlar el tráfico de cada subred de acuerdo al rol de grupos de usuarios/máquinas: Equipos activos, contratistas, oficinas y Wireless.

Para la conectividad WAN la Agencia tiene un canal dedicado de 128Mb, segmentado para cada grupo de acceso a la red, contratado con ETB (Empresa de Telefonía de Bogotá) y vinculados a un enrutador Cisco que realiza la conmutación de forma transparente de acuerdo con el destino del paquete enviado, si se trata de una petición hacía cada uno de los sitios de la red, la navegación se realiza a través del canal nombrado a las necesidades actuales de la Agencia, se hace necesario aplicar traffic shapers a las políticas de navegación de las redes, así como filtros web y controles de aplicaciones para cada VLAN, con el fin de optimizar la seguridad y el uso del canal.

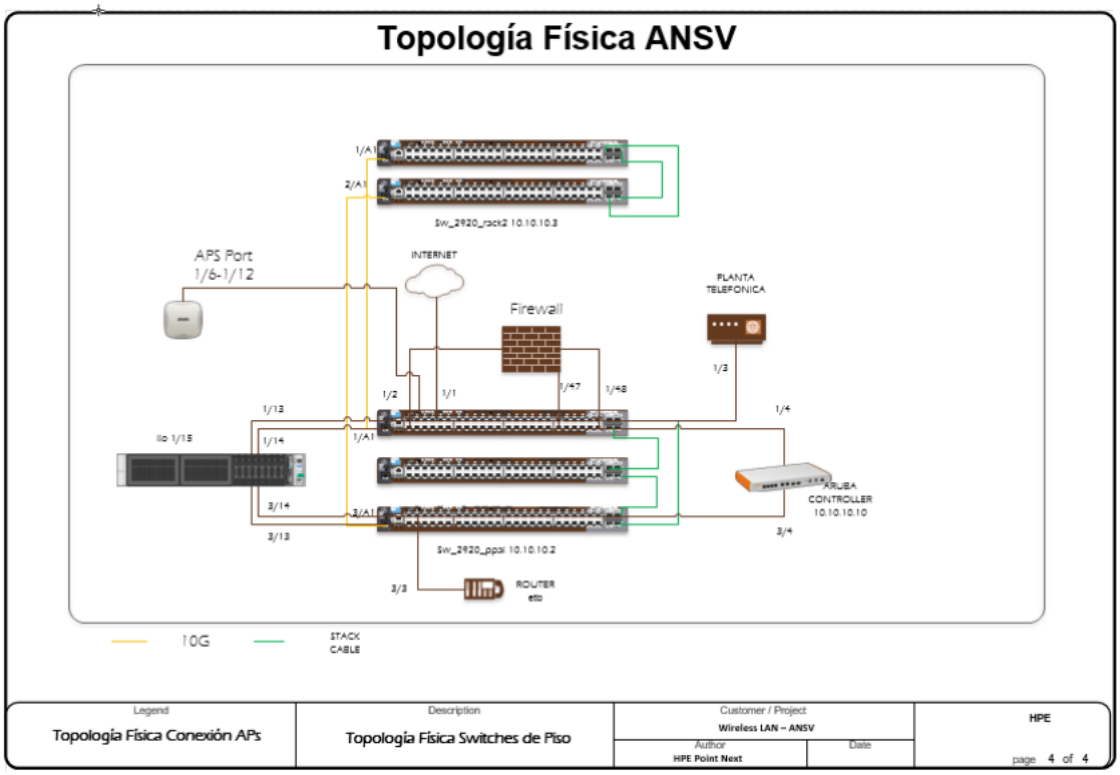
De igual forma se requiere adquirir un nuevo dispositivo de seguridad, con el fin de permitir la alta disponibilidad y la comunicación bidireccional en la seguridad de la información de la entidad.

3. RED

La red LAN de la Agencia Nacional de Seguridad Vial cuenta con un switch de Núcleo 3Com, donde convergen las conexiones de los servidores, los switches de distribución de las dos alas y el equipo de seguridad perimetral, formando una topología simple extendida con centro en el switch de núcleo, adicionalmente operan varias VLANs que segmentan la red a nivel lógico.

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

La movilidad es de todos Mintransporte



De la mano de cualquier adquisición o mejora a nivel técnico, es importante implementar políticas en el manejo de los recursos tecnológicos, para brindar apoyo y orientación a los funcionarios, contratistas y demás colaboradores con respecto a la seguridad de la información, acorde a las necesidades y requisitos de la entidad.

4. TRANSICIÓN DE IPV4 A IPV6

Se debe establecer un plan para hacer la transición de las direcciones IPv4 existente actualmente por la IPv6 debido a que la totalidad de los equipos informáticos de la Entidad soportan la nueva versión de IP; por tal razón en la vigencia actual es indispensable determinar los requerimientos para llevar a cabo dicha implementación.

5. SERVIDORES

Bajo la administración de la oficina de Gestión TIC existe 1 enclosure, servidor de almacenamiento. En el servidor mediante la herramienta Hyper-V de Microsoft se encuentran implementadas diferentes máquinas virtuales donde se alojan bases de datos y aplicaciones tales como Gestión Documental y el Sistema de Mesa de Servicios; de igual forma en el mismo servidor se encuentran hospedadas un total de 7 máquinas virtuales, con sistemas operativos Windows y Linux. Estas máquinas incluyen los entornos de producción y pruebas de los

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

La movilidad es de todos Mintransporte

sistemas de información institucionales, los controladores de dominio y toda la configuración del Directorio Activo.
No obstante, y de acuerdo con lo anterior se hace indispensable adquirir nuevos servidores físicos con el fin de separar los aplicativos de la entidad y mantener un plan de contingencia ante desastres con nuevo hardware.

6. APLICACIONES Y BASES DE DATOS

El análisis de aplicaciones conectadas es primordial para poder establecer posibles fallos de implementación que conducen a vulnerabilidades en cualquiera de las capas de las arquitecturas desplegadas. Los puntos de control más relevantes que se verificarán estarán concentrados en: validar desbordamientos de pilas, verificación de cadenas y secuencias inválidas, datos inconsistentes de control, inspección de Metadatos que conducen a fugas de información, errores de validación, errores de procesamiento, entre otros.

Las bases de datos manejadas actualmente por la entidad están instaladas en un servidor físico Dell PowerEdge T610 de bajo rendimiento, en este momento tienen alojadas: Bases de datos de lesionados y siniestrados y las copias de seguridad diarias de las mismas.

En la actualidad no existen en la entidad aplicaciones desarrolladas y contratadas que tengan vínculos con algún gestor de bases de datos relacional y/o servidores de despliegue donde sea inminente generar un estudio de seguridad multicapa para identificar riesgos potenciales; hechos que al momento de adquirir o desarrollar sistemas de información con características específicas requerirán además de lo anterior contemplar otras actividades como: documentación de estadísticas de rendimiento, incluyendo los posibles cambios de configuración y sincronización que esto conlleva y realizar afinamientos periódicos con su correspondiente documentación, para un rendimiento óptimo de la base de datos.

7. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
2019-01-31	Documento Original. Primera versión	00

8. CONTROL DE FIRMAS

Elaboró
Firma

Angela Riveros Sierra
Profesional Especializado TICS

Aprobó
Firma

Juana Caycedo Gutiérrez
Secretaria General (E)

Revisó: Eder Carrascal Cuadrado – Profesional Especializado Oficina Asesora de Planeación

Av. La Esperanza calle 24 No. 62 – 49
Complejo Empresarial - Estación 2 Piso 9
PBX 739 9080 - www.ansv.gov.co - @ansvcol

La movilidad es de todos Mintransporte