MINISTERIO DE TRANSPORTE

MEMORANDO
20231510056553
02-06-2023

Bogotá D.C.

PARA: *Clara Elizabeth Ramírez, Coordinadora – Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones* (E)

DE: Luz Stella Conde Romero – Jefe Oficina de Control Interno

ASUNTO: Informe definitivo Proceso Gestión de Tecnologías de la Información y las comunicaciones TIC´S – Seguimiento Ejecución Contratos

En cumplimiento al plan de acción de esta Oficina, me permito presentarle el informe de Auditoría realizada por el funcionario Wilson Gonzalez Tapias al proceso Gestión de Tecnologías de la Información y las comunicaciones TIC´S – Seguimiento Ejecución Contratos

Producto de la auditoría efectuada, anexo el informe que contiene observación sobre las cuales le solicitamos describir en el cuadro "RESUMEN DE OBSERVACIONES" las acciones, responsables y fechas de cumplimiento tendientes a subsanarlas.

Igualmente le comunico que dando cumplimiento al Decreto 338 de 2019, este informe será puesto en conocimiento del señor Ministro, como destinatario principal.

Por lo anterior, le solicito que en un término máximo de diez (10) días calendario, contados a partir de la fecha de recibo de este informe, enviar su respuesta y el cuadro debidamente diligenciado, de conformidad con la circular 20163000041133 del 09/03/2016.

Cordialmente,

LUZ STELLA CONDE ROMERO
Jefe de Oficina Control Interno

Anexo: Informe de Auditoria

Elaboró: Wilson Gonzalez T
Revisó: Luz Stella conde Romero

MEMORANDO

20231510056553

02-06-2023

OFICINA DE CONTROL INTERNO
INFORME DE AUDITORÍA
GRUPO TIC´S

Dependencia y/o Grupo auditado: *Gestión de Tecnologías de la Información y las comunicaciones TIC´S –*	***Dependencia Jerárquica:*** ***Despacho ministro***
Responsable del Proceso: *Dra. Clara Elizabeth Ramirez, Coordinadora – Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones*	***Auditoría realizada por:*** *Wilson Gonzalez Tapias – Profesional especializado*
Motivo de la auditoría: ***Plan de acción 2023***	
Inicio de la auditoría: *01/03/2023*	***Terminación de la auditoría:*** *28/05/2023*

Introducción.

La Oficina de Control Interno, en ejercicio de las facultades otorgadas por la Ley 87 de 1993 y modificada por la Ley 1474 de 2011 y demás modificaciones, tiene como función realizar la evaluación independiente al sistema de Control Interno, así como a las actividades y actuaciones de la administración, entre otros, con el fin de determinar la efectividad del control interno, el cumplimiento de la gestión institucional y los objetivos del ministerio, realizando recomendaciones para asesorar al Representante legal en busca del mejoramiento continuo del sistema de control interno.
De acuerdo a lo anterior y dada la importancia establecida en los Decretos 2060 de 2015 que adiciona el Decreto 1079 de 2015 y reglamenta los Sistemas Inteligentes para la Infraestructura, el Tránsito y el Transporte (SIT), y dado que el Ministerio de Transporte, es el ente rector de los Sistemas Inteligentes para la Infraestructura, el Tránsito y el Transporte (SIT), y que realizará todas las gestiones necesarias para la creación, implementación y funcionamiento del Sistema Inteligente Nacional para la Infraestructura, el Tránsito y el Transporte – SINITT, contratos de sistema de gestión de seguridad de la información sus vulnerabilidades y recomendaciones, adquisición de hardware y software entre otros, la Oficina de Control Interno por muestreo efectuara análisis y seguimiento de las actividades de contratación que se realicen frente al cumplimiento de la norma y efectividad del objeto contratado año 2022 a la fecha.

1. *Objetivo de la auditoría.*

Verificación y análisis de la documentación y del producto esperado, los reglamentos técnicos, estándares, protocolos y uso de la tecnología en los proyectos de SIT y demás contratos de seguridad y desarrollos adquiridos

2. *Alcance.*

Análisis y seguimiento ejecución de CONTRATOS ejecutados por el Grupo Tic´s en el periodo 2021 a la fecha

3. *Metodología.*

La auditoría se desarrolló tomando como referencia la normatividad vigente establecida en el Decreto 2060 de 2015 que adiciona el Decreto 1079 de 2015 y reglamenta los Sistemas Inteligentes para la Infraestructura, el Tránsito y el Transporte (SIT), artículo 84 de la Ley 1450 de 201, Decreto 2482 de 2012 por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión, entre otros, un análisis de las acciones ejecutadas y acciones por ejecutar la cual debe desarrollarse conforme a los principios que rigen la función y los procedimientos administrativos consagrados en los artículos 209 de la Constitución Política, la Ley 489 de 1998, la Ley 1437 de 2011, así como la información entregada a través de OneDrive y enlaces para consulta de la información.

4. *Análisis de Contratos:*

A continuación, presentamos el análisis de la información de los contratos:

4.1.5 ***CONTRATO 690 DE 2022.*** *Una vez realizada la inversión en los contratos 517 del 2021 por valor de $1.234.410.000, Contrato 506 de 2021 por valor de $ 658.299.226, Contrato 507 de 2021 por valor de $154.987.000, Contrato 508 de 2021 por valor de 168.200.000 y 630, 631, 632, 633, 637 por valor de $2.743.640.649 denominados RENOVACIÓN Y ADQUISICIÓN DE SOLUCIONES TECNOLÓGICAS A NIVEL DE INFRAESTRUCTURA, SEGURIDAD Y BASES DE DATOS PARA EL MINISTERIO DE TRANSPORTE y con el propósito de definir y validar los niveles de exposición en que se encuentra en la plataforma tecnológica de Ministerio de Transporte, frente a posibles ataques y/o accesos no autorizados por parte de delincuentes informáticos, se adelantó el contrato 690/2022 por lo cual los resultados de este contrato fueron tomados como base por la Oficina de Control Interno para determinar la eficacia de las herramientas objeto de los contratos de aseguramiento previamente suscritos y ejecutados por el ministerio.*

4.1 CONTRATO 690 DE 2022. ADQUISICIÓN DE SERVICIOS DE ETHICAL HACKING PARA LA REMEDIACIÓN DE VULNERABILIDADES Y SOPORTE PARA LA GESTIÓN DE INCIDENTES DEL MINISTERIO DE TRANSPORTE por valor de $ 153.314.268.

Observaciones y Recomendaciones

La Oficina de Control interno de este Ministerio con el fin de evaluar la efectividad de los contratos de aseguramiento para la información, bases de datos y demás sistemas en los cuales se ha invertido valores significativos para evitar posibles vulnerabilidades y que permitirían el Intercambio seguro de información por medio de mecanismos de cifrado, monitoreo y verificación del flujo de información en las bases de datos de la entidad; la reducción de riesgos en las bases de datos, como el análisis de vulnerabilidades periódicos especializados en esta infraestructura; detectar posibles anomalías o incidentes en las bases de datos y tomó como base el resultado y diagnóstico obtenido por Ethical Hacking (Contrato 690/2022) cuyá finalidad consistió en verificar las vulnerabilidades existentes, para determinar y evaluar la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, verificar los niveles de exposición en que se encuentra la plataforma tecnológica de Ministerio de Transporte, frente a posibles ataques y/o accesos no autorizados por parte de delincuentes informáticos, entre otras; este contrato (690/2022) se suscribió y desarrolló de manera posterior a los contratos de aseguramiento analizados en la presente auditoría.

A continuación, presentamos los resultados del diagnóstico de contrato Ethical Hacking (Contrato 690/2022) y los comparamos con los objetos y finalidad de los contratos de aseguramiento suscritos y ejecutados con anterioridad.

Respecto a los contratos antes descritos nos permitimos presentar un análisis de los mismos vs el resultado del contrato_690 DE 2022. ADQUISICIÓN DE SERVICIOS DE ETHICAL HACKING PARA LA REMEDIACIÓN DE VULNERABILIDADES Y SOPORTE PARA LA GESTIÓN DE INCIDENTES DEL MINISTERIO DE TRANSPORTE, RESPUESTA TIC

Contrato/objeto	***Aspectos relevantes de las fichas técnicas***	***Aspectos encontrados por ethikal hacking (contrato 690 DE 2022).***	***Respuesta Grupo TIC al Borrador del informe preliminar***	***Observación Oficina de control interno***
517 del 2021 por valor de $1.234.410.000 *Objeto: Renovación y adquisición de soluciones tecnológicas a nivel de infraestructura para el fortalecimiento de la seguridad y bases de datos, bajo el marco de las tecnologías de la información y las comunicaciones y sus servicios its del ministerio de transporte.*	*En el **lote1**: indicaba \... "RENOVACIÓN DE LICENCIAMIENTO SOPORTE Y ACTUALIZACIÓN PARA LOS EQUIPOS DE SEGURIDAD PERIMETRAL FORTINET".* *-Software de seguridad y protección* *-Equipo de seguridad de red* *-Equipo de servicio de red.* *Reducción de riesgos solo permitiendo conexiones seguras, así como otras incidencias técnicas. Disponiendo una infraestructura actualizada que requiera un mínimo mantenimiento, lo que permite tener un sistema mucho más seguro.* *Indica en el **lote 3**. \... Esta solución ha permitido incrementar la seguridad tanto de la infraestructura de servidores, como proteger a los equipos de usuario final. Por este motivo, se requiere realizar la renovación de la garantía y licenciamiento de la solución ajustando algunas cantidades en el licenciamiento para aumentar la protección en activos considerados como críticos para la entidad y donde*	*Se adelantaron pruebas de Pruebas de caja negra y Externo, Prueba CGI SQL Injection, Repositorio GIT Abierto, Directorios Navegables, TLS 1.0 Detectado (Transport Layer Security, seguridad de la capa de transporte),* *vulnerabilidades en la seguridad de la información y de la red, El Protocolo ssl para navegadores web y servidores que permite la autenticación, encriptación y desencriptación de datos enviados a través de Internet pueden verse afectados entre otros resultados del análisis – ver informe de **ethikal hacking.***	*El licenciamiento del soporte de estos equipos de seguridad perimetral (Fortinet) finaliza en mayo de 2020, dejando así de recibir actualizaciones por parte del fabricante lo que ocasionaría vulnerabilidades en la seguridad de la información. En consecuencia, se requiere contratar la renovación del licenciamiento por un año para los equipos de seguridad perimetral mencionados anteriormente y que se encuentran operando en conjunto con la red de datos del ministerio de Transporte.*	*Teniendo en cuenta los aspectos relevantes de las fichas técnicas establecidas en los estudios previos de los contratos, podemos indicar que las renovaciones contratadas de los servicios de seguridad frente al resultado del contrato 690 de 2022, se indica que se encontraron múltiples debilidades de riesgo críticas, alto, medio, y bajo que son necesarios tener en cuenta para evitar posibles situaciones que puedan ocasionar daños, perdida de información y 7 o destrucción de esta.* *Se puede deducir con el resultado de las pruebas que en los riesgos críticos y alto al realizar las pruebas de caja Negra externas y en las pruebas de caja gris y blanca las conexiones no son seguras, no obstante, lo adquirido a través del contrato 517/2021.*

	deberán enfocarse mayores esfuerzos en la protección. *\...Mantener la protección contra malware debidamente actualizada, ya que una solución de seguridad sin actualización aumentará la probabilidad de sufrir ataques cibernéticos recientemente desarrollados. c) Monitoreo de los sistemas de información. La solución de seguridad permite verificar posibles amenazas detectadas con el objetivo de actuar rápidamente en caso de algún evento o incidente de seguridad.* ***Lote 4***.\ *Reducción de riesgos solo permitiendo conexiones seguras, así como otras incidencias técnicas, disponiendo una infraestructura actualizada que requiera un mínimo mantenimiento, lo que permite tener un sistema mucho más seguro.* *Mitigar los riesgos de seguridad y vulnerabilidades de día cero en la red de datos, implantación de malware, saturación de anchos de banda WAN, ataques externos e internos que pudiesen dejar sin servicios de internet y sistemas de información del Ministerio de Transporte; de ataques de denegación de servicio y el acceso de archivos que pudiesen ejecutarse al interior de la red comprometiendo la integridad de la información;* *Mantener la protección contra malware debidamente actualizada, ya que una solución de seguridad sin actualización aumentará la*			

	probabilidad de sufrir ataques cibernéticos recientemente desarrollados. actualizaciones hacia nuevas versiones en los dispositivos de seguridad. *La solución de seguridad permite verificar posibles amenazas detectadas con el objetivo de actuar rápidamente en caso de algún evento o incidente de seguridad entre otros.*			
Contrato 506 de 2021. *Por valor de $ 658.299.226, cuyo objeto fue:* *RENOVACIÓN Y ADQUISICIÓN DE SOLUCIONES TECNOLÓGICAS A NIVEL DE INFRAESTRUCTURA PARA EL FORTALECIMIENTO DE LA SEGURIDAD Y BASES DE DATOS, BAJO EL MARCO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Y SUS SERVICIOS ITS DEL MINISTERIO DE TRANSPORTE.*	*En los estudios previos SE PRETENDIA SATISFACER CON LA CONTRATACIÓN:* *\... Reducción de riesgos solo permitiendo conexiones seguras.* *Para mitigar los riesgos de seguridad y vulnerabilidades de día cero en la red de datos, implantación de malware, saturación de anchos de banda WAN, ataques externos e internos que pudiesen dejar sin servicios de internet y sistemas de información del Ministerio de Transporte; de ataques de denegación de servicio y el acceso de archivos que pudiesen ejecutarse al interior de la red comprometiendo la integridad de la información;* *Mantener la protección contra malware debidamente actualizada, ya que una solución de seguridad sin actualización aumentará la probabilidad de sufrir ataques cibernéticos recientemente desarrollados.* *La solución de seguridad permitiría verificar posibles amenazas detectadas con el objetivo de actuar rápidamente en caso de algún evento o*	*Se identifica una alta cantidad de vulnerabilidades críticas en Apache Tomcat, PHP y Oracle que es de inmediata atención para evitar que un atacante informático pueda explotarlas.* *Se identifica una alta cantidad de vulnerabilidades de denegación de servicio, debido a la falta de actualización de parches sobre las diversas plataformas.* *ver informe de* ***ethikal hacking.***	*El grupo TIC indica en su respuesta \... que se evidencia una confusión y descontextualización, respecto a las renovaciones de dispositivos de seguridad y el ejercicio de Ethical Hacking.* *No obstante, lo anterior manifiestan \...Así mismo indican que En el sentido anterior y aclarando que un ethical no pretende indicar que la infraestructura de seguridad de una entidad no es apropiada o eficiente. Como se plasma en la observación del informe, la mayoría de las observaciones reflejadas en el informe, son causadas por obsolescencia tecnológica o falta de recursos para su remplazo.* *la observación a la que se hace referencia en el informe: "**podemos indicar que el resultado esperado con la contratación de aseguramiento relacionada en este informe no se alcanzó**; **el ministerio de transporte (en Apache Tomcat, PHP y Oracle)**,indican que " es demeritoria y poco coherente, con respecto a las vulnerabilidades establecidas, las cuales derivan de ámbitos de obsolescencia y por lo cual falta de parches, recursos para renovar sistemas de información que no pueden ser migrados y por lo cual se debe conservar las versiones de PHP y Tomcat (Se requiere personal especializado en desarrollo para migración de portales). así como, Oracle referente a una mala aplicación de parametrización sobre un servidor.*	*Teniendo en cuenta los aspectos relevantes de las fichas técnicas establecidas en los estudios previos de los contratos, podemos indicar que las renovaciones contratadas de los servicios de seguridad no se lograron; el resultado del contrato 690 de 2022, evidencia que no cubrió la necesidad contratada, como se puede apreciar se indica que se encontraron múltiples debilidades de riesgo críticas, alto, medio, y bajo que son necesarios tener en cuenta para evitar posibles situaciones que puedan ocasionar daños, perdida de información y /o destrucción de esta.* *Se puede deducir con el resultado de las pruebas que en los riesgos críticos y alto al realizar las pruebas de caja Negra externas y en las pruebas de caja gris y blanca las conexiones no son seguras.* *Se debe analizar los parches que ofrecen los sistemas contratados y mantenerlos actualizados.* *Se debe realizar un inventario de sistemas obsoletos y presentar un plan de renovación de los mismos; análisis que se debió de realizar antes de invertir los recursos del contrato 506 de 2021, cuyo objeto precisamente era el de renovación y adquisición de soluciones tecnológicas.*

	incidente de seguridad entre otros.		*Es de tener en cuenta que un ataque de día cero o una configuración incorrecta de seguridad de una aplicación, pueden o no ser mitigadas, ya que, al no estar descubiertas por nadie, los equipos de seguridad puede que no estén preparados para contenerlas, por eso también son importantes estos ejercicios, en el proceso de descubrir estas vulnerabilidades y poderlas compensar con las medidas existentes. O solicitar recursos a la alta dirección.*	
Contrato 507 de 2021 por valor de $154.987.000 *RENOVACIÓN Y ADQUISICIÓN DE SOLUCIONES TECNOLÓGICAS A NIVEL DE INFRAESTRUCTURA PARA EL FORTALECIMIENTO DE LA SEGURIDAD Y BASES DE DATOS, BAJO EL MARCO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Y SUS SERVICIOS ITS DEL MINISTERIO DE TRANSPORTE*	*Dentro de los estudios previos se pretendía:* *\...* *Reducción de riesgos solo permitiendo conexiones seguras, así como otras incidencias técnicas, disponiendo una infraestructura actualizada que requiera un mínimo mantenimiento, lo que permite tener un sistema mucho más seguro.* *Para mitigar los riesgos de seguridad y vulnerabilidades de día cero en la red de datos, implantación de malware, saturación de anchos de banda WAN, ataques externos e internos que pudiesen dejar sin servicios de internet y sistemas de información del Ministerio de Transporte; de ataques de denegación de servicio y el acceso de archivos que pudiesen ejecutarse al interior de la red comprometiendo la integridad de la información; es necesario contar con estos equipos operando adecuadamente.*	*Se identifica una alta cantidad vulnerabilidades críticas en Apache Tomcat, PHP y Oracle que es de inmediata atención para evitar que un atacante informático pueda explotarlas.* *Se identifica una alta cantidad de vulnerabilidades de denegación de servicio, debido a la falta de actualización de parches sobre las diversas plataformas.* *ver informe de* ***ethikal hacking.***	*No obstante, lo anterior manifiestan \...Así mismo indican que En el sentido anterior y aclarando que un ethical no pretende indicar que la infraestructura de seguridad de una entidad no es apropiada o eficiente. Como se plasma en la observación del informe, la mayoría de las observaciones reflejadas en el informe, son causadas por obsolescencia tecnológica o falta de recursos para su remplazo.* *la observación a la que se hace referencia en el informe: "****podemos indicar que el resultado esperado con la contratación de aseguramiento relacionada en este informe no se alcanzó****; el ministerio de transporte (en Apache Tomcat, PHP y Oracle),indica TIC que " es desmeritoria y poco coherente, con respecto a las vulnerabilidades establecidas, las cuales derivan de ámbitos de obsolescencia y por lo cual falta de parches, recursos para renovar sistemas de información que no pueden ser migrados y por lo cual se debe conservar las versiones de PHP y Tomcat (Se requiere personal especializado en desarrollo para migración de portales). así como, Oracle referente a una mala aplicación de parametrización sobre un servidor.* *Es de tener en cuenta que un ataque de día cero o una configuración incorrecta de seguridad de una aplicación, pueden o no ser mitigadas, ya que, al no estar*	*Teniendo en cuenta los aspectos relevantes de las fichas técnicas establecidas en los estudios previos de los contratos, podemos indicar que las renovaciones contratadas de los servicios de seguridad frente al resultado del contrato 690 de 2022, se indica que se encontraron múltiples debilidades de riesgo críticas, alto, medio, y bajo que son necesarios tener en cuenta para evitar posibles situaciones que puedan ocasionar daños, perdida de información y 7 o destrucción de esta.* *Se puede deducir con el resultado de las pruebas que en los riesgos críticos y alto al realizar las pruebas de caja Negra externas y en las pruebas de caja gris y blanca las conexiones no son seguras.* *Se debe analizar los parches que ofrecen los sistemas contratados y mantenerlos actualizados.* *Se debe realizar un inventario de sistemas obsoletos y presentar un plan de renovación de los mismos.* *Se debe realizar un inventario de sistemas obsoletos y presentar un plan de renovación de los mismos; análisis que se debió de realizar antes de invertir los recursos del contrato 506 de 2021, cuyo objeto precisamente era el de renovación y adquisición de soluciones tecnológicas.*

	Mantener la protección contra malware debidamente actualizada, ya que una solución de seguridad sin actualización aumentará la probabilidad de sufrir ataques cibernéticos recientemente desarrollados. *Monitoreo de los sistemas de información. La solución de seguridad permite verificar posibles amenazas detectadas con el objetivo de actuar rápidamente en caso de algún evento o incidente de seguridad.*		*descubiertas por nadie, los equipos de seguridad puede que no estén preparados para contenerlas, por eso también son importantes estos ejercicios, en el proceso de descubrir estas vulnerabilidades y poderlas compensar con las medidas existentes. O solicitar recursos a la alta dirección.*	
Contrato 508 de 2021 por valor de 168.200.000 *Renovación y adquisición de soluciones tecnológicas a nivel de infraestructura para el fortalecimiento de la seguridad y bases de datos, bajo el marco de las tecnologías de la información y las comunicaciones y sus servicios its del ministerio de transporte.* ***lote 1:*** *"renovación de licenciamiento soporte y actualización para los equipos de seguridad perimetral fortinet".*	*en las fichas técnicas se establecía:* ***lote 1****: "renovación de licenciamiento soporte y actualización para los equipos de seguridad perimetral fortinet".* *\... se requiere realizar la renovación de la garantía, licenciamiento y actualización de los equipos que soportan los sistemas de seguridad informática y perimetral permitiendo entre otros:* *reducción de riesgos solo permitiendo conexiones seguras, así como otras incidencias técnicas. disponiendo una infraestructura actualizada que requiera un mínimo mantenimiento, lo que permite tener un sistema mucho más seguro.* ***lote 2****: "adquisición e implementación de*	*Se identifica una alta cantidad de parches pendientes de aplicar, es requerido ser aplicado de manera inmediata por las falencias de seguridad que se identifican en los hosts remotos.* *• Se identifica una alta cantidad de vulnerabilidades de denegación de servicio,* *debido a la falta de actualización de parches sobre las diversas plataformas.* *Se identifica una alta cantidad vulnerabilidades críticas en Apache Tomcat, PHP* *y Oracle que es de inmediata atención para evitar que un atacante informático pueda explotarlas.*	*\... Así mismo se da claridad que no todos los parches en una entidad pueden ser aplicados, ya que pueden afectar la disponibilidad de los sistemas de información, por lo cual se implementan, medidas compensatorias, que no eliminan el riesgo, pero mitigan su probabilidad. así mismo, es importante denotar que diariamente pueden salir una cantidad considerable de parches para sistemas operativos y sistemas de información, los mismos no pueden ser aplicados de forma abrupta, deben ser probados con el fin de no afectar la disponibilidad o funcionamiento de los sistemas.*	*Teniendo en cuenta los aspectos relevantes de las fichas técnicas establecidas en los estudios previos de los contratos, podemos indicar que las renovaciones contratadas de los servicios de seguridad frente al resultado del contrato 690 de 2022, se indica que se encontraron múltiples debilidades de riesgo críticas, alto, medio, y bajo que son necesarios tener en cuenta para evitar posibles situaciones que puedan ocasionar daños, perdida de información y / o destrucción de esta.* *Se puede deducir con el resultado de las pruebas que en los riesgos críticos y alto al realizar las pruebas de caja Negra externas y en las pruebas de caja gris y blanca las conexiones no son seguras.* *Se debe realizar un inventario de sistemas obsoletos y presentar un plan de renovación de los mismos; análisis que se debió de realizar antes de invertir los recursos del contrato 508 de 2021, cuyo objeto precisamente era el de renovación y adquisición de soluciones tecnológicas*

	infraestructura para bases de datos oracle (oda)". ***lote 3**: "renovación, adquisición e implementación del licenciamiento de endpoint".* ***lote 4**: "renovación de las diferentes soluciones tecnológicas para fortalecer la seguridad de la información".*	*ver informe de **ethikal hacking***		
Para el año 2022 adelantaron los contratos 630, 631, 632, 633, 637 denominados RENOVACIÓN Y ADQUISICIÓN DE SOLUCIONES TECNOLÓGICAS A NIVEL DE INFRAESTRUCTURA, SEGURIDAD Y BASES DE DATOS PARA EL MINISTERIO DE TRANSPORTE por valor de $2.743.640.649.	*En los estudios previos se establecía:* *ANEXO TÉCNICO LOTE 1 "RENOVACIÓN FIREWALL DE BASES DE DATOS (IMPERVA)".* *ANEXO TÉCNICO LOTE 2 "ADQUISICIÓN DE SOFTWARE DE CIBERINTELIGENCIA PARA LA DETECCIÓN Y REMEDIACIÓN AUTOMÁTICA DE TRÁFICO MALICIOSO".* *ANEXO TÉCNICO LOTE 3 "RENOVACIÓN DE LICENCIAMIENTO DE ENDPOINT DE SEGURIDAD".* *ANEXO TÉCNICO LOTE4 "RENOVACIÓN WEB APPLICATION SCANNER (WAS)".* *ANEXO TÉCNICO LOTE 5 "RENOVACION PARA LA SEGURIDAD DE LA INFRAESTRUCTURA TECNOLOGICA (SEGURIDAD PERIMETRAL)".*	*Se identifica una alta cantidad de vulnerabilidades críticas de denegación de servicio,* *Se identifica una alta cantidad vulnerabilidades críticas en Apache Tomcat, PHP y Oracle que es de inmediata atención para evitar que un atacante informático pueda explotarlas.* *Se identifica una alta cantidad de vulnerabilidades de denegación de servicio, debido a la falta de actualización de parches sobre las diversas plataformas* *ver informe de **ethikal hacking***	*\... En consecuencia, se requiere contratar la renovación del licenciamiento por un año para los equipos de seguridad perimetral mencionados anteriormente y que se encuentran operando en conjunto con la red de datos del ministerio de Transporte.* *El Grupo TIC viene implementado mejores prácticas para gobierno de TIC, minimizar los riesgos de indisponibilidad e incrementar la seguridad de la información del Ministerio, lo cual requiere entre otros de la implementación de una solución de protección de malware, rasonware y demás riesgos de seguridad en las estaciones de trabajo y servidores de la Entidad, sistemas de bases de datos y actualización en el licenciamiento de soporte de los sistemas de seguridad.*	*Teniendo en cuenta los aspectos relevantes de las fichas técnicas establecidas en los estudios previos de los contratos, podemos indicar que las renovaciones contratadas de los servicios de seguridad frente al resultado del contrato 690 de 2022, se indica que se encontraron múltiples debilidades de riesgo críticas, alto, medio, y bajo que son necesarios tener en cuenta para evitar posibles situaciones que puedan ocasionar daños, perdida de información y 7 o destrucción de esta.* *Se puede deducir con el resultado de las pruebas que en los riesgos críticos y alto al realizar las pruebas de caja Negra externas y en las pruebas de caja gris y blanca las conexiones no son seguras.* *Se debe analizar los parches que ofrecen los sistemas contratados y mantenerlos actualizados.* *Se debe realizar un inventario de sistemas obsoletos y presentar un plan de renovación de los mismos; análisis que se debió de realizar antes de invertir los recursos del contrato 630,631,632,633 y 637 de 2022, cuyo objeto precisamente era el de renovación y adquisición de soluciones tecnológicas*

	ANEXO TÉCNICO LOTE 6 "ADQUISICIÓN DE NODOS Y MODULOS DE MEMORIA RAM PARA LA HIPERCONVERGENCIA EXISTENTE DEL MINISTERIO DE TRANSPORTE". *Detectar posibles factores de amenaza e infección por malware en los equipos de cómputo y servidores del Ministerio.* *Orquestar actividades de detección y de respuesta a posibles amenazas que se identifiquen dentro de la red, con el objetivo de reducir los tiempos de reacción y de respuesta de la entidad.* *Asegurar el correcto funcionamiento de la entidad, reduciendo las probabilidades de infección por malware y ransomware en los equipos de cómputo y servidores.* *Permitir el intercambio seguro de información por medio de mecanismos de cifrado.* *Detectar vulnerabilidades críticas con el objetivo reducir posibles superficies de ataque aprovechables por ciberdelincuentes, entre otros.*			

Respuesta Grupo TIC´s al Presente Informe:

A continuación, anexamos la respuesta dada por el Grupo TICS de este ministerio la cual en su contexto se encuentra en el cuadro anterior.

Respecto a que según TIC indica que se evidencia una confusión y descontextualización, respecto a las renovaciones de dispositivos de seguridad y el ejercicio de Ethical Hacking nos permitimos indicar lo siguiente:

***Respuesta Oficina de Control Interno**.*

*Para esta Oficina es claro que un hacker ético consiste en tratar de violar la seguridad del sistema informático de una organización, con autorización previa de la misma, para encontrar **agujeros o errores y que estos puedan ser corregidos antes de que sean explotados por los ciberdelincuentes.** Por lo tanto, al observar y analizar todos los aspectos indicados en las fichas técnicas que hacen parte del contrato en la que se pretendía asegurar al ministerio comparado con todas las observaciones presentadas por el hacker ético se ven claramente la vulnerabilidad que pudieron ser tenidas en cuenta en los procesos de contratación para la ADQUISICIÓN DE SOLUCIONES TECNOLÓGICAS A NIVEL DE INFRAESTRUCTURA, SEGURIDAD Y BASES DE DATOS PARA EL MINISTERIO DE TRANSPORTE.*

Mal diríamos hoy que todo lo que se encontró por el hacker ético es producto de tener Infraestructura obsoleta, Sistemas de información obsoletos, Sistemas de información obsoletos, Configuraciones incorrectas de parámetros, Aplicación incorrecta de prácticas de desarrollo seguro, Configuración incorrecta de arquitectura de seguridad como lo expresa el Oficial de Seguridad de la Información – contratista de la Oficina de Planeación, cuando el ministerio ha venido invirtiendo cuantiosos recursos en actualizaciones y adquisiciones de Hardware y Software y en RENOVACIÓN Y ADQUISICIÓN DE SOLUCIONES TECNOLÓGICAS A NIVEL DE INFRAESTRUCTURA, SEGURIDAD Y BASES DE DATOS algunas de estas contrataciones se efectuaron muy recientemente como es el caso de los procesos que se auditaron a través de este informe

Respuesta Grupo TICs

-Es importante que se tengan en cuenta que la información, que se encuentra en el informe de Ethical Hacking es reservada, ya que constituye un riesgo para la seguridad nacional y un daño inminente a los bienes del estado, considerando que los informes de Control Interno podrán ser publicados, o de acceso por diferentes partes, la esta información no puede ir allí. Ya que les da información y herramientas a los ataques sobre vulnerabilidades de nuestra infraestructura tecnológica, por lo cual se pide que en uniforme se referencie los numerales de los documentos, pero no se brinde la información de la vulnerabilidad, ya que sería una violación directa a los acuerdos de confidencialidad y a la seguridad de la Entidad.

Respuesta control interno

El informe inicialmente fue remitido en borrador exclusivamente al Coordinador de grupo TICs quien al interior de su dependencia lo socializo. En el informe final no se está reportando específicamente el resultado obtenido por Ethical Hacking, lo que si constituye un riesgo es que este informe sea conocido por contratistas que en cualquier momento se retiran de la entidad. Consideramos que esta información debe ser conocida por personal de planta ojalá del más alto nivel.

Respuesta Grupo TICS

Todos los aspectos anteriores son los que rigen un proceso de Ethical hacking, y por lo cual la observación a la que se hace referencia en el informe "podemos indicar que el resultado esperado con la contratación de aseguramiento relacionada en este informe no se alcanzó; el ministerio de transporte (en Apache Tomcat, PHP y Oracle)," es desmeritoria y poco coherente, con respecto a las vulnerabilidades establecidas, las cuales derivan de ámbitos de obsolescencia y por lo cual falta de parches, recursos para renovar sistemas de información que no pueden ser migrados y por lo cual se debe conservar las versiones de PHP y Tomcat (Se requiere personal especializado en desarrollo para migración de portales). así como, Oracle referente a una mala aplicación de parametrización sobre un servidor.

Es de tener en cuenta que un ataque de día cero o una configuración incorrecta de seguridad de una aplicación, pueden o no ser mitigadas, ya que, al no estar descubiertas por nadie, los equipos de seguridad puede que no estén preparados para contenerlas, por eso también son importantes estos ejercicios, en el proceso de descubrir estas vulnerabilidades y poderlas compensar con las medidas existentes. O solicitar recursos a la alta dirección.

Respuesta Control Interno:

La Oficina de control Interno tuvo en cuenta algunos aspectos de la respuesta sin embargo es claro que las fichas técnicas de los contratos indicaban que se pretendía asegurar al ministerio de los delincuentes informáticos como se observa en algunos casos asi "\…Reducción de riesgos solo permitiendo conexiones seguras, así como otras incidencias técnicas. Disponiendo una infraestructura actualizada que requiera un mínimo mantenimiento, lo que permite tener un sistema mucho más seguro"

Es cierto que, aunque en la actualidad no existen sistemas 100% seguros, es posible mantener un sistema de gestión de seguridad de la información basado en las mejores prácticas de la industria, que permita al ministerio acercarse a un nivel adecuado de seguridad, el cual debe ser complementado con tareas de seguimiento, aprendizaje y principalmente de gestión para eliminar aquellas brechas de seguridad que nos hacen débiles frente a las amenazas; situación que se debió haber alcanzado con los contratos de seguridad suscritos materia de la presente auditoria.

4.2 Observaciones y Recomendaciones Generales

El objetivo del ethical hacking es descubrir las deficiencias de los sistemas e infraestructuras digitales, como, por ejemplo, los errores de software, evaluar los riesgos de seguridad y participar de manera constructiva en la corrección de los fallos de seguridad descubiertos. Una prueba de estrés para la seguridad del sistema puede tener lugar en cualquier momento, a veces incluso después de un hackeo ilegal. Sin embargo, lo ideal sería que los hackers éticos se anticiparan a los ciberdelincuentes y, al hacerlo, evitaran daños mayores.

El propósito fue definir y validar los niveles de exposición en que se encuentra la plataforma tecnológica de Ministerio de Transporte, frente a posibles ataques y/o accesos no autorizados por parte de delincuentes informáticos.

El contrato con ethikal hacking debió haber sido suscrito y ejecutado antes de haberse efectuado la inversión los contratos de aseguramiento objeto de esta auditoria; de esta forma se hubiese contado con un diagnóstico oportuno para diseñar los objetos contractuales y no al contrario como sucedió.

A continuación, mostramos los niveles descritos por el HACKER ETICO a fin se analicen y de acuerdo con su nivel de criticidad sean valorados y solucionados en la medida en que se brinden los medios económicos para hacerlo, igualmente y de acuerdo con lo indicado en los estudios previos se debe dar cumplimiento a lo allí establecido en su totalidad.

Niveles de riesgo para las vulnerabilidades.

NIVEL DE RIESGO CRÍTICO
Corresponde a la vulnerabilidad que permitiría a un atacante informático el ingreso total de la máquina violando todos los principios de seguridad de la información como confidencialidad, integridad y disponibilidad de toda la infraestructura.

NIVEL DE RIESGO ALTO
corresponde vulnerabilidades por medio de las cuales fácilmente un intruso puede obtener control total del dispositivo, con posibilidades de comprometer la seguridad de toda la red. Las vulnerabilidades de este tipo incluyen la obtención de privilegios para leer y modificar archivos, ejecución remota de código, presencia de puertas traseras (Backdoors), entre otros.

NIVEL DE RIESGO MEDIO
corresponde a las vulnerabilidades por medio de las cuales es posible obtener acceso a información específica almacenada en los dispositivos, incluyendo configuraciones de seguridad. Las vulnerabilidades de este tipo incluyen la divulgación de contenido de archivos, divulgación de reglas de filtrado y mecanismos de seguridad, uso de servicios sin autorización, entre otros.

NIVEL DE RIESGO BAJO
corresponde a las vulnerabilidades por medio de las cuales un intruso puede recolectar información de los dispositivos (Sistema Operativo, puertos abiertos, servicios, etc.), posiblemente se puede usar dicha información para buscar otras vulnerabilidades.

Ver informe técnico de ETHIKAL HACKING

Las pruebas adelantadas por ETHICAL HACKING, se indican a continuación:

PRUEBAS CAJA NEGRA EXTERNO
-JQUERY XSS
-CGI SQL INJECTION
-REPOSITORIO GIT ABIERTO
-DIRECTORIOS NAVEGABLES
-TLS 1.0 DETECTADO
-WEBSERVER VERSIÓN NO SOPORTADA
-APACHE MÚLTIPLES VULNERABILITIES
-OPENSSL 1.1.1 VULNERABLE
-PHP MÚLTIPLES VULNERABILITIES
-ORACLE CREDENCIALES EXPUESTAS

-WORDPRESS CREDENCIALES EXPUESTAS

PRUEBAS CAJA GRIS Y BLANCA INTERNO
-HP DATAPROTECTOR MÚLTIPLES VULNERABILITIES
-ORACLE WEBLOGIC SERVER JAVA OBJECT DESERIALIZATION
-MICROSOFT RDP RCE BLUEKEEP
-SNMP AGENT DEFAULT COMMUNITY NAME
-ORACLE GLASSFISH SERVER DENIAL OF SERVICE
-APACHE LOG4SHELL RCE
- AUTENTICACIÓN SESIÓN NULA SMB
-MS17-010 ETERNAL BLUE
-PHP VULNERABILIDADES BUFFER OVERFLOW
-JQUERY XSS

-Teniendo en cuenta el alto costo en contratos de aseguramiento para la información, bases de datos y demás sistemas en los cuales ha invertido el ministerio en valores significativos para evitar posibles vulnerabilidades y que permitirían el Intercambio seguro de información por medio de mecanismos de cifrado; monitoreo y verificación del flujo de información en las bases de datos de la entidad; la reducción de riesgos en las bases de datos, como el análisis de vulnerabilidades periódicos especializados en esta infraestructura; que en su esencia permitirían detectar posibles anomalías o incidentes en las bases de datos, se observa que de acuerdo a los resultados de la verificación a través de la firma Ethical Hacking , podemos indicar que el ministerio de transporte, presenta una cantidad de vulnerabilidades significativa y críticas que son de inmediata atención dado que en cualquier momento podemos ser intervenidos por delincuentes informáticos en los que podrían modificar, alterar, borrar utilizar de forma indebida la información que reposa en las bases de datos.

Teniendo en cuenta que el ministerio no ha actualizado una gran cantidad de parches estos deben ser analizados y determinar cuáles deben ser actualizados de inmediato, de tal forma que las falencias identificadas de seguridad informática y que son identificados en los hosts remotos sean solucionadas evitando así ser intervenidos por delincuentes informáticos.

5. Contrato 530 de 2021

Seguimiento ejecución del contrato 530 de 2021

Objeto: DISEÑO, IMPLEMENTACIÓN Y DESPLIEGUE DE LA SOLUCION TECNOLÓGICA (HARDWARE Y SOFTWARE) DE LA PRIMERA ETAPA DEL SISTEMA INTELIGENTE NACIONAL PARA LA INFRAESTRUCTURA, EL TRANSITO Y EL TRANSPORTE (SINITT) EN ARAS DE INTEGRAR, GESTIONAR Y BRINDAR LA INFORMACION DEL SECTOR TRANSPORTE DE CONFORMIDAD CON LAS POLITICAS DE LOS ITS DECRETO 2060 DE 2015.

Valor: $2.584.000.000 M/CTE

Estado del contrato 530 de 2021

Este contrato se encuentra en liquidación, se solicitó la elaboración del presente trámite en el mes de octubre del 2022, por medio de memorando No. 20223070101423. En la actualidad el grupo de contratos lo tiene en estudio.

En referencia a la implementación de la solución tecnología la empresa ERT como cita en el último entregable, dio la transferencia de conocimiento al equipo ITS.

Se indica que el presente contrato cobija la estructuración e implementación del Sistema Inteligente para la infraestructura, el tránsito y el transporte – SINITT. En el cual su alcance, era la arquitectura del sistema, ConOPS, implementación de estándares y desarrollo de software del sistema en su primera etapa.

5.1 Observación Oficina de control Interno:

Es importante indicar que la Oficina de Control interno en su proceso de desarrollo de la Auditoria entrevisto a la líder del proyecto para que nos informara sobre la operatividad del sistema en comento, sin embargo, manifestó que en su momento el sistema no se encontraba en producción y que no conocía de su desarrollo y operatividad de este.

Ante el valor invertido y el seguimiento de la ejecución de este contrato se indica que este desarrollo actualmente no se encuentra en producción.

La oficina de Control Interno, en su etapa de discusión del informe, convocó al área auditada a reunión el día 17 de mayo del 2023, pero los funcionarios de esa dependencia no se presentaron y pidieron su aplazamiento, la reunión finalmente se efectuó vía teams el 25 de mayo; en esa reunión los funcionarios del área auditada no efectuaron comentarios precisos y directos a las observaciones del informe preliminar, volvieron a solicitar plazo para enviar comentarios hasta el 31 de mayo de 2023, pero en esa fecha tampoco se allegó ningún comentario al informe preliminar ajustado.

Por lo que a continuación presentamos el informe final:

Teniendo en cuenta la importancia de este desarrollo, el esquema para la interoperabilidad con el SINITT su integración con la ANI a través de un web service, Información sobre la Concesión de Villavicencio, Información sobre la concesión Bogotá Villeta, Información sobre Transporte Público (Transmilenio), Relación de las mediciones de segmentos de vías en Medellín, Relación entre localización de peajes y mediciones de peajes electrónicos y entrega de información de tarifas de peajes y dada la importancia establecida en los mismos estudios previos en el que Ministerio de Transporte y el Gobierno Nacional al determinar la importancia de los ITS para toda la nación y con el conocimiento que estos sistemas deben cumplir con factores clave tales como: interoperabilidad, escalabilidad, integración, compatibilidad y neutralidad tecnológica; es claro que se debe contar con una carta de navegación para desarrollar armónicamente los ITS que a su vez, producen servicios hacia los ciudadanos en términos de infraestructura, tránsito y transporte. Se requiere que este sistema provea los beneficios esperados se disponga de la información que procesa y permita que brinde los beneficios por el cual se contrató este sistema.

Debe tenerse en cuenta lo anteriormente registrado y se debe analizar técnicamente la funcionalidad del producto recibido y determinarse posibles incumplimientos por parte del contratista, para ser tenidos en cuenta en el proceso de liquidación del contrato.

Este contrato se encuentra en liquidación, se solicitó la elaboración del presente trámite en el mes de octubre del 2022, por medio de memorando No. 20223070101423. En la actualidad el grupo de contratos lo tiene en estudio.

En referencia a la implementación de la solución tecnología la empresa ERT como cita en el último entregable, dio la transferencia de conocimiento al equipo ITS (contratista)

Se indica que el presente contrato cobija tan solo la primera parte del estructuración e implementación del Sistema Inteligente para la infraestructura, el tránsito y el transporte – SINITT. En el cual su alcance, era la arquitectura del sistema, ConOPS, implementación de estándares y desarrollo de software del sistema en su primera etapa.

5.2 Respuesta Grupo TIC:

Es una imprecisión citar que el presente desarrollo no se encuentra en producción, en razón a que, si se encuentra en producción, las cuales puede encontrar en los siguientes enlaces:

***https://sipi-sinitt.mintransporte.gov.co/inicio-sesion**: Enlace para personal al interior de la Entidad y las Entidades adscritas*

https://siscontrol-sinitt.mintransporte.gov.co/inicio-sesion: Usuarios registrados en el Ministerio de transporte en el sistema.

Es decir, el desarrollo de la empresa ERT fue entregado en su totalidad, probado por los ingenieros de la Entidad en su momento.

Ahora bien, otra instancia es el plan piloto de conexión de las concesiones Bogotá Villeta y Bogotá Villavicencio, Centro de Control Medellín, en razón a que este plan piloto es un proyecto que se está ejecutando con el Gobierno de Corea del Sur. Se han venido realizando mesas de trabajo con el Gobierno de Corea del Sur, y se les mostro el desarrollo ya realizado.

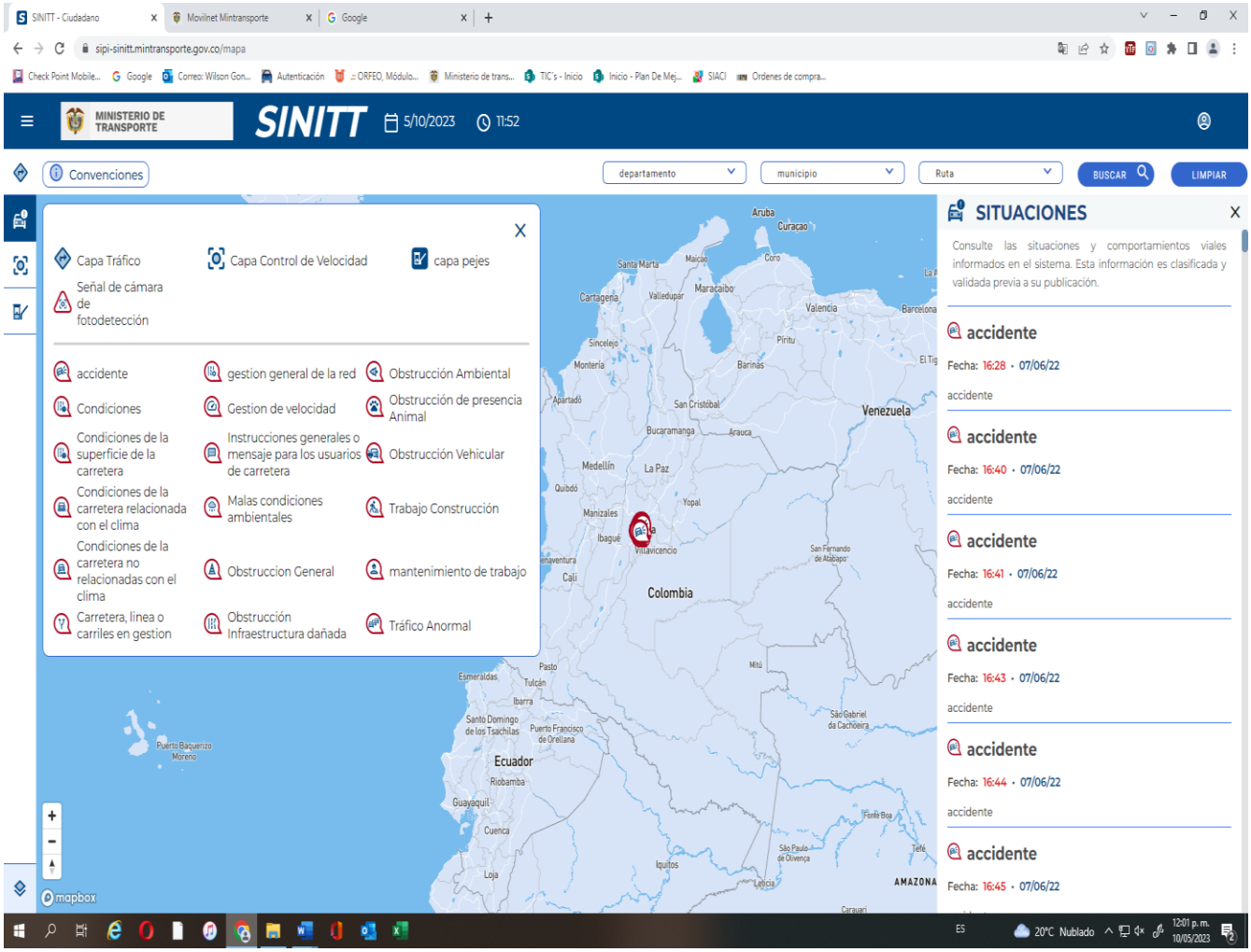
En la actualidad se está realizando los trabajos requeridos para culminar con la presente fase de implementación del SINITT, no obstante, esta por cronograma termina en diciembre de 2024.

Adicional, cabe resaltar que tal como lo cita el objeto del presente contrato 530 de 2021, era para realizar la PRIMERA FASE del SINITT, es decir el alcance no es para la totalidad del SINITT, que ahora bien como está citado en el Plan Maestro ITS, es un proyecto para implementar en un lapso de 10 años.

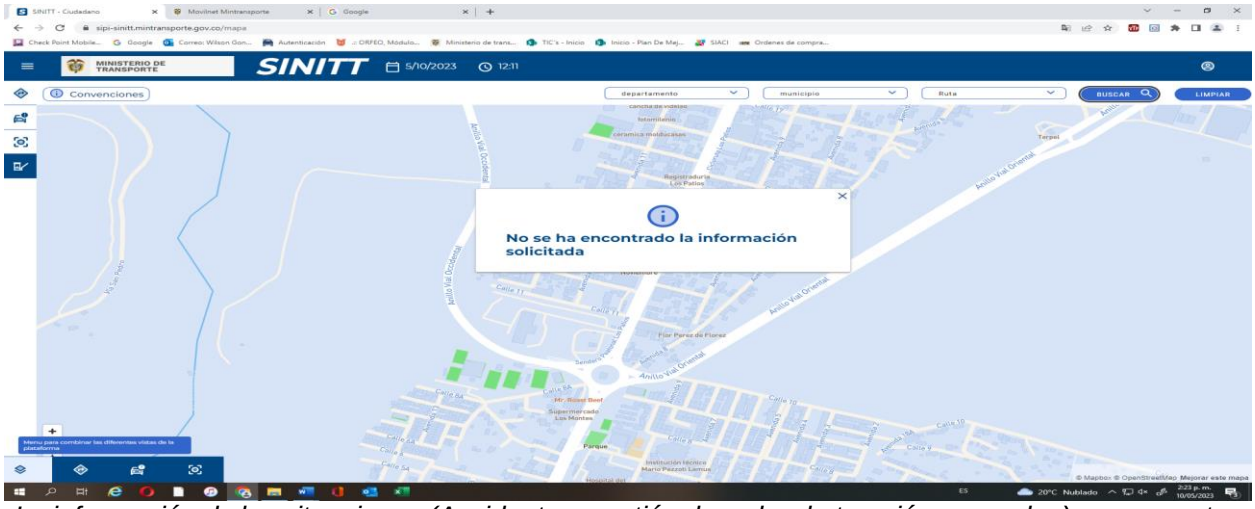
5.3 Observaciones de la Oficina de Control Interno:

Una vez y después que se presenta el informe preliminar el grupo tic da respuesta y nos envía el link para realizar la consulta del sistema nos permitimos indicar lo siguiente:

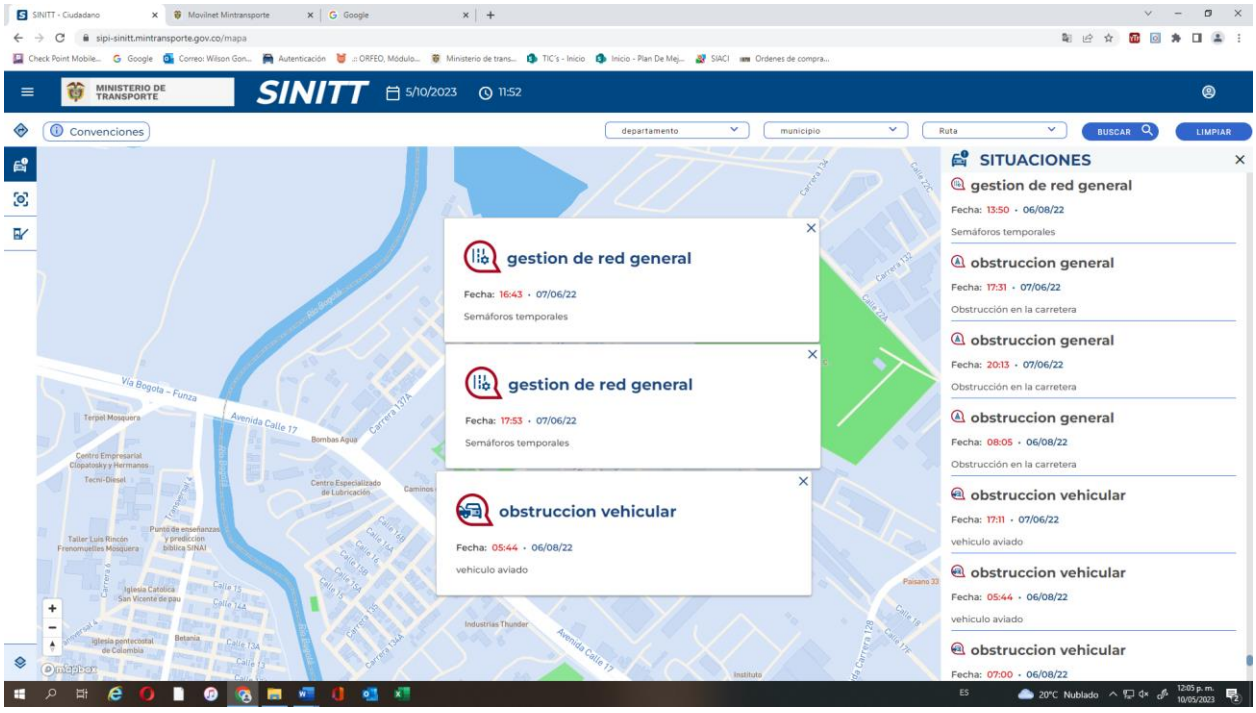
- *El sistema muestra las convenciones de consulta, pero no permite hacer la selección de una de ellas para hacer filtro y generar la respectiva consulta.*

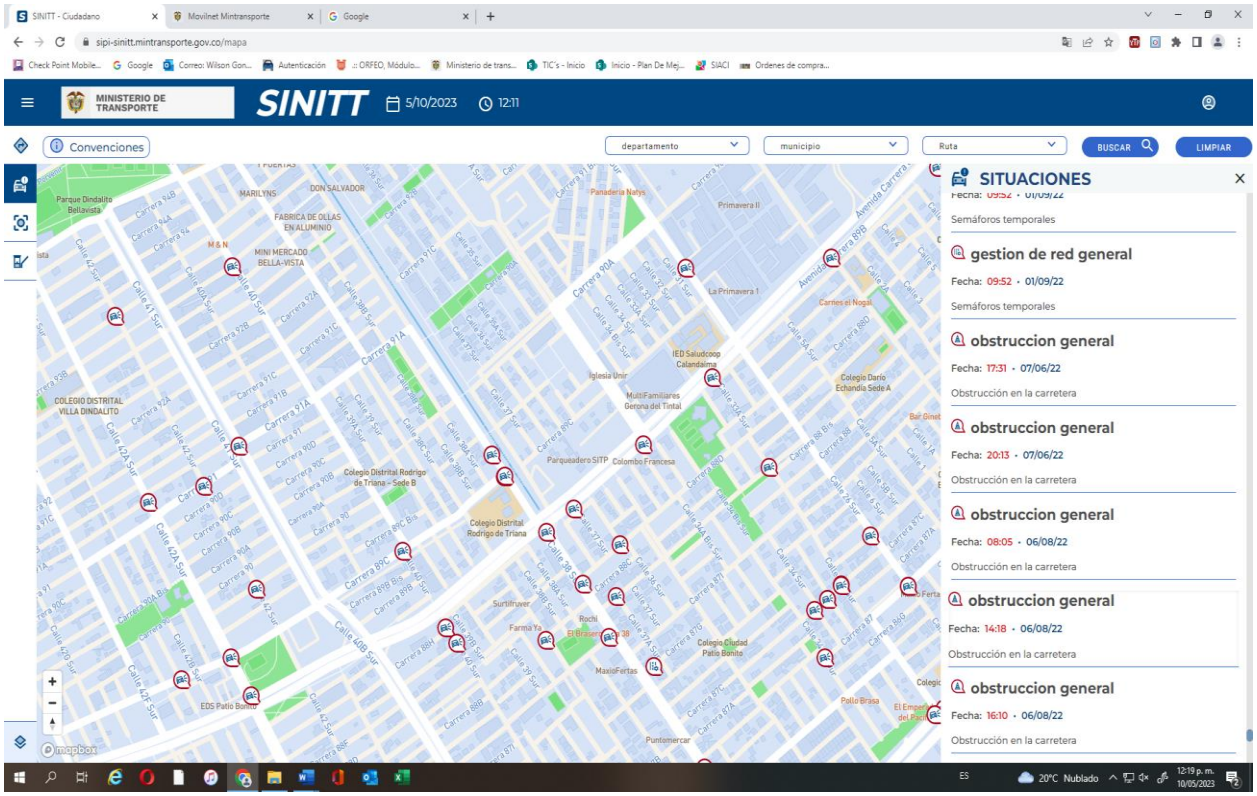


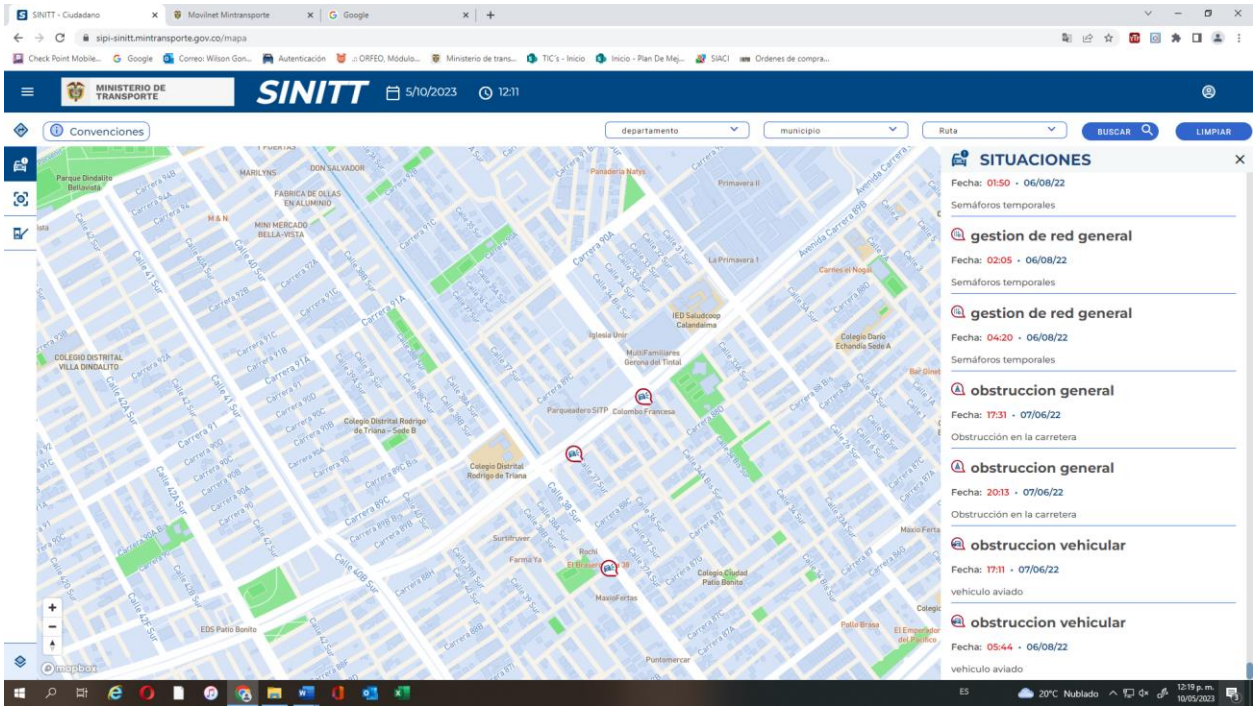
-Al ingresar al menú que muestra las diferentes vistas de la plataforma, no muestra resultados



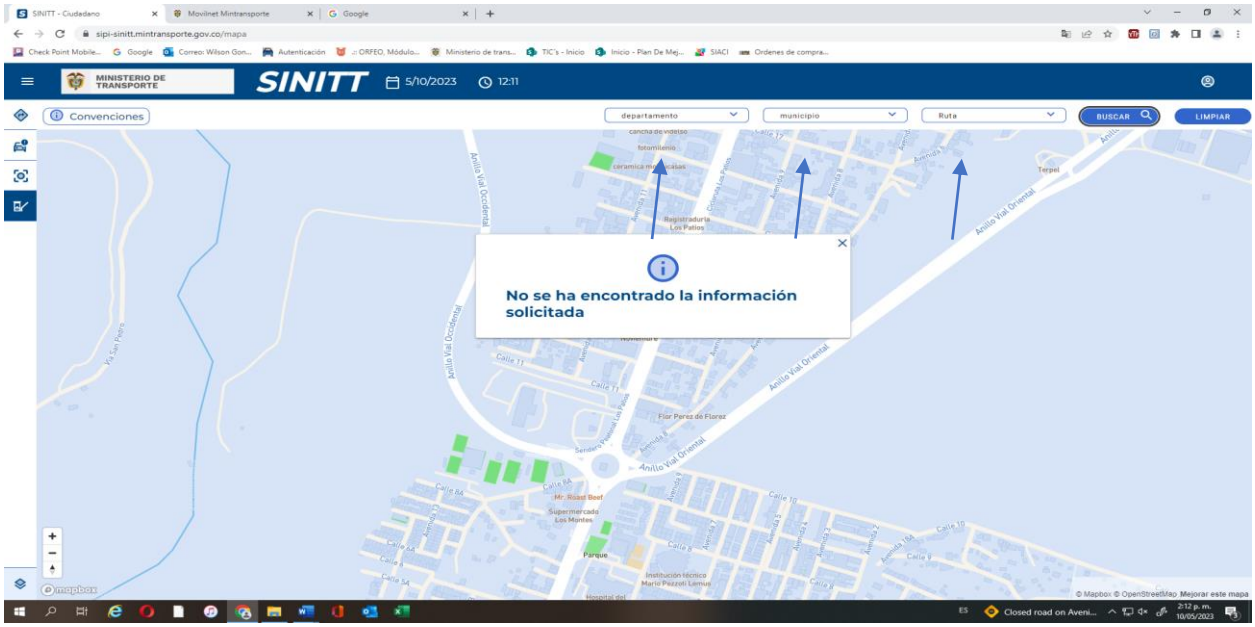
-La información de las situaciones (Accidentes, gestión de red y obstrucción generales) se encuentran totalmente desactualizadas la fecha más reciente en el sistema de estas tres (3) situaciones a aparecen con última fecha de actualización a agosto de 2022,







-Al realizar búsqueda por departamento, municipio, ruta, se observa que no fija el dato de la búsqueda en los campos, y en los pocos casos que se tienen, no muestra el resultado por cuanto la información está totalmente incompleta tal y como se indica a continuación:



Teniendo en cuenta la importancia de este desarrollo, el esquema para la interoperabilidad con el SINITT su integración con la ANI a través de un web service, Información sobre la Concesión de Villavicencio, Información sobre la concesión Bogotá Villeta, Información sobre Transporte Público (Transmilenio), Relación de las mediciones de segmentos de vías en Medellín, Relación entre localización de peajes y mediciones de peajes electrónicos y entrega de información de tarifas de peajes y dada la importancia establecida en los mismos estudios previos en el que Ministerio de Transporte y el Gobierno Nacional al determinar la importancia de los ITS para toda la nación y con el conocimiento que estos sistemas deben cumplir con factores clave tales como: interoperabilidad, escalabilidad, integración, compatibilidad y neutralidad tecnológica; es claro que se debe contar con una carta de navegación para desarrollar armónicamente los ITS que a su vez, producen servicios hacia los ciudadanos en términos de infraestructura, tránsito y transporte.

Se requiere que este sistema provea los beneficios esperados se disponga de la información que procesa de forma actualizada brinde los beneficios por el cual se contrató este sistema.

Debe tenerse en cuenta lo anteriormente registrado y se debe analizar técnicamente la funcionalidad del producto recibido y determinarse posibles incumplimientos por parte del contratista, para ser tenidos en cuenta en el proceso de liquidación del contrato.

5.4 Código fuente de página visible en cada búsqueda:

Este sistema muestra el código fuente en todos los campos de los módulos, por lo cual existe el riesgo de que los ciberdelincuentes utilicen el código fuente para explotar vulnerabilidades o incrustar malware en el software existente. Con acceso a él, los actores hostiles podrían comprometer un sistema, robar datos y apoderarse de una máquina completa.

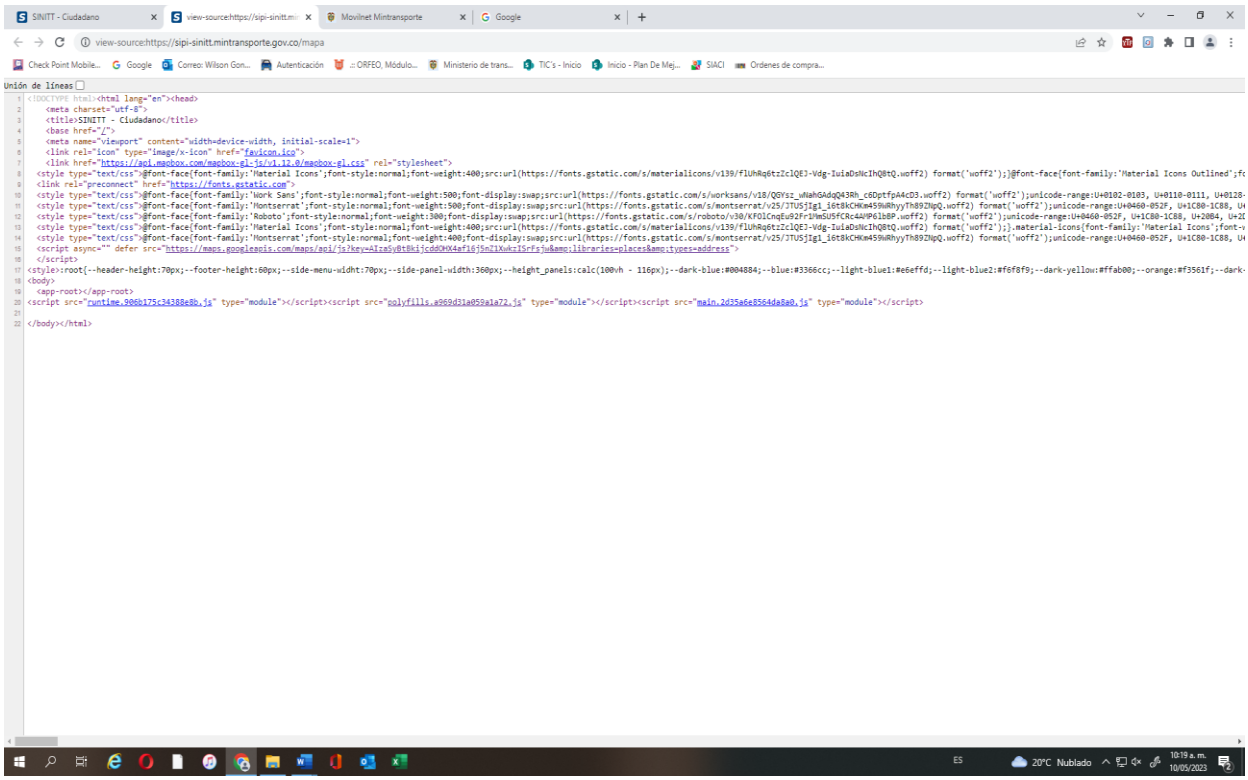
Teniendo en cuenta que el código fuente es una estructura interna de un software antes de ser compilada para convertirse en un software en sí mismo. El código fuente es un componente

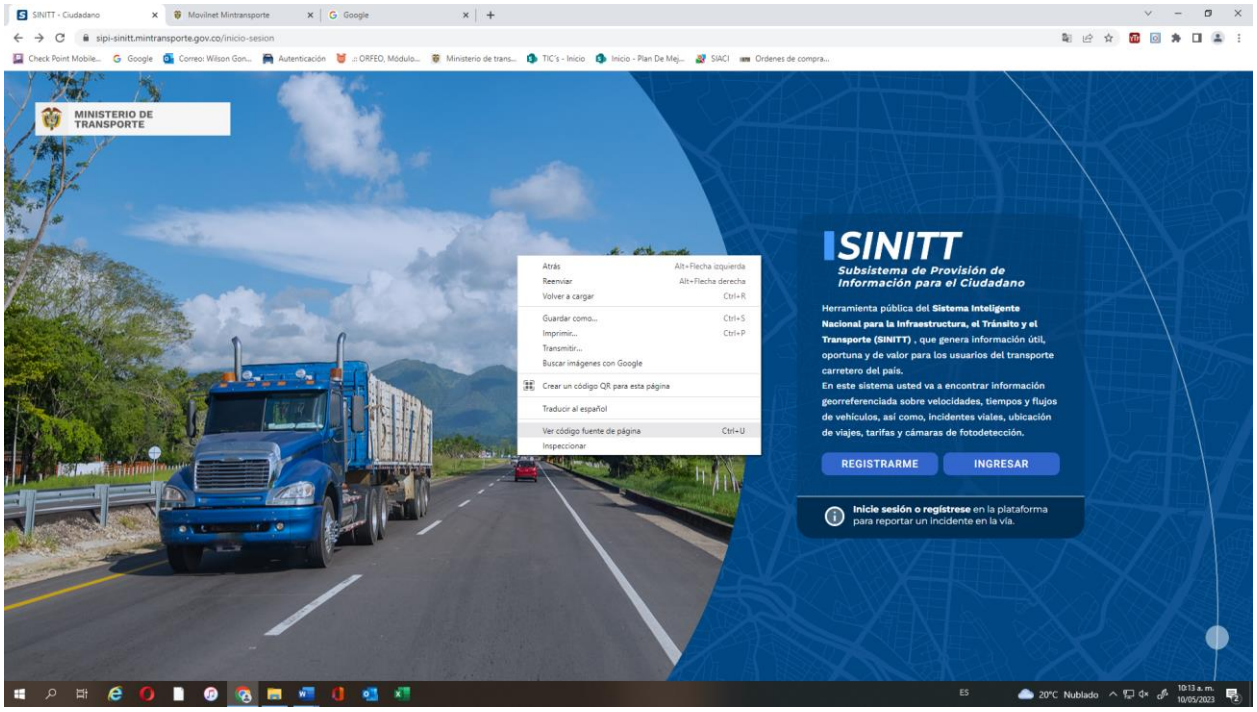
fundamental de un programa informático que está compuesto por palabras o símbolos escritos de forma ordenada. Tiene la particularidad de que puede ser fácilmente leído y comprendido por un ser humano, siendo este el principal riesgo de seguridad vinculado a los códigos fuente.

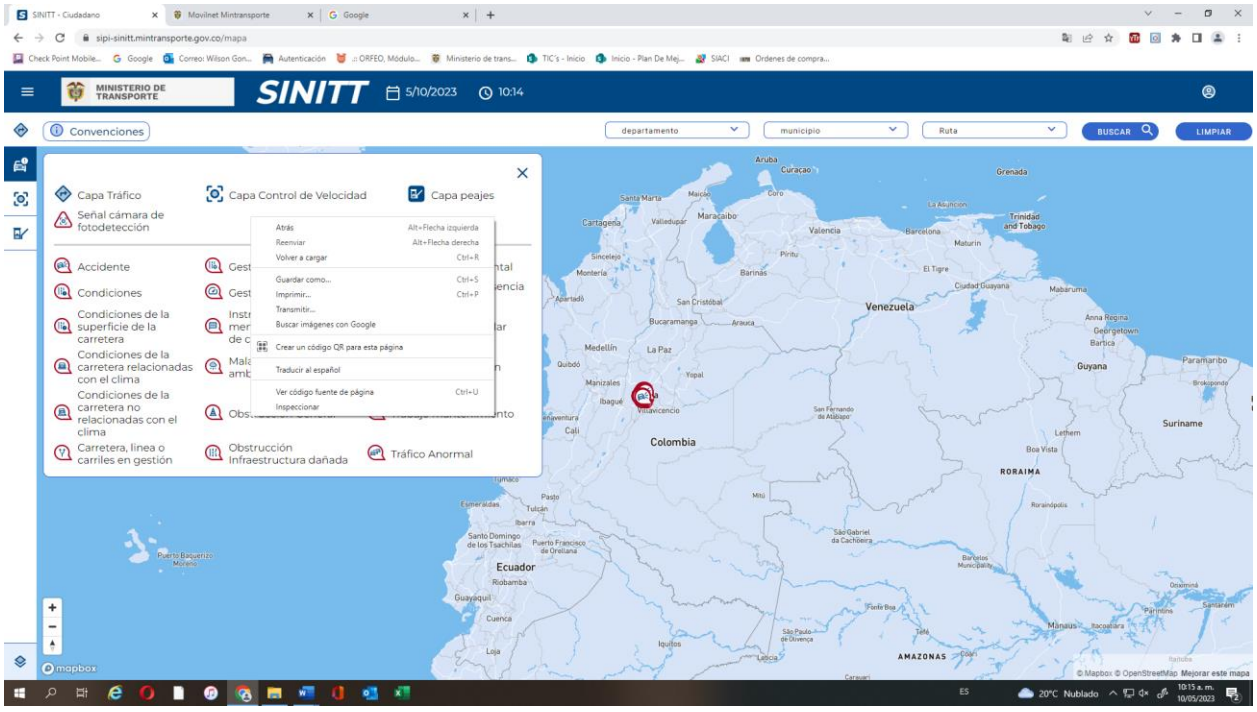
El código fuente es el "esqueleto" de un software. Por lo tanto, existe riesgo que los ciberdelincuentes puedan tener acceso a esta información dándole la posibilidad de examinar todas sus características internas en busca de puntos vulnerables para el desarrollo de exploits, principalmente gracias a la legibilidad del código, El acceso directo al código hace que este proceso sea mucho más sencillo, ya que permite buscar de forma directa debilidades que, en algunos casos, son ampliamente conocidas por los delincuentes. Si tienen éxito en su búsqueda, los delincuentes pueden llegar a crear los temidos exploits zero-day que le brinden la oportunidad, por ejemplo, de ejecutar comandos de forma remota, pudiendo comprometer a todos los usuarios de la versión vulnerable de ese software.

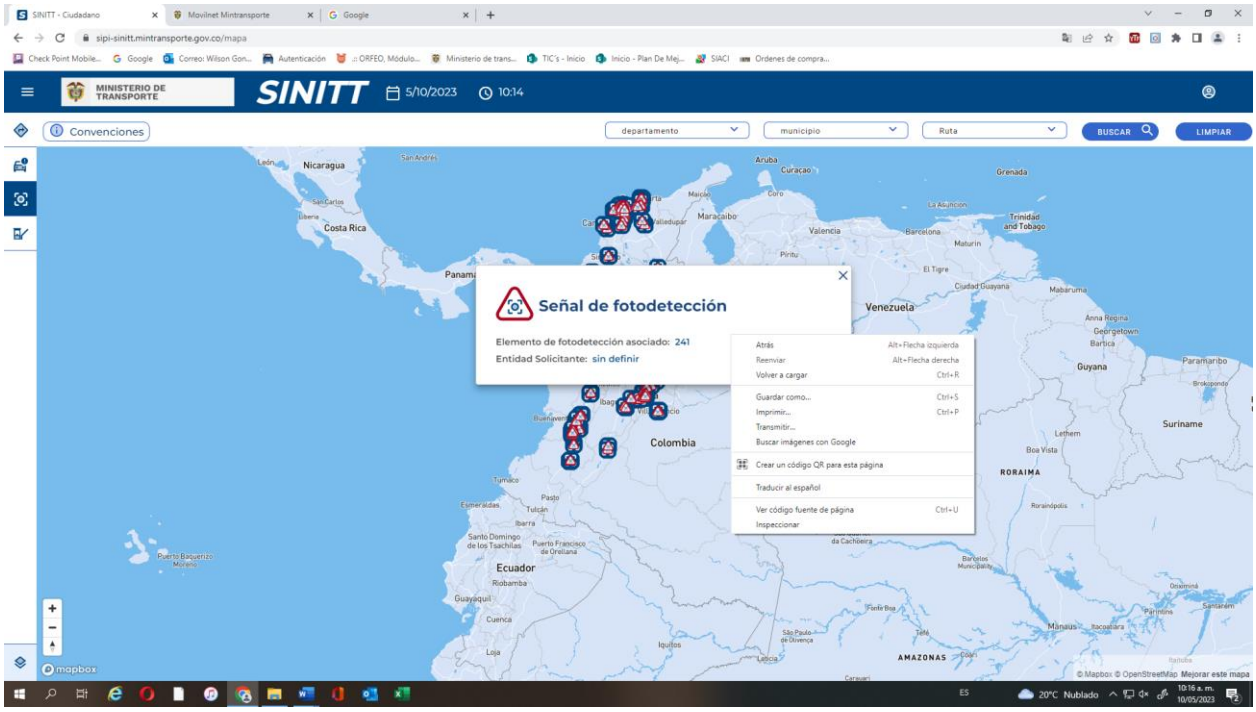
A través de los códigos fuente estos ciberdelincuentes pueden Descubrir nuevos objetivos dentro o fuera de la empresa, generalmente, cuando los datos de autenticación aparecen en el código fuente, estos datos suelen estar asociados al acceso a una determinada ubicación, que puede ser un servicio externo o interno al entorno, y para que tenga éxito también se debe proporcionar una dirección de acceso. El formato de estas direcciones suele oscilar entre direcciones IP y URL entre otros.

A continuación, mostramos algunos códigos fuentes expuestos en el sistema:




MINISTERIO DE TRANSPORTE
SINITT
Subsistema de Provisión de Información para el Ciudadano
Herramienta pública del Sistema Inteligente Nacional para la Infraestructura, el Tránsito y el Transporte (SINITT) , que genera información útil, oportuna y de valor para los usuarios del transporte carretero del país.
En este sistema usted va a encontrar información georreferenciada sobre velocidades, tiempos y flujos de vehículos, así como, incidentes viales, ubicación de viajes, tarifas y cámaras de fotodetección.
REGISTRARME
INGRESAR
Inicie sesión o regístrese en la plataforma para reportar un incidente en la vía.


MINISTERIO DE TRANSPORTE
SINITT
5/10/2023
10:14
Convenciones
departamento
municipio
Ruta
BUSCAR
LIMPIAR
Capa Tráfico
Capa Control de Velocidad
Capa peajes
Señal cámara de fotodetección
Accidente
Condiciones
Condiciones de la superficie de la carretera
Condiciones de la carretera relacionadas con el clima
Condiciones de la carretera no relacionadas con el clima
Carretera, linea o carriles en gestión
Obstrucción Infraestructura dañada
Tráfico Anormal
Colombia
Venezuela
Ecuador
Guyana
Suriname
RORAIMA
AMAZONAS



5.6 Recomendaciones:

Recomendamos para el caso del código fuente de página visible, se recomienda dar protección orientada a los datos, no a un servidor o estación en sí, un camino interesante es asegurarse de que solo las personas adecuadas tengan acceso a la información confidencial, como los códigos fuente, aplicar una política de privilegios mínimos y revisar los permisos continuamente

Realizar una Evaluación de riesgos de seguridad de la información basado en las siguientes actividades:

1. *Establecer y delimitar un marco de evaluación de riesgos*
2. *Inventariar los activos de información*
3. *Identificar puntos vulnerables y amenazas potenciales*
4. *Determinar el impacto de las amenazas*
5. *Crear un plan de gestión de riesgos.*

Es importante indicar que gran parte de esta evaluación de riesgos fue realizada por el hacker ético contratado por el ministerio – deben establecerse acciones para mitigar los riesgos del informe de ethical hacking.

Finalmente tener presente las OBLIGACIONES ESPECIFICAS DEL CONTRATISTA:

1. Cumplir con todas las especificaciones del servicio señaladas en la propuesta y en el Anexo Técnico "DISEÑO, IMPLEMENTACIÓN Y DESPLIEGUE DE LA SOLUCIÓN TECNOLÓGICA (HARDWARE Y SOFTWARE) DE LA PRIMERA ETAPA DEL SISTEMA INTELIGENTE

NACIONAL PARA LA INFRAESTRUCTURA, EL TRANSITO Y EL TRANSPORTE (SINITT) EN ARAS DE INTEGRAR, GESTIONAR Y BRINDAR LA INFORMACIÓN DEL SECTOR TRANSPORTE DE CONFORMIDAD CON LAS POLÍTICAS DE LOS ITS DECRETO 2060 DE 2015" .

2. Poner a disposición del Ministerio de Transporte su capacidad técnica, experiencia y conocimientos para cumplir con el desarrollo del objeto contractual.

3. Garantizar la calidad de los desarrollos de software que haga para el Ministerio de Transporte basados en la ***metodología TDD*** *para pruebas de software.*

4. Garantizar que los desarrollos realizados ***cumplan con los requerimientos de seguridad, estándares de desarrollo, y diseño de alto nivel entregados por el Ministerio de Transporte.***

5. Validar los requisitos transversales, funcionales y no funcionales entregados por el Grupo GTIC/ITS del Ministerio de Transporte y hacer las observaciones y aportes que haya lugar.

6. Realizar el diseño detallado, es decir, el diseño de la arquitectura de hardware, software y la selección de productos open source y/o comerciales y/o funcionalidades que se serán adquiridos y utilizados para el desarrollo del SINITT y sus subsistemas. Este diseño detallado deberá realizarse tomando como base el diseño de alto nivel entregado por el Ministerio de Transporte y deberá priorizar la adopción de componentes open source ampliamente probados y con soportes en comunidades sobre productos comerciales equivalentes. El conjunto de documentos que componen el diseño será aprobado por el Ministerio de Transporte.

7. ***Realizar el desarrollo de software en los lenguajes de programación Python, Java, ó .Net para el back-end y Angular para el front-end;*** *así mismo, seguir las directivas de desarrollo que el Ministerio de Transporte ya tiene formuladas.*

8. Desarrollar el software bajo la ***metodología de desarrollo de componentes****.*

9. Realizar todas las etapas del ciclo de vida del software expuestas en la metodología en V y la metodología de desarrollo por componentes, cumpliendo con los objetivos, entradas y productos de cada etapa para todos los requerimientos y proyectos demandados por el Ministerio de Transporte. En particular, se deberán entregar al Ministerio de Transporte o quien este designe todos los documentos especificados en el aparte 7 ENTREGABLES DEL PROYECTO del Anexo Técnico "DISEÑO, IMPLEMENTACIÓN Y DESPLIEGUE DE LA SOLUCIÓN TECNOLÓGICA (HARDWARE Y SOFTWARE) DE LA PRIMERA ETAPA DEL SISTEMA INTELIGENTE NACIONAL PARA LA INFRAESTRUCTURA, EL TRANSITO Y EL TRANSPORTE (SINITT) EN ARAS DE INTEGRAR, GESTIONAR Y BRINDAR LA INFORMACIÓN DEL SECTOR TRANSPORTE DE CONFORMIDAD CON LAS POLÍTICAS DE LOS ITS DECRETO 2060 DE 2015". Todo esto teniendo de referencia el Plan Maestro de Implementación abordado en la metodología V.

10. Desarrollar el software para el sistema, esto con ajuste a la especificación de requisitos y a la documentación de diseño detallado a nivel de componentes.

11. Realizar pruebas unitarias, de stress y puesta de producción que serán utilizadas para verificar que los productos cumplen con el diseño detallado teniendo de referencia la metodología en V.

12. ***Desarrollar y realizar Plan de Pruebas, con el cual se debe verificar que los componentes suministrados coinciden con el Diseño Detallado documentado y previamente aprobado por el Ministerio de Transporte.***

13. Realizar plan de integración para la aprobación del Ministerio de Transporte. Este plan debe contemplar la forma en que se combinan con éxito los componentes de hardware y software, subsistemas y sistemas en un todo, completo y funcional.

14. ***Realizar la integración y verificación del sistema de conformidad con el plan de integración previamente aprobado por el Ministerio de Transporte.***

15. Presentar el sistema desarrollado al Ministerio de Transporte con el objeto de que sea validado.
16. Entregar al Ministerio de Transporte el Código Fuente del desarrollo realizado a la terminación del contrato.
17. ***Realizar plan de transferencia de conocimiento para la aprobación del Ministerio de Transporte.***
18. Realizar la transferencia de conocimiento de conformidad con el plan previamente aprobado por el Ministerio de Transporte.
19. Suministrar el personal mínimo requerido y acordado de acuerdo con la oferta presentada.
20. Una vez cumplidos los requisitos de perfeccionamiento y ejecución del contrato, constituir a su costo un patrimonio autónomo para recibir los pagos que realice el Ministerio de Transporte.

Entregables una vez elaborado el proyecto

Producto 4- Implementación

Entrega: Al finalizar el quinto mes de ejecución del contrato. Este producto debe contener los siguientes entregables: *Información que será verificada con el responsable del proyecto*

1. Parametrización del Software o la Plataforma tecnológica
2. ***Implementación, verificación y validación del Software o Plataforma tecnológica que soporte la Integración de los sistemas de información a vincular.***
3. ***Implementación, verificación y validación Software o Plataforma tecnológica que soporta la integración con los centros de control con las entidades a vincular***
4. Implementación, verificación y validación del esquema de seguridad para la conexión del SINITT con los actores estratégicos.
5. ***Implementación, verificación y validación de la aplicación web para el ciudadano***
6. Implementación, verificación y validación del software de control local (front-end) para los servicios ITS implementar
7. Implementación, verificación y validación del servidor GIS y los webmaps (incluyendo el enfoque de Datex II) en función de los servicios ITS priorizados
8. Plan de Pruebas de las implementaciones realizadas
9. Ejecución de las pruebas incluidas en el plan de pruebas
10. ***Despliegue del Software o la Plataforma tecnológica****.*
11. ***Transferencia de conocimiento al equipo que el Ministerio de Transporte designe****.*

Producto 5 – Generación de documentos

Entrega: A más tardar el 17 de diciembre de 2021.
Este producto debe contener los siguientes entregables:

Información que será verificada con el responsable del proyecto

1. Artefactos generados en la construcción del Sistema (Código fuente, scripts de bases de datos, parametrización, instaladores, manual de usabilidad de la plataforma tecnológica, manual de instalación y configuración, código para el despliegue de la infraestructura en la nube).
2. Informe final de la capacitación y transferencia de conocimiento realizada de conformidad con la metodología aprobada en el producto 1

3. Código fuente con sus respectivos comentarios
4. Repositorio tipo GIT para cada subsistema ITS aquí dispuesto
5. Informe de cobertura de las pruebas de cada uno de los subsistemas y desarrollos e implementaciones aquí descritos junto con las pruebas de integración e interoperabilidad
6. Modelo de datos lógico y físico final del SINITT basado en Datex II
7. Modelo de Seguridad Final del SINITT
8. Listado de servicios de integraciones (servicios web u otros artefactos)
9. Manuales de Usuario de todos los elementos aquí dispuestos
10. Manual de Procesos para el SINITT y su interrelación con los actores estratégicos y su CCO (Centro de control de operaciones asociado a Centro de Control Integrado de Tráfico)
11. Diagrama de flujo de datos (DTD) alineado a Datex II.
12. Diagramas de arquitecturas con sus explicaciones respectivas.

(las negrillas son nuestras)

Cordialmente,

WILSON GONZALEZ TAPIAS
Profesional Especializado.

Cuadro Resumen de Observaciones

Anexo 1

Observaciones	Recomendaciones	Dependencia Responsable	Acciones	Responsable	Fecha de cumplimiento
***CONTRATO 690 DE 2022**. Una vez realizada la inversión en los contratos 517 del 2021 por valor de $1.234.410.000, Contrato 506 de 2021 por valor de $ 658.299.226, Contrato 507 de 2021 por valor de $154.987.000, Contrato 508 de 2021 por valor de 168.200.000 y 630, 631, 632, 633, 637 por valor de $2.743.640.649 denominados RENOVACIÓN Y ADQUISICIÓN DE SOLUCIONES TECNOLÓGICAS A NIVEL DE INFRAESTRUCTURA, SEGURIDAD Y BASES DE DATOS PARA EL MINISTERIO DE TRANSPORTE y con el propósito de definir y validar los niveles de exposición en que se encuentra en la plataforma tecnológica de Ministerio de Transporte, frente a posibles ataques y/o accesos no autorizados por parte de delincuentes informáticos, se adelantó el contrato 690/2022 por lo cual los resultados de este contrato dentro de los aspectos relevantes de las fichas técnicas establecidas en los estudios previos de los contratos antes descritos, podemos indicar que las renovaciones contratadas de los servicios de seguridad frente al resultado del contrato 690 de 2022, se observan múltiples vulnerabilidades de riesgo críticas, alto, medio, y bajo que son necesarios tener en cuenta para evitar posibles situaciones que puedan ocasionar daños, perdida de información y/ o destrucción de esta.*	*-Se debe realizar un inventario de sistemas obsoletos y presentar un plan de renovación de estos; análisis que se debió de realizar antes de invertir los recursos de los contratos de seguridad perimetral que en su objeto establecía RENOVACIÓN Y ADQUISICIÓN DE SOLUCIONES TECNOLÓGICAS A NIVEL DE INFRAESTRUCTURA, SEGURIDAD Y BASES DE DATOS PARA EL MINISTERIO DE TRANSPORTE, lo ideal sería que los hackers éticos se anticiparan a los ciberdelincuentes y, al hacerlo, podrían evitar que los ciberdelincuentes ocasiones daños a la institución, en los que podrían modificar, alterar, borrar utilizar de forma indebida la información que reposa en las bases de datos.* *-Se debe analizar los parches que ofrecen los sistemas contratados y mantenerlos actualizados, en especial los nuevos que se desarrollen por parte de las casas matrices.*	*Grupo Tic*			
Se observa que de acuerdo a los resultados de la verificación a través de la firma Ethical Hacking, que el ministerio de transporte presenta una cantidad de vulnerabilidades significativa y críticas que son de inmediata atención dado que en cualquier momento podemos ser intervenidos por delincuentes informáticos en los que podrían modificar, alterar, borrar utilizar de forma indebida la información que reposa en las bases de datos.	*-Ver informe de ethikal hacking y tomar las acciones necesarias para evitar posibles riesgos significativos de seguridad informática.*	*Grupo Tic*			

Seguimiento ejecución Contrato 530 de 2021*. Objeto: DISEÑO, IMPLEMENTACIÓN Y DESPLIEGUE DE LA SOLUCION TECNOLÓGICA (HARDWARE Y SOFTWARE) DE LA PRIMERA ETAPA DEL SISTEMA INTELIGENTE NACIONAL PARA LA INFRAESTRUCTURA, EL TRANSITO Y EL TRANSPORTE (SINITT) EN ARAS DE INTEGRAR, GESTIONAR Y BRINDAR LA INFORMACION DEL SECTOR TRANSPORTE DE CONFORMIDAD CON LAS POLITICAS DE LOS ITS DECRETO 2060 DE 2015.* *Valor: $2.584.000.000 M/CTE.* *-El sistema muestra las convenciones de consulta, pero no permite hacer la selección de una de ellas para hacer filtro y generar la respectiva consulta. (Ver informe anexo)* *-Al ingresar al menú que muestra las diferentes vistas de la plataforma, no muestra resultados. (Ver informe anexo)* *-La información de las situaciones (Accidentes, gestión de red y obstrucción generales) se encuentran totalmente desactualizadas la fecha más reciente en el sistema de estas tres (3) situaciones aparecen con última fecha de actualización a agosto de 2022, (Ver informe anexo)* *-Al realizar búsqueda por departamento, municipio, ruta, se observa que no fija el dato de la búsqueda en los campos, y en los pocos casos que se tienen, no muestra el resultado por cuanto la información está totalmente incompleta (Ver informe anexo)*	*Debe tenerse en cuenta lo anteriormente registrado y se debe analizar técnicamente la funcionalidad del producto recibido y determinarse posibles incumplimientos por parte del contratista, para ser tenidos en cuenta en el proceso de liquidación del contrato.*	*Grupo Tic*			
No se observa en su desarrollo el esquema para la interoperabilidad con el SINITT, *su integración con la ANI a través de un web service, Información sobre la Concesión de Villavicencio, Información sobre la concesión Bogotá Villeta, Información sobre Transporte Público (Transmilenio), la información de las mediciones de segmentos de vías en Medellín, Relación entre localización de peajes y mediciones de peajes electrónicos (desactualizadas), la entrega de información de tarifas de peajes (y dada la importancia establecida en los mismos estudios previos en el que Ministerio de Transporte y el Gobierno Nacional al determinar la importancia de los ITS para toda la nación y con el conocimiento que estos sistemas deben cumplir con factores clave tales como: interoperabilidad, escalabilidad, integración, compatibilidad y neutralidad tecnológica; es claro que el sistema no provee esta información por lo que se indica que este sistema no brinda los datos esperados en la solución contratada.*	*Se debe contar con una carta de navegación para desarrollar armónicamente los ITS que, a su vez, producen servicios hacia los ciudadanos en términos de infraestructura, tránsito y transporte.* *Se debe analizar el cumplimiento de la ejecución de este contrato para determinar posibles incumplimientos y responsabilidades en su ejecución*	*Grupo Tic*			
Se observa visualización del Código fuente de página visible en cada búsqueda. *Este sistema muestra el código fuente en todos los campos de los módulos, por lo cual existe el riesgo de que los ciberdelincuentes utilicen el código fuente para explotar vulnerabilidades o incrustar malware en el software existente. Con acceso a él, los actores hostiles podrían comprometer un*	*se recomienda dar protección orientada a los datos, no a un servidor o estación en sí, un camino interesante es asegurarse de que solo las personas adecuadas tengan acceso a*	*Grupo Tic*			

sistema, robar datos y apoderarse de una máquina completa. *Teniendo en cuenta que el código fuente es una estructura interna de un software antes de ser compilada para convertirse en un software en sí mismo. El código fuente es un componente fundamental de un programa informático que está compuesto por palabras o símbolos escritos de forma ordenada. Tiene la particularidad de que puede ser fácilmente leído y comprendido por un ser humano, siendo este el principal riesgo de seguridad vinculado a los códigos fuente.* *A través de los códigos fuente estos ciberdelincuentes pueden Descubrir nuevos objetivos dentro o fuera de la empresa, generalmente, cuando los datos de autenticación aparecen en el código fuente, estos datos suelen estar asociados al acceso a una determinada ubicación, que puede ser un servicio externo o interno al entorno.*	*la información confidencial, como los códigos fuente, aplicar una política de privilegios mínimos y revisar los permisos continuamente.* *En especial los permisos dados a contratistas que ya no pertenecen al ministerio de transporte.*				
Los entregables y la ubicación de los archivos físicos y lógicos del sistema contratado al momento de realizar la auditoria eran desconocidos por el personal de planta dado que en su mayoría los contratistas no se les renovó el contrato.	*Se debe analizar la posibilidad de incluir en los diferentes procesos de compra, desarrollo tanto de hardware como de software personal de planta para que no se presenten situaciones de asistencia técnica en los mismos una vez los contratistas dejen de prestar el servicio a la entidad o en su defecto transferir el conocimiento y entrega de la información antes de la terminación de los contratos.*	*Grupo Tic*			