**Portal web:** www.supertransporte.gov.co
**Oficina Administrativa:** Calle 63 No. 9A-45, Bogotá D.C
**PBX:** 352 67 00
**Correspondencia:** Calle 37 No. 28B-21, Bogotá D.C
**Línea Atención al Ciudadano:** 01 8000 915615

# M E M O R A N D O

*20202000076353*

No. 20202000076353
Bogotá, 24-12-2020

Para: **Camilo Pabón Almanza**
Superintendente de Transporte

De: Jefe Oficina de Control Interno

Asunto: Informe definitivo auditoría Proceso Gestión de TICS política de seguridad y privacidad de la información de la Superintendencia de Transporte y Evaluación de riesgos y controles - Política de Administración del Riesgo del 1 enero a 31 de octubre de 2020 - Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

En cumplimiento del plan anual de auditorías aprobado para la vigencia 2020, mediante acta 01 del 10 de marzo de 2020 y modificado mediante acta 02 del 24 de julio del 2020 del Comité Institucional de Coordinación de Control Interno y lo establecido en el Decreto 648 de 2017, Artículo 2.2.21.5.3 “De las oficinas de control interno las Unidades u oficinas de control interno o quien haga sus veces, desarrollaran su labor a través de los siguientes roles: Liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control”, así también lo contemplado en el Modelo Integrado de Planeación y Gestión (MIPG) las Dimensiones Gestión con valores para resultados y Control Interno, componente evaluación del riesgo, la Oficina de Control Interno realizó la Auditoría Gestión de TICS, correspondiente al período comprendido entre el 01 de enero al 31 de octubre de 2020 y a la Política de Administración del Riesgo (selectivo).

Acorde con lo establecido en el proceso Seguimiento y Evaluación Independiente a la Gestión Institucional, procedimiento Auditorías Internas, Seguimiento y Evaluación frente al presente informe definitivo, se recibió la respectiva retroalimentación mediante memorando número 20201100074943 radicado en Orfeo y comunicado por el correo Institucional por la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC el día lunes 21 de diciembre de 2020, se procedió por parte del auditor a hacer nuevamente la verificación para posteriormente elaborar el presente informe definitivo, el informe queda en firme.

Los hallazgos y observaciones configurados requieren implementación de acciones, por lo cual se debe formular el respectivo plan de mejoramiento por parte del responsable de la dependencia, el cual se encuentra dispuesto en la cadena de valor de la Entidad http://intranet.supertransporte.gov.co/CadenaValor/index.htm-Plan y se debe suscribir teniendo en cuenta la identificación del proceso y el (los) hallazgo(s)u observaciones que ha(n) sido señalada(s) en el presente informe, realizar el análisis de causas, determinar y ejecutar el plan de acción que elimine la causa raíz de la situación evidenciada, es

importante que remitan el plan suscrito firmado en PDF y en Excel a los correos joseramírez@supertransporte.gov.co y jefacturacontrolinterno@supertransporte.gov.co, para posterior seguimiento y verificación a la eficacia y efectividad de las acciones por parte del auditor (como Tercera Línea de Defensa). Allegar el plan de mejoramiento a más tardar el 6 de enero de 2021.

Se hace la salvedad, que las recomendaciones se hacen con el propósito de aportar a la mejora continua de los procesos; y estas se acogen y se implementan, por decisión del líder del proceso.

No obstante, la Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones" art. 12 - Funciones de los auditores internos. Serán funciones del asesor, coordinador, auditor interno o similar las siguientes: literal k) indica "Verificar que se implanten las medidas respectivas recomendadas".

Y en el Artículo 3º.- Características del Control Interno. Son características del Control Interno las siguientes:

a. "El Sistema de Control Interno forma parte integrante de los sistemas contables, financieros, de planeación, de información y operacionales de la respectiva entidad;

En cada área de la organización, el funcionario encargado de dirigirla es responsable por control interno ante su jefe inmediato de acuerdo con los niveles de autoridad establecidos en cada entidad".

Agradecemos su oportuna gestión, con el objetivo de fortalecer el Sistema de Control Interno de la Entidad.

Cordial saludo,

**Alba Enidia Villamil Muñoz**
Jefe Oficina de Control Interno

Copia: Comité Institucional de Coordinación de Control Interno: Camilo Pabón Almanza - Superintendente de Transporte; María Pierina González Falla - Secretaria General, María Fernanda Serna Quiroga - Jefe Oficina Jurídica; Álvaro Ceballos Suárez - Superintendente Delegado de Puertos; Wilmer Arley Salazar Arias - Superintendente Delegado de Concesiones e Infraestructura; Adriana Margarita Urbina Pinedo - Superintendente Delegado de Tránsito y Transporte; Adriana Tapiero Cáceres - Superintendente Delegada para la Protección de Usuarios del Sector Transporte; Javier Pérez Pérez - Jefe Oficina de Tecnologías de la Información y las Comunicaciones; Diego Felipe Díaz Burgos - Jefe Oficina Planeación; Jaime Rodríguez - Director Financiero.

Elaboró y Verificó: José Ignacio Ramírez Ríos – Auditor - Profesional Especializado OCI auditor OCI
C:\Users\JoseRamirez\Desktop\SPT-OCI\2020-200-CNTROL INTRNO\200-21.03\MEMORANDOS\ Memo_InfrmeDfntvo_GstiónTICS-24dic2020. docx

Evaluación: ___X___ Seguimiento: _____ Auditoría Interna:___X___.

FECHA: 24/12/2020

**NOMBRE DEL INFORME:**

Informe definitivo auditoría Proceso Gestión de TICS política de seguridad y privacidad de la información de la Superintendencia de Transporte y Evaluación de riesgos y controles - Política de Administración del Riesgo del 1 enero a 31 de octubre de 2020 - Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

## 1. OBJETIVO GENERAL

Verificar el Sistema de Control Interno del proceso Gestión TICS.

## 2. OBJETIVOS ESPECIFICOS

- Verificar las actividades del PEI y PAI con corte 31 de octubre de 2020.
- Verificar los proyectos de inversión de la OTIC.
- Verificar el cumplimiento de la la política de seguridad de la información de la Superintendencia de Transporte.
- Verificar los riesgos y controles asociados

## 3. ALCANCE

Proceso Gestión TICS y Política de Seguridad y privacidad de la Información - (según selectivo).

## 4. MARCO NORMATIVO O CRITERIOS DE AUDITORÍA, EVALUACIÓN O SEGUIMIENTO

- Ley 87 de 1993, “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.”
- Decreto 1499 de 11 de septiembre de 2017, “*Por medio del cual se modifica el Decreto 1083 de 2015, Decreto únicoreglamentrio del sector público, en lo relacionado con el sistema de gestión establecido en el artículo 133 de la Ley 1753 de 2015*”.
- Decreto 1008 del 14 de junio de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.

- Guía para la administración del riesgo y el diseño de controles en entidades públicas, riesgos de gestión, corrupción y seguridad digital, versión 4, octubre 2018, Departamento Administrativo de la Función Pública.
- Guía Rol de las Unidades de Control Interno, Auditoria Interna o quien haga sus veces. Dirección de Gestión y Desempeño Institucional, diciembre de 2018.
- Manual de Gobierno Digital. Manual para la Implementación de la Política de Gobierno Digital Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1. Incorpora los lineamientos para la integración al Portal Único del Estado Colombiano.
- Resolución 14099, del 10 de diciembre de 2019 "Por la cual se actualiza el Modelo Integrado de Planeación y Gestión – MIPG en la Superintendencia de Transporte, se crean algunas instancias administrativa y se dictan otras disposiciones.
- Resolución 60362 de 21 de noviembre de 2017, "*Por la cual se adopta la Política de Seguridad de la Información para la Superintendencia de Puertos y Transporte*".
- Cadena de valor.
- Política de seguridad de la información, 2 de julio de 2019, Versión 4.2.
- Demás normatividad aplicable.

## 5. METODOLOGÍA

La auditoría al proceso se realizó según selectivo, aplicando las normas de auditoría, técnicas de observación, revisión documental, entre otros.

Se consultó la información publicada en la Intranet y la página web de la Entidad.

En el desarrollo de la auditoría se realizó la verificación de la información y análisis para la generación del informe definitivo que será comunicado con los hallazgos y/u observaciones según proceda, conclusiones y recomendaciones que aporten a la mejora continua y al desempeño del proceso.

Se comunicó el informe preliminar mediante radicado 20202000073153 del 15 de diciembre de 2020, respecto del cual la Oficina de TIC's dio respuesta mediante radicado 20201100074943 del 21 de diciembre de 2020, realizando la retroalimentación respectiva, no obstante no allegaron soportes adicionales.

Con base en esta información el auditor procedió a realizar la nuevamente la verificación para la generación del informe definitivo.

## 6. PRESENTACIÓN DE RESULTADOS

Resumen de hallazgos u observaciones realizadas en el presente Informe definitivo Auditoría Gestión TICS, los cuales se detallan a continuación:

| Ítem | Hallazgo u Observación | Responsable del proceso | Requiere Plan de Mejoramiento S/N | Cierra Hallazgo informes anteriores | Observación | Página |
|---|---|---|---|---|---|---|
| 1 | **H01A-011 dicv20-(AC)GTICS** | Oficina de Tecnologías de la Información y las Comunicaciones | S | N | **Hallazgo (AC Acción Correctiva)**<br>**H01A-011dicv20-(AC)GTICS**<br>El documento de las actualizacioes anuales del Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, no se encuentran publicado en la página web de la Superintendencia de Transporte.<br>Se incumple la guia elaborada por MinTIC: G.ES.06. Guía cómo estructurar el Plan Estratégico de Tecnologías de la Información – PETI, numeral 2.2 Alcance del documento "*Se describe claramente el alcance del PETI teniendo en cuenta que debe proyectarse a máximo cuatro años y debe actualizarse cada año. El alcance del PETI debe indicar lo que efectivamente debe lograr la Entidad durante la vigencia del PETI. (…)*".<br>Se incumple el alcance del PETI publicado para el cuatrenio 2017 - 2020 en el que se debe adopto la actualización anual, esta no se evidenció la publicación en la web de la Entidad, "*El alcance de estos documentos es describir la estrategia de ejecución de los proyectos de Tecnologías de la Información en la Superintendencia de Puertos y Transporte* ***durante el período 2017-2020 haciendo una actualización anual****, con el fin de mejorar la gestión y cumplimiento de los objetivoss estratégicos de la Entidad, Vigilancia, Inspección y Control alineados con la estrategía sectorial Transportte Nacional*".".<br>Se incumple el Artículo 2.2.22.3.14. *"Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: (…).*<br>Se incumple el numeral e. "*Asegurar la oportunidad y confiabilidad de la información y de sus registros*;", y numeral f. "*Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos;",* del Artículo 2º.- *"Objetivos del sistema de Control Interno. Atendiendo los principios constitucionales que debe caracterizar la administración pública, el diseño y el desarrollo del Sistema de Control Interno se orientará al logro de los siguientes objetivos fundamentales:* ", Ley 87 de 1993.<br><br>Situación que puede conllevar a la posible materialización de riesgos de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC en la vigencia 2020 impactando la gestión de la disponibilidad de recursos necesarios para alcanzar los objetivos institucionales y cumplir las funciones delegadas. | 7, 8 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | **H002A-011 dicv20-(AC)GTICS** | Oficina de Tecnologías de la Información y las Comunicaciones | S | N | **Hallazgo (AC Acción Correctiva)**<br>**H02A-011dicv20-(AC)GTICS**<br>El documento Plan de contingencia de TI , ni el Plan de tratamiento de riesgos de TI se encuentran publicados en la página web de la Superintendencia de Transporte a la fecha.<br>Se incumple el Artículo 2.2.22.3.14. *"Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: (…).*<br>Se incumple el numeral e. "*Asegurar la oportunidad y confiabilidad de la información y de sus registros*;", y numeral f. "*Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos;",* del Artículo 2º.- *"Objetivos del sistema de Control Interno. Atendiendo los principios constitucionales que debe caracterizar la administración pública, el diseño y el desarrollo del Sistema de Control Interno se orientará al logro de los siguientes objetivos fundamentales: "*, Ley 87 de 1993.<br>Situación que puede conllevar a la posible materialización de riesgos de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC en la vigencia 2020 impactando la gestión de la disponibilidad de recursos necesarios para alcanzar los objetivos institucionales y cumplir las funciones delegadas. | 8 |
| 3 | **O001A-211dic20-(AP)GTICS** | Oficina de Tecnologías de la Información y las Comunicaciones | S | N | **Observación (AP Acción Preventiva)**<br>**O001A-11dic20-(AP)GTICS**<br>El Auditor observó en el Sistema de Seguimiento a Proyectos de Inversión enlace https://spi.dnp.gov.co vigencia 2020, que presentan retraso en la ejecución de las actividades programadas para los productos.<br>Se esta incumpliendo el numeral 3 "*Formular, decidir oportunamente o ejecutar los planes de desarrollo y los presupuestos, y cumplir las leyes y normas que regulan el manejo de los recursos económicos públicos, o afectos al servicio público*." Ley 734 de 2002 "*por la cual se expide el Código Disciplinario Único, Artículo 34. Deberes. Son deberes de todo servidor público:*". Lo que puede con llevar a recorte presupuestal por falta de ejecución. Situación que puede conllevar a la posible materialización de riesgos de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC en la vigencia 2020 impactando la gestión de la disponibilidad de recursos necesarios para alcanzar los objetivos institucionales y cumplir las funciones delegadas. | 23 |

Fuente: Elaboración propia del auditor.

## Verificar el Sistema de Control Interno del proceso Gestión TICS.

## Prueba Realizada

Se verifico el cumplimiento del objetivo y del alcance del proceso Transversal Gestión de TICS acorde con lo publicado en la cadena de valor y su caracterización.

No se evidenció publicación del Plan Estratégico de Tecnologías de la Información - PETI, Plan Estratégico de Seguridad de la Información - PESI, Plan de contingencia de TI, ni Plan de tratamiento de riesgos TI.

**Situaciones evidenciadas**
El Auditor evidenció en la cadena de valor de la Entidad, el objetivo y el alcance del Proceso Transversal Gestión de TICS:

1. **OBJETIVO:** "*Disponer e implementar políticas, estándares y soluciones tecnológicas seguras y de calidad que contribuyan al cumplimiento de los objetivos estratégicos de la entidad, generen valor y soporten los procesos, trámites y servicios de la Superintendencia de Transporte.*"

2. **ALCANCE:** "*Inicia con la construcción del Plan Estratégico de las Tecnologías de la Información y Comunicaciones – PETIC y el PESI en donde se plantea los lineamientos y proyectos en materia de gestión de TI, Transformación Digital, y Seguridad de la Información asociados a todos los dominios de la Arquitectura Empresarial: gestión de TI, gobierno de TI, sistemas de información, infraestructura tecnológica, seguridad digital. Luego se definen políticas, estándares y buenas prácticas de gestión de TI y seguridad, posteriormente se implementa las políticas definidas y se estructuran y ejecutan proyectos, luego se define e implementa un modelo de gobierno de TI sobre los proyectos y la operación de TI, paralelamente se presta soporte y mantenimiento a los sistemas de información e infraestructura y se evalúa todo el proceso dentro de la mejora continua. Desde el proceso de gestión de TI, se garantiza que la infraestructura y los soluciones para la gestión estratégica de información se encuentren disponibles.*"

Se evidenció que el objetivo y el alcance del proceso transversal Gestión de TICS se encuentran alineados con los objetivos estratégicos: Fortalecer las Tecnologías de la Información y las Comunicaciones, y Fortalecimiento Institucional del PEI y PAI, los cuales contemplan los seguimientos a las metas para la vigencia 2020.

Sin embargo, al realizar el seguimiento a la ejecución del objetivo y alcance del proceso no esta alineado, no se observó la actualización anual como lo propone la guia elaborada por MinTIC: G.ES.06. Guía cómo estructurar el Plan Estratégico de Tecnologías de la Información – PETI, numeral 2.2 Alcance del documento "*Se describe claramente el alcance del PETI teniendo en cuenta que debe proyectarse a máximo cuatro años y debe actualizarse cada año. El alcance del PETI debe indicar lo que efectivamente debe lograr la Entidad durante la vigencia del PETI. (…)*", y al realizar el seguimiento al alcance del PETI publicado para el cuatrenio 2017 - 2020 en el que se debe adopto la actualización anual, esta no se evidenció la publicación en la web de la Entidad, "*El alcance de estos documentos es describir la estrategía de ejecución de los proyectos de Tecnologías de la Información en la Superintendencia de Puertos y Transporte* ***durante el período 2017-2020 haciendo una actualización anual****, con el fin de mejorar la gestión y cumplimiento de los objetivoss estratégicos de la Entidad, Vigilancia, Inspección y Control alineados con la estrategía sectorial Transportte Nacional*"."."

Tambien, se observó en el objetivo "***6.2 Verificar los proyectos de inversión de la OTIC."*** de este informe, la falta de ejecución de los proyectos de inversión relacionados en el Sistema de Seguimiento a Proyetos de Inversión (SPI.gov.co).

Se observó que los objetivos especificos del PETI versión 2.0 de 07/12/2017
“

- *Organizar la Gestión de TIC de la entidad a través de la Estratégia GEL y Arquitectura Empresarial TI.*
- *Diseñar el diagnostico de la entidad frente a los seis dominios del Marco de Referencia TI.*
- *Establecer una infraestructura de Tecnologías de la Información donde permita tener disponibilidad, confidencalidad de integridad respecto al manejo de la información.*
- *Implementar la Arquitectura Empresarial bajo los criterios establecidos por Gobierno en Línea.*
- *Extender la capacidad de la prestación de servicios ofrecidos a través de la infraestructura tecnológica de la entidad generando un valor agregado con la ciudadania.*
- *Establecer el mapa de ruta para el desarrollo del PETI en la Supertransporte.*
- *Establecer a un alto nivel de seguridad y privacidad de la Información.*
- *Implementar un proceso de mejora continuua en la implementación de procesos de TI.*”

se encuentran desalineados con la normativa emitidad por MINTIC, el PETI esta elaborado bajo la estratégia Gobierno en Línea – GEL, no se evidenció la transición a la Estratégia Gobierno Digital, Decreto 1008 de 14 de junio de 2018 “*Por el cual se establecen los lineamientos geenrale de la política de Gobierno Digital y se subroga el capítulo 1 del titulo 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*”, ni la Arquitectura Empresarial – AE de la transición a la Estratégia Gobierno Digital como lo indica la guia G.ES.06. de MINTIC.

Igualmente, no se evidenció publicado en la página web de la Entidad el Plan Estratégico de Seguridad de la Información – PESI, Plan de contingencia de TI, ni el Plan de tratamiento de riesgos de TI para la vigencia 2020.

Se evidenció en correo Institucional allegado el día jueves 26/11/2020 19:04, que el PETI sera presentado en el próximo Comité de Gestión y Desempeño para revisión :

“*De acuerdo con la solicitud realizada por correo electrónico el día 25 de noviviembre, remitimos los siguientes avances:*

- *PETI: Según lo acordado en el comité de Gestión y Desampeño del mes de noviembre, el documento será presentado en el próximo comité de Gestión y Desempeño para revisión.*
- *PESI: Se realizó desde la OTIC la generación del Plan Estratégico de Seguridad de la Información. Se adjunta Documento.*
- *Plan de tratamiento de riesgos TI: Desde OTIC se realiza con el seguimiento a los riesgos del proceso de Gestión TIC, de acuerdo con la periodicidad definida para el seguimiento a las matrices de riesgos de la entidad. El plan de tratamiento de riesgos que se sigue en la OTIC corresponde a lo definido en el Plan de tratamiento de riesgos de la entidad.*

- *Plan de tratamiento de riesgos de TI: en la presente vigencia se encuentra en revisión el Plan de desastres del 2019, de acuerdo con las necesidades actuales de la entidad y los cambios previstos."*

El Auditor evidenció documento borrador PESI denominado PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PESI V7.docx allegado por la OTIC, en el cual el objetivo general y el alcance del Plan Estratégico de Seguridad y Privacidad de la Información – PESI Vigencia 2020-2022:
Objetivo General: "*Establecer el conjunto de proyectos de seguridad y privacidad de la información de la Superintendencia de Transporte, con el fin de contribuir y mejorar la seguridad y privacidad de la información en la entidad para el periodo 2020-2022*"
Alcance: "*Definir la hoja de ruta de proyectos que debe seguir la Oficina de Tecnologías de la Información - OTIC para el periodo 2020-2022 con el propósito de adelantar las acciones y planes de trabajo que permitan ejecutar la política de seguridad y privacidad de la información y avanzar en la implementación en el Modelo de Seguridad y Privacidad de la Información en la Superintendencia de Transporte para salvaguardar la seguridad y privacidad de los activos de información.""*, se encuentran alineados con los objetivos estratégicos de la Entidad "*Fortalecimiento Institucional, y Fortalecer las Tecnologías de la Información y las Comunicaciones*" se encuentran alineados, sin embargo, el PESI no ha sido aprobado para la vigencia 2020 y de acuerdo a la periodicidad 2020-2022 deberia estar adoptado por una resolución, publicado en la página Web de la Entidad y evaluandose la gestión de esta vigencia.

En el documento borrador del PESI se observó que los controles de seguridad del documento solo son enunciados, no informan en que consiste y como se ejcutan, para los controles de seguridad de los datos e información realizan una breve explicación de los componentes y relacionan que controles se realizan, no informan en que consisten, en la política de seguridad y privacidad de la información enuncian los lineamientos, no relacionan el enlace donde se pueden consultar.

Los proyectos del PESI son solamente nombrados, no detallan en que consisten y el estado de ejecución en el que se encuentran.

**Hallazgo 001 de 2020 (AC Acción Correctiva)**
**H01A-07dicv20-(AC)GTICS**
El documento de las actualizacioes anuales del Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, no se encuentran publicado en la página web de la Superintendencia de Transporte.
Se incumple la guia elaborada por MinTIC: G.ES.06. Guía cómo estructurar el Plan Estratégico de Tecnologías de la Información – PETI, numeral 2.2 Alcance del documento "*Se describe claramente el alcance del PETI teniendo en cuenta que debe proyectarse a máximo cuatro años y debe actualizarse cada año. El alcance del PETI debe indicar lo que efectivamente debe lograr la Entidad durante la vigencia del PETI. (…)*".
Se incumple el alcance del PETI publicado para el cuatrenio 2017 - 2020 en el que se debe adopto la actualización anual, esta no se evidenció la publicación en la web de la Entidad, "*El alcance de estos documentos es describir la estrategia de ejecución de los proyectos de Tecnologías de la Información en la Superintendencia de Puertos y Transporte* ***durante el período 2017-2020 haciendo una actualización anual****, con el fin de mejorar la gestión y*

*cumplimiento de los objetivoss estratégicos de la Entidad, Vigilancia, Inspección y Control alineados con la estrategía sectorial Transportte Nacional*".".
Se incumple el Artículo 2.2.22.3.14*. "Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: (…).*
Se incumple el numeral e. "*Asegurar la oportunidad y confiabilidad de la información y de sus registros*;", y numeral f. "*Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos;",* del Artículo 2º.- *"Objetivos del sistema de Control Interno. Atendiendo los principios constitucionales que debe caracterizar la administración pública, el diseño y el desarrollo del Sistema de Control Interno se orientará al logro de los siguientes objetivos fundamentales:* ", Ley 87 de 1993.
Situación que puede conllevar a la posible materialización de riesgos de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC en la vigencia 2020 impactando la gestión de la disponibilidad de recursos necesarios para alcanzar los objetivos institucionales y cumplir las funciones delegadas.

**Hallazgo 002 de 2020 (AC Acción Correctiva)**
**H02A-07dicv20-(AC)GTICS**
El documento Plan Estratégico de Seguridad de la Información - PESI, Plan de contingencia de TI , ni el Plan de tratamiento de riesgos de TI se encuentran publicados en la página web de la Superintendencia de Transporte a la fecha.
Se incumple el Artículo 2.2.22.3.14*. "Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: (…).*
Se incumple el numeral e. "*Asegurar la oportunidad y confiabilidad de la información y de sus registros*;", y numeral f. "*Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos;",* del Artículo 2º.- *"Objetivos del sistema de Control Interno. Atendiendo los principios constitucionales que debe caracterizar la administración pública, el diseño y el desarrollo del Sistema de Control Interno se orientará al logro de los siguientes objetivos fundamentales:* ", Ley 87 de 1993.
Situación que puede conllevar a la posible materialización de riesgos de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC en la vigencia 2020 impactando la gestión de la disponibilidad de recursos necesarios para alcanzar los objetivos institucionales y cumplir las funciones delegadas.

3. **Líder:** Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones.

Se evidenció que el responsable del Proceso Transversal Gestión TICS que aparece en la caracterización no labora en la Entidad.

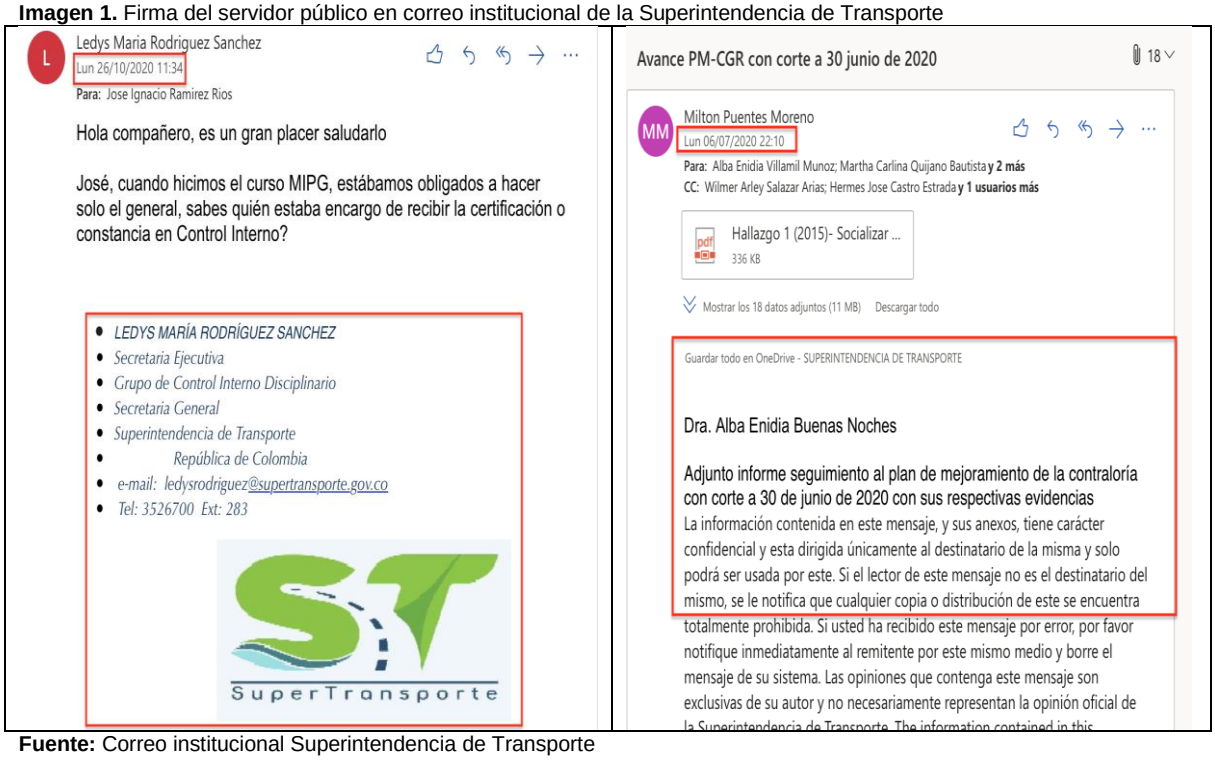
4. **Ciclo PHVA:** Descripción del Proceso Transversal Gestión de TICS.

Se observó las herramientas fundamentales para la gestión por procesos:

5. Documentos de referencia Internos (Manuales, instructivo y formatos) (según selectivo).

El auditor evidenció en el instructivo TIC-IN003 Instructivo Firma Correo Electrónico, que no se esta cumpliendo el objetivo "*Este documento indica los pasos necesarios para que cada funcionario pueda actualizar la firma y logo utilizados en el correo electrónico"*, el Alcance "*Este instructivo aplica para todo los funcionarios y contratistas que tengan correo electrónico con el dominio de la Superintendencia de Transporte.*", el numeral "*3. Desarrollo de las actividades (…)*", en el instructivo no se evidenció enlace para que el servidor público realice el proceso, de instalar la firma en el correo institucional, se observó incumplimiento en la aplicación del instructivo Firma Correo Electrónico por parte de los servidores públicos para que realicen el proceso de la firma del correo institucional, no se observó seguimiento por parte de la OTIC a los servidores públicos del uso de la firma en el correo institucional . Ver Imagen 1.

**Imagen 1.** Firma del servidor público en correo institucional de la Superintendencia de Transporte




**Fuente:** Correo institucional Superintendencia de Transporte

6. Indicadores de proceso
   Se evidenció ficha técnica firmada por los responsables, el objeto del proceso "Mantener actualizada la Superintendencia de Transporte con herramientas de últimas tecnologías en

cuanto a hardware y software" no esta alineado con el indicador Nivel de satisfacción *"(No de solicitudes atendidas / No de Solicitudes recibidas) * 100*".

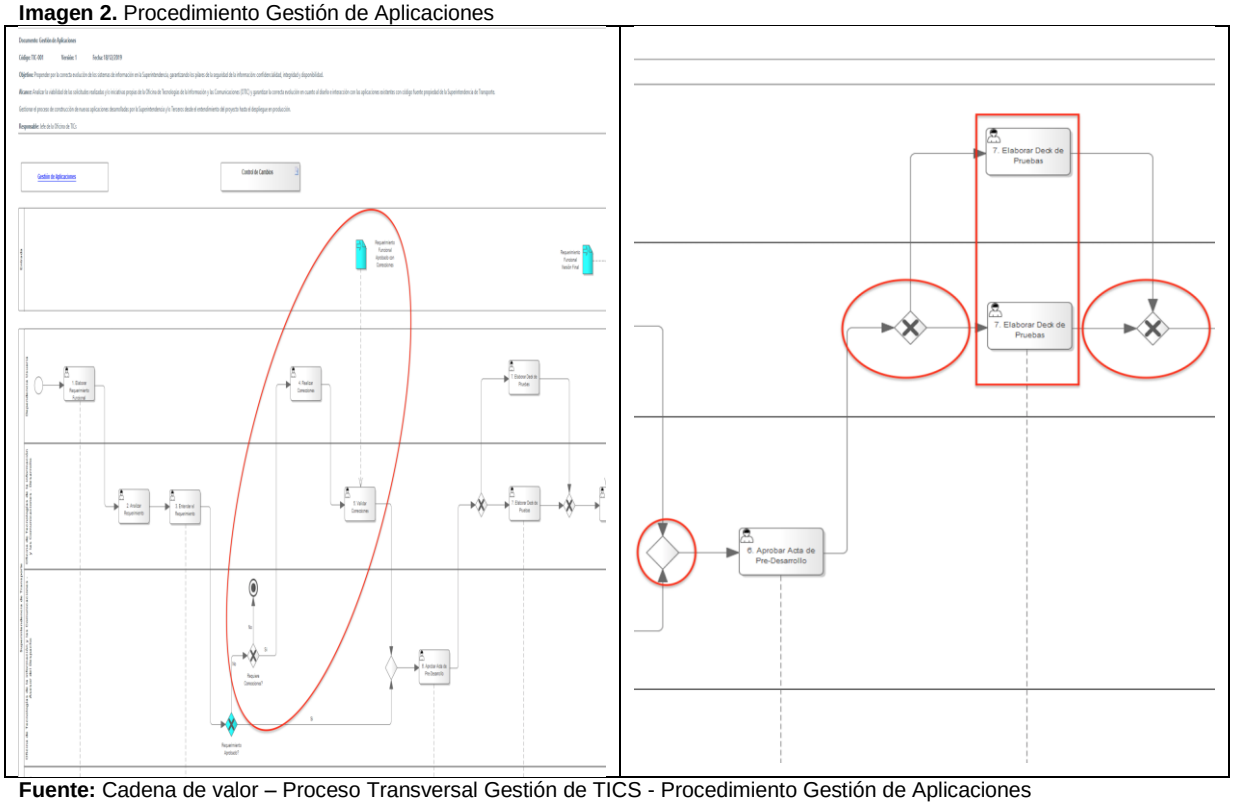
7. Documento firmado de la caracterización.

8. Procedimientos (según selectivo)

   Gestión de Aplicaciones: El auditor evidenció en el diagrama BMPN: si el proceso requiere correcciones, realiza correcciones (actividad 4. Realizar correcciones), valida correcciones (actividad 5. Validar correcciones) y continua el proceso. Después de realizar las correcciones el proceso debe retornar para verificarlo si requiere nuevas correcciones o continua. Si el proceso se va por la condición del no este finaliza, por esta opción el proceso debería continuar para ser desarrollado e implementado.

   Al continuar el proceso se realizan validaciones que les falta ser documentadas e independiente por la opción que tome Si o No, realiza la misma actividad. Ver Imagen 2.

**Imagen 2.** Procedimiento Gestión de Aplicaciones



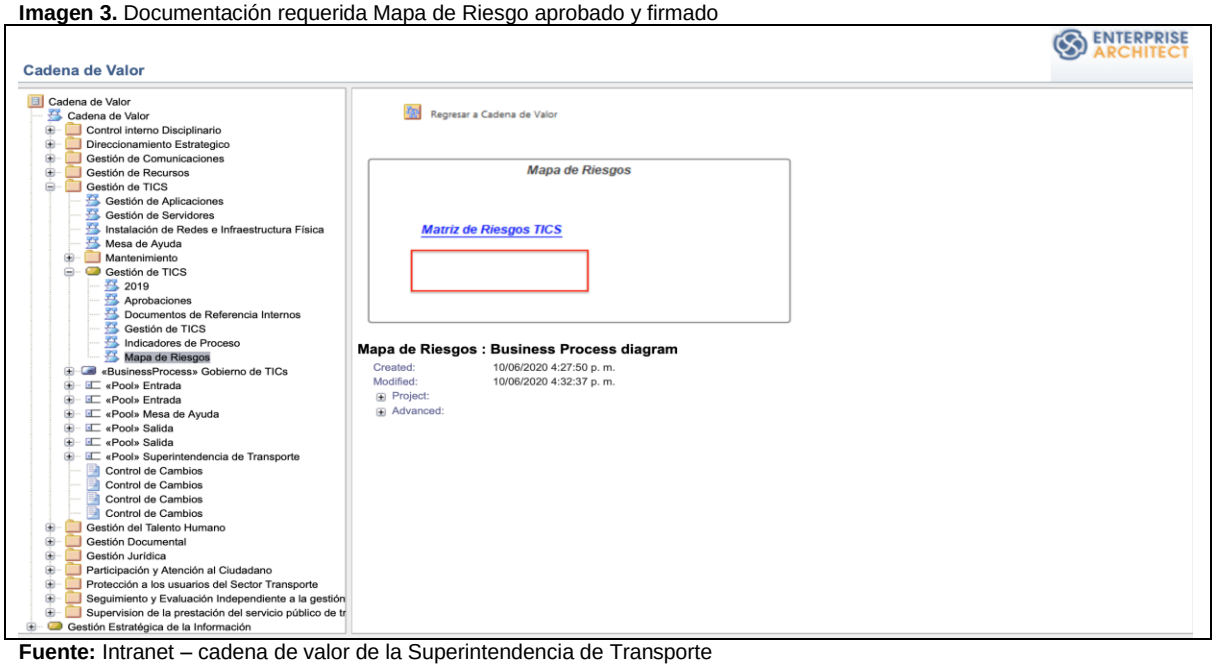

**Fuente:** Cadena de valor – Proceso Transversal Gestión de TICS - Procedimiento Gestión de Aplicaciones

9. Mapa de Riesgos (según selectivo)
   El auditor evidenció desactualización en el campo responsable. En la información que contempla el control externo, el ítem procesos "*Procesos: <u>En la cadena de valor se encuentra identificado como proceso de apoyo</u>, es necesario continuar su documentación e implementación del modelo de seguridad y privacidad de la información*.", El proceso de Gestión de TICS es un Proceso Transversal y no de apoyo.

Se evidenció gestión en la ejecución de los riegos de seguridad digital con la implementación de herramientas que realizan controles de acceso no autorizados desde fuera de la red de la Entidad como son la doble autenticación, seguimiento a IPs dudosas, filtros de acceso realizado por el aplicativo FORTINET y los reportes de alerta que genera.

No se evidenció en opción Mapa de Riesgos el documento del mapa de riesgo firmado por los responsables, solo se observó la matriz del mapa de riesgo en Excel. Ver Imagen 3.

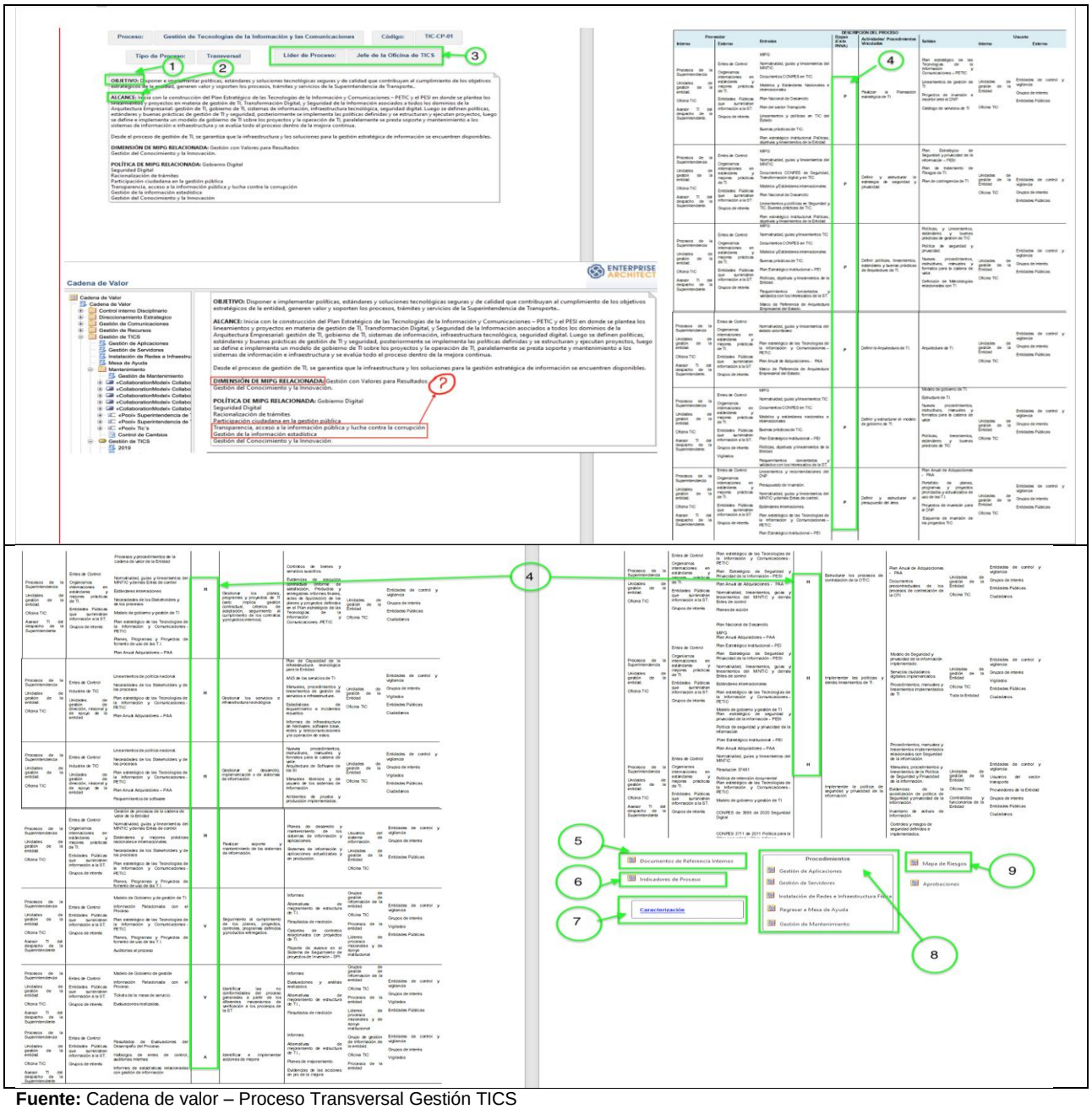
**Imagen 3.** Documentación requerida Mapa de Riesgo aprobado y firmado




**Fuente:** Intranet – cadena de valor de la Superintendencia de Transporte

El auditor evidenció en la caracterización que se alinearon dos políticas sin adoptar la dimensión a la cual corresponde (Política Gestión de la Información Estadística y Política Transparencia, acceso a la información pública y lucha contra la corrupción, estas corresponden a la 5a Dimensió: Información y Comunicación). Ver Imagen 4.

**Imagen 4.** Caracterización del Proceso Transversal Gestión TICS.




**Fuente:** Cadena de valor – Proceso Transversal Gestión TICS

## Inventario de Aplicaciones de la OTIC – ST

El auditor evidenció en el inventario de aplicaciones que la Oficina de Tecnologías de las Comunicaciones administra 8 aplicativos de apoyo: 3 fabricados en casa y 5 externos.

De los aplicativos de apoyo: El aplicativo TAUX la Entidad no cuenta con los derecho sobre el código fuente, mientras que sobre los aplicativos Orfeo, Nómina, Glpi, Digiturno, Consola TAUX, Solicitud de Usuarios, Biblioteca Virtual la Superintendencia de Transporte tiene o adquirio los derecho sobre el código Fuente.

Los aplicativos que no cuentan con arquitectura tecnológica WEB son: Digiturbo y TAUX, presentan interoperatividad con otros aplicativos internos el GLPI con OCS y se estan realizando acuerdos para el aplicativo consola TAUX con PSE para interoperatividad externa.

De los 12 aplicativos misionales, 9 son fabricados en casa y 3 externos, los aplicativos misionales sobre los que la Entidad no tiene derecho del código fuente es el VIGIA, los aplicativos Temis sgl, fuentes externas, connecta, matriz de investigación, trámites, consultas. Tránsito, organismos de apoyo, puertos,formularios, bioseguridad (saspro), sala de audiencia y rutas son propiedad de la Superintendencia tde Transporte el código Fuente.

Los aplicativos que no cuentan con arquitectura tecnológica WEB es SALA DE AUDIENCIA. Presentan interoperatividad con otros aplicativos internos: TEMIS con VIGIA, TRÁMITES con VIGIA y ORFEO, y SASPRO con VIGIA. El aplicativo con interoperatividad externa la consola TRÁMITES.

Los aplicativos sobre los que la Entidad cuenta con los derecho del código fuente se pueden adaptar o realizar reingenieria de acuerdo a las nuevas necesidades del momena. Ver Imagen 5.

**Imagen 5.** Inventario de aplicaciones de la Superintendnecia de Transporte -ST OTIC

**Oficina de Tecnologías de la Información y las Comunicaciones**
**Inventario activos de información - Sistemas de Información**
**fecha del documento: Octubre 2020**

| Categoria | Cantidad | Estado | Aplicativos | FABRICANTE | Derechos Código Fuentes - DCF | Arquitectura tecnológica | Integrado con otros SI internos | SI Externos con los que interopera |
|---|---|---|---|---|---|---|---|---|
| Sistema de Apoyo | 8 | 8 - Activos | ORFEO<br>HEINSOHN NÓMINA<br>GLPI<br>DIGITURNO<br>CONSOLA TAUX<br>SOLICITUD USUARIOS<br>BIBLIOTECA VIRTUAL<br>TAUX | 3 - Internos<br>5 - Externos | 7 - DCF<br>1 - NDCF (TAUX) | 6 - WEB<br>2 - N. A.<br>(DIGITURNO,TAUX) | GLPI - OCS | CONSOLA TAUX - PSE<br>(próximamente) |
| Sistema Misional | 12 | 10 - Activos<br>2 - Inactivos | VIGIA<br>TEMIS SGL<br>FUENTES EXTERNAS<br>CONNECTA<br>MATRIZ DE INVESTIGACIONES<br>TRÁMITES<br>CONSULTAS TRÁNSITO<br>ORGANISMOS DE APOYO<br>PUERTOS<br>FORMULARIOS<br>BIOSEGURIDAD (SASPRO)<br>SALA DE AUDIENCIA (I)<br>RUTAS (I) | 9-Internos<br>3 - Externos | 11 - DCF<br>1 - NDCF (VIGIA) | 11 - WEB<br>1 - N.A.<br>(SALA DE AUDIENCIA) | TEMIS SGL - VIGIA<br>TRÁMITES - VIGIA, ORFEO<br>SASPRO - VIGIA | TRÁMITES |

**Fuente:** Análisis Auditor de la Oficina de Control Interno

## Recomendaciones

- Revisar la alineación de la dimensión con sus correspondientes políticas del Modelo Integrado de Planeación y Gestión – MIPG que se encuentran en la caracterización del Proceso Transversal Gestión de TICS de la Entidad.
- Actualizar en la caracterización el responsable del Proceso Transversal Gestión de TICS.
- Revisar y ajustar el procedimiento para ser ejecutado el instructivo TIC-IN003 Instructivo Firma Correo Electrónico desde la intranet.
- Revisar el procedimiento Gestión de Aplicaciones.
- Implementar los aplicativos con arquitectura tecnológica WEB.

- Evaluar la viabilidad de adquirir una solución que remplace el aplicativo TAUX, porque no se dispone de soporte del proveedor para satisfacer las necesidades del usuario de la Entidad, ni de ley.
- Relacionar las resoluciones que adoptaron las políticas: Política de Gestión de Riesgos, Política de protección de datos personales, Política de Seguridad y privacidad de la información.
- Revisar el indicador de los numerales 6.10 Implementación de firmas digitales, 6.12 Implementación de estampados cronológicos, 6.13 Establecer sistema centralizado para actualizaciones de estaciones de trabajo y servidores, 6.14 Implementar correlacionador de eventos de seguridad, 6.16 Ejecutar Pruebas de ethical hacking, 6.17 Mitigación de eventos de Ingeniería social plan de seguridad y privacidad de la informacion - pesi v7.
- Informar como se alinean con el PETI los numerales 6.10, 6.11, 6.12, 6.13, 6.14, 6.15, 6.16, 6.17 del plan de seguridad y privacidad de la informacion - pesi v7.

### 6.1 Verificar las actividades del PEI y PAI con corte 30 de octubre de 2020.

**Prueba Realizada**
El auditor verificó los objetivos estratégicos del PAI a octubre de 2020

**Prueba Realizada**
El auditor verificó los objetivos estratégicos del PAI a octubre – OTIC, en la página web de la Superintendencia de Transporte, botón de transparencia, planes Institucionales.

**Situaciones evidenciadas**
El auditor evidenció ocho indicadores en el archivo Excel denominado PAI-PEI-3erTrmstre2020.xlsx, con corte tercer trimestre de la vigencia 2020 de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, donde no existe un universo (alcance periódico) contra el cual se mida la gestión como se muestra a continuación:

- Aprobación de Estudios Previos Definitivos.
- % Avance en el Mejoramiento del Data Center.
- % Implementación de APP PQRS de la ST
- % implementación de PETIC.
- % de Implementación de ISO 27001 para el Sistema de gestión de Seguridad de la Información.
- # Datos abiertos Certificados en la ruta de excelencia.
- # Datos abiertos Certificados en la ruta de excelencia.
- Entregar y Aprobar Política de Seguridad de la Información.

Igualmente, se evidenció en las actividades alineadas a las metas y objetivos estratégicos del Plan de Acción Institucional – PAI de la Entidad con corte octubre de 2020 lo siguiente:

**OE2 Fortalecer las Tecnologías de la Información y las Telecomunicaciones**

**Avance del 0% - 3 Actividades,** el auditor evidenció incumplimiento en la ejecución de las actividades:

- Proceso de Contratación. Planeado 0%, Ejecutado 0%
- Alinear un Proceso en ISO 27001 para el Sistema de Gestión de la Seguridad de la Información y postularlo a Certificación. Planeado 40%, Ejecutado 0%.
- Actualizar modelo de continuidad de negocio - Servicios TICS.

**Avance del 10% - 1 Actividad,** el auditor evidenció incumplimiento en la ejecución de la actividad:

Planeado 100%. Ejecutado 10%
- Elaborar Evaluación Técnica de las Ofertas.

**Avance del 40% - 1 Actividad,** El auditor evidenció cumplimiento en la ejecución de la actividad:

Planeado 40%. Ejecutado 40%
- Poner en producción la Fase 2 Implementación Sistema Único de Trámites.

**Avance del 50% - 2 Actividades,** el auditor evidenció cumplimiento en la ejecución de las actividades:

Planeado 50%. Ejecutado 50%
- Implementación de aplicación móvil (APP) para Recepción, Radicación y Consulta de PQRSD en línea.
- Documento PETI implementado para ST y alineado al Sector."

**Avance del 50% - 2 Actividades,** el auditor evidenció cumplimiento en la ejecución de las actividades:

Planeadas a octubre 1. Ejecutadas a octubre 1
- Apoyar el proceso de actualización de datos abiertos de la entidad.
- Efectuar los mantenimientos preventivos a los servicios tecnológicos de la Entidad necesarios para soportar sus procesos, asegurar la continuidad en la operación TI, su disponibilidad y rendimiento.

**Avance del 60% - 3 Actividades,** el auditor evidenció cumplimiento en la ejecución de las actividades:

Planeado 60%. Ejecutado 60%
- Evaluación Continua de herramientas de desarrollo
- Inteligencia de negocios - Elaborar 10 Tableros de Control con información de Fuentes Externas e Internas
- Implementar Sistema de Gestión del Conocimiento

**Avance del 70% - 1 Actividad,** el auditor evidenció cumplimiento en la ejecución de la actividad:
Planeado 70%. Ejecutado 70%
- Adquisiciones de DATACENTER - Centro de Información.

**Avance del 75% - 1 Actividad,** el auditor evidenció cumplimiento en la ejecución de las actividades:

Planeado 75%. Ejecutado 75%
- Fortalecer la estructura Vigía y realizar Cambios de módulos de Capa de Aplicación.

**Avance del 80% - 10 Actividades,** el auditor evidenció cumplimiento en la ejecución de las actividades:

Planeado 80% Ejecutado 80%
- Levantar procesos y estructurar el sistema
- Desarrollar e implementar las soluciones
- Actualizar e Implementar de Política de Seguridad de la Información y Protección de Datos Personales
- Implementar avances en el modelo de Seguridad y Privacidad de la información - MSPI
- Actualización de activos de información, matriz de riesgos de TIC y verificación de aplicación de controles.
- Implementar el Software de Almacén (Probable Interfaz con el SIIF)
- Evaluar mejoras del software de Inteligencia de Negocios de acuerdo con las necesidades de la entidad y del sector.
- Desarrollar e implementar el sistema de notificación electrónica fase I-IUIT, fase II - Transversal, y para notificaciones personales usar dispositivos biométricos que interactúen los sistemas de información de la entidad junto a la Registraduría para validar la identidad del notificado.

- Actualizar la Política de Seguridad de la Información de la Entidad. Planeado a octubre de 2020 el 100%, ejecutado 80%. El auditor evidenció incumplimiento en la ejecución de la actividad.

- Implementar la Transformación Digital y Desmaterialización de trámites. Planeado a octubre de 2020 el 90%, ejecutado 80%. El auditor evidenció incumplimiento en la ejecución de la actividad.

**Avance del 90% - 2 Actividades,** el auditor evidenció cumplimiento en la ejecución de las actividades:

Planeado 90%. Ejecutado 90%
- Realizar pruebas
- Implementar protocolo IPV6

**Avance del 100% - 5 Actividades,** el auditor evidenció cumplimiento en la ejecución de las actividades:

- Elaborar términos de referencia
- Validar decisión para actualizar o implementar el nuevo Sistema de Gestión Documental.
- Elaborar y entregar de los Estudios Previos.
- Efectuar mantenimiento software GLPI

- Definir el futuro del sistema Misional VIGIA mediante mesas de trabajo con las áreas involucradas.

**OE5 Fortalecimiento Institucional**

**Avance del 80% - 1 Actividad,** el auditor evidenció cumplimiento en la ejecución de las actividades:

Planeadas 2020 37
Planeadas 28. Ejecutadas 28
- Gestión Quejas, Reclamos, Solicitudes y Denuncias.

Ver Imagen 6.

**Imagen 6.** Indicadores de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC

| OBJETIVOS | CANTIDAD ATIVIDADES | Total Planeado | % Planeado a octubre de 2020 | % Avance Ejecutado a octubre de 2020 | % Cumplimiento corte octubre de 2020 | % Cumplimirento Planeado vs. Ejecutado 2020 | Observaciones de la OCI |
|---|---|---|---|---|---|---|---|
| OE2 Fortalecer las Tecnologías de la Información y las Telecomunicaciones. | 3 | 100% | 47% | 0% | 0% | 0% | 0%,40%,100%<br>**3 Actividades - 0%**<br>- Proceso de Contratación. **Planeado 0%, Ejecutado 0%**<br>- Alinear un Proceso en ISO 27001 para el Sistema de Gestión de la Seguridad de la Información y postularlo a Certificación. **Planeado 40%, Ejecutado 0%.**<br>- Actualizar modelo de continuidad de negocio - Servicios TICS. **Planeado 100%, Ejecutado 0%.** |
| | 1 | 100% | 100% | 10% | 10% | 10% | **1 Actividad - 10%**<br>**Planeado 100%. Ejecutado 10%**<br>- Elaborar Evaluación Técnica de las Ofertas. |
| | 1 | 100% | 40% | 40% | 100% | 40% | **1 Actividad - 40%**<br>**Planeado 40%. Ejecutado 40%**<br>- Poner en producción la Fase 2 |
| | 2 | 100% | 50% | 50% | 100% | 50% | **2 Actividades - 50%**<br>**Planeado 50%. Ejecutado 50%**<br>- Implementación de aplicación móvil (APP) para Recepción, Radicación y Consulta de PQRSD en línea.<br>- Documento PETI implementado para ST y alineado al Sector. |
| | 2 | 100% | 50% | 50% | 100% | 50% | **2 Actividades - 50%**<br>Planeadas 2020 2<br>**Planeadas a sep 1. Ejecutadas a sep 1**<br>- Apoyar el proceso de actualización de datos abiertos de la entidad.<br>- Efectuar los mantenimientos preventivos a los servicios tecnológicos de la Entidad necesarios para soportar sus procesos, asegurar la continuidad en la operación TI, su disponibilidad y rendimiento. |
| | 3 | 100% | 60% | 60% | 100% | 60% | **3 Actividades - 60%**<br>**Planeado 60. Ejecuatado 60%**<br>- Evaluación Continua de herramientas de desarrollo<br>- Inteligencia de negocios - Elaborar 10 Tableros de Control con información de Fuentes Extenas e Internas<br>- Implementar Sistema de Gestión del Conocimiento |
| | 1 | 100% | 70,00% | 70% | 100,00% | 70% | 1 Actividades -70%<br>**Planeado 70% Ejecutado 70%**<br>- Adquisiciones de DATACENTER - Centro de Información. |
| | 1 | 100% | 75% | 75% | 100% | 75% | **1 Actividades -75%**<br>**Planeado 75%. Ejecutado 75%**<br>- Fortalecer la estructura Vigía y realizar Cambios de módulos de Capa de Aplicación. |
| | 10 | 100% | 80% | 80% | 100% | 80% | **10 Actividades - 80%**<br>**Planeado 80% Ejecutado 80%**<br>- Levantar procesos y estructurar el sistema<br>- Desarrollar e implementar las soluciones<br>- Actualizar e Implementar de Política de Seguridad de la - Información y Protección de Datos Personales<br>- Implementar avances en el modelo de Seguridad y Privacidad de la información - MSPI<br>- Actualizacion de activos de información, matriz de riesgos de TIC y verificación de aplicación de controles.<br>- Implementar el Software de Almacén (Probable Interfaz con el SIIF)<br>- Evaluar mejoras del software de Inteligencia de Negocios de acuerdo a las necesidades de la entidad y del sector.<br>- Desarrollar e implementar el sistema de notificación electrónica fase I-IUIT, fase II - Transversal, y para notificaciones personales usar dispositivos biométricos que interactúen los sitemas de información de la entidad junto a la Registraduría para validar la identidad del notificado.<br><br>- Actualizar la Política de Seguridad de la Información de la Entidad. **Planeado a octubre de 2020 el 100%, ejecutado 80%.**<br>- Implementar la Transformación Digital y Desmaterialización de trámites. **Planeado a octubre de 2020 el 90%, ejecutado 80%.** |
| | 2 | 100% | 90% | 90% | 100% | 90% | **2 Actividades -90%**<br>**Planeado900%. Ejecutado 90%**<br>- Realizar pruebas<br>- Implementar protocolo IPV6 |
| | 5 | 100% | 100% | 100% | 100% | 100% | **5 Actividades -100%**<br>**Planeado 100%. Ejecutado 100%**<br>- Elaborar términos de referencia<br>- Validar decisión para actualizar o implementar el nuevo Sistema de Gestión Documental.<br>- Elaborar y entregar de los Estudios Previos.<br>- Efectuar mantenimiento software GLPI<br>- Definir el futuro del sistema Misional VIGIA mediante mesas de trabajo con las áreas involucradas |
| Avance OE2 a corte octubre, vigencia 2020 | 31 | 100% | 69% | 57% | 83% | 57% | |
| OE5 Fortalecimiento Institucional | 1 | 100% | 75,68% | 75,68% | 100% | 76% | **1 Actividades -80%**<br>Planeadas 2020 37<br>**Planeadas a sep 28. Ejecutadas a sep 28**<br>- Gestión Quejas, Reclamos, Solicitudes y Denuncias. |
| Avance OE5 a corte octubre, vigencia 2020 | 1 | 100% | 76% | 76% | 100% | 76% | |
| **Avance a corte octubre, vigencia 2020** | **32** | **100%** | **72%** | **66%** | **91%** | **66%** | |

**Fuente:** Auditor Oficina de Control Interno – OCI

## Recomendaciones

1. Revisar la formulación de los indicadores relacionados donde se defina el alcance periódico (universo contra el cual se va a medir).
2. Revisar y trazar contingencia para las actividades que presentan retraso.

### 6.2 Verificar los proyectos de inversión de la OTIC.

**Prueba Realizada**
Se verificó la ejecución inversiones en sistema de seguimiento a proyectos de inversión, enlace: https://spi.dnp.gov.co/Consultas/ResumenEjecutivoEntidad.aspx?id=img_Por%20Entidad, los proyectos Fortalecimiento a la supervisión integral a los vigilados a nivel nacional y Mejoramiento de la gestión y capacidad institucional para la supervisión integral a los vigilados a nivel nacional.

**Situaciones evidenciadas**

El auditor evidenció los proyectos de inversión para el objetivo estratégico Fortalecer las Tecnologías de la Información y las Telecomunicaciones.

**Objetivo del proyecto de inversión:** Aumentar la eficiencia y calidad en la gestión de los procesos de apoyo de la Superintendencia de Transporte.

**Proyecto de inversión Código 2018011000653** - Mejoramiento de la gestión y capacidad Institucional para la supervisión integral a los vigilados a nivel nacional:

**Programa:** Fortalecimiento de la gestión y dirección del Sector Transporte.

**Objetivos Específicos**: Contar con la Arquitectura tecnológica suficiente.

- **Producto:** Servicios de información actualizados.

**Cumplimiento:** 40%
Se observó que a la fecha el monto obligado es de ciento veintisiete millones trecientos mil trescientos cincuenta y ocho pesos ($127.300.358), habiéndose presupuestado un total de tres mil ochocientos once mil millones de pesos ($3.811.000.000), discriminado como se muestra a continuación:

1. Desarrollar, optimizar y/o adquirir software ($1.648.000.000), obligado ($0).
2. Contar con servicios informáticos conexos ($515.000.000), obligado ($0).
3. Operar el aplicativo misional a través de servicios de hosting ($154.500.000), obligado ($0).

Actividad: Contar con la prestación de servicios de apoyo, presupuesto mil cuatrocientos noventa y tres millones quinientos mil pesos ($1.493.500.000) y a la fecha solo se ha obligado ciento veintisiete millones trecientos mil trecientos cincuenta y ocho pesos ($127.300.358).
El presupuesto disponible para la ejecución del producto Servicios de información actualizado es de tres mil ocho cientos once millones de pesos ($3.811.000.000), a la fecha se ha obligado ciento veitisiete millones trescientos mil trescientos cincuenta y ocho pesos **(**$127.300.358), equivalente al 3.34%.

- **Producto:** Servicios tecnológicos

**Cumplimiento:** 5%
Se observó que a la fecha el monto obligado es de cuarenta y tres millones seiscientos treinta y dos mil cuatrocientos trece pesos ($43.632.413), habiéndose presupuestado un total de dos mil cuatrocientos setenta y dos millones de pesos ($2.472.000.000), discriminado como se muestra a continuación en las siguientes actividades:

1. Definir estudios tecnológicos ($51.500.000), obligado ($0).
2. Adquisición de hardware y repotencialización de la plataforma tecnológica ($1.545.000.000), obligado ($0).

Actividad: Mantener infraestructura tecnológica, presupuesto setecientos veintiún millones de pesos ($721.000.000) y a la fecha solo se ha obligado diez millones noventa y nueve mil ochenta pesos ($10.099.080), ejecutado el 1,40%.

Actividad: Realizar estudios o consultorías informáticas, presupuesto ciento cincuenta y cuatro mil quinientos mil pesos ($154.500.000) y a la fecha solo se ha obligado treinta y tres millones quinientos treinta y tres mil trescientos treinta y tres pesos ($33.533.333), ejecutado 21,7%.

El presupuesto disponible para la ejecución del producto Servicios tecnológicos es de dos mil cuatro cientos setenta y dos millones de pesos ($2.472.000.000), a la fecha se ha obligado cuarenta y tres millones seiscientos treinta y dos mil cuatrocientos trece pesos **(**$43.632.413), equivalente al 1.77%. Ver Imagen 7.

**Recomendación**
Realizar monitoreo y seguimiento para asegurar acorde con lo planeado, la ejecución de las actividades de los proyectos de inversión, en aras de prevenir la posible materialización de eventos de riesgos.

**Imagen 7.** Seguimiento proyectos de inversión OTIC Superintendencia de Transporte - Proyecto de inversión Código 2018011000653

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **PROYECTO DE INVERSIÓN:** | **MEJORAMIENTO DE LA GESTIÓN Y CAPACIDAD INSTITUCIONAL PARA LA SUPERVISIÓN INTEGRAL A LOS VIGILADOS A NIVEL NACIONAL** | | | | | | | | | |
| | **LINK DEL PROYECTO:** https://spi.dnp.gov.co/Consultas/Detalle.aspx?vigencia=2020&periodo=9&proyecto=2018011000653 | | | | | | | | | | |
| | **FICHA EBI:**https://suifp.dnp.gov.co/DescargasFichas/Fichas/2018011000653/2020/2020-2018011000653-00000000000630324-SPI.pdf | | | | | | | | | | |
| | **OBJETIVO ESPECÍFICO:** Aumentar la eficiencia y calidad en la gestión de los procesos de apoyo de la Supertransporte. | | | | | | | | | | |
| | **Código BPIN:** 2018011000653 | | | | | | | | | | |
| **PRODUCTO** | **ACTIVIDADES** | **FECHA DE INICIO** | **FECHA FIN** | **VALOR VIGENTE** | **VALOR EJECUTADO (OBLIGADO con corte a septiembre)** | **METAS INDICADOR (2019-2024)** | **AVANCE INDICADOR (2019-2024)** | **RESPONSABLE** | **%EJECUCIÓN Frente al presupuesto obligado** | **SOPORTES - OTIC** | **SOPORTES- OAP** |
| Servicios de información Actualizados | Desarrollar, optimizar y/o adquirir software | 29/01/19 | 31/12/24 | 2.341.000.000 | 0 | 5 | 2 | Javier Pérez Pérez | 3,34% | Publicación proceso SAMC 004-2020 IMPLEMENTACIÓN Y CONFIGURACIÓN DE LA ÚLTIMA VERSIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL ORFEO PARA LA SUPERINTENDENCIA DE TRANSPORTE. ( $ 225.778.510). Proceso en evaluación y observaciones. Publicado en el SECOP II.<br><br>Publicación de proceso SAMC 003-2020 Adquirir la licencia de uso de software que permita la gestión, administración, control, toma física, y conciliación contable de los activos de propiedad de la Superintendencia de Transporte y la implementación del mismo. ( $184.807.000) Adjudicado por ( $ 118.434.631) CT 341 de 2020. Publicado en el SECOP II.<br><br>Adquisición a través del proceso IPMC 007-2020 de una licencia para la creación de contenidos para el desarrollo de experiencias interactivas y adaptativas de la plataforma e-Learning de la Superintendencia de Transporte. ($ 13.975.000). Publicado en el SECOP II.<br><br>Etapa precontractual para el proceso de Adquisición de licencias arquitect para el modelamiento de procesos de la entidad. | Se realizan estudios previos para la adquisición del software Isprint para la generación de contenidos de plataforma e-learning |
| | Servicios informáticos conexos | 29/01/19 | 31/12/24 | 515.000.000 | 0 | | | | | Proceso precontractural para la Implementación de servicio en la nube Oracle para la Superintendencia de Transporte al amparo del Acuerdo Marco de Precios CCE-908-1-AMP-2019. | Se realizan los estudios previos y proceso precontractural para la Implementación de servicio en la nube Oracle para la Superintendencia de Transporte al amparo del Acuerdo Marco de Precios CCE-908-1-AMP-2019. |
| | Operar el aplicativo misional a través de servicios de hosting | 29/01/19 | 31/12/24 | 154.500.000 | 0 | | | | | | |
| | Contar con la prestación de servicios de apoyo | 29/01/19 | 31/12/24 | 800.500.000 | 127.300.358 | | | | | Ejecución de los contratos CT 139, CT 141, CT 142, CT 230, CT 260, CT 261. Se encuentran publicados en el SECOP II.<br><br>Se firma contrato 327 de 2020 con objeto: Prestar sus servicios profesionales en la Oficina de Tecnologías de la Información y las Comunicaciones, adelantando actividades para la codificación del software y soporte a los sistemas de información de la Superintendencia de Transporte. ($ 16.083.720).<br><br>Se firma contrato 336 de 2020 con objeto: Prestar sus servicios profesionales en la Oficina de Tecnologías de la Información y las Comunicaciones, adelantando actividades de adaptación de la interfaz gráfica de las aplicaciones, y aplicativos para mejorar la experiencia de los usuarios de la Superintendencia. ($ 10.060.637). | Contratos por prestación de servicios para garantizar la operación de TI de la Superintendencia de Transporte. Los contratos se realizan con pagos de acuerdo con las obligaciones definidas, los contratos son los siguientes: CT 139, CT 141, CT 191, CT 142, CT 173, CT 230. |
| | | | | $ 3.811.000.000 | $ 127.300.358 | | | | | | |

**Fuente:** Oficina de Tecnologías de la Información y las Comunicaciones

**Objetivo del proyecto de inversión:** Fortalecer la Vigilancia, Inspección y Control a los vigilados por parte de la Superintendencia de Transporte.
**Proyecto de inversión Código 2018011000655** – Fortalecimiento a la supervisión integral a los vigilados a nivel Nacional:

**Programa:** Regulación y supervisión

de Infraestructura y servicios de transporte.

**Objetivos Específicos**: Gestionar la información de la prestación del servicio público de transporte, su infraestructura, servicios conexos y complementarios.

- **Producto:** Documentos de Investigación.

- **Cumplimiento:** 41,67%

Se observó que a la fecha el monto obligado es de Sesenta millones ciento sesenta y seis mil setecientos cincuenta y nueve pesos ($60.166.759), habiéndose presupuestado un total de dos mil ochenta y cuatro millones de pesos ($2.084.000.000), discriminado como se muestra a continuación:

1. Adecuar, Suministrar y Dotar el Centro de Control de Monitoreo de Actividades de Transporte ($ 312.000.000), obligado ($0).
2. Identificar información del Sector ($418.000.000), obligado ($0).
3. Procesar y divulgar información del Sector ($624.000.000), obligado ($0).

Actividad: Revisar y analizar la información del Sector, presupuesto setecientos treinta millones de pesos ($730.000.000) y a la fecha solo se ha obligado sesenta millones ciento sesenta y seis mil setecientos cincuenta y nueve pesos ($60.166.759), ejecutado 8,24%.

El presupuesto disponible para la ejecución del producto Documentos de Investigación es de dos mil ochenta y cuatro de pesos ($2.084.000.000), a la fecha se ha obligado sesenta millones ciento sesenta y seis mil setecientos cincuenta y nueve pesos **(**$60.166.759), equivalente al 2.89%. Ver Imagen 8.

**Imagen 8.** Seguimiento proyectos de inversión OTIC Superintendencia de Transporte - Proyecto de inversión Código 2018011000655

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **PROYECTO DE INVERSIÓN:** | **FORTALECIMIENTO A LA SUPERVISIÓN INTEGRAL A LOS VIGILADOS A NIVEL NACIONAL** | | | | | | | | | |
| **LINK DEL PROYECTO:** https://suifp.dnp.gov.co/DescargasFichas/Fichas/2018011000655/2020/2020-2018011000655-00000000000630316-SPI.pdf | | | | | | | | | | |
| **FICHA EBI:** https://suifp.dnp.gov.co/DescargasFichas/Fichas/2018011000655/2020/2020-2018011000655-00000000000630316-SPI.pdf | | | | | | | | | | |
| **OBJETIVO ESPECÍFICO:** Gestionar la información de la prestación del servicio público de transporte, su infraestructura, servicios conexos y complementarios. | | | | | | | | | | |
| **Código BPIN:** 2018011000655 | | | | | | | | | | |
| **ACTIVIDADES** | **FECHA DE INICIO** | **FECHA FIN** | **VALOR VIGENTE** | **VALOR EJECUTADO (OBLIGADO)** | **METAS INDICADOR (2019-2024)** | **AVANCE INDICADOR (2019-2024)** | **RESPONSABLE** | **%EJECUCIÓN Frente al presupuesto obligado** | **SOPORTES - OTIC** | **SOPORTES- OAP** |
| Adecuar, Suministrar y Dotar el Centro de Control de Monitoreo de Actividades de Transporte. | 2019-Jan-01 | 2024-Dec-31 | $ 312.000.000 | $ 63.123.000 | 24 | 10 | JEFE OFICINA TIC ING. JAVIER PÉREZ | 16,22% | https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/ordenes-compra/54445 | Inicia el proceso de adquisición de licencias Microsoft: 50 licencias office 365 E3, 1 licencia para Visual Studio, 6 licencias Power BI. Esta compra se realiza a través de la Tienda Virtual del estado colombiano - TVEC. |
| Identificar información del Sector | 2019-Jan-01 | 2024-Dec-31 | $ 78.000.000 | | | | | | | |
| Revisar y analizar la información del Sector | 2019-Jan-01 | 2024-Dec-31 | $ 370.000.000 | $ 60.166.759 | | | | | Ejecución de los contratos CT 138, CT 179, CT 180, de acuerdo con las obligaciones incluidas. | Se esta desarrollando la actividad a través de personal contratado. |
| Procesar y divulgar información del Sector | 2019-Jan-01 | 2024-Dec-31 | $ - | | | | | | | |

**Fuente:** Oficina de Tecnologías de la Información y las Comunicaciones

## Recomendación

Realizar monitoreo y seguimiento para asegurar acorde con lo planeado, la ejecución de las actividades de los proyectos de inversión, en aras de prevenir la posible materialización de eventos de riesgo.

**Observación O001 de 2020 (AP Acción Preventiva)**
**O001A-26nov20-(AP)GTICS**
El Auditor observó en el Sistema de Seguimiento a Proyectos de Inversión enlace https://spi.dnp.gov.co vigencia 2020, que presentan retraso en la ejecución de las actividades programadas para los productos.

Se esta incumpliendo el numeral 3 "*Formular, decidir oportunamente o ejecutar los planes de desarrollo y los presupuestos, y cumplir las leyes y normas que regulan el manejo de los recursos económicos públicos, o afectos al servicio público.*" Ley 734 de 2002 "*por la cual se expide el Código Disciplinario Único, Artículo 34. Deberes. Son deberes de todo servidor público.*". Lo que puede con llevar a recorte presupuestal por falta de ejecución. Situación que puede conllevar a la posible materialización de riesgos de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC en la vigencia 2020 impactando la gestión de la disponibilidad de recursos necesarios para alcanzar los objetivos institucionales y cumplir las funciones delegadas.

**6.3 Verificar el cumplimiento de la la política de seguridad de la información de la Superintendencia de Transporte.** (Según selectivo).

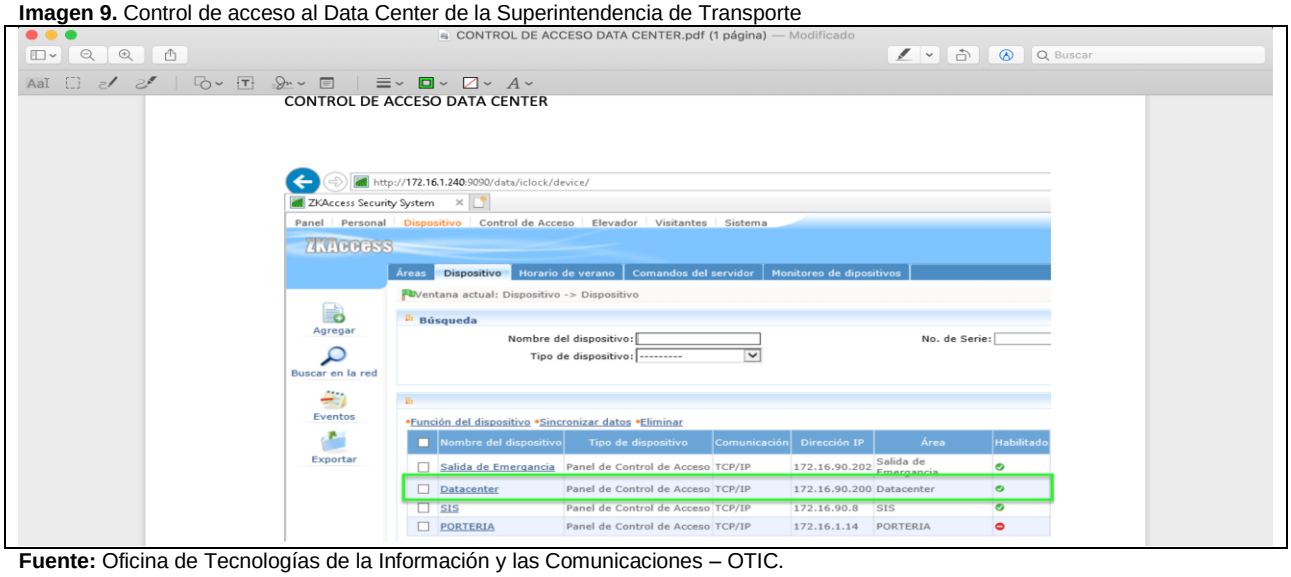
**Prueba Realizada**
Componentes de la política de seguridad de la información diligenciados por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC en el documento Excel denominado Mtriz-PltcaSgrdadInfrmción Noviembre 20.xlsx.

**Situaciones evidenciadas**
El auditor evidenció los componentes de la política de seguridad de la información de los seguimientos y controles realizados por la OTIC para garantizar la seguridad física y ambiental de la infraestructura de la Entidad para:

**a. Las áreas protegidas y el Centro de Datos se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por la Oficina de Tecnologías de la Información y las Comunicaciones, a fin de permitir el acceso solo a personal autorizado.**

Se observó documento PDF denominado CONTROL DE ACCESO DATA CENTER.pdf donde se verifica que el Data Center tiene habilitado el control de Acceso, este control se realiza a través del aplicativo ZKAccess Security System. No se evidenció los servidores que se encuentran autorizados a ingresar al Data Center de la Entidad. Ver Imagen 9.

**Imagen 9.** Control de acceso al Data Center de la Superintendencia de Transporte

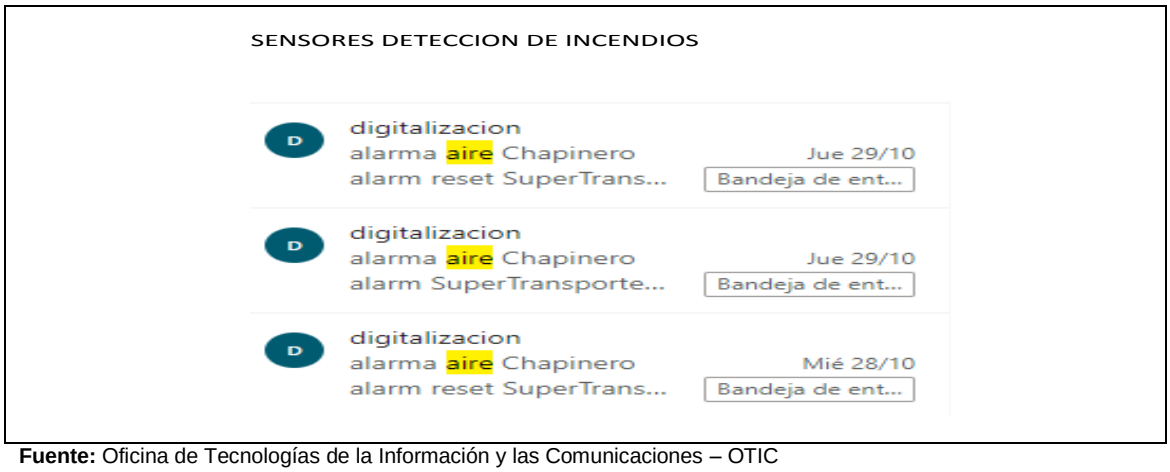



**Fuente:** Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

**b. Para la selección de las áreas protegidas y la ubicación del Centro de Datos se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad de las instalaciones.**

El auditor evidenció documento PDF denominado SENSORES DETECCION DE INCENDIOS.pdf, de los correos allegados al administrador del Data Center de las alarmas generadas por los sensores por aire de presión "*el cuenta con sensores integrados de detección de incendios y de humedad y generan alerta que se notifican a través del correo electrónico*", del Centro de Datos de la Entidad "alarma aire Chapinero, alarm reset Super Transporte", para los días miércoles 28 y 29 de octubre de 2020, no se evidenció contenido del correo y contingencia al contenido de estos correos de aviso de precausión. Ver Imagen 10.

**Imagen 10.** Notificación por correo del estado del aire acondicionado del Data Centerde la Superintendneica de Transporte.

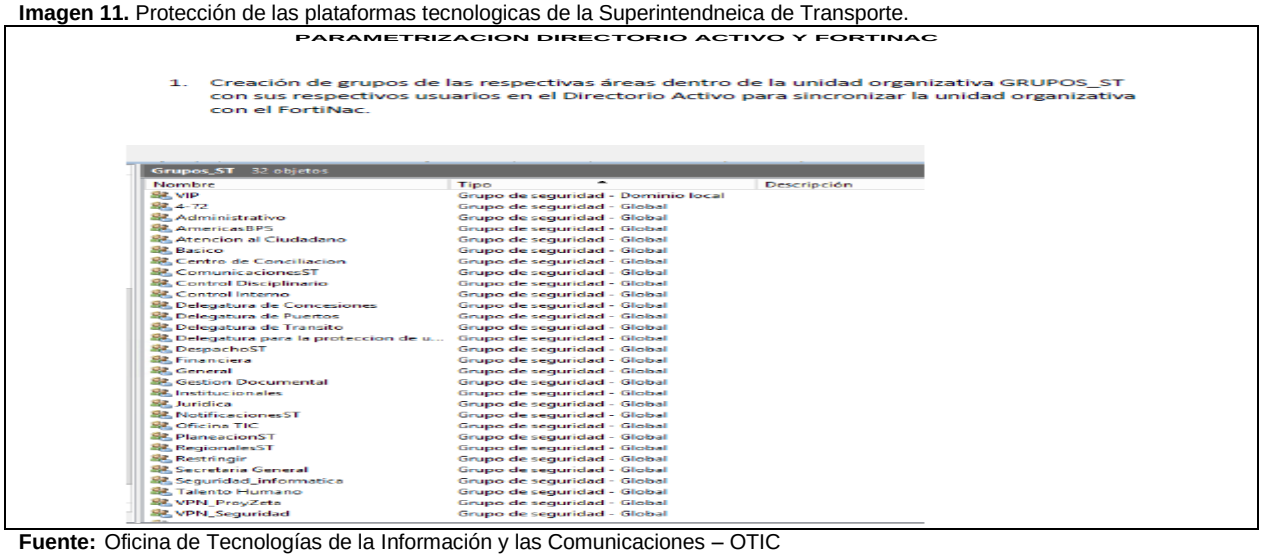



**Fuente:** Oficina de Tecnologías de la Información y las Comunicaciones – OTIC

**c. Las plataformas tecnológicas serán ubicadas y protegidas de tal manera que reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.**

El auditor evidenció documento PDF denominado DIRECTORIO ACTIVO Y FORTINAC.pdf, de los controles de acceso y de Directorio activo con sus respectivos usuarios creados en el directorio activo para sincronizar la unidad organizativa con el FortiNac. Se observó 30 registros con nombre de usuario de las dependencias, oficinas y Delegadas de la Entidad, la asignación del tipo de acceso "*Grupo de seguridad – Domino local, Grupo de seguridda – Global*" controlados desde el aplicativo FortiNac. Ver Imagen 11.

**Imagen 11.** Protección de las plataformas tecnologicas de la Superintendneica de Transporte.

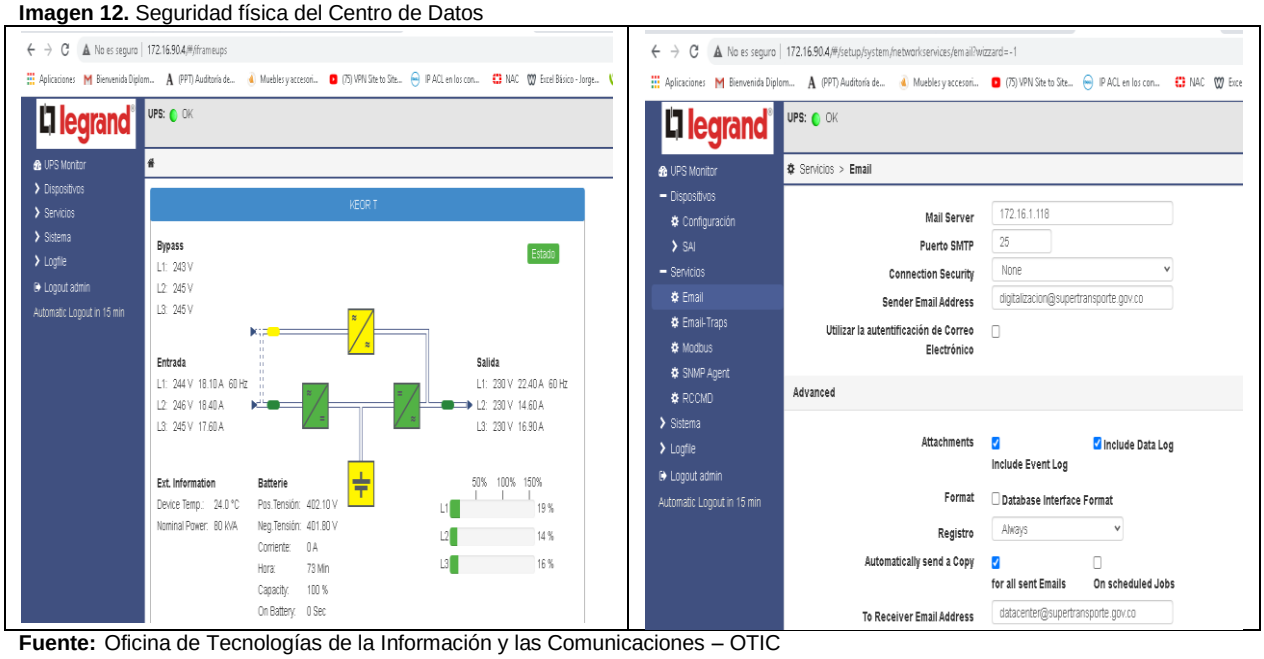



**Fuente:** Oficina de Tecnologías de la Información y las Comunicaciones – OTIC

**f.Como se garantiza la seguridad física del Centro de Datos, incluyendo entre otros los siguientes subsistemas: I. Sistema Eléctrico suplementario, II. Sistema de Control de Acceso, III. Sistema de protección contra incendios.**

El auditor evidenció documento PDF denominado SISTEMA ELÉCTRICO SUPLEMENTARIO UPS.pdf, donde se realiza seguimiento por las alertas generadas. Por el sistema eléctrico suplementario UPS desde la ruta del enlace *"---.--.--.-/#/iframeups*". Ver Imagen 12.

**Imagen 12.** Seguridad física del Centro de Datos




**Fuente:** Oficina de Tecnologías de la Información y las Comunicaciones – OTIC

Se evidenció "*6.4 Evidenciar los seguimientos y controles se han realizado a la seguridad y Mantenimiento de los Equipos de la Entidad para:*" numeral d:

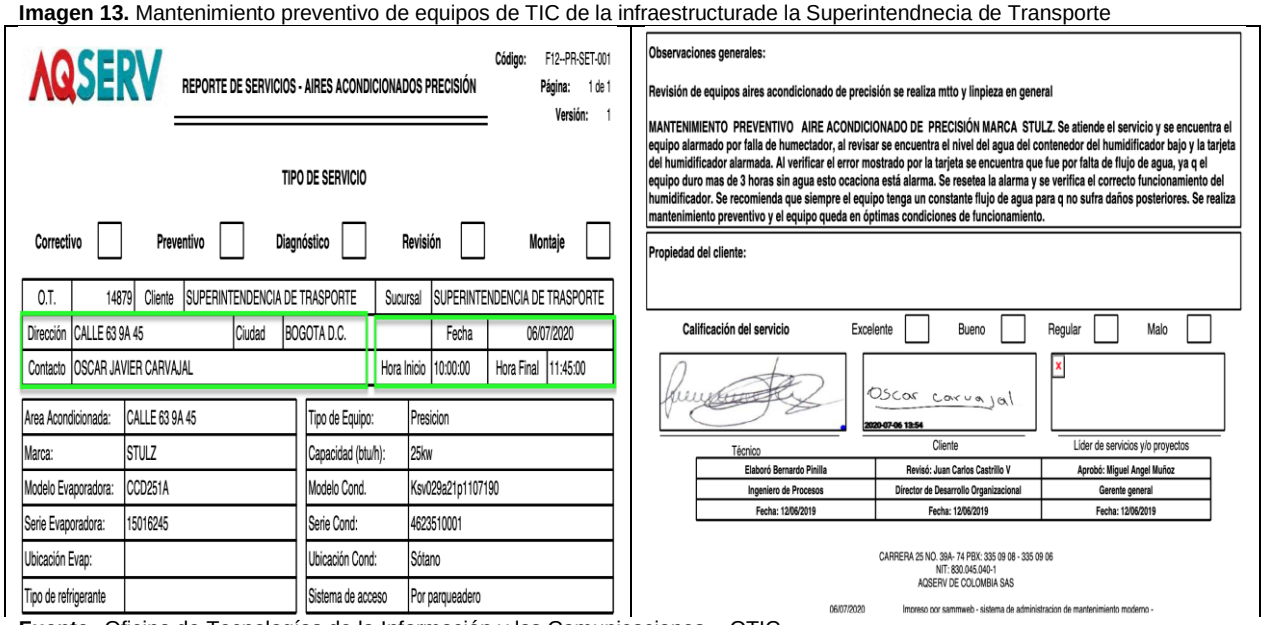
**d. Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes**.

Se evidenció documento PDF denominado Mantenimiento Aires de Precisión.pdf, del mantenimiento realizado por el proveedor AQSERV - al mantenimiento realizado a Aires de Presición, Mantenimiento UPS el día 6 de julio de 2020, hora de inicio 10:00, hora final 11:45, en la dirección calle 63 9ª 45 ciudad de Bogotá, D.C., en el documento se evidencia que el

estado de los criterios aplicados se encuentran en el rango cumple o no aplica, no se observó estado no cumple. La empresa AQSERV en la revisión de equipos de aires acondicionados de precisión se realiza mantenimiento y limpieza en general dejo como observación general: "*MANTENIMIENTO GENERAL PREVENTIVO AIRE ACINDICIONADO MARCA STULZ. Se etiende el servicio y se encuentra el equipo alarmado por falla de humectador, al revisar se encuentra el nivel del agua del contenedor del humidificador bajo y la tarjeta del humificador alarmada. Al verificar el error mostrado por la trjeta se encuentra que fue por falta de flujo de agua, ya que el equipo duro mas de 3 horas sin agua esto ocasiona está alarma. Se resetea la alarma y se verifica el correcto funcionamiento del humificador. Se recomienda que siempre el equipo tenga un constante flujo de agua para que no sufra daños posteriores. Se realiza mantenimiento preventivo y el equipo en óptimas condiciones de funcionamiento.*", el documento se encuentra firmado por la persona que califico el servicio y por el servidor público que de la Entidad que atendio el servicio.

Se evidenció que la alarma activada por el sistema de aire se genero por falta de seguimiento y control del dispositivo, lo que puede acarrear en el daño de este. Ver Imagen 13.

**Imagen 13.** Mantenimiento preventivo de equipos de TIC de la infraestructurade la Superintendnecia de Transporte



AQSERV — REPORTE DE SERVICIOS - AIRES ACONDICIONADOS PRECISIÓN

Código: F12-PR-SET-001 | Página: 1 de 1 | Versión: 1

TIPO DE SERVICIO

Correctivo ☐ Preventivo ☐ Diagnóstico ☐ Revisión ☐ Montaje ☐

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| O.T. | 14879 | Cliente | SUPERINTENDENCIA DE TRASPORTE | Sucursal | SUPERINTENDENCIA DE TRASPORTE | | |
| Dirección | CALLE 63 9A 45 | Ciudad | BOGOTA D.C. | | Fecha | 06/07/2020 | |
| Contacto | OSCAR JAVIER CARVAJAL | | | Hora Inicio | 10:00:00 | Hora Final | 11:45:00 |

| | | | |
|---|---|---|---|
| Area Acondicionada: | CALLE 63 9A 45 | Tipo de Equipo: | Presicion |
| Marca: | STULZ | Capacidad (btu/h): | 25kw |
| Modelo Evaporadora: | CCD251A | Modelo Cond. | Ksv029a21p1107190 |
| Serie Evaporadora: | 15016245 | Serie Cond: | 4623510001 |
| Ubicación Evap: | | Ubicación Cond: | Sótano |
| Tipo de refrigerante | | Sistema de acceso | Por parqueadero |

**Observaciones generales:**

Revisión de equipos aires acondicionado de precisión se realiza mtto y linpieza en general

MANTENIMIENTO PREVENTIVO AIRE ACONDICIONADO DE PRECISIÓN MARCA STULZ. Se atiende el servicio y se encuentra el equipo alarmado por falla de humectador, al revisar se encuentra el nivel del agua del contenedor del humidificador bajo y la tarjeta del humidificador alarmada. Al verificar el error mostrado por la tarjeta se encuentra que fue por falta de flujo de agua, ya q el equipo duro mas de 3 horas sin agua esto ocaciona está alarma. Se resetea la alarma y se verifica el correcto funcionamiento del humidificador. Se recomienda que siempre el equipo tenga un constante flujo de agua para q no sufra daños posteriores. Se realiza mantenimiento preventivo y el equipo queda en óptimas condiciones de funcionamiento.

**Propiedad del cliente:**

**Calificación del servicio** Excelente ☐ Bueno ☐ Regular ☐ Malo ☐

Oscar carvajal
2020-07-06 13:54

Técnico | Cliente | Líder de servicios y/o proyectos

| Elaboró Bernardo Pinilla | Revisó: Juan Carlos Castrillo V | Aprobó: Miguel Angel Muñoz |
|---|---|---|
| Ingeniero de Procesos | Director de Desarrollo Organizacional | Gerente general |
| Fecha: 12/06/2019 | Fecha: 12/06/2019 | Fecha: 12/06/2019 |

CARRERA 25 NO. 39A- 74 PBX: 335 09 08 - 335 09 06
NIT: 830.045.040-1
AQSERV DE COLOMBIA SAS

06/07/2020 Impreso por sammweb - sistema de administracion de mantenimiento moderno -

**Fuente:** Oficina de Tecnologías de la Información y las Comunicaciones – OTIC

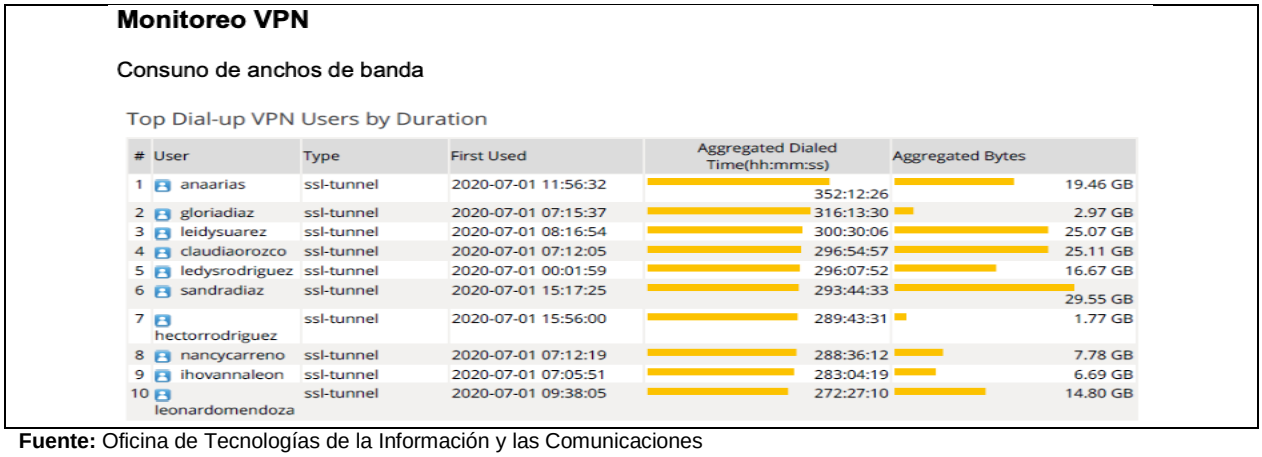
**Se evidenció "*8.2 Evidenciar el Uso Adecuado de los Activos de Información para*:", numeral unico:**

**La información, los sistemas, las aplicaciones, los servicios y los equipos (computadores de escritorio, portátiles, impresoras, redes, Internet, dispositivos móviles, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) de todas y cada una de las dependencias y entidades de la Superintendencia de Transporte, son activos de información que se proporcionan a los funcionarios y contratistas para cumplir con sus respectivas actividades laborales. La Superintendencia de Transporte se reservan el derecho de monitorear y supervisar su información,**

**sistemas, servicios y equipos, de acuerdo con lo establecido en la presente política, así como en la legislación nacional vigente.**

El auditor evidenció documento PDF denominado MONITOREO DE RED y VPN.pdf, de las aplicaciones mas utilizdas en la red "*La siguiente sección muestra las 30 aplicaciones principales que cruzan la red en función de la cantidad de ancho de banda que están utilizando, clasificadas por categoría de aplicación y tecnología. La calificación de riesgo también se enumera para cada aplicación junto con su recuento de sesiones. Esto proporciona una vista más completa de las aplicaciones que se ejecutan en la red y da como resultado una mejor toma de decisiones para las políticas generales de control de aplicaciones y la gestión de riesgos comerciales.* " y el consumo de ancho de banda por parte de los servidores públicos que se conectan por la VPN. Se observó tiempos de acceso a la VPN de 272 a 352 horas de conexión de algunos servidores públicos y consumo exajerados de ancho de banda. Ver Imagen 14.

**Imagen 14.** Monitoreo del consumo de ancho de banda de los servidores públicos de la Superintendencia de Transporte por la VPN.



**Monitoreo VPN**

Consuno de anchos de banda

Top Dial-up VPN Users by Duration

| # | User | Type | First Used | Aggregated Dialed Time(hh:mm:ss) | Aggregated Bytes |
|---|---|---|---|---|---|
| 1 | anaarias | ssl-tunnel | 2020-07-01 11:56:32 | 352:12:26 | 19.46 GB |
| 2 | gloriadiaz | ssl-tunnel | 2020-07-01 07:15:37 | 316:13:30 | 2.97 GB |
| 3 | leidysuarez | ssl-tunnel | 2020-07-01 08:16:54 | 300:30:06 | 25.07 GB |
| 4 | claudiaorozco | ssl-tunnel | 2020-07-01 07:12:05 | 296:54:57 | 25.11 GB |
| 5 | ledysrodriguez | ssl-tunnel | 2020-07-01 00:01:59 | 296:07:52 | 16.67 GB |
| 6 | sandradiaz | ssl-tunnel | 2020-07-01 15:17:25 | 293:44:33 | 29.55 GB |
| 7 | hectorrodriguez | ssl-tunnel | 2020-07-01 15:56:00 | 289:43:31 | 1.77 GB |
| 8 | nancycarreno | ssl-tunnel | 2020-07-01 07:12:19 | 288:36:12 | 7.78 GB |
| 9 | ihovannaleon | ssl-tunnel | 2020-07-01 07:05:51 | 283:04:19 | 6.69 GB |
| 10 | leonardomendoza | ssl-tunnel | 2020-07-01 09:38:05 | 272:27:10 | 14.80 GB |

**Fuente:** Oficina de Tecnologías de la Información y las Comunicaciones

### 8.2.1 Evidenciar los seguimientos y controles del Uso de Internet para

Se evidenció en documento PDF denominado Perfiles de navegación.pdf para el seguimiento y monitoreo "*8.2.1 Evidenciar los seguimientos y controles del Uso de Internet para:*" se identificó permisos en la web para los diferentes perfiles definidos que no tienen que ver con las funciones propias de la Superintendencia de Transporte. Ver Imagen 15.

**Imagen 15.** Perfiles de navegación en la Superintendencia de Transporte

**Fortalecimiento perfiles de navegación**

Durante la vigencia del año 2020 se ha fortalecido los perfiles de navegación según las necesitadas de la entidad con el fin de optimizar el uso de los canales de internet, se define en 4 grupos:

- Basico
- General
- Seguridad informática
- VIP

Perfiles de seguridad WEB.

| Categoria | Restringido Perfil 1 Allow / Deny | Basico Perfil 2 Allow / Deny | General Perfil 3 Allow / Deny | Seguridad Informática Perfil 4 Allow / Deny | VIP Perfil 5 Allow / Deny |
|---|---|---|---|---|---|
| Drug Abuse | Deny | Deny | Deny | Deny | Deny |
| Hacking | Deny | Deny | Deny | Allow | Deny |
| Illegal or Unethical | Deny | Deny | Deny | Deny | Deny |
| Discrimination | Deny | Deny | Deny | Deny | Deny |
| Explicit Violence | Deny | Deny | Deny | Deny | Deny |
| Extremist Groups | Deny | Deny | Deny | Deny | Deny |
| Proxy Avoidance | Deny | Deny | Deny | Deny | Deny |
| Plagiarism | Deny | Deny | Deny | Deny | Deny |
| Child Abuse | Deny | Deny | Deny | Deny | Deny |
| Alternative Beliefs | Deny | Deny | Deny | Deny | Deny |
| Abortion | Deny | Deny | Deny | Deny | Deny |
| Other Adult Materials | Deny | Deny | Deny | Deny | Deny |
| Advocacy Organizations | Deny | Deny | Deny | Deny | Deny |
| Gambling | Deny | Deny | Deny | Deny | Deny |
| Nudity and Risque | Deny | Deny | Deny | Deny | Deny |
| Pornography | Deny | Deny | Deny | Deny | Deny |
| Dating | Deny | Deny | Deny | Deny | Deny |
| Weapons (sales) | Deny | Deny | Deny | Deny | Deny |
| Marijuana | Deny | Deny | Deny | Deny | Deny |
| Sex Education | Deny | Deny | Deny | Deny | Deny |
| Alcohol | Deny | Deny | Deny | Deny | Deny |
| Tobacco | Deny | Deny | Deny | Deny | Deny |
| Lingerie and Swimsuit | Deny | Deny | Deny | Deny | Deny |
| Sports Hunting and War Games | Deny | Deny | Deny | Deny | Deny |
| Freeware and Software Downloads | Deny | Deny | Deny | Deny | Deny |
| File Sharing and Storage | Deny | Allow | Allow | Allow | Allow |
| Streaming Media and Download | Deny | Deny | Allow | Deny | Deny |
| Peer-to-peer File Sharing | Deny | Allow | Allow | Allow | Allow |
| Internet Radio and TV | Deny | Deny | Allow | Allow | Allow |
| Internet Telephony | Deny | Deny | Deny | Deny | Allow |
| Malicious Websites | Deny | Deny | Deny | Deny | Deny |
| Phishing | Deny | Deny | Deny | Deny | Deny |
| Spam URLs | Deny | Deny | Deny | Deny | Deny |
| Advertising | Deny | Deny | Deny | Deny | Deny |
| Brokerage and Trading | Deny | Deny | Deny | Deny | Deny |
| Games | Deny | Deny | Deny | Deny | Deny |
| Web-based Email | Deny | Allow | Allow | Allow | Allow |
| Entertainment | Deny | Deny | Deny | Deny | Allow |
| Arts and Culture | Deny | Deny | Deny | Deny | Allow |
| Education | Deny | Deny | Allow | Allow | Allow |
| Health and Wellness | Deny | Deny | Deny | Deny | Allow |
| Job Search | Deny | Deny | Deny | Deny | Deny |
| Medicine | Deny | Allow | Allow | Allow | Allow |
| News and Media | Deny | Deny | Deny | Deny | Allow |
| Social Networking | Deny | Deny | Allow | Allow | Allow |
| Political Organizations | Deny | Deny | Deny | Deny | Allow |
| Reference | Deny | Deny | Deny | Deny | Deny |
| Global Religion | Deny | Deny | Deny | Deny | Deny |
| Shopping and Auction | Deny | Deny | Deny | Deny | Deny |
| Society and Lifestyles | Deny | Deny | Deny | Deny | Allow |
| Sports | Deny | Deny | Deny | Deny | Allow |
| Travel | Deny | Deny | Deny | Deny | Allow |
| Personal Vehicles | Deny | Deny | Deny | Deny | Deny |
| Dynamic Content | Deny | Deny | Deny | Deny | Deny |
| Meaningless Content | Deny | Deny | Deny | Deny | Deny |
| Folklore | Deny | Deny | Deny | Deny | Deny |
| Web Chat | Deny | Deny | Deny | Allow | Allow |
| Instant Messaging | Deny | Deny | Allow | Allow | Allow |
| Newsgroups and Message Boards | Deny | Allow | Allow | Allow | Allow |
| Digital Postcards | Deny | Deny | Deny | Deny | Deny |
| Child Education | Deny | Deny | Deny | Deny | Deny |
| Real Estate | Deny | Deny | Deny | Deny | Deny |
| Restaurant and Dining | Deny | Deny | Deny | Deny | Allow |
| Personal Websites and Blogs | Deny | Deny | Deny | Deny | Allow |
| Content Servers | Deny | Deny | Deny | Deny | Deny |
| Domain Parking | Deny | Deny | Deny | Deny | Deny |
| Personal Privacy | Deny | Deny | Deny | Deny | Deny |
| Finance and Banking | Deny | Deny | Allow | Allow | Allow |
| Search Engines and Portals | Deny | Allow | Allow | Allow | Allow |
| General Organizations | Deny | Deny | Deny | Deny | Allow |
| Business | Deny | Deny | Deny | Deny | Allow |
| Information and Computer Security | Deny | Deny | Deny | Allow | Deny |
| Government and Legal Organizations | Deny | Allow | Allow | Allow | Allow |
| Information Technology | Deny | Deny | Deny | Allow | Allow |
| Armed Forces | Deny | Deny | Deny | Deny | Deny |
| Web Hosting | Deny | Deny | Deny | Deny | Deny |
| Secure Websites | Deny | Deny | Deny | Allow | Deny |
| Web-based Applications | Deny | Deny | Deny | Deny | Deny |
| Unrated | Deny | Deny | Deny | Allow | Deny |

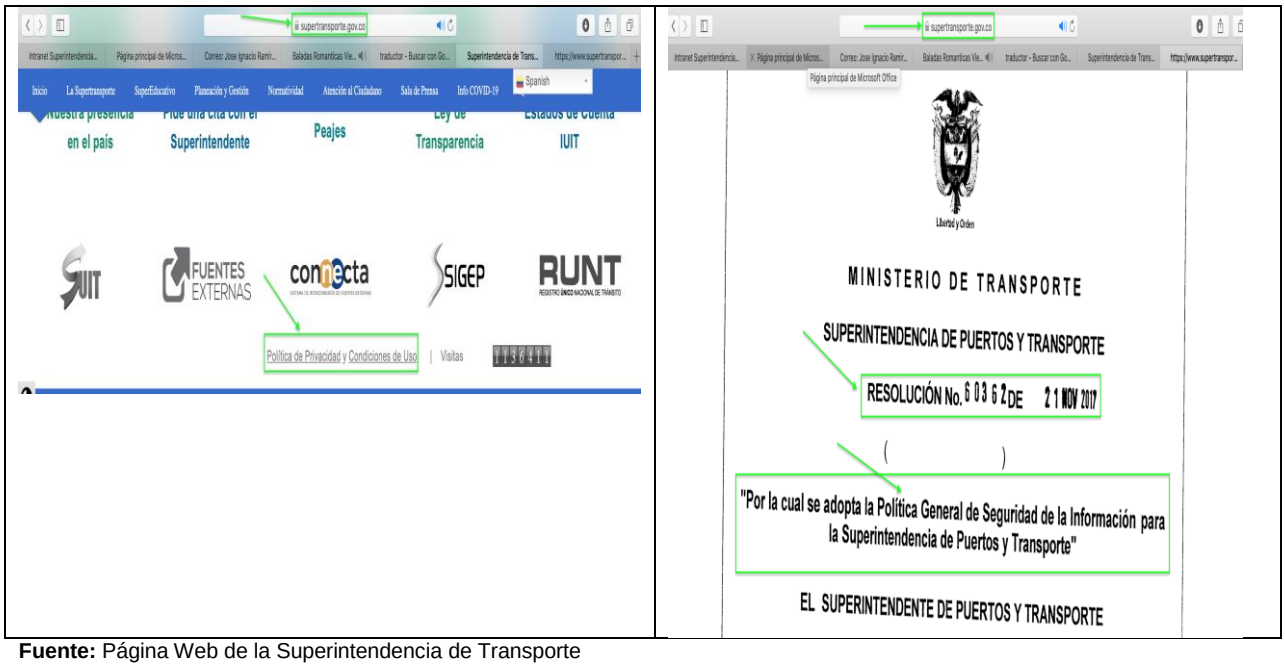
**Fuente:** Oficina de Tecnologías de la Información y las Comunicaciones

El auditor evidenció "*8.2.5 Evidenciar los controles y seguimientos realizados al Sistemas de Acceso Público en:*" numeral b.

**b. El portal institucional deberá contener la política de privacidad y uso, así como la política de seguridad del mismo.**

Se evidenció en la página web de la Superintendencia de Transporte publlicada la Política General de Seguridad de la Información para la Superintendencia de Transporte. Resolución 60362 de 21 de noviembre de 2017 "*Por la cual se adopta la Política General de Seguridad de la Información para la Superintendencia de Puertos y Transporte*". Imagen 16.

**Imagen 16.** Publicación en la página de la Superintendecia de Transporte la Política General de Seguridad de la Información para la Superintendencia de Transporte




**Fuente:** Página Web de la Superintendencia de Transporte

Se evidenció comunicados de prevención "*8.5 Evidenciar los seguimientos y controles de Protección contra Software Malicioso en la Superintendencia en epoca de la emergencia sanitaria en/para*:" en documento PDF denominado COMUNICADOS PREVENCION -.pdf, numeral f y h.

**f. La Entidad será responsable de que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza y h. La entidad debe implementar las acciones necesarias para mitigar los riesgos de seguridad de acuerdo a los reportes y boletines emitidos por la Policía Nacional y los entes de Seguridad informática.**

Se evidenció por el correo institucional de comunicaciones de los días 15 de octubre de 2020 Alerta de información Importante – correo de estafa, 19 de octubre de 2020 Conferencia de seguridad informática – mitigar riesgos y amenazas por el uso de nuevas tecnologías, alertas de suplantación y phishing en documento PDF denominado COMUNICADOS PREVENCION -.pdf. Ver Imagen 17.

**Imagen 17.** Capacitaciones y comunicados de prevención uso de nuevas tecnologías


**FUENTE:** Correo interirucional y Oficina de Tecnologías de la Información y las Comunicaciones

**Recomendaciones**

- Realizar monitoreo y seguimiento diario a la información que es manipulada por los servidores públicos que presentan consumo de ancho de banda mayor a 500 megas.
- Realizar estudio y establecer tiempos máximos de conexión diaria a la VPN y consumo de ancho de banda.
- Revisar los accesos a los perfiles, se indentificó permisos que no tiene que ver con las funciones de los servidores públicos de la Superintendencia de Transporte.

**6.4 Verificar los riesgos y controles asociados.**

**Prueba Realizada**

Se realizó en el informe de evaluación de riesgos de la Oficina de Tecnologías de la Información y las Comunicaciones.

***Situaciones evidenciadas***
El Auditor evidenció seguimiento a los riesgos de gestión del proceso Transversal Gestión de TICS.

- **Riesgo 2.** Operativo: Falta de personal para la operación del Centro de Cómputo.
- **Control**:
  1. Inclusión al finalizar cada vigencia, de los items de las contrataciones en el PAA.

**1.1 Asignación del Responsable**
Se evidenció en el Mapa de Riesgo del Proceso Transversal Gestión TICS el responsable Carlos Oscar Quintero - Asesor del Despacho / Maximino Vargas - Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

**Recomendación**
Actualizar en el Mapa de Riesgos del Proceso Transversal Gestión TICS el responsable.

**1.2 Segregación y autoridad del responsable**
Se evidenció que el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC es el responsable del Proceso Transversal Gestión de TICS y tiene la autoridad adecuada y segregación de funciones en la ejecución del contro.

**2. Periodicidad**
Se evidenció fecha de seguimiento en el Mapa de Riesgos allegado por la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

**3. Propósito**
Se evidenció que las actividades que se desarrollan en el control realmente buscan por si solo prevenir o detectar las causas que pueden dar origen al riesgo.

Con corte a 31 de enero se publicó el Plan Anual de adquisiciones - PAA, donde se incluyen las líneas para contratación de personal en la modalidad de prestación de servicios para garantizar la operación tecnológica en la Entidad y la generación de información de la OTICs. Igualmente se realizó la actualización de la información frente a la contratación por prestación de servicios para mantener la operación tecnológica en la entidad. Ver enlace https://supertransporte.gov.co/documentos/2020/Agosto/Administrativa_25/PAA-2020-VERSION-18.xlsx.

**4. Cómo se realiza la actividad de control**
Se evidenció documento PAA-2020-VERSION-18.xlsx donde se realizó la programación de las necesidades del personal contratista:

Prestar sus servicios de apoyo a la gestión en la Oficina de Tecnologías de la Información y las Comunicaciones

- Soporte operación de la infraestructura tecnológica con que cuenta la entidad
- Acompañamiento en la implementación de proyectos de fortalecimiento

- Soporte técnico en servidores físicos y virtuales, para la correcta operación de la infraestructura tecnológica de la entidad
- Realizar actividades de recepción, clasificación y archivo documental, así como la radicación y trámite de memorandos y oficios que sean requeridos por la oficina
- Administración de la plataforma office 365 y página web de la entidad.
- Actividades para el mejoramiento de la arquitectura tecnológica de la entidad, especialmente para el desarrollo de software, aplicaciones WEB, internet y bases de datos, en servidores Linux y Windows.
- Prestación de servicios especializados de fábrica de software para atender los requerimientos de los sistemas de información misionales de la superintendencia de transporte
- Contratistas de Prestación de Servicios Profesionales. Entre otros.

**5. Qué pasa con las observaciones o desviaciones**
Se evidenció documento PAA-2020-VERSION-18.xlsx donde se realizó la programación de las necesidades del personal contratista.

**6. Evidencia de la ejecución del control**
Se evideció rastro de la ejecución del control que permite a cualquier tercero con la evidencia llegar a la misma conclusión.

**Análisis de los resultados de los riesgos:**

**2. Riesgo Operativo: Falta de personal para la operación del Centro de Cómputo.** Presenta solidez del conjunto de controles para la adecuada mitigación de este (Rango Fuerte = Fuerte), por tal razón no debe establecer acciones para fortalecer el control. Ver Tabla 01.

**OFICINA DE CONTRO INTERNO**
**FORMATO BASADO EN LA GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS- V4 -OCT.2018**

**NOMBRE DE LA DEPENCIA: Oficina de Tecnologías de la Información y las Comunicaciones**
**PROCESO: Proceso Transversal Gestión TICS**
**RESPONSABLE DEL PROCESO: Carlos Oscar Quintero - Asesor del Despacho - Oficina de Tecnologías de la Información y las Comunicaciones**
**FECHA INFORME EVALUACIÓN: 16-06-2020**

**Tabla 01**
**PESO PARTICIPACIÓN DE CADA VARIABLE EN EL DISEÑO DEL CONTROL PARA LA MITIGACIÓN DEL RIESGO**

| Proceso Estratégico y Transversal - Direccionamiento Estratégico<br>PESO O PARTICIPACIÓN DE CADA VARIABLE EN EL DISEÑO DEL CONTROL PARA LA MITIGACIÓN DEL RIESGO | | | CALIFICACIÓN DEL CONTROL RIESGOS DE GESTIÓN<br>2. Operativo<br>Falta de personal para la operación del Centro de Cómputo |
|---|---|---|---|
| CRITERIO DE EVALUACIÓN | OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN | PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL | 1. Inclusión al finalizar cada vigencia, de los items de las contrataciones en el PAA |
| 1.1 Asignación del responsable | Asignado | 15 | 15 |
| | No Asignado | 0 | |
| 1.2 Segregación y autoridad del responsable | Adecuado | 15 | 15 |
| | Inadecuado | 0 | |
| 2. Periodicidad | Oportuna | 15 | 15 |
| | Inoportuna | 0 | |
| 3. Propósito | Prevenir | 15 | 15 |
| | Detectar | 10 | |
| | No es un control | 0 | |
| 4. Cómo se realiza la actividad de control | Confiable | 15 | 15 |
| | No confiable | 0 | |
| 5. Qué pasa con las observaciones o desviaciones | Se investigan y resuelven oportunamente | 15 | 15 |
| | No se investigan y resuelven oportunamente | 0 | |
| 6. Evidencia de la ejecución del control | Completa | 10 | 10 |
| | Incompleta | 5 | |
| | No existe | 0 | |
| PESO TOTAL DE LA EVALUACIÓN DEL DISEÑO DEL CONTROL | | | 100 |
| | | | RANGO FUERTE |

**Fuente:** Análisis Auditor Oficina de Control Interno - OCI
Tabla eleboración propia de los auditores de OCI.

- **Riesgo 3.** Seguridad Dígital: Afectación de la integridad de los datos de los Sistemas de Información de la Entidad.
- **Controles**:

**1.1 Asignación del Responsable**

Se evidenció en el Mapa de Riesgo del Proceso Transversal Gestión TICS que el responsable Carlos Oscar Quintero - Asesor del Despacho / Maximino Vargas - Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

**Recomendación**

Actualizar en el Mapa de Riesgos del Proceso Transversal Gestión TICS el responsable.

**1.2 Segregación y autoridad del responsable**

Se evidenció que el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC es el responsable del Proceso Transversal Gestión TICS tiene la autoridad y adecuada segregación de funciones en la ejecución del control.

**2. Periodicidad**

Se evidenció fecha de seguimiento en el Mapa de Riesgos allegado por la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC**.**

**3. Propósito**

Se evidenció en documento PDF denominado3_Activación de la regla DoS.pdf, activación de la regla DoS (At
aque de denegación de servicios) en el FortiWeb , con el fin de evitar peticiones o conexiones masivas de usuarios ocasionando bloquear los servicios.

**4. Cómo se realiza la actividad de control**

Se evidenció en el aplicativo FortiWeb la activación de la regla DoS (Ataques de denegación de servicios) evitando la conexión masiva de usuarios ocasionando bloquear los servicios:

1. Predefined, HTTP Session Based Prevention: Enable, HTTP Dos Prevention: Enable.
2. Web_site, HTTP Session Based Prevention: Enable, HTTP Dos Prevention: Enable.

**5. Qué pasa con las observaciones o desviaciones**

Se realizó seguimiento al doble factor de autenticación a usuarios: Gestion documental y notificaciones.xlsx, Hablitación FMA concesiones.xlsx, meetingAttendanceList (1) (1).csv y meetingAttendanceList (2) (1).csv

**6. Evidencia de la ejecución del control**

Se dejó evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión.

**Análisis de los resultados de los riesgos:**

**3. Riesgo Seguridad Dígital: Afectación de la integridad de los datos de los Sistemas de Información de la Entidad.** Presenta solidez del conjunto de controles para la adecuada mitigación de este (Rango Fuerte = Fuerte), por tal razón no debe establecer acciones para fortalecer el control. Ver Tabla 2.

**OFICINA DE CONTRO INTERNO**
**FORMATO BASADO EN LA GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS- V4 -OCT.2018**

**NOMBRE DE LA DEPENCIA: Oficina de Tecnologías de la Información y las Comunicaciones**
**PROCESO: Proceso Transversal Gestión TICS**
**RESPONSABLE DEL PROCESO: Carlos Oscar Quintero – Asesor del Despacho – Oficina de Tecnologías de la Información y las Comunicaciones**
**FECHA INFORME EVALUACIÓN: 16-06-2020**

**Tabla 02**
**PESO PARTICIPACIÓN DE CADA VARIABLE EN EL DISEÑO DEL CONTROL PARA LA MITIGACIÓN DEL RIESGO**

| Proceso Estratégico y Transversal – Direccionamiento Estratégico<br>PESO O PARTICIPACIÓN DE CADA VARIABLE EN EL DISEÑO DEL CONTROL PARA LA MITIGACIÓN DEL RIESGO | | | CALIFICACIÓN DEL CONTROL RIESGOS DE GESTIÓN |
|---|---|---|---|
| | | | 3. Seguridad Dígital Afectación de la integridad de los datos de los Sistemas de Información de la Entidad |
| CRITERIO DE EVALUACIÓN | OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN | PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL | 1. Se desarrollan tablas de auditoría a las base de datos de los sistemas misionales. |
| 1.1 Asignación del responsable | Asignado | 15 | 15 |
| | No Asignado | 0 | |
| 1.2 Segregación y autoridad del responsable | Adecuado | 15 | 15 |
| | Inadecuado | 0 | |
| 2. Periodicidad | Oportuna | 15 | 15 |
| | Inoportuna | 0 | |
| 3. Propósito | Prevenir | 15 | 15 |
| | Detectar | 10 | |
| | No es un control | 0 | |
| 4. Cómo se realiza la actividad de control | Confiable | 15 | 15 |
| | No confiable | 0 | |
| 5. Qué pasa con las observaciones o desviaciones | Se investigan y resuelven oportunamente | 15 | 15 |
| | No se investigan y resuelven oportunamente | 0 | |
| 6. Evidencia de la ejecución del control | Completa | 10 | 10 |
| | Incompleta | 5 | |
| | No existe | 0 | |
| PESO TOTAL DE LA EVALUACIÓN DEL DISEÑO DEL CONTROL | | | 100 |
| | | | RANGO FUERTE |

**Fuente:** Análisis Auditor Oficina de Control Interno - OCI
Tabla eleboración propia de los auditores de OCI.

- **Riesgo 4.** Estratégico: Reporte de seguimiento de Planes Institucionales fuera de las fechas establecidas.

- **Controles**:

**1.1 Asignación del Responsable**

Se evidenció en el Mapa de Riesgo del Proceso Transversal Gestión TICS que el responsable Carlos Oscar Quintero - Asesor del Despacho / Maximino Vargas - Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

**Recomendación**

Actualizar en el Mapa de Riesgos del Proceso Transversal Gestión TICS el responsable.

**1.2 Segregación y autoridad del responsable**

Se evidenció que el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC es el responsable del Proceso Transversal Gestión TICS tiene la autoridad y adecuada segregación de funciones en la ejecución del control.

**2. Periodicidad**

Se evidenció fecha de seguimiento en el Mapa de Riesgos allegado por la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

**3. Propósito**

Se evidenció seguimiento en documento PDF denominado 4_Application Risk and Control.pdf, eventos reportados en el WAF, reporte del firewall sobre el listado de aplicaciones de alto riesgo monitoreadas. Este informe proporció los resultados del análisis de riesgos de aplicaciones que Fortinet realizó para la Entidad.

**4. Cómo se realiza la actividad de control**

Se evidenció documento PDF denominado 4_Application Risk and Control.pdf generado por FORTINET, este informe evidencia los eventos de seguridad críticos y de alto riesgo detectados para el mes de agosto.

**5. Qué pasa con las observaciones o desviaciones**

Se evidenció seguimiento al reporte de riesgos y controles, MONITOREO DE RED y VPN.pdf, seguimiento a las aplicaciones que se ejecutan en la red y da como resultado una mejor toma de decisiones para las políticas generales de control de aplicaciones gestión de riesgos comerciales.

**6. Evidencia de la ejecución del control**

Se evideció rastro de la ejecución del control que permite a cualquier tercero con la evidencia llegar a la misma conclusión.

**Análisis de los resultados de los riesgos:**

**4. Riesgo Seguridad Dígital: Acceso no autorizado a la red.** Presenta solidez del conjunto de controles para la adecuada mitigación de este (Rango Fuerte = Fuerte), por tal razón no debe establecer acciones para fortalecer el control. Ver Tabla 3.

**OFICINA DE CONTRO INTERNO**
**FORMATO BASADO EN LA GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS- V4 -OCT.2018**

**NOMBRE DE LA DEPENCIA: Oficina de Tecnologías de la Información y las Comunicaciones**
**PROCESO: Proceso Transversal Gestión TICS**
**RESPONSABLE DEL PROCESO: Carlos Oscar Quintero - Asesor del Despacho - Oficina de Tecnologías de la Información y las Comunicaciones**
**FECHA INFORME EVALUACIÓN: 16-06-2020**

**Tabla 03**
**PESO PARTICIPACIÓN DE CADA VARIABLE EN EL DISEÑO DEL CONTROL PARA LA MITIGACIÓN DEL RIESGO**

| Proceso Estratégico y Transversal - Direccionamiento Estratégico<br>PESO O PARTICIPACIÓN DE CADA VARIABLE EN EL DISEÑO DEL CONTROL PARA LA MITIGACIÓN DEL RIESGO | | | CALIFICACIÓN DEL CONTROL RIESGOS DE GESTIÓN<br>4. Seguridad Dígital<br>Acceso no autorizado a la red. |
|---|---|---|---|
| CRITERIO DE EVALUACIÓN | OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN | PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL | 1. Se realiza seguimiento a las políticas del firewall implementado. |
| 1.1 Asignación del responsable | Asignado | 15 | 15 |
| | No Asignado | 0 | |
| 1.2 Segregación y autoridad del responsable | Adecuado | 15 | 15 |
| | Inadecuado | 0 | |
| 2. Periodicidad | Oportuna | 15 | 15 |
| | Inoportuna | 0 | |
| 3. Propósito | Prevenir | 15 | 15 |
| | Detectar | 10 | |
| | No es un control | 0 | |
| 4. Cómo se realiza la actividad de control | Confiable | 15 | 15 |
| | No confiable | 0 | |
| 5. Qué pasa con las observaciones o desviaciones | Se investigan y resuelven oportunamente | 15 | 15 |
| | No se investigan y resuelven oportunamente | 0 | |
| 6. Evidencia de la ejecución del control | Completa | 10 | 10 |
| | Incompleta | 5 | |
| | No existe | 0 | |
| PESO TOTAL DE LA EVALUACIÓN DEL DISEÑO DEL CONTROL | | | 100 |
| | | | RANGO FUERTE |

**Fuente:** Análisis Auditor Oficina de Control Interno - OCI
Tabla eleboración propia de los auditores de OCI.

- **Riesgo 5.** Seguridad Dígital: Ataques informáticos.

- **Controles**:

**1.1 Asignación del Responsable**

Se evidenció en el Mapa de Riesgo del Proceso Transversal Gestión TICS que el responsable Carlos Oscar Quintero - Asesor del Despacho / Maximino Vargas - Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

**Recomendación**

Actualizar en el Mapa de Riesgos del Proceso Transversal Gestión TICS el responsable.

**1.2 Segregación y autoridad del responsable**

Se evidenció que el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC es el responsable del Proceso Transversal Gestión TICS tiene la autoridad y adecuada segregación de funciones en la ejecución del control.

**2. Periodicidad**

Se evidenció fecha de seguimiento en el Mapa de Riesgos allegado por la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

**3. Propósito**

Se evidenció documento PDF denominado 5_bloqueo de ips maliciosas.pdf, donde se identificó las direcciones ip´s maliciosas evidenciadas en el reporte No. 12 del CSIRT en las listas negras del firewall.

**4. Cómo se realiza la actividad de control**

Se realizó seguimiento e implemento el bloqueo de las Ip´s registradas en el reporte No. 12 del CRIST en las listas negras del firewall, documento PDF denominado 5_bloqueo de ips maliciosas.pdf.

**5. Qué pasa con las observaciones o desviaciones**

Se realizó seguimiento e implemento el bloqueo de las Ip´s registradas en el reporte No. 12 del CRIST en las listas negras del firewall, documento PDF denominado 5_bloqueo de ips maliciosas.pdf.

**6. Evidencia de la ejecución del control**

Se evideció rastro de la ejecución del control que permite a cualquier tercero con la evidencia llegar a la misma conclusión.

**Análisis de los resultados de los riesgos:**

**5. Riesgo Seguridad Dígital: Ataques informáticos.** Presenta solidez del conjunto de controles para la adecuada mitigación de este (Rango Fuerte = Fuerte), por tal razón no debe establecer acciones para fortalecer el control. Ver Tabla 4.

**OFICINA DE CONTRO INTERNO**
**FORMATO BASADO EN LA GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS- V4 -OCT.2018**

**NOMBRE DE LA DEPENCIA: Oficina de Tecnologías de la Información y las Comunicaciones**
**PROCESO: Proceso Transversal Gestión TICS**
**RESPONSABLE DEL PROCESO: Carlos Oscar Quintero - Asesor del Despacho - Oficina de Tecnologías de la Información y las Comunicaciones**
**FECHA INFORME EVALUACIÓN: 16-06-2020**

**Tabla 04**
**PESO PARTICIPACIÓN DE CADA VARIABLE EN EL DISEÑO DEL CONTROL PARA LA MITIGACIÓN DEL RIESGO**

| Proceso Estratégico y Transversal - Direccionamiento Estratégico<br>PESO O PARTICIPACIÓN DE CADA VARIABLE EN EL DISEÑO DEL CONTROL PARA LA MITIGACIÓN DEL RIESGO | | | CALIFICACIÓN DEL CONTROL RIESGOS DE GESTIÓN |
|---|---|---|---|
| | | | 5. Seguridad Dígital Ataques informáticos |
| CRITERIO DE EVALUACIÓN | OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN | PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL | 1. Revisión de seguridad informática en los controles de acceso a los sistemas de información. |
| 1.1 Asignación del responsable | Asignado | 15 | 15 |
| | No Asignado | 0 | |
| 1.2 Segregación y autoridad del responsable | Adecuado | 15 | 15 |
| | Inadecuado | 0 | |
| 2. Periodicidad | Oportuna | 15 | 15 |
| | Inoportuna | 0 | |
| 3. Propósito | Prevenir | 15 | 15 |
| | Detectar | 10 | |
| | No es un control | 0 | |
| 4. Cómo se realiza la actividad de control | Confiable | 15 | 15 |
| | No confiable | 0 | |
| 5. Qué pasa con las observaciones o desviaciones | Se investigan y resuelven oportunamente | 15 | 15 |
| | No se investigan y resuelven oportunamente | 0 | |
| 6. Evidencia de la ejecución del control | Completa | 10 | 10 |
| | Incompleta | 5 | |
| | No existe | 0 | |
| PESO TOTAL DE LA EVALUACIÓN DEL DISEÑO DEL CONTROL | | | 100 |
| | | | RANGO FUERTE |

**Fuente:** Análisis Auditor Oficina de Control Interno - OCI
Tabla eleboración propia de los auditores de OCI.

- **Riesgo 6.** Estratégico: Reporte de seguimiento de Planes Institucionales fuera de las fechas establecidas.
- **Controles**:

**1.1 Asignación del Responsable**

Se evidenció en el Mapa de Riesgo del Proceso Transversal Gestión TICS que el responsable Carlos Oscar Quintero - Asesor del Despacho / Maximino Vargas - Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

**Recomendación**

Actualizar en el Mapa de Riesgos del Proceso Transversal Gestión TICS el responsable.

**1.2 Segregación y autoridad del responsable**

Se evidenció que el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC es el responsable del Proceso Transversal Gestión TICS tiene la autoridad y adecuada segregación de funciones en la ejecución del control.

**2. Periodicidad**

Se evidenció fecha de seguimiento en el Mapa de Riesgos allegado por la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

**3. Propósito**

No se observó evidencia de la participación en el proceso de adquisición del software de inventarios que garantice el ciclo de vida de los bienes y servicios. Archivo Soporte: 6_Estudios Previos Software COMENTARIOS 1.docx.

**4. Cómo se realiza la actividad de control**

No se observó evidencia de la participación en el proceso de adquisición del software de inventarios que garantice el ciclo de vida de los bienes y servicios. Archivo Soporte: 6_Estudios Previos Software COMENTARIOS 1.docx.

**5. Qué pasa con las observaciones o desviaciones**

No se observó evidencia de la participación en el proceso de adquisición del software de inventarios que garantice el ciclo de vida de los bienes y servicios. Archivo Soporte: 6_Estudios Previos Software COMENTARIOS 1.docx.

**6. Evidencia de la ejecución del control**

No se evideció rastro de la ejecución del control que permite a cualquier tercero con la evidencia llegar a la misma conclusión.

**Análisis de los resultados de los riesgos:**

**6. Riesgo Estratégico: Reporte de seguimiento de Planes Institucionales fuera de las fechas establecidas.** Presenta solidez del conjunto de controles para la adecuada mitigación de este (Rango Debil = Debil), por tal razón debe establecer acciones para fortalecer el control. Ver Tabla 5.

**OFICINA DE CONTRO INTERNO**
**FORMATO BASADO EN LA GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS- V4 -OCT.2018**

**NOMBRE DE LA DEPENCIA: Oficina de Tecnologías de la Información y las Comunicaciones**
**PROCESO: Proceso Transversal Gestión TICS**
**RESPONSABLE DEL PROCESO: Carlos Oscar Quintero - Asesor del Despacho - Oficina de Tecnologías de la Información y las Comunicaciones**
**FECHA INFORME EVALUACIÓN: 16-06-2020**

**Tabla 05**
**PESO PARTICIPACIÓN DE CADA VARIABLE EN EL DISEÑO DEL CONTROL PARA LA MITIGACIÓN DEL RIESGO**

| Proceso Estratégico y Transversal - Direccionamiento Estratégico<br>PESO O PARTICIPACIÓN DE CADA VARIABLE EN EL DISEÑO DEL CONTROL PARA LA MITIGACIÓN DEL RIESGO | | | CALIFICACIÓN DEL CONTROL RIESGOS DE GESTIÓN<br>6. Tecnológico Perdida de Equipos de Cómputo |
|---|---|---|---|
| CRITERIO DE EVALUACIÓN | OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN | PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL | 1. Control de inventario de los activos tecnológicos existentes en la entidad. |
| 1.1 Asignación del responsable | Asignado | 15 | 15 |
| | No Asignado | 0 | |
| 1.2 Segregación y autoridad del responsable | Adecuado | 15 | 15 |
| | Inadecuado | 0 | |
| 2. Periodicidad | Oportuna | 15 | 0 |
| | Inoportuna | 0 | |
| 3. Propósito | Prevenir | 15 | 0 |
| | Detectar | 10 | |
| | No es un control | 0 | |
| 4. Cómo se realiza la actividad de control | Confiable | 15 | 0 |
| | No confiable | 0 | |
| 5. Qué pasa con las observaciones o desviaciones | Se investigan y resuelven oportunamente | 15 | 0 |
| | No se investigan y resuelven oportunamente | 0 | |
| 6. Evidencia de la ejecución del control | Completa | 10 | 0 |
| | Incompleta | 5 | |
| | No existe | 0 | |
| PESO TOTAL DE LA EVALUACIÓN DEL DISEÑO DEL CONTROL | | | 30 |
| | | | RANGO DEBIL |

**Fuente:** Análisis Auditor Oficina de Control Interno - OCI
Tabla eleboración propia de los auditores de OCI.

**Recomendaciones**

- Actualizar y publicar el Mapa de Riesgos firmado por el responsable del proceso.

**6.5 Verificar el cumplimiento de las actividades de los roles frente a las responsabilidades establecidas por línea de defensa en la política de administración del riesgo.**

**Prueba Realizada**

Se evidenció el seguimiento al mapa de riesgos del proceso Transversal Gestión de TICS.

**Situaciones evidenciadas**

**2. Operativo: Falta de personal para la operación del Centro de Cómputo.**

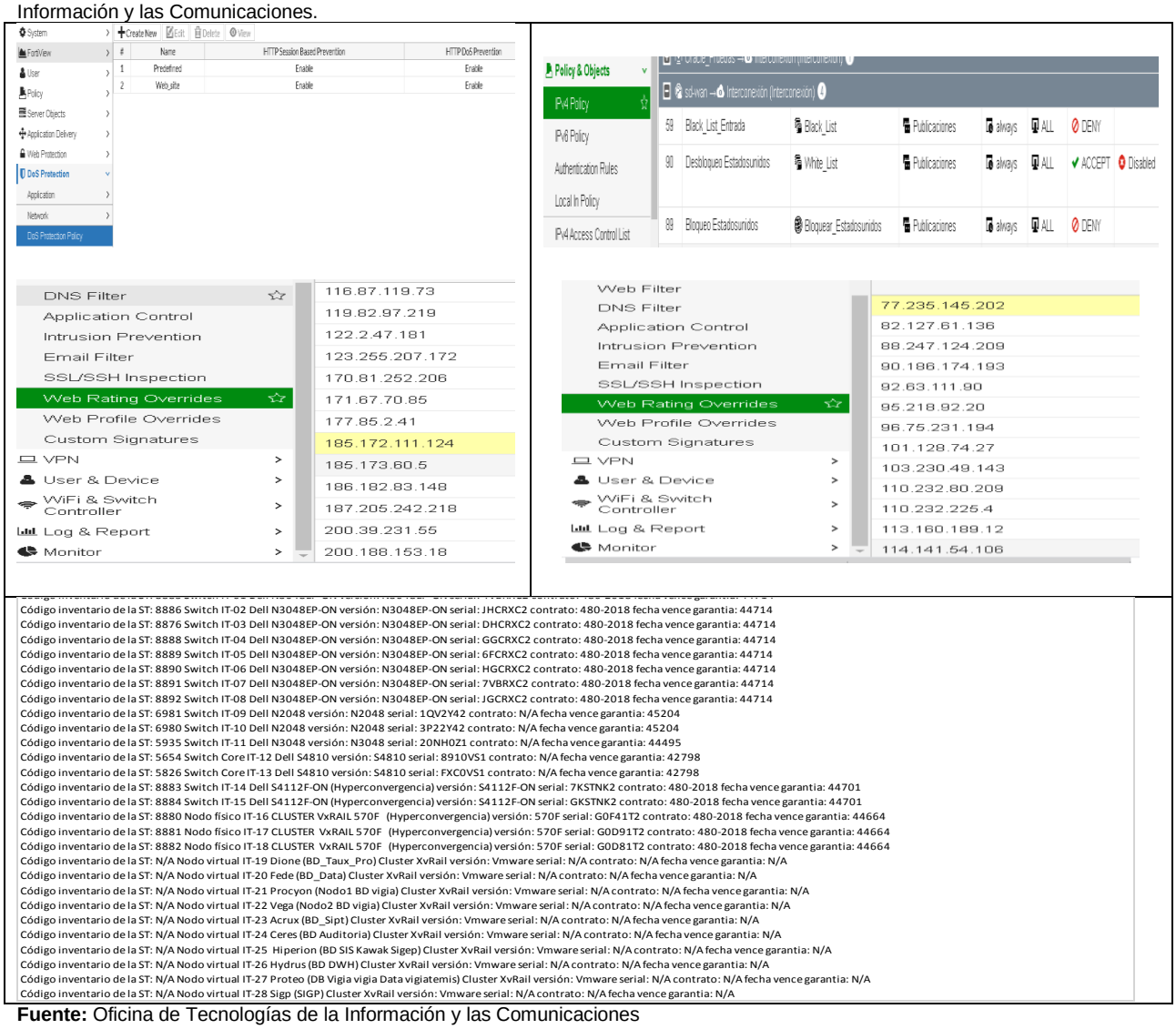
**Acciones:**

1. Solicitud de la contratación con suficiente tiempo de anticipación para agilizar el proceso de contratación.
2. Creación de una estructura de Oficina de Tecnologías de acuerdo al decreto 2409 de 2018.
3. Inclusión de actividades en el Proyecto de Inversión para garantizar la adqusición de soluciones y servicios que soporten la operación tecnológica de la entidad.

El Auditor evidenció con corte a 31 de enero que se publicó el Plan Anual de adquisiciones - PAA, donde se observó las líneas para contratación de personal en la modalidad de prestación de servicios para garantizar la operación tecnológica en la Entidad y la generación de información de la OTICs. se realizó la actualización de la información frente a la contratación por prestación de servicios para mantener la operación tecnológica en la Entidad https://supertransporte.gov.co/documentos/2020/Agosto/Administrativa_25/PAA-2020-VERSION-18.xlsx

Se evidenció la creación de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC de acuerdo a lo establecido en el Decreto 2409 de 2018 adoptando en la cadena de valor el Proceso Transversal Gestión TICS y el fortalecimiento de su infraestructura a través de sus dispositivos, como Fortinet que tiene la capacidad de identificar el uso de aplicaciones externas que se utilizan en la red y realizar bloqueo selectivo para minimizar el riesgo por perdida de datos, activación de la regla DoS (Ataques denegación de servicios) a través del aplicativo FortiWeb el cual evita peticiones o conexiones masivas externos buscando bloquear los servicios de red de la Entidad, también permite realizar bloqueos de accesos maliciosos por ataques a de IPs de otros países.
Igualmente, se evidenció infraestructura física de los dispositivos de la Entidad(muestra aleatoria) que fortalecen la infraestructura física de la Entidad. Ver Imagen 18.

**Imagen 18.** Dispositivos que fortalecen la Infraestructura de la Superintendencia de Transporte Oficina de Tecnologías de la Información y las Comunicaciones.




**Fuente:** Oficina de Tecnologías de la Información y las Comunicaciones

## 3. Seguridad Digital: Afectación de la integridad de los datos de los Sistemas de Información de la Entidad

**Acciones:**

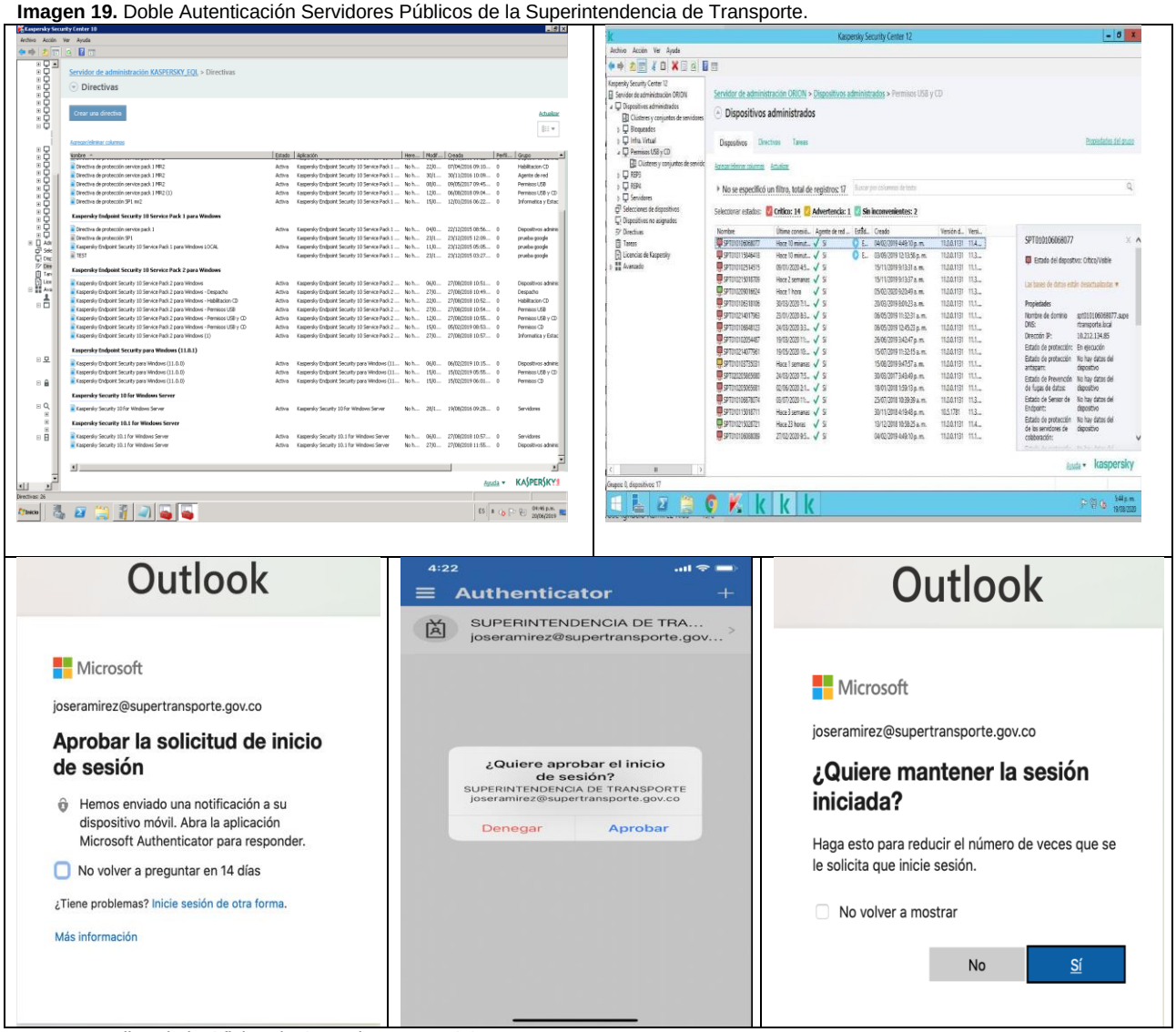
1. Seguimiento semanal de las tablas de auditoria implementadas para cada sistema de información.
2. Restricción o control de puertos USB y acceso a páginas web de transferencia de archivos. Política de Seguridad de la Información.
3. Los nuevos desarrollos en la entidad contemplan logs de auditoría a nivel de tablas de bases de datos.

Activación de la regla DoS (Ataque de denegación de servicios) en el FortiWeb, con el fin de evitar peticiones o conexiones masivas de usuarios ocasionando bloquear los servicios. Soporte: 3_Activación de la regla DoS.pdf

El Auditor evidenció la implementación del doble factor de autenticación para el ingreso a las cuentas de usuario de office 365 de los funcionarios y contratistas de la Entidad. Soporte: capacitaciones seguridad.rar

Se evidenció documento de la verificación de la regla de restricción de USB de los equipos que están y no autorizados, documento PDF denominado H4 2019 AC VerificacionRegla USB.pdf. Ver Imagen 19.

**Imagen 19.** Doble Autenticación Servidores Públicos de la Superintendencia de Transporte.




**Fuente:** Auditor de la Oficina de Control Interno – OCI

**4. Seguridad Digital: Accesos no autorizados a la red.**

**Acciones:**

1. Se configuró el firewall con integración al directorio activo de la entidad, y doble control de autenticación para usuarios de administración del firewall.
2. Configuración de reglas con la limitación únicamente a los puertos necesarios de navegación, implementación de reglas por perfiles y filtrado web, filtrado de aplicación e implementación de logs.
3. Ajustar la configuración del firewall al detectar accesos desde url´s sospechosas o reportadas por otras entidades.
4. Implementación de reglas de filtrado de contenidos en el WAF.

El Auditor observó que el aplicativo FORTINET generó informe de seguimiento con fecha 3 de agosto de 2020, reporte del firewall sobre el listado de aplicaciones de alto riesgo monitoreadas. Se identificó las 20 principales aplicaciones de alto riesgo, de las cuales se muestran a continuación las de nivel de riesgo 5 (riesgo crítico) y 4 (riesgo alto). Cada aplicación se enumera con su respectiva categoría, tecnología, número de usuarios, ancho de banda y sesiones. FortiGuard Labs ha determinado que estas aplicaciones representan posibles vectores para el compromiso de datos, la intrusión de la red o una reducción en el rendimiento de la red.), documento PDF denominado 4_Application Risk and Control.pdf. Ver Imagen 20.

**Imagen 20.** Aplicaciones con mayor riesgo en la Internet

| # | Risk | Application Name | Category | Technology | User | Bandwidth | Session |
|---|---|---|---|---|---|---|---|
| 1 | 5 | SurfEasy.VPN | Proxy | Client-Server | 2 | 0 B | 6 |
| 2 | 4 | TeamViewer | Remote.Access | Client-Server | 6 | 969.55 MB | 590,975 |
| 3 | 4 | AnyDesk | Remote.Access | Client-Server | 7 | 504.10 MB | 198,879 |
| 4 | 4 | Thunder.Xunlei | P2P | Peer-to-Peer | 1 | 3.53 MB | 1,064 |
| 5 | 4 | VNC | Remote.Access | Client-Server | 1 | 208 B | 1 |
| 6 | 4 | RDP | Remote.Access | Client-Server | 1 | 260 B | 1 |

**Fuente:** Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

**5. Seguridad Digital: Ataques informáticos.**

**Acciones:**

1. Revisión y ajuste del código fuente de los aplicativos desarrollados en la Superintendencia para implementar controles de acceso y aplicar una función de ScriptCase para evitar la inyección de sql en el logueo al aplicativo.
2. Se adopta el desarrollo en otros frameworks como .NET y APEX.
3. Se realizan los desarrollos desacoplados para evitar conexión directa a la base de datos.

Se evidenció documento PDF denominado 5_bloqueo de ips maliciosas.pdf, en el que se encuentra el reporte sobre el incidente de seguridad presentado en algunas cuentas office de la Entidad, con los bloqueos de IP's maliciosas reportadas por el CSIR de la Policía nacional 77.235.145.202 y 185.172.111.124. Ver Imagen 13.

**6. Tecnológico: Pérdida de Equipos de Cómputo.**
**Acciones:**

1. Actualización del inventario de equipos de cómputo asignado por usuario y gestionado a través de la herramienta GLPI.
2. Actualización y generación de alertas por asignación, cambio y actualización.

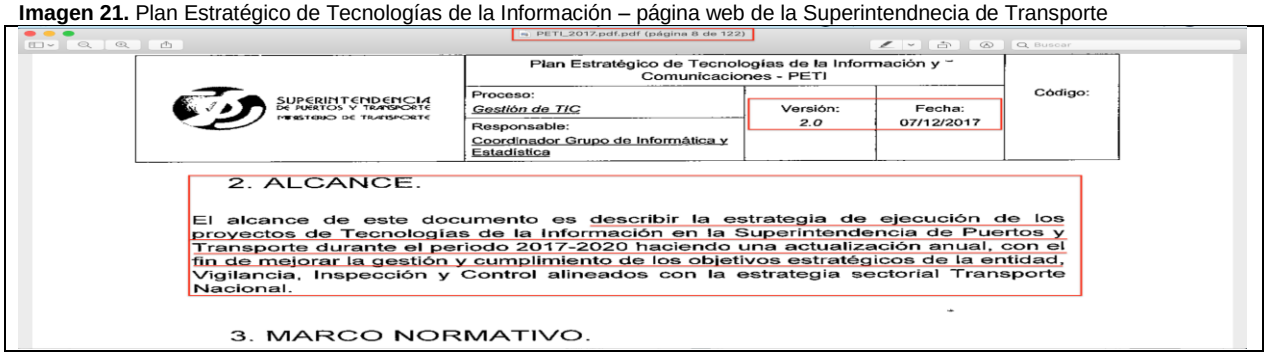
No se observó evidencia de la herramienta GLPI, ni archivo Soporte denominado 6_Estudios Previos Software COMENTARIOS 1.docx, de la participación en el proceso de adquisición del software de inventarios que garantice el ciclo de vida de los bienes y servicios.

**Respuesta de la Oficina de Control Interno - OCI a las observaciones presentadas por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC**

**Respuesta OCI hallazgo H01A-011 dicv20-(AC)GTICS**
Con base en las observaciones realizadas en el memorando radicado en Orfeo número 20201100074943 de 21 de diciembre de 2020, al Informe preliminar de auditoría al Proceso Gestión de TICS política de seguridad y privacidad de la información de la Superintendencia de Transporte y Evaluación de riesgos y controles - Política de Administración del Riesgo del 1 enero a 31 de octubre de 2020 - Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, el auditor de la OCI evidenció en el alcance del documento PETI_2017.pdf "***El alcance de este documento es describir la estrategia de ejecución de los proyectos de Tecnologías de la Información en la Superintendencia de Puertos y Transporte durante el periodo 2017-2020 haciendo una actualización anual****, con el fin de mejorar la gestión y cumplimiento de los objetivos estratégicos de la entidad, Vigilancia, Inspección y Control alineados con la estrategia sectorial Transporte Nacional.",* este documento se encontraba publicado en la página web de la Entidad, sólo se evidenció el PETI para las vigencias 2021-2022 y no se observó la versión anterior 2017 a 2020, en este sentido, es importante indicar que deben estar publicadas todas las versiones, para dar cumplimiento a la Ley 1712, como se observa en las siguientes imágenes:

El hallazgo **H01A-011 dicv20-(AC)GTICS** se mantiene. Ver Imagen 21

**Imagen 21.** Plan Estratégico de Tecnologías de la Información – página web de la Superintendnecia de Transporte


PETI_2017.pdf.pdf (página 8 de 122)

| | Plan Estratégico de Tecnologías de la Información y Comunicaciones - PETI | | | Código: |
|---|---|---|---|---|
| SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE MINISTERIO DE TRANSPORTE | Proceso: Gestión de TIC | Versión: 2.0 | Fecha: 07/12/2017 | |
| | Responsable: Coordinador Grupo de Informática y Estadística | | | |

2. ALCANCE.

El alcance de este documento es describir la estrategia de ejecución de los proyectos de Tecnologías de la Información en la Superintendencia de Puertos y Transporte durante el periodo 2017-2020 haciendo una actualización anual, con el fin de mejorar la gestión y cumplimiento de los objetivos estratégicos de la entidad, Vigilancia, Inspección y Control alineados con la estrategia sectorial Transporte Nacional.

3. MARCO NORMATIVO.


**Fuente:** Evidencias de la OCI y Página web de la Superintendencia de Transporte

**Respuesta OCI hallazgo H01A-011 dicv20-(AC)GTICS**

**Recomendaciones**

- El PETI aprobado es para la vigencia 2021-2022, se publicó el 21 de diciembre de 2020 para la vigencia 2020-2022, modificar el documento y la periodicidad de la publicación en la página web de la Entidad.
- Volver a publicar el PETI 2017-2020 en la página web de la Superintendencia de Transporte, hay que conservar la traza.
- Hacer monitoreo y seguimiento a la ejecución de las actividades del PETI, asegurando adicionalmente la ejecución de recursos que tengan asignadas las actividades para el cumplimiento de metas y prevenir la posible materialización de riesgos.

**Respuesta OCI H02A-07dicv20-(AC)GTICS**

El auditor evidenció publicación del documento Plan Estratégico de Seguridad de la Información – PESI dando cumplimiento según programación del Plan de Acción Institucional – PAI vigencia 2020 y publicado el 21 de diciembre de 2020 en el siguiente enlace de la página web de la Entidad https://www.supertransporte.gov.co/documentos/2020/Diciembre/OTIC_21/PLAN-DE-SEGURIDAD-Y-PRIVACIDAD-DE-LA-INFORMACION-PESI-1.0-2020-2022.pdf, respecto al PESI se omite del hallazgo, sin embargo no observó Plan de contingencia de TI, ni el Plan de tratamiento de riesgos de TI se encuentran publicados en la página web de la Superintendencia de Transporte a la fecha, el hallazgo se mantiene respecto a estos planes.

El hallazgo queda redactado de la siguiente forma:

**Hallazgo 002 de 2020 (AC Acción Correctiva)**
**H02A-07dicv20-(AC)GTICS**

El documento Plan de contingencia de TI , ni el Plan de tratamiento de riesgos de TI se encuentran publicados en la página web de la Superintendencia de Transporte a la fecha.
Se incumple el Artículo 2.2.22.3.14*. "Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: (…).*
Se incumple el numeral e. "*Asegurar la oportunidad y confiabilidad de la información y de sus registros*;", y numeral f. "*Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos;",* del Artículo 2º.- *"Objetivos del sistema de Control Interno. Atendiendo los principios constitucionales que debe caracterizar la administración pública, el diseño y el desarrollo del Sistema de Control Interno se orientará al logro de los siguientes objetivos fundamentales:* ", Ley 87 de 1993.

Situación que puede conllevar a la posible materialización de riesgos de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC en la vigencia 2020 impactando la gestión de la disponibilidad de recursos necesarios para alcanzar los objetivos institucionales y cumplir las funciones delegadas.

**Respuesta OCI O001A-26nov20-(AP)GTICS**

El hallazgo **H01A-011 dicv20-(AC)GTICS** se mantiene, no se proporciono evidencia para reevaluarlo.

## 7. CONCLUSIONES

El Sistema de Control Interno del Proceso de Gestión de TIC´s, es susceptible de mejora acorde con las recomendaciones realizadas por parte de la Oficina de Control Interno.

Los resultados de este informe y las evidencias obtenidas de acuerdo con los criterios definidos se refieren a los documentos aportados, consultados en la cadena de valor y verificados, no se hacen extensibles a otros soportes.

## 8. RECOMENDACIONES

Acorde con lo establecido en el proceso Seguimiento y Evaluación Independiente a la Gestión Institucional, procedimiento Auditorías Internas, Seguimiento y Evaluación frente al presente informe definitivo, se recibió la respectiva retroalimentación mediante memorando número 20201100074943 radicado en Orfeo y comunicado por el correo Institucional por la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC el día lunes 21 de diciembre de 2020, se procedió por parte del auditor a hacer nuevamente la verificación para posteriormente elaborar el presente informe definitivo, el informe queda en firme.

Los hallazgos y observaciones configurados requieren implementación de acciones, por lo cual se debe formular el respectivo plan de mejoramiento por parte del responsable de la

dependencia, el cual se encuentra dispuesto en la cadena de valor de la Entidad http://intranet.supertransporte.gov.co/CadenaValor/index.htm-Plan y se debe suscribir teniendo en cuenta la identificación del proceso y el (los) hallazgo(s)u observaciones que ha(n) sido señalada(s) en el presente informe, realizar el análisis de causas, determinar y ejecutar el plan de acción que elimine la causa raíz de la situación evidenciada, es importante que remitan el plan suscrito y en Excel a los correos joseramírez@supertransporte.gov.co y jefacturacontrolinterno@supertransporte.gov.co, para posterior seguimiento y verificación a la eficacia y efectividad de las acciones por parte del auditor (como Tercera Línea de Defensa). Allegar el plan de mejoramiento a más tardar el 6 de enero de 2021.

Se hace la salvedad, que las recomendaciones se hacen con el propósito de aportar a la mejora continua de los procesos; y estas se acogen y se implementan, por decisión del líder del proceso.

No obstante, la Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones" art. 12 - Funciones de los auditores internos. Serán funciones del asesor, coordinador, auditor interno o similar las siguientes: literal k) indica "Verificar que se implanten las medidas respectivas recomendadas".

Y en el Artículo 3º.- Características del Control Interno. Son características del Control Interno las siguientes:

a. "El Sistema de Control Interno forma parte integrante de los sistemas contables, financieros, de planeación, de información y operacionales de la respectiva entidad;

En cada área de la organización, el funcionario encargado de dirigirla es responsable por control interno ante su jefe inmediato de acuerdo con los niveles de autoridad establecidos en cada entidad".

Agradecemos su oportuna gestión, con el objetivo de fortalecer el Sistema de Control Interno de la Entidad.

**Alba Enidia Villamil Muñoz**
**Jefe Oficina de Control Interno**
**Coordinadora Plan Anual de Auditoría**

**José Ignacio Ramírez Ríos**
Profesional Especializado -OCI
Auditor responsable de la verificación

Elaboró y verificó: José Ignacio Ramírez Ríos Profesional Especializado- Auditor Oficina Control Interno – OCI.
C:\Users\joseramirez\Desktop\SPT-OCI\2020-200-CNTROL INTRNO\200-21.03\Informes de Auditoría\Gestión de TICS\InformeDefinitivo Auditoria TICS 24dic2020.docx