Primer Cuatrimestre
Riesgos de Seguridad de la información - 2025

Oficina de Tecnologías de la Información y las Comunicaciones

Junio

2025

Tabla de contenido

1.Introducción.

En cumplimiento a la Política de Administración de Riesgos de la Superintendencia de Transporte el Manual de Gestión de Riesgos de Seguridad y el Modelo de Seguridad y Privacidad de la Información, específicamente lo relacionado con el seguimiento a los Riesgos de Seguridad de la información definidos por los procesos, a continuación, se presentan los resultados evidenciados durante el primer cuatrimestre de la vigencia 2025.

El presente informe se realiza teniendo en cuenta la estructura de la cadena de valor de la entidad establecida bajo los artículos 17 y 18 de la resolución 518 de 2019, mediante el cual la entidad está conformada por 16 procesos entre estratégicos, misionales, de apoyo y de evaluación y control, los cuales son:

ESTRATÉGICOS.

1. Direccionamiento Estratégico.
2. Gestión del Conocimiento y la Innovación.
3. Gestión de Comunicaciones.
4. Gestión de TICS.

MISIONALES.

5. Vigilancia.
6. Inspección.
7. Control.
8. Gestión de relacionamiento con el ciudadano.

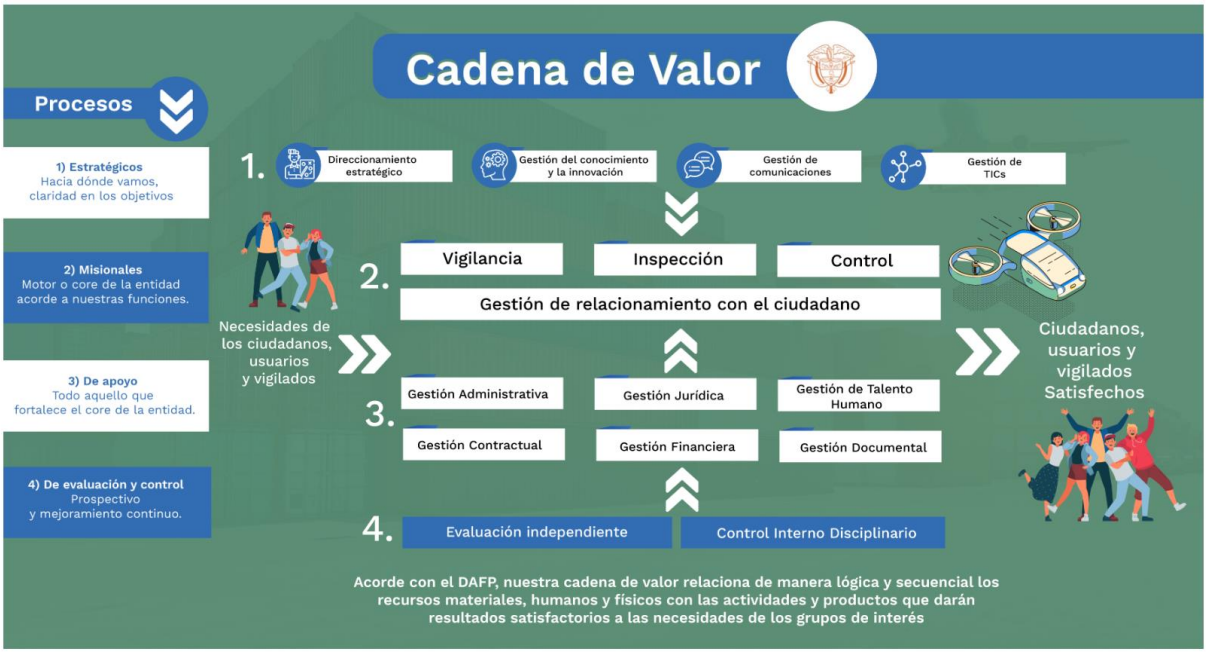
APOYO.

9. Gestión Administrativa.
10. Gestión Jurídica.
11. Gestión de Talento Humano.
12. Gestión Contractual.
13. Gestión Financiera.
14. Gestión Documental.

EVALUACIÓN Y CONTROL.

15. Evaluación independiente.
16. Control interno Disciplinario.

Ilustración 1. Cadena de Valor.



Fuente: Página Web Institucional.

2. Consideraciones previas.

- La Superintendencia de Transporte bajo el ejercicio establecido en la Política de Administración de Riesgos, en el proceso de gestión Tics en cabeza de la Oficina de las Tecnologías y las Comunicaciones, realiza el monitoreo de los controles asociados a los riesgos de Seguridad de la información de forma cuatrimestral con el fin de fortalecer la Gestión del Riesgo en la entidad protegiendo el cumplimiento de los objetivos establecidos para cada uno de los procesos.

- Se efectúa el cargue de las evidencias de los controles establecidos a los riesgos de forma cuatrimestral en el repositorio de la entidad denominado "*Repositorio Evidencias*" establecido por la Oficina Asesora de Planeación y que ha sido compartido con los responsables de la ejecución de los controles para desarrollar el ejercicio de seguimiento.

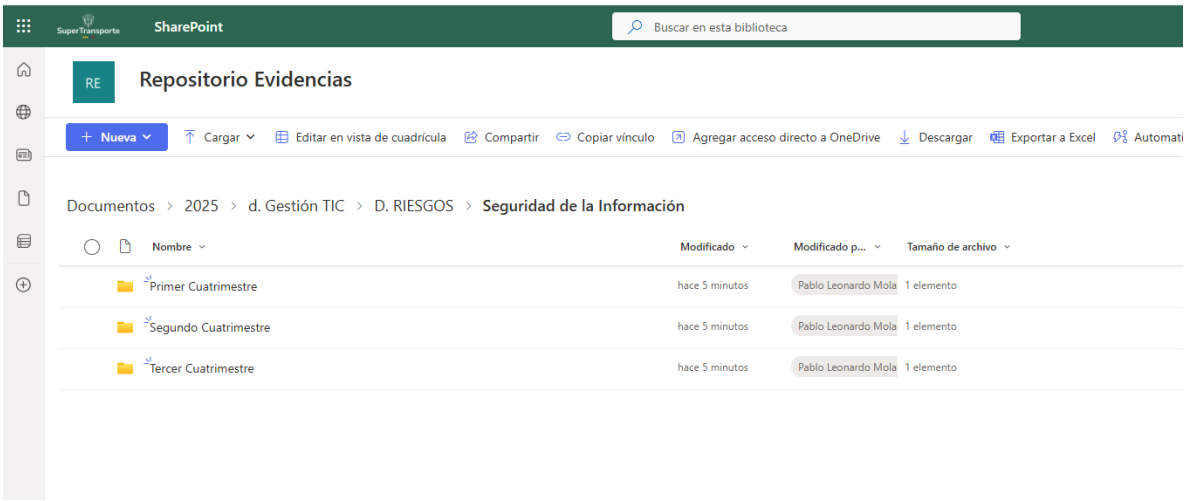
- La Entidad adopta la "*Guía para la Administración del Riesgo y el diseño de controles en entidades públicas*" del Departamento Administrativo de la Función Pública, que avanzó a su Versión 6, motivando la actualización de la Política de Administración de Riesgos de la entidad, documento que se encuentra actualizado y publicado en la intranet, así como en la cadena de valor bajo el código DE-PO-001 V5. Los riesgos y controles cumplen con lo establecidos.

3. Matriz de Riesgos de Seguridad de la Información.

Para el Primer Cuatrimestre del año 2025, se gestionaron los riesgos establecidos en la Matriz de Riesgos de seguridad de la información, la cual hace parte del Mapa de Riesgos Institucional Versión 3 y está disponible para consulta en el repositorio asignado por la Oficina Asesora de Planeación denominado "*Repositorio evidencias*" a la cual se puede acceder mediante el siguiente enlace:

https://supertransporte.sharepoint.com/sites/RepositorioEvidencias/Documentos%20compartidos/Forms/AllItems.aspx?id=%2Fsites%2FRepositorioEvidencias%2FDocumentos%20compartidos%2F2025%2Fd%2E%20Gesti%C3%B3n%20TIC%2FD%2E%20RIESGOS%2FSeguridad%20de%20la%20Informaci%C3%B3n&p=true&ct=1750952073623&or=Teams%2DHL&ga=1&LOF=1

Ilustración 2. Repositorio Evidencias



Fuente: SharePoint "Repositorio Evidencias"

A su vez, el mapa también se encuentra publicada en la página web de la entidad en el micrositio detallado a continuación: Transparencia y acceso información pública / Planeación, Presupuesto e Informes / **Mapa de Riesgo Institucional.**

A la matriz se puede acceder siguiendo el siguiente enlace:

https://www.supertransporte.gov.co/index.php/transparencia-planeacion-presupuesto-e-informes/mapa-de-riesgo-institucional/

Ilustración 3. Mapa de Riesgo Institucional en Página Web

Fuente. Página web SuperTransporte.

En "*Repositorio Evidencias*" se tiene la información relacionada con los riesgos y los controles ejercidos.

4. Análisis de la Matriz de Riesgos.

Los Riesgos de seguridad de la información identificados pueden detallarse con sus respectivas causas y consecuencias en cumplimiento con lo establecido en la Política de Administración del Riesgo DE-PO-01 y el Manual de Gestión de Riesgos de Seguridad TIC-MA-007 V3

No. de Riesgo	¿QUÉ? IMPACTO	¿CÓMO? CAUSA INMEDIATA	¿PORQUÉ? CAUSA RAÍZ	DESCRIPCIÓN DEL RIESGO	TIPO	SELECCIONE FUENTE GENERADORA DEL EVENTO
R1	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la informacion de la entidad	Por ausencia de copias de seguridad al momento de presentarse algun evento como daño físico, catastrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la informacion de la entidad.	Debido a inconvenientes y demoras en los procesos contractuales o falta de monitoreo al momento de realizar las copias de seguridad	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la informacion de la entidad Por ausencia de copias de seguridad al momento de presentarse algun evento como daño físico, catastrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la informacion de la entidad. Debido a inconvenientes y demoras en los procesos contractuales o falta de monitoreo al momento de realizar las copias de seguridad	G Daños Activos Físicos	Evento Externo
R2	Posibilidad de Perdida de disponibilidad e integridad en la infraestructura tecnologica critica de la entidad	Por la ocurrencia de algun evento como daño físico, catastrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la infaestructura tecnologica de la entidad	Debido a inconvenientes y demoras en los procesos de restauracion o falta de dispositivos de respaldo	Posibilidad de Perdida de disponibilidad e integridad en la infraestructura tecnologica critica de la entidad Por la ocurrencia de algun evento como daño físico, catastrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la infaestructura tecnologica de la entidad Debido a inconvenientes y demoras en los procesos de restauracion o falta de dispositivos de respaldo	G Daños Activos Físicos	Evento Externo
R3	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura onpremise e informacion de la entidad	Por la ocurrencia de algun evento de ciberseguridad que ponen en amenaza la infaestructura tecnologica onpremise y la informacion de la entidad	Debido a que un cibercriminal traspasa los controles de seguridad de la entidad	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura onpremise e informacion de la entidad Por la ocurrencia de algun evento de ciberseguridad que ponen en amenaza la infaestructura tecnologica onpremise y la informacion de la entidad Debido a que un cibercriminal traspasa los controles de seguridad de la entidad	G Daños Activos Físicos	Evento Externo
R4	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura web e informacion de la entidad	Por la ocurrencia de algun evento de ciberseguridad que pone en amenaza la infaestructura y aplicaciones web de la entidad	Debido a que un cibercriminal traspasa los controles de seguridad de la entidad	Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura web e informacion de la entidad Por la ocurrencia de algun evento de ciberseguridad que pone en amenaza la infaestructura y aplicaciones web de la entidad Debido a que un cibercriminal traspasa los controles de seguridad de la entidad	G Daños Activos Físicos	Evento Externo

Fuente: Mapa de Riesgos Institucional-2025

A continuación, se relacionan los riesgos y sus controles:

Riesgo 1

Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la información de la entidad Por ausencia de copias de seguridad al momento de presentarse algún evento como daño físico, catástrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la información de la entidad. Debido a inconvenientes y demoras en los procesos contractuales o falta de monitoreo al momento de realizar las copias de seguridad.

Controles

1. Líder del proceso de TIC y el Líder de infraestructura verifica Anualmente la continuidad de las licencias y herramientas en las aplicaciones de la entidad. A través de sesiones verifica la necesidad de contratación de herramientas y licencias de las copias de seguridad. En caso de identificar falencias se informa a Líder del proceso de TIC.

2. El Líder y equipo de infraestructura monitorea semestralmente el proceso de las copias de seguridad efectuando el mantenimiento y revisión de fallas por parte del proveedor. En caso de identificar falencias se informa a Líder del proceso de TIC.

3. El Líder y equipo de infraestructura revisa semestralmente documentan y restauran las copias de seguridad. Mediante mesas técnicas valida el proceso. En caso de identificar falencias se informa a Líder del proceso de TIC.

Riesgo 2

Posibilidad de Perdida de disponibilidad e integridad en la infraestructura tecnológica critica de la entidad Por la ocurrencia de algún evento como daño físico, catástrofes naturales, perdida de los servicios esenciales, fallas técnicas que pone en amenaza la infraestructura tecnológica de la entidad Debido a inconvenientes y demoras en los procesos de restauración o falta de dispositivos de respaldo.

Controles

1. Líder del proceso de TIC y el Líder de infraestructura verifica semestralmente los planes de mantenimiento de la infraestructura crítica y la restauración, a través de la revisión de los contratos, y validación de las necesidades de mantenimiento de equipos. En caso de identificar falencias se informa a Líder del proceso de TIC.

2. El Líder y equipo de infraestructura monitorea semestralmente el estado de la infraestructura tecnológica. Realizando seguimiento de cada dispositivo critico en la infraestructura de la entidad. En caso de identificar falencias se informa a Líder del proceso de TIC

Riesgo 3

Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura onpremise e información de la entidad Por la ocurrencia de algún evento de ciberseguridad que ponen en amenaza la infraestructura tecnológica onpremise y la información de la entidad Debido a que un cibercriminal traspasa los controles de seguridad de la entidad.

Controles

1. El oficial de seguridad de la entidad ejecuta trimestralmente la implementación del MSPI, A través de acciones, tareas, actividades y evidencias de los dominios, en caso de identificar falencias se informa a Líder del proceso de TIC.

2. Líder del proceso de TIC y el Líder de infraestructura verifica semestralmente los contratos con los proveedores y los planes de restauración de los servicios. A través de sesiones verifica la necesidad de contratación de herramientas y licencias de las copias de seguridad. En caso de identificar falencias se informa al comité correspondiente.

3. El oficial de seguridad de la entidad valida trimestralmente estableciendo y ejecutando el plan de análisis de vulnerabilidades, A través mesas de trabajo y uso de herramientas de especializadas, En caso de identificar falencias se informa a Líder del proceso de TIC.

4. El oficial de seguridad de la entidad realiza trimestralmente el re-testeo y toma las acciones para remediar los hallazgos A través mesas de trabajo y uso de herramientas de vulnerabilidades, remite por correo electrónico los requerimientos y ajustes necesarios En caso de identificar falencias se informa a Líder del proceso de TIC.

Riesgo 4

Posibilidad de Perdida de disponibilidad, integridad y confidencialidad en la infraestructura web e información de la entidad Por la ocurrencia de algún evento de ciberseguridad que pone en amenaza la infraestructura y aplicaciones web de la entidad Debido a que un cibercriminal traspasa los controles de seguridad de la entidad.

Controles

1. Líder del proceso de TIC y el Líder de infraestructura verifica trimestralmente garantizando los contratos con los proveedores y los planes de restauración de los servicios, A través de sesiones verifica la necesidad de contratación de herramientas y licencias de las copias de seguridad. En caso de identificar falencias se informa a Líder del proceso de TIC.

2. El oficial de seguridad de la entidad valida trimestralmente estableciendo y ejecutando el plan de análisis de vulnerabilidades web, a través mesas de trabajo y uso de herramientas de especializadas. En caso de identificar falencias se informa a Líder del proceso de TIC.

3. El oficial de seguridad de la entidad realiza trimestralmente realizando el re-testeo de la página y toma las acciones para remediar los hallazgos A través mesas de trabajo y uso de herramientas de vulnerabilidades, remite por correo electrónico los requerimientos y ajustes necesarios En caso de identificar falencias se informa a Líder del proceso de TIC.

5. Materialización de Riesgos.

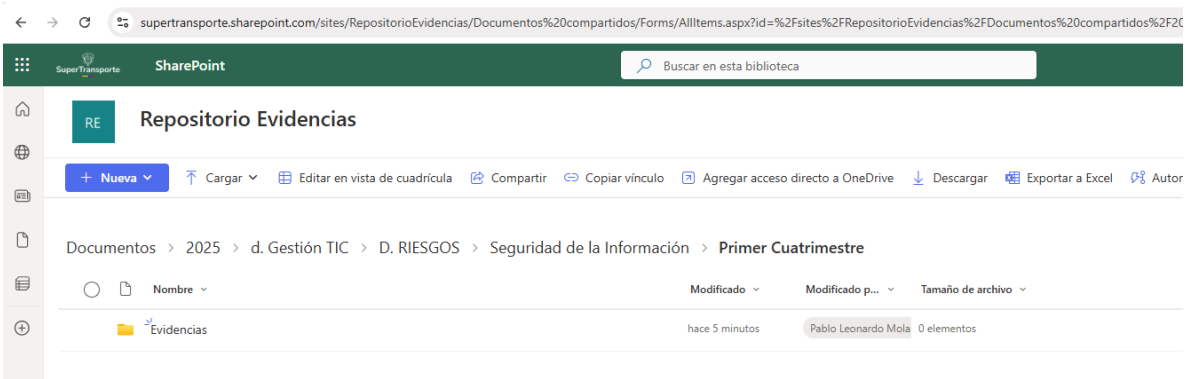
Durante el Primer Cuatrimestre de 2025 la Oficina de Tecnologías de la información y las comunicaciones **NO** recibió alertas correspondientes a la posible materialización de riesgos de Seguridad de la información. En las mesas de trabajo realizadas para evaluar los controles y los riesgos actuales, se indagó sobre el tema sin alguna novedad.

6. Cargue Evidencias y Seguimiento.

La Política de Administración de Riesgos menciona la realización del seguimiento de la ejecución de los controles estructurados de forma cuatrimestral. Para ello, se puso a disposición la Carpeta en el SharePoint de la Oficina Asesora de Planeación “repositorio Evidencias” para que se relacionen allí las evidencias correspondientes a la ejecución de los controles.

Mediante el siguiente enlace se puede acceder al SharePoint y verificar la información reportada en la matriz y para cada uno de los soportes.

https://supertransporte.sharepoint.com/sites/RepositorioEvidencias/Documentos%20compartidos/Forms/AllItems.aspx?id=%2Fsites%2FRepositorioEvidencias%2FDocumentos%20compartidos%2F2025%2Fd%2E%20Gesti%C3%B3n%20TIC%2FD%2E%20RIESGOS%2FSeguridad%20de%20la%20Informaci%C3%B3n%2FPrimer%20Cuatrimestre&viewid=1835f521%2D2bf3%2D4bdc%2Da069%2Dc7d66c62fe20&p=true&ct=1750952073623&or=Teams%2DHL&ga=1&LOF=1



7. Recomendaciones de la evaluación Tercer Cuatrimestre de 2025. (enero-febrero-marzo-abril)

En el marco del proceso de validación y seguimiento continuo de la matriz de riesgos de seguridad informática, y en cumplimiento de los lineamientos definidos en la Política de Administración de Riesgos, el Modelo de Seguridad y Privacidad de la Información y la Resolución 5095 de la Superintendencia de Transporte, se establecen las siguientes acciones prioritarias para robustecer el modelo de gestión de riesgos tecnológicos:

- **Monitoreo Constante de la Infraestructura**

El monitoreo en tiempo real es clave para la detección oportuna de incidentes y la prevención de accesos no autorizados.

- Actualización y gestión de parches (Patch Management): Establecer un proceso automatizado para aplicar parches de seguridad críticos y actualizaciones del sistema operativo y aplicaciones.
- Supervisión del tráfico de red: Utilizar herramientas de análisis de tráfico (como NDR - Network Detection and Response) para identificar patrones anómalos y posibles brechas de seguridad.
- Revisión de logs críticos: Automatizar la recolección, análisis y retención de registros de acceso y eventos del sistema.

- **Análisis Periódico de Vulnerabilidades**

La identificación proactiva de debilidades es fundamental para una postura de defensa efectiva.

- Ejecutar escaneos de vulnerabilidades automáticos de manera mensual y complementarlos con pruebas manuales trimestrales (por ejemplo, pruebas de penetración ética).
- Colaboración continua con CSIRT Colombia: Establecer un canal directo de intercambio de información sobre amenazas emergentes y alertas tempranas, así como recibir asesoría en el manejo de incidentes de alto impacto.

➢ **Mantenimiento de Controles Preventivos**

Fortalecer la primera línea de defensa es esencial para la reducción de la superficie de ataque.

- Configuración robusta de Firewalls y Sistemas IDS/IPS: Establecer reglas basadas en políticas zero-trust, segmentación de red, y detección de patrones de ataque conocidos.
- Auditorías técnicas periódicas: Evaluar y validar la correcta operación y cobertura de los controles, incluyendo pruebas de evasión (evasion techniques) para identificar puntos ciegos.

➢ **Fortalecimiento de la Autenticación Multifactor (MFA)**

- Ampliar la cobertura del uso de MFA a todos los accesos privilegiados, aplicaciones críticas y plataformas en la nube.
- Integrar MFA con herramientas de identidad federada (como SAML o Azure AD) para facilitar la administración centralizada.

➢ **Políticas de Contraseñas Seguras**

- Adoptar directrices sobre contraseñas, que incluyen:
  - Uso de frases de paso (passphrases) seguras.
  - Validación contra listas negras de contraseñas comprometidas.
  - Eliminación de requisitos arbitrarios como caducidad forzada, a menos que exista evidencia de compromiso.

➢ **Detección de Actividades Sospechosas**

- Configurar alertas automatizadas para actividades atípicas como:
  - Elevación de privilegios.
  - Transferencias de archivos no autorizadas.
  - Conexiones desde ubicaciones geográficas inusuales.

- **Monitoreo de Actividades de Usuarios**
  - Establecer un programa de auditoría de usuarios privilegiados, incluyendo la grabación de sesiones y análisis de logs.
  - Aplicar principios de mínimos privilegios y separación de funciones para limitar el alcance de acciones individuales.

- **Capacitación y Concienciación**
    - Simulaciones de ataques de phishing.
    - Talleres prácticos para la gestión segura de datos.
    - Actualización periódica sobre nuevas amenazas.
    - Aumentar la meta de campañas de sensibilización: pasar de 20 a por lo menos 36 campañas anuales, cubriendo temáticas como ransomware, ingeniería social, suplantación digital, buenas prácticas de ciberseguridad.

- **Revisión y Actualización de Políticas de Seguridad**
  - Establecer un comité de revisión de políticas de seguridad que evalúe:
    - El cumplimiento de las políticas frente a la normativa vigente.
    - Su aplicabilidad frente a cambios tecnológicos y organizacionales.
  - Incorporar lineamientos de normas internacionales como ISO/IEC

- **Fomento de la Mejora Continua**
  - Actualizar trimestralmente la matriz de riesgos con base en indicadores de amenazas reales, incidentes reportados y cambios en la arquitectura tecnológica.
  - Realizar simulacros de ciberincidentes (tabletop exercises y pruebas técnicas) semestralmente, evaluando la capacidad de respuesta, comunicación y recuperación ante incidentes.

8. Conclusiones.

Al cierre del **primer cuatrimestre de 2025**, la Oficina de Tecnologías y Comunicaciones (OTIC) de la Superintendencia de Transporte continúa consolidando su rol como un actor estratégico en la protección de los activos tecnológicos y en la gestión de la seguridad de la información institucional. Durante este período, se ha avanzado significativamente en la implementación de las estrategias definidas en la matriz de riesgos de seguridad informática, alineadas con la Política de Administración de Riesgos, el Manual de Gestión de Riesgos de Seguridad y el Modelo de Seguridad y Privacidad de la Información (MSPI). Estos lineamientos han permitido mantener un enfoque preventivo, adaptable y centrado en la mejora continua frente a las amenazas emergentes del entorno digital.

Se destaca el fortalecimiento de las actividades de monitoreo y análisis de vulnerabilidades, así como la continuidad en la implementación de controles técnicos avanzados, entre ellos la autenticación multifactor, el monitoreo de usuarios y la automatización de procesos de detección de amenazas. Estas acciones han mejorado la capacidad de respuesta frente a eventos de seguridad y reducido el nivel de exposición a incidentes críticos.

Asimismo, las alianzas estratégicas con el MinTransporte y su herramienta WAS de análisis de vulnerabilidades se han mantenido activas, facilitando el acceso a conocimiento especializado, buenas prácticas y mecanismos de respuesta oportuna. La participación en estas redes ha sido clave para enriquecer el enfoque operativo y fortalecer la postura defensiva institucional.

Estos resultados reflejan un avance sostenido hacia una gestión madura y resiliente de la ciberseguridad, y sientan las bases para el cumplimiento de los objetivos estratégicos trazados para el resto de la vigencia 2025, incluyendo el fortalecimiento de capacidades en respuesta a incidentes, y protección de la infraestructura crítica de información.

Revisó:
SuperTransporte
Firmado digitalmente por ROMERO HERNANDEZ URIAS
Urías Romero
Jefe Oficina de Tecnologías y Comunicaciones

Elaboró: Sebastián López C.
Sebastian Lopez Ciro - Contratista OTIC