



Informe de Seguimiento Superintendencia de Transporte

 CIBERSEGURIDAD INSTITUCIONAL

MARZO 2026

Proyecto: Gestión de Ciberseguridad Institucional — Seguimiento Operativo y Técnico

Elaborado por: Virgilio Salgado Escorce

Fecha: 04 de Marzo de 2026 | **Lugar:** Barranquilla, Atlántico

Documento N.º: 001 | **Clasificación:** Uso Institucional Restringido

Tabla de Contenido

01	02
Introducción	Enfoque del Proyecto
Contexto institucional y alcance del seguimiento	Buenas prácticas: OWASP, NIST e ISO
03	04
Monitoreo Deep Web y Dark Web	Escaneos Externos
Filtraciones y credenciales expuestas	Infraestructura, servidores y aplicaciones
05	06
Evaluación de Servicios e Inventario	Estado General del Avance
Control, trazabilidad y alineación ISO/NIST	Orientación de mejora continua
07	08
Próximas Fases	Cierre y Conclusiones Estratégicas
Formación, capacitación y concientización	Recomendaciones accionables y priorizadas

1. Introducción

En el marco del proyecto institucional de ciberseguridad de la Superintendencia de Transporte, el presente documento consolida el seguimiento a las actividades ejecutadas dentro del período establecido, con el fin de evidenciar el avance operativo, el enfoque metodológico y la alineación con buenas prácticas reconocidas internacionalmente.

El seguimiento se orienta a demostrar que la gestión de seguridad no se limita a acciones puntuales, sino que se está conduciendo como un **proceso continuo, medible y basado en riesgo**, fortaleciendo la capacidad institucional para prevenir, detectar y responder a escenarios de exposición, vulnerabilidad y amenaza.

1.1 Alcance y Enfoque Integral del Seguimiento

Este avance se soporta en una aproximación integral que combina:

Identificación Temprana

Detección de filtraciones y credenciales comprometidas antes de su materialización en incidentes.

Evaluación de Postura Externa

Análisis de la infraestructura tecnológica desde la perspectiva del atacante externo.

Consolidación de Inventarios

Depuración de servicios para mejorar el control, la trazabilidad y el cumplimiento de lineamientos de referencia.

Lo anterior permite mantener una visión realista de la superficie de ataque, priorizar brechas con base en criticidad y reforzar lineamientos técnicos y administrativos que sostengan la seguridad en el tiempo.

1.2 Propósito del Documento

El seguimiento desarrollado permite demostrar que la gestión de la seguridad de la información no se limita a acciones aisladas, sino que se implementa como un **proceso continuo, medible y basado en riesgos**. Este enfoque contribuye al fortalecimiento de la capacidad institucional para prevenir, detectar y responder de manera oportuna ante escenarios de exposición, vulnerabilidad y amenaza.

El avance alcanzado se sustenta en un enfoque integral que articula la identificación temprana de filtraciones y credenciales comprometidas, la evaluación de la postura externa de la infraestructura tecnológica, así como la consolidación de inventarios y servicios. Lo anterior permite mejorar el control, la trazabilidad y el cumplimiento de lineamientos de referencia, manteniendo una visión actualizada de la superficie de ataque y priorizando las brechas de acuerdo con su criticidad.

2. Enfoque del Proyecto Bajo Buenas Prácticas

 OWASP

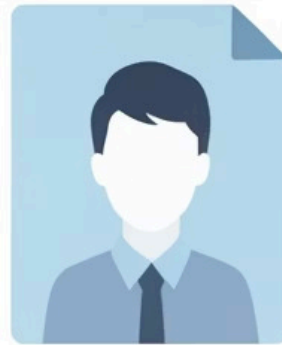
 NIST

 ISO/IEC 27000

El proyecto se ejecuta bajo un enfoque alineado con marcos de referencia internacionalmente reconocidos como el **NIST Cybersecurity Framework** y la familia de normas **ISO/IEC 27000**, complementado con criterios técnicos aplicados en la evaluación de aplicaciones y servicios conforme a lineamientos de **OWASP**.



NIST CSF: Protect, Detect, and Identify functions within the framework. Multi-layered protection and analysis.



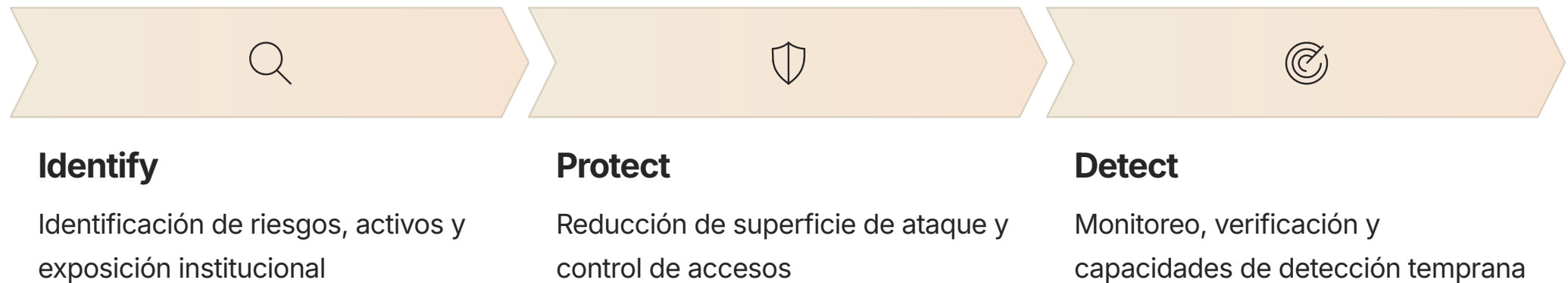
ISO/IEC 270000
Traceable, auditable Information Security Management Systems for continuous security improvement.



OWASP: Framework for application security evaluation, including authentication, session management, and robust input validation.

2.1 Perspectiva NIST Cybersecurity Framework

Desde la perspectiva de NIST, las actividades desarrolladas se enmarcan principalmente en las funciones de **identificación (Identify)**, **protección (Protect)** y **detección (Detect)**, entendiendo que la madurez organizacional se alcanza cuando la entidad no solo conoce sus activos, sino también la forma en que estos se exponen y cómo se validan los controles implementados.



La madurez real se logra cuando la organización no solo conoce sus activos, sino que también conoce cómo se exponen y cómo se validan los controles en operación.

2.2 Perspectiva ISO/IEC 27000

Desde el enfoque ISO, las actividades se articulan con la implementación y sostenimiento de un **sistema de gestión de seguridad de la información (SGSI)** trazable, auditable y orientado a la mejora continua.

En este contexto, los hallazgos técnicos trascienden la identificación de vulnerabilidades y se convierten en insumos para:

Toma de Decisiones Estratégicas

Los hallazgos alimentan decisiones de priorización y control de cambios a nivel directivo.

Priorización de Riesgos

Endurecimiento de configuraciones y definición de lineamientos basados en criticidad.

Fortalecimiento de Controles

Fortalecimiento de responsabilidades internas sobre activos, servicios y proveedores tecnológicos.

Esto implica que los hallazgos técnicos no se quedan únicamente en reportes de vulnerabilidades, sino que alimentan decisiones de priorización, control de cambios, endurecimiento de configuraciones, definición de lineamientos y fortalecimiento de responsabilidades internas sobre activos, servicios y proveedores tecnológicos.

2.3 Perspectiva OWASP

El componente OWASP complementa el enfoque con criterios técnicos utilizados en evaluaciones de aplicaciones y servicios. Bajo estos referentes, se revisan condiciones asociadas a:

Autenticación y Control de Sesiones

Verificación de mecanismos de autenticación robusta y gestión segura de sesiones de usuario.

Validación de Entradas

Revisión de controles sobre datos ingresados para prevenir inyecciones y manipulación de parámetros.

Exposición de Información Sensible

Identificación de datos institucionales expuestos inadvertidamente en interfaces públicas.

Fallos de Configuración

Detección de configuraciones inseguras y posibles vectores de abuso en plataformas web.

3. Actividades Ejecutadas: Monitoreo de Filtraciones y Credenciales Expuestas

DEEP WEB

DARK WEB

DETECCIÓN TEMPRANA

Durante el período evaluado, se ha implementado un componente de monitoreo especializado orientado a la **detección temprana de filtraciones, exposición de credenciales y posibles evidencias de compromiso** asociadas a dominios, correos institucionales y activos digitales de la Superintendencia de Transporte.

Este monitoreo se fundamenta en la correlación de información proveniente de fuentes abiertas y entornos de acceso restringido (Deep Web y Dark Web), con el objetivo de identificar señales de riesgo antes de su materialización en incidentes de seguridad.

Id	Leaked Accounts	Applications	Type	Last Seen	Action
36369583...	k*****t@hotmail.com	aplicaciones.supertransporte.gov.co	combolist	2026-03-24	View
3635513999	9*****9	vigia.supertransporte.gov.co	combolist	2026-03-24	View
3632510281	9*****3	sinst.supertransporte.gov.co, pesv.sup...	combolist	2026-03-24	View
3631099578	0****4	pesv.supertransporte.gov.co	combolist	2026-03-24	View
36235437...	9*****1	vigia.supertransporte.gov.co, pesv.su...	combolist	2026-03-24	View
36208207...	8*****5	aplicaciones.supertransporte.gov.co	combolist	2026-03-24	View
36145840...	6*****x	vigia.supertransporte.gov.co, sim.sup...	combolist	2026-03-23	View



3.1 Metodología de Monitoreo en Entornos Restringidos

Este trabajo se ha basado en búsquedas sistemáticas y correlación de indicios en fuentes abiertas y entornos de acceso restringido, con el objetivo de identificar señales de riesgo antes de que se conviertan en incidentes operativos.

Este tipo de monitoreo aporta valor porque permite conocer si existen:



Credenciales Reutilizadas

Combinaciones filtradas de usuario/contraseña asociadas a dominios institucionales.



Tokens o Accesos Publicados

Tokens de sesión o credenciales de acceso expuestos en foros o mercados clandestinos.



Evidencia Indirecta de Acceso

Menciones o indicios de acceso no autorizado a sistemas o información institucional.

3.2 Proceso de Análisis ante Hallazgos Relevantes

Cuando se detecta un hallazgo relevante, se procede a realizar un análisis estructurado que comprende las siguientes etapas:

Validación del Alcance

Confirmar sistemas y límites afectados.

Evaluación de Criticidad

Determinar impacto y prioridad de respuesta.

Análisis de Contexto

Reunir evidencia y entorno del hallazgo.

Recomendaciones de Contención

Definir medidas inmediatas y mitigación.

Este proceso garantiza que cada hallazgo sea tratado con rigor técnico, evitando tanto la subestimación como la sobreacción ante indicadores de riesgo.

3.3 Recomendaciones de Contención Generadas

Como resultado del proceso de análisis, se generan recomendaciones de contención específicas, entre las cuales se destacan:



Rotación de Credenciales

Cambio inmediato de contraseñas comprometidas o potencialmente expuestas en entornos de acceso restringido.



Implementación de Autenticación Multifactor (MFA)

Endurecimiento de autenticación mediante la aplicación de MFA en cuentas institucionales críticas.



Ajuste de Políticas de Contraseñas

Fortalecimiento de los requisitos de complejidad, longitud y caducidad de contraseñas institucionales.



Revisión de Accesos Privilegiados

Auditoría y depuración de cuentas con privilegios elevados para reducir la superficie de exposición.

3.4 Valor Estratégico del Componente de Monitoreo

Este componente aporta un valor significativo al permitir la identificación de riesgos asociados a la reutilización de credenciales, exposición histórica de información y errores humanos, los cuales constituyen uno de los **principales vectores de ataque en entornos institucionales**.

En conjunto, este frente se integra al objetivo institucional de disminuir el riesgo asociado a errores humanos, reutilización de contraseñas y exposición histórica de credenciales, que suelen ser uno de los vectores más explotados en intrusiones a entidades públicas.



Incidentes por Factor Humano

Proporción estimada de incidentes de seguridad originados en errores humanos o credenciales comprometidas.



Mayor Riesgo sin MFA

Incremento del riesgo de compromiso de cuentas sin autenticación multifactor habilitada.



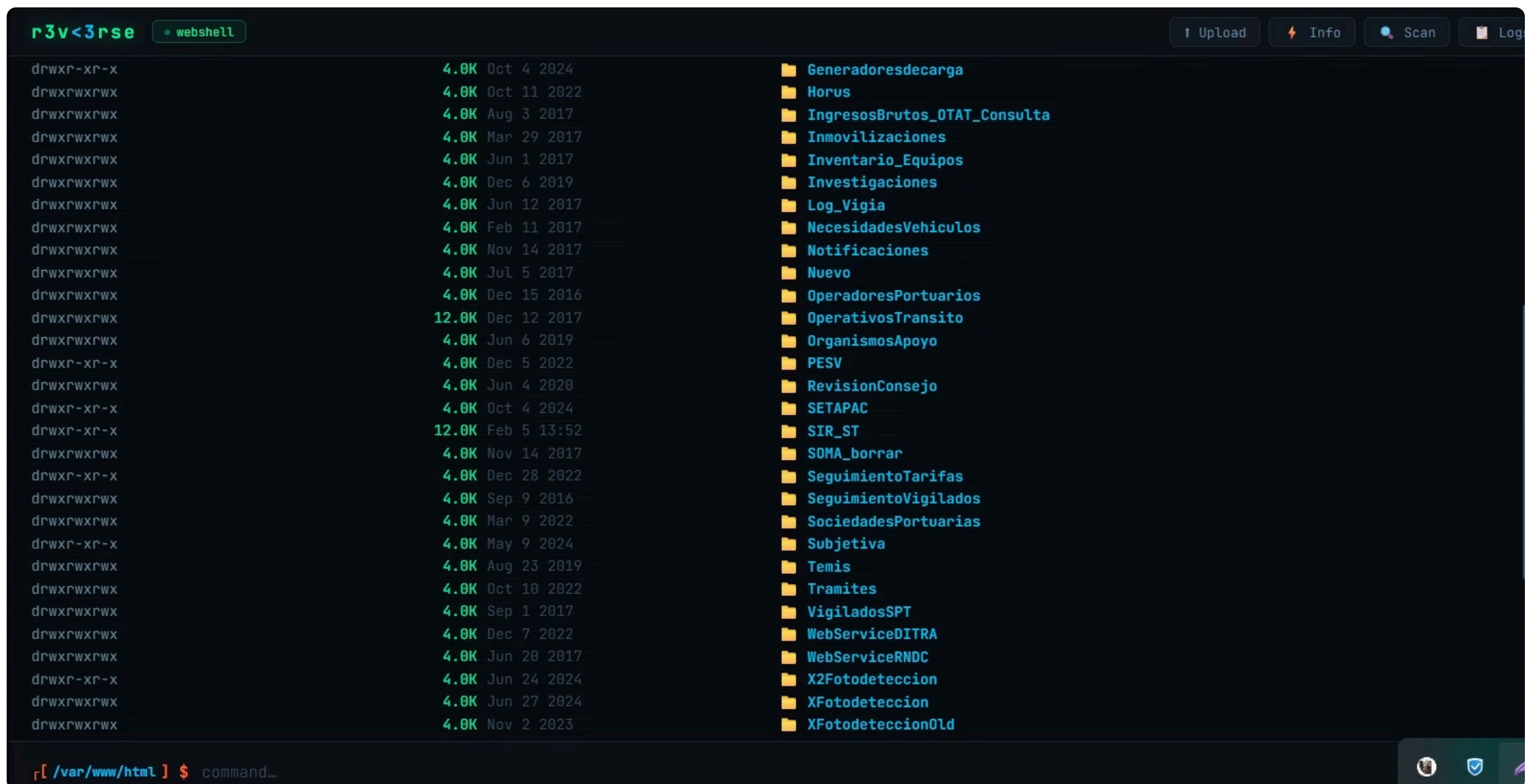
Monitoreo Continuo

Cobertura de monitoreo en fuentes abiertas y entornos restringidos durante todo el período.

4. Actividades Ejecutadas: Escaneos Externos a Infraestructura, Servidores y Aplicaciones

De manera complementaria, se han desarrollado escaneos externos orientados a evaluar la **postura de exposición de la infraestructura tecnológica**, servidores y servicios publicados por la entidad.

Este ejercicio se aborda desde una lógica de "superficie de ataque" y verificación técnica, buscando identificar condiciones que incrementen la probabilidad de explotación desde Internet.



4.1 Alcance de los Escaneos Externos

Los escaneos externos cubren los siguientes elementos de la infraestructura tecnológica de la Superintendencia:

1

Dispositivos y Servidores Publicados

Evaluación de todos los activos con presencia en Internet, incluyendo servidores web, de correo y de aplicaciones.

2

Servicios y Puertos Expuestos

Identificación de servicios innecesarios expuestos y puertos abiertos sin control o justificación técnica.

3

Versiones con Vulnerabilidades Conocidas

Detección de componentes de software desactualizados con vulnerabilidades públicamente documentadas (CVE).

4

Mecanismos de Cifrado y Encabezados

Revisión de debilidades en cifrado TLS/SSL y ausencia de encabezados de seguridad HTTP.

4.2 Hallazgos Típicos Identificados en Escaneos

Este ejercicio permite identificar las siguientes categorías de hallazgos que incrementan la probabilidad de explotación desde Internet:

Categoría de Hallazgo	Descripción Técnica	Nivel de Riesgo
Configuraciones inseguras	Parámetros de servidor o aplicación que exponen información o habilitan funciones no requeridas	Alto
Servicios innecesarios expuestos	Puertos y servicios activos sin justificación operativa ni control de acceso por origen	Alto
Versiones vulnerables	Software con CVEs conocidos sin parche aplicado, explotables remotamente	Crítico
Debilidades en cifrado	Uso de protocolos TLS obsoletos o cifrados débiles en comunicaciones institucionales	Medio-Alto
Encabezados de seguridad ausentes	Falta de headers HTTP como CSP, HSTS, X-Frame-Options en portales web	Medio

4.3 Análisis de Aplicaciones Web Institucionales

Adicionalmente, se ha incorporado un enfoque específico sobre **aplicaciones web institucionales**, considerando su nivel de exposición. Las plataformas de cara al ciudadano suelen concentrar mayor probabilidad de pruebas hostiles, abuso de funcionalidades y explotación de fallas comunes.

Bajo lineamientos de OWASP, se analizan aspectos relacionados con:

Autenticación y Gestión de Sesiones

Verificación de la robustez de los mecanismos de autenticación y la correcta gestión del ciclo de vida de las sesiones de usuario.

Validación de Entradas

Análisis de controles sobre datos ingresados por usuarios para prevenir inyecciones SQL, XSS y otras vulnerabilidades de entrada.

Exposición de Información Sensible

Identificación de datos institucionales o personales expuestos inadvertidamente a través de interfaces públicas.

Posibles Vectores de Abuso

Detección de funcionalidades que, aunque no sean críticas individualmente, en conjunto aumentan la probabilidad de incidentes si no se gestionan con disciplina técnica y continuidad.

4.4 Acciones Correctivas y Preventivas Derivadas

Los resultados obtenidos permiten priorizar acciones correctivas y preventivas, orientadas no solo al parcheo de vulnerabilidades, sino a la **reducción estructural del riesgo**. Los resultados de estos escaneos se vienen utilizando para priorizar acciones correctivas y preventivas, no solo desde una perspectiva de "parcheo", sino también desde la reducción estructural del riesgo:

Endurecimiento de Configuraciones

Aplicación de configuraciones seguras en servidores, aplicaciones y dispositivos de red.

Cierre de Servicios No Requeridos

Eliminación de componentes que agregan exposición sin aportar valor al servicio institucional.

Control de Accesos por Origen

Revisión de reglas de firewall y fortalecimiento de segmentación de red.

Adopción de Mejores Prácticas TLS

Actualización de protocolos de cifrado y eliminación de versiones obsoletas en comunicaciones.

5. Evaluación de Servicios e Inventario: Control, Trazabilidad y Alineación con ISO/NIST

Como actividad transversal, se ha avanzado en la **consolidación y depuración del inventario de activos y servicios tecnológicos** de la entidad, reconociendo que un control efectivo solo es posible sobre aquellos elementos que han sido identificados y gestionados.

Este ejercicio incluye la identificación de activos, clasificación por criticidad, definición de responsables, mapeo de dependencias y revisión del ciclo de vida operativo de cada componente.

5.1 Componentes del Proceso de Inventario

La intención es que el inventario no sea un listado estático, sino una **herramienta viva** que soporte decisiones de seguridad, continuidad y cumplimiento. El proceso de consolidación del inventario comprende los siguientes componentes:

Identificación de Activos

Levantamiento exhaustivo de todos los activos tecnológicos de la Superintendencia.

Definición de Responsables

Asignación formal de propietarios y custodios para cada activo identificado.

1

2

3

4

Clasificación por Criticidad

Categorización de activos según su impacto potencial en la operación institucional.

Mapeo de Dependencias

Documentación de las relaciones e interdependencias entre activos y servicios.

5.2 El Inventario como Herramienta Dinámica de Gobierno

El inventario se concibe como una herramienta dinámica que soporta la toma de decisiones en materia de seguridad, continuidad y cumplimiento, permitiendo la implementación efectiva de prácticas como:



Gestión de Riesgos

Habilitación de prácticas de gestión de riesgos basadas en el conocimiento real de los activos y sus dependencias.



Administración de Vulnerabilidades

Priorización de vulnerabilidades según el impacto potencial sobre activos críticos identificados.



Control de Cambios

Gestión estructurada de modificaciones en la infraestructura con trazabilidad completa.

5.3 Alineación del Inventario con Lineamientos ISO y NIST

Este componente es clave para sostener lineamientos de referencia ISO y NIST, ya que habilita prácticas como gestión de riesgos, administración de vulnerabilidades, priorización por impacto, control de cambios, y definición de controles coherentes según la criticidad del servicio.

Alineación ISO/IEC 27001

El inventario soporta el Anexo A de ISO 27001, específicamente los controles de gestión de activos (A.8), garantizando trazabilidad y auditoría del ciclo de vida de cada componente tecnológico.

Alineación NIST CSF

Desde la perspectiva NIST, el inventario habilita la función "Identify" (ID.AM), que establece que los activos físicos y de software deben ser inventariados y gestionados de forma consistente con la estrategia de riesgo organizacional.

También permite avanzar hacia una postura más madura donde las acciones de seguridad se integran con la operación, evitando que la seguridad dependa únicamente de revisiones reactivas o de esfuerzos aislados.

5.4 Revisión del Ciclo de Vida Operativo

La revisión del ciclo de vida operativo de cada componente tecnológico es un elemento diferenciador de este proceso, ya que permite identificar activos en estado de obsolescencia, sin soporte del fabricante o con configuraciones heredadas que representan riesgos no gestionados.

Activos en Soporte Activo

Componentes con soporte vigente del fabricante, actualizaciones disponibles y controles de seguridad aplicables.

Activos en Fin de Vida (EOL)

Componentes sin soporte del fabricante que representan riesgo elevado por ausencia de parches de seguridad.

Activos con Configuraciones Heredadas

Sistemas con configuraciones no revisadas que pueden contener vulnerabilidades acumuladas no gestionadas.

6. Estado General del Avance y Orientación de Mejora Continua

Con base en las actividades ejecutadas, se evidencia un **avance significativo en el fortalecimiento de las capacidades institucionales** para la identificación y gestión de riesgos de ciberseguridad.

La combinación entre monitoreo de filtraciones/credenciales y escaneos externos aporta una visión más completa del riesgo real, permitiendo tratar tanto la amenaza asociada a información comprometida como las debilidades técnicas en infraestructura y aplicaciones.

6.1 Logros Alcanzados en el Período

La integración del monitoreo de credenciales, el análisis de exposición externa y la consolidación del inventario tecnológico ha permitido obtener una visión más completa del riesgo, facilitando la toma de decisiones informadas y priorizadas.



Visibilidad de Exposición

Construcción de capacidades de identificación temprana y evaluación técnica de la exposición institucional.



Base de Gobierno

Consolidación del inventario y evaluación de servicios que fortalece la base de gobierno necesaria para sostener lineamientos técnicos y administrativos con continuidad.



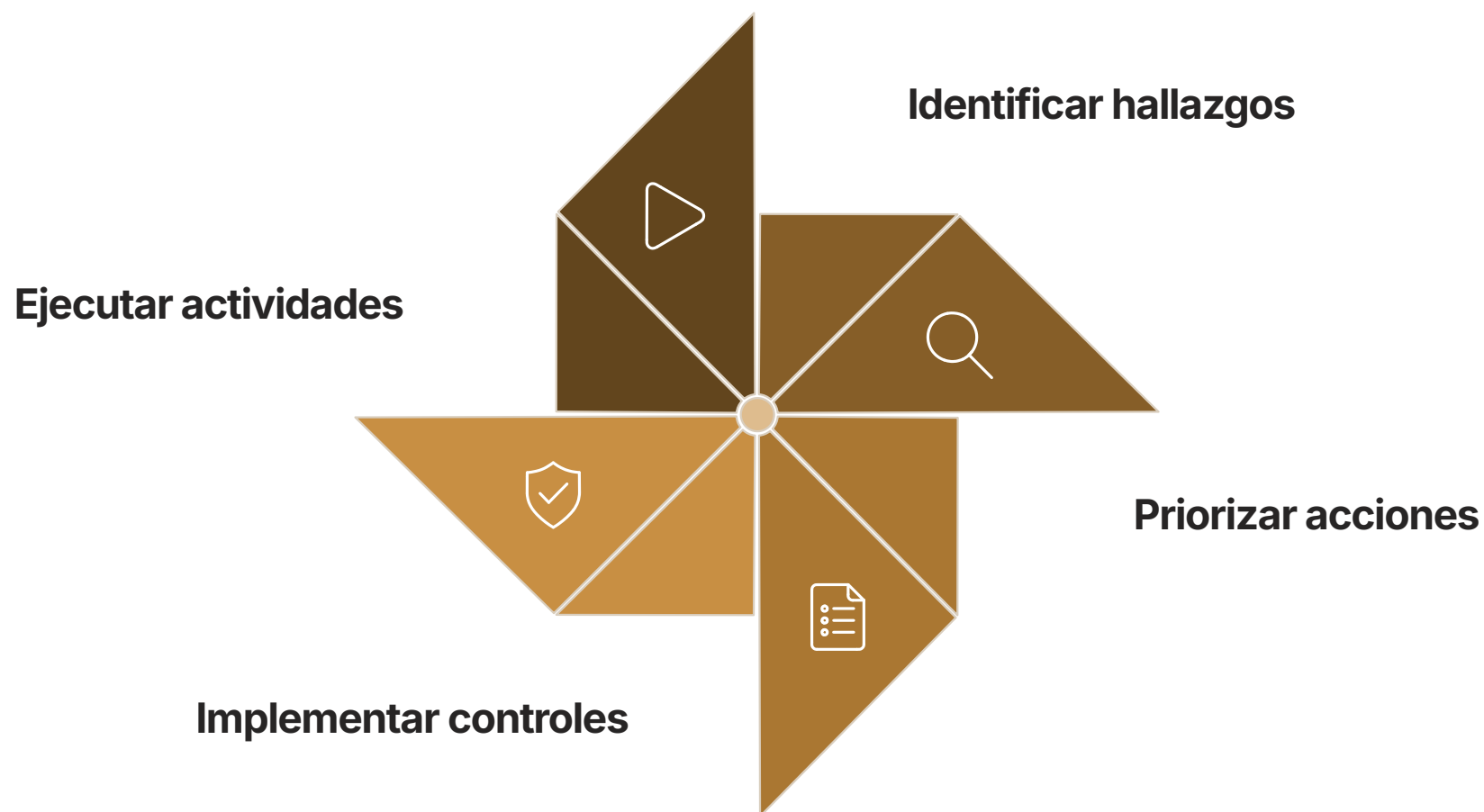
Decisiones Informadas

Generación de insumos técnicos que permiten priorizar acciones con base en criticidad y riesgo real.

6.2 Orientación hacia la Mejora Continua

El enfoque adoptado se orienta a la mejora continua, transformando los hallazgos en acciones concretas de mitigación, fortalecimiento de controles y estandarización de prácticas, con el objetivo de elevar el nivel de madurez institucional en ciberseguridad.

El objetivo no es únicamente "corregir lo encontrado", sino reducir estructuralmente la superficie de ataque y elevar la madurez institucional, asegurando que la Superintendencia mantenga una postura de seguridad más robusta, medible y sostenible frente al contexto actual de amenazas.



6.3 Transformación de Hallazgos en Acciones Concretas

En línea con el enfoque de mejora continua, el seguimiento se orienta a que los hallazgos se transformen en acciones concretas de:

1

Cierre de Brechas Identificadas

Atención directa a las vulnerabilidades y exposiciones detectadas durante el período.

2

Estandarización de Lineamientos

Formalización de prácticas de verificación periódica y estándares técnicos aplicables.

3

Fortalecimiento de Controles Preventivos

Implementación de controles que reduzcan la probabilidad de ocurrencia de incidentes futuros.

4

Elevación de Madurez Institucional

Postura de seguridad más robusta, medible y sostenible frente al contexto actual de amenazas.

6.4 Visión Integral del Riesgo Institucional

De forma complementaria, la consolidación del inventario y la evaluación de servicios fortalece la base de gobierno necesaria para sostener lineamientos técnicos y administrativos con continuidad.





7. Próximas Fases: Formación, Capacitación y Concientización en Ciberseguridad

Como parte de la estrategia de sostenibilidad del proyecto, se incorporará un **componente formal de formación y concientización en ciberseguridad** dirigido a los diferentes actores de la Superintendencia de Transporte.

Este frente se plantea como un habilitador clave, dado que una proporción significativa de los incidentes modernos se origina o se potencia por factores humanos, debilidades en hábitos de seguridad, desconocimiento de buenas prácticas o falta de criterios para identificar comportamientos sospechosos y riesgos en el uso cotidiano de la tecnología.

7.1 Justificación del Componente de Formación

Este componente busca fortalecer la cultura organizacional, considerando que una proporción significativa de los incidentes de seguridad se origina en factores humanos, tales como:

Desconocimiento de Buenas Prácticas

Falta de criterios para identificar comportamientos sospechosos y riesgos en el uso cotidiano de la tecnología.

Reutilización de Credenciales

Uso de contraseñas débiles o repetidas en múltiples sistemas, amplificando el impacto de filtraciones.

Exposición a Ingeniería Social

Vulnerabilidad ante técnicas de phishing, vishing y otras formas de manipulación psicológica.

Prácticas Inseguras en Trabajo Remoto

Uso inadecuado de herramientas corporativas y redes no seguras en entornos de trabajo remoto.

7.2 Objetivos del Plan de Capacitación

Se ejecutarán cursos orientados a fortalecer capacidades y cultura organizacional, de manera que el personal adquiera un entendimiento práctico de los riesgos más comunes y de las responsabilidades mínimas necesarias para proteger la información institucional.

1 Estandarizar Conceptos Esenciales de Ciberseguridad

Establecer un lenguaje y comprensión común sobre riesgos, amenazas y buenas prácticas en toda la organización.

2 Mejorar la Toma de Decisiones en el Día a Día

Dotar al personal de criterios prácticos para identificar y responder adecuadamente ante situaciones de riesgo.

3 Reducir Escenarios de Exposición por Factor Humano

Disminuir incidentes derivados de credenciales débiles, manejo inadecuado de información e ingeniería social.

7.3 Contenidos Temáticos del Programa de Formación

Esta iniciativa permitirá estandarizar conceptos esenciales, mejorar la toma de decisiones en el día a día, y reducir escenarios de exposición derivados de:

Credenciales Débiles y Reutilización de Contraseñas

Buenas prácticas en gestión de contraseñas, uso de gestores y habilitación de MFA.

Manejo Inadecuado de Información

Clasificación, almacenamiento y transmisión segura de información institucional sensible.

Ingeniería Social

Reconocimiento y respuesta ante técnicas de phishing, pretexting y otras formas de manipulación.

Trabajo Remoto y Herramientas Corporativas

Prácticas seguras en el uso de dispositivos, redes y plataformas en entornos de trabajo remoto.

7.4 Integración de la Formación con el Enfoque Metodológico

La formación y concientización se integrará con el enfoque metodológico del proyecto, alineándose con lineamientos de referencia como NIST e ISO, donde el **componente humano se reconoce como un control crítico** para soportar el funcionamiento efectivo de políticas, procedimientos y controles técnicos.

Articulación con Hallazgos Técnicos

Este plan de capacitación se articulará con los hallazgos y aprendizajes obtenidos durante los escaneos, monitoreos y evaluaciones realizadas, permitiendo que los contenidos respondan a riesgos reales identificados en el contexto institucional.

Contribución al Cierre de Brechas

La formación contribuirá directamente al cierre de brechas identificadas, fortaleciendo la resiliencia y la capacidad preventiva de la entidad frente al contexto actual de amenazas.

7.5 Audiencias Objetivo del Programa de Concientización

En este sentido, se desarrollarán programas de capacitación orientados a mejorar las prácticas de seguridad, la identificación de riesgos y la toma de decisiones en el uso de tecnologías, contribuyendo a la reducción de escenarios de exposición.



Alta Dirección

Formación orientada a la toma de decisiones estratégicas en ciberseguridad y gestión del riesgo institucional.



Personal Operativo

Concientización sobre buenas prácticas cotidianas, manejo de información y reconocimiento de amenazas.



Personal Técnico

Capacitación especializada en configuraciones seguras, gestión de vulnerabilidades y respuesta a incidentes.

8. Cierre del Informe

El avance del proyecto evidencia la consolidación de una **postura de ciberseguridad más estructurada**, alineada con estándares internacionales y orientada a la mejora continua.

Las acciones implementadas no solo permiten atender las vulnerabilidades identificadas, sino también fortalecer las capacidades institucionales para gestionar el riesgo de manera proactiva, sostenible y alineada con el contexto actual de amenazas.

8.1 Conclusiones Estratégicas

Gestión Continua y Basada en Riesgo

La Superintendencia de Transporte ha avanzado en la implementación de un modelo de gestión de ciberseguridad continuo, medible y basado en riesgo, superando el enfoque reactivo y puntual.

Visibilidad Integral de la Superficie de Ataque

La combinación de monitoreo en entornos restringidos y escaneos externos proporciona una visión completa y actualizada de la exposición institucional.

Base de Gobierno Tecnológico Fortalecida

La consolidación del inventario de activos establece los cimientos necesarios para una gestión de seguridad trazable, auditable y alineada con estándares internacionales.

Alineación con Marcos Internacionales

Las actividades ejecutadas demuestran coherencia con los marcos NIST CSF, ISO/IEC 27001 y OWASP, posicionando a la entidad en una trayectoria de madurez reconocible y verificable.

8.2 Recomendaciones Estratégicas Priorizadas

Con base en los hallazgos y el avance del proyecto, se presentan las siguientes recomendaciones estratégicas, ordenadas por prioridad:

1

Implementar MFA de Forma Generalizada

Prioridad: Crítica. Extender la autenticación multifactor a todas las cuentas institucionales, comenzando por accesos privilegiados y sistemas críticos.

2

Formalizar el Proceso de Gestión de Vulnerabilidades

Prioridad: Alta. Establecer un ciclo formal de identificación, priorización, remediación y verificación de vulnerabilidades con periodicidad definida.

3

Completar y Mantener el Inventario de Activos

Prioridad: Alta. Finalizar la depuración del inventario tecnológico y establecer un proceso de actualización continua con responsables definidos.

4

Ejecutar el Plan de Formación y Concientización

Prioridad: Media-Alta. Implementar el programa de capacitación en ciberseguridad para todos los actores de la Superintendencia, priorizando contenidos basados en riesgos reales identificados.

8.3 Recomendaciones Técnicas Específicas

Adicionalmente, se presentan las siguientes recomendaciones técnicas específicas derivadas de las actividades ejecutadas:

Área Técnica	Recomendación	Marco de Referencia
Gestión de Credenciales	Implementar política de rotación periódica de contraseñas y prohibición de reutilización	NIST SP 800-63B / ISO 27001 A.9
Seguridad en Aplicaciones Web	Implementar encabezados de seguridad HTTP (CSP, HSTS, X-Frame-Options) en todos los portales	OWASP Top 10 / A05:2021
Cifrado en Tránsito	Deshabilitar TLS 1.0 y 1.1, migrar a TLS 1.3 en todos los servicios publicados	NIST SP 800-52 / ISO 27001 A.10
Segmentación de Red	Revisar y fortalecer la segmentación entre zonas de red para limitar el movimiento lateral	NIST CSF PR.AC / ISO 27001 A.13
Gestión de Parches	Establecer ciclo mensual de aplicación de parches críticos con ventana de mantenimiento definida	NIST CSF ID.RA / ISO 27001 A.12

8.4 Hoja de Ruta de Corto Plazo (0–3 Meses)

Para el período inmediato, se recomienda priorizar las siguientes acciones de cierre de brechas identificadas:



Rotación de Credenciales Comprometidas

Ejecutar rotación inmediata de todas las credenciales identificadas como expuestas en el monitoreo de Dark Web.



Aplicación de Parches Críticos

Remediar las vulnerabilidades críticas identificadas en los escaneos externos con mayor urgencia.



Revisión de Reglas de Firewall

Auditar y depurar las reglas de firewall para cerrar servicios innecesarios expuestos a Internet.

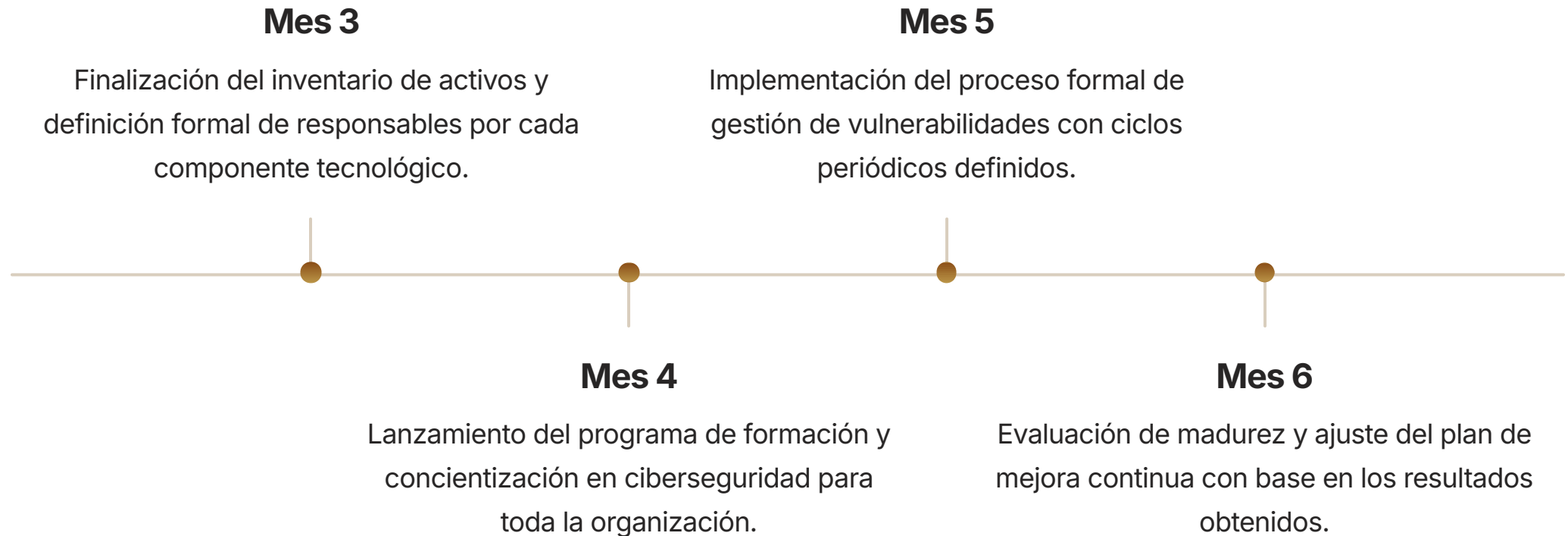


Despliegue Inicial de MFA

Iniciar el despliegue de autenticación multifactor en cuentas privilegiadas y sistemas críticos.

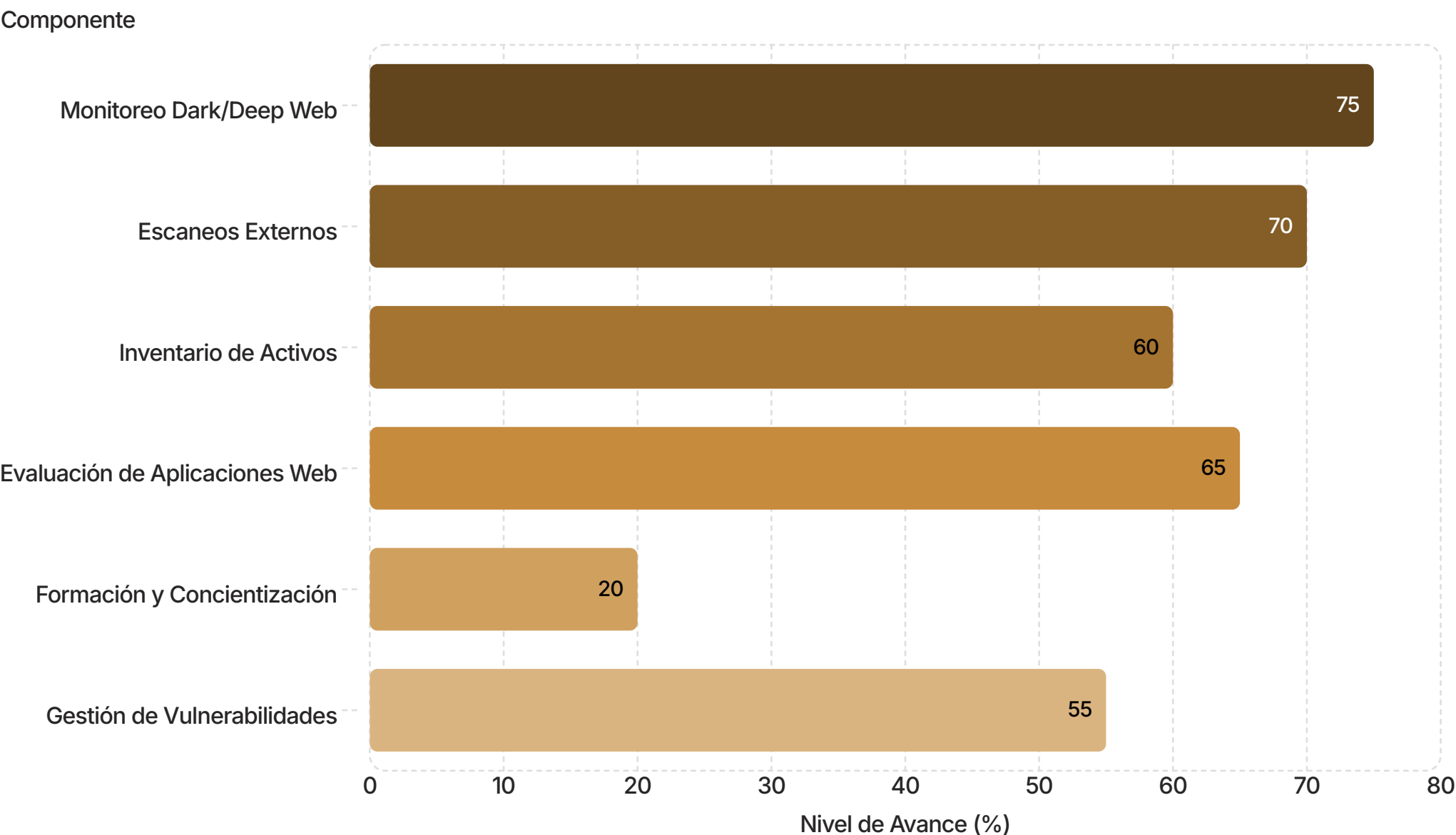
8.5 Hoja de Ruta de Mediano Plazo (3–6 Meses)

En el mediano plazo, el proyecto debe avanzar hacia la consolidación de capacidades institucionales sostenibles:



Resumen Ejecutivo del Avance

A continuación se presenta un resumen ejecutivo del estado de avance de los componentes principales del proyecto de ciberseguridad institucional:



El gráfico refleja el estado de avance estimado por componente al cierre del período evaluado. Los componentes de monitoreo y escaneos externos presentan el mayor nivel de madurez, mientras que la formación y concientización se encuentra en fase de planificación para las próximas fases del proyecto.

Alineación con Marcos de Referencia Internacionales

El siguiente cuadro resume la alineación de las actividades ejecutadas con los principales marcos de referencia internacionales aplicables al proyecto:

Actividad del Proyecto	NIST CSF	ISO/IEC 27001	OWASP
Monitoreo Dark/Deep Web	DE.CM-7 / ID.RA-2	A.12.4 / A.16.1	—
Escaneos Externos de Infraestructura	ID.RA-1 / PR.IP-12	A.12.6 / A.18.2	—
Evaluación de Aplicaciones Web	ID.RA-1 / PR.DS-2	A.14.2 / A.12.6	Top 10 / ASVS
Inventario de Activos	ID.AM-1 / ID.AM-2	A.8.1 / A.8.2	—
Formación y Concientización	PR.AT-1 / PR.AT-2	A.7.2.2 / A.6.1	—

Declaración de Conformidad y Firma

El presente informe de seguimiento ha sido elaborado con base en las actividades técnicas ejecutadas durante el período evaluado, siguiendo los lineamientos metodológicos establecidos para el proyecto institucional de ciberseguridad de la Superintendencia de Transporte.

El avance del proyecto evidencia la consolidación de una postura de ciberseguridad más estructurada, alineada con estándares internacionales y orientada a la mejora continua. Las acciones implementadas no solo permiten atender las vulnerabilidades identificadas, sino también fortalecer las capacidades institucionales para gestionar el riesgo de manera proactiva, sostenible y alineada con el contexto actual de amenazas.

N.º	Nombre	Fecha	Firma
001	Virgilio Salgado Escorce	04 de Marzo de 2026	_____

Lugar de elaboración: Barranquilla, Atlántico, Colombia

Información del Documento

Entidad Superintendencia de Transporte de Colombia	Tipo de Documento Informe de Seguimiento — Proyecto Institucional de Ciberseguridad
Período Evaluado Marzo 2026	Clasificación Uso Institucional Restringido
Nota de Confidencialidad: El presente documento contiene información técnica de carácter institucional relacionada con la postura de ciberseguridad de la Superintendencia de Transporte. Su contenido es de uso exclusivo de las partes autorizadas y no debe ser divulgado, reproducido ni distribuido sin autorización expresa de la entidad. La información aquí contenida está sujeta a las disposiciones legales aplicables en materia de protección de datos y seguridad de la información en Colombia.	

Elaborado por: Virgilio Salgado Escorce — Consultor Senior en Ciberseguridad / Barranquilla, Atlántico, Colombia / Marzo 2026