

MATRIZ KPIs/KRIs

SUPERINTENDENCIA DE TRANSPORTE

CREADO POR: Virgilio Salgado Escorce

FECHA: Marzo 2026

LUGAR: Barranquilla, Atlántico



SuperTransporte



Registro de Autoría

Documento oficial de la Superintendencia de Transporte — Marzo 2026

Nombre	Fecha
Virgilio Salgado Escorce	04/Marzo/2026

Tabla de Contenido

01	02	03
1. Introducción	2. Objetivos 2.1 Objetivo General · 2.2 Objetivos Específicos	3. Desarrollo: Propuesta de Matrices KPIs/KRIs 3.1 Identificar · 3.2 Proteger · 3.3 Detectar · 3.4 Responder · 3.5 Recuperar
04	05	
4. Recomendación de Operación de la Matriz	5. Conclusión	

1. Introducción

La gestión moderna de la ciberseguridad en entidades con alta criticidad operativa y regulatoria, como una Superintendencia, requiere más que controles técnicos puntuales: demanda un modelo de medición continuo que permita evidenciar el estado real de la postura de seguridad, la efectividad de las acciones implementadas y la evolución del riesgo en el tiempo.

En este contexto, una **matriz de indicadores (KPIs y KRIs)** se convierte en un mecanismo estructural para transformar eventos, alertas y datos operativos en información gerencial útil, verificable y trazable.

KPIs y KRIs: Definición y Propósito

KPIs — Key Performance Indicators

Los **KPIs** permiten medir el desempeño del programa de seguridad: qué tan eficientemente se ejecutan las actividades de protección, detección, respuesta y recuperación.

KRIs — Key Risk Indicators

Los **KRIs** permiten medir exposición y riesgo: qué tan vulnerable o comprometida está la Entidad frente a amenazas, brechas, incumplimientos o fallas de control.

La combinación de ambos habilita una visión completa: **desempeño vs. riesgo, operación vs. exposición.**

Articulación Técnica y de Gobernanza

Estas matrices, además, permiten articular el trabajo técnico con la gobernanza, ya que conectan el día a día con decisiones estratégicas:

→ **Operación diaria**

Vulnerabilidades, parches, alertas, backups, identidades, incidentes

→ **Decisiones estratégicas**

Priorización, presupuesto, fortalecimiento de capacidades, adquisición de herramientas y control de proveedores

2. Objetivos

2.1 Objetivo General

Definir un conjunto de posibles indicadores KPIs/KRIs que podrían aplicarse en la Superintendencia de Transporte para medir de manera periódica la madurez operativa y la exposición al riesgo en ciberseguridad, soportando la gestión del programa y el cumplimiento de lineamientos institucionales.

2.2 Objetivos Específicos

1

Indicadores medibles

Establecer indicadores medibles para áreas críticas como inventario de activos, gestión de identidades, vulnerabilidades, monitoreo, continuidad y respuesta a incidentes.

2

Lógica de medición

Definir la lógica de medición (fórmulas), fuentes de datos, periodicidad y propósito de cada indicador.

3

Intención clara

Asegurar que cada indicador tenga una intención clara: mejorar control, reducir exposición, evidenciar cumplimiento y soportar decisiones.

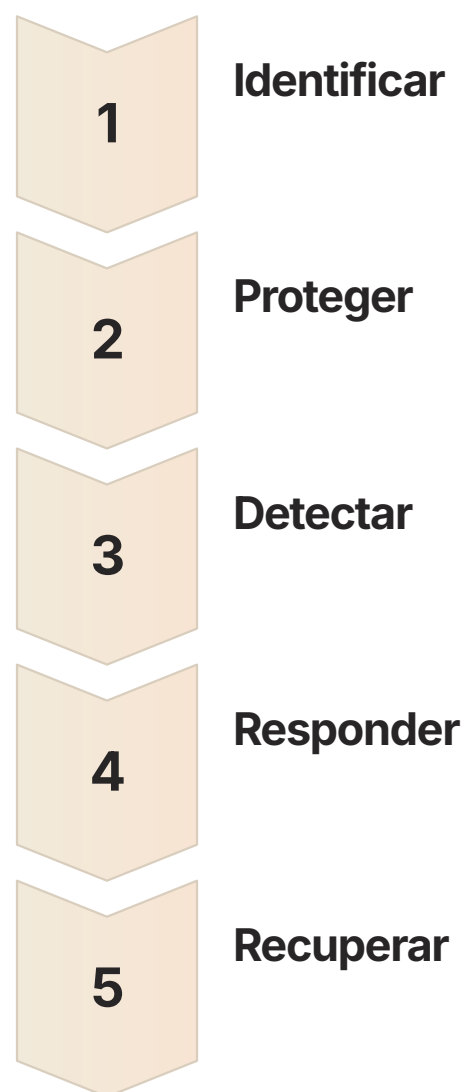
4

Estructura auditable

Proponer una estructura de matriz auditable que permita presentar resultados en comités, informes de seguimiento y planes de mejoramiento.

3. Desarrollo: Propuesta de Matrices KPIs/KRIs

La siguiente propuesta organiza los indicadores por dominios alineados con una lógica similar a NIST (**Identificar, Proteger, Detectar, Responder y Recuperar**). En la práctica, esta estructura facilita que la Entidad pueda asignar responsables por proceso, conectar los indicadores con controles y construir tableros ejecutivos.



DOMINIO 3.1

3.1 Dominio: Identificar Gobierno, inventario y gestión de riesgo

Este dominio agrupa los indicadores relacionados con la visibilidad y el control sobre los activos tecnológicos, la gobernanza de lo crítico y la gestión del riesgo asociado a terceros.

Indicador 1

Cobertura de inventario de activos
(KPI)

Indicador 2

Activos críticos con clasificación y
dueño asignado (KPI)

Indicador 3

Proveedores críticos evaluados en
seguridad (KRI)

Indicador 1. Cobertura de inventario de activos (KPI)

¿Qué mide?

El nivel de control y visibilidad sobre activos tecnológicos (servidores, endpoints, aplicaciones, servicios expuestos, bases de datos, redes, equipos de seguridad).

¿Cómo medirlo?

Porcentaje de activos registrados frente al universo de activos identificados/estimados.

Fórmula

(Activos registrados en inventario / Activos totales estimados) × 100

¿Por qué medirlo?

Si un activo no está inventariado, normalmente queda fuera de parches, monitoreo, hardening y control de cambios; esto se traduce en exposición silenciosa y hallazgos recurrentes en auditoría.

Indicador 2. Activos críticos con clasificación y dueño asignado (KPI)

¿Qué mide?

El nivel de gobernanza sobre lo crítico (sistemas misionales, plataformas externas, servicios de atención, integraciones).

¿Cómo medirlo?

Porcentaje de activos críticos que tienen clasificación (confidencialidad, integridad, disponibilidad) y propietario responsable (owner).

Fórmula

(Activos críticos con owner y clasificación / Total activos críticos) × 100

¿Por qué medirlo?

Sin dueño no hay priorización real ni responsables de remediación; las brechas se quedan "sin doliente".

Indicador 3. Proveedores críticos evaluados en seguridad (KRI)

¿Qué mide?

El riesgo asociado a terceros que soportan infraestructura, desarrollo, nube, SOC, soporte, licenciamiento o datos.

¿Cómo medirlo?

Número o porcentaje de proveedores críticos con evaluación vigente (seguridad, acuerdos, cláusulas, SLA, evidencias).

Fórmula

(Proveedores críticos evaluados / Proveedores críticos totales) × 100

¿Por qué medirlo?

El riesgo de terceros suele ser una vía de entrada frecuente; medirlo fuerza disciplina contractual y de verificación.

3.2 Dominio: Proteger

Identities, hardening, patches, seguridad de configuración

Este dominio agrupa los indicadores relacionados con la protección activa de la infraestructura, las identidades y las configuraciones de seguridad.

Indicador 4

Cobertura de MFA en usuarios corporativos **(KPI)**

Indicador 5

Cuentas privilegiadas sin controles reforzados **(KRI)**

Indicador 6

Cumplimiento de parchado crítico **(KPI)**

Indicador 7

Vulnerabilidades críticas "envejecidas" **(KRI)**

Indicador 8

Cumplimiento de hardening en endpoints y servidores **(KPI)**

Indicador 4. Cobertura de MFA en usuarios corporativos (KPI)

¿Qué mide?

El nivel de protección de acceso de usuarios (especialmente en correo, VPN, paneles administrativos y nube).

¿Cómo medirlo?

Porcentaje de usuarios activos con MFA habilitado.

Fórmula

$(\text{Usuarios con MFA} / \text{Usuarios activos totales}) \times 100$

¿Por qué medirlo?

Gran parte de incidentes se originan en credenciales; MFA reduce drásticamente la efectividad de credenciales filtradas.

Indicador 5. Cuentas privilegiadas sin controles reforzados (KRI)

¿Qué mide?

El riesgo por cuentas admin sin MFA, sin PAM, sin rotación de credenciales o sin segmentación.

¿Cómo medirlo?

Conteo de cuentas privilegiadas que incumplen requisitos mínimos.

Fórmula

cuentas privilegiadas que no cumplen baseline

¿Por qué medirlo?

La cuenta privilegiada es el "camino corto" del atacante; una sola cuenta débil puede comprometer dominio, servidores y datos.

Indicador 6. Cumplimiento de parchado crítico (KPI)

¿Qué mide?

Eficiencia en remediación de vulnerabilidades críticas mediante actualizaciones.

¿Cómo medirlo?

Porcentaje de activos con parches críticos aplicados dentro del plazo definido (por ejemplo 15 o 30 días).

Fórmula

(Activos parchados en SLA / Activos con parches críticos pendientes) × 100

¿Por qué medirlo?

El tiempo de exposición es el factor que más correlaciona con incidentes reales; reduce superficie de ataque.

Indicador 7. Vulnerabilidades críticas "envejecidas" (KRI)

¿Qué mide?

Riesgo acumulado por CVEs críticas abiertas por encima del umbral permitido.

¿Cómo medirlo?

Número de vulnerabilidades críticas abiertas > X días.

Fórmula

vulnerabilidades CVSS alto/crítico con antigüedad > X días

¿Por qué medirlo?

La vulnerabilidad sin remediar es una puerta abierta; el "aging" es señal de deuda técnica y falta de priorización.

Indicador 8. Cumplimiento de hardening en endpoints y servidores (KPI)

¿Qué mide?

Nivel de cumplimiento de una línea base segura (CIS, baseline institucional o proveedor).

¿Cómo medirlo?

Porcentaje de equipos que cumplen la configuración mínima.

Fórmula

$(\text{Equipos conformes} / \text{Equipos evaluados}) \times 100$

¿Por qué medirlo?

Muchos ataques no requieren "exploits sofisticados"; se apoyan en configuraciones débiles o servicios innecesarios.

3.3 Dominio: Detectar

Monitoreo, SOC, logs, visibilidad

Este dominio agrupa los indicadores relacionados con la capacidad de detección de eventos, la cobertura de monitoreo y la visibilidad sobre amenazas activas.

Indicador 9

Cobertura de monitoreo de logs **(KPI)**

Indicador 10

Alertas críticas sin triage oportuno **(KRI)**

Indicador 11

Tiempo medio de detección (MTTD) **(KPI)**

Indicador 12

Credenciales expuestas en fuentes abiertas/dark web **(KRI)**

Indicador 9. Cobertura de monitoreo de logs (KPI)

¿Qué mide?

Qué tanto de la infraestructura realmente genera evidencia utilizable para detectar incidentes.

¿Cómo medirlo?

Porcentaje de activos críticos enviando logs al SIEM o repositorio central.

Fórmula

$$(\text{Activos críticos con logs centralizados} / \text{Activos críticos totales}) \times 100$$

¿Por qué medirlo?

Sin logs, no hay investigación ni trazabilidad; también se afectan auditorías y procesos disciplinarios.

Indicador 10. Alertas críticas sin triage oportuno (KRI)

¿Qué mide?

Riesgo por alertas críticas no revisadas en el tiempo definido.

¿Cómo medirlo?

Número de alertas high/critical que no tuvieron análisis inicial dentro de 24h (o SLA definido).

Fórmula

alertas críticas fuera de SLA de triage

¿Por qué medirlo?

Una alerta crítica no atendida puede significar un incidente en progreso.

Indicador 11. Tiempo medio de detección (MTTD) (KPI)

¿Qué mide?

Velocidad de detección desde que ocurre un evento relevante hasta que se identifica como incidente/alerta accionable.

¿Cómo medirlo?

Promedio del tiempo entre timestamp del evento inicial y timestamp del primer triage válido.

Fórmula

promedio (hora triage – hora evento)

¿Por qué medirlo?

Mientras más tarda la detección, más se expande el impacto.

Indicador 12. Credenciales expuestas en fuentes abiertas/dark web (KRI)

¿Qué mide?

Exposición de identidades institucionales por filtraciones externas.

¿Cómo medirlo?

Número de hallazgos de credenciales asociadas a dominios/correos institucionales, identificadas por monitoreo.

Fórmula

credenciales detectadas por periodo

¿Por qué medirlo?

La exposición de credenciales convierte el perímetro en irrelevante; obliga a reforzar MFA, rotación y concientización.

DOMINIO 3.4

3.4 Dominio: Responder

Gestión de incidentes, coordinación, SLA, lecciones aprendidas

Este dominio agrupa los indicadores relacionados con la capacidad de respuesta ante incidentes, el cumplimiento de tiempos comprometidos y la gestión de causas raíz.

Indicador 13

Cumplimiento de SLA de atención de incidentes **(KPI)**

Indicador 14

Tiempo medio de respuesta/contención (MTTR) **(KPI)**

Indicador 15

Incidentes repetitivos por misma causa **(KRI)**

Indicador 13. Cumplimiento de SLA de atención de incidentes (KPI)

¿Qué mide?

Desempeño del proceso de respuesta frente a tiempos comprometidos según severidad.

¿Cómo medirlo?

Porcentaje de incidentes atendidos dentro del SLA por severidad.

Fórmula

$(\text{Incidentes dentro de SLA} / \text{Incidentes totales}) \times 100$

¿Por qué medirlo?

Asegura disciplina operativa y visibilidad; facilita justificar recursos.

Indicador 14. Tiempo medio de respuesta/contención (MTTR) (KPI)

¿Qué mide?

Cuánto tarda la Entidad en contener o mitigar un incidente una vez identificado.

¿Cómo medirlo?

Promedio entre "incidente confirmado" y "incidente contenido/mitigado".

Fórmula

promedio (hora contención – hora confirmación)

¿Por qué medirlo?

MTTR alto indica fallas en coordinación, playbooks, herramientas o capacidad instalada.

Indicador 15. Incidentes repetitivos por misma causa (KRI)

¿Qué mide?

Riesgo de recurrencia por ausencia de remediación estructural (causa raíz).

¿Cómo medirlo?

Conteo de incidentes similares en un periodo, agrupados por causa.

Fórmula

incidentes con misma causa / periodo

¿Por qué medirlo?

Si se repite, no se corrigió el control; suele ser indicador de deuda y de controles incompletos.

3.5 Dominio: Recuperar

Continuidad, backups, restauración, resiliencia

Este dominio agrupa los indicadores relacionados con la capacidad real de recuperación ante incidentes, la confiabilidad de los backups y el cumplimiento de objetivos de continuidad operativa.

Indicador 16

Tasa de éxito de backups **(KPI)**

Indicador 17

Backups en Warning/Failed sin gestión **(KRI)**

Indicador 18

Pruebas de restauración ejecutadas y exitosas **(KPI)**

Indicador 19

Cumplimiento de RTO/RPO en sistemas críticos **(KRI)**

Indicador 16. Tasa de éxito de backups (KPI)

¿Qué mide?

Confiabilidad operativa del sistema de copias de seguridad.

¿Cómo medirlo?

Porcentaje de trabajos de backup finalizados en estado OK.

Fórmula

$(\text{Backups OK} / \text{Backups totales}) \times 100$

¿Por qué medirlo?

Es un control crítico frente a ransomware, fallas de infraestructura y error humano.

Indicador 17. Backups en Warning/Failed sin gestión (KRI)

¿Qué mide?

Riesgo por fallas recurrentes no atendidas (sin corrección ni evidencias).

¿Cómo medirlo?

Cantidad de backups en Warning/Failed que permanecen sin ticket, sin RCA o sin acciones.

Fórmula

backups Warning/Failed sin gestión por periodo

¿Por qué medirlo?

Un backup "existente" pero no restaurable es un falso positivo de seguridad; medirlo mejora disciplina de continuidad.

Indicador 18. Pruebas de restauración ejecutadas y exitosas (KPI)

¿Qué mide?

Capacidad real de recuperación, no solo ejecución de backups.

¿Cómo medirlo?

Porcentaje de pruebas de restauración exitosas sobre pruebas planificadas.

Fórmula

(Restauraciones exitosas / Restauraciones planificadas)
× 100

¿Por qué medirlo?

La única evidencia real de recuperación es restaurar; esto reduce hallazgos y aumenta resiliencia.

Indicador 19. Cumplimiento de RTO/RPO en sistemas críticos (KRI)

¿Qué mide?

Riesgo de indisponibilidad prolongada o pérdida de datos por encima de lo aceptable.

¿Cómo medirlo?

Número de sistemas críticos que no cumplen objetivos de RTO/RPO definidos.

Fórmula

sistemas críticos fuera de RTO/RPO

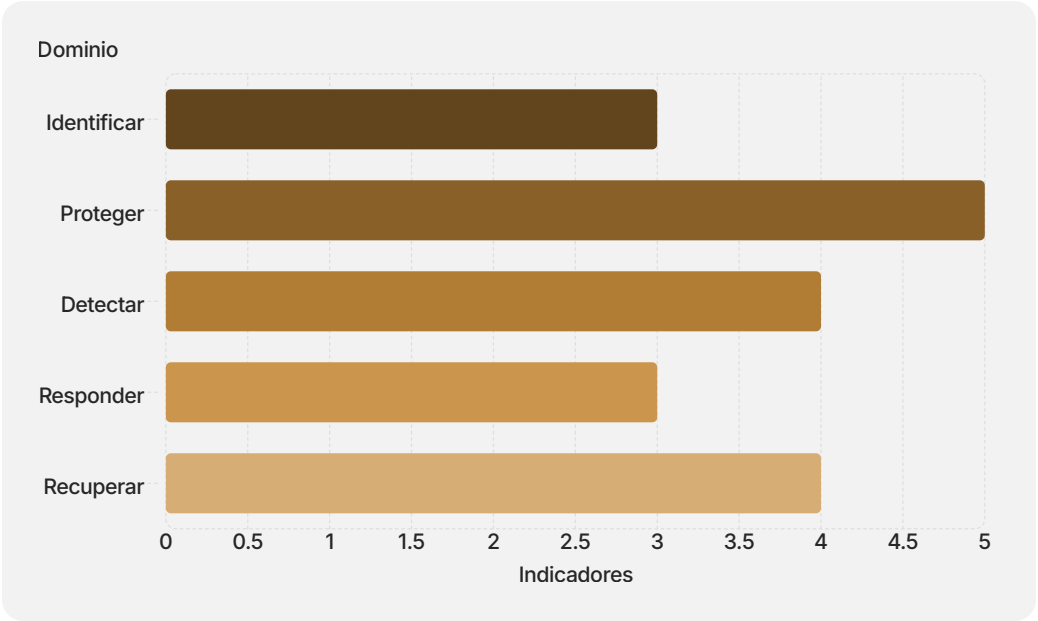
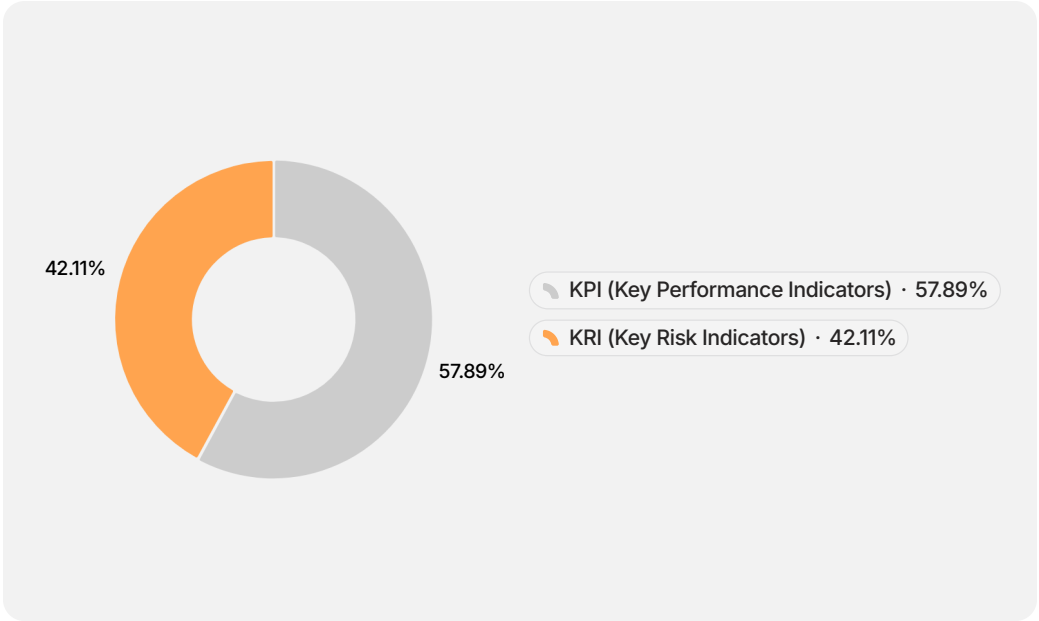
¿Por qué medirlo?

Conecta ciberseguridad con continuidad operativa y misión institucional.

Resumen de Indicadores por Dominio

#	Nombre del Indicador	Dominio	Tipo	Foco
1	Cobertura de inventario de activos	Identificar	KPI	Control
2	Activos críticos con clasificación y dueño asignado	Identificar	KPI	Gobernanza
3	Proveedores críticos evaluados en seguridad	Identificar	KRI	Riesgo
4	Cobertura de MFA en usuarios corporativos	Proteger	KPI	Identidad
5	Cuentas privilegiadas sin controles reforzados	Proteger	KRI	Riesgo
6	Cumplimiento de parchado crítico	Proteger	KPI	Remediación
7	Vulnerabilidades críticas "envejecidas"	Proteger	KRI	Exposición
8	Cumplimiento de hardening en endpoints y servidores	Proteger	KPI	Configuración
9	Cobertura de monitoreo de logs	Detectar	KPI	Visibilidad
10	Alertas críticas sin triage oportuno	Detectar	KRI	Riesgo
11	Tiempo medio de detección (MTTD)	Detectar	KPI	Velocidad
12	Credenciales expuestas en fuentes abiertas/dark web	Detectar	KRI	Exposición
13	Cumplimiento de SLA de atención de incidentes	Responder	KPI	Desempeño
14	Tiempo medio de respuesta/contención (MTTR)	Responder	KPI	Velocidad
15	Incidentes repetitivos por misma causa	Responder	KRI	Recurrencia
16	Tasa de éxito de backups	Recuperar	KPI	Continuidad
17	Backups en Warning/Failed sin gestión	Recuperar	KRI	Riesgo
18	Pruebas de restauración ejecutadas y exitosas	Recuperar	KPI	Resiliencia
19	Cumplimiento de RTO/RPO en sistemas críticos	Recuperar	KRI	Continuidad

Distribución de Indicadores por Tipo



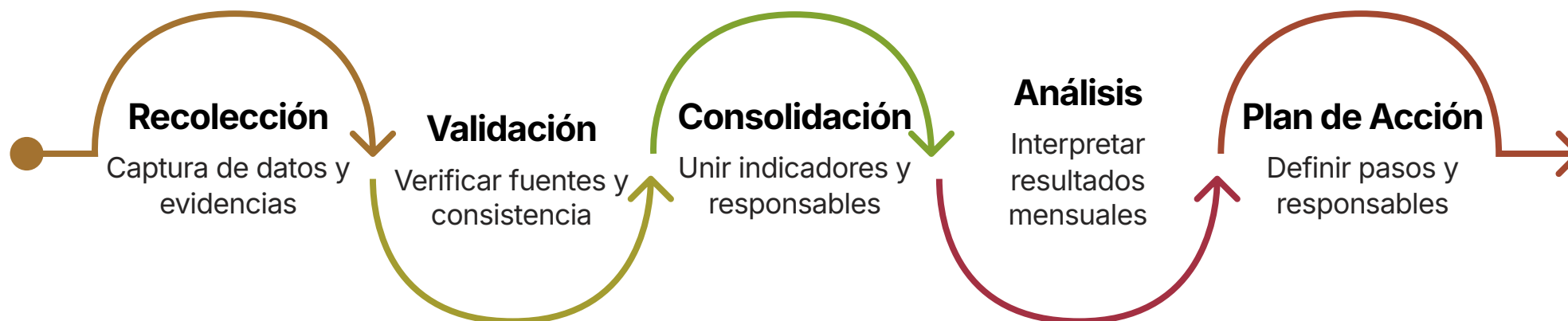
SECCIÓN 4

4. Recomendación de Operación de la Matriz

Cómo usarla

Para que la matriz sea útil en la práctica, se recomienda que la Entidad la opere como un **ciclo mensual**: recolección de datos, validación, consolidación, análisis y plan de acción.

Ciclo Mensual de Operación



La matriz debe tener responsables asignados por indicador, evidencias almacenadas y consistencia de fuentes.

Tablero Ejecutivo

De forma complementaria, se recomienda mantener un **tablero ejecutivo** con una selección reducida de indicadores críticos (por ejemplo 10–12), presentados en semáforo con tendencia, para facilitar la lectura en comité.

Responsables por indicador

Cada indicador debe tener un responsable asignado que garantice la recolección y validación de datos.

Evidencias almacenadas

Toda medición debe contar con evidencias documentadas y trazables para auditoría.

Consistencia de fuentes

Las fuentes de datos deben ser consistentes entre periodos para garantizar comparabilidad.

Selección reducida (10–12 indicadores)

Presentados en semáforo con tendencia, para facilitar la lectura en comité.

Preguntas Directivas que Debe Responder la Matriz

En una Superintendencia, estos indicadores deben permitir responder preguntas directas de dirección y control interno:



¿Qué tan expuestos estamos?

Nivel de exposición actual frente a amenazas y brechas identificadas.



¿Qué se ha corregido?

Acciones de remediación ejecutadas y controles cerrados en el periodo.



¿Qué sigue abierto?

Brechas, hallazgos y vulnerabilidades pendientes de cierre.



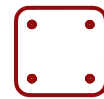
¿Qué tan rápido reaccionamos?

Tiempos de detección, respuesta y contención ante incidentes.



¿Qué evidencia tenemos?

Trazabilidad documental de acciones, controles y resultados.



¿Qué está bloqueando el cierre de brechas?

Obstáculos operativos, presupuestales o de capacidad que impiden la remediación.

5. Conclusión

La implementación de una matriz de KPIs/KRIs permite a la Superintendencia de Transporte pasar de una visión reactiva de la seguridad a una gestión estructurada basada en evidencia.

El Principio de Medición

Medir no es un fin, sino el mecanismo para controlar: **lo que no se mide no se administra**, y lo que no se administra tiende a convertirse en hallazgos repetitivos, riesgos acumulados y exposición institucional.

Alcance de la Propuesta

Esta propuesta presenta indicadores que cubren desde la visibilidad de activos y la protección de identidades hasta la detección de alertas, la respuesta a incidentes y la capacidad real de recuperación, habilitando un programa de mejora continua que fortalece tanto la postura técnica como la gobernanza.



Visión Reactiva vs. Gestión Estructurada

Visión Reactiva *(antes)*

- Respuesta a eventos sin medición sistemática
- Hallazgos repetitivos sin causa raíz resuelta
- Riesgos acumulados sin visibilidad gerencial
- Exposición institucional no cuantificada

Gestión Estructurada Basada en Evidencia *(después)*

- Medición continua y periódica de indicadores
- Remediación estructural con causa raíz identificada
- Visibilidad gerencial en comités y tableros
- Postura técnica y gobernanza fortalecidas

Resumen Ejecutivo: Dominio Identificar

#	Indicador	Fórmula	Tipo
1	Cobertura de inventario de activos	$(\text{Activos registrados} / \text{Activos totales estimados}) \times 100$	KPI
2	Activos críticos con clasificación y dueño asignado	$(\text{Activos críticos con owner y clasificación} / \text{Total activos críticos}) \times 100$	KPI
3	Proveedores críticos evaluados en seguridad	$(\text{Proveedores críticos evaluados} / \text{Proveedores críticos totales}) \times 100$	KRI

Resumen Ejecutivo: Dominio Proteger

#	Indicador	Fórmula	Tipo
4	Cobertura de MFA en usuarios corporativos	$(\text{Usuarios con MFA} / \text{Usuarios activos totales}) \times 100$	KPI
5	Cuentas privilegiadas sin controles reforzados	# cuentas privilegiadas que no cumplen baseline	KRI
6	Cumplimiento de parchado crítico	$(\text{Activos parchados en SLA} / \text{Activos con parches críticos pendientes}) \times 100$	KPI
7	Vulnerabilidades críticas "envejecidas"	# vulnerabilidades CVSS alto/crítico con antigüedad > X días	KRI
8	Cumplimiento de hardening en endpoints y servidores	$(\text{Equipos conformes} / \text{Equipos evaluados}) \times 100$	KPI

Resumen Ejecutivo: Dominio Detectar

#	Indicador	Fórmula	Tipo
9	Cobertura de monitoreo de logs	(Activos críticos con logs centralizados / Activos críticos totales) × 100	KPI
10	Alertas críticas sin triage oportuno	# alertas críticas fuera de SLA de triage	KRI
11	Tiempo medio de detección (MTTD)	promedio (hora triage – hora evento)	KPI
12	Credenciales expuestas en fuentes abiertas/dark web	# credenciales detectadas por periodo	KRI

Resumen Ejecutivo: Dominios Responder y Recuperar

#	Indicador	Fórmula	Tipo
13	Cumplimiento de SLA de atención de incidentes	$(\text{Incidentes dentro de SLA} / \text{Incidentes totales}) \times 100$	KPI
14	Tiempo medio de respuesta/contención (MTTR)	promedio (hora contención – hora confirmación)	KPI
15	Incidentes repetitivos por misma causa	# incidentes con misma causa / periodo	KRI
16	Tasa de éxito de backups	$(\text{Backups OK} / \text{Backups totales}) \times 100$	KPI
17	Backups en Warning/Failed sin gestión	# backups Warning/Failed sin gestión por periodo	KRI
18	Pruebas de restauración ejecutadas y exitosas	$(\text{Restauraciones exitosas} / \text{Restauraciones planificadas}) \times 100$	KPI
19	Cumplimiento de RTO/RPO en sistemas críticos	# sistemas críticos fuera de RTO/RPO	KRI

Beneficios del Programa de Mejora Continua

La implementación de esta matriz habilita un **programa de mejora continua** que fortalece tanto la postura técnica como la gobernanza de la Superintendencia de Transporte.

1

Postura técnica fortalecida

Reducción de superficie de ataque, mejora en tiempos de detección y respuesta, y mayor resiliencia operativa.

2

Gobernanza mejorada

Conexión entre operación técnica y decisiones directivas, con evidencia trazable y auditable.

3

Cumplimiento evidenciado

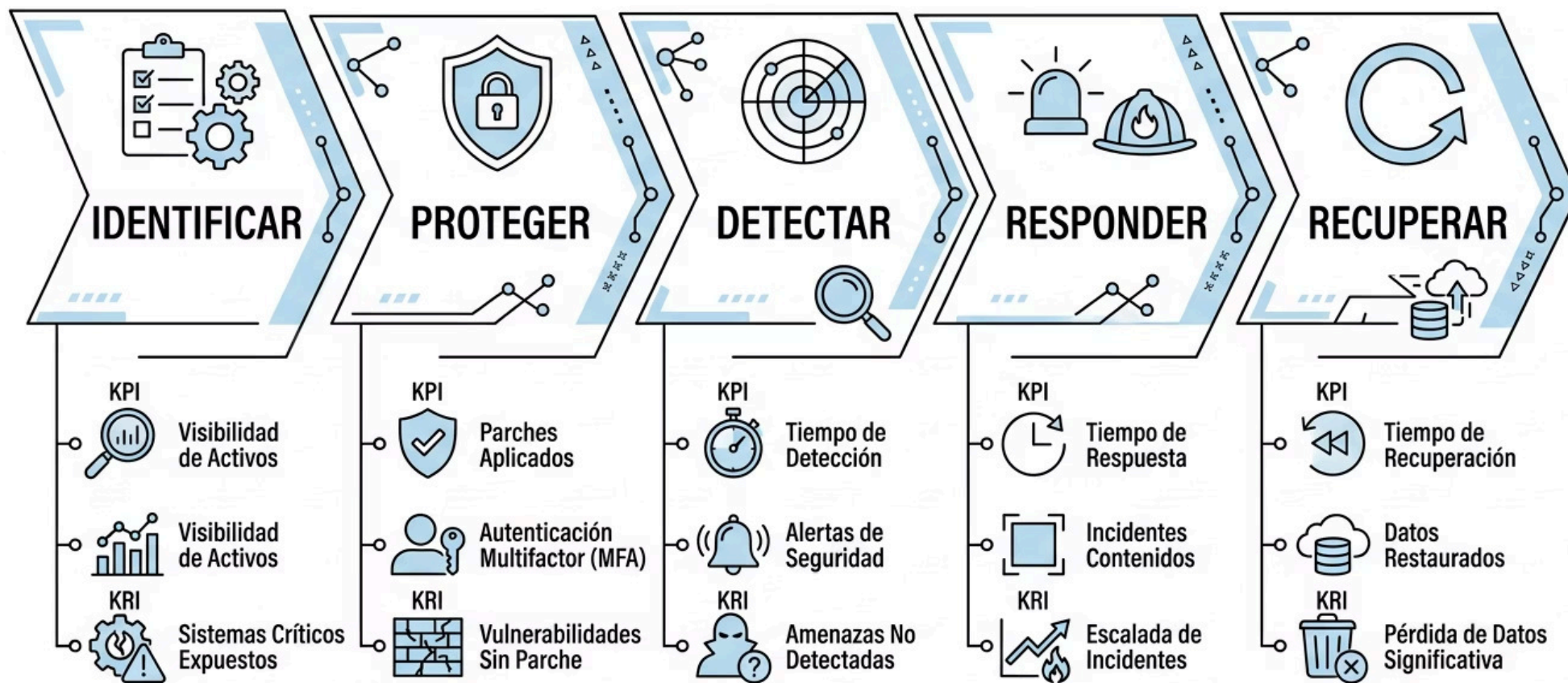
Soporte documental para comités, auditorías, planes de mejoramiento e informes de seguimiento.

4

Reducción de hallazgos repetitivos

Identificación y cierre estructural de causas raíz que generan recurrencia de incidentes y brechas.

Alineación con el Marco NIST



La estructura de dominios NIST facilita que la Entidad pueda asignar responsables por proceso, conectar los indicadores con controles y construir tableros ejecutivos.

Superintendencia de Transporte

Matriz KPIs/KRIs — Ciberseguridad

Autor Virgilio Salgado Escorce	Fecha Marzo 2026
Lugar Barranquilla, Atlántico	Total Indicadores 19 KPIs/KRIs — 5 Dominios NIST
 Documento de uso institucional. El contenido de este informe es de carácter técnico y confidencial, destinado a la gestión interna de ciberseguridad de la Superintendencia de Transporte.	