



SuperTransporte



Evaluación de Madurez en Ciberseguridad

Diagnóstico Estructural según NIST / ISO

Entidad destinataria: Superintendencia de Transporte — República de Colombia

Elaborado por: Virgilio Salgado Escorce — Consultor Senior en Ciberseguridad y Gestión del Riesgo Tecnológico

Fecha del informe: Marzo 2026 | **Sede:** Barranquilla, Atlántico

Informe técnico institucional elaborado con base en los marcos de referencia internacionales NIST Cybersecurity Framework e ISO/IEC 27001, orientado a la toma de decisiones estratégicas en materia de ciberseguridad para entidades del sector público.

Control de Versiones y Aprobación del Documento

El presente informe ha sido elaborado bajo los estándares de una firma consultora especializada en ciberseguridad, gestión del riesgo tecnológico y auditoría de sistemas de información. Su contenido es de carácter técnico-institucional y está destinado a la revisión por parte de directivos, auditores, organismos de control y autoridades de supervisión.

No.	Nombre	Fecha	Firma
001	Virgilio Salgado Escorce	04/Marzo/2026	V. Salgado E.

 Este documento es de uso institucional restringido. Su distribución debe realizarse conforme a los lineamientos de clasificación de la información de la Superintendencia de Transporte.

Tabla de Contenido

01	02	03
Resumen Ejecutivo Síntesis del diagnóstico, nivel general de madurez, principales riesgos y recomendaciones clave.	Contexto Institucional y Objetivo del Diagnóstico Rol de la Superintendencia de Transporte y propósito de la evaluación.	Alcance Metodológico y Metodología de Evaluación Enfoque estructurado, revisión documental y análisis técnico de controles.
04	05	06
Marco de Referencia Internacional (NIST / ISO) Fundamentos del NIST Cybersecurity Framework y principios ISO.	Diagnóstico Actual de Ciberseguridad Estado de controles, hallazgos relevantes y análisis del entorno de riesgo.	Evaluación de Madurez por Dominios Análisis detallado de los ocho dominios de ciberseguridad evaluados.
07	08	
Visualizaciones, Roadmap e Indicadores Radar de madurez, matriz de riesgos, mapa de brechas, roadmap y KPIs/KRIs.	Cierre y Conclusiones Estratégicas Síntesis de hallazgos y ruta de fortalecimiento institucional.	

Resumen Ejecutivo

Síntesis del Diagnóstico

La Superintendencia de Transporte, en atención a la criticidad de sus servicios digitales y al rol institucional que desempeña, requiere fortalecer de manera sostenida su postura de ciberseguridad para garantizar la **confidencialidad, integridad y disponibilidad** de la información. El presente informe plantea el marco narrativo y técnico para una Evaluación de Madurez en Ciberseguridad, con un diagnóstico estructural alineado a referentes internacionales, con el fin de orientar decisiones, priorizar acciones y consolidar un programa de cierre de brechas con enfoque de mejora continua.

La madurez en ciberseguridad no se limita a contar con herramientas; se evidencia en la capacidad real de **gobernar el riesgo, prevenir y detectar amenazas, responder ante incidentes y sostener controles medibles, verificables y auditables**.

Nivel General de Madurez

Nivel 2 – Básico / En transición hacia Nivel 3 (Intermedio). Controles parciales con oportunidades significativas de fortalecimiento.

Principales Riesgos

Vulnerabilidades en aplicaciones web, exposición de credenciales, controles perimetrales con efectividad limitada y debilidades en el ciclo de desarrollo.

Impacto Estratégico

Alta probabilidad de explotación en servicios públicos misionales. Riesgo de accesos no autorizados y afectación a la continuidad operativa.

Recomendaciones Clave

Fortalecer gobernanza, elevar efectividad de controles, robustecer detección y respuesta, e institucionalizar el desarrollo seguro con aseguramiento continuo.

Contexto Institucional

La Superintendencia de Transporte es una entidad del Estado colombiano con funciones de inspección, vigilancia y control sobre el sector transporte. En el ejercicio de sus funciones misionales, la entidad gestiona plataformas digitales, sistemas de información y servicios en línea que soportan procesos críticos de regulación, supervisión y atención ciudadana.

La naturaleza pública de sus servicios, la interconexión con terceros, el acceso remoto y la operación continua de sus plataformas configuran un ecosistema tecnológico con una **superficie de exposición significativa** frente a amenazas cibernéticas actuales. En este contexto, la ciberseguridad no es únicamente una función técnica, sino un **componente estratégico de la gestión institucional** que incide directamente en la confianza ciudadana, la continuidad de los servicios y el cumplimiento del mandato legal de la entidad.

- ❏ La criticidad de los servicios digitales de la Superintendencia de Transporte exige una postura de ciberseguridad madura, medible y sostenida, alineada con los más altos estándares internacionales de gestión del riesgo tecnológico.

Objetivo del Diagnóstico

El objetivo para el presente año es **cerrar la mayoría de brechas de seguridad pendientes y consolidar lineamientos de ciberseguridad firmes, sostenibles y verificables**, que fortalezcan tanto la operación tecnológica como la disciplina de gobierno. La finalidad no es únicamente corregir hallazgos aislados, sino elevar el nivel de madurez mediante prácticas consistentes, medición de efectividad, gestión del riesgo basada en evidencia y capacidades institucionales estables.

En consecuencia, la evaluación de madurez se concibe como un **instrumento de gestión** que conecta hallazgos con decisiones, facilita priorización, soporta la justificación de inversiones y permite control de avances con criterios claros y auditables.

Orientar Decisiones Estratégicas

Traducir hallazgos técnicos en prioridades de control y asignación de responsabilidades con seguimiento mediante indicadores.

Priorizar Acciones de Mejora

Establecer una hoja de ruta clara para mejorar la postura de seguridad, reducir la exposición al riesgo y fortalecer la resiliencia de las plataformas tecnológicas.

Consolidar Programa Continuo

Establecer el cierre de brechas como un proceso continuo con control, medición y evidencia, orientado a reducir el riesgo sobre los servicios críticos.

Alcance Metodológico de la Evaluación

La presente evaluación de madurez en ciberseguridad tiene como alcance **analizar el estado actual de las capacidades institucionales** en materia de gestión del riesgo, controles de seguridad, monitoreo, respuesta ante incidentes y prácticas de desarrollo seguro.

El análisis se realiza considerando los lineamientos de marcos internacionales de referencia y tomando como base la evidencia disponible en la organización, incluyendo:



Configuraciones Tecnológicas

Revisión de la arquitectura de seguridad, controles perimetrales, firewall Fortinet y FortiClient, y parametrización de componentes críticos.



Procesos Operativos

Análisis de procedimientos de gestión de incidentes, control de cambios, gestión de accesos y continuidad del servicio.



Prácticas de Desarrollo

Evaluación del ciclo de vida del software, controles de seguridad en el desarrollo y mecanismos de aseguramiento continuo.



Controles Implementados

Verificación de controles en infraestructura y plataformas digitales, incluyendo efectividad real frente a vectores de ataque actuales.

Este alcance permite establecer un **diagnóstico técnico que facilita la priorización de acciones de mejora** y el fortalecimiento progresivo de la postura institucional de ciberseguridad.

Metodología de Evaluación de Madurez

La evaluación se desarrolla mediante un **enfoque estructurado que combina revisión documental, análisis técnico de controles existentes y contraste con buenas prácticas internacionales.**



Para cada dominio de ciberseguridad se analiza el nivel de formalización, consistencia operativa, capacidad de monitoreo y evidencia de control. A partir de este análisis se determina el nivel de madurez alcanzado por la organización y se identifican las principales brechas que requieren fortalecimiento.

El resultado permite establecer una **visión clara del estado actual de la seguridad institucional** y orientar la toma de decisiones estratégicas.

Modelo de Niveles de Madurez

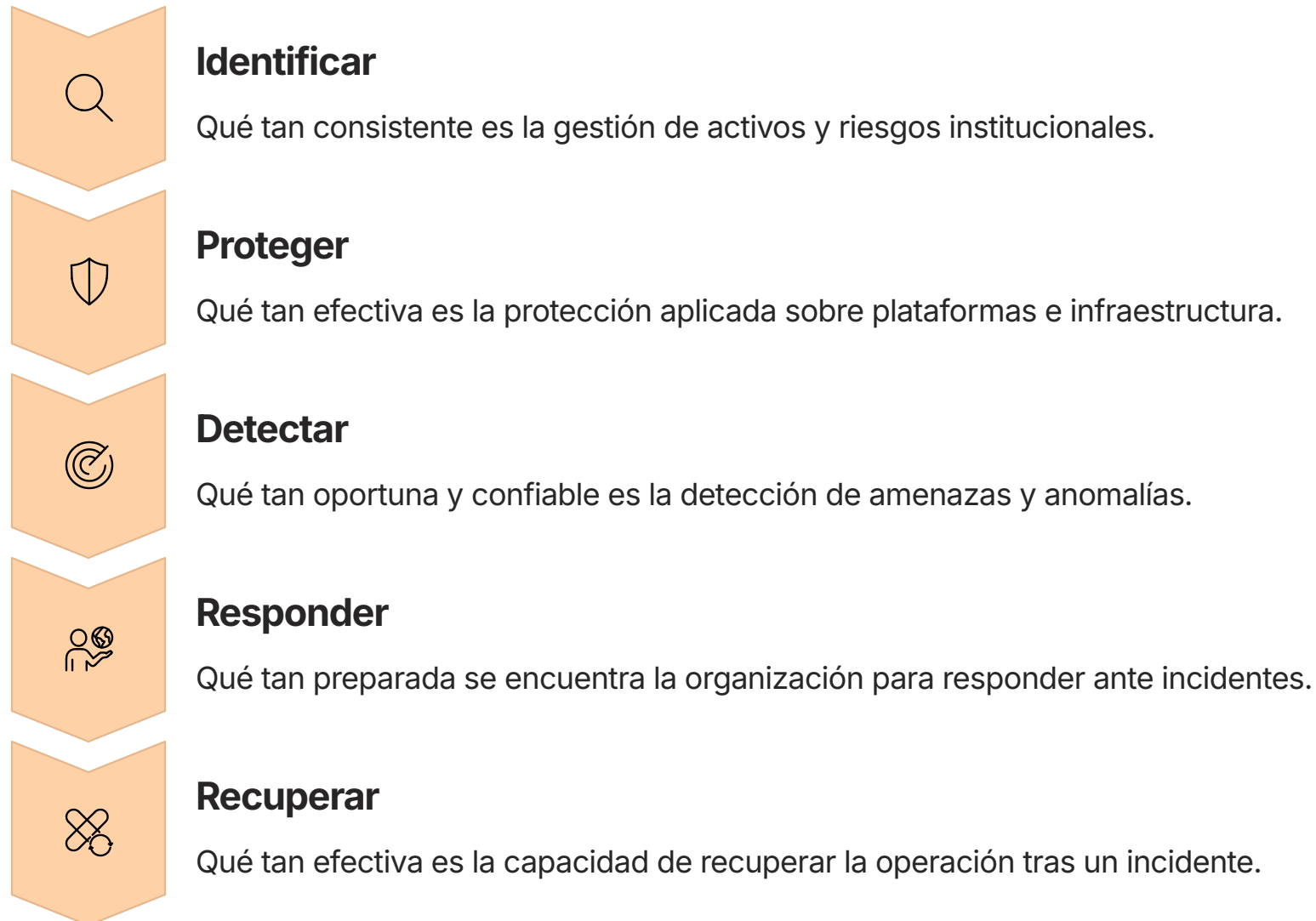
El modelo de madurez utilizado contempla **cinco niveles progresivos**, alineados con las mejores prácticas internacionales de evaluación de capacidades en ciberseguridad:



Este modelo permite **medir la evolución institucional** y establecer metas de fortalecimiento de ciberseguridad con criterios objetivos y verificables.

Marco de Referencia Internacional: NIST Cybersecurity Framework

El enfoque NIST permite **organizar y evaluar la ciberseguridad de manera integral**, articulando la gestión del riesgo con la operación técnica. Su utilidad para una evaluación de madurez radica en que facilita evidenciar:



En escenarios de plataformas web expuestas, interconexión con terceros, acceso remoto y operación continua, NIST ofrece una estructura clara para **traducir hallazgos técnicos en prioridades de control, asignación de responsabilidades y seguimiento con indicadores**, evitando que la seguridad se convierta en un conjunto de acciones reactivas sin continuidad.

Marco de Referencia Internacional: Principios ISO de Seguridad de la Información

El enfoque ISO, bajo la lógica de un **sistema de gestión de seguridad de la información**, complementa el componente operativo al institucionalizar la seguridad mediante políticas, roles, procesos, evidencia y medición. ISO aporta **sostenibilidad, trazabilidad y control formal**, permitiendo que la seguridad no dependa únicamente del esfuerzo de equipos técnicos o de herramientas puntuales, sino de una gestión repetible, auditable y mejorable.

Aporte del Enfoque ISO

- Institucionalización de la seguridad mediante políticas y roles formales
- Continuidad del control independiente de personas o herramientas
- Gobernanza fortalecida y trazabilidad de decisiones
- Soporte para procesos de verificación interna o externa
- Gestión repetible, auditable y mejorable

Complementariedad NIST + ISO

En conjunto, NIST e ISO permiten unir el enfoque de **"capacidad operativa"** con el de **"gobierno y sostenibilidad"**, fortaleciendo la madurez desde lo estratégico hasta lo técnico.

Esta aproximación facilita asegurar la continuidad del control, fortalecer la gobernanza y soportar procesos de verificación interna o externa.

Antecedentes de Evaluación y Hallazgos Relevantes

Durante el año anterior se ejecutó una evaluación de ciberseguridad que evidenció **vulnerabilidades relevantes en el ecosistema de aplicaciones web y exposición de credenciales** asociadas a componentes y procesos internos. Estos hallazgos incrementaban el riesgo de accesos no autorizados, abuso de privilegios y afectaciones a la continuidad de los servicios.

Vulnerabilidades en Aplicaciones Web

Fallas de control de acceso, validaciones insuficientes, exposición de configuraciones y manejo inadecuado de sesiones y secretos.

Exposición de Credenciales

Credenciales asociadas a componentes y procesos internos expuestas, incrementando el riesgo de accesos no autorizados y abuso de privilegios.

Configuraciones Inseguras

Superficies de exposición innecesarias y configuraciones que amplían la superficie de ataque disponible para actores maliciosos.

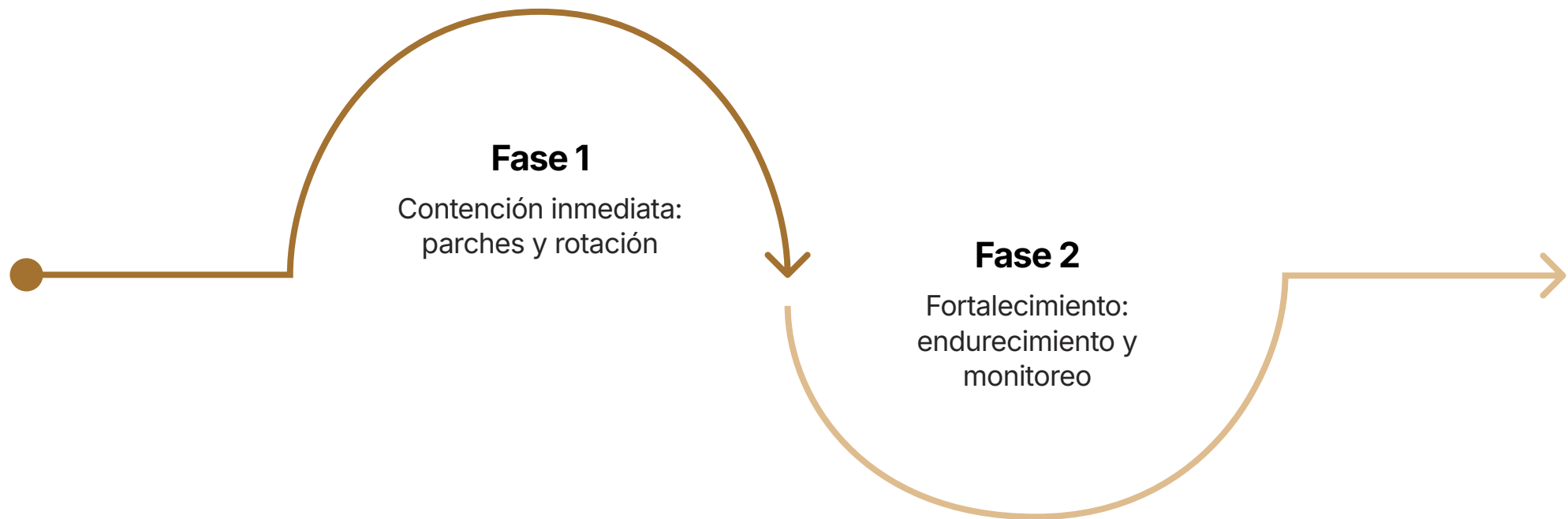
Controles con Efectividad Limitada

Controles preventivos y detectivos con efectividad limitada frente a vectores de ataque actuales, sin alertas oportunas ni bloqueos efectivos.

La evidencia indicó que el riesgo no se concentraba únicamente en infraestructura, sino también en **aspectos del ciclo de vida del desarrollo, configuraciones inseguras y superficies de exposición innecesarias**.

Acciones de Remediación Ejecutadas

A partir del diagnóstico anterior se implementaron **acciones de remediación y contención que solventaron una parte importante de las debilidades identificadas**, reduciendo riesgos inmediatos y fortaleciendo componentes priorizados.



Sin embargo, por la dinámica del entorno de amenazas y la evolución de las plataformas, el esfuerzo debe consolidarse como un **programa continuo de cierre de brechas y fortalecimiento institucional**. Las acciones puntuales de remediación, aunque necesarias, no son suficientes para garantizar una postura de seguridad sostenida frente a un panorama de amenazas en constante evolución.

- ❏ El aprendizaje del diagnóstico anterior, junto con las remediaciones ya ejecutadas, permite establecer una ruta clara para el presente año: fortalecer gobierno, elevar la efectividad de los controles existentes, robustecer la detección y la respuesta, e institucionalizar el desarrollo seguro con aseguramiento continuo.

Diagnóstico Actual: Estado de los Controles de Seguridad

El estado actual de los controles de seguridad de la Superintendencia de Transporte refleja una organización en **transición entre el nivel Básico y el nivel Intermedio** de madurez. Se identifican controles implementados en componentes clave, pero con oportunidades significativas de fortalecimiento en consistencia, efectividad y cobertura.

Área de Control	Estado Actual	Nivel de Madurez
Controles perimetrales (Fortinet)	Implementados, parametrización parcial	Nivel 2 - Básico
Gestión de identidades y accesos	Controles parciales, sin gestión centralizada	Nivel 2 - Básico
Monitoreo y detección	Capacidad limitada, alertas no sistemáticas	Nivel 1 - 2
Respuesta a incidentes	Procedimientos informales, sin playbooks	Nivel 1 - 2
Seguridad en desarrollo	Prácticas no formalizadas, sin SSDLC	Nivel 1
Gobernanza y gestión del riesgo	Políticas parciales, sin métricas formales	Nivel 2 – Básico

Diagnóstico Actual: Análisis del Entorno de Riesgo

Desde la perspectiva NIST, las vulnerabilidades y exposiciones evidenciadas el año anterior deben interpretarse como **indicadores directos de brechas en la capacidad institucional para gestionar el riesgo de forma consistente** y prevenir su materialización. En particular, cuando se identifican debilidades en aplicaciones web y exposición de credenciales, el riesgo deja de ser teórico y se convierte en un **escenario operativo con alta probabilidad de explotación**, especialmente en entornos donde los servicios son públicos o soportan procesos misionales.

Riesgo de Acceso No Autorizado

Alta probabilidad. Credenciales expuestas y controles de acceso insuficientes facilitan el acceso no autorizado a sistemas críticos.

Riesgo de Explotación Web

Alta probabilidad. Vulnerabilidades en aplicaciones web públicas con vectores de ataque conocidos y explotables.

Riesgo de Continuidad

Impacto alto. Afectaciones a la disponibilidad de servicios misionales con impacto directo en la operación institucional.

Riesgo de Reincidencia

Probabilidad media-alta. Sin prácticas de desarrollo seguro formalizadas, las vulnerabilidades tienden a reaparecer en nuevas versiones.

Consideraciones de Arquitectura y Controles Perimetrales

La arquitectura actual incorpora componentes de seguridad perimetral y de acceso remoto, incluyendo **firewall Fortinet y el uso de FortiClient**, lo cual constituye una base relevante dentro de la estrategia de protección. No obstante, la presencia de estos controles no garantiza una defensa efectiva si no existe una gobernanza adecuada, parametrización alineada a riesgos reales, monitoreo continuo e integración con capacidades de detección y respuesta.

Controles Existentes

- Firewall Fortinet como control perimetral principal
- FortiClient para acceso remoto seguro
- Segmentación básica de red
- Controles de acceso a nivel de infraestructura

Oportunidades de Fortalecimiento

- Reglas y endurecimiento de configuraciones
- Visibilidad y correlación de eventos
- Alertamiento oportuno y bloqueos efectivos
- Integración con capacidades de detección y respuesta
- Monitoreo continuo con señales accionables

Los hallazgos previos y la evidencia operativa reflejaron escenarios en los cuales, **pese a contar con estos controles, no se evidenciaron alertas oportunas ni bloqueos efectivos frente a ataques actuales**, lo que indica oportunidades de fortalecimiento en reglas, endurecimiento, visibilidad, correlación de eventos y capacidad de respuesta.

Seguridad en el Desarrollo y Aseguramiento Continuo

Adicionalmente, se identificaron **debilidades asociadas a errores lógicos y fallas propias del desarrollo**, lo que confirma la necesidad de incorporar seguridad desde el ciclo de vida de software. En plataformas web, el riesgo se materializa con frecuencia en:



Fallas de Control de Acceso

Ausencia de validaciones adecuadas que permiten acceso no autorizado a funcionalidades o datos sensibles.



Validaciones Insuficientes

Entradas de usuario no validadas que habilitan inyecciones, manipulación de parámetros y otros vectores de ataque.



Exposición de Configuraciones y Secretos

Credenciales, tokens y configuraciones sensibles expuestas en código fuente, repositorios o respuestas de la aplicación.



Manejo Inadecuado de Sesiones

Gestión deficiente de sesiones que facilita secuestro de sesión, escalada de privilegios y suplantación de identidad.

Por ello, el fortalecimiento institucional debe integrar **buenas prácticas de desarrollo seguro y mecanismos de aseguramiento continuo**, de manera que la seguridad sea verificable durante todo el ciclo y no únicamente posterior a la liberación.

Postura de Ciberseguridad: Perspectiva NIST

Bajo el enfoque NIST, la postura esperada no es limitarse a la corrección puntual de hallazgos, sino **fortalecer la capacidad de identificar de manera continua activos críticos y superficies de exposición**, elevar la efectividad de los controles de protección, y consolidar mecanismos de detección y respuesta que permitan visibilidad real, alertamiento oportuno y contención.

La ausencia de señales claras de bloqueo o alertas efectivas frente a ataques actuales, aun contando con controles perimetrales, **refuerza la necesidad de mejorar la madurez operativa** para que la seguridad sea medible y demostrable, y no únicamente declarativa.

1

Identificación Continua

Fortalecer la capacidad de identificar de manera continua activos críticos y superficies de exposición.

2

Protección Efectiva

Elevar la efectividad de los controles de protección con parametrización alineada a riesgos reales.

3

Detección Oportuna

Consolidar mecanismos de detección que permitan visibilidad real y alertamiento oportuno.

4

Respuesta y Contención

Desarrollar capacidades de respuesta y contención ante incidentes con procedimientos formalizados.

Postura de Ciberseguridad: Perspectiva ISO

De acuerdo con la lógica ISO, la criticidad de los hallazgos refleja la necesidad de **robustecer la gobernanza y la institucionalización de la seguridad**, asegurando que la gestión de riesgos, los controles, la operación y la mejora continua estén formalmente establecidos, ejecutados y documentados con evidencia verificable.

La presencia de vulnerabilidades recurrentes o fallas lógicas en el desarrollo señala oportunidades de fortalecimiento en **políticas, procedimientos, responsabilidades y aseguramiento del ciclo de vida del software**, de manera que los controles no dependan de esfuerzos aislados, sino de un sistema de gestión estable que garantice consistencia, repetibilidad y seguimiento.

Gobernanza Formal

Consolidar lineamientos firmes que obliguen a prácticas de desarrollo seguro, control de cambios con enfoque de riesgo y gestión adecuada de credenciales.

Sistema de Gestión Estable

Establecer un sistema de gestión que garantice consistencia, repetibilidad y seguimiento, independiente de esfuerzos aislados.

Verificación Continua

Implementar mecanismos de verificación continua que eleven la capacidad institucional para sostener mejoras y evitar reincidencias.

Postura Integrada NIST + ISO: Imperativo Estratégico

En consecuencia, y considerando la criticidad evidenciada, la postura alineada a NIST e ISO **exige fortalecer la madurez de forma prioritaria**, enfocándose en mejorar la efectividad real de los controles tecnológicos, incrementar visibilidad y capacidad de detección ante amenazas actuales, y consolidar una gobernanza que garantice que la seguridad sea parte estructural del negocio digital.

Esto implica asumir que el cierre de brechas no es un evento, sino un proceso continuo, con control, medición y evidencia, orientado a reducir el riesgo sobre los servicios críticos de la Superintendencia y asegurar la continuidad y confianza en sus plataformas.

Efectividad Real de Controles	Visibilidad y Detección	Gobernanza Estructural
Mejorar la efectividad real de los controles tecnológicos más allá de su mera implementación.	Incrementar visibilidad y capacidad de detección ante amenazas actuales con señales accionables.	Consolidar una gobernanza que garantice que la seguridad sea parte estructural del negocio digital.

Dominios de Evaluación de Madurez

La evaluación de madurez considera **dominios alineados con buenas prácticas internacionales de ciberseguridad**. El análisis de estos dominios permite obtener una visión integral del ecosistema de seguridad institucional.



Cada dominio es evaluado de forma independiente para determinar su nivel de madurez actual, identificar brechas específicas y establecer acciones de mejora priorizadas con criterios claros y auditables.

Dominio 1: Gobernanza y Gestión del Riesgo

La gobernanza de ciberseguridad constituye el **fundamento sobre el cual se sostiene toda la estrategia de protección institucional**. Sin una gobernanza sólida, los controles técnicos carecen de dirección, los recursos se asignan sin criterio de riesgo y la mejora continua no es posible.

Estado Actual

Controles parciales o en fortalecimiento. Políticas de seguridad en desarrollo, sin métricas formales de gestión del riesgo. Responsabilidades de ciberseguridad no completamente formalizadas.

Nivel Objetivo: Intermedio / Avanzado

- Política de seguridad de la información aprobada y comunicada
- Comité de seguridad activo con reuniones periódicas
- Metodología formal de gestión del riesgo tecnológico
- Indicadores de riesgo (KRIs) definidos y monitoreados
- Auditorías internas de ciberseguridad programadas

Acción recomendada: Implementar controles y monitoreo continuo. Formalizar la estructura de gobernanza de ciberseguridad con roles, responsabilidades, políticas aprobadas y un proceso de gestión del riesgo basado en evidencia.

Dominio 2: Gestión de Activos Críticos

La gestión efectiva de activos es un **prerrequisito fundamental para cualquier programa de ciberseguridad**. No es posible proteger lo que no se conoce. La identificación, clasificación y gestión del ciclo de vida de los activos tecnológicos permite priorizar controles y reducir la superficie de exposición.

Inventario de Activos

Establecer y mantener un inventario actualizado de activos tecnológicos críticos, incluyendo hardware, software, datos y servicios en la nube.

Clasificación por Criticidad

Clasificar los activos según su criticidad para los procesos misionales, estableciendo niveles de protección diferenciados.

Gestión del Ciclo de Vida

Implementar procesos formales para la incorporación, modificación y retiro de activos tecnológicos con criterios de seguridad.

Dominio	Nivel Actual	Nivel Objetivo
Gestión de activos	Por evaluar	Intermedio / Avanzado

Acción recomendada: Implementar controles y monitoreo continuo. Desarrollar un inventario de activos críticos con clasificación por criticidad y propietario asignado.

Dominio 3: Gestión de Identidades y Accesos

La gestión de identidades y accesos es uno de los **dominios con mayor impacto directo en la reducción del riesgo**. Los hallazgos previos evidenciaron exposición de credenciales y controles de acceso insuficientes, lo que incrementa significativamente el riesgo de accesos no autorizados y abuso de privilegios.



Autenticación Robusta

Implementar autenticación multifactor (MFA) para todos los accesos a sistemas críticos, especialmente acceso remoto y administración de plataformas.



Gestión de Credenciales

Implementar políticas formales de gestión de credenciales, rotación periódica y eliminación de cuentas inactivas o de servicio con privilegios excesivos.



Principio de Mínimo Privilegio

Revisar y ajustar los privilegios de acceso aplicando el principio de mínimo privilegio necesario para cada rol y función.



Revisión Periódica de Accesos

Establecer procesos de revisión periódica de accesos para detectar y corregir desviaciones respecto a los perfiles autorizados.

Dominio 4: Protección de Infraestructura Tecnológica

La protección de la infraestructura tecnológica abarca los controles técnicos aplicados sobre redes, servidores, endpoints y servicios que soportan la operación de la Superintendencia. Una **arquitectura de seguridad madura debe traducirse en prevención efectiva, señales accionables, contención y capacidad de análisis**, más allá de la implementación de componentes.



Endurecimiento de Controles Perimetrales

Revisar y optimizar las reglas del firewall Fortinet, eliminando reglas permisivas innecesarias y alineando la configuración a los riesgos reales identificados.



Segmentación de Red

Implementar segmentación de red efectiva que limite el movimiento lateral en caso de compromiso, protegiendo los activos más críticos.



Gestión de Vulnerabilidades

Establecer un proceso formal de gestión de vulnerabilidades con escaneo periódico, priorización por criticidad y seguimiento de remediación.

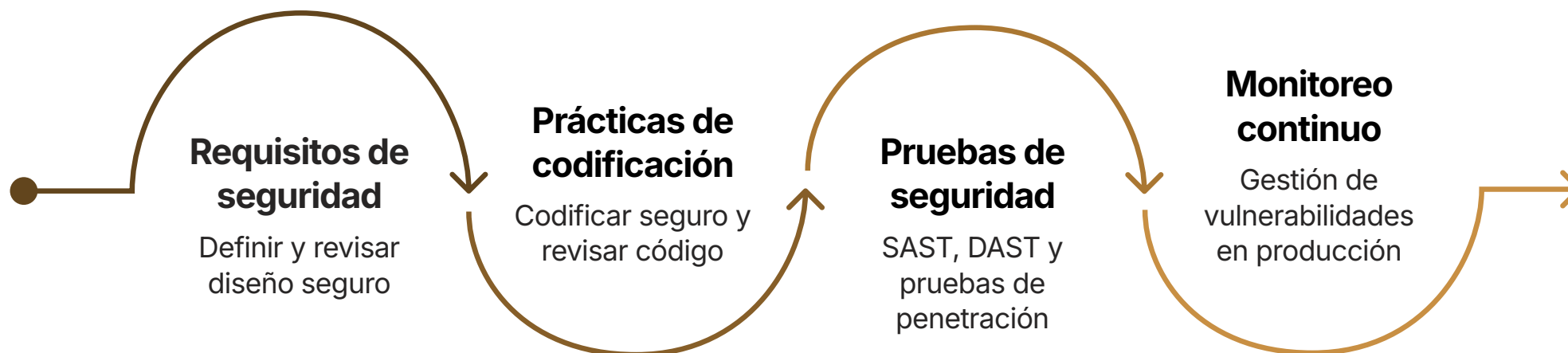


Protección de Endpoints

Fortalecer la protección de endpoints con controles de detección y respuesta (EDR) integrados con capacidades de correlación de eventos.

Dominio 5: Seguridad en el Desarrollo de Software

En este marco, el **escaneo continuo** y las **validaciones sistemáticas sobre las plataformas** deben convertirse en una **disciplina permanente** para prevenir reincidencias, detectar tempranamente debilidades y sostener el cierre progresivo de brechas.



El fortalecimiento institucional debe integrar buenas prácticas de desarrollo seguro y mecanismos de aseguramiento continuo, de manera que la seguridad sea **verificable durante todo el ciclo y no únicamente posterior a la liberación**. Esto incluye la adopción de un Ciclo de Vida de Desarrollo Seguro (SSDLC), la incorporación de pruebas de seguridad automatizadas y la formación continua de los equipos de desarrollo.

Dominio 6: Monitoreo y Detección de Amenazas

El monitoreo y la detección de amenazas constituyen la **capacidad de visibilidad operativa** de la organización frente al panorama de amenazas. Los hallazgos previos evidenciaron que, pese a contar con controles perimetrales, no se generaron alertas oportunas ni bloqueos efectivos frente a ataques actuales, lo que indica una brecha significativa en esta capacidad.

Correlación de Eventos (SIEM)

Implementar o fortalecer una plataforma de correlación de eventos de seguridad (SIEM) que centralice logs y genere alertas basadas en reglas de detección actualizadas.

Monitoreo Continuo 24/7

Establecer capacidades de monitoreo continuo con cobertura de los activos críticos, incluyendo plataformas web, infraestructura y accesos remotos.

Inteligencia de Amenazas

Incorporar fuentes de inteligencia de amenazas (Threat Intelligence) para enriquecer la detección con indicadores de compromiso actualizados.

Análisis de Comportamiento

Implementar capacidades de análisis de comportamiento de usuarios y entidades (UEBA) para detectar anomalías que evadan controles tradicionales.

Dominio 7: Respuesta ante Incidentes

La capacidad de respuesta ante incidentes determina la **velocidad y efectividad con la que la organización puede contener, erradicar y recuperarse de un ataque cibernético**. Una respuesta tardía o desorganizada amplifica significativamente el impacto de cualquier incidente de seguridad.

01	02
Preparación	Identificación y Clasificación
Desarrollar y mantener un Plan de Respuesta a Incidentes (IRP) con roles, responsabilidades, procedimientos y playbooks para los escenarios de mayor riesgo.	Establecer criterios claros para la identificación, clasificación y escalamiento de incidentes de seguridad según su severidad e impacto.
03	04
Contención y Erradicación	Recuperación y Lecciones Aprendidas
Definir procedimientos de contención inmediata y erradicación de amenazas con criterios de decisión claros y autoridades definidas.	Establecer procesos de recuperación ordenada y documentación de lecciones aprendidas para mejorar continuamente la capacidad de respuesta.

Acción recomendada: Implementar controles y monitoreo continuo. Formalizar el proceso de gestión de incidentes con un equipo de respuesta designado, procedimientos documentados y ejercicios de simulación periódicos.

Dominio 8: Continuidad y Recuperación de Servicios

La continuidad y recuperación de servicios garantiza que la Superintendencia de Transporte pueda **mantener o restablecer sus operaciones críticas ante cualquier evento disruptivo**, incluyendo incidentes de ciberseguridad, fallas tecnológicas o desastres. Este dominio es especialmente crítico dado el rol misional de la entidad.

Estado Actual

Controles parciales o en fortalecimiento. Planes de continuidad no completamente formalizados. Capacidades de recuperación ante desastres (DR) sin pruebas periódicas documentadas.

Acciones Recomendadas

- Desarrollar y mantener un Plan de Continuidad del Negocio (BCP)
- Implementar un Plan de Recuperación ante Desastres (DRP) con RTO y RPO definidos
- Establecer respaldos periódicos con pruebas de restauración documentadas
- Realizar ejercicios de continuidad al menos una vez al año
- Integrar la continuidad con el proceso de gestión de incidentes

Modelo de Madurez de Ciberseguridad: Tabla de Referencia

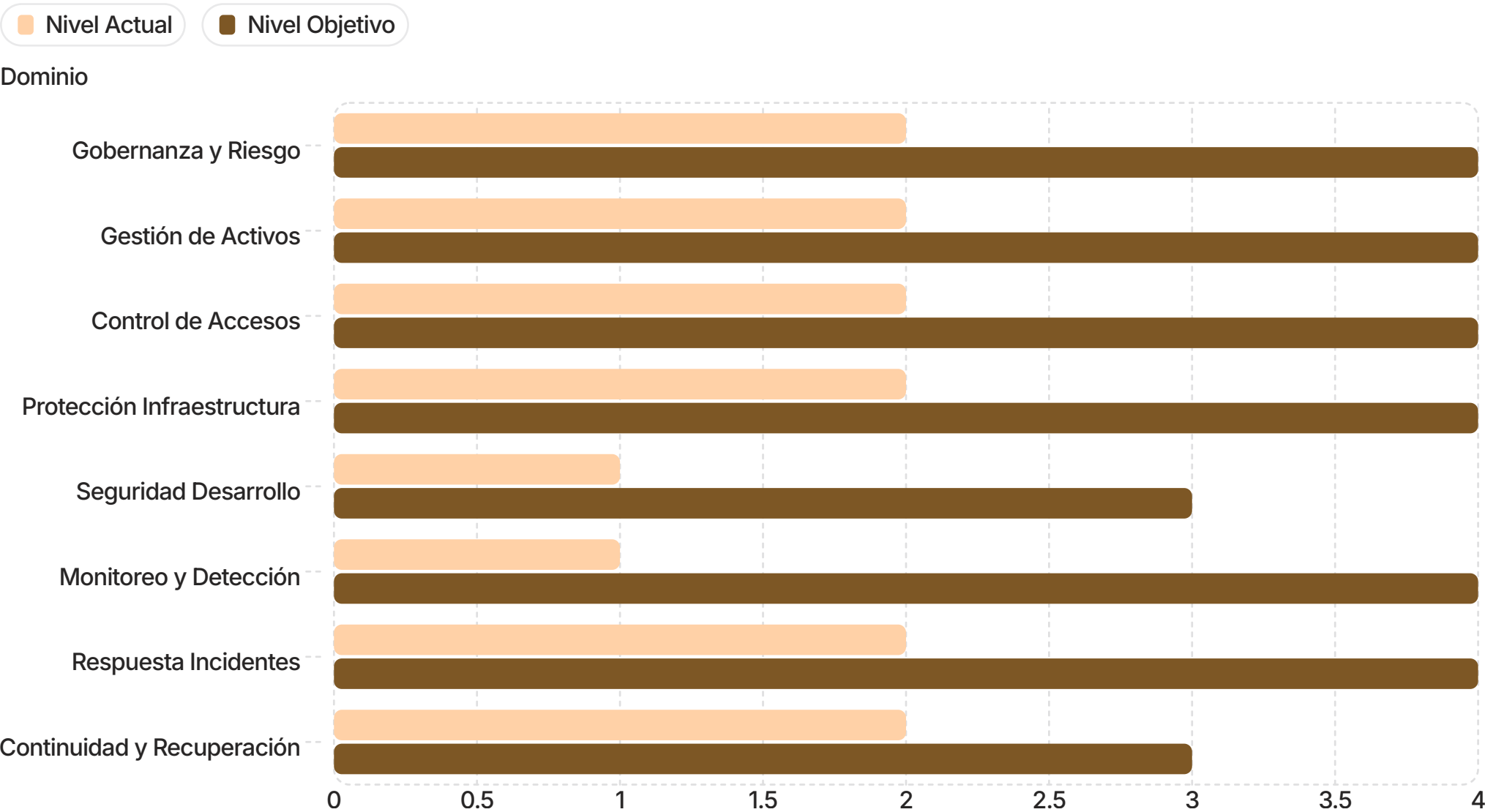
El modelo de madurez utilizado contempla cinco niveles progresivos que permiten medir la evolución institucional y establecer metas de fortalecimiento de ciberseguridad.

Nivel	Denominación	Características	Indicadores Clave
1	Inicial	Controles ad hoc, procesos informales y dependientes de acciones reactivas. Sin documentación formal.	Sin políticas, sin inventario, respuesta reactiva
2	Básico /Repetible	Existencia de controles mínimos y algunas prácticas definidas. Procesos repetibles pero no estandarizados.	Controles básicos implementados, algunas políticas
3	Intermedio / Definido	Procesos documentados y controles aplicados de forma consistente. Gestión formal del riesgo iniciada.	Políticas aprobadas, controles consistentes, métricas básicas
4	Avanzado / Gestionado	Gestión estructurada con monitoreo continuo y métricas de seguridad. Mejora basada en datos.	KPIs/KRIs activos, monitoreo continuo, auditorías regulares
5	Optimizado	Mejora continua basada en indicadores, automatización y gestión integral del riesgo. Cultura de seguridad consolidada.	Automatización, inteligencia de amenazas, mejora continua

Nivel actual estimado de la organización: Nivel 2 – Básico / Repetible, en transición hacia el Nivel 3 – Intermedio / Definido, con brechas significativas en monitoreo, detección y desarrollo seguro.

Visualización del Nivel de Madurez: Gráfica Comparativa por Dominio

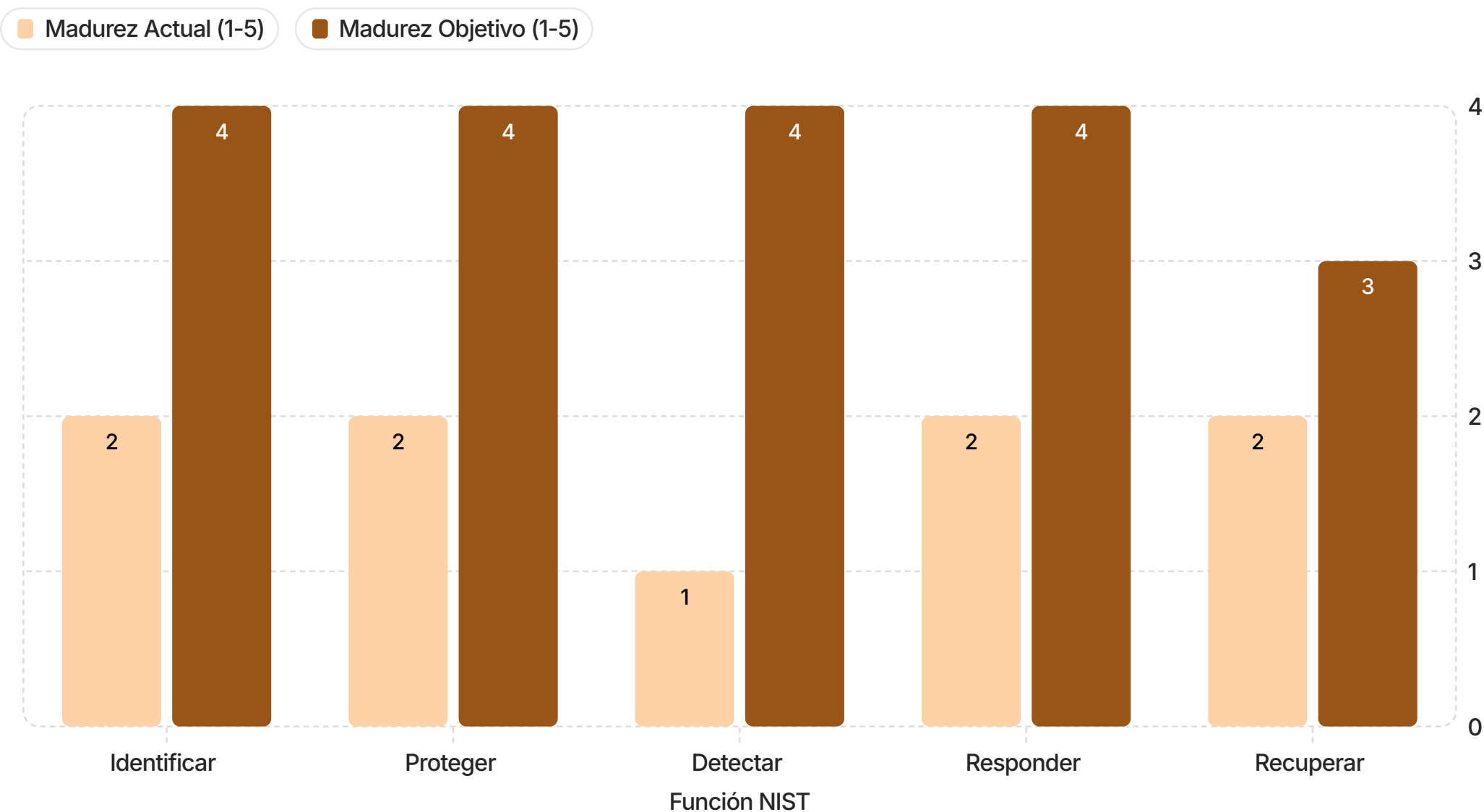
La siguiente gráfica ilustra de forma referencial el nivel de madurez institucional en los dominios evaluados. Esta visualización permite identificar de manera rápida las áreas que requieren mayor fortalecimiento.



La brecha más significativa se observa en los dominios de **Monitoreo y Detección** y **Seguridad en el Desarrollo de Software**, donde el nivel actual es el más bajo y el nivel objetivo requiere un salto de madurez considerable. Estos dominios deben ser priorizados en el plan de acción.

Radar de Madurez de Ciberseguridad (NIST Framework)

El siguiente gráfico muestra el nivel de madurez en los dominios clave de ciberseguridad, permitiendo una visualización rápida de las fortalezas y brechas institucionales.



Source:

El análisis por funciones NIST revela que la función **Detectar** presenta la brecha más crítica, con un nivel actual de 1 frente a un objetivo de 4. Las funciones de **Identificar, Proteger, Responder y Recuperar** se encuentran en nivel 2, requiriendo fortalecimiento sistemático para alcanzar los niveles objetivo.

Mapa de Brechas de Ciberseguridad

El siguiente cuadro permite identificar de forma estructurada las brechas existentes entre el estado actual y el nivel de madurez esperado, facilitando la priorización de acciones de mejora.

Dominio	Situación Actual	Acción Recomendada
Gobernanza y gestión del riesgo	Controles parciales o en fortalecimiento	Implementar controles y monitoreo continuo
Gestión de activos	Controles parciales o en fortalecimiento	Implementar controles y monitoreo continuo
Control de accesos e identidades	Controles parciales o en fortalecimiento	Implementar controles y monitoreo continuo
Protección de infraestructura	Controles parciales o en fortalecimiento	Implementar controles y monitoreo continuo
Seguridad en el desarrollo de software	Controles parciales o en fortalecimiento	Implementar controles y monitoreo continuo
Monitoreo y detección	Controles parciales o en fortalecimiento	Implementar controles y monitoreo continuo
Respuesta a incidentes	Controles parciales o en fortalecimiento	Implementar controles y monitoreo continuo
Continuidad y recuperación	Controles parciales o en fortalecimiento	Implementar controles y monitoreo continuo

Análisis de Brechas: Priorización Estratégica

A partir del mapa de brechas identificado, se establece una priorización estratégica de las acciones de mejora considerando el **impacto en la reducción del riesgo, la viabilidad de implementación y la urgencia operativa**.

Prioridad Crítica

Monitoreo y detección de amenazas. Seguridad en el desarrollo de software. Gestión de credenciales y accesos privilegiados.

Prioridad Alta

Gobernanza y gestión del riesgo. Control de accesos e identidades. Respuesta ante incidentes con playbooks formalizados.

Prioridad Media

Protección de infraestructura (endurecimiento). Gestión de activos críticos con inventario actualizado.

Prioridad Estándar

Continuidad y recuperación de servicios. Formalización de políticas y procedimientos de seguridad.

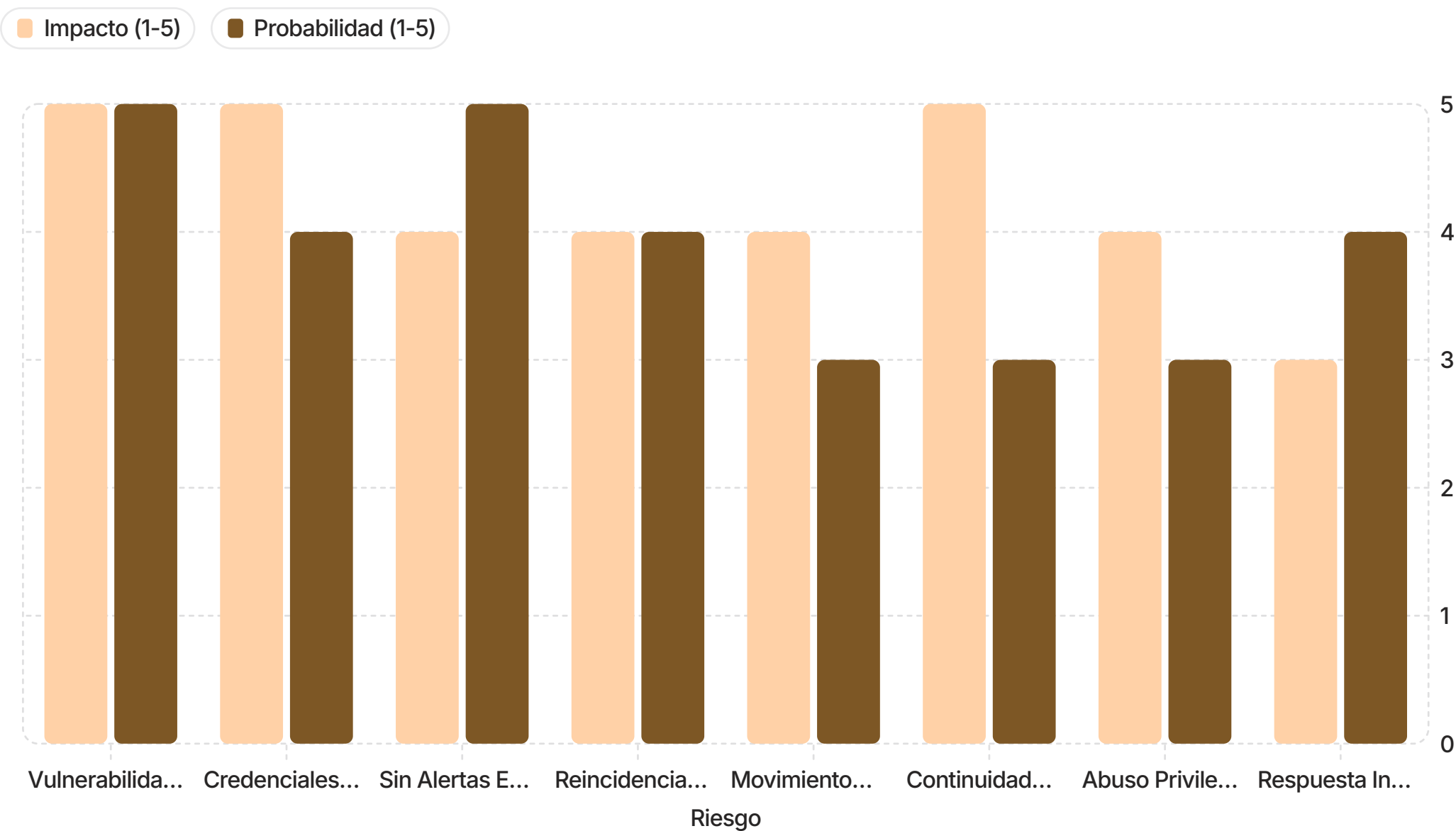
Matriz de Riesgos de Ciberseguridad

La siguiente matriz clasifica los principales riesgos de ciberseguridad identificados según su **impacto y probabilidad**, siguiendo una metodología similar a ISO 27005, permitiendo identificar los riesgos críticos que requieren atención prioritaria.

Riesgo Identificado	Impacto	Probabilidad	Nivel de Criticidad
Explotación de vulnerabilidades en aplicaciones web	Alto	Alta	 Crítico
Acceso no autorizado por credenciales expuestas	Alto	Alta	 Crítico
Ausencia de alertas efectivas ante ataques activos	Alto	Alta	 Crítico
Reincidencia de vulnerabilidades por falta de SSDLC	Alto	Media	 Alto
Movimiento lateral por segmentación insuficiente	Alto	Media	 Alto
Afectación a continuidad de servicios misionales	Muy Alto	Media	 Alto
Abuso de privilegios por controles de acceso débiles	Alto	Media	 Alto
Falta de respuesta organizada ante incidentes	Medio	Alta	 Alto

Visualización de la Matriz de Riesgos

La siguiente gráfica muestra la distribución de los riesgos identificados según su nivel de criticidad, facilitando la comprensión del panorama de riesgo institucional.



Los riesgos con mayor combinación de impacto y probabilidad son la **explotación de vulnerabilidades web, la exposición de credenciales y la ausencia de alertas efectivas**. Estos tres riesgos deben ser abordados con carácter de urgencia en el plan de acción inmediato.

Roadmap Estratégico de Fortalecimiento: Corto Plazo (0–3 Meses)

El roadmap estratégico de fortalecimiento de ciberseguridad a 12 meses se estructura en tres horizontes temporales. Las acciones de **corto plazo (0–3 meses)** se enfocan en la reducción inmediata del riesgo crítico identificado.

1 Remediación de Vulnerabilidades Críticas Ejecutar escaneo completo de vulnerabilidades en plataformas web y aplicar parches y correcciones a las vulnerabilidades críticas y altas identificadas.	2 Rotación y Gestión de Credenciales Rotar todas las credenciales comprometidas o expuestas, implementar políticas de contraseñas robustas y habilitar MFA en accesos críticos.
3 Endurecimiento de Controles Perimetrales Revisar y optimizar las reglas del firewall Fortinet, eliminar reglas permisivas innecesarias y configurar alertas básicas de seguridad.	4 Formalización de Gobernanza Básica Designar formalmente el responsable de ciberseguridad, establecer el comité de seguridad y aprobar la política de seguridad de la información.

Roadmap Estratégico: Mediano Plazo (3-6 Meses)

Las acciones de **mediano plazo (3 - 6 meses)** se enfocan en la consolidación de capacidades de detección, respuesta y desarrollo seguro, elevando el nivel de madurez de manera sostenida.

1

Implementación de Capacidades de Monitoreo

Desplegar o fortalecer la plataforma SIEM, configurar reglas de detección para los vectores de ataque más relevantes y establecer procedimientos de respuesta a alertas.

2

Plan de Respuesta a Incidentes

Desarrollar el Plan de Respuesta a Incidentes (IRP) con playbooks para los escenarios de mayor riesgo, designar el equipo de respuesta y realizar el primer ejercicio de simulación.

3

Incorporación de Seguridad en el Desarrollo

Implementar las primeras prácticas de SSDLC, incluyendo revisión de código con enfoque de seguridad, pruebas SAST/DAST y capacitación del equipo de desarrollo.

4

Inventario y Clasificación de Activos

Completar el inventario de activos tecnológicos críticos con clasificación por criticidad, propietario asignado y nivel de protección requerido.

Roadmap Estratégico: Largo Plazo (6-12 Meses)

Las acciones de **largo plazo (6-12 meses)** se enfocan en la consolidación de la madurez institucional, la institucionalización de la mejora continua y el fortalecimiento de la gobernanza de ciberseguridad.

1

Programa de Gestión del Riesgo Tecnológico

Implementar una metodología formal de gestión del riesgo tecnológico con evaluaciones periódicas, registro de riesgos actualizado y seguimiento de controles.

2

Continuidad y Recuperación Formalizada

Desarrollar y probar el Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP) con RTO y RPO definidos para los servicios críticos.

3

Programa de Aseguramiento Continuo

Establecer un programa de escaneo continuo, pruebas de penetración periódicas y revisiones de seguridad sistemáticas sobre todas las plataformas.

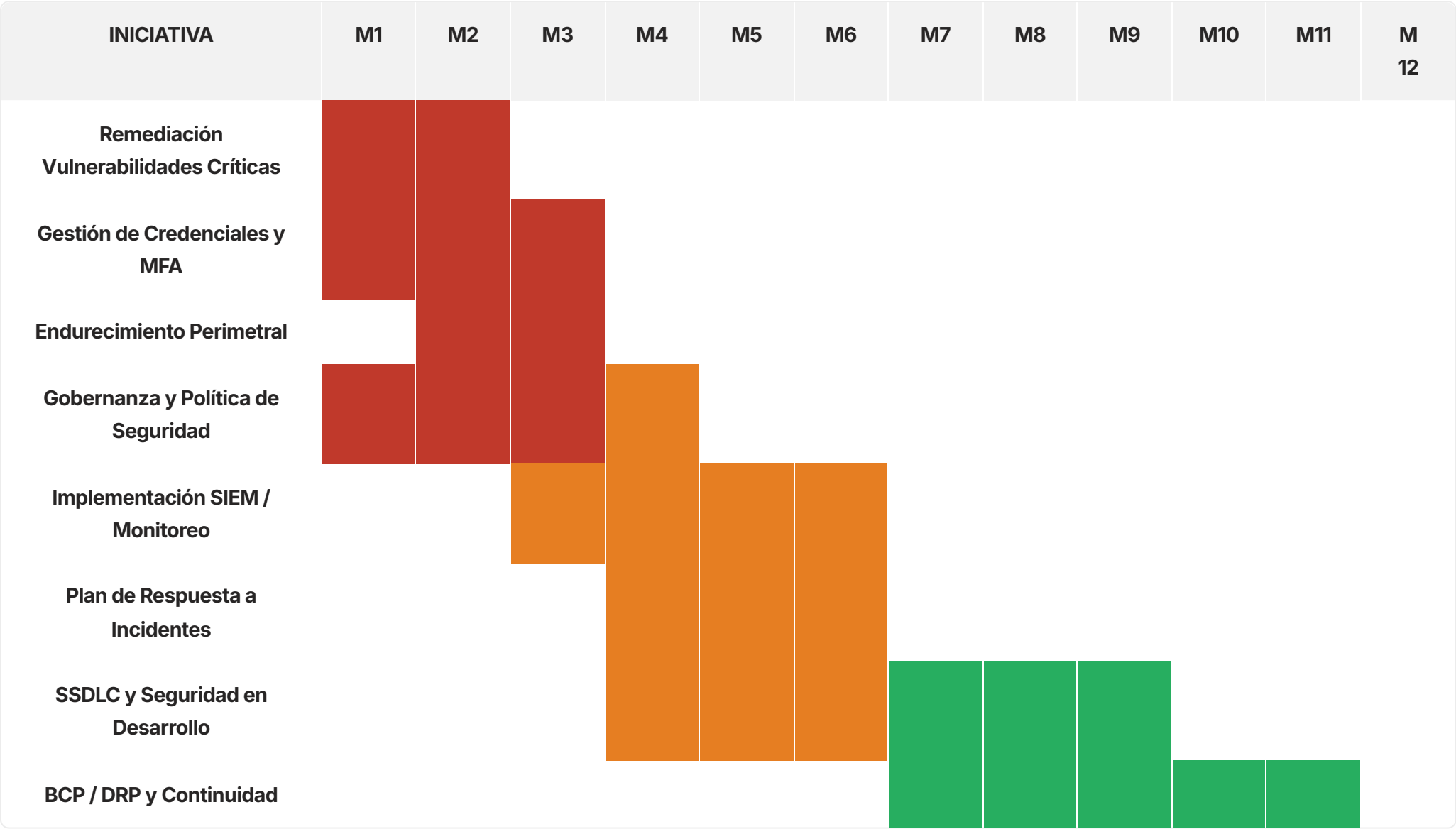
4

Cultura de Ciberseguridad

Implementar un programa de concienciación y formación en ciberseguridad para todos los funcionarios, con énfasis en los equipos técnicos y directivos.

Visualización del Roadmap a 12 Meses

El siguiente diagrama presenta de forma visual el roadmap estratégico de fortalecimiento de ciberseguridad, organizado por horizontes temporales y áreas de acción prioritaria.



● Corto Plazo (0–3 meses) | ● Mediano Plazo (3–6 meses) | ● Largo Plazo (6–12 meses)

El roadmap prioriza las acciones de mayor impacto en la reducción del riesgo durante los primeros tres meses, seguidas de la consolidación de capacidades de detección y respuesta en el mediano plazo, y la institucionalización de la mejora continua en el largo plazo.

Indicadores de Desempeño de Ciberseguridad: KPIs

Los **Indicadores Clave de Desempeño (KPIs)** permiten medir la efectividad de los controles de ciberseguridad y el avance en el cierre de brechas. Estos indicadores deben ser monitoreados de forma periódica y reportados a la dirección.

<30d	100%	<4h	95%
Tiempo de Remediación	Cobertura MFA	Tiempo de Detección	Parches Aplicados
Tiempo promedio para remediar vulnerabilidades críticas desde su identificación hasta su cierre.	Porcentaje de accesos a sistemas críticos protegidos con autenticación multifactor.	Tiempo promedio de detección de incidentes de seguridad desde su ocurrencia.	Porcentaje de vulnerabilidades críticas y altas con parche aplicado dentro del plazo establecido.

KPI	Meta	Frecuencia de Medición
Vulnerabilidades críticas abiertas	0 por más de 30 días	Semanal
Cobertura de monitoreo de activos críticos	100%	Mensual
Incidentes resueltos dentro del SLA	>90%	Mensual
Pruebas de seguridad en desarrollo	100% de releases	Por release
Ejercicios de continuidad realizados	Mínimo 1 por año	Anual

Indicadores de Riesgo de Ciberseguridad: KRIs

Los **Indicadores Clave de Riesgo (KRIs)** permiten anticipar el deterioro de la postura de seguridad y activar acciones preventivas antes de que los riesgos se materialicen. Son el complemento estratégico de los KPIs.

KRI 1: Vulnerabilidades Críticas Sin Remediar

Número de vulnerabilidades críticas identificadas con más de 30 días sin remediación. Umbral de alerta: >3 vulnerabilidades críticas abiertas.

KRI 2: Intentos de Acceso No Autorizado

Número de intentos de acceso no autorizado detectados por semana. Umbral de alerta: incremento >50% respecto a la línea base.

KRI 3: Incidentes de Seguridad Recurrentes

Número de incidentes de seguridad con causa raíz similar en los últimos 90 días. Umbral de alerta: >2 incidentes con causa raíz idéntica.

KRI 4: Cobertura de Monitoreo

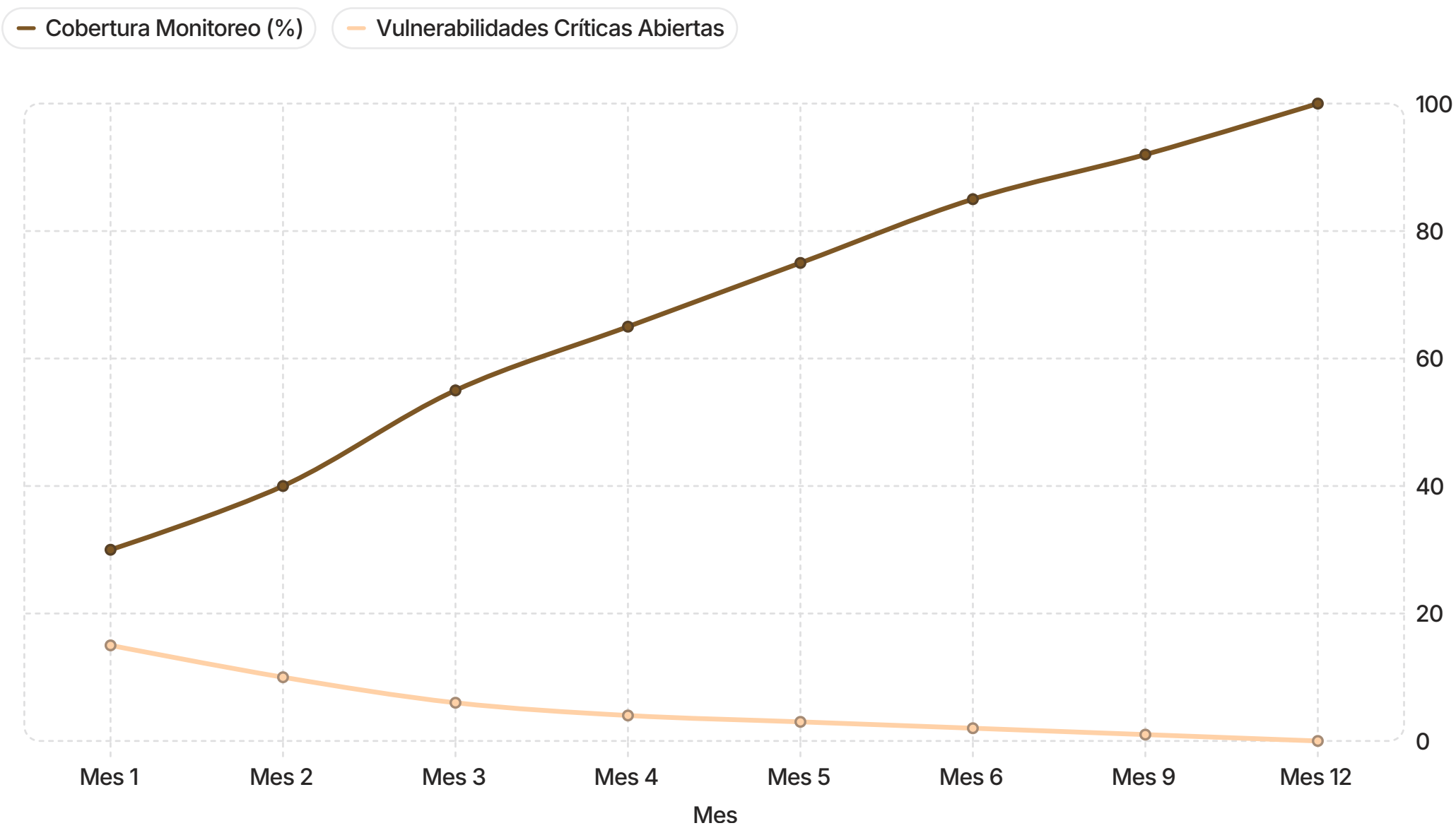
Porcentaje de activos críticos sin cobertura de monitoreo activo. Umbral de alerta: >10% de activos críticos sin monitoreo.

KRI 5: Tiempo de Detección de Incidentes

Tiempo promedio de detección de incidentes de seguridad. Umbral de alerta: tiempo de detección >24 horas para incidentes críticos.

Evolución de KPIs: Tendencia de Mejora Esperada

La siguiente gráfica muestra la evolución esperada de los principales KPIs de ciberseguridad a lo largo del año, como resultado de la implementación del roadmap estratégico.



La tendencia esperada muestra una **reducción progresiva de vulnerabilidades críticas abiertas** hasta alcanzar cero al final del año, acompañada de un incremento sostenido en la cobertura de monitoreo hasta alcanzar el 100% de los activos críticos.

Interpretación de Resultados y Línea Base de Madurez

Los resultados de la evaluación deben interpretarse como una **línea base de madurez que permite orientar el fortalecimiento institucional** en materia de ciberseguridad. El propósito del diagnóstico no es únicamente identificar debilidades, sino establecer una hoja de ruta clara para mejorar la postura de seguridad, reducir la exposición al riesgo y fortalecer la resiliencia de las plataformas tecnológicas.

La mejora de la madurez en ciberseguridad debe entenderse como un proceso continuo que integra gobernanza, tecnología, procesos y cultura organizacional.

Línea Base Establecida

Nivel 2 – Básico / Repetible como punto de partida para el programa de mejora continua.

Meta a 12 Meses

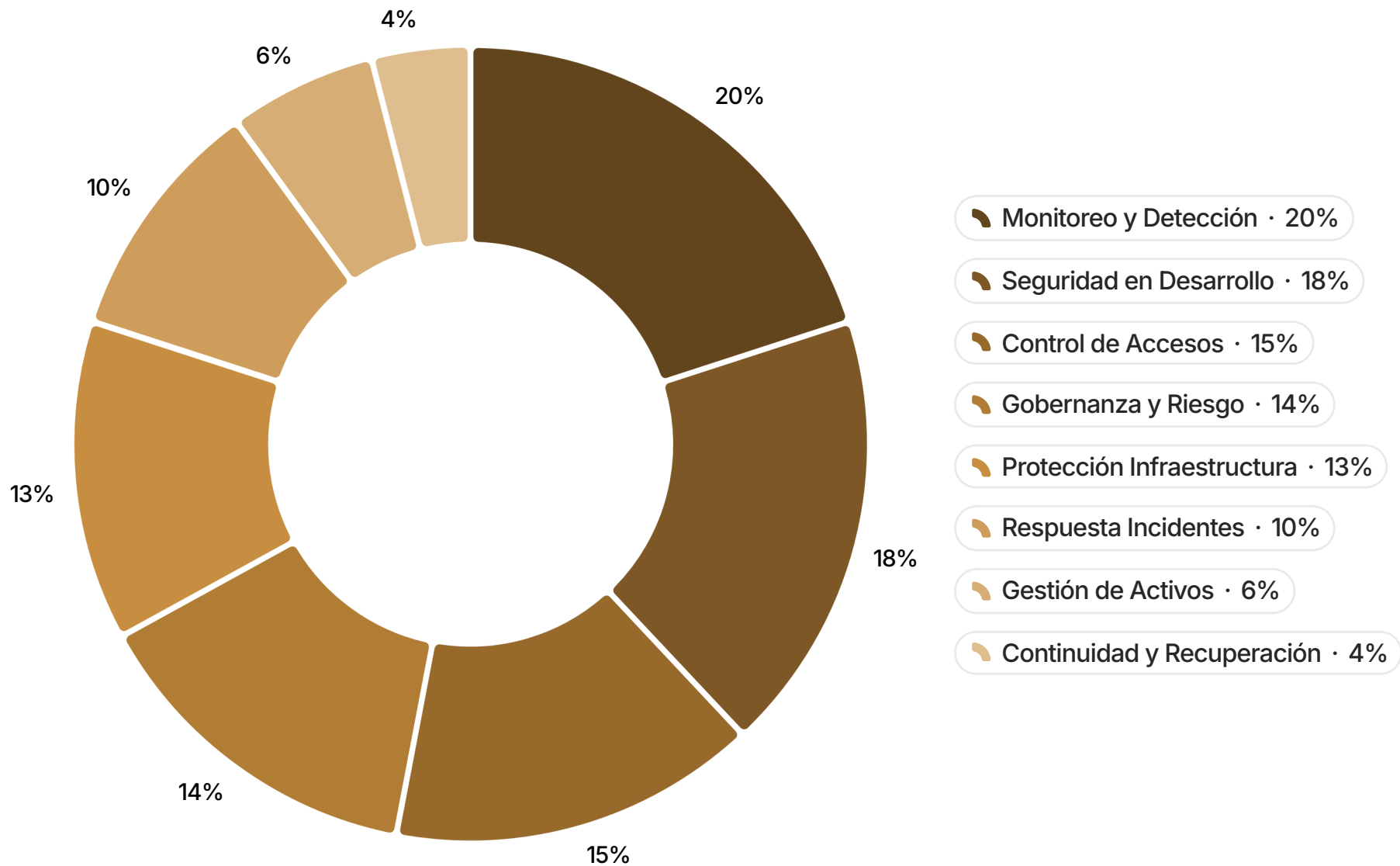
Alcanzar Nivel 3 – Intermedio / Definido en todos los dominios, con avances hacia Nivel 4 en los dominios críticos.

Visión a 3 Años

Consolidar Nivel 4 – Avanzado / Gestionado como estándar institucional, con capacidades de mejora continua establecidas.

Análisis de Distribución del Riesgo por Dominio

La siguiente gráfica muestra la distribución del nivel de riesgo residual por dominio de ciberseguridad, considerando los controles actuales y las brechas identificadas.



Los dominios de **Monitoreo y Detección (20%)** y **Seguridad en el Desarrollo (18%)** concentran el mayor nivel de riesgo residual, confirmando la necesidad de priorizarlos en el plan de acción inmediato.

Recomendaciones Estratégicas: Gobernanza y Gestión del Riesgo

Para fortalecer la gobernanza y la gestión del riesgo de ciberseguridad, se recomienda implementar las siguientes acciones con carácter prioritario:

1 Formalizar la Estructura de Gobernanza

Designar formalmente un Responsable de Seguridad de la Información (CISO o equivalente), establecer el Comité de Seguridad con participación directiva y definir roles y responsabilidades claras.

2 Aprobar la Política de Seguridad de la Información

Desarrollar y aprobar una Política de Seguridad de la Información alineada con ISO 27001, comunicarla a todos los funcionarios y establecer mecanismos de cumplimiento.

3 Implementar Metodología de Gestión del Riesgo

Adoptar una metodología formal de gestión del riesgo tecnológico (ISO 27005 o similar), con evaluaciones periódicas, registro de riesgos y seguimiento de controles con indicadores.

Recomendaciones Estratégicas: Controles Técnicos Prioritarios

Las siguientes recomendaciones técnicas abordan las brechas de mayor criticidad identificadas en el diagnóstico, con enfoque en la reducción inmediata del riesgo operativo:

Autenticación Multifactor (MFA)

Implementar MFA de forma obligatoria para todos los accesos a sistemas críticos, especialmente acceso remoto vía FortiClient, consolas de administración y plataformas web con datos sensibles.

Gestión Centralizada de Identidades

Implementar una solución de gestión centralizada de identidades y accesos (IAM/PAM) que permita control granular, auditoría de accesos y detección de anomalías.

Correlación de Eventos de Seguridad

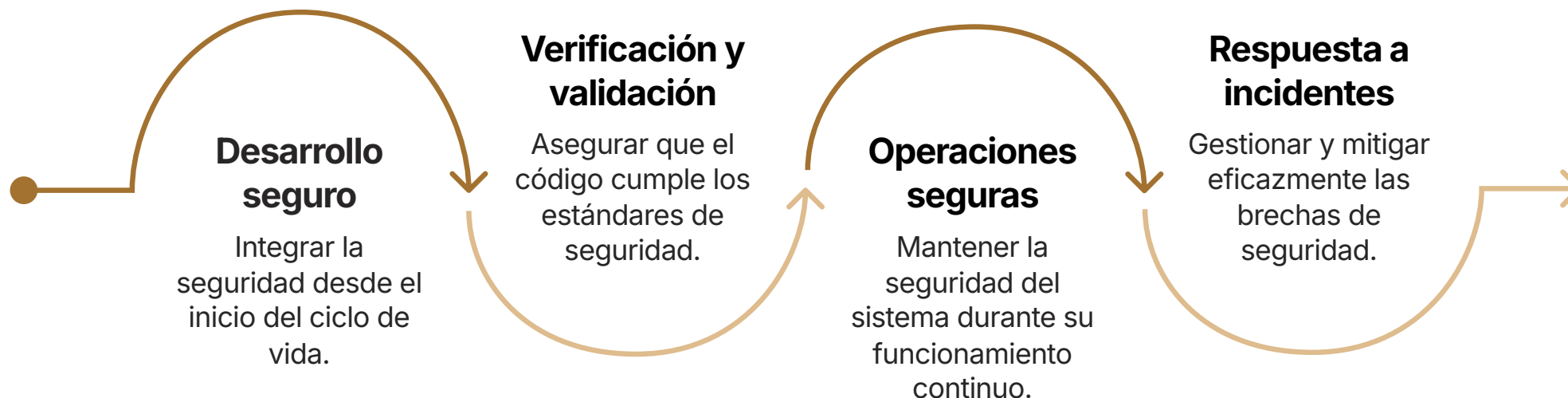
Desplegar o fortalecer la plataforma SIEM con reglas de detección actualizadas, integración de fuentes de log críticas y procedimientos de respuesta a alertas documentados.

Escaneo Continuo de Vulnerabilidades

Establecer un programa de escaneo continuo de vulnerabilidades sobre todas las plataformas web y de infraestructura, con priorización por criticidad y seguimiento de remediación.

Recomendaciones Estratégicas: Desarrollo Seguro y Aseguramiento Continuo

El fortalecimiento de la seguridad en el desarrollo de software es una de las acciones de mayor impacto para prevenir la reincidencia de vulnerabilidades y reducir el riesgo en las plataformas web de la Superintendencia.



En este marco, el escaneo continuo y las validaciones sistemáticas sobre las plataformas deben convertirse en una **disciplina permanente para prevenir reincidencias, detectar tempranamente debilidades y sostener el cierre progresivo de brechas**. La formación continua de los equipos de desarrollo en prácticas de codificación segura es un componente esencial de este programa.

Recomendaciones Estratégicas: Monitoreo, Detección y Respuesta

La consolidación de capacidades de monitoreo, detección y respuesta es el **componente más crítico del programa de fortalecimiento**, dado que los hallazgos previos evidenciaron la ausencia de alertas oportunas y bloqueos efectivos frente a ataques actuales.



Centro de Operaciones de Seguridad

Evaluar la viabilidad de establecer o contratar capacidades de SOC (Security Operations Center) para monitoreo continuo 24/7 de los activos críticos.



Inteligencia de Amenazas

Suscribirse a fuentes de inteligencia de amenazas relevantes para el sector público colombiano e integrarlas con los controles de detección existentes.



Playbooks de Respuesta

Desarrollar playbooks de respuesta para los escenarios de mayor riesgo: compromiso de credenciales, explotación web, ransomware y acceso no autorizado.

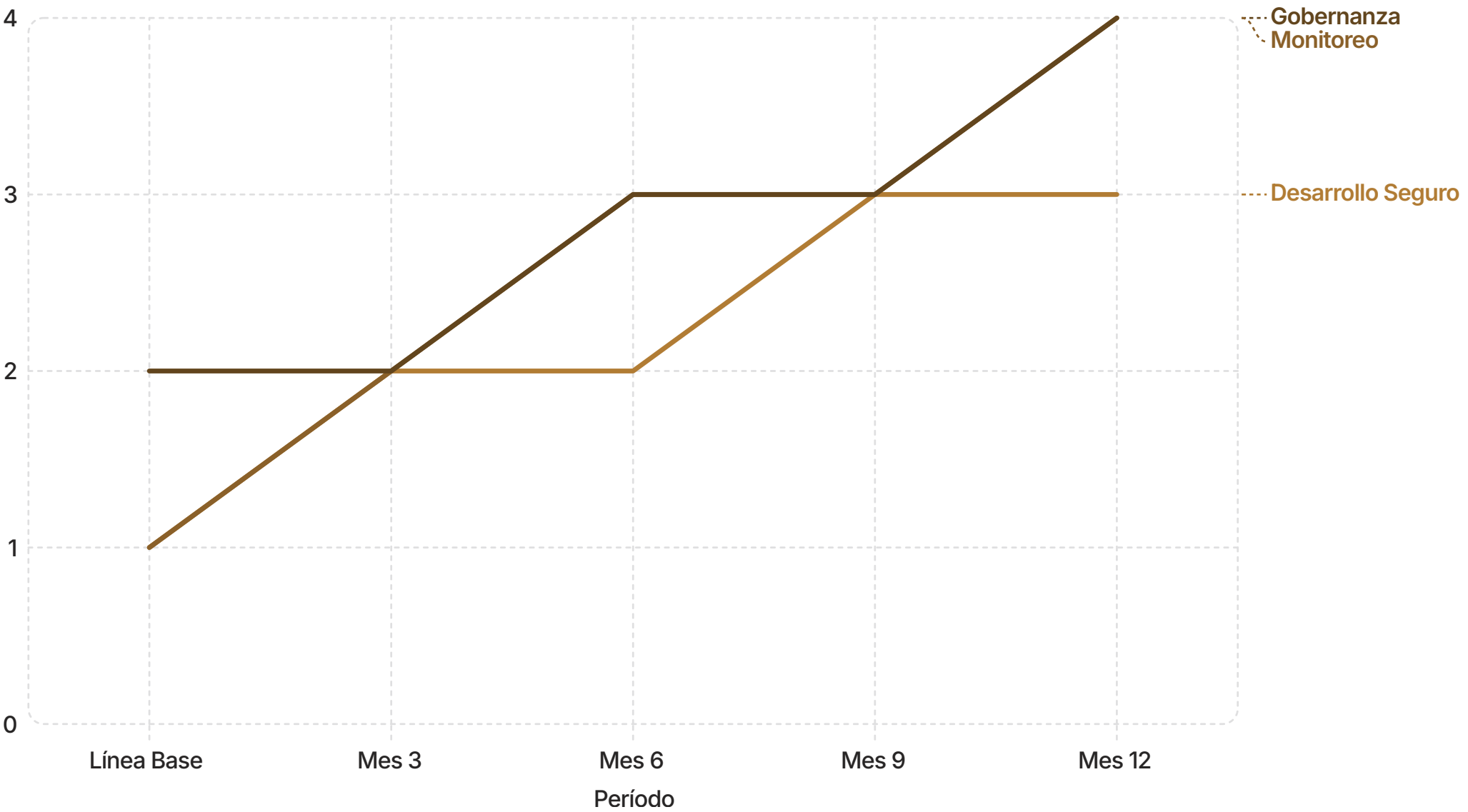


Ejercicios de Simulación

Realizar ejercicios periódicos de simulación de incidentes (tabletop exercises) para validar la efectividad de los procedimientos de respuesta y mejorar continuamente.

Análisis de Tendencias: Evolución de la Madurez Esperada

La siguiente gráfica muestra la evolución esperada del nivel de madurez por dominio a lo largo del año, como resultado de la implementación del roadmap estratégico.



La evolución esperada muestra que al finalizar el año, los dominios de **Gobernanza y Monitoreo** alcanzarán el Nivel 4 – Avanzado, mientras que **Desarrollo Seguro** alcanzará el Nivel 3 – Intermedio, sentando las bases para continuar la mejora en el siguiente ciclo.

Consideraciones de Cumplimiento Normativo

La Superintendencia de Transporte, como entidad del Estado colombiano, está sujeta a un marco normativo que establece obligaciones específicas en materia de seguridad de la información y protección de datos. El fortalecimiento de la ciberseguridad no es únicamente una decisión estratégica, sino también un **imperativo de cumplimiento normativo**.

Política de Gobierno Digital

Lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para la seguridad digital en entidades del Estado colombiano.

Ley 1581 de 2012

Régimen de protección de datos personales en Colombia. Obligaciones de seguridad en el tratamiento de datos personales de ciudadanos.

CONPES 3995 de 2020

Política Nacional de Confianza y Seguridad Digital. Marco estratégico para la gestión de riesgos de seguridad digital en Colombia.

Modelo de Seguridad y Privacidad (MSPI)

Modelo de Seguridad y Privacidad de la Información del MinTIC, alineado con ISO 27001, de obligatorio cumplimiento para entidades del Estado.

Factores Críticos de Éxito del Programa

El éxito del programa de fortalecimiento de ciberseguridad depende de la convergencia de factores organizacionales, técnicos y culturales. Los siguientes factores son determinantes para garantizar la sostenibilidad de las mejoras implementadas:



Compromiso Directivo

El apoyo activo de la alta dirección es fundamental para garantizar la asignación de recursos, la priorización de iniciativas y la cultura de seguridad institucional.



Asignación de Recursos

La inversión adecuada en tecnología, talento humano y capacitación es un prerequisite para la implementación efectiva del programa de fortalecimiento.



Trabajo Transversal

La ciberseguridad requiere la participación activa de todas las áreas de la organización, no únicamente del equipo de tecnología.



Medición y Mejora Continua

El establecimiento de indicadores claros y la revisión periódica del programa garantizan la mejora continua y la adaptación al entorno de amenazas.

Cierre: Síntesis del Diagnóstico

La Evaluación de Madurez en Ciberseguridad bajo diagnóstico estructural NIST/ISO se establece como **base para consolidar una gestión integral, medible y sostenida**, orientada a reducir el riesgo real sobre plataformas, infraestructura y procesos.

El aprendizaje del diagnóstico anterior, junto con las remediaciones ya ejecutadas, permite establecer una ruta clara para el presente año: fortalecer gobierno, elevar la efectividad de los controles existentes, robustecer la detección y la respuesta, e institucionalizar el desarrollo seguro con aseguramiento continuo.

Con ello, la Superintendencia de Transporte podrá **consolidar lineamientos firmes y coherentes con la criticidad de sus servicios**, elevando su madurez y reduciendo su exposición frente a amenazas actuales.

Cierre: Imperativo Estratégico de la Ciberseguridad

La ciberseguridad en la Superintendencia de Transporte no puede seguir siendo tratada como una función técnica periférica. La criticidad de sus servicios digitales, la naturaleza pública de sus plataformas y el impacto directo sobre los ciudadanos y el sector transporte colombiano exigen que la ciberseguridad sea **parte estructural del negocio digital institucional**.

1

Hoy

Nivel 2 Básico: Controles parciales, brechas significativas en detección y desarrollo seguro. Riesgo operativo elevado.

2

En 12 Meses

Nivel 3 - 4: Intermedio/Avanzado: Controles consistentes, monitoreo activo, gobernanza formalizada. Riesgo gestionado.

3

En 3 Años

Nivel 4 - 5: Avanzado/Optimizado: Mejora continua, automatización, cultura de seguridad consolidada. Resiliencia institucional.

Conclusiones Estratégicas

A partir del diagnóstico realizado, se establecen las siguientes conclusiones estratégicas que deben orientar las decisiones de la Superintendencia de Transporte en materia de ciberseguridad:

1 La madurez actual es insuficiente frente a la criticidad de los servicios

El nivel 2 – Básico identificado no es coherente con la criticidad de los servicios digitales de la entidad y el impacto potencial de un incidente de seguridad sobre la operación institucional y la confianza ciudadana.

3 El cierre de brechas es un proceso continuo, no un evento

La sostenibilidad de las mejoras requiere la institucionalización de la ciberseguridad como un proceso de gestión continua, con indicadores, evidencia y mejora sistemática.

2 Las brechas más críticas requieren atención inmediata

Los dominios de monitoreo y detección, seguridad en el desarrollo y gestión de credenciales presentan las brechas más significativas y deben ser priorizados en el plan de acción inmediato.

4 La gobernanza es el habilitador de todo lo demás

Sin una gobernanza sólida, los controles técnicos carecen de dirección y sostenibilidad. La formalización de la estructura de gobernanza es el primer paso crítico del programa.

Próximos Pasos Inmediatos

Para iniciar la implementación del programa de fortalecimiento de ciberseguridad, se recomienda ejecutar los siguientes pasos inmediatos en los próximos 30 días:



Presentación a la Alta Dirección

Presentar los resultados del diagnóstico y el roadmap estratégico a la alta dirección para obtener el compromiso y la aprobación de los recursos necesarios.



Designación del Equipo de Ciberseguridad

Designar formalmente el responsable de ciberseguridad y conformar el equipo de trabajo para la implementación del programa.



Escaneo Inicial de Vulnerabilidades

Ejecutar un escaneo completo de vulnerabilidades sobre todas las plataformas web y de infraestructura para establecer la línea base técnica definitiva.



Plan de Acción Detallado

Desarrollar el plan de acción detallado para el corto plazo (0-3 meses) con responsables, fechas, recursos y criterios de éxito definidos.

Glosario de Términos Técnicos

A continuación se presenta un glosario de los principales términos técnicos utilizados en el presente informe, para facilitar su comprensión por parte de todos los lectores:

Término	Definición
NIST CSF	Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología de EE.UU. Organiza la ciberseguridad en cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar.
ISO 27001	Estándar internacional para sistemas de gestión de seguridad de la información. Establece requisitos para implementar, mantener y mejorar un SGSI.
SIEM	Security Information and Event Management. Plataforma de correlación y análisis de eventos de seguridad en tiempo real.
SSDLC	Secure Software Development Lifecycle. Ciclo de vida de desarrollo de software con prácticas de seguridad integradas en cada fase.
MFA	Multi-Factor Authentication. Autenticación que requiere dos o más factores de verificación para acceder a un sistema.
KPI / KRI	Key Performance Indicator / Key Risk Indicator. Indicadores de desempeño y riesgo para medir la efectividad de los controles de seguridad.
BCP / DRP	Business Continuity Plan / Disaster Recovery Plan. Planes para garantizar la continuidad y recuperación de operaciones ante eventos disruptivos.
SAST / DAST	Static/Dynamic Application Security Testing. Pruebas de seguridad de aplicaciones en código fuente (estático) y en ejecución (dinámico).

Referencias y Marcos Normativos

El presente informe se fundamenta en los siguientes marcos de referencia internacionales, estándares y normativas aplicables:

NIST Cybersecurity Framework v2.0

National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Versión 2.0, 2024.

ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, 2022.

ISO/IEC 27005:2022

Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization, 2022.

CONPES 3995 de 2020

Política Nacional de Confianza y Seguridad Digital. Consejo Nacional de Política Económica y Social, República de Colombia, 2020.

Modelo de Seguridad y Privacidad (MSPI)

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Modelo de Seguridad y Privacidad de la Información para entidades del Estado colombiano.

OWASP Top 10

Open Web Application Security Project. Top 10 Web Application Security Risks. Referencia para la identificación y mitigación de vulnerabilidades en aplicaciones web.

Firma y Certificación del Informe

El presente informe técnico de Evaluación de Madurez en Ciberseguridad ha sido elaborado con base en los más altos estándares de la consultoría especializada en ciberseguridad, gestión del riesgo tecnológico y auditoría de sistemas de información para entidades gubernamentales.

No.	Nombre	Fecha	Firma
001	Virgilio Salgado Escorce	16/Marzo/2026	V. Salgado E.

 Este informe ha sido elaborado exclusivamente para la Superintendencia de Transporte de Colombia. Su contenido es de carácter técnico - institucional y confidencial. Cualquier reproducción, distribución o uso no autorizado está prohibido. La información contenida en este documento debe ser tratada conforme a los lineamientos de clasificación de la información de la entidad.

Barranquilla, Atlántico — Marzo 2026