



**Agencia
Nacional Digital**



Informe de seguimiento

Superintendencia de Transporte

Entregables de la fase orientados al fortalecimiento
institucional de la ciberseguridad

Fase de Seguimiento

Documento técnico para entrega institucional



**Agencia
Nacional Digital**



CONTROL DE CAMBIOS DEL DOCUMENTO

REVISIÓN No.	FECHA	DESCRIPCIÓN	AUTOR DEL CAMBIO
1	---	Creación del documento	Virgilio Salgado



Agencia Nacional Digital



Contenido

1. Introducción	4
2. Objetivo general	4
3. Objetivos específicos	5
4. Marco legal y normativo	5
5. Desarrollo del seguimiento gerencial.....	6
6. Análisis estadístico ejecutivo.....	8
7. Conclusión	8
8. Recomendaciones gerenciales	9



Agencia Nacional Digital



1. Introducción

El presente informe de seguimiento gerencial tiene como propósito exponer, desde una perspectiva estratégica y ejecutiva, el estado general de la seguridad tecnológica evidenciado durante las actividades de auditoría de ciberseguridad y validación posterior efectuadas sobre activos institucionales priorizados. Este documento no busca profundizar en aspectos técnicos particulares ni en la descripción detallada de vulnerabilidades específicas, sino presentar a nivel directivo una visión consolidada del grado de exposición identificado, la criticidad de los hallazgos, el nivel de afectación potencial sobre la operación institucional y la necesidad de fortalecer de manera prioritaria la postura de ciberseguridad de la entidad.

Como resultado del ejercicio realizado, evidenciamos que la superficie tecnológica evaluada presenta debilidades relevantes de seguridad que impactan de manera directa la protección de los activos institucionales, la confidencialidad de la información, la integridad de los sistemas y la disponibilidad de los servicios. Los resultados reflejan que, aunque existen algunos controles implementados, estos no han sido suficientes para contener integralmente los riesgos detectados ni para impedir escenarios de compromiso sobre componentes sensibles de la infraestructura evaluada.

Este seguimiento permite a la alta dirección contar con un insumo claro para la toma de decisiones, la priorización de acciones correctivas y la formulación de medidas de fortalecimiento institucional en materia de seguridad digital. A su vez, ofrece una lectura ejecutiva sobre el nivel actual de exposición, la urgencia de intervención y la necesidad de avanzar hacia una estrategia integral de remediación, monitoreo y mejora continua.

2. Objetivo general

Presentar un informe de seguimiento gerencial sobre el estado de la ciberseguridad de los activos evaluados, con el fin de consolidar los resultados generales de la auditoría y del proceso de validación posterior, exponer el nivel de riesgo institucional identificado y servir como base para la toma de decisiones orientadas al fortalecimiento de la seguridad de la información y la reducción de la exposición tecnológica de la entidad.



Agencia Nacional Digital



3. Objetivos específicos

Consolidar de forma ejecutiva los principales resultados obtenidos durante las actividades de evaluación de seguridad realizadas sobre sistemas y componentes institucionales.

Exponer el nivel general de criticidad de los hallazgos identificados, desde un enfoque estadístico y gerencial, sin entrar en detalle técnico de cada debilidad. Describir el impacto institucional derivado de las condiciones de riesgo detectadas, incluyendo afectaciones potenciales sobre plataformas, información y componentes asociados a bases de datos.

Valorar el nivel actual de la postura de ciberseguridad de la entidad con base en la evidencia obtenida durante la auditoría y el re-test realizado sobre activos críticos.

Orientar a la dirección sobre la necesidad de adoptar acciones prioritarias de contención, remediación y fortalecimiento estructural de la seguridad digital.

4. Marco legal y normativo

El presente informe de seguimiento se enmarca en los principios y lineamientos que regulan la protección de la información, la seguridad digital y la gestión de riesgos tecnológicos dentro del contexto institucional colombiano. En primer lugar, se toma como referencia la **Ley 1273 de 2009**, que fortalece la protección jurídica de la información y de los sistemas informáticos, estableciendo conductas punibles relacionadas con el acceso abusivo a sistemas, la interceptación de datos y otras afectaciones a entornos digitales. De igual manera, se considera la **Ley 1581 de 2012**, asociada a la protección de datos personales, en la medida en que la seguridad de las plataformas y bases de datos constituye un elemento fundamental para preservar la confidencialidad y el tratamiento adecuado de la información.

Asimismo, se reconoce la importancia de la **Ley 1712 de 2014**, en equilibrio con los principios de disponibilidad, integridad y reserva de la información pública, así como del **Decreto 1078 de 2015**, que compila la reglamentación del sector TIC y sirve de soporte para la adopción de lineamientos de seguridad digital en entidades públicas. Desde el punto de vista técnico y metodológico, el seguimiento se alinea con buenas prácticas reconocidas internacionalmente en materia de pruebas de seguridad, evaluación de controles y fortalecimiento de la postura institucional, tomando como referencia marcos como **NIST**, **OWASP** y estándares asociados a la gestión de seguridad de la información. Estos referentes no solo respaldan la validez del ejercicio realizado, sino que



Agencia Nacional Digital



además orientan las decisiones de mejora y priorización de remediaciones dentro de la entidad.

5. Desarrollo del seguimiento gerencial

En el marco de las actividades de auditoría de ciberseguridad adelantadas sobre los activos definidos dentro del alcance institucional, consolidamos un panorama de riesgo que evidencia la existencia de hallazgos relevantes sobre diferentes componentes tecnológicos evaluados. Desde una perspectiva estadística, el resultado general del ejercicio permitió identificar un total de **14 hallazgos**, distribuidos en **7 de criticidad alta** y **7 de criticidad media**, sin presencia de hallazgos clasificados como bajos. Esta distribución muestra que el 100% de las situaciones identificadas requieren atención prioritaria o significativa, al no tratarse de observaciones menores, sino de condiciones con capacidad real de afectar la seguridad de la operación institucional.

Desde una visión gerencial, este resultado permite concluir que la entidad presenta una **postura de ciberseguridad intermedia con brechas críticas relevantes**, en la que algunos mecanismos de protección y administración se encuentran presentes, pero persisten debilidades estructurales que incrementan la exposición frente a escenarios de acceso no autorizado, compromiso de sistemas y afectación de información sensible. En otras palabras, el entorno evaluado no refleja una condición de colapso generalizado, pero sí evidencia un nivel de madurez insuficiente para garantizar una protección robusta y sostenida frente a amenazas con impacto real sobre activos estratégicos.

Uno de los aspectos más relevantes observados durante el seguimiento fue la confirmación de que determinadas condiciones de riesgo previamente advertidas continúan teniendo impacto sobre la seguridad del ecosistema evaluado. En especial, el proceso de validación posterior realizado sobre un activo crítico demostró que la remediación aplicada no fue plenamente efectiva, manteniéndose una condición de exposición severa con capacidad de comprometer la plataforma analizada y los recursos asociados a ella. El re-test concluyó expresamente que la plataforma evaluada **no superó satisfactoriamente la validación de remediación**, lo que confirma la persistencia de un riesgo crítico y la necesidad de respuesta inmediata por parte de la entidad.

A nivel institucional, el hallazgo más sensible del seguimiento consiste en que, durante las actividades realizadas, evidenciamos afectación sobre componentes asociados a bases de datos, incluyendo acceso a recursos



Agencia Nacional Digital



vinculados a **CONSOLA_TAUX**, lo que representa un evento de alta relevancia desde el punto de vista gerencial. Sin entrar en la naturaleza técnica detallada del vector utilizado, el hecho de que se haya alcanzado acceso sobre este tipo de componentes implica una situación de riesgo mayor para la entidad, en la medida en que compromete no solo la seguridad de una plataforma específica, sino también la confianza sobre la segregación, protección y resguardo de la información alojada en entornos institucionales de soporte misional.

En términos ejecutivos, esto significa que el riesgo identificado trasciende el plano meramente técnico y adquiere una dimensión estratégica. La posibilidad de alcanzar acceso a componentes relacionados con bases de datos representa una amenaza directa sobre la confidencialidad de la información, la integridad de registros institucionales, la continuidad de la operación y la estabilidad reputacional de la entidad. Además, evidencia que un incidente de esta naturaleza no se limitaría a una afectación aislada, sino que podría extender sus consecuencias hacia otros sistemas, servicios o procesos conectados con el entorno comprometido.

De manera complementaria, el seguimiento nos permitió establecer que la infraestructura analizada presenta señales de debilidad en aspectos de endurecimiento, gestión de accesos, controles de exposición y protección de componentes críticos. Aunque el informe técnico original documenta la existencia de múltiples tipos de hallazgos, desde esta visión gerencial lo relevante es que el conjunto de resultados confirma una **superficie de ataque amplia**, con exposición suficiente para permitir escenarios de reconocimiento, acceso indebido, compromiso de componentes internos y debilitamiento de las barreras de protección institucional.

También resulta importante resaltar que la existencia de controles perimetrales o de filtrado no garantiza por sí sola una mitigación efectiva del riesgo, cuando persisten debilidades estructurales o condiciones no corregidas dentro del entorno. El re-test evidenció precisamente que la sola presencia de mecanismos de defensa no fue suficiente para neutralizar el riesgo validado, lo que confirma la necesidad de abordar la seguridad desde una perspectiva integral: eliminación de exposiciones, corrección de causas raíz, rotación de accesos comprometidos, fortalecimiento de configuraciones y validación posterior de cierre.

Bajo esta lectura, puede afirmarse que el nivel general de ciberseguridad de la entidad, para los activos evaluados, requiere fortalecimiento prioritario. La organización cuenta con una base sobre la cual estructurar su mejora, pero los resultados demuestran que aún existen brechas importantes que deben ser



Agencia Nacional Digital

intervenidas con enfoque de riesgo, priorización técnica y acompañamiento de la alta dirección. La situación actual exige no solo correcciones puntuales, sino también medidas de gobernanza, seguimiento continuo y consolidación de una cultura de seguridad alineada con la criticidad de los servicios institucionales.

6. Análisis estadístico ejecutivo

Con base en la información consolidada del ejercicio, el comportamiento general de los hallazgos puede resumirse de la siguiente manera:

- **Total de hallazgos identificados:** 14
- **Hallazgos de criticidad alta:** 7
- **Hallazgos de criticidad media:** 7
- **Hallazgos de criticidad baja:** 0

Esto equivale a la siguiente distribución porcentual:

- **50%** de los hallazgos corresponde a criticidad alta
- **50%** de los hallazgos corresponde a criticidad media
- **0%** corresponde a criticidad baja

Desde una visión gerencial, esta estadística es especialmente relevante porque evidencia que **la totalidad de los hallazgos detectados se ubica en niveles de riesgo que demandan gestión prioritaria o intervención significativa**. La ausencia de hallazgos bajos indica que el ejercicio no identificó situaciones marginales o de simple mejora, sino debilidades con impacto potencial suficiente para comprometer activos, procesos o información institucional relevante.

7. Conclusión

Con base en el seguimiento realizado, concluimos que la entidad presenta un nivel de exposición importante en materia de ciberseguridad sobre los activos evaluados, evidenciando brechas que deben ser atendidas con prioridad institucional. Los resultados consolidados muestran que los hallazgos identificados no son de carácter menor, sino que corresponden en su totalidad a condiciones de criticidad alta y media, lo cual refleja una situación que



Agencia Nacional Digital



requiere decisiones oportunas, intervención técnica estructurada y control gerencial permanente.

Asimismo, el seguimiento confirma que en al menos uno de los activos críticos revisados la remediación aplicada no ha sido suficiente, manteniéndose una condición de riesgo severa con capacidad de comprometer la plataforma y sus componentes asociados. De forma particularmente sensible, se logra evidenciar un impacto sobre recursos vinculados a bases de datos, incluyendo componentes relacionados con **CONSOLA_TAUX**, lo cual eleva significativamente la importancia institucional del riesgo detectado y obliga a considerar este resultado como una alerta prioritaria para la seguridad de la información y la continuidad operativa.

En términos generales, la entidad no parte de un escenario sin controles, pero sí enfrenta una condición en la que dichos controles resultan insuficientes frente al nivel de exposición identificado. Por ello, el resultado del seguimiento debe interpretarse como una oportunidad para fortalecer la gobernanza de ciberseguridad, acelerar las acciones de remediación, robustecer los mecanismos de protección y establecer un esquema continuo de revisión, validación y mejora. La respuesta institucional frente a este panorama debe ser integral, priorizada y sostenida, con participación tanto de las áreas técnicas como de los niveles directivos.

8. Recomendaciones gerenciales

Recomendamos priorizar de manera inmediata un plan de remediación institucional enfocado en el cierre efectivo de los hallazgos de mayor criticidad, acompañado de seguimiento ejecutivo y validaciones posteriores que permitan confirmar su corrección real. Igualmente, resulta necesario fortalecer los controles de acceso, la protección de componentes sensibles, la gestión segura de credenciales, el endurecimiento de plataformas y la revisión integral de los entornos comprometidos.

Desde una perspectiva de dirección, también recomendamos establecer una hoja de ruta de ciberseguridad que contemple responsables, criterios de priorización, clasificación de prioridades, monitoreo de cumplimiento y nuevas validaciones técnicas sobre los activos más sensibles. El seguimiento no debe limitarse al cierre documental de los hallazgos, sino a la verificación efectiva de que las condiciones de riesgo hayan sido eliminadas o reducidas a niveles aceptables para la operación institucional.