XX Congreso Nacional de Ciencias y Tecnología
APANAC 2025
40 años de ciencias y tecnología

ISSN: 2805-1807
XX Congreso Nacional de Ciencia y Tecnología
30 de septiembre al 3 de octubre 2025

EVALUACIÓN DE LA CIBERSEGURIDAD EN LA METROLOGÍA: ANALIZANDO LA RESILIENCIA ANTE AMENAZAS DIGITALES

González, Edwin
Centro Nacional de Metrología de Panamá (CENAMEP AIP)
Panamá, Panamá
ORCID: 0009-0009-8216-5055

Carrión, Alfonso
Centro Nacional de Metrología de Panamá (CENAMEP AIP)
Panamá, Panamá
ORCID: 0000-0002-6099-8744

Abstract

The increase in cyber incidents demonstrates that metrology laboratories are also exposed to risks that can compromise the reliability of their measurements. Consequently, this study assessed the cybersecurity maturity of CENAMEP AIP and secondary laboratories, as well as the knowledge level of their staff. The objective of this project was to identify gaps in policies, best practices and incident response plans, as well as to strengthen the security posture through training and simulations. A diagnostic assessment was carried out, using CSF 2.0–based interviews (i.e. a cybernetic security framework); in addition, training activities and controlled phishing simulations were implemented using Smartfense. The findings revealed that 68% of the staff had not received prior training and that most organizations lacked a formal incident response plan. The simulations indicated an initial reduction in risky behavior, followed by monthly variations linked to awareness levels and threat detection capability. In conclusion, significant deficiencies in security management were identified, which can be mitigated through basic policies, clear procedures and continuous awareness programs, reaffirming that the human factor remains the most vulnerable component in institutional cybersecurity.

Keywords: awareness, cybersecurity, simulations, phishing, Smartfense.

Resumen

El aumento de incidentes cibernéticos demuestra que los laboratorios metrológicos también están expuestos a riesgos que pueden afectar la confiabilidad de sus mediciones; por ello,

https://doi.org/10.33412/apanac.2025.63

este estudio evaluó la madurez en ciberseguridad del CENAMEP AIP y de laboratorios secundarios, así como el nivel de conocimiento de su personal sobre este tema. El objetivo de este proyecto fue identificar brechas en políticas, buenas prácticas y en los planes de respuesta a incidentes (PRI), así como fortalecer la postura de seguridad mediante capacitación y simulaciones. Se aplicó una prueba diagnóstica inicial; luego, se realizaron entrevistas basadas en la herramienta CSF 2.0 (marco de seguridad cibernética, por sus siglas en inglés) y se desarrollaron actividades formativas y campañas de phishing controladas a través de la plataforma Smartfense. Los resultados mostraron que el 68% del personal no contaba con capacitación previa y que la mayoría de las organizaciones carecía de un plan formal de respuesta a incidentes. Las simulaciones evidenciaron una reducción inicial del comportamiento riesgoso, seguida de variaciones mensuales asociadas al nivel de atención y detección de amenazas. En conclusión, se identificaron deficiencias importantes en la gestión de la seguridad que pueden mitigarse mediante políticas básicas, procedimientos claros y programas continuos de sensibilización, reafirmando que el factor humano sigue siendo el elemento más vulnerable dentro de la ciberseguridad institucional.

Palabras claves: concientización, ciberseguridad, simulaciones, phishing, Smartfense.

1. INTRODUCCIÓN

En los últimos años, los reportes de incidentes cibernéticos han ido en aumento, evidenciando que ninguna organización está libre de estos riesgos digitales, incluyendo las empresas dedicadas a la metrología científica, legal e industrial. La metrología se encuentra inmersa en un cambio de paradigma, debido al proceso de transformación digital en la industria y sociedad. Hoy en día, es tarea de los laboratorios digitalizar las mediciones, transmitirlas y automatizar los procesos de entrega de la información al cliente, evitando el error humano [1].

Muchas de estas organizaciones carecen de políticas robustas de seguridad informática o de planes de respuesta a incidentes (PRI) bien definidos, lo que deja vulnerable su infraestructura a ataques que podrían comprometer la confiabilidad de los datos metrológicos y - en consecuencia - afectar la credibilidad técnica y operativa de los sistemas de medición implementados por ellos. Adicionalmente, es posible afirmar que el factor humano continúa siendo uno de los principales puntos de debilidad en materia de ciberseguridad. Más aún, la limitada capacitación y/o la concientización del personal facilita el éxito de ataques por parte de ciberdelincuentes.

Ante esta realidad, surge la necesidad de evaluar el nivel de madurez en ciberseguridad

https://doi.org/10.33412/apanac.2025.63

del CENAMEP AIP y los laboratorios secundarios en Panamá, con el fin de detectar vulnerabilidades, fortalecer las capacidades del personal, establecer estrategias preventivas y correctivas que garanticen la continuidad y confidencialidad de los servicios metrológicos en el país. Junto a esto se busca fortalecer la ciberseguridad institucional mediante la capacitación de los colaboradores empleando, entre otras herramientas, la plataforma comercial Smartfense para evaluar y mejorar el conocimiento en ciberseguridad a través de actividades interactivas como videos, simulaciones y pruebas.

2. METODOLOGÍA

Análisis del conocimiento en ciberseguridad, buenas prácticas y efectividad del plan de respuesta a incidentes (PRI)

Se realizó un análisis de conocimiento sobre ciberseguridad para evaluar cuántos colaboradores han recibido capacitación previamente. Esto se realizó aplicando una prueba diagnóstica en un formulario virtual (con la gran mayoría de preguntas en modalidad cerrada), que consultó sobre la terminología básica asociada a ciberseguridad y casos cotidianos a nivel personal y profesional, en los que se debe tomar decisiones enfatizando la seguridad cibernética.

Posteriormente, en reuniones presenciales junto al encargado de tecnología o representante de la organización de las entidades participantes, se identificaron carencias o limitaciones en la implementación de políticas de seguridad, buenas prácticas y si éstas cuentan con un plan de respuesta de incidentes (PRI) formalizado. Para esta actividad se tomó como base el Marco de Seguridad Cibernética (CSF) 2.0. Éste está diseñado para ayudar a las organizaciones de todos los tamaños y sectores (que incluye a la industria, el gobierno, la academia y las organizaciones sin fines de lucro), para gestionar y reducir sus riesgos de seguridad cibernética [2]. Con ayuda de este marco de trabajo se identificaron categorías para el análisis, moldeadas a las necesidades o situaciones presentes en las entidades metrológicas.

La Figura 1 muestra las funciones de la herramienta CSF como una rueda continua, pues todos sus componentes y funciones se relacionan entre sí. Por ejemplo, una organización categorizará los activos en “Identificar” y tomará medidas para asegurar esos activos en “Proteger”.

https://doi.org/10.33412/apanac.2025.63

Figura 1. Funciones de la herramienta CSF.

Mejora de la postura de seguridad cibernética

Como propuesta de mejora, se asignaron actividades de aprendizaje para aumentar el conocimiento de ciberseguridad de los participantes; estas actividades se desarrollaron en la plataforma Smartfense (Figura 2) que fue provista por el CENAMEP AIP, desde junio del año 2025. Adicionalmente, se implementaron simulaciones de ataques de phishing, utilizando una herramienta de simulación controlada, proporcionada por la misma plataforma, con el fin de analizar las acciones y el comportamiento de los colaboradores en esos incidentes (agosto a noviembre de 2025). Se trata de una instancia que los equipos fuera del departamento de tecnologías de la información (TI) no sienten como necesaria, o bien, son de poca comprensión. Esta "desconexión" representa un riesgo para la organización, ya que compromete dos de sus recursos intangibles más importantes: la información y las personas [3].

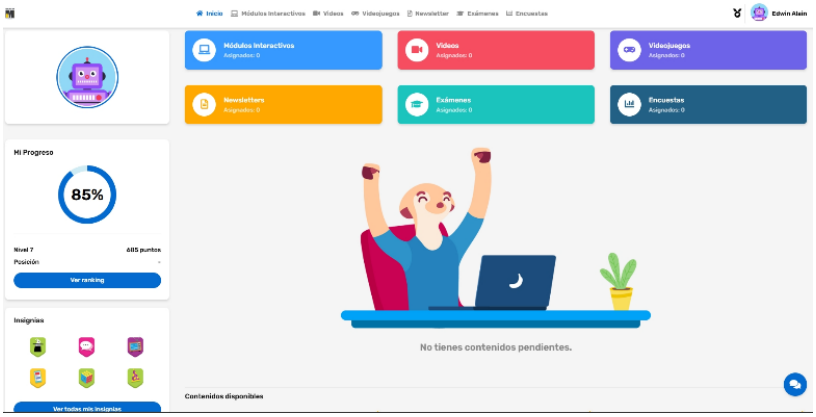

Figura 2. Vista principal de la plataforma Smartfense.

https://doi.org/10.33412/apanac.2025.63

3. RESULTADOS Y DISCUSIÓN

Análisis de conocimiento en ciberseguridad, buenas prácticas y efectividad del PRI

En esta fase del estudio se observaron y compararon las respuestas de los participantes al diagnóstico inicial realizado. Los datos se presentan en términos de porcentaje para aquellas preguntas que se consideraron más relevantes en el contexto de la ciberseguridad en la metrología en Panamá. Los hallazgos más destacados se presentan a continuación.

Como resultado del estudio realizado a los participantes, se muestra en la Figura 3 que el 68% (24 participantes) no han recibido capacitación previa sobre temas de ciberseguridad, lo cual es indicativo de que este proyecto sea una valiosa "puerta de entrada" para conocer y sensibilizar más sobre ciberseguridad. El restante 32% (11 participantes) ha recibido capacitación anteriormente; sin embargo, mantenerse actualizado en este tema es importante, lo cual representó una gran oportunidad para este estudio.

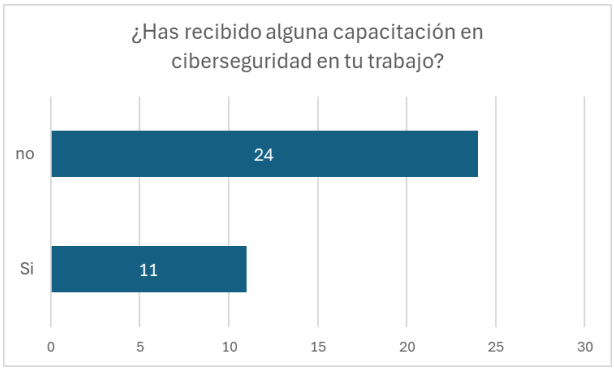

Figura 3. Resumen de los resultados de las acciones de capacitación previa en ciberseguridad.

Por otro lado, se realizaron consultas a cuatro organizaciones (CENAMEP AIP y tres laboratorios secundarios en Panamá, a los que se les asignó un código al azar "Lab. Sec."), en el aspecto de identificación de buenas prácticas. Dentro de los hallazgos destacables (Figura 4), se observa que el CENAMEP y el Lab. Sec. 3 obtuvieron los puntajes más altos, demostrando que ambas entidades sí aplican buenas prácticas dentro de sus procesos e infraestructura. En contraste, los participantes Lab. Sec. 1 y 2 presentan deficiencias en ciberseguridad en sus entornos tecnológicos, las mismas que representan oportunidades de mejora.

https://doi.org/10.33412/apanac.2025.63

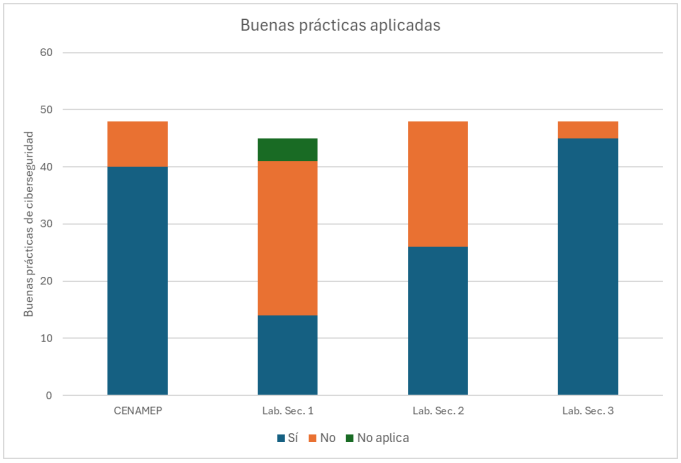

Figura 4. Resultados del formulario de identificación de buenas prácticas en metrología.

Por otro lado, para realizar las consultas a los encargados de tecnología y/o a los representantes de las entidades participantes, se realizó una prueba de la efectividad del PRI, teniendo en cuenta que dicho plan existiese de manera formal en las políticas de la organización, o bien, que haya un procedimiento ya establecido que detalle la acción de cada persona (o sección) involucrada en el plan. En este sentido, la Figura 5 muestra que tres de las cuatro organizaciones no contaban con dicho plan previamente establecido; esto evidencia un limitado planeamiento para afrontar incidentes cibernéticos que pueden detener la operabilidad de la empresa. La organización que sí contaba con un PRI establecido no decidió continuar con las pruebas de eficiencia y organización, para ejecutar acciones de simulacro del plan.

Figura 5. Presencia o ausencia de un plan de respuesta a incidentes (PRI).

https://doi.org/10.33412/apanac.2025.63

Sobre la mejra de la postura de seguridad cibernética

En esta etapa se hicieron evaluaciones del rendimiento del personal en las actividades asignadas de la capacitación y el comportamiento en simulaciones de phishing (Figura 6).

Se observa que, en los primeros meses del estudio, hubo una mayor acción de los participantes de la capacitación. Esto indica que, aunque no hubiese un conocimiento completo de los contenidos de toda la plataforma, los participantes mostraron un compromiso creciente, al participar del proyecto, demostrando interés y disponibilidad a las distintas actividades (o tareas) asignadas.

En contraste, para los últimos meses del estudio se observa una disminución en la participación (Figura 6). Esto puede deberse a saturación del tiempo de los participantes (por la carga de trabajo frente al cierre del año calendario), o bien, por prioridad laboral frente a otras asignaciones y la proximidad del cierre administrativo de este proyecto en ciberseguridad en metrología.

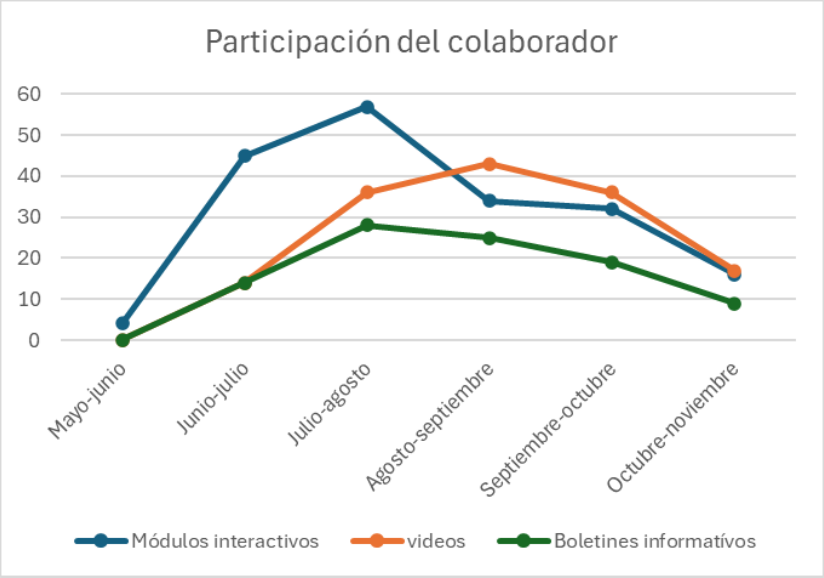

Figura 6. Participación de los colaboradores en las actividades de la plataforma Smartfense.

Finalmente, el comportamiento de los participantes frente a las simulaciones se presenta en la Figura 7. Es destacable indicar que durante cuatro campañas de simulación de phishing que desarrolló este proyecto, se observaron variaciones en el comportamiento de los participantes.

En la primera campaña de simulación, en agosto de 2025 (Figura 7), se registró el mayor nivel de interacción riesgosa, con 16 correos electrónicos abiertos, 10 descargas de archivos sospechosos y cinco ingresos de datos en portales web. En septiembre, por su parte, se

https://doi.org/10.33412/apanac.2025.63

evidenció una disminución notable en todas las categorías, alcanzando valores de cinco correos electrónicos abiertos, cero descargas y cero ingresos de datos en portales web.

Sin embargo, en octubre se observó un repunte parcial, con 10 correos electrónicos abiertos, tres descargas y dos ingresos de datos en portales (Figura 7). Esta instancia sugiere fluctuaciones en la atención del usuario, o en su capacidad de detección de amenazas, ya que en esa campaña la simulación tenía mayor trabajo de preparación para convencer al usuario. Por último, en noviembre de 2025 se mostró un comportamiento similar al mes de septiembre; este cambio pudo ser porque la campaña no fue tan personalizada como la de octubre. Estas variaciones permiten identificar patrones de riesgo y niveles de madurez en la concientización del personal.

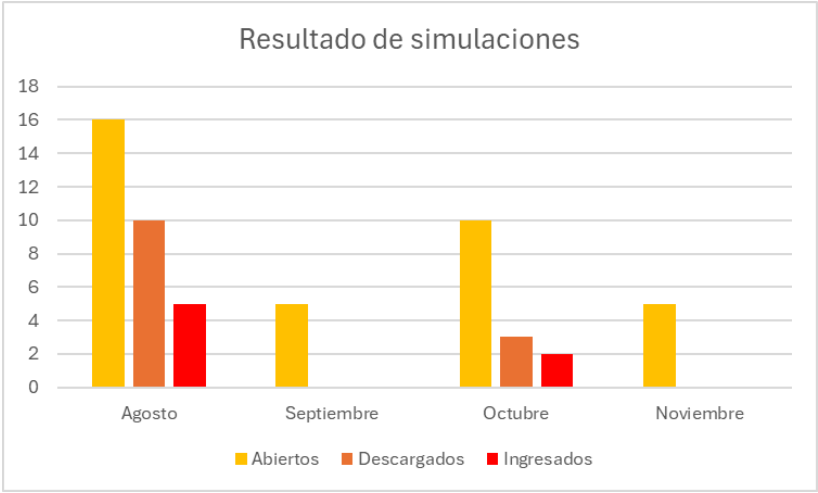

Figura 7. Resultados del comportamiento de los usuarios durante las simulaciones.

4. CONCLUSIONES Y RECOMENDACIONES

Este estudio permitió analizar el nivel de madurez en ciberseguridad del CENAMEP AIP y de algunos laboratorios secundarios en Panamá, evidenciando buenas prácticas pero también falencias relevantes. Aunque los laboratorios secundarios sean empresas pequeñas, muchas de las mejoras no requieren grandes inversiones, sino acciones para establecer y cumplir políticas y procedimientos básicos de seguridad. Ante los datos presentados (ver Sección 3, “Simulaciones”), esta indicación aplica también al CENAMEP AIP.

Los resultados de las simulaciones demostraron que, si bien hubo una reducción inicial del comportamiento riesgoso, la reincidencia observada (en noviembre) confirma que la concientización en ciberseguridad no es un proceso lineal ni permanente. Se requiere atención constante. Estas variaciones refuerzan la necesidad de mantener programas continuos de

https://doi.org/10.33412/apanac.2025.63

capacitación y refuerzo, especialmente considerando que el factor humano sigue siendo la vulnerabilidad más crítica.

Se recomienda formalizar y aplicar un conjunto de políticas y procedimientos que regulen aspectos clave de la seguridad informática, como por ejemplo, la asignación de roles, la segmentación de datos, el uso de contraseñas robustas y la planificación de la continuidad del negocio/empresa en el ambiente de la ciberseguridad. Todas estas prácticas pueden implementarse sin costo significativo y con un alto impacto en la protección institucional. Asimismo, es esencial mantener procesos de sensibilización continua para que el personal reconozca su rol como pilar fundamental de la ciberseguridad en la organización. En este marco, este proyecto abre una ventana importante: es necesario continuar este tipo de estudios y actividades para la constante protección del patrimonio informático del CENAMEP AIP, los laboratorios secundarios de metrología y otras empresas a nivel nacional.

Referencias

[1] I. Aguiar Guillermo, R. Sosa Vera y G. Fuentes Estévez, “Transformación digital de la información documentada en los laboratorios de ensayo y calibración”. Mem. Calid. UH, no. 1, noviembre de 2024.

[2] Instituto Nacional de Estándares y Tecnología, “El Marco de Seguridad Cibernética (CSF) 2.0 del NIST”. NIST Cybersecurity White Paper, NIST CSWP 29 spa., 2024. [Online]. Disponible en: https://doi.org/10.6028/NIST.CSWP.29.spa.

[3] S. M. Martínez, Beltrán, “Todos seguros: una nueva cultura de cuidado de la información”. Proyecto de grado, Universidad del Bosque, Bogotá, 2025. Accedido el 12 de noviembre de 2025. [En línea]. Disponible en: https://hdl.handle.net/20.500.12495/18057.

Agradecimientos

Se agradece a la Secretaría Nacional de Ciencia, Tecnología e Innovación (SENACYT, Panamá) por cofinanciar el “Programa de Pasantías Metrológicas - Ciclo 2025 a 2026” (Contrato de Subsidio Económico DDCCT No. 144-2024), que permitió llevar a cabo este proyecto. Asimismo, se agradece a todo el personal del CENAMEP AIP, a los laboratorios secundarios por el tiempo y el interés en este proyecto y a la Universidad Tecnológica de Panamá (UTP), por su apoyo técnico y científico en la ejecución de este estudio.

Autorización y Licencia CC

https://doi.org/10.33412/apanac.2025.63