Instituto Nacional de Estadística
Subgerencia
Administrativa Financiera
RECIBIDO
26 MAYO 2025
Por: Hora: 12:00

Instituto Nacional de Estadística
Gerencia
RECIBIDO
26 MAYO 2025
Por: Hora: 12:00

Instituto Nacional de Estadística

OFICIO AI-187-2025
Guatemala 26 de mayo de 2025.

Mgtr.
Oscar José Chávez Valdez
Gerente
Instituto Nacional de Estadística
Su Despacho

Mgtr. Chávez Valdez:

De conformidad con el nombramiento de auditoría interna NAI 009-2025, con fecha 01 de abril de 2025, referente a la auditoría de Cumplimiento en el Departamento de Mantenimiento de Infraestructura de Redes y Equipos, realizada por el período comprendido entre el 01 de abril de 2024 y el 31 de marzo de 2025.

La auditoría se ejecutó en estricta conformidad con las Normas Generales y Técnicas de Control Interno Gubernamental, las Normas de Auditoría Interna Gubernamental (NAIGUB), el Manual de Auditoría Interna Gubernamental (MAIGUB) y la Ordenanza de Auditoría Interna Gubernamental establecidas por el Contralor General de Cuentas, así como el Manual de Procesos de Auditoría Interna, el Marco Profesional para la Práctica Profesional de la Auditoría Interna y el Acuerdo Número A-047-2021 Manual de Auditoría de Tecnología de la Información.

En virtud de lo anterior, se adjunta el informe correspondiente, en el que se detallan la información general, el fundamento legal, las normas de auditoría aplicadas, los objetivos, el alcance, las limitaciones, las estrategias y los resultados obtenidos en la auditoría.

Atentamente,

DIRECCIÓN DE AUDITORÍA INTERNA
INSTITUTO NACIONAL DE ESTADÍSTICA
DIRECTOR
I.N.E.
Guatemala, C.A.

Licda. Rosa Lidia Tatuán Lemus
Directora de Auditoría Interna

C.c. Archivo.

Instituto Nacional
de Estadística

INSTITUTO NACIONAL DE ESTADÍSTICA (INE)

INFORME DE AUDITORÍA INTERNA
Departamento de Mantenimiento de Infraestructura de Redes y Equipo
Del 01 de Abril de 2024 al 31 de Marzo de 2025
CAI 00009

GUATEMALA, 26 de Mayo de 2025

ine.gob.gt PBX 2315-4700
8ª calle 9-55 zona 1, Guatemala

Instituto Nacional
de Estadística

Guatemala, 26 de Mayo de 2025

Mgtr:
Oscar José Chávez Valdez
INSTITUTO NACIONAL DE ESTADÍSTICA (INE)
Su despacho

Señor(a):

De acuerdo a nombramiento de auditoría interna No. NAI-009-2025, emitido con fecha 01-04-2025, hacemos de su conocimiento el informe de auditoría interna, actuamos de conformidad con la ordenanza de auditoría interna Gubernamental y Manual de Auditoría Interna

Sin otro particular, atentamente

F. _____
José Antonio Samayoa Gaytán
Auditor,Coordinador

F. _____
Rosa Lidia Tatuán Lemus
Supervisor

Auditoría Interna
ine.gob.gt PBX 2315-4700
8ª calle 9-55 zona 1, Guatemala

Indice

1. INFORMACIÓN GENERAL

1.1 MISIÓN

Somos una institución técnica, rectora del Sistema Estadístico Nacional, que recopila, analiza, produce y difunde estadísticas oficiales, que coadyuven a la toma de decisiones en función de mejorar la calidad de vida para todos los guatemaltecos.

1.2 VISIÓN

Ser una institución técnica innovadora y moderna, reconocida nacional e internacionalmente por la confiabilidad, oportunidad, transparencia y eficiencia de la información estadística que recopila, analiza, produce y difunde.

2. FUNDAMENTO LEGAL

- Ley Orgánica del Instituto Nacional de Estadística y su Reglamento. Decreto Ley No. 3-85 • Ley Orgánica de la Contraloría General de Cuentas y su Reglamento Decreto No. 31-2002 del Congreso de la República y Acuerdo Gubernativo No. 96-2019
- Acuerdo Número A-062-2021, de fecha 12 de octubre de 2021, emitido por la Contraloría General de Cuentas, con el cual se aprobó el Sistema Informático de Auditoría Gubernamental para las Unidades de Auditoría Interna (SAG-UDAI-WEB)
- Acuerdo Número A-070-2021, de fecha 08 de noviembre de 2021, emitido por la Contraloría General de Cuentas, con el cual se aprobó las disposiciones siguientes:
  1. Normas de Auditoría Interna Gubernamental NAIGUB-
  2. Ordenanza de Auditoría Interna Gubernamental
  3. Manual de Auditoría Interna Gubernamental, -MAIGUB-
- Acuerdo Número A-047-2021, Manual de Auditoría de Tecnología de la información

Nombramiento(s) No.
009-2025

3. IDENTIFICACIÓN DE LAS NORMAS DE AUDITORIA INTERNA OBSERVADAS

Para la realización de la auditoría se observaron las Normas de Auditoría Interna Gubernamental siguientes:

NAIGUB-1 Requerimientos generales;
NAIGUB-2 Requerimientos para el personal de auditoría interna;
NAIGUB-3 Evaluaciones a la actividad de auditoría interna; NAIGUB-4 Plan Anual de Auditoría;
NAIGUB-5 Planificación de la auditoría;
NAIGUB-6 Realización de la auditoría; NAIGUB-7 Comunicación de resultados; NAIGUB-8 Seguimiento a recomendaciones.

4. OBJETIVOS

4.1 GENERAL

Verificar y evaluar los controles implementados en las Operaciones de IT

4.2 ESPECÍFICOS

Medir el desempeño de las políticas y procedimientos implementados, determinando si logran mitigar riesgos y garantizar la protección de los activos tecnológicos. Evaluar la eficiencia de los mecanismos de control y supervisión para reducir tiempos de respuesta y mejorar la capacidad de reacción ante incidentes. Asegurar que los controles implementados contribuyen al cumplimiento de los objetivos institucionales y mejoran la seguridad general de las operaciones de TI.

5. ALCANCE

Identificación de deficiencias, vulnerabilidades y riesgos de seguridad informática, verificar cumplimiento normativo y analizar la efectividad de los controles.

No.	Área Asignada	Universo	Cálculo Matemático	Elementos	Muestreo no estadístico
1	Área general	0	NO		0
2	Deficiencias en controles para asegurar la información en la Infraestructura Tecnológica	25	NO		25

5.1 LIMITACIONES AL ALCANCE

No hubo limitación al alcance.

6. ESTRATEGIAS

Estrategias para la Recolección de Información y Pruebas de Auditoría: Como parte del proceso de auditoría, se realizaran las siguientes estrategias para evaluar las operaciones de TI:

1. Inspección documental donde se verifican documentos relacionados con la normativa interna de la Dirección de Informática como el manual de puestos y funciones manual de procesos, políticas de seguridad, procedimientos operativos, informes de gestión, registros de incidentes, configuraciones de los sistemas e informes de auditora informática realizados por la Contraloría General de Cuentas.

2. Cuestionarios y solicitudes de información permiten formular preguntas clave sobre la ejecución de los procesos de administración de sistemas de información, seguridad

informática y protección de datos. A través de estas preguntas estructuradas, se obtienen percepciones sobre el cumplimiento de controles, la efectividad de los procesos y la identificación de posibles vulnerabilidades que no sean evidentes en los registros documentales.

3. Pruebas técnicas y análisis de vulnerabilidades incluye la ejecución de pruebas específicas para evaluar la seguridad y efectividad de los controles implementados. Por ejemplo, pruebas de acceso, revisión de configuraciones de seguridad, simulaciones de ataques para evaluar la respuesta del sistema, y observación del uso de herramientas y procedimientos por parte del personal informático.

Estas estrategias complementan la auditoría, proporcionando evidencia objetiva para evaluar la eficacia de los controles implementados.

7. RESULTADOS DE LA AUDITORÍA

De acuerdo al trabajo de auditoría realizado se informa que no existen riesgos materializados

8. CONCLUSIÓN ESPECÍFICA

Durante la Auditoría, se evaluaron los controles de seguridad lógica implementados en la infraestructura tecnológica del Instituto Nacional de Estadística. Se analizó la evidencia proporcionada por la Dirección de Informática sobre los controles aplicados en su ámbito de competencia, incluyendo:

- Controles de actualizaciones de seguridad
- Controles para el licenciamiento de software
- Controles de acceso
- Controles de autenticación multifactor
- Controles antispam
- Controles antimalware
- Controles de prevención sobre instalación y ejecución de código malicioso
- Controles para el respaldos para aplicaciones críticas
- Inventario de activos tecnológicos
- Controles de monitoreo de eventos de seguridad Office 365

En cuanto a la solución de correo electrónico institucional, se verificó que mantiene la configuración de los protocolos SPF, DKIM y DMARC para reforzar la seguridad del servicio de comunicación electrónica. Asimismo, se constató la gestión activa del hardware y software en la red de datos, la evaluación y mitigación de algunas

vulnerabilidades, y el control de privilegios administrativos en estaciones de trabajo, redes y aplicaciones.

Como oportunidades de mejora, para optimizar los controles, dado que podrían representar un riesgo potencial para los activos, sus sistemas o la información contenida. A continuación, se detallan los principales aspectos observados:

1. Se recomienda reforzar las políticas de navegación de internet para bloquear el acceso a contenido web categorizado como explícito. Se ha identificado sitios con acceso lo que representa un riesgo para la seguridad y el cumplimiento de las normas institucionales. La implementación de restricciones adecuadas contribuirá a mantener un entorno digital seguro evitando la exposición a contenido inapropiado. Se recomienda realizar un análisis detallado para definir los criterios de bloqueo y garantizar una aplicación efectiva de las medidas de seguridad.
2. Se recomienda fortalecer las políticas de navegación para restringir el acceso a sitios web relacionados con la venta de armas y las apuestas en línea. La implementación de estas restricciones contribuirá a reducir los riesgos asociados a actividades potencialmente ilegales o perjudiciales, reforzando la seguridad de la red institucional y promoviendo un entorno digital más seguro para los usuarios.
3. Se recomienda evitar la exposición del equipo de seguridad firewall a través de su dirección IP pública (https://154.196.0.226), lo que permitiría su visibilidad desde cualquier punto de internet y aumentaría el riesgo de accesos no autorizados. Para mitigar esta vulnerabilidad, se debe configurar el acceso exclusivamente para un conjunto limitado de direcciones IP confiables y previamente verificadas, garantizando un control más estricto sobre las conexiones permitidas. Esta medida debe aplicarse a todas las interfaces de gestión y cualquier otro punto de administración de firewalls o dispositivos de seguridad dentro de la red, reduciendo la superficie de ataque y fortaleciendo la protección de la infraestructura institucional.
4. Se recomienda restringir el acceso al equipo de seguridad firewall, evitando una exposición innecesaria a múltiples accesos internos sin restricciones, como los asociados a las direcciones IP https://129.0.4.1, https://129.0.8.1, https://129.0.12.1 y https://129.0.16.1. En su lugar, se debe configurar el acceso exclusivamente para un conjunto limitado de direcciones IP confiables y previamente verificadas, garantizando un control más estricto sobre las conexiones autorizadas. Esta medida debe aplicarse a todas las interfaces de gestión, así como a cualquier otro punto de administración de firewalls o dispositivos de seguridad dentro de la red, minimizando el riesgo de accesos no autorizados y fortaleciendo la protección de la infraestructura institucional.
5. Se recomienda implementar el control de acceso web en ESET Endpoint Security como una medida adicional de protección. Esta funcionalidad permitirá restringir el acceso a páginas web que puedan contener material ofensivo o inapropiado, evitando la exposición a contenido perjudicial para los usuarios y la infraestructura institucional. La aplicación de esta política fortalecerá la seguridad, garantizando un entorno de navegación más seguro y alineado con los estándares organizacionales.
6. Para garantizar la protección del formulario de solicitud de información pública y mitigar el riesgo de spam o ataques automatizados, se recomienda implementar reCAPTCHA.

7. La falta de esta medida de seguridad deja el formulario expuesto a abusos, como el envío masivo de solicitudes falsas, lo que compromete la integridad y confiabilidad de la información recibida. La incorporación de reCAPTCHA permitirá diferenciar entre usuarios legítimos y bots maliciosos, reduciendo significativamente la posibilidad de ataques y asegurando el adecuado funcionamiento del sistema de solicitudes.
8. Implementar medidas específicas de seguridad lógica en la infraestructura de aplicaciones web institucionales del INE. Como parte de esta estrategia, se deben definir restricciones a nivel de dominios y subdominios para limitar el acceso desde la dark web y deep web, particularmente desde redes como Tor o I2P, comúnmente utilizadas para navegar por estas capas ocultas de internet. El uso de estas redes facilita la ejecución de actividades maliciosas como ataques de fuerza bruta, scraping masivo de datos y ataques de denegación de servicio (DDoS), lo que compromete la disponibilidad y seguridad de la página web institucional. Para mitigar estos riesgos, se insta a realizar un análisis detallado y establecer mecanismos de protección que permitan reforzar la seguridad y garantizar la estabilidad operativa del sitio.
9. Actualmente está en uso el rango de direcciones IP 129.0.4.0 a 129.0.60.0 dentro de la red interna del Instituto Nacional de Estadística, sin embargo, estas direcciones IP son de uso público y no están destinadas para uso interno. Se considera que utilizar IPs de rangos públicos en una red interna representa un riesgo significativo de seguridad, aumentando la exposición a accesos no autorizados y posibles vulnerabilidades. Por ello, realizar los análisis pertinentes y proceder con la migración hacia un rango de direcciones IP privadas adecuado, como el subconjunto de 10.0.0.0/8, 172.16.0.0/12 o 192.168.0.0/16, asegurando una configuración segura y alineada con las mejores prácticas de administración de redes.
10. Habilitar la autenticación multifactor (MFA) en Office 365 para usuarios clave, incluyendo al Gerente, Subgerentes, Directores y Jefes de Departamento. Actualmente, el sistema de correo electrónico institucional depende exclusivamente de la autenticación con usuario y contraseña, lo que lo hace vulnerable a amenazas como ataques de phishing, robo de credenciales y ataques de fuerza bruta. La implementación de MFA agregaría una capa adicional de protección, reduciendo significativamente el riesgo de accesos no autorizados y fortaleciendo la seguridad de la información institucional.

Luego del envío del oficio AI-179-2025, en el cual se informaron los principales aspectos observados, los responsables de la Dirección de Informática han presentado pruebas de descargo mediante los oficios DI-181-2025. Tras el análisis correspondiente, se ha determinado que se han atendido los siguientes aspectos:

1. Se recomienda evitar la exposición del equipo de seguridad firewall a través de su dirección IP pública (https://154.196.0.226), lo que permitiría su visibilidad desde cualquier punto de internet y aumentaría el riesgo de accesos no autorizados. Para mitigar esta vulnerabilidad, se debe configurar el acceso exclusivamente para un conjunto limitado de direcciones IP confiables y previamente verificadas, garantizando un control más estricto sobre las conexiones permitidas. Esta medida debe aplicarse a todas las interfaces de gestión y cualquier otro punto de administración de firewalls o

dispositivos de seguridad dentro de la red, reduciendo la superficie de ataque y fortaleciendo la protección de la infraestructura institucional.

2. Se recomienda restringir el acceso al equipo de seguridad firewall, evitando una exposición innecesaria a múltiples accesos internos sin restricciones, como los asociados a las direcciones IP https://129.0.4.1, https://129.0.8.1, https://129.0.12.1 y https://129.0.16.1. En su lugar, se debe configurar el acceso exclusivamente para un conjunto limitado de direcciones IP confiables y previamente verificadas, garantizando un control más estricto sobre las conexiones autorizadas. Esta medida debe aplicarse a todas las interfaces de gestión, así como a cualquier otro punto de administración de firewalls o dispositivos de seguridad dentro de la red, minimizando el riesgo de accesos no autorizados y fortaleciendo la protección de la infraestructura institucional.

3. Para garantizar la protección del formulario de solicitud de información pública y mitigar el riesgo de spam o ataques automatizados, se recomienda implementar reCAPTCHA. La falta de esta medida de seguridad deja el formulario expuesto a abusos, como el envío masivo de solicitudes falsas, lo que compromete la integridad y confiabilidad de la información recibida. La incorporación de reCAPTCHA permitirá diferenciar entre usuarios legítimos y bots maliciosos, reduciendo significativamente la posibilidad de ataques y asegurando el adecuado funcionamiento del sistema de solicitudes.

Realizado el análisis pertinente, en el cual la Dirección de Informática presentó sus pruebas de descargo se concluyó que, si bien algunos aspectos han sido atendidos, otros continúan en proceso y/o en fase de implementación.

1. Reforzar las políticas de navegación de internet para bloquear el acceso a contenido web categorizado como explícito, así como sitios relacionados con la venta de armas y las apuestas en línea. La implementación de estas restricciones contribuirá a reducir los riesgos asociados a actividades potencialmente ilegales o perjudiciales, además de garantizar un entorno digital seguro y alineado con las normas institucionales. Para lograr una aplicación efectiva de estas medidas de seguridad, se recomienda mantener un monitoreo constante sobre el equipo de seguridad firewall permitiendo definir criterios de bloqueo adecuados.

2. Implementar el control de acceso web mediante la solución ESET Endpoint Security como una medida complementaria de protección. Esta funcionalidad permite restringir el acceso a sitios web clasificados con contenido explícito, ofensivo o inapropiado, reduciendo la exposición de los usuarios a material potencialmente dañino y protegiendo la infraestructura institucional. La adopción de esta política fortalecerá significativamente la seguridad del entorno digital, ofreciendo una capa adicional de control que complementa al sistema de seguridad firewall, el cual presenta limitaciones en este tipo de filtrado.

3. Implementar medidas específicas de seguridad lógica en la infraestructura de aplicaciones web institucionales del INE. Como parte de esta estrategia, se deben definir restricciones a nivel de dominios y subdominios para limitar el acceso desde la dark web y deep web, particularmente desde redes como Tor o I2P, comúnmente utilizadas para navegar por estas capas ocultas de internet. El uso de estas redes facilita la ejecución de actividades maliciosas como ataques de fuerza bruta, scraping masivo de datos y ataques de denegación de servicio (DDoS), lo que compromete la disponibilidad y seguridad de la página web institucional. Para mitigar estos riesgos, se insta a realizar un análisis detallado y establecer mecanismos de protección que permitan reforzar la seguridad y garantizar la estabilidad operativa del sitio.

4. Actualmente está en uso el rango de direcciones IP 129.0.4.0 a 129.0.60.0 dentro de la red interna del Instituto Nacional de Estadística, sin embargo, estas direcciones IP son de uso público y no están destinadas para uso interno. Se considera que utilizar IPs de rangos públicos en una red interna representa un riesgo significativo de seguridad, aumentando la exposición a accesos no autorizados y posibles vulnerabilidades. Por ello, realizar los análisis pertinentes y proceder con la migración hacia un rango de direcciones IP privadas adecuado, como el subconjunto de 10.0.0.0/8, 172.16.0.0/12 o 192.168.0.0/16, asegurando una configuración segura y alineada con las mejores prácticas de administración de redes.

5. Habilitar la autenticación multifactor (MFA) en Office 365 para usuarios clave, incluyendo al Gerente, Subgerentes, Directores y Jefes de Departamento. Actualmente, el sistema de correo electrónico institucional depende exclusivamente de la autenticación con usuario y contraseña, lo que lo hace vulnerable a amenazas como ataques de phishing, robo de credenciales y ataques de fuerza bruta. La implementación de MFA agregaría una capa adicional de protección, reduciendo significativamente el riesgo de accesos no autorizados y fortaleciendo la seguridad de la información institucional. Es importante destacar que la presencia de un firewall institucional no es suficiente para mitigar los riesgos asociados al acceso externo, por lo que la implementación de MFA resulta fundamental.

6. Sobre la compatibilidad con SD- WAN para balanceo de carga y failover instantáneo dado que actualmente no se cuenta con una solución SD- WAN implementada en la infraestructura de red, es recomendable la adopción de esta tecnología. La implementación de SD- WAN permitirá optimizar la gestión del tráfico, mejorar la eficiencia en el uso de los enlaces de conectividad y garantizar una mayor resiliencia ante fallos. Si bien la redundancia existente, basada en dos fibras ópticas independientes de un mismo proveedor, esta configuración aún depende de una única entidad proveedora. Para fortalecer la disponibilidad del servicio, se recomienda evaluar la posibilidad de incorporar un segundo proveedor de conectividad. Esto garantizaría una redundancia más robusta y una mayor protección frente a posibles interrupciones a nivel de proveedor.

Recomendaciones:
Se recomienda a la Dirección de Informática, dar seguimiento a los aspectos que permanecen en proceso de implementación para reforzar los controles y mitigar los riesgos tecnológicos identificados en la infraestructura tecnológica del Instituto Nacional de Estadística.

9. EQUIPO DE AUDITORÍA

F. _____
José Antonio Samayoa Gaytán
Auditor, Coordinador

DIRECCIÓN DE AUDITORIA INTERNA INSTITUTO NACIONAL DE ESTADÍSTICA AUDITOR I.N.E. Guatemala, C.A.

F. _____
Rosa Lidia Tatuán Lemus
Supervisor

DIRECCIÓN DE AUDITORIA INTERNA INSTITUTO NACIONAL DE ESTADÍSTICA SUPERVISOR I.N.E. Guatemala, C.A.

ANEXO

Nombramiento CAI 00009.

Instituto Nacional
de Estadística

AUDITORÍA INTERNA
INSTITUTO NACIONAL DE ESTADÍSTICA (INE)
NOMBRAMIENTO DE AUDITORÍA (DE) CUMPLIMIENTO
No. NAI-009-2025

CAI: 00009
Guatemala, 01 de abril de 2025

Equipo de Auditoría
Rosa Lidia Tatuán Lemus (Supervisor)
José Antonio Samayoa Gaytán (Auditor, Coordinador)

En cumplimiento al Acuerdo número A-070-2021, de fecha 28 de octubre de 2021, emitido por el Contralor General de Cuentas, artículo 1 y 2 y en cumplimiento a las funciones de Auditoría Interna se le(s) designa para que se constituya(n) en la (el) Departamento de Mantenimiento de Infraestructura de Redes y Equipo; para que practiquen auditoría (de) Cumplimiento por el período comprendido del 01 de abril de 2024 al 31 de marzo de 2025.

Esta auditoría debe: Verificar y evaluar los controles implementados en las Operaciones de IT

El riesgo identificado que dio origen al nombramiento es: Deficiencias en controles para asegurar la información en la Infraestructura Tecnológica

Los resultados de su actuación, los harán constar en papeles de trabajo e informe, emitiendo la conclusión correspondiente al área evaluada. El informe final debe presentarse el 30-05-2025

Licda. Rosa Lidia Tatuán Lemus
Directora de Auditoria Interna
Instituto Nacional de Estadística

DIRECCIÓN DE AUDITORIA INTERNA
INSTITUTO NACIONAL DE ESTADÍSTICA
DIRECTOR
I.N.E. Guatemala, C.A.