



**Estudio sobre la revisión de accesos y seguridad de los
sistemas de información existentes en el Ministerio.
TI-ESP-001-2026**

San José, 14 de agosto de 2026.

MIVAH-AI-0088-2026

Señor.
Guillermo Carazo Ramírez.
Ministro.
Ministerio de Vivienda y Asentamientos Humanos.

Asunto: Resumen Ejecutivo de los Resultados del Estudio sobre la revisión de accesos y seguridad de los sistemas de información existentes en el Ministerio (TI-ESP-001-2026).

Estimado Jerarca:

Un gusto saludarle. Este informe fue elaborado en cumplimiento del Plan Anual de Trabajo 2026, el objetivo principal fue evaluar los controles de acceso y los mecanismos de seguridad implementados en los sistemas de información del Ministerio, con el fin de verificar su conformidad con el marco normativo vigente, identificar vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de la información institucional, y proponer mejoras que fortalezcan la gestión de riesgos tecnológicos y la protección de activos digitales. El estudio abarcó el periodo entre el 01 de enero de 2024 al 31 de diciembre de 2025 y se aplicó en el Ministerio de Vivienda y Asentamientos Humanos, en el Departamento de Tecnologías de Información y Comunicación. No se encontraron limitaciones que afectaran los objetivos o el alcance planificado. La veracidad de la información es responsabilidad de la Administración Activa, mientras que la Auditoría Interna es responsable de emitir una opinión sobre el control interno.

¿Por qué es importante?

Una auditoría de accesos y seguridad informática es fundamental para garantizar que solo el personal autorizado maneje la información sensible del Ministerio. Este proceso mitiga el riesgo de filtraciones, alteraciones o pérdidas de datos críticos mediante la detección temprana de vulnerabilidades en los sistemas. Asimismo, asegura el estricto cumplimiento de las normativas legales vigentes y fortalece la confianza ciudadana en la gestión pública. En última instancia, la revisión continua protege la continuidad operativa y blinda la infraestructura tecnológica institucional contra amenazas digitales internas y externas.

¿Cómo lo Auditamos?

De acuerdo con nuestros objetivos en el desarrollo del estudio de Auditoría, se definieron aspectos relevantes para verificar los controles aplicados en la creación y modificación de cuentas de red y en la asignación de privilegios de acceso a la información, comprobando el cumplimiento del principio de "necesidad de saber", la

**Estudio sobre la revisión de accesos y seguridad de los
sistemas de información existentes en el Ministerio.
TI-ESP-001-2026**

incompatibilidad de funciones y los reportes oportunos de ingresos de personal, para prevenir fugas de información y accesos no autorizados. Además, se evalúa las capacidades de monitoreo de la red, el aseguramiento de la resiliencia tecnológica y la implementación de controles de detección ante posibles ciberataques, revisando la aplicación de actualizaciones permanentes, el análisis de vulnerabilidades y el reporte obligatorio de incidentes al CSIRT-CR y se verifica el mantenimiento de la operatividad de los sistemas y la planificación de recuperación ante contingencias, asegurando la existencia, adopción y prueba de los planes de continuidad operativa y recuperación ante desastres (DRP), para mitigar los impactos por caídas o mal funcionamiento de servicios tecnológicos indispensables.

¿Qué encontramos?

Derivado del análisis realizado, se determinaron oportunidades de mejora en el proceso de administración de la política de contraseñas de los sistemas del MIVAH, ya que presenta debilidades de seguridad al mantener deshabilitada la exigencia de complejidad tecnológica. Esta configuración permisiva faculta a los usuarios el empleo de claves simples¹. Aunque el DTIC administra de forma correcta la creación operativa de credenciales, la falta de parámetros técnicos estrictos compromete la confidencialidad, el secreto y la protección integral de la infraestructura informática. El DTIC presenta oportunidades de mejora en el control, seguimiento y respaldo documental para la atención de las vulnerabilidades del sitio web institucional reportadas por el CSIRT-CR en los años 2024 y 2025. Asimismo, existe una oportunidad de mejora para formalizar el flujo de comunicación interno y alinearse con las mejores prácticas del Decreto N° 45061-MICITT, estableciendo la obligación de reportar de forma inmediata al CSIRT-CR cualquier incidente interno detectado en un plazo máximo de 24 horas. Finalmente, la institución debe mejorar su gestión de continuidad operativa y seguridad informática, ello debido a la falta de actualización, formalización y seguimiento continuo de sus instrumentos técnicos. Específicamente, el Plan de Contingencia base data del año 2011 y, aunque el DTIC ha mostrado proactividad reciente con pruebas específicas, las evaluaciones carecen de un cronograma institucionalizado, simulacros documentados y canales oficiales de comunicación. Por otra parte, el Plan Estratégico de Seguridad Informática se encuentra limitado en su ejecución por la inactividad de la plaza del Oficial de Seguridad Informática ante el Servicio Civil y por la ausencia de manuales, procedimientos y lineamientos operativos esenciales para la estandarización del control interno.

¿Qué sigue?

Para mitigar los riesgos identificados y fortalecer el Sistema de Control Interno de accesos y seguridad de los sistemas de información existentes en el Ministerio, esta Auditoría recomienda lo siguiente:

¹ Contraviniendo de forma directa el Artículo 8, inciso l) del Reglamento de Normas de Uso y Administración de las Tecnologías de Información institucionales.

**Estudio sobre la revisión de accesos y seguridad de los
sistemas de información existentes en el Ministerio.
TI-ESP-001-2026**

A la Jefatura del DTIC: Habilitar y configurar la política de complejidad de contraseñas en los servidores institucionales, obligando al uso combinado de letras mayúsculas, minúsculas, números y caracteres especiales, en alineación con las normativas de ciberseguridad. Implementar un registro formal y centralizado para la gestión de vulnerabilidades de sitio web institucional reportadas por el CSIRT-CR, establecer un procedimiento documentado que contemple las etapas de recepción, análisis, asignación, seguimiento y cierre de las vulnerabilidades, definir responsables y plazos de atención para cada recomendación emitida, mantener evidencia documental que respalde las acciones realizadas e incorporar mecanismos de monitoreo y control periódico, que permitan verificar la efectividad de las medidas implementadas. Además, actualizar integralmente el Plan de Contingencia Institucional conforme a los riesgos cibernéticos y tecnologías actuales, implementar alternativas viables para asumir las funciones especializadas de seguridad informática mientras se resuelve la ocupación de la plaza correspondiente, y consolidar, formalizar y oficializar los manuales y procedimientos operativos necesarios para el cumplimiento del Plan Estratégico de Seguridad Informática y establecer un mecanismo formal para la planificación, ejecución, documentación, evaluación, seguimiento y comunicación de pruebas y simulacros del Plan de Contingencia, que contemple un cronograma, la definición de responsables permanentes, criterios de evaluación estandarizados, el registro documental de los resultados y su comunicación a las partes interesadas para asegurar la mejora continua y la vigencia del plan.

Finalmente, como parte del valor agregado de esta auditoría, y con el fin de robustecer las buenas prácticas operativas actuales, se recomienda a la Jefatura del DTIC implementar las siguientes mejoras administrativas para: establecer un registro centralizado y estandarizado que documente la trazabilidad histórica en la creación de usuarios y la asignación de permisos a carpetas compartidas (formalizadas) y mantener activa una bitácora ininterrumpida que documente la aplicación de las actualizaciones de los sistemas y servidores, garantizando la memoria institucional independientemente de la administración de turno.

Sin otro particular, se despiden atentamente.

RONALD ESTEBAN ARAYA LEANDRO
(FIRMA)

Firmado digitalmente por
RONALD ESTEBAN
ARAYA LEANDRO (FIRMA)
Fecha: 2026.08.14
12:00:12 -06'00'

Ronald Araya Leandro.
Auditor Interno.
RAL.

C:
01 de 05 Sra. Marisol Castro González. Viceministra de Planificación.
02 de 05 Sr. José David Rodríguez Arce. Jefe Despacho Ministerial.
03 de 05 Sr. Andrés Pérez Ulloa, jefe, Departamento de Tecnologías de Información y Comunicación.
04 de 05 Sra. Ashley Chacón Rivera, asesora del Despacho Ministerial de Vivienda y Asentamientos Humanos.
05 de 05 Archivo.