

CIRCULAR
BANHVI-DTI-CI-0009-2025

PARA: Lcda. Ericka Masís Calderón
Asesoría Legal
Lic. Mauricio González Zumbado
Auditoría Interna
Lic. David López Pacheco
Junta Directiva
Licda. Nayudel Montoya Solano
Dirección FONAVI
MBA. Margoth Campos Barrantes
Dirección Administrativa
Lic. Christian Corrales Jiménez
Área de Proveeduría
Licda. Hellen Godínez Jiménez
Área de Recursos Humanos
Lic. José Pablo Durán Rodríguez
Departamento Financiero Contable
Arq. Mariella Salas Rodríguez
Departamento Técnico
Licda. Rita Solano Granados
Oficialía de Cumplimiento
Licda. Merlyn Jiménez Pérez
Unidad de Cumplimiento Normativo
Licda. Ana Julia Fernández Chavarría
Unidad de Tesorería
Licda. Kenlly Vega Ulloa
Unidad de Riesgos
Licda. Magaly Longhan Moya
Unidad de Planificación
Lic. Ronald Espinoza Ávila
Unidad de Comunicaciones

DE: MGT. Genaro Fuentes Abarca
Jefe, Departamento de Tecnologías de Información

ASUNTO: **Uso de Asistentes Virtuales**

FECHA: 01 de octubre de 2025

Reciban un cordial saludo. En atención a diversas consultas recibidas sobre asistentes virtuales, en especial acerca de Read AI, el Departamento de TI se dio a la tarea de realizar un análisis integral, haciendo hincapié en la seguridad y privacidad de los datos. Este tipo de herramientas se integran con plataformas como Teams y Zoom, y su función principal es crear transcripciones y resúmenes automáticos de reuniones virtuales

A pesar de contar con muchos aspectos positivos, tales como la automatización en la toma de notas, resumir reuniones, encontrar de manera más rápida información relevante en

grabaciones o mensajes, además de la integración con varias aplicaciones, es importante considerar los riesgos que podría conllevar un uso incorrecto.

El análisis realizado por el DTI se centró en la herramienta Read AI, desarrollada por la empresa estadounidense Read AI, Inc. No obstante, las conclusiones obtenidas pueden aplicarse a otros asistentes virtuales similares. A continuación, se detallan los principales puntos:

- La herramienta podría comprometer la información institucional más sensible si no se trata adecuadamente. Por ejemplo: grabaciones sin consentimiento, exposición de información sensible o confidencial, accesos no autorizados a grabaciones, resúmenes o notas, filtración de datos voluntaria o involuntaria, entre otros.
- Uso sin consentimiento explícito: en algunos casos la herramienta puede estar presente en reuniones sin que todos los participantes sean debidamente informados, lo cual podría generar molestias, e incluso implicaciones legales, si se graba o transcribe sin el consentimiento previo de las personas involucradas.
- Aunque los datos se almacenen de forma cifrada, siempre existirá el riesgo de exposición por vulnerabilidades técnicas, errores de configuración o ataques internos.
- A pesar de no ser un riesgo relacionado directamente con la privacidad de los datos, es importante señalar que muchas de las transcripciones generadas no son 100% precisas, ya que pueden verse afectadas por factores como acentos, ruidos o superposición de voces, lo que podría dar lugar a interpretaciones erróneas.
- Los datos en reposo se almacenan en AWS (Amazon Web Services), en la región este de Estados Unidos, sitio en la nube en el que el BANHVI no mantiene una cuenta, contrato de soporte, SLAs¹ acuerdos de confidencialidad u otros controles similares que garanticen la confidencialidad y disponibilidad de la información.
- Si bien es cierto el tratamiento principal de los datos obtenidos corresponde a la generación de resúmenes, notas y puntos importantes a través de las grabaciones, los mismos, en especial las notas y los audios, son utilizados por el proveedor para entrenar y mejorar la herramienta a través del aprendizaje virtual (machine learning).
- En caso de no adquirir un plan de pago, Read AI u otras herramientas similares, solicitan una cantidad considerable de permisos, incluyendo acceso al calendario, cámara, micrófono, video, acceso a archivos y extensiones del navegador.
- Muchos de los permisos mencionados anteriormente son innecesarios para el funcionamiento básico de la herramienta, pudiendo desencadenar eventos que pongan en riesgo la privacidad de los datos institucionales, como filtración de información confidencial, vigilancia no autorizadas o vulnerabilidades de seguridad.
- Los planes gratuitos no se consideran adecuados para entornos empresariales, ya que no existirá soporte oficial ni responsabilidad por parte del fabricante de la herramienta.

Con el fin de garantizar la seguridad de la información, se deshabilitará la herramienta Read AI en las cuentas de Microsoft Teams. Asimismo, se solicita que, en las reuniones con externos donde esta herramienta se encuentre habilitada, se proceda a desactivarla.

¹Es un documento formal entre un proveedor de servicios y un cliente que establece los niveles esperados de servicio. Su objetivo es garantizar que el proveedor cumpla ciertos estándares de calidad, disponibilidad y tiempos de respuesta.

Finalmente, se insta a utilizar las herramientas institucionales autorizadas, tales como:

- Microsoft Teams, para la grabación y transcripción de reuniones, ya que ofrece funcionalidades integradas que cumplen con los lineamientos de seguridad y privacidad.
- Copilot, como solución basada en inteligencia artificial para la generación de ideas y apoyo en tareas de productividad.

Cualquier consulta al respecto quedo a disposición de ustedes.

GFA/jag/maa*//

c.e.: Lic. Dagoberto Hidalgo Cortés, Gerente General
 Lic. Carlos Castro Miranda, Gerencia General
 MBA. Tricia Hernández Brenes, Subgerencia Financiera
 MBA. Walter Muñoz Caravaca, Sugerencia Operativa