



DESPACHO MINISTERIAL
Página 1 de 4

CIRCULAR

MICITT-DM-CIRC-008-2026

Fecha:	10 de julio, 2026
Para:	Personas funcionarias, contratistas y terceros con acceso a los activos de información Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
De:	Antonette Williams Barnett Ministra a.i. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
Asunto:	Comunicación oficial y entrada en vigor de la Política de Seguridad de la Información y Ciberseguridad del MICITT (Código MICITT-DGDCFD-PSI-V.01, Versión 1.0)

Estimadas personas funcionarias, contratistas y terceros:

Reciban un cordial saludo. Por este medio se comunica de manera oficial la aprobación y entrada en vigor de la Política de Seguridad de la Información y Ciberseguridad del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), identificada con el código MICITT-DGDCFD-PSI-V.01, Versión 1.0, de fecha 15 de febrero de 2026, elaborada por la Dirección de Ciberseguridad.

Esta Política establece las directrices, principios, roles y responsabilidades necesarios para proteger la confidencialidad, integridad y disponibilidad de la información y de los activos tecnológicos del MICITT, en línea con las buenas prácticas nacionales e internacionales en la materia (INTE/ISO/IEC 27001, INTE/ISO/IEC 27002, COBIT® 2019, NIST SP 800-53, entre otras) y con el marco normativo costarricense aplicable, incluyendo la Ley General de Control Interno N.º 8292, la Ley de Protección de la Persona frente al tratamiento de sus datos personales N.º 8968 y el Decreto Ejecutivo N.º 45061, Reglamento para la Gobernanza en Ciberseguridad y la Resiliencia Cibernética de las Instituciones Gubernamentales.

1. Alcance

La Política es de acatamiento obligatorio para todas las personas colaboradoras, contratistas, terceros y partes interesadas que tengan acceso, temporal o indefinido, a los activos de información del MICITT (hardware, software, redes, sistemas, datos y toda



CIRCULAR

MICITT-DM-CIRC-008-2026

información generada, procesada, almacenada o transmitida por la Institución), independientemente del medio o formato en que se encuentre.

2. Objetivos principales

Entre otros propósitos, la Política busca fortalecer la resiliencia y seguridad de la infraestructura digital institucional; definir con claridad los roles y responsabilidades en materia de seguridad de la información y ciberseguridad; implementar controles técnicos, físicos y administrativos que mitiguen los riesgos correspondientes; fomentar una cultura institucional de seguridad de la información; asegurar el cumplimiento legal, normativo y contractual aplicable; y fortalecer el Sistema de Control Interno del MICITT en estas materias.

3. Obligaciones inmediatas del personal

Con el fin de garantizar la adecuada implementación de la Política, se solicita a cada Dirección y Jefatura instruir a su personal sobre los siguientes puntos, que aplican a todo colaborador, contratista y tercero con acceso a activos de información del MICITT:

Instancia	Responsabilidad principal	Plazo
Todo el personal, incluido el de nuevo ingreso	Conocer, comprender y firmar la declaración de conocimiento de la Política, así como las declaraciones de confidencialidad y no divulgación de información, para su resguardo en el expediente personal.	Según coordinación con Recursos Humanos
Titulares subordinados y jefaturas	Garantizar la implementación de los controles de seguridad de la información y ciberseguridad en su unidad, y reportar de forma oportuna cualquier vulnerabilidad o incumplimiento detectado.	Permanente
Personas colaboradoras	Velar por la protección física y lógica de los activos de información asignados, usar	Permanente

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones

200 metros Oeste de Casa Presidencial, Edificio MIRA

Tel. 2539-2270

despacho.ministerial@micitt.go.cr



CIRCULAR

MICITT-DM-CIRC-008-2026

	únicamente software y herramientas autorizadas por la Unidad de Servicios Tecnológicos, y reportar cualquier evento o incidente de seguridad de la información o ciberseguridad al superior inmediato y a la Dirección de Ciberseguridad.	
Proveedores y personal externo (outsourcing)	Suscribir el acuerdo de confidencialidad correspondiente cuando tengan acceso a información confidencial o sensible, con vigencia de hasta tres años posteriores a la finalización de los trabajos.	Previo al acceso a la información

4. Gestión de incidentes

Se recuerda que cualquier evento que transgreda lo dispuesto en la Política constituye un incidente de seguridad de la información y debe ser informado de inmediato al superior jerárquico y notificado a la Dirección de Ciberseguridad, siguiendo los protocolos de actuación definidos para este tipo de eventos.

5. Consultas y disponibilidad del documento

El texto completo de la Política de Seguridad de la Información y Ciberseguridad (MICITT-DGDCFD-PSI-V.01) se encuentra disponible para consulta de todo el personal a través de los canales institucionales habituales. Las consultas sobre su alcance o aplicación pueden dirigirse a la Dirección de Ciberseguridad.

El incumplimiento de lo dispuesto en esta Política dará lugar a la aplicación de las sanciones disciplinarias establecidas en la normativa vigente, sin perjuicio de las responsabilidades civiles, penales o de otra índole que pudieran derivarse, de conformidad con el artículo 39 de la Ley General de Control Interno.



DESPACHO MINISTERIAL

Página 4 de 4

CIRCULAR

MICITT-DM-CIRC-008-2026

Se agradece la atención y el compromiso de todas las personas funcionarias, contratistas y terceros con el cumplimiento de esta Política, fundamental para la protección de la información institucional y de los servicios que el MICITT brinda a la ciudadanía.

Cordialmente,



Antonette Williams Barnett

Ministra a.i.

Despacho Ministerial

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones

200 metros Oeste de Casa Presidencial, Edificio MIRA

Tel. 2539-2270

despacho.ministerial@micitt.go.cr