

Escuela Militar de Ingeniería

“Mcal. Antonio José de Sucre”



RAC – 17

REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

2026



RESOLUCIÓN DEL CONSEJO SUPERIOR ACADÉMICO RCSA REG. N° 023/2026

La Paz, 8 de septiembre de 2026

VISTOS Y CONSIDERANDO:

Que, la Escuela Militar de Ingeniería creada mediante Ley N° 286 de 10 de noviembre de 1950, tiene como Misión, formar y especializar profesionales de excelencia, con valores éticos, morales y cívicos; caracterizados por su Responsabilidad, Liderazgo y Disciplina.

Que, el Estatuto Orgánico de la EMI aprobado mediante Resolución del Consejo Superior de Decisiones N° RCSD 003/2021 de 22 de abril de 2021, en su Título III Capítulo III, determina en su Artículo 25: "El Consejo Superior Académico es el máximo órgano de dirección y gobierno de la Escuela Militar de Ingeniería "Mcal. Antonio José de Sucre" - EMI, donde se debaten y aprueban regularizaciones de orden académico disciplinario, administrativo, financiero y jurídico de la institución a nivel de Grado y Posgrado" III Artículo 29° del mismo Estatuto, establece dentro de las atribuciones del Consejo Superior Académico: "(...) a. Aprobar los reglamentos y la normativa interna en general de la Escuela Militar de Ingeniería "Mcal. Antonio José de Sucre" - EMI. d. Emitir resoluciones que faciliten la administración académica disciplinaria, administrativa, financiera y jurídica".

Que, mediante INFORME DE NECESIDAD EMI-DNTIC-INF. N° 188/2026 de fecha Agosto 18 de 2026, el Director Nacional de Tecnologías de Información y Comunicación CONCLUYE y RECOMIENDA lo siguiente: "III.- CONCLUSIONES. A.- La Escuela Militar de Ingeniería requiere contar un Reglamento de Tecnologías de Información y Comunicación que regule de manera integral la gestión tecnológica institucional. B.- La aprobación del Reglamento permitirá fortalecer la gobernanza digital, la seguridad de la información, la gestión de datos, el desarrollo de sistemas informáticos y la transformación digital institucional. C.- El Reglamento constituye un instrumento normativo necesario para establecer responsabilidades, controles y procedimientos relacionados con el uso y administración de las Tecnologías de Información y Comunicación en la EMI. D.- Su aprobación contribuirá al cumplimiento de los objetivos institucionales establecidos en el Plan de Desarrollo Universitario y a la mejora continua de los procesos académicos, administrativos y tecnológicos"/// IV. RECOMENDACIONES. A.- Aprobar el Reglamento de Tecnologías de Información y Comunicación de la Escuela Militar de Ingeniería "Mcal. Antonio José de Sucre", elaborado por la Dirección Nacional de Tecnologías de Información y Comunicación. B.- Remitir el proyecto de Reglamento a las instancias institucionales correspondientes para su revisión y consideración dentro del procedimiento de aprobación establecido por la normativa interna de la EMI. C.- Disponer su posterior socialización e implementación en todas las unidades organizacionales de la institución".

Que, mediante INFORME TECNICO EMI - DNP. - INF. N° 111/2026 de fecha agosto 21 de 2026, elaborado por el Director Nacional de Planificación, CONCLUYE y RECOMIENDA señalando textualmente: "III.- CONCLUSIONES. Se procedió a la revisión y análisis del proyecto del Reglamento de Tecnologías de Información y Comunicación elaborado por el Tcnl. DIM. Cristian Mauricio Altamirano Martínez, Director Nacional de Tecnologías de Información y Comunicación, el mismo tiene un respaldo normativo interno en actual vigencia y se encuentra coherente para su aprobación, de acuerdo a exigencias administrativas de la Escuela Militar de Ingeniería "Mcal. Antonio José de Sucre"/// IV. RECOMENDACIONES. Es pertinente el proyecto del Reglamento de Tecnologías de Información y Comunicación, el cual se denomina RAC-17; el cual tiene una estructura compuesta por 9 Capítulos, 47 Artículos y 2 Anexos (...)".

H.T. 30 0805



**RESOLUCIÓN DEL CONSEJO SUPERIOR ACADÉMICO
RCSA REG. N° 023/2026**

La Paz, 8 de septiembre de 2026

Que, la Dirección Nacional Jurídica mediante INFORME EMI-DNJ-INF. LEGAL N° 263/2026 de fecha 2 de septiembre de 2026, establece en sus Conclusiones que la propuesta de Reglamento Académico RAC-17 "Reglamento Tecnologías de Información y Comunicación", de la Escuela Militar de Ingeniería "Mcal. Antonio José de Sucre", no transgrede ninguna normativa legal vigente. Asimismo, recomienda que los antecedentes e Informes emitidos sean derivados a Secretaría General de la Escuela Militar de Ingeniería para la proyección de la Resolución del Consejo Superior Académico aprobando la propuesta de Reglamento Académico RAC-17 "Reglamento de Tecnologías de Información y Comunicación" de la EMI sugerida en el INFORME DE NECESIDAD EMI-DNTIC-INF. N° 188/2026 de fecha Agosto 18 de 2026 emitido por el Director Nacional de Tecnologías de Información y Comunicación.

Que, reunidos los miembros del Consejo Superior Académico, con la finalidad de dar una solución a la problemática planteada, tuvieron a bien considerar disponer la elaboración de la Resolución correspondiente.

POR TANTO:

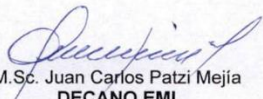
**EL CONSEJO SUPERIOR ACADÉMICO EN USO DE LAS
ATRIBUCIONES PREVISTAS EN LAS DISPOSICIONES
REGLAMENTARIAS VIGENTES,**

RESUELVE:

Artículo Primero.- Aprobar y poner en vigencia el "REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN" RAC-17 de la Escuela Militar de Ingeniería "Mcal. Antonio José de Sucre", compuesta por 9 (nueve) Capítulos, 47 (cuarenta y siete) Artículos y 2 (dos) anexos, sugerida mediante INFORME DE NECESIDAD EMI-DNTIC-INF. N° 188/2026 de fecha Agosto 18 de 2026 emitido por el Director Nacional de Tecnologías de Información y Comunicación.

Artículo Segundo.- Quedan encargados de la ejecución y cumplimiento de la presente Resolución, el Vicerrectorado de Grado, Decanato, Direcciones Nacionales, Direcciones de las Unidades Académicas, Direcciones del Tecnológico y Unidades Organizacionales de la Escuela Militar de Ingeniería "Mcal. Antonio José de Sucre".

Regístrese, Comuníquese y Archívese.


M.Sc. Juan Carlos Patzi Mejía
DECANO EMI

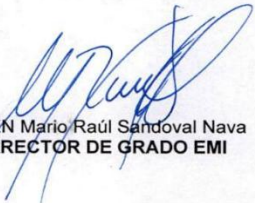

Cnl. DAEN Augusto Cossio Alvarez
VICERRECTOR DE POSGRADO EMI

COMANDO GENERAL DEL EJÉRCITO
ESCUELA MILITAR DE INGENIERÍA
"Mcal. ANTONIO JOSÉ DE SUCRE"
BOLIVIA



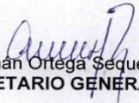
**RESOLUCIÓN DEL CONSEJO SUPERIOR ACADÉMICO
RCSA REG. N° 023/2026**

La Paz, 8 de septiembre de 2026


Cnl. DAEN Mario Raúl Sandoval Nava
VICERRECTOR DE GRADO EMI


Gral. Brig. Jhonny Antezana Cáceres
RECTOR
ESCUELA MILITAR DE INGENIERÍA

Es Conforme


Ing. Renán Ortega Sequeros
SECRETARIO GENERAL

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

ÍNDICE

CAPÍTULO I	1
DISPOSICIONES GENERALES	1
ARTÍCULO 1º. OBJETO.....	1
ARTÍCULO 2º. FINALIDAD	1
ARTÍCULO 3º. ALCANCE	2
ARTÍCULO 4º. MARCO LEGAL Y NORMATIVO	2
ARTÍCULO 5º. DEFINICIONES	5
ARTÍCULO 6º. PRINCIPIOS RECTORES TIC	10
CAPÍTULO II	12
GOBERNANZA Y GESTIÓN DE LA INFORMACIÓN INSTITUCIONAL	12
ARTÍCULO 7º. GOBERNANZA TIC INSTITUCIONAL.....	12
ARTÍCULO 8º. RESPONSABILIDAD FUNCIONAL DEL DATO Y ADMINISTRACIÓN TECNOLÓGICA	13
ARTÍCULO 9º. COMITÉ INSTITUCIONAL DE GOBIERNO DIGITAL Y SEGURIDAD DE LA INFORMACIÓN	15
ARTÍCULO 10º. POLITICAS DE CONTROL DE ACCESO Y GESTIÓN DE IDENTIDADES.....	16
ARTÍCULO 11º. CLASIFICACIÓN DE LA INFORMACIÓN.....	18
ARTÍCULO 12º. AUDITORÍA Y TRAZABILIDAD.....	20
ARTÍCULO 13º. GOBIERNO DE DATOS INSTITUCIONAL	21
ARTÍCULO 14º. PROTECCIÓN DE DATOS PERSONALES, PRIVACIDAD Y TRATAMIENTO DE INFORMACIÓN SENSIBLE	23
ARTÍCULO 15º. CIUDADANÍA DIGITAL Y VALIDACIÓN ELECTRÓNICA	26
ARTÍCULO 16º. FIRMA DIGITAL Y FIRMA DIGITALIZADA	27
CAPÍTULO III	30
GESTIÓN DE ACTIVOS DE INFORMACIÓN	30
ARTÍCULO 17º. GESTIÓN DE ACTIVOS DE INFORMACIÓN.....	30
ARTÍCULO 18º. INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN	30
ARTÍCULO 19º. PROPIEDAD Y CUSTODIA DE LOS ACTIVOS DE INFORMACIÓN	31

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

ARTÍCULO 20º.	ETIQUETADO Y MANEJO DE LA INFORMACIÓN.	31
ARTÍCULO 21º.	USO ACEPTABLE DE ACTIVOS TECNOLÓGICOS	32
ARTÍCULO 22º.	DEVOLUCIÓN DE ACTIVOS INSTITUCIONALES.	32
ARTÍCULO 23º.	DISPOSICIÓN FINAL Y ELIMINACIÓN SEGURA DE ACTIVOS Y MEDIOS DE ALMACENAMIENTO	33
CAPÍTULO IV		34
POLÍTICAS DE INGENIERÍA DE SOFTWARE Y SOPORTE TECNOLÓGICO		34
ARTÍCULO 24º.	USO DE SERVICIOS WEB, NUBE Y CORREO INSTITUCIONAL	34
ARTÍCULO 25º.	SOPORTE TECNOLÓGICO Y MESA DE SERVICIOS	36
ARTÍCULO 26º.	GESTIÓN DE SERVICIOS TIC (SLA, CATÁLOGO, INCIDENTES)	38
ARTÍCULO 27º.	SISTEMAS ACADÉMICOS Y RESTRICCIONES ESPECIALES	40
CAPÍTULO V		42
CIBERSEGURIDAD, INFRAESTRUCTURA Y CONTINUIDAD OPERATIVA		42
ARTÍCULO 28º.	POLÍTICAS DE CIBERSEGURIDAD	42
ARTÍCULO 29º.	USO Y SALVAGUARDA DE LA INFRAESTRUCTURA	44
ARTÍCULO 30º.	GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	46
ARTÍCULO 31º.	GESTIÓN DE INCIDENTES Y CONTINUIDAD	46
CAPÍTULO VI		49
DESARROLLO DE SISTEMAS INFORMÁTICOS		49
ARTÍCULO 32º.	REGULACIÓN DEL CICLO DE DESARROLLO E IMPLEMENTACIÓN	49
ARTÍCULO 33º.	NORMAS DE DESARROLLO	51
ARTÍCULO 34º.	NORMAS PARA DISEÑO DE BASE DE DATOS	53
ARTÍCULO 35º.	NORMAS DE SEGURIDAD EN EL DESARROLLO	55
ARTÍCULO 36º.	NORMAS DE CALIDAD DE SOFTWARE	57
ARTÍCULO 37º.	NORMAS DE IMPLEMENTACIÓN	59
ARTÍCULO 38º.	ARQUITECTURA TECNOLÓGICA	61
ARTÍCULO 39º.	PROHIBICIONES	63

CAPÍTULO VII.....	66
CUMPLIMIENTO, CONTROL Y CAPACITACIÓN.....	66
ARTÍCULO 40°. PROHIBICIONES	66
ARTÍCULO 41°. SUPERVISIÓN Y AUDITORÍA TIC	67
ARTÍCULO 42°. CAPACITACIÓN Y CONCIENTIZACIÓN TECNOLÓGICA.....	69
CAPÍTULO VIII.....	71
RESPONSABILIDADES E INCUMPLIMIENTOS.....	71
ARTÍCULO 43°. RESPONSABILIDADES	71
ARTÍCULO 44°. TIPIFICACIÓN DE FALTAS INFORMÁTICAS.....	72
ARTÍCULO 45°. MEDIDAS SANCIONATORIAS	75
CAPÍTULO IX.....	78
DISPOSICIONES FINALES.....	78
ARTÍCULO 46°. ACTUALIZACIÓN NORMATIVA.....	78
ARTÍCULO 47°. VIGENCIA.....	79
ANEXO A	82
FORMULARIO DE REQUERIMIENTO PARA DESARROLLO, MEJORA O INTEGRACIÓN DE SISTEMAS	82
ANEXO B	86
FORMULARIO DE SOPORTE TÉCNICO	86

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

CAPÍTULO I DISPOSICIONES GENERALES

Artículo 1º.OBJETO

El presente Reglamento tiene por objeto normar la planificación, implementación, administración, integración, operación, control y mejora continua de las Tecnologías de Información y Comunicación (en adelante TIC) en la Escuela Militar de Ingeniería “Mcal. Antonio José de Sucre” (en adelante EMI), estableciendo los lineamientos, principios, normas técnicas, responsabilidades y mecanismos de control para la gestión de sistemas informáticos, infraestructura tecnológica, servicios digitales, ciberseguridad, desarrollo de software, gobierno de datos y transformación digital institucional.

Artículo 2º.FINALIDAD

La finalidad del presente Reglamento es garantizar que la gestión de las TIC en la EMI sea eficiente, segura, interoperable, sostenible y orientada a resultados, contribuyendo al fortalecimiento de la gobernanza digital, la protección de la información institucional, la continuidad operativa y la toma de decisiones basada en datos.

Asimismo, busca coadyuvar a la transformación digital institucional mediante la implementación de sistemas integrados, servicios digitales confiables y el uso adecuado de tecnologías, en cumplimiento del marco normativo nacional vigente en materia de telecomunicaciones, tecnologías de información, gobierno y ciudadanía digitales y en alineación con el Plan Estratégico Institucional (PEI), el Modelo Académico institucional y los objetivos estratégicos de la EMI.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Artículo 3º.ALCANCE

Las disposiciones establecidas en el presente Reglamento son de cumplimiento obligatorio para todas las unidades organizacionales de la EMI, así como para el personal militar, personal civil, docentes, estudiantes, investigadores, administrativos, operadores de sistemas, técnicos, usuarios autorizados y cualquier persona natural o jurídica que, en el ejercicio de sus funciones o actividades, haga uso, gestione, administre, desarrolle, mantenga o tenga acceso a los sistemas informáticos, infraestructura tecnológica, redes, servicios digitales y recursos TIC institucionales.

Asimismo, el presente Reglamento es aplicable a todas las plataformas tecnológicas institucionales, sistemas académicos, administrativos y financieros, servicios en la nube, bases de datos, medios digitales, dispositivos informáticos, redes de comunicación, servicios de correo institucional, mecanismos de intercambio de información, procesos digitales y demás activos de información que sean parte o soporte de la gestión institucional de la EMI.

El cumplimiento de este Reglamento se extenderá, cuando corresponda, a proveedores, contratistas, consultores y terceros que desarrollen, implementen o interactúen con soluciones tecnológicas institucionales, quienes deberán sujetarse a las políticas, normas técnicas y procedimientos establecidos por la Dirección Nacional de Tecnologías de Información y Comunicación (en adelante DNTIC), en concordancia con la normativa nacional vigente.

Artículo 4º.MARCO LEGAL Y NORMATIVO

El presente Reglamento se fundamenta y se rige por la normativa legal vigente del Estado Plurinacional de Bolivia, así como por la

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

normativa interna de la EMI, constituyendo su marco de referencia para la gestión de las TIC.

En tal sentido, el presente Reglamento se encuentra alineado, entre otros, con los siguientes instrumentos normativos:

a) Marco Constitucional y Legal General:

- Constitución Política del Estado;
- Ley N° 164 de 08 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación;
- Ley N° 1080 de 11 de julio de 2018, Ley de Ciudadanía Digital;
- Ley N° 777 de 21 de enero de 2016, Ley del Sistema de Planificación Integral del Estado (SPIE).

b) Reglamentación y normativa complementaria en materia TIC y gobierno digital:

- Decreto Supremo N° 1391 de 24 de octubre de 2012, Reglamento General a la Ley N° 164;
- Decreto Supremo N° 1793 de 13 de noviembre de 2013, Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, incluyendo firma digital, software libre y gobierno electrónico;
- Decreto Supremo N° 3251 de 12 de julio de 2017, relativo a la implementación de gobierno electrónico, interoperabilidad, software libre y estándares abiertos;
- Decreto Supremo N° 3525 de 04 de abril de 2018, que regula el gobierno digital, el uso de portales del Estado, interoperabilidad, archivo y tramitación digital;
- Decreto Supremo N° 4326 de 07 de septiembre de 2020, referente al régimen de infracciones y sanciones en el sector

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

de telecomunicaciones y TIC.

c) Entidades regulatorias, lineamientos y normas técnicas:

- Disposiciones, lineamientos, estándares técnicos y resoluciones emitidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT);
- Lineamientos técnicos, servicios digitales, estándares de interoperabilidad, firma digital, ciudadanía digital y demás directrices emitidas por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC).

d) Normativa institucional y planificación estratégica:

- Estatuto Orgánico de la Escuela Militar de Ingeniería “Mcal. Antonio José de Sucre”;
- Plan Estratégico Institucional (PEI);
- Reglamentos Académicos y Administrativos vigentes (RAC y RAD);
- Manual de Organización y Funciones (MOF);
- Manual de Puestos (MP);
- Políticas, directrices y disposiciones internas emitidas por la EMI en materia de Tecnologías de Información y Comunicación.

e) Buenas prácticas y estándares de referencia:

- Estándares y marcos de buenas prácticas internacionales aplicables a la gestión TIC, tales como ISO/IEC 27001 (Seguridad de la Información), ISO/IEC 20000 (Gestión de Servicios TI), COBIT (Gobernanza de TI) y ITIL (Gestión de Servicios TI), en la medida que sean adoptados por la institución;
- En caso de conflicto o vacío normativo, se aplicará de forma

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

supletoria la normativa de mayor jerarquía del ordenamiento jurídico nacional y los principios de legalidad, seguridad de la información, interoperabilidad y continuidad operativa.

f) Normativa y estándares técnicos de referencia:

La gestión de las TIC podrá apoyarse en estándares internacionales reconocidos, entre ellos:

- ISO/IEC 27001:2022 Sistemas de Gestión de Seguridad de la Información;
- ISO/IEC 27002:2022 Controles de Seguridad de la Información;
- ISO/IEC 27005 Gestión de Riesgos de Seguridad de la Información;
- ISO 22301 Sistema de Gestión de la Continuidad del Negocio;
- ISO/IEC 20000 Sistemas de Gestión de Servicios TIC;
- COBIT 2019 para Gobierno y Gestión de TI;
- ITIL 4 para Gestión de Servicios;
- OWASP ASVS y OWASP Top 10 para desarrollo seguro;
- NIST Cybersecurity Framework (CSF 2.0);
- NIST SP 80-53 Rev. 5.

Artículo 5º. DEFINICIONES

Para efectos de aplicación del presente Reglamento, se adoptan las siguientes definiciones:

Acceso Privilegiado: Nivel de acceso avanzado que permite administrar sistemas o infraestructura.

Activo de Información: Todo recurso que tiene valor para la

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

institución y que soporta la información, incluyendo datos, sistemas, infraestructura tecnológica, aplicaciones, servicios digitales, dispositivos, documentación y personal.

Administración Tecnológica: Conjunto de actividades orientadas a la planificación, implementación, operación, mantenimiento, monitoreo y control de los recursos tecnológicos institucionales.

API (Interfaz de Programación de Aplicaciones): Mecanismo que permite la integración e interoperabilidad entre sistemas.

Área Usuaría: Unidad organizacional responsable funcional de un proceso institucional y de la generación, validación, actualización, integridad y uso de la información que administra a través de sistemas institucionales.

Autenticación: Proceso mediante el cual se verifica la identidad de un usuario para acceder a un sistema.

Autorización: Proceso mediante el cual se otorgan permisos a un usuario para realizar acciones en un sistema.

Backup (Respaldo): Copia de seguridad de la información que permite su recuperación en caso de pérdida o incidente.

Base de Datos: Conjunto estructurado de datos organizados y almacenados de forma digital, diseñados para facilitar su acceso, gestión, consulta, actualización y control.

Ciberseguridad: Conjunto de políticas, controles, procedimientos y tecnologías orientadas a proteger los sistemas, redes, infraestructura y datos institucionales frente a amenazas, vulnerabilidades e incidentes informáticos.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Ciudadanía Digital: Mecanismo mediante el cual las personas ejercen derechos y obligaciones a través del uso de las TIC en su interacción con entidades públicas y privadas, mediante autenticación digital segura y servicios electrónicos.

Continuidad Operativa: Capacidad de mantener servicios tecnológicos en funcionamiento ante incidentes o fallas.

Control de Accesos: Conjunto de mecanismos que regulan quién puede acceder a los sistemas y datos.

Dato: Representación básica de información susceptible de ser procesada, almacenada y transmitida por medios digitales.

Dato en Reposo: Información digital almacenada en medios físicos o virtuales de manera permanente o temporal.

Dato en Tránsito: Información digital que se encuentra en proceso de transmisión a través de redes de comunicación.

Desarrollo de Software: Proceso estructurado que comprende el análisis, diseño, programación, pruebas, implementación, mantenimiento y mejora de sistemas informáticos.

DNTIC: Dirección Nacional de Tecnologías de Información y Comunicación de la EMI, responsable de la gestión tecnológica institucional.

Firma Digital: Mecanismo criptográfico que permite autenticar la identidad de una persona y garantizar la integridad y validez jurídica de un documento electrónico, equivalente a la firma manuscrita.

Firma Digitalizada: Es la representación gráfica de una firma manuscrita obtenida mediante escaneo u otro medio de

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

digitalización, incorporada en un documento electrónico, la cual no constituye, por sí misma, un mecanismo criptográfico de validación de identidad ni garantiza la integridad del documento.

Gobierno de Datos: Conjunto de políticas, procesos y responsabilidades orientadas a la gestión adecuada de los datos institucionales, garantizando su calidad, integridad, disponibilidad, seguridad y uso estratégico.

Gobierno Digital: Uso estratégico de las Tecnologías de Información y Comunicación para mejorar la gestión institucional, la prestación de servicios y la interacción con los usuarios, promoviendo eficiencia, transparencia e interoperabilidad.

Incidente de Seguridad: Evento que compromete la confidencialidad, integridad o disponibilidad de la información.

Incidente Informático: Evento o conjunto de eventos que afectan o pueden afectar la seguridad, disponibilidad, integridad o confidencialidad de los sistemas o la información institucional.

Interoperabilidad: Capacidad de los sistemas y aplicaciones para intercambiar información y utilizarla de manera eficiente, permitiendo la integración de procesos y servicios entre diferentes plataformas tecnológicas.

Infraestructura Tecnológica: Conjunto de recursos físicos y lógicos que soportan la operación de los sistemas informáticos, incluyendo servidores, redes, centros de datos, equipos de comunicación y dispositivos.

Pasarela de Pagos del Estado: Conjunto de servicios tecnológicos que permiten la automatización de transacciones electrónicas entre los usuarios y entidades públicas para el pago de servicios o trámites

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

mediante medios digitales seguros.

Servicios Digitales: Servicios prestados mediante tecnologías de información que permiten la interacción, gestión y acceso a procesos institucionales de forma electrónica.

Software Libre: Software cuyo código fuente es accesible, permitiendo su uso, modificación y distribución, conforme a estándares abiertos y a políticas de soberanía tecnológica del Estado.

Sistema Informático: Conjunto integrado de componentes tecnológicos, aplicaciones, datos y procedimientos que permiten el procesamiento de información para apoyar la gestión institucional.

Sistema Integrado de Gestión (SIGA-EMI): Plataforma tecnológica institucional que integra los sistemas académicos, administrativos y financieros, orientada a la automatización, interoperabilidad y gestión eficiente de los procesos institucionales.

SLA (Service Level Agreement) (Acuerdo de Nivel de Servicio): Compromiso formal que establece los niveles de atención, disponibilidad y respuesta de los servicios TIC.

Trazabilidad: Capacidad de registrar y rastrear las acciones realizadas en los sistemas.

Usuario: Persona autorizada que accede a sistemas, plataformas o recursos tecnológicos institucionales, en el marco de sus funciones o actividades.

Usuario Privilegiado: Usuario con permisos elevados de administración sobre sistemas o infraestructura tecnológica.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Vulnerabilidad: Debilidad en un sistema que puede ser explotada para comprometer la seguridad.

Artículo 6º. PRINCIPIOS RECTORES TIC

La gestión de las TIC en la EMI se regirá por los siguientes principios:

- a) **Alineación Estratégica:** Las TIC deberán contribuir directamente al cumplimiento de los objetivos institucionales definidos en el Plan Estratégico Institucional PEI y demás instrumentos de planificación estratégica.
- b) **Gestión por Resultados:** La implementación y uso de las TIC estarán orientados a la mejora continua de los procesos institucionales, la eficiencia operativa y la generación de valor para la gestión académica, administrativa y de apoyo.
- c) **Interoperabilidad:** Los sistemas y plataformas tecnológicas deberán integrarse y compartir información de manera eficiente, garantizando la compatibilidad y articulación entre los distintos procesos institucionales, en concordancia con las políticas nacionales de gobierno digital.
- d) **Seguridad de la Información:** La gestión TIC deberá garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional, mediante la implementación de políticas, controles y medidas de seguridad adecuadas.
- e) **Gobierno de Datos:** Los datos institucionales deberán ser gestionados de forma estructurada, segura, íntegra y oportuna, asegurando su calidad, disponibilidad y uso estratégico para la toma de decisiones.
- f) **Soberanía Tecnológica:** Se promoverá el uso de software libre,

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

estándares abiertos y soluciones tecnológicas que fortalezcan la autonomía tecnológica institucional, en concordancia con la normativa nacional vigente.

- g) Estandarización Tecnológica:** La implementación de soluciones tecnológicas deberá sujetarse a estándares técnicos institucionales que garanticen uniformidad, compatibilidad, sostenibilidad y facilidad de mantenimiento.
- h) Acceso Controlado y Responsabilidad Funcional:** El acceso a sistemas y datos institucionales se realizará bajo principios de control, autorización y trazabilidad, siendo las áreas usuarias responsables de la gestión funcional de la información y la DNTIC responsable de la administración tecnológica.
- i) Continuidad Operativa:** Los servicios tecnológicos institucionales deberán garantizar su disponibilidad y capacidad de recuperación ante fallas, incidentes o contingencias, asegurando la continuidad de las operaciones institucionales.
- j) Transformación Digital:** Las TIC deberán consolidarse como un eje estratégico para la modernización institucional, mediante la automatización de procesos, la digitalización de servicios y el fortalecimiento del gobierno digital.
- k) Cumplimiento Normativo:** Toda gestión TIC deberá desarrollarse en estricto cumplimiento de la normativa nacional vigente en materia de telecomunicaciones, tecnologías de información, gobierno digital y seguridad de la información, así como de la normativa interna de la EMI.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

CAPÍTULO II GOBERNANZA Y GESTIÓN DE LA INFORMACIÓN INSTITUCIONAL

Artículo 7º. GOBERNANZA TIC INSTITUCIONAL

La gobernanza de las TIC en la EMI se ejercerá mediante un conjunto de políticas, lineamientos, normas técnicas, procesos y mecanismos de control orientados a garantizar el uso estratégico, eficiente, seguro e integrado de la tecnología en el cumplimiento de los objetivos institucionales.

La DNTIC, constituye la instancia rectora en materia tecnológica a nivel institucional, siendo responsable de planificar, normar, dirigir, coordinar, supervisar y evaluar la gestión de las TIC, así como de definir la arquitectura tecnológica institucional, los estándares técnicos, los lineamientos de seguridad de la información, interoperabilidad y desarrollo de sistemas informáticos.

La gobernanza TIC se orienta a:

- a)** Asegurar la alineación de las TIC con los objetivos estratégicos establecidos en el Plan Estratégico Institucional (PEI).
- b)** Garantizar la integración e interoperabilidad de los sistemas académicos, administrativos y financieros en un entorno tecnológico unificado.
- c)** Promover la transformación digital institucional mediante la automatización de procesos, la digitalización de servicios y la implementación de sistemas integrados.
- d)** Fortalecer el gobierno de datos, asegurando la gestión adecuada, oportuna y segura de la información institucional.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- e) Establecer mecanismos de control, seguimiento y evaluación del desempeño de los servicios tecnológicos.

Las Unidades de Tecnologías de Información y Comunicación (UTIC) y demás unidades organizacionales deberán sujetarse a los lineamientos técnicos y normativos emitidos por la DNTIC, manteniendo coordinación permanente para la implementación, operación y mejora de los servicios tecnológicos institucionales.

Las decisiones relacionadas con la adquisición, desarrollo, implementación, integración o modificación de sistemas informáticos, infraestructura tecnológica y servicios digitales deberán ser coordinadas y validadas técnicamente por la DNTIC, en el marco de la gobernanza TIC institucional.

En el ejercicio de la gobernanza TIC, se deberá garantizar la correcta diferenciación entre la responsabilidad funcional de los procesos y datos, atribuida a las áreas usuarias, y la responsabilidad de la administración tecnológica, atribuida a la DNTIC.

Artículo 8º. RESPONSABILIDAD FUNCIONAL DEL DATO Y ADMINISTRACIÓN TECNOLÓGICA

La gestión de la información institucional en la EMI se regirá bajo el principio de separación entre la responsabilidad funcional del dato y la administración tecnológica de los sistemas.

La responsabilidad funcional del dato corresponde a las áreas usuarias, direcciones, unidades académicas y administrativas, y demás instancias organizacionales definidas en el Manual de Organización y Funciones (MOF) y normativa vigente, siendo responsables de:

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- a)** La generación, registro, validación y actualización de la información en los sistemas institucionales.
- b)** La veracidad, integridad, oportunidad y calidad de los datos.
- c)** La emisión, certificación, validación y uso oficial de la información.
- d)** El cumplimiento de la normativa vigente aplicable a los procesos de su competencia.

Por su parte, la DNTIC es responsable de la administración tecnológica, asegurando:

- a)** La disponibilidad, operatividad y mantenimiento de los sistemas informáticos.
- b)** La seguridad de la información en la infraestructura tecnológica.
- c)** La integración e interoperabilidad de los sistemas institucionales.
- d)** El control de accesos, perfiles y permisos en las plataformas tecnológicas.
- e)** La implementación de mecanismos de respaldo, recuperación y continuidad operativa.

La DNTIC no asume responsabilidad sobre el contenido, validez, exactitud o legalidad de la información registrada en los sistemas, siendo dicha responsabilidad exclusiva de las áreas usuarias en el ámbito de sus competencias.

La modificación, validación o aprobación de información institucional, especialmente aquella de carácter académico,

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

administrativo o financiero, deberá regirse por los procedimientos establecidos en la normativa institucional vigente, siendo ejecutada exclusivamente por las instancias competentes.

Todo acceso, registro o modificación de información en los sistemas institucionales deberá ser trazable y estar debidamente respaldado mediante mecanismos de auditoría y control definidos por la DNTIC.

Artículo 9°. COMITÉ INSTITUCIONAL DE GOBIERNO DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

El Comité Institucional de Gobierno Digital y Seguridad de la Información es la instancia de coordinación, análisis, seguimiento y recomendación estratégica en materia de TIC dentro de la EMI.

El Comité tendrá como finalidad apoyar la toma de decisiones institucionales relacionadas con la transformación digital, la gobernanza de datos, la seguridad de la información, la interoperabilidad de sistemas y la optimización del uso de recursos tecnológicos, en concordancia con el Plan Estratégico Institucional (PEI) y la normativa vigente.

Son funciones del Comité:

- a)** Analizar y proponer lineamientos estratégicos para la gestión y desarrollo de las TIC a nivel institucional.
- b)** Evaluar iniciativas, proyectos tecnológicos y sistemas institucionales en función de su prioridad, impacto y alineación estratégica.
- c)** Promover la implementación de políticas de gobierno digital, interoperabilidad y transformación digital.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- d) Supervisar el cumplimiento de políticas institucionales relacionadas con seguridad de la información y protección de datos.
- e) Recomendar acciones de mejora continua en la gestión tecnológica institucional.
- f) Coadyuvar al seguimiento de la implementación del Sistema Integrado de Gestión (SIGA-EMI) y otros sistemas institucionales.

El Comité estará conformado por representantes de las instancias estratégicas de la EMI, incluyendo autoridades académicas, administrativas y técnicas, siendo la DNTIC la instancia responsable de la coordinación técnica del mismo.

La conformación específica, periodicidad de reuniones y funcionamiento del Comité serán establecidos mediante disposición interna emitida por la autoridad competente.

Las recomendaciones emitidas por el Comité tendrán carácter técnico – estratégico y servirán de base para la toma de decisiones institucionales en materia de TIC.

Artículo 10º. POLITICAS DE CONTROL DE ACCESO Y GESTIÓN DE IDENTIDADES

La EMI establece políticas de control de acceso y gestión de identidades con el fin de garantizar la seguridad, confidencialidad, integridad y disponibilidad de la información institucional y de los sistemas tecnológicos.

La DNTIC es responsable de implementar, administrar y controlar los

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

mecanismos de autenticación, autorización y administración de identidades digitales de los usuarios que acceden a los sistemas institucionales.

El acceso a los sistemas, plataformas tecnológicas, servicios digitales y recursos informáticos institucionales estará sujeto a los siguientes lineamientos:

- a)** Todo usuario deberá contar con una identidad digital única, personal e intransferible para el acceso a los sistemas institucionales.
- b)** El acceso a los sistemas se otorgará en función de roles, perfiles y niveles de responsabilidad definidos por las áreas competentes, bajo el principio de mínimo privilegio.
- c)** La asignación, modificación y revocación de accesos deberá ser solicitada formalmente por el área usuaria correspondiente y gestionada por la DNTIC.
- d)** Las cuentas de usuario deberán ser deshabilitadas o eliminadas cuando el usuario deje de pertenecer a la institución o cambie de funciones que no requieran acceso a determinados sistemas.
- e)** Se deberán implementar mecanismos de autenticación segura, tales como contraseñas robustas, autenticación multifactor u otros controles que garanticen la protección de accesos.
- f)** Los accesos a sistemas críticos deberán ser registrados y monitoreados, asegurando la trazabilidad de las acciones realizadas por los usuarios.
- g)** Los usuarios privilegiados deberán sujetarse a controles específicos de seguridad, supervisión y auditoría por parte de la

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

DNTIC.

- h) El uso de las credenciales de acceso es responsabilidad exclusiva del usuario, quedando prohibido su uso compartido o su divulgación a terceros.
- i) El acceso a los sistemas deberá ajustarse a las políticas de seguridad de la información y a la normativa vigente en materia de gobierno digital y protección de datos.

La DNTIC deberá establecer procedimientos, controles y herramientas que permitan la gestión eficiente de identidades digitales, incluyendo la integración, cuando corresponda, con mecanismos nacionales de autenticación y ciudadanía digital.

Artículo 11°.CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información generada, administrada o custodiada por la EMI deberá clasificarse conforme a su nivel de sensibilidad, confidencialidad, criticidad y riesgo institucional, con el objeto de establecer controles adecuados para su almacenamiento, acceso, transmisión, conservación y eliminación.

La clasificación institucional comprenderá como mínimo las siguientes categorías:

a) Información Pública

Información cuya divulgación no genera riesgo para la institución y puede ser difundida libremente.

- Información institucional publicada;
- Convocatorias;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- Reglamentos públicos;
- Información estadística autorizada;

b) Información de Uso Interno

Información destinada exclusivamente al personal de la institución cuyo acceso se limita a usuarios autorizados.

- Memorándums;
- Manuales internos;
- Informes administrativos;
- Procedimientos.

c) Información Confidencial

Información cuyo acceso no autorizado puede afectar la operación institucional.

- Expedientes académicos;
- Información financiera;
- Contraseñas;
- Información de personal.

d) Información Restringida

Información cuya divulgación puede comprometer la seguridad institucional, afectar investigaciones, procesos disciplinarios o generar responsabilidad administrativa o legal.

- Credenciales maestras;
- Claves criptográficas;
- Configuración de servidores;
- Planes de continuidad;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- Informes de vulnerabilidades;
- Respaldos críticos.

Artículo 12º. AUDITORÍA Y TRAZABILIDAD

La EMI garantizará la implementación de mecanismos de auditoría y trazabilidad en los sistemas informáticos, plataformas tecnológicas y servicios digitales institucionales, con el objetivo de asegurar el control, supervisión, seguimiento y verificación de las actividades relacionadas con la gestión de la información.

La DNTIC es responsable de establecer, implementar y mantener mecanismos técnicos que permitan el registro, almacenamiento, monitoreo y análisis de las actividades realizadas en los sistemas institucionales, garantizando la integridad, disponibilidad y confidencialidad de los registros de auditoría.

Los sistemas institucionales deberán contar con registros de auditoría (logs) que permitan identificar, como mínimo:

- a)** Accesos de usuarios (inicio y cierre de sesión);
- b)** Operaciones realizadas sobre datos (creación, modificación, eliminación y consulta crítica);
- c)** Asignación y cambios en roles, perfiles y permiso;
- d)** Accesos e intervenciones de usuarios privilegiados;
- e)** Eventos de seguridad, fallos, incidentes y actividades inusuales.

Los registros de auditoría deberán ser protegidos contra alteraciones, eliminaciones o accesos no autorizados, manteniendo su integridad y disponibilidad para fines de control, supervisión y

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

verificación.

La información registrada en los mecanismos de auditoría podrá ser utilizada para:

- a)** Procesos de control interno y auditoría institucional;
- b)** Investigación de incidentes de seguridad de la información;
- c)** Verificación del cumplimiento de normativas institucionales;
- d)** Sustento de procesos administrativos, disciplinarios o legales.

La DNTIC, en coordinación con las instancias competentes, establecerá los procedimientos para la revisión, conservación, respaldo y análisis de los registros de auditoría, definiendo periodos de retención y niveles de acceso a dicha información.

Las áreas usuarias deberán operar los sistemas institucionales conforme a los procedimientos establecidos, asegurando que toda acción relevante quede debidamente registrada y sea susceptible de verificación.

Artículo 13°.GOBIERNO DE DATOS INSTITUCIONAL

La EMI establece el Gobierno de Datos Institucional como el conjunto de políticas, lineamientos, responsabilidades, procesos y mecanismos de control orientados a garantizar la adecuada gestión de los datos en todo su ciclo de vida, asegurando su calidad, integridad, disponibilidad, seguridad y uso estratégico.

El Gobierno de Datos tendrá como finalidad consolidar la información institucional como un activo estratégico para la toma de decisiones,

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

la planificación, el control de gestión y la mejora continua de los procesos académicos, administrativos y de apoyo.

Las áreas usuarias, conforme a sus atribuciones establecidas en el Manual de Organización y Funciones (MOF) y normativa vigente, son responsables de la creación, validación, actualización, integridad, consistencia y uso adecuado de los datos que administran en los sistemas institucionales.

La DNTIC, es responsable de la administración tecnológica de los datos, debiendo garantizar:

- a) La disponibilidad y accesibilidad de los datos a través de los sistemas institucionales;
- b) La implementación de mecanismos de seguridad para la protección de los datos;
- c) La integración e interoperabilidad de la información entre sistemas institucionales;
- d) La implementación de mecanismos de respaldo, recuperación y continuidad de los datos;
- e) La trazabilidad de la información mediante sistemas de auditoría.

El Gobierno de Datos institucional se regirá por los siguientes lineamientos:

- a) **Calidad de datos:** La información deberá ser precisa, completa, consistente y actualizada;
- b) **Integridad:** Los datos deberán mantenerse libres de

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

alteraciones no autorizadas;

- c) **Disponibilidad:** La información deberá estar accesible cuando sea requerida por las instancias autorizadas;
- d) **Confidencialidad:** El acceso a los datos estará restringido de acuerdo con niveles de autorización y clasificación de la información;
- e) **Interoperabilidad:** Los sistemas deberán compartir información de manera estructurada y eficiente, conforme a estándares institucionales y normativa vigente;
- f) **Responsabilidad:** Cada área organizacional será responsable del uso adecuado y control de los datos en su ámbito de competencia.

La DNTIC, en coordinación con las áreas usuarias y las instancias competentes, podrá establecer normas técnicas, procedimientos y mecanismos de control para la gestión, clasificación, estandarización, intercambio y uso de los datos institucionales.

El uso de los datos institucionales para fines distintos a los establecidos en la normativa vigente o sin la debida autorización será considerado incumplimiento y sujeto a las acciones de control y medidas correspondientes

Artículo 14º. PROTECCIÓN DE DATOS PERSONALES, PRIVACIDAD Y TRATAMIENTO DE INFORMACIÓN SENSIBLE

La EMI reconoce la protección de los datos personales, la privacidad y la confidencialidad de la información como principios fundamentales para la gestión de las TIC, debiendo adoptar las

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

medidas técnicas, administrativas y organizacionales necesarias para resguardar la información que administra en el cumplimiento de sus funciones institucionales.

La gestión y tratamiento de datos personales deberá efectuarse exclusivamente para fines institucionales legítimos, en el marco de las competencias de la EMI y de conformidad con la normativa nacional vigente.

A efectos del presente Reglamento se entiende por:

- a) Datos personales:** Información vinculada o referida a una persona natural identificada o identificable.
- b) Información sensible:** Datos cuya divulgación, alteración, pérdida o acceso no autorizado pueda afectar derechos, la privacidad, la seguridad o los intereses legítimos de una persona o de la institución.

La recolección, registro, almacenamiento, consulta, procesamiento, transferencia, intercambio y eliminación de datos deberá sujetarse a los siguientes principios:

- Legalidad;
- Finalidad institucional;
- Confidencialidad;
- Integridad;
- Disponibilidad;
- Minimización del acceso a la información;
- Responsabilidad en el tratamiento de los datos.

Las unidades organizacionales que administren información académica, administrativa, financiera, laboral, disciplinaria, médica o

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

cualquier otra información sensible serán responsables de garantizar el adecuado uso y protección de dichos datos en el ámbito de sus competencias.

La DNTIC deberá implementar mecanismos tecnológicos que permitan proteger los datos institucionales mediante controles de acceso, autenticación, trazabilidad, respaldo, recuperación, monitoreo y demás medidas de seguridad necesarias para prevenir la pérdida, alteración, divulgación o acceso no autorizado.

El acceso a datos personales o información sensible será restringido únicamente a usuarios autorizados y en función de las responsabilidades asignadas, aplicando el principio de necesidad de acceso y mínimo privilegio.

La transferencia o intercambio de información institucional con entidades externas deberá realizarse únicamente cuando exista autorización expresa de la autoridad competente, mandato legal o necesidad institucional debidamente justificada, aplicando las medidas de seguridad y control correspondientes.

Toda consulta, acceso, modificación o tratamiento de información sensible deberá quedar registrada en los mecanismos de auditoría y trazabilidad definidos por la DNTIC.

Queda prohibido el uso, divulgación, reproducción, copia, extracción o tratamiento de datos personales o información sensible para fines distintos de los establecidos por la normativa institucional o sin la autorización correspondiente.

El incumplimiento de las disposiciones establecidas en el presente artículo será considerado falta informática y dará lugar a las acciones de control, medidas disciplinarias y responsabilidades que correspondan conforme a la normativa vigente.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Artículo 15°. CIUDADANÍA DIGITAL Y VALIDACIÓN ELECTRÓNICA

La EMI promoverá la implementación y utilización de mecanismos de ciudadanía digital y validación electrónica en sus sistemas informáticos institucionales, con la finalidad de fortalecer la transformación digital, optimizar la prestación de servicios digitales y garantizar la identificación segura de los usuarios.

La DNTIC es responsable de establecer los lineamientos técnicos, estándares de interoperabilidad, mecanismos de autenticación y procedimientos necesarios para la implementación de servicios de validación electrónica en los sistemas institucionales.

Los sistemas de información de la EMI podrán integrar mecanismos de autenticación tecnológica que permitan verificar la identidad de usuarios internos y externos mediante servicios de ciudadanía digital u otros mecanismos de validación electrónica autorizados por la normativa nacional vigente.

La validación electrónica de usuarios deberá garantizar, como mínimo:

- a)** La identificación inequívoca del usuario;
- b)** La autenticidad de las operaciones realizadas;
- c)** La trazabilidad de las transacciones efectuadas en los sistemas institucionales;
- d)** La integridad de los registros electrónicos;
- e)** La protección de los datos personales y la información institucional.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

La DNTIC deberá implementar controles de registro, monitoreo y auditoría que permitan verificar las operaciones realizadas mediante mecanismos de ciudadanía digital o validación electrónica, garantizando la conservación de evidencias digitales para fines de control, supervisión y auditoría.

La utilización de mecanismos de ciudadanía digital y validación electrónica deberá sujetarse a las disposiciones establecidas por la normativa nacional vigente y a los procedimientos internos definidos por la EMI.

Toda acción realizada mediante mecanismos de autenticación y validación electrónica en los sistemas institucionales producirá los efectos administrativos correspondientes dentro del ámbito de competencia de la EMI, siempre que se encuentre debidamente registrada y sea verificable mediante los mecanismos de control implementados por la DNTIC.

Artículo 16°. FIRMA DIGITAL Y FIRMA DIGITALIZADA

La EMI reconoce el uso de mecanismos de firma digital y firma digitalizada en el ámbito de los sistemas y servicios digitales institucionales, de conformidad con la normativa nacional vigente y los procedimientos internos establecidos.

A efectos del presente Reglamento, se establece la siguiente diferenciación:

- a) Firma Digital:** Mecanismo de autenticación electrónica basado en certificados digitales emitidos por una entidad certificadora autorizada, que permite verificar la identidad del firmante, garantizar la integridad del documento electrónico y proporcionar evidencias de autenticidad y no repudio, conforme a la normativa

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

vigente del Estado Plurinacional de Bolivia.

- b) Firma Digitalizada:** Representación gráfica o imagen electrónica de una firma manuscrita obtenida mediante escaneo, captura digital u otro procedimiento similar, incorporada a un documento o sistema informático.

La firma digital tendrá plena validez jurídica en los términos establecidos por la normativa nacional aplicable.

La imagen electrónica o representación gráfica de una firma manuscrita incorporada en un sistema (Firma Digitalizada), por sí sola, no constituye un mecanismo criptográfico de autenticación ni produce efectos jurídicos. Las operaciones validadas internamente en los sistemas mediante el uso de credenciales de usuario constituirán únicamente una “Trazabilidad de Sesión Autenticada”, con valor administrativo interno, sin atribuirse las presunciones legales de autoría y no repudio exclusivas de la Firma Digital.

La validez institucional de las actuaciones realizadas mediante firma digitalizada estará condicionada al cumplimiento simultáneo de los siguientes requisitos:

- a)** Que el usuario haya sido previamente identificado y autenticado mediante las credenciales institucionales correspondientes.
- b)** Que la operación realizada se encuentre registrada en los mecanismos de auditoría y trazabilidad del sistema.
- c)** Que la acción pueda ser atribuida de forma inequívoca al usuario responsable.
- d)** Que el trámite o procedimiento se encuentre habilitado para su utilización por disposición institucional expresa.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

La DNTIC establecerá los lineamientos técnicos, estándares de seguridad y controles necesarios para la implementación, administración y supervisión de los mecanismos de firma digital y firma digitalizada utilizados en los sistemas institucionales.

La falsificación, alteración, uso no autorizado, suplantación de identidad o utilización indebida de mecanismos de firma digital o firma digitalizada constituirá falta grave o muy grave, según corresponda, sin perjuicio de las responsabilidades administrativas, civiles o penales establecidas por la normativa vigente.

La DNTIC es responsable de establecer los lineamientos técnicos, mecanismos de control y procedimientos para:

- a)** La implementación de firma digital en sistemas institucionales;
- b)** La gestión de documentos electrónicos firmados digitalmente;
- c)** La validación de identidad mediante sistemas institucionales y ciudadanía digital, cuando corresponda;
- d)** El control y uso adecuado de firmas digitalizadas dentro de plataformas institucionales.

Los sistemas informáticos institucionales podrán incorporar mecanismos de autenticación electrónica, firma digital y validación mediante ciudadanía digital, en conformidad con los lineamientos establecidos por el Estado.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

CAPÍTULO III GESTIÓN DE ACTIVOS DE INFORMACIÓN

Artículo 17°.GESTIÓN DE ACTIVOS DE INFORMACIÓN

La EMI establece la Gestión de Activos de Información como el conjunto de políticas, procedimientos y controles destinados a identificar, proteger, administrar y controlar los activos de información institucionales durante todo su ciclo de vida, garantizando su adecuada utilización, seguridad y disponibilidad.

La DNTIC, en coordinación con las unidades organizacionales competentes, es responsable de establecer lineamientos y mecanismos de control para la gestión de activos de información institucionales.

Artículo 18°.INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Todos los activos de información deberán ser identificados, inventariados, registrados y clasificados de acuerdo con su importancia, valor institucional, criticidad y nivel de sensibilidad.

El inventario de activos deberá incluir, cuando corresponda:

- Sistemas informáticos;
- Bases de datos;
- Infraestructura tecnológica;
- Equipos de computación;
- Dispositivos móviles;
- Medios de almacenamiento;
- Documentación física y digital;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- Servicios tecnológicos;
- Recursos de comunicación y conectividad.

La clasificación de los activos de información podrá considerar niveles de información pública, de uso interno, confidencial o restringida, conforme a los lineamientos establecidos por la DNTIC.

Artículo 19°. PROPIEDAD Y CUSTODIA DE LOS ACTIVOS DE INFORMACIÓN

Todo activo de información institucional deberá tener un responsable funcional y un custodio tecnológico claramente identificados.

La responsabilidad funcional corresponderá a la unidad organizacional propietaria del proceso o de la información, siendo responsable de su contenido, actualización, uso y clasificación.

La custodia tecnológica corresponderá a la DNTIC respecto a la administración, almacenamiento, disponibilidad, respaldo y protección tecnológica de los activos que se encuentren bajo su gestión.

La asignación de responsabilidades deberá mantenerse actualizada y documentada.

Artículo 20°. ETIQUETADO Y MANEJO DE LA INFORMACIÓN

La información institucional deberá ser identificada y manejada de acuerdo con su nivel de clasificación y sensibilidad.

Los activos de información que contengan información confidencial, restringida o sensible deberán incorporar mecanismos de identificación física o lógica que permitan reconocer su nivel de

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

protección y las restricciones aplicables para su acceso, uso, almacenamiento, reproducción o transferencia.

La DNTIC, podrá establecer estándares de etiquetado, clasificación y manejo de información para toda la institución.

Artículo 21º.USO ACEPTABLE DE ACTIVOS TECNOLÓGICOS

Los activos tecnológicos institucionales deberán ser utilizados exclusivamente para fines académicos, administrativos, científicos, de investigación o de apoyo institucional.

Los usuarios serán responsables del uso adecuado de los activos asignados, debiendo protegerlos contra pérdida, daño, robo, uso indebido o acceso no autorizado.

Queda prohibido utilizar activos tecnológicos institucionales para fines personales, comerciales, ilícitos o contrarios a la normativa vigente.

Artículo 22º.DEVOLUCIÓN DE ACTIVOS INSTITUCIONALES

Toda persona que concluya su relación laboral, contractual, académica o funcional con la EMI deberá devolver los activos institucionales que le hayan sido asignados.

La devolución comprenderá equipos informáticos, dispositivos móviles, credenciales de acceso, medios de almacenamiento, documentación y cualquier otro recurso institucional bajo su responsabilidad.

La unidad competente y la DNTIC deberán verificar la devolución de los activos y gestionar la revocación de accesos, permisos y

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

credenciales tecnológicas correspondientes.

Artículo 23°. DISPOSICIÓN FINAL Y ELIMINACIÓN SEGURA DE ACTIVOS Y MEDIOS DE ALMACENAMIENTO

La disposición final de equipos informáticos, medios de almacenamiento y otros activos tecnológicos deberá realizarse mediante procedimientos que garanticen la protección de la información institucional.

Previo a la transferencia, reutilización, baja o disposición final de un activo tecnológico, se deberán aplicar mecanismos de eliminación segura de información, borrado seguro, destrucción física o cualquier otro procedimiento que impida la recuperación no autorizada de los datos almacenados.

La DNTIC establecerá los procedimientos técnicos y controles necesarios para la gestión segura de la disposición final de activos tecnológicos institucionales.

Toda eliminación o disposición final de activos deberá quedar debidamente documentada y respaldada mediante registros institucionales.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

CAPÍTULO IV POLÍTICAS DE INGENIERÍA DE SOFTWARE Y SOPORTE TECNOLÓGICO

Artículo 24º. USO DE SERVICIOS WEB, NUBE Y CORREO INSTITUCIONAL

La EMI regula el uso de servicios web, plataformas en la nube y correo electrónico institucional con el fin de garantizar la seguridad de la información, la protección de los datos institucionales, la continuidad de los servicios y el cumplimiento de la normativa vigente en materia de tecnologías de información y gobierno digital.

La DNTIC es la instancia responsable de autorizar, implementar, administrar y supervisar el uso de servicios web, soluciones en la nube y plataformas digitales institucionales.

El uso de servicios en la nube y plataformas web deberá registrarse por los siguientes lineamientos:

- a)** Todo servicio en la nube utilizado para almacenamiento, procesamiento o gestión de información institucional deberá contar con autorización expresa de la DNTIC.
- b)** La contratación o uso de servicios tecnológicos externos deberá cumplir con criterios de seguridad de la información, disponibilidad, respaldo, ubicación de datos y normativa vigente.
- c)** Se deberá priorizar el uso de soluciones tecnológicas institucionales o autorizadas, evitando el almacenamiento de información institucional en plataformas no autorizadas.
- d)** Los servicios en la nube deberán garantizar mecanismos adecuados de respaldo, recuperación y protección de datos.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- e)** La integración de servicios en la nube con sistemas institucionales deberá cumplir estándares de interoperabilidad y seguridad definidos por la DNTIC.

El correo electrónico institucional constituye un medio oficial de comunicación de la EMI, por lo que su uso deberá cumplir los siguientes parámetros:

- a)** Toda comunicación oficial interna y externa deberá realizarse mediante cuentas de correo institucional autorizadas.
- b)** Las cuentas de correo institucional son personales, intransferibles y de uso exclusivo para actividades académicas, administrativas y funcionales.
- c)** La creación, modificación, suspensión y eliminación de cuentas de correo será gestionada exclusivamente por la DNTIC conforme a la condición laboral, académica o contractual del usuario.
- d)** El uso del correo institucional deberá observar las políticas de seguridad de la información, confidencialidad y uso adecuado de los recursos tecnológicos.
- e)** Está prohibido el uso del correo institucional para fines personales, comerciales, ilícitos o contrarios a la normativa institucional vigente.

La DNTIC deberá establecer mecanismos de control, monitoreo y protección para el uso de servicios web, nube y correo institucional, incluyendo filtros de seguridad, respaldo de información y medidas de prevención ante amenazas tecnológicas.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Artículo 25°. SOPORTE TECNOLÓGICO Y MESA DE SERVICIOS

La EMI establece el servicio de Soporte Tecnológico como el conjunto de actividades orientadas a la atención, solución y seguimiento de incidentes, requerimientos, consultas y problemas relacionados con el uso de los sistemas informáticos, infraestructura tecnológica y servicios digitales institucionales.

La DNTIC es la instancia responsable de organizar, implementar, administrar y supervisar la Mesa de Servicios TIC, la cual constituye el punto único de contacto entre los usuarios y la gestión tecnológica institucional.

Las solicitudes de asistencia técnica deberán registrarse a través de los canales oficiales definidos por la DNTIC, incluyendo el uso del formulario establecido en el ANEXO “B” del presente Reglamento cuando corresponda.

La Mesa de Servicios TIC tendrá como funciones principales:

- a)** Registrar, clasificar y canalizar los incidentes, requerimientos y consultas de los usuarios.
- b)** Brindar atención técnica de primer nivel y coordinar el soporte de segundo y tercer nivel cuando corresponda.
- c)** Realizar el seguimiento y cierre de los casos atendidos, garantizando su resolución.
- d)** Mantener registros actualizados de los servicios prestados, asegurando su trazabilidad.
- e)** Generar reportes e indicadores para la mejora continua del servicio.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

El soporte tecnológico institucional se registrará por los siguientes lineamientos:

- a)** Todo incidente o requerimiento deberá ser registrado mediante los canales oficiales definidos por la DNTIC.
- b)** La atención de los casos se gestionará en función de su prioridad, impacto y urgencia, estableciendo niveles de servicio.
- c)** La DNTIC podrá definir tiempos de respuesta y atención (niveles de servicio) conforme a la criticidad del servicio o sistema afectado.
- d)** Los usuarios deberán proporcionar información veraz y suficiente para la atención de sus solicitudes.
- e)** Las intervenciones técnicas realizadas deberán quedar debidamente registradas para efectos de control y auditoría.
- f)** La atención de soporte deberá orientarse a la solución definitiva del problema y a la prevención de recurrencias.

La DNTIC podrá establecer procedimientos, herramientas tecnológicas y mecanismos de gestión para la operación de la Mesa de Servicios, incluyendo la automatización de procesos, gestión de tickets, monitoreo de servicios y evaluación de la calidad del soporte.

El uso adecuado del servicio de soporte tecnológico es responsabilidad de los usuarios institucionales, quienes deberán utilizar los canales oficiales establecidos y cumplir los procedimientos definidos.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Artículo 26°.GESTIÓN DE SERVICIOS TIC (SLA, CATÁLOGO, INCIDENTES)

La EMI establece la Gestión de Servicios de TIC como el conjunto de procesos destinados a planificar, organizar, entregar, operar y mejorar los servicios tecnológicos institucionales, garantizando su calidad, disponibilidad, seguridad y continuidad.

La DNTIC es responsable de diseñar, implementar, administrar y supervisar la gestión de servicios TIC, en concordancia con estándares de buenas prácticas y las necesidades institucionales.

La gestión de servicios TIC se fundamenta en los siguientes componentes:

- a) Catálogo de servicios TIC:** La DNTIC deberá establecer y mantener actualizado un catálogo de servicios tecnológicos institucionales, que incluirá la descripción de los servicios, alcance, condiciones de uso, responsables, horarios de atención y niveles de servicio asociados.
- b) Acuerdos de nivel de servicio (SLA):** La DNTIC definirá niveles de servicio para los servicios TIC, estableciendo tiempos de respuesta, tiempos de resolución, prioridades de atención y condiciones de operación, en función de la criticidad y el impacto institucional de los servicios.
- c) Gestión de incidentes:** Todo incidente que afecte el funcionamiento de los sistemas, infraestructura o servicios TIC deberá ser registrado, clasificado, atendido y resuelto conforme a procedimientos definidos por la DNTIC, priorizando la restauración oportuna de los servicios afectados.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- d) Gestión de requerimientos:** Las solicitudes de servicios tecnológicos deberán ser registradas, evaluadas y atendidas conforme a los procedimientos establecidos, garantizando trazabilidad y control de las actividades realizadas.
- e) Gestión de problemas:** La DNTIC deberá identificar, analizar y gestionar las causas raíz de incidentes recurrentes, implementando soluciones que eviten su repetición.
- f) Monitoreo y mejora continua:** La DNTIC deberá medir el desempeño de los servicios TIC mediante indicadores, generando reportes periódicos que permitan evaluar la calidad del servicio y establecer acciones de mejora continua.

Los servicios TIC deberán ser prestados bajo criterios de:

- Disponibilidad.
- Continuidad operativa.
- Seguridad de la información.
- Eficiencia en la atención.
- Satisfacción del usuario.

Todas las solicitudes, incidentes y actividades relacionadas con los servicios TIC deberán ser gestionadas a través de los canales oficiales definidos por la DNTIC, garantizando su registro, seguimiento y trazabilidad.

Las unidades organizacionales y usuarios deberán cumplir con los procedimientos establecidos para la solicitud y uso de los servicios TIC, siendo responsables del uso adecuado de los mismos.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Artículo 27°. SISTEMAS ACADÉMICOS Y RESTRICCIONES ESPECIALES

Los sistemas académicos de la EMI constituyen plataformas tecnológicas de apoyo a la gestión académica, sujetas a la normativa institucional vigente, en especial a los Reglamentos Académicos (RAC), el Modelo Académico y demás disposiciones aplicables.

La DNTIC, es responsable de la administración tecnológica de los sistemas académicos, garantizando su disponibilidad, operatividad, seguridad, integridad técnica y correcto funcionamiento.

Las funciones de carácter académico, tales como el registro, modificación, validación, aprobación y certificación de información académica, corresponden exclusivamente a las instancias académicas competentes definidas en la normativa institucional vigente.

En tal sentido:

- a)** La DNTIC no tiene competencia para registrar, modificar, validar o aprobar información académica, incluyendo calificaciones, evaluaciones, historiales académicos, registros de estudiantes, certificaciones o cualquier otro dato de carácter académico.
- b)** La responsabilidad sobre la veracidad, integridad, actualización y legalidad de la información académica recae en los docentes, jefaturas de carrera, direcciones de unidades académicas y demás instancias competentes, conforme a los reglamentos académicos vigentes.
- c)** Toda modificación de información académica deberá realizarse bajo procedimientos formales establecidos en la normativa institucional, quedando prohibida cualquier modificación directa

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

fuera de dichos procedimientos.

- d)** Los sistemas académicos deberán contar con mecanismos de control de acceso, trazabilidad y registro de auditoría que permitan identificar todas las acciones realizadas por los usuarios.
- e)** La habilitación, apertura, cierre o control de periodos académicos en los sistemas será realizada por la DNTIC conforme a instrucciones de la instancia académica competente.
- f)** La emisión de documentos académicos oficiales deberá cumplir con los flujos de validación, aprobación y firma establecidos por la normativa institucional, pudiendo utilizar mecanismos de firma digital autorizados.

Cualquier intervención técnica en sistemas académicos deberá realizarse bajo procedimientos controlados, asegurando la integridad de la información y la trazabilidad de las acciones efectuadas.

El uso indebido de los sistemas académicos, la alteración no autorizada de datos o el incumplimiento de los procedimientos establecidos será considerado falta grave y estará sujeto a las medidas de control y sanción conforme a la normativa institucional vigente.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

CAPÍTULO V CIBERSEGURIDAD, INFRAESTRUCTURA Y CONTINUIDAD OPERATIVA

Artículo 28°.POLÍTICAS DE CIBERSEGURIDAD

La EMI establece las políticas de ciberseguridad como el conjunto de lineamientos, controles, medidas técnicas y organizacionales destinados a proteger los sistemas informáticos, infraestructura tecnológica, redes y datos institucionales frente a amenazas, vulnerabilidades e incidentes de seguridad.

La DNTIC, es la instancia responsable de diseñar, implementar, administrar y supervisar las políticas de ciberseguridad institucional, en coordinación con las unidades organizacionales y conforme a la normativa vigente.

Las políticas de ciberseguridad institucional se regirán por los siguientes principios y lineamientos:

- a) **Protección de la información:** Garantizar la confidencialidad, integridad y disponibilidad de la información institucional mediante mecanismos de control y seguridad adecuados.
- b) **Gestión de riesgos:** Identificar, evaluar y mitigar los riesgos asociados a la seguridad de la información, estableciendo medidas preventivas y correctivas.
- c) **Seguridad por diseño:** Incorporar controles de seguridad desde la fase de diseño y desarrollo de sistemas informáticos.
- d) **Control de accesos:** Implementar mecanismos de autenticación, autorización y gestión de identidades conforme a políticas institucionales.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- e) **Monitoreo y detección:** Establecer mecanismos de monitoreo continuo para la detección de eventos de seguridad, actividades sospechosas e incidentes informáticos.
- f) **Gestión de vulnerabilidades:** Implementar procesos de identificación, evaluación y corrección de vulnerabilidades en sistemas, aplicaciones e infraestructura tecnológica.
- g) **Actualización y mantenimiento:** Garantizar la actualización periódica de sistemas, software, firmware y plataformas tecnológicas para reducir riesgos de seguridad.
- h) **Concienciación y capacitación:** Promover la formación continua de los usuarios en buenas prácticas de seguridad de la información y uso responsable de los recursos tecnológicos.
- i) **Respuesta a incidentes:** Establecer procedimientos para la identificación, notificación, análisis, contención, recuperación y documentación de incidentes de seguridad.
- j) **Cumplimiento normativo:** Asegurar que todas las acciones relacionadas con la ciberseguridad se desarrollen en concordancia con la normativa nacional vigente y las políticas institucionales.

La DNTIC, deberá establecer procedimientos específicos, herramientas tecnológicas y mecanismos de control que permitan la implementación efectiva de las políticas de ciberseguridad, así como la evaluación periódica de su cumplimiento.

Las unidades organizacionales y usuarios institucionales deberán cumplir obligatoriamente las políticas de ciberseguridad, siendo responsables del uso adecuado de los recursos tecnológicos y de la protección de la información bajo su responsabilidad.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Artículo 29º. USO Y SALVAGUARDA DE LA INFRAESTRUCTURA

La EMI establece que la infraestructura tecnológica institucional constituye un activo estratégico, por lo que su uso, administración, protección y conservación deberán realizarse bajo criterios de seguridad, eficiencia, continuidad operativa y responsabilidad institucional.

La DNTIC, es la instancia responsable de planificar, implementar, administrar, mantener, supervisar y proteger la infraestructura tecnológica institucional, incluyendo servidores, redes, equipos de comunicación, dispositivos informáticos, centros de datos y plataformas tecnológicas.

El uso de la infraestructura tecnológica se regirá por los siguientes lineamientos:

- a)** Los recursos tecnológicos institucionales deberán ser utilizados exclusivamente para fines académicos, administrativos e institucionales, conforme a las funciones asignadas.
- b)** Queda prohibido el uso indebido, no autorizado o con fines personales, comerciales o ilícitos de los equipos, redes o servicios tecnológicos.
- c)** La instalación, configuración, traslado, modificación o retiro de equipos tecnológicos deberá ser realizado o autorizado por la DNTIC.
- d)** No se permitirá la conexión de dispositivos, equipos o redes no autorizadas a la infraestructura tecnológica institucional.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- e) Los usuarios serán responsables del adecuado uso y cuidado de los equipos asignados, debiendo reportar de manera inmediata cualquier falla, daño o incidente.
- f) Se deberán aplicar medidas de seguridad física y lógica para la protección de la infraestructura tecnológica, incluyendo control de acceso a ambientes críticos, monitoreo de redes y protección contra amenazas.
- g) La infraestructura tecnológica deberá contar con mecanismos de mantenimiento preventivo, correctivo y evolutivo que garanticen su continuidad operativa.
- h) La DNTIC, deberá mantener inventarios actualizados de los activos tecnológicos, así como registros de configuración, mantenimiento y estado de los mismos.
- i) La infraestructura tecnológica crítica deberá contar con mecanismos de redundancia, respaldo y recuperación ante fallas o contingencias.

Las unidades organizacionales deberán coordinar con la DNTIC cualquier requerimiento relacionado con infraestructura tecnológica, garantizando el cumplimiento de los estándares institucionales.

El daño, manipulación indebida, uso no autorizado o incumplimiento de las disposiciones establecidas en el presente artículo será considerado falta y estará sujeto a las acciones de control y sanción conforme a la normativa institucional vigente.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Artículo 30°.GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La EMI implementara un proceso permanente de gestión de riesgos de seguridad de la información, con el objeto de identificar, analizar, evaluar, tratar, monitorear y revisar los riesgos que pueden afectar los activos de información institucionales.

La DNTIC, será responsable de coordinar la gestión técnica de riesgos, debiendo:

- a) Identificar activos de información;
- b) Identificar amenazas;
- c) Identificar vulnerabilidades;
- d) Evaluar impacto;
- e) Evaluar probabilidad;
- f) Determinar el nivel de riesgo;
- g) Definir controles de tratamiento;
- h) Elaborar matrices de riesgo;
- i) Mantener actualizado el registro institucional de riesgos.
- j) Revisar periódicamente la efectividad de los controles implementados.

Artículo 31°.GESTIÓN DE INCIDENTES Y CONTINUIDAD

La EMI establece la gestión de incidentes informáticos y la continuidad operativa como procesos fundamentales para garantizar la disponibilidad, seguridad y resiliencia de los servicios tecnológicos institucionales.

La DNTIC, es la instancia responsable de implementar, administrar y supervisar los procedimientos de gestión de incidentes y continuidad de servicios tecnológicos.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

La gestión de incidentes informáticos comprende el conjunto de actividades orientadas a la identificación, registro, clasificación, análisis, contención, solución y documentación de eventos que afecten o puedan afectar la seguridad, disponibilidad o funcionamiento de los sistemas, infraestructura tecnológica o información institucional.

Los incidentes informáticos deberán ser gestionados conforme a los siguientes lineamientos:

- a)** Todo incidente deberá ser reportado de manera inmediata a través de los canales oficiales definidos por la DNTIC;
- b)** Los incidentes deberán ser registrados, clasificados y priorizados en función de su impacto y criticidad;
- c)** Se deberán aplicar medidas de contención y recuperación para restablecer los servicios afectados en el menor tiempo posible;
- d)** Todo incidente deberá ser documentado, asegurando la trazabilidad de las acciones realizadas;
- e)** Se deberán realizar análisis de causa raíz y establecer acciones correctivas y preventivas.

La continuidad operativa tecnológica estará orientada a garantizar la prestación ininterrumpida de los servicios críticos, mediante la implementación de planes, mecanismos y medidas de recuperación ante fallas o desastres.

Para este efecto, la DNTIC deberá:

- a)** Implementar políticas de respaldo (backup) de la información institucional, definiendo periodicidad, almacenamiento y

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

recuperación de datos;

- b)** Establecer y mantener procedimientos de recuperación de sistemas y datos en caso de fallas, incidentes o desastres;
- c)** Identificar servicios críticos y establecer formalmente las métricas de continuidad operativa, definiendo de manera obligatoria el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO) para cada sistema institucional priorizado;
- d)** Realizar pruebas periódicas de restauración de datos y recuperación de sistemas;
- e)** Implementar mecanismos de redundancia y contingencia para los servicios tecnológicos críticos;
- f)** Documentar y actualizar los planes de continuidad y recuperación tecnológica.

Las unidades organizacionales deberán colaborar con la DNTIC en la gestión de incidentes y en la aplicación de medidas de continuidad operativa, reportando oportunamente cualquier evento que afecte los servicios tecnológicos.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

CAPÍTULO VI DESARROLLO DE SISTEMAS INFORMÁTICOS

Artículo 32°.REGULACIÓN DEL CICLO DE DESARROLLO E IMPLEMENTACIÓN

La EMI establece como obligatoria la aplicación de un ciclo de vida de desarrollo de sistemas para la creación, modificación, integración, implementación y mantenimiento de soluciones informáticas institucionales, con el fin de garantizar la calidad, seguridad, interoperabilidad y sostenibilidad de los sistemas tecnológicos.

La DNTIC es la instancia responsable de definir, implementar y supervisar la aplicación del ciclo de desarrollo de software en la institución, estableciendo metodologías, estándares técnicos, procedimientos y herramientas para su ejecución.

Toda solicitud de desarrollo, mejora o integración de sistemas deberá ser formalizada mediante el formulario institucional establecido en el ANEXO “A” del presente Reglamento.

Todo sistema informático institucional deberá desarrollarse e implementarse conforme a las siguientes fases mínimas:

- a) **Levantamiento de requerimientos:** Identificación, análisis y documentación de necesidades funcionales y técnicas, en coordinación con el área usuaria responsable del proceso;
- b) **Análisis y diseño:** Definición de la arquitectura del sistema, estructura de datos, flujos de proceso, controles de seguridad y criterios de interoperabilidad;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- c) **Desarrollo o construcción:** Programación y configuración del sistema conforme a estándares técnicos institucionales, utilizando repositorios controlados y mecanismos de versionamiento;
- d) **Pruebas:** Ejecución de pruebas técnicas, funcionales, de seguridad y de rendimiento que garanticen el correcto funcionamiento del sistema;
- e) **Validación funcional:** Aprobación formal del sistema por parte del área usuaria, asegurando que cumple con los requerimientos establecidos;
- f) **Implementación:** Despliegue del sistema en ambiente de producción bajo procedimientos de control de cambios, incluyendo respaldo previo y mecanismos de reversión;
- g) **Documentación:** Elaboración obligatoria de documentación técnica y funcional del sistema, incluyendo manuales de usuario, manuales técnicos y registro de versiones;
- h) **Mantenimiento y mejora continua:** Actualización, corrección y evolución del sistema conforme a nuevas necesidades institucionales.

Todo desarrollo o implementación de sistemas deberá:

- a) Estar debidamente autorizado por la instancia competente;
- b) Cumplir con los estándares técnicos definidos por la DNTIC;
- c) Garantizar la seguridad de la información desde su diseño;
- d) Asegurar la interoperabilidad con otros sistemas institucionales;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- e) Contar con respaldo documental y trazabilidad de cambios.

Queda prohibida la implementación de sistemas informáticos fuera del proceso establecido en el presente artículo, así como el uso de soluciones tecnológicas no autorizadas por la DNTIC.

La DNTIC, podrá definir metodologías de desarrollo ágiles, tradicionales o híbridas, así como herramientas tecnológicas de apoyo, en función de la complejidad y naturaleza de los proyectos.

Artículo 33°.NORMAS DE DESARROLLO

La EMI establece que todo desarrollo de sistemas informáticos institucionales deberá cumplir obligatoriamente con normas técnicas, metodológicas y de seguridad que garanticen la calidad, confiabilidad, interoperabilidad, sostenibilidad y alineación con los objetivos institucionales.

La DNTIC, es la instancia responsable de definir, implementar, supervisar y actualizar las normas de desarrollo de software institucional, así como de regular los estándares aplicables a su construcción, mantenimiento e integración.

Todo desarrollo de sistemas deberá regirse por los siguientes lineamientos:

- a) **Estandarización del desarrollo:** Los sistemas deberán ser desarrollados bajo estándares técnicos institucionales definidos por la DNTIC, incluyendo estructura de código, nomenclatura, arquitectura, documentación y buenas prácticas de programación,
- b) **Control de versiones:** Todo desarrollo deberá gestionarse mediante herramientas de control de versiones institucionales,

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

permitiendo la trazabilidad de cambios, versiones y actualizaciones;

- c) **Repositorios institucionales:** El código fuente de todos los sistemas deberán almacenarse en repositorios institucionales autorizados, garantizando su seguridad, disponibilidad y control;
- d) **Documentación obligatoria:** Todo sistema deberá contar con documentación técnica y funcional actualizada, incluyendo especificaciones, arquitectura, manuales técnicos y de usuario;
- e) **Seguridad desde el diseño:** Los sistemas deberán incorporar medidas de seguridad desde su etapa de desarrollo, considerando controles de acceso, validación de datos, protección de información y prevención de vulnerabilidades,
- f) **Interoperabilidad:** Los sistemas deberán diseñarse de manera que permitan su integración con otros sistemas institucionales, facilitando el intercambio de información conforme a estándares definidos,
- g) **Uso de estándares abiertos y software libre:** Se deberá priorizar la adopción de tecnologías basadas en estándares abiertos y software libre, en concordancia con la normativa nacional y la soberanía tecnológica;
- h) **Ambientes de desarrollo diferenciados:** Todo sistema deberá contar con ambientes separados de desarrollo, pruebas y producción, evitando la manipulación directa en entornos productivos,
- i) **Control de calidad:** Los desarrollos deberán someterse a procesos de revisión técnica, pruebas y validación antes de su implementación en producción;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- j) **Autorización institucional:** Ningún sistema informático podrá ser desarrollado, adquirido o implementado sin la autorización y validación técnica de la DNTIC;

Queda prohibido el desarrollo, implementación o uso de sistemas informáticos institucionales fuera del marco normativo establecido en el presente artículo, así como el uso de software no autorizado o no validado por la DNTIC.

La DNTIC podrá establecer lineamientos adicionales, metodologías de desarrollo, herramientas tecnológicas y estándares específicos en función de la evolución tecnológica y las necesidades institucionales.

Artículo 34°.NORMAS PARA DISEÑO DE BASE DE DATOS

La EMI establece que el diseño, implementación y gestión de bases de datos institucionales deberá cumplir obligatoriamente con normas técnicas que garanticen la integridad, consistencia, seguridad, disponibilidad y correcto uso de la información institucional.

La DNTIC, es la instancia responsable de definir, supervisar y estandarizar las normas para el diseño de bases de datos, en concordancia con los lineamientos de gobierno de datos y desarrollo de sistemas institucionales.

El diseño de bases de datos deberá regirse por los siguientes lineamientos:

- a) **Modelo de datos:** Toda base de datos deberá diseñarse utilizando modelos formales estructurados (tales como el modelo relacional) o modelos no estructurados/semiestructurados (tales como bases NoSQL, orientadas a grafos o documentos), debidamente documentados y seleccionados según el

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

requerimiento técnico, escalabilidad y la arquitectura tecnológica institucional";

- b) **Normalización de datos:** Las estructuras de datos deberán cumplir principios de normalización que eviten redundancia innecesaria, inconsistencias y dependencia de datos;
- c) **Integridad de datos:** Se deberán garantizar mecanismos de integridad mediante el uso de claves primarias, claves foráneas, restricciones y validaciones que aseguren la consistencia de la información;
- d) **Gobierno y responsabilidad del dato:** Cada conjunto de datos deberá estar asociado a un área usuaria responsable, conforme al modelo de gobierno de datos institucional;
- e) **Seguridad de la información:** Las bases de datos deberán implementar controles de acceso, cifrado de datos sensibles, gestión de privilegios y protección contra accesos no autorizados;
- f) **Separación de ambientes:** Las bases de datos deberán operar en ambientes diferenciados (desarrollo, pruebas y producción), evitando la manipulación directa de datos en entornos productivos;
- g) **Auditoría y trazabilidad:** Las bases de datos deberán incorporar mecanismos de registro que permitan identificar modificaciones, accesos y operaciones realizadas sobre la información;
- h) **Interoperabilidad de datos:** Las estructuras de datos deberán diseñarse de forma que faciliten el intercambio de información entre sistemas institucionales, en concordancia con estándares definidos por la DNTIC;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- i) **Respaldo y recuperación:** Las bases de datos deberán contar con mecanismos de respaldo periódico y procedimientos de recuperación ante fallas o pérdida de información;
- j) **Documentación obligatoria:** Toda base de datos deberá contar con documentación actualizada que incluya estructura, relaciones, diccionario de datos, definiciones y responsabilidades asociadas.

Queda prohibida la creación, modificación o uso de bases de datos institucionales fuera de los estándares definidos por la DNTIC, así como la generación de repositorios de datos no autorizados o no documentados.

La DNTIC, podrá establecer normas adicionales, herramientas y procedimientos técnicos para la gestión, optimización y control de bases de datos, conforme a la evolución tecnológica y necesidades institucionales.

Artículo 35°.NORMAS DE SEGURIDAD EN EL DESARROLLO

La EMI establece que todo desarrollo de sistemas informáticos institucionales deberá incorporar medidas de seguridad desde su diseño, implementación y mantenimiento, con el fin de proteger la información, los procesos institucionales y la infraestructura tecnológica frente a riesgos y amenazas.

La DNTI, es la instancia responsable de definir, implementar y supervisar las normas de seguridad en el desarrollo de software, en concordancia con las políticas de ciberseguridad institucional.

Los desarrollos de sistemas deberán cumplir obligatoriamente con los siguientes lineamientos de seguridad:

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- a) **Seguridad por diseño:** Los sistemas deberán incorporar controles de seguridad desde las fases iniciales de análisis y diseño, considerando riesgos, amenazas y requerimientos de protección de información;
- b) **Validación de entradas y salidas:** Se deberán aplicar mecanismos de validación y control sobre los datos ingresados y procesados por el sistema, a fin de evitar vulnerabilidades y errores;
- c) **Protección contra vulnerabilidades:** Los sistemas deberán implementar medidas de protección frente a amenazas comunes, tales como inyección de código, accesos no autorizados, manipulación de datos y otras vulnerabilidades de aplicaciones;
- d) **Gestión de autenticación y autorización:** Se deberán implementar mecanismos seguros de autenticación y control de accesos, de acuerdo con los perfiles de usuario definidos;
- e) **Protección de datos sensibles:** La información de carácter sensible deberá ser protegida mediante mecanismos de cifrado, enmascaramiento o control de acceso adecuado;
- f) **Gestión segura de credenciales:** Queda prohibido el almacenamiento de contraseñas o credenciales en texto plano, debiendo utilizarse mecanismos seguros de almacenamiento y gestión;
- g) **Registro y monitoreo:** Los sistemas deberán generar registros de auditoría que permitan el seguimiento de accesos y actividades relevantes;
- h) **Actualización y parches de seguridad:** Los sistemas deberán ser mantenidos actualizados, aplicando correcciones de

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

seguridad y mejoras continuas;

- i) **Pruebas de seguridad:** Previa a su implementación, los sistemas deberán someterse a pruebas de seguridad que permitan identificar y corregir vulnerabilidades;
- j) **Revisión de código:** La DNTIC podrá establecer mecanismos de revisión técnica del código fuente para asegurar el cumplimiento de estándares de seguridad,

Todo desarrollo deberá cumplir con estándares y buenas prácticas de seguridad de la información, priorizando la protección de los activos institucionales y la confiabilidad de los sistemas.

Queda prohibida la implementación de sistemas que no cumplan con las normas de seguridad establecidas en el presente artículo.

La DNTIC podrá establecer lineamientos, herramientas y procedimientos adicionales en materia de seguridad en el desarrollo, conforme a la evolución tecnológica y a los riesgos identificados.

Artículo 36°.NORMAS DE CALIDAD DE SOFTWARE

La EMI establece que todo sistema informático institucional deberá cumplir con normas de calidad de software que garanticen su correcto funcionamiento, confiabilidad, eficiencia, seguridad y adecuación a los requerimientos institucionales.

La DNTIC, es la instancia responsable de definir, implementar y supervisar los estándares y criterios de calidad aplicables al desarrollo y mantenimiento de sistemas informáticos.

Los sistemas deberán cumplir obligatoriamente con los siguientes

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

lineamientos de calidad:

- a) **Cumplimiento de requerimientos:** El sistema deberá satisfacer los requerimientos funcionales y técnicos definidos durante su fase de análisis;
- b) **Pruebas obligatorias:** Todo sistema deberá someterse a pruebas técnicas, funcionales y de integración antes de su implementación, incluyendo validación de resultados esperados;
- c) **Pruebas de usuario:** El sistema deberá ser validado por el área usuaria responsable, mediante procesos de aceptación formal que garanticen su funcionamiento conforme a los requerimientos establecidos;
- d) **Disponibilidad y rendimiento:** El sistema deberá operar de manera estable, garantizando tiempos de respuesta adecuados y continuidad en su funcionamiento;
- e) **Usabilidad:** Los sistemas deberán diseñarse considerando facilidad de uso, accesibilidad y comprensión por parte de los usuarios institucionales;
- f) **Mantenibilidad:** El software deberá estar estructurado de forma que permita su actualización, mejora y corrección sin afectar su operatividad;
- g) **Compatibilidad:** Los sistemas deberán ser compatibles con la infraestructura tecnológica institucional y otros sistemas existentes;
- h) **Documentación de calidad:** Todo sistema deberá contar con documentación que permita su comprensión, uso, mantenimiento y evolución;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- i) **Control de errores:** Los sistemas deberán incorporar mecanismos de detección, registro y manejo de errores que permitan su corrección oportuna;
- j) **Mejora continua:** Los sistemas deberán ser evaluados periódicamente para identificar oportunidades de mejora en su funcionamiento y desempeño.

La implementación de sistemas en ambiente de producción deberá contar con la validación técnica de la DNTIC y la aceptación formal del área usuaria, siendo obligatoria la verificación de cumplimiento de los criterios de calidad establecidos.

Queda prohibida la implementación de sistemas que no hayan cumplido con los procesos de prueba, validación y control de calidad definidos en el presente artículo.

La DNTIC, podrá establecer metodologías, herramientas y procedimientos adicionales para asegurar la calidad de los sistemas informáticos, conforme a las necesidades institucionales y evolución tecnológica.

Artículo 37°.NORMAS DE IMPLEMENTACIÓN

La EMI establece que la implementación de sistemas informáticos institucionales deberá realizarse bajo procedimientos controlados que garanticen la estabilidad operativa, la seguridad de la información y la continuidad de los servicios tecnológicos.

La DNTIC, es la instancia responsable de planificar, autorizar, ejecutar y supervisar las actividades de implementación de sistemas informáticos en ambiente de producción.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

La implementación de sistemas deberá regirse por los siguientes lineamientos:

- a) **Validación previa obligatoria:** Todo sistema deberá contar con pruebas técnicas, funcionales y de seguridad aprobadas, así como con la validación formal del área usuaria, antes de su implementación;
- b) **Gestión de cambios:** La implementación deberá realizarse bajo procedimientos formales de gestión de cambios, debidamente autorizados y documentados;
- c) **Ambiente controlado de producción:** El despliegue de sistemas deberá efectuarse en entornos productivos controlados, evitando modificaciones directas sin autorización previa;
- d) **Respaldo previo (backup):** Antes de cualquier implementación o actualización, se deberán realizar respaldos de los sistemas, bases de datos y configuraciones, a fin de garantizar la recuperación en caso de fallas;
- e) **Plan de reversión (rollback):** Toda implementación deberá contar con un plan de contingencia que permita revertir cambios en caso de errores o fallas críticas;
- f) **Registro de implementación:** Todas las actividades de implementación deberán quedar debidamente documentadas y registradas para efectos de control, trazabilidad y auditoría;
- g) **Minimización de impacto:** Las implementaciones deberán planificarse de manera que reduzcan el impacto en la operación institucional, preferentemente en horarios definidos por la DNTIC;
- h) **Monitoreo post - implementación:** Posterior a la

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

implementación, se deberá realizar el seguimiento del sistema para verificar su correcto funcionamiento y estabilidad;

- i) Comunicación institucional:** Las implementaciones que afecten sistemas o servicios deberán ser comunicadas oportunamente a los usuarios o áreas involucradas.

Queda prohibida la implementación de sistemas, actualizaciones o cambios directamente en ambiente de producción sin cumplir los procedimientos establecidos en el presente artículo.

La DNTIC, podrá establecer metodologías, herramientas y procedimientos complementarios para la gestión de implementaciones, conforme a las necesidades institucionales y avances tecnológicos.

Artículo 38°.ARQUITECTURA TECNOLÓGICA

La EMI establece la Arquitectura Tecnológica Institucional como el conjunto organizado de principios, estándares, modelos, componentes y lineamientos que definen la estructura, integración, operación, seguridad y evolución de los sistemas informáticos, infraestructura tecnológica y servicios digitales institucionales.

La DNTIC, es la instancia rectora responsable de diseñar, implementar, actualizar y controlar la arquitectura tecnológica institucional, asegurando su alineación con el Plan Estratégico Institucional (PEI), la normativa vigente y los objetivos estratégicos de transformación digital de la EMI.

La arquitectura tecnológica institucional se registrará por los siguientes lineamientos:

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- a) **Integración sistémica:** Los sistemas académicos, administrativos, financieros y de apoyo deberán operar de forma integrada en un entorno tecnológico unificado, evitando la existencia de soluciones aisladas o no interoperables;
- b) **Sistema Integrado de Gestión (SIGA-EMI):** La arquitectura tecnológica deberá orientarse a la implementación, consolidación y evolución del Sistema Integrado de Gestión de la EMI, como plataforma central para la automatización, control y gestión institucional;
- c) **Interoperabilidad institucional:** Los sistemas deberán intercambiar información mediante mecanismos estandarizados, asegurando consistencia, confiabilidad y eficiencia en la gestión de datos;
- d) **Estandarización tecnológica:** Las plataformas, herramientas, lenguajes, bases de datos y componentes tecnológicos deberán cumplir con los estándares definidos por la DNTIC, garantizando uniformidad, sostenibilidad y compatibilidad tecnológica;
- e) **Centralización de la información:** La información institucional deberá gestionarse en repositorios autorizados y controlados, evitando la duplicidad, dispersión o almacenamiento en sistemas no oficiales;
- f) **Escalabilidad y sostenibilidad:** La arquitectura deberá permitir la expansión, adaptación y evolución de los sistemas conforme a las necesidades institucionales y avances tecnológicos;
- g) **Seguridad de la arquitectura:** Todos los componentes tecnológicos deberán incorporar controles de seguridad que protejan la confidencialidad, integridad, disponibilidad y trazabilidad de la información;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- h) Soberanía tecnológica:** Se promoverá el uso de software libre, estándares abiertos y soluciones tecnológicas que permitan la independencia, control y sostenibilidad tecnológica institucional.

Toda iniciativa de desarrollo, adquisición, integración o implementación de soluciones tecnológicas deberá alinearse obligatoriamente a la arquitectura tecnológica institucional definida por la DNTIC.

Queda prohibida la implementación de sistemas o soluciones tecnológicas que no se integren a la arquitectura institucional o que generen entornos tecnológicos paralelos, fragmentados o no interoperables.

La DNTIC podrá emitir lineamientos, modelos de referencia, estándares técnicos y documentación complementaria necesarios para la gestión, control y evolución de la arquitectura tecnológica institucional.

Artículo 39°.PROHIBICIONES

En el ámbito del desarrollo, implementación, administración y uso de sistemas informáticos y recursos tecnológicos de la EMI, se establecen las siguientes prohibiciones:

- a)** Desarrollar, adquirir, implementar o utilizar sistemas informáticos institucionales sin la autorización, validación o supervisión técnica de la DNTIC;
- b)** Implementar cambios, modificaciones o actualizaciones en sistemas o bases de datos directamente en ambiente de producción sin cumplir los procedimientos de control establecidos;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- c)** Crear, mantener o utilizar bases de datos paralelas, no autorizadas o no documentadas, que contengan información institucional;
- d)** Almacenar información institucional en medios, plataformas o servicios no autorizados por la DNTIC, incluyendo servicios en la nube no institucionales;
- e)** Compartir, transferir o divulgar información institucional sin autorización o fuera de los procedimientos establecidos;
- f)** Utilizar software no autorizado, sin licencia o que no cumpla con los estándares técnicos definidos por la DNTIC;
- g)** Manipular, alterar o eliminar información institucional sin cumplir los procedimientos formales establecidos por la normativa vigente;
- h)** Compartir credenciales de acceso, utilizar cuentas de terceros o permitir el acceso no autorizado a sistemas institucionales;
- i)** Instalar, conectar o configurar equipos, dispositivos o redes no autorizadas en la infraestructura tecnológica institucional;
- j)** Deshabilitar, modificar o evadir mecanismos de seguridad implementados en sistemas, redes o servicios tecnológicos;
- k)** Omitir el registro, documentación o trazabilidad de actividades relacionadas con el desarrollo, implementación o uso de sistemas informáticos,
- l)** Realizar acciones que comprometan la integridad, disponibilidad, confidencialidad o seguridad de la información institucional;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- m)** Utilizar los recursos tecnológicos institucionales para fines personales, ilícitos o no relacionados con las funciones institucionales;

Las acciones descritas en el presente artículo serán consideradas incumplimientos graves a la normativa institucional y estarán sujetas a las medidas de control, responsabilidades administrativas y sanciones correspondientes, conforme a la normativa vigente de la EMI.

La DNTIC, en coordinación con las instancias competentes, podrá establecer controles adicionales para prevenir y detectar el incumplimiento de las disposiciones señaladas.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

CAPÍTULO VII CUMPLIMIENTO, CONTROL Y CAPACITACIÓN

Artículo 40°.PROHIBICIONES

El cumplimiento del presente Reglamento es de carácter obligatorio para todas las unidades organizacionales, personal militar, personal civil, docentes, administrativos, estudiantes, operadores de sistemas, usuarios autorizados y terceros que utilicen, administren o interactúen con los recursos tecnológicos de la EMI.

La DNTIC, en el ámbito de sus competencias, es responsable de velar por el cumplimiento de las disposiciones establecidas en el presente Reglamento, mediante la aplicación de controles técnicos, administrativos y operativos.

Las unidades organizacionales de la EMI deberán:

- a)** Cumplir con las políticas, normas técnicas, procedimientos y lineamientos establecidos en el presente Reglamento;
- b)** Coordinar con la DNTIC la implementación, uso y mejora de los sistemas informáticos, servicios digitales e infraestructura tecnológica;
- c)** Garantizar el uso adecuado de los recursos tecnológicos y la protección de la información institucional bajo su responsabilidad;
- d)** Aplicar las disposiciones relacionadas con la gestión de datos, seguridad de la información y control de accesos, conforme a sus competencias;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

La DNTIC, podrá establecer mecanismos de control, seguimiento y verificación del cumplimiento del presente Reglamento, incluyendo revisiones técnicas, monitoreo de sistemas, auditorías internas y reportes de gestión.

El incumplimiento de las disposiciones establecidas en el presente Reglamento dará lugar a la aplicación de medidas de control, responsabilidades administrativas y sanciones, conforme a la normativa institucional vigente.

Las disposiciones del presente Reglamento deberán ser aplicadas en coordinación con el Manual de Organización y Funciones (MOF), los Reglamentos Académicos (RAC) y demás normativa institucional aplicable, asegurando coherencia normativa y funcional.

Artículo 41°. SUPERVISIÓN Y AUDITORÍA TIC

La EMI establece que la supervisión y auditoría de las TIC constituyen mecanismos fundamentales para verificar el cumplimiento del presente Reglamento, asegurar la correcta gestión tecnológica institucional y garantizar la protección de la información.

La DNTIC, en el ámbito de sus competencias, es responsable de ejecutar actividades de supervisión técnica continua sobre los sistemas informáticos, infraestructura tecnológica, servicios digitales y gestión de datos institucionales.

La supervisión TIC comprende:

- a)** El monitoreo continuo del funcionamiento de los sistemas y servicios tecnológicos;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- b)** La verificación del cumplimiento de políticas, normas técnicas y procedimientos establecidos;
- c)** La evaluación del uso adecuado de los recursos tecnológicos institucionales;
- d)** El control de accesos, registros y trazabilidad de actividades en sistemas informáticos.

La auditoría TIC constituye un proceso formal de evaluación que podrá ser realizado de manera interna o externa, con el fin de:

- a)** Verificar el cumplimiento del marco normativo institucional en materia TIC;
- b)** Evaluar la eficacia de los controles de seguridad de la información y ciberseguridad;
- c)** Determinar la integridad, disponibilidad y confiabilidad de los sistemas y datos institucionales;
- d)** Identificar riesgos, vulnerabilidades y oportunidades de mejora en la gestión tecnológica;
- e)** Generar recomendaciones para fortalecer la gobernanza TIC y los procesos institucionales.

Las auditorías TIC podrán ser desarrolladas en coordinación con las instancias institucionales competentes, incluyendo áreas de control interno, auditoría y otras instancias autorizadas.

La DNTIC deberá disponer de registros, reportes, evidencias técnicas y documentación necesarias que permitan sustentar los procesos de supervisión y auditoría TIC.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Las unidades organizacionales y usuarios institucionales deberán colaborar con las actividades de supervisión y auditoría, proporcionando la información requerida en el marco de la normativa vigente.

Los resultados de las auditorías TIC podrán dar lugar a recomendaciones, acciones correctivas o la aplicación de medidas de control, conforme a la normativa institucional vigente.

El incumplimiento o la obstrucción de los procesos de supervisión y auditoría será considerado falta y estará sujeto a las acciones correspondientes conforme a la normativa institucional.

Artículo 42°.CAPACITACIÓN Y CONCIENCIACIÓN TECNOLÓGICA

La EMI establece que la capacitación y concienciación tecnológica como un proceso permanente orientado a fortalecer las competencias digitales de los usuarios institucionales, promover el uso adecuado de los recursos tecnológicos y garantizar el cumplimiento de las políticas de seguridad de la información.

La DNTIC, en coordinación con las instancias competentes, es responsable de planificar, organizar, ejecutar y evaluar programas de capacitación y concienciación en materia de TIC.

La capacitación tecnológica institucional se orientará a:

- a)** Fortalecer las habilidades y competencias digitales de los usuarios en el uso de sistemas informáticos, servicios digitales y herramientas tecnológicas institucionales;
- b)** Promover el cumplimiento de las políticas de seguridad de la

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

información y buenas prácticas en el uso de recursos tecnológicos;

- c)** Sensibilizar a los usuarios sobre riesgos asociados a la ciberseguridad, tales como accesos no autorizados, pérdida de información, ingeniería social y uso indebido de sistemas;
- d)** Capacitar en el uso adecuado de los sistemas institucionales, incluyendo el Sistema Integrado de Gestión (SIGA-EMI) y plataformas tecnológicas asociadas;
- e)** Difundir lineamientos sobre protección de datos, confidencialidad de la información y responsabilidad en la gestión de datos institucionales;
- f)** Fomentar la adopción de procesos de transformación digital en las unidades organizacionales.

La DNTIC podrá desarrollar programas, talleres, guías, manuales, campañas de concienciación y otros mecanismos de formación tecnológica, de acuerdo con las necesidades institucionales.

Las unidades organizacionales deberán participar y coadyuvar en los procesos de capacitación, promoviendo la asistencia de su personal y el cumplimiento de los lineamientos establecidos.

Los usuarios institucionales son responsables de participar en los procesos de capacitación y aplicar los conocimientos adquiridos en el ejercicio de sus funciones.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

CAPÍTULO VIII RESPONSABILIDADES E INCUMPLIMIENTOS

Artículo 43°.RESPONSABILIDADES

Todas las unidades organizacionales, personal militar, personal civil, docentes, administrativos, estudiantes, operadores de sistemas, usuarios autorizados y terceros que utilicen o interactúen con los recursos tecnológicos de la EMI son responsables del cumplimiento de las disposiciones establecidas en el presente Reglamento.

Las responsabilidades en materia de TIC son de carácter personal e institucional, debiendo ser ejercidas de acuerdo con las funciones asignadas, el Manual de Organización y Funciones (MOF) y la normativa vigente.

Son responsabilidades generales de los usuarios y unidades organizacionales:

- a)** Utilizar los sistemas informáticos, servicios digitales y recursos tecnológicos institucionales de manera adecuada, responsable y conforme a su finalidad;
- b)** Cumplir con las políticas, normas técnicas, procedimientos y lineamientos establecidos en el presente Reglamento;
- c)** Proteger la información institucional a la que tengan acceso, garantizando su confidencialidad, integridad y disponibilidad;
- d)** No compartir credenciales de acceso ni permitir el uso de sus cuentas por terceros;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- e) Registrar y gestionar información veraz, completa y oportuna en los sistemas institucionales, conforme a sus funciones;
- f) Reportar oportunamente incidentes, fallas, vulnerabilidades o eventos que puedan afectar la seguridad o funcionamiento de los sistemas;
- g) Respetar los procedimientos establecidos para el uso, modificación y validación de la información institucional;
- h) Participar en programas de capacitación y concienciación tecnológica promovidos por la DNTIC;
- i) Salvaguardar los equipos, dispositivos y recursos tecnológicos asignados, evitando su uso indebido o no autorizado;
- j) Cumplir con las políticas de control de acceso, seguridad de la información, gobierno de datos y uso de infraestructura tecnológica.

Las autoridades y responsables de unidades organizacionales deberán asegurar el cumplimiento de las disposiciones del presente Reglamento dentro de sus áreas, promoviendo el uso adecuado de las tecnologías y la correcta gestión de la información.

La DNTIC, es responsable de garantizar la administración tecnológica, emitir lineamientos técnicos y supervisar el cumplimiento de las disposiciones establecidas en el presente Reglamento.

Artículo 44°. TIPIFICACIÓN DE FALTAS INFORMÁTICAS

Las acciones u omisiones que contravengan las disposiciones establecidas en el presente Reglamento serán consideradas faltas

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

informáticas y estarán sujetas a medidas de control y sanción conforme a la normativa institucional vigente.

Las faltas informáticas se clasifican en leves, graves y muy graves, en función de su impacto sobre la seguridad de la información, la operación de los sistemas y los intereses institucionales.

a) Faltas leves: Son aquellas acciones u omisiones que no comprometen de manera significativa la seguridad, integridad o continuidad de los sistemas, tales como:

- 1.- Utilizar los recursos tecnológicos institucionales para el acceso a plataformas de entretenimiento o fines ajenos a las funciones designadas, por primera vez y sin generar perjuicio operativo;
- 2.- Omitir el llenado de registros en los sistemas de información excediendo los plazos establecidos en los manuales procedimentales, sin comprometer la integridad de la base de datos;
- 3.- Incumplimiento menor de procedimientos establecidos para el uso de sistemas;
- 4.- Omisión en el registro oportuno de información sin afectar su integridad;
- 5.- Retraso en la atención de requerimientos o reportes relacionados con TIC.

b) Faltas graves: Son aquellas acciones u omisiones que afectan el funcionamiento de los sistemas, la integridad de los datos o el cumplimiento normativo institucional, tales como:

- 1.- Uso indebido o no autorizado de sistemas informáticos institucionales;
- 2.- Manipulación de información institucional sin cumplir los procedimientos establecidos;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- 3.- Compartir credenciales o permitir el acceso a terceros no autorizados;
- 4.- Almacenamiento de información institucional en plataformas no autorizadas;
- 5.- Instalación de software o conexión de dispositivos sin autorización de la DNTIC,
- 6.- Incumplimiento reiterado de políticas de seguridad de la información;
- 7.- Obstaculización de procesos de control, supervisión o auditoría TIC.

c) Faltas muy graves: Son aquellas acciones u omisiones que comprometen la seguridad institucional, la integridad de la información o generan daño significativo a los sistemas o a la institución, tales como:

- 1.- Alteración, eliminación o manipulación intencional de datos institucionales sin autorización;
- 2.- Acceso no autorizado a sistemas, bases de datos o información sensible;
- 3.- Uso de sistemas informáticos con fines ilícitos, fraudulentos o contrarios a la normativa institucional;
- 4.- Desarrollo, implementación o uso de sistemas paralelos que comprometan la integridad de la información institucional;
- 5.- Sabotaje, daño intencional o alteración de infraestructura tecnológica;
- 6.- Divulgación no autorizada de información confidencial o sensible;
- 7.- Cualquier acción que genere pérdida significativa de información, interrupción de servicios o afectación institucional grave.

La clasificación de la falta deberá considerar su impacto, intencionalidad, reincidencia y consecuencias sobre los sistemas, los

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

datos y la institución.

Las faltas tipificadas en el presente artículo serán evaluadas por las instancias competentes, pudiendo dar lugar a medidas correctivas, disciplinarias o legales conforme a la normativa vigente de la EMI.

Artículo 45°.MEDIDAS SANCIONATORIAS

Las faltas informáticas establecidas en el presente Reglamento darán lugar a la aplicación de medidas correctivas, disciplinarias y/o sancionatorias, conforme a la gravedad de la falta, su impacto institucional, la intencionalidad y la reincidencia del infractor, en concordancia con la normativa vigente de la EMI.

Las medidas sancionatorias serán aplicadas por las instancias competentes, de acuerdo con el tipo de personal o usuario involucrado, considerando el Estatuto Orgánico, el Reglamento de Régimen Interno, los Reglamentos Académicos (RAC), el Manual de Organización y Funciones (MOF) y demás disposiciones institucionales aplicables.

Las sanciones podrán comprender, entre otras, las siguientes medidas:

- a)** Amonestación verbal o escrita;
- b)** Suspensión temporal de accesos a sistemas, servicios digitales o recursos tecnológicos institucionales;
- c)** Restricción o cancelación de privilegios en sistemas informáticos;
- d)** Separación temporal o definitiva de funciones relacionadas con el uso o administración de sistemas;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- e) Procesos administrativos disciplinarios internos conforme a la normativa institucional vigente;
- f) Remisión a instancias superiores o jurisdiccionales competentes, en caso de que la falta implique responsabilidades civiles, administrativas o penales;
- g) Reparación de daños ocasionados a los sistemas, infraestructura tecnológica o información institucional, cuando corresponda;

La asignación de sanciones se realizará en función de la clasificación de la falta, conforme a los siguientes criterios:

- a) **Faltas leves:** Podrán dar lugar a amonestaciones verbales o escritas, así como medidas correctivas;
- b) **Faltas graves:** Podrán dar lugar a suspensión temporal de accesos, restricción de privilegios o inicio de procesos administrativos disciplinarios;
- c) **Faltas muy graves:** Podrán dar lugar a la suspensión total de accesos, separación de funciones, procesos administrativos, civiles o penales conforme a la normativa vigente.

La aplicación de sanciones deberá regirse por los principios de proporcionalidad, debido proceso, legalidad y responsabilidad, garantizando el derecho a la defensa del presunto infractor.

Las acciones sancionatorias derivadas del incumplimiento del presente Reglamento se aplicarán sin perjuicio de otras responsabilidades establecidas en la normativa institucional o en la legislación nacional vigente.

La DNTIC, podrá emitir informes técnicos cuando corresponda, a fin

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

de sustentar los procesos de evaluación y determinación de responsabilidades.

El incumplimiento reiterado de las disposiciones establecidas en el presente Reglamento podrá agravar la sanción correspondiente conforme a la normativa institucional vigente.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

CAPÍTULO IX DISPOSICIONES FINALES

Artículo 46°.ACTUALIZACIÓN NORMATIVA

El presente Reglamento de Tecnologías de Información y Comunicación, deberá ser objeto de revisión periódica, con el propósito de asegurar su actualización, pertinencia y alineación con la evolución tecnológica, la normativa nacional vigente y los objetivos estratégicos de la EMI.

La DNTIC, es la instancia responsable de proponer la actualización, modificación o complementación del presente Reglamento, en coordinación con las instancias institucionales competentes.

La actualización normativa deberá considerar, al menos, los siguientes aspectos:

- a)** Cambios en la normativa nacional aplicable en materia de telecomunicaciones, tecnologías de información, gobierno digital, seguridad de la información y protección de datos;
- b)** Modificaciones en la estructura organizacional, el Manual de Organización y Funciones (MOF) y la normativa interna de la EMI;
- c)** Evolución de la arquitectura tecnológica institucional, sistemas informáticos y servicios digitales;
- d)** Resultados de auditorías, supervisiones y evaluaciones técnicas realizadas;
- e)** Identificación de riesgos, vulnerabilidades o necesidades de mejora en la gestión tecnológica institucional;

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

- f) Avances tecnológicos, buenas prácticas y estándares internacionales aplicables.

Las propuestas de actualización deberán ser elevadas a la autoridad competente para su revisión, validación y aprobación conforme a los procedimientos institucionales vigentes.

La implementación de modificaciones al presente Reglamento será de aplicación obligatoria desde su aprobación formal, debiendo ser difundida a todas las unidades organizacionales y usuarios institucionales.

La DNTIC podrá emitir lineamientos, instructivos y disposiciones complementarias para la adecuada aplicación del presente Reglamento, sin contradecir su contenido.

Artículo 47º. VIGENCIA

El presente Reglamento de Tecnologías de Información y Comunicación de la EMI entrará en vigencia a partir de la fecha de su aprobación mediante Resolución expresa de la autoridad competente.

A partir de su entrada en vigencia, todas las disposiciones contenidas en el presente Reglamento serán de cumplimiento obligatorio para las unidades organizacionales, personal militar, personal civil, docentes, administrativos, estudiantes, operadores de sistemas, usuarios autorizados y terceros vinculados al uso, gestión o administración de recursos tecnológicos institucionales.

Quedan sin efecto todas las disposiciones, normas internas, instructivos o prácticas institucionales que sean contrarias al presente Reglamento.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

La DNTIC, en coordinación con las instancias competentes, deberá realizar la difusión del presente Reglamento dentro de la institución, a fin de garantizar su conocimiento, aplicación y cumplimiento.

Las unidades organizacionales deberán adoptar las medidas necesarias para la implementación y adecuación a las disposiciones del presente Reglamento, en el ámbito de sus competencias.

ANEXOS

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

ANEXO A FORMULARIO DE REQUERIMIENTO PARA DESARROLLO, MEJORA O INTEGRACIÓN DE SISTEMAS

DATOS GENERALES

DATOS	INFORMACIÓN
Unidad Solicitante	
Responsable Solicitante	
Cargo	
Correo Institucional	
Fecha de Solicitud	
Teléfono Interno	

INFORMACIÓN DEL REQUERIMIENTO

Nombre del Sistema o Módulo

Tipo de Solicitud

- ☐ Nuevo Sistema
- ☐ Nuevo Módulo
- ☐ Mejora
- ☐ Integración
- ☐ Reporte
- ☐ Aplicación Móvil
- ☐ Otro

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Descripción de la Necesidad

Objetivo del Requerimiento

Beneficios Esperados

- ☐ Optimización de Procesos
- ☐ Reducción de Tiempo
- ☐ Automatización
- ☐ Seguridad
- ☐ Integración Institucional
- ☐ Gobierno Digital
- ☐ Otro

Usuarios Beneficiarios

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

Información que Administrará

- ☐ Académica
 - ☐ Administrativa
 - ☐ Financiera
 - ☐ Recursos Humanos
 - ☐ Investigación
 - ☐ Otra
-

Nivel de Prioridad

- ☐ Alta
 - ☐ Media
 - ☐ Baja
-

VALIDACIÓN

Responsable del Área Solicitante

Nombre:

Firma:

Fecha:

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

USO EXCLUSIVO DE LA DNTIC

ASPECTO	RESULTADO
Factibilidad Técnica	
Factibilidad Operativa	
Factibilidad Económica	
Recomendación	
Prioridad Institucional	

Responsable de Evaluación DNTIC:

Nombre: _____

Firma: _____

Fecha: _____

APROBACIÓN

- ☐ Aprobado
☐ Observado
☐ Rechazado

Autoridad Competente: _____

Firma: _____

Fecha: _____

RECOMENDACIONES GENERALES

El presente formulario deberá ser requerido en oficinas de la DNTIC. Para su llenado correspondiente.

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

ANEXO B FORMULARIO DE SOPORTE TÉCNICO

		FORMULARIO DE SOPORTE TÉCNICO		Escuela Militar de Ingeniería DNTIC Área de Soporte Técnico 2025 – F – 002	
1. INFORMACIÓN DEL USUARIO					
NOMBRE DEL SOLICITANTE:		CARGO:		DÍA	MES
LUGAR DE TRABAJO		ÁREA	CELULAR / INTERNO	# CASO (Soporte Técnico)	
2. INFORMACIÓN GENERAL DEL SOPORTE					
Indique el motivo de su solicitud marcando alguna(s) de las opciones sombreadas y en negrilla.					
☐ Asistencia Técnica Indique los problemas que presenta el equipo:		☐ Revisión y/o Mantenimiento Indique los dispositivos con problemas:		☐ Instalar / Reinstalar Programas Seleccione los programas a instalar:	
☐ No enciende. ☐ Se reinicia ☐ Malware (virus) ☐ Configurar correo ☐ Archivos perdidos ☐ Bloqueo /Lentitud ☐ Mensaje de error ☐ Conexión a la Red ☐ Configuración de impresora ☐ Otros		☐ Impresora ☐ Teclado ☐ Pantalla ☐ Regulador ☐ CPU ☐ Parlante ☐ Mouse ☐ Otros		☐ Todos (Completa) ☐ Aplicaciones ☐ Office ☐ Lector PDF ☐ Driver ☐ Antivirus ☐ Restablecimiento de credenciales SIGA-EMI. ☐ Soporte para acceso a Servicios de Nube. ☐ Configuración/Contingencia de Firma Digital. ☐ Interrupción de conexión de Red. ☐ Falla de interoperabilidad de módulos. ☐ Otros	
OBSERVACIONES (Información adicional, breve detalle de las fallas, aclaración de otros problemas o lista de otros programas)					

	REGLAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	RAC-17
		VERSIÓN 1.0
		2026

☐ **Otros** (Si ninguna de las anteriores opciones satisface los requerimientos de su solicitud)

DESCRIPCIÓN (Breve detalle de su solicitud)

Recuerde firmar su solicitud en la parte inferior, favor no escribir en la siguiente sección, es para uso exclusivo del área de Soporte Técnico.

3. DIAGNOSTICO Y SOLUCIONES			
DIAGNOSTICO	DIA	MES	AÑO
SOLUCIÓN	DIA	MES	AÑO
OBSERVACIONES			

RECOMENDACIONES GENERALES

- 1.- Seleccionado **Todos** en la ficha de **Instalar / Reinstalar programas** el equipo se formateará y todos los datos del usuario contenido en la **partición del sistema operativo** (generalmente la C:\) se perderán, a menos que se indique que elementos. Se deberán respaldar previamente.
- 2.- Si solicita una copia de seguridad (respaldo), se lo realizara en un CD o DVD.
- 3.- Si requiere respaldar otras carpetas o archivos favor anotar la ruta completa de estos, ejemplo **"C:\PERSONAL\DOCUMENTOS"**. El área de Soporte Técnico no se hará responsable por el respaldo de los archivos de usuario que no se indiquen con claridad en la presente solicitud.
- 4.- El presente formulario deberá ser requerido en oficinas de la DNTIC. Para su llenado correspondiente.