

Supplementary Table S1. Composition and Selection of the Documentary and Technical Corpus

The corpus was assembled at the level of individual documentary or technical records and subsequently organized into 14 analytical evidence categories (E01–E14). Counts distinguish records initially identified, duplicated or superseded records removed, other exclusions based on the predefined analytical criteria, and the final records retained for analysis.

Evidence category	Evidence type	Initially identified	Duplicate / superseded removed	Other excluded	Final included	Period represented	Main exclusion / selection note
E01	Strategic IT planning (PETI)	2	0	0	2	July 2024	PETI and associated strategic-planning evidence retained.
E02	Institutional planning (PEDI and related planning records)	3	0	1	2	2023	Only planning records directly used to establish institutional alignment were retained.
E03	IT Committee minutes, resolutions, and governance records	10	2	1	7	2023–April 2026	Duplicate/superseded governance records and material without additional analytical value were excluded.
E04	Information Security Committee and security-governance records	6	1	1	4	2024–April 2026	Duplicated/superseded records and material outside the analytical purpose were excluded.
E05	EGSI, information-security policies, procedures, and risk records	10	2	1	7	to April 2025	Superseded policy/procedure versions and non-contributory material were excluded.
E06	Cloud-migration, continuity, rollback, monitoring, and incident records	8	1	1	6	2 September–10 October 2024 + post-migration monitoring	Only primary or traceable technical records supporting migration execution and post-migration monitoring were retained.
E07	API Gateway, microservices, interoperability, security, and logging records	9	1	1	7	2023–2025	Duplicate/superseded technical records and material not directly supporting the interoperability analysis were excluded.
E08	Institutional systems and process-automation documentation	14	2	1	11	2023–April 2026	Only system/process records directly contributing evidence to the application layer were retained.
E09	Dashboards, analytics, and decision-support reports	6	1	1	4	2024–April 2026	The final set retained only dashboards/reports directly analyzed for evidence-informed management.
E10	AI-assisted academic-production information-processing records, delivery records, and usability tests	4	1	1	2	2024–April 2026	Only records supporting the bounded AI-assisted function and human-reviewed institutional use were retained.
E11	UX/UI, accessibility, and usability-improvement records	6	1	1	4	2023–April 2026	Records were retained when they documented accessibility-oriented or user-centered design activity; no WCAG conformance claim was inferred.
E12	MMGSI-Cloud baseline, evidence matrix, gap analysis, roadmap, and follow-up records	12	2	1	9	June 2025–April 2026	Duplicate/superseded materials were removed; the final reassessment outside the case-study temporal boundary was excluded.
E13	DINARP authorization and public-interoperability documentation	4	0	0	4	December 2024	All retained records directly supported the legal, institutional, or operational basis of public interoperability.
E14	External Prosecutor’s Office review of the automated admission allocation process	4	0	1	3	January 2026	Only records directly examined in the study were retained; material merely referenced but not independently analyzed was excluded.
TOTAL	—	98	14	12	72	2023–April 2026	Final analytical corpus: 72 records organized into 14 evidence categories.

Note. Selection was conducted at the individual-record level. Records were retained when they originated from an identifiable institutional or external source, were directly relevant to at least one research question or MITD-UTMACH layer, and contained sufficient temporal and contextual information to support analytical interpretation. Duplicate records, superseded versions, purely promotional material, records outside the analytical scope, insufficiently verifiable material, and records that added no additional analytical evidence were excluded.

Confidentiality. Restricted institutional records are represented through evidence categories rather than reproduced. Server names, network identifiers, detailed technical configurations, personal data, and other operationally sensitive information are omitted.

Independent coding review. A second researcher independently reviewed 18 records (25% of the final corpus) using the finalized coding manual (Supplementary Table S2). The review confirmed the original coding assignments for all reviewed records, and no discrepancies requiring recoding were identified.

Supplementary Table S2. Coding Manual for the Documentary Analysis of MITD-UTMACH

Purpose. This coding manual operationalizes the deductive, inductive/refined, and higher-order analytical codes used to analyze the documentary and technical evidence supporting the reconstruction of MITD-UTMACH. Evidence examples are paraphrased to preserve institutional confidentiality.

Primary theme / MITD-UTMACH layer	Code	Origin	Operational definition	Inclusion rule	Representative evidence example	Principal evidence categories	RQ
Strategic Alignment	SA-01 Strategic alignment	Deductive	Evidence showing explicit linkage between institutional objectives and IT priorities, projects, resources, or actions.	Apply when a record connects institutional strategy with technology planning or prioritization.	PETI initiatives aligned with institutional development objectives.	E01, E02	RQ1, RQ4
Strategic Alignment	SA-02 Portfolio prioritization	Deductive/refined	Evidence showing selection, sequencing, or prioritization of digital initiatives according to institutional needs.	Apply when projects or initiatives are organized as an institutional portfolio rather than as isolated technical actions.	PETI project portfolio and prioritized technological initiatives.	E01, E02	RQ1
Governance and Management	GM-01 Decision rights and accountability	Deductive	Formal assignment of authority, responsibilities, oversight, or decision-making functions related to IT.	Apply to formal committees, roles, resolutions, or assigned responsibilities.	IT Committee, Information Security Committee, Information Security Officer, and Data Protection Delegate.	E03-E05	RQ1, RQ4
Governance and Management	GM-02 Security governance	Deductive	Institutional mechanisms governing information-security responsibilities, policies, risk, and controls.	Apply to evidence of formal security governance rather than isolated technical security measures.	Information Security Committee records and EGSI documentation.	E04, E05	RQ1, RQ2
Governance and Management	GM-03 Risk and compliance governance	Deductive	Evidence relating security, privacy, regulatory requirements, or institutional accountability to formal governance actions.	Apply when risks, controls, legal obligations, or compliance evidence influence institutional decisions.	EGSI controls, data-protection responsibilities, and DINARP conditions.	E04, E05, E13	RQ2, RQ4
Technological Architecture	TA-01 Cloud infrastructure	Deductive	Evidence of migration, deployment, or operation of institutional infrastructure in cloud environments.	Apply to documented cloud infrastructure decisions, migration actions, or resulting infrastructure capabilities.	Migration of 52 institutional servers.	E06	RQ1, RQ2
Technological Architecture	TA-02 Service continuity	Deductive/refined	Evidence of planning or controls intended to preserve institutional service operation during technological change.	Apply only when continuity planning, monitoring, recovery, or operational records are explicitly documented.	Migration records documenting continuity-oriented planning, 99.85% average uptime, and no critical incidents attributable to the migration during the documented monitoring period.	E06	RQ2, RQ4
Technological Architecture	TA-03 Technical interoperability	Deductive	Technical mechanisms enabling communication and information exchange among systems.	Apply to APIs, microservices, integration specifications, or system-to-system communication mechanisms.	API architecture and microservices specifications.	E07	RQ1, RQ2
Technological Architecture	TA-04 Governance-bound interoperability	Inductive/refined	Interoperability supported not only technically but also by formal authorization, institutional purpose, assigned responsibility, and security/data-protection conditions.	Apply when technical exchange is linked to institutional authorization or governance.	DINARP authorization governing access to public interoperability services.	E07, E13	RQ2, RQ4
Institutional Applications	IA-01 Integrated institutional applications	Deductive	Digital applications supporting academic or administrative university functions within the institutional ecosystem.	Apply to documented implementation or integration of institutional systems.	SIUTMACH, SIGEDA, EVEA, Help Desk, research, scholarship, and employment systems.	E08	RQ1, RQ2
Institutional Applications	IA-02 Process automation	Deductive	Replacement or reduction of manual activities through documented digital processing.	Apply only where the evidence establishes actual automated processing.	Automated admission allocation process.	E08	RQ2
Institutional Applications	IA-03 Process traceability and reviewability	Inductive/refined	Ability to reconstruct or review an institutional digital process through documented rules, records, or external review.	Apply when process evidence permits reconstruction or formal review of actions or outcomes.	Admission allocation records and Prosecutor's Office review.	E08, E14	RQ2, RQ4
Data-driven Management	DM-01 Institutional analytics	Deductive	Use of integrated institutional information, indicators, dashboards, or analytics to support management.	Apply where institutional data are transformed into information used for monitoring or decision support.	Institutional dashboards and analytics reports.	E09	RQ1, RQ2
Data-driven Management	DM-02 Evidence-informed decision support	Deductive/refined	Evidence that information products are made available to support accountable institutional decisions without replacing human judgment.	Apply when data outputs are connected to monitoring, planning, or management decisions.	Dashboards supporting academic and administrative monitoring.	E09	RQ2, RQ4
Data-driven Management	DM-03 AI-assisted information	Inductive	Bounded use of AI to support institutional information-processing tasks.	Apply only when AI assists a documented task and does not autonomously make the institutional	Organization, preliminary validation, and visualization of academic-production records.	E10	RQ2

Primary theme / MITD-UTMACH layer	Code	Origin	Operational definition	Inclusion rule	Representative evidence example	Principal evidence categories	RQ
	processing			decision.			
Data-driven Management	DM-04 Human oversight	Inductive	Explicit human verification, correction, or approval of technology- or AI-assisted outputs before institutional use.	Apply when authorized personnel remain responsible for validating outputs.	Human review of AI-assisted academic-production outputs.	E10	RQ2, RQ4
Cross-cutting Capability	CC-01 Accessibility-oriented design	Deductive	Evidence that accessibility or inclusive-design considerations were incorporated into digital-service development or redesign.	Apply to documented accessibility-oriented criteria without assuming formal WCAG compliance.	Accessibility guidelines and UX/UI redesign records.	E11	RQ2, RQ4
Cross-cutting Capability	CC-02 User-centered design / usability	Deductive	Evidence concerning navigation, usability, interface quality, or alignment with user needs.	Apply to UX/UI redesign or usability-improvement records.	Navigation and usability-improvement documentation.	E11	RQ2
Continuous Assessment and Improvement	CI-01 Evidence-based maturity assessment	Deductive	Systematic use of documentary and organizational evidence to assess cloud security governance capabilities.	Apply to evidence used in MMGSI-Cloud assessment rather than general implementation evidence alone.	MMGSI-Cloud assessment records and maturity reports.	E12	RQ3
Continuous Assessment and Improvement	CI-02 Gap identification	Deductive	Identification of weaknesses, incomplete capabilities, or improvement priorities derived from assessment evidence.	Apply when assessment evidence is explicitly translated into identified gaps or priorities.	MMGSI-Cloud gap analysis.	E12	RQ3
Continuous Assessment and Improvement	CI-03 Improvement roadmap	Deductive	Translation of assessment results into prioritized institutional improvement actions.	Apply to formal planning actions originating from identified assessment gaps.	MMGSI-Cloud improvement roadmap.	E12	RQ3, RQ4
Continuous Assessment and Improvement	CI-04 Monitoring and feedback	Inductive/refined	Evidence showing that implementation outcomes are monitored and fed back into assessment, planning, or strategic review.	Apply to documented follow-up or reassessment relationships connecting evidence to future institutional actions.	August 2025-April 2026 improvement follow-up.	E12	RQ3, RQ4
Cross-layer Mechanism	CM-01 Vertical alignment	Analytical / higher-order	Relationship connecting strategy and governance decisions with technological architecture, applications, and data management.	Apply during second-cycle coding when evidence demonstrates linkage across at least two architectural layers.	PETI priorities linked to governance and implemented technological initiatives.	E01-E09	RQ1, RQ4
Cross-layer Mechanism	CM-02 Governance-bound interoperability	Analytical / higher-order	Relationship combining technical interoperability with authorization, accountability, security, and data governance.	Apply only where technical and governance/legal evidence converge.	E07 technical integration interpreted jointly with E13 authorization.	E07, E13	RQ2, RQ4
Cross-layer Mechanism	CM-03 Evidence-based feedback loop	Analytical / higher-order	Relationship linking implementation evidence, assessment, gap identification, roadmap definition, monitoring, and strategic review.	Apply when evidence supports multiple consecutive stages of the continuous-improvement cycle.	E12 assessment and follow-up linked to the broader MITD-UTMACH architecture.	E01-E12	RQ3, RQ4

Note. Deductive codes were derived from the theoretical framework and research questions. Inductive/refined codes were incorporated or further specified during iterative documentary analysis when implementation characteristics were not fully represented by the initial coding structure. Higher-order analytical mechanisms were developed during second-cycle analysis to explain relationships among codes and MITD-UTMACH layers. Multiple coding was permitted when a documentary segment provided evidence for more than one analytical dimension. Codes were not treated as mutually exclusive; each assigned code required explicit support in the source record. Evidence examples are paraphrased to preserve institutional confidentiality and should not be interpreted as reproductions of restricted source documents.

Abbreviations. MITD-UTMACH, Integrated University Digital Transformation Model; MMGSI-Cloud, Maturity Model for Information Security Governance in Cloud Computing; PETI, Strategic Information Technology Plan; EGSI, Governmental Information Security Scheme; DINARP, Dirección Nacional de Registros Públicos; RQ, research question.

Supplementary Table S3. De-identified Summary of the Institutional Cloud-Migration Process and Post-Migration Monitoring

This supplementary table summarizes the cloud-migration evidence represented by E06. Server names, network identifiers, detailed configurations, and resource allocations are omitted for operational-security reasons.

Panel A. Migration sequence by operational lot

Migration lot	Execution period	Servers (n)	De-identified functional scope
Lot 1	2–8 September 2024	11	Base infrastructure and test environments; selected network/monitoring, support, and laboratory services.
Lot 2	9–18 September 2024	15	Web portals, repositories, and internal/support services.
Lot 3	19–29 September 2024	11	Academic and administrative applications, including selected learning and admission-related services.
Lot 4	30 September–10 October 2024	15	Critical systems, principal databases, core academic services, and authentication/directory services.
Total	2 September–10 October 2024	52	Institutional server portfolio migrated through four staged operational lots.

Panel B. Functional profile of the migrated server portfolio

Functional category	Servers (n)	Examples of institutional function (de-identified)
Institutional applications	15	Academic and administrative applications.
Web portals / CMS	8	Institutional websites and content-management services.
Databases	6	PostgreSQL/MySQL and other institutional data services.
Support / communication / utility services	6	Electronic signature, notifications, telephony, and related services.
Infrastructure / network / monitoring	6	DNS, proxy/balancing, monitoring, and supporting infrastructure.
Academic / e-learning platforms	5	Learning environments and academic platforms.
Authentication and directory services	3	Directory and authentication services.
Storage / repositories	3	Institutional repositories and file-storage services.
Total	52	—

Panel C. Continuity, rollback, and post-migration monitoring controls

Control domain	Documented practice
Migration modality	Private-cloud and virtualized IaaS environment; staged execution using proxy/load-balancing mechanisms where applicable.
Continuity safeguards	Migration activities were scheduled primarily during night/weekend maintenance windows, with gradual traffic redirection and verification that the target service was active before completion of each migration stage.
Rollback / recovery safeguards	Pre-migration hot snapshots and complete database/file backups were retained to support restoration if required.
Immediate technical verification	Network reachability and service ports, web-service responses, database connectivity, and authentication were checked after migration activities.
Monitoring variables	Availability of network/services, HTTP responses, CPU, RAM, disk utilization, response latency, database-service status, application/system logs, and reported incidents.
Monitoring sources	Zabbix availability/port checks, HTTP/Nginx logs, Linux/Windows system logs, application logs, and support-incident records.
Monitoring period	Post-migration monitoring continued for 15 days following the execution of each migration lot.

Panel D. Documented post-migration operational indicators

Indicator	Documented value	Interpretive boundary
Average server availability (uptime)	99.85%, calculated as the arithmetic mean of the individual uptime percentages of the monitored servers during their respective 15-day post-migration monitoring periods.	Institutional operational metric derived from post-migration monitoring records; not an independently audited availability or service-level metric.
Critical incidents attributable to migration	0 critical incidents involving outage of central services	Restricted to incidents documented as attributable to the migration during the monitored period.
Minor support requests	Cache- or DNS-related adjustments resolved within the first 24 hours of each migration window	Descriptive operational evidence; no standardized pre-migration baseline was available for formal effect-size comparison.

Note. The figures and practices summarized above were derived from the institutional technical migration matrix and associated operational information provided for evidence category E06. For each monitored server, uptime was calculated as the proportion of recorded available time relative to the expected monitored time during its respective 15-day post-migration monitoring window. The reported 99.85% average server uptime represents the arithmetic mean of the resulting individual server uptime percentages across the migrated server portfolio. The reported uptime and incident counts are documentary/operational indicators and should not be interpreted as independently audited availability or service-level metrics. No homogeneous historical baseline was available to support formal pre/post effect-size estimation.

Abbreviations. CMS = content management system; DNS = Domain Name System; HTTP = Hypertext Transfer Protocol; IaaS = Infrastructure as a Service; RAM = random-access memory.