

Type of the Paper: Article

Identity Governance and Digital Transformation of the University Document Ecosystem: A Socio-Technical Model with Microsoft Entra and Five OBS Domains

Luis Adrián Fernández Tenelanda^{1*}, Danna Yolanda Solis Espinoza²

¹ Pontificia Universidad Católica del Ecuador Sede Esmeraldas

² Pontificia Universidad Católica del Ecuador Sede Esmeraldas

luis.fernandez@pucese.edu.ec

Abstract: This article evaluates the sociotechnical governance of SharePoint Online and Microsoft Entra at PUCE Esmeraldas, integrating five OBS domains: strategy, digital transformation, operations, information and analytics, and governance/GRC. The corpus covers 172 days of evidence (March 4–August 22, 2026) and separates operational controls from unproven capabilities. Information architecture reaches level 3; automation is in transition 2→3; identity and access, GRC, and observability reach level 2; the conservative global level is 2. The document details 18 hubs, 24 sites, registered application authentication, metrics reduced from 180 to 5 minutes, and an access BPMN process. Conditional Access, PIM, Access Reviews, Lifecycle Workflows, and Purview remain NR until SKU availability and configuration export are secured. The result is a governed roadmap connecting value, security, adoption, and learning without mistaking licensable capabilities for actual results.

Keywords: IT governance; Microsoft Entra; Digital transformation; Change management; Higher education

Introduction

Implementing a repository does not guarantee transformation. Over time, new sites, personal workflows, unowned connections, permanent groups, and administrative decisions known only to single individuals inevitably emerge. The underlying risk is not purely technical: the university loses institutional memory, audit capacity, and operational continuity when the system depends on opaque configurations or specific individuals. Digital transformation alters how an organization creates value through digital technologies, requiring strategic, organizational, and cultural capabilities [4,5]. In higher education, this complexity is heightened by departmental autonomy, process diversity, privacy compliance requirements, and academic cycles. Consequently, governance must strike a balance between standardization and local flexibility. This article designs a sociotechnical model to govern the document ecosystem of PUCE Esmeraldas. It addresses three core questions: (Q1) How can technical decisions be aligned with institutional goals?; (Q2) What identity controls effectively reduce risk without impeding service delivery?; and (Q3) How can a maturity and adoption roadmap be structured? The framework aligns with five relevant modules from the current OBS plan applicable to this case, without attempting to replace the full curriculum [13]. Integrating Framework of Five Domains: (Sociotechnical Model of IT Governance and Transformation)

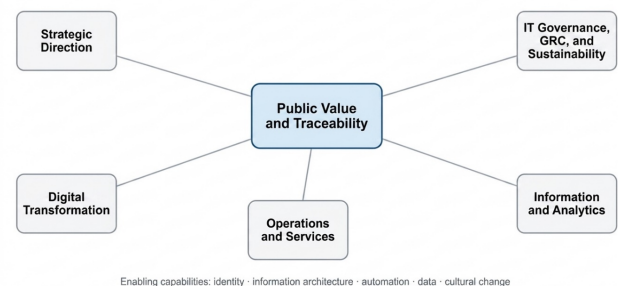


Figure 1. Integration of Five Domains to Govern Document Value

Table 1. OBS Framework Integration for Document Governance

Selected OBS Domain	Application to Document System	Governance Artifact	Metric
Strategic Direction	Align document families and capabilities with institutional goals	Benefits map and service portfolio	Realized vs. committed benefits
Digital Transformation	Redesign value chain, user experience, and operating model	Future VSM and adoption roadmap	PCE, adoption rate, and user satisfaction
Operations Management	Ensure availability, manage changes, problems, maintenance, and support	Service catalog, SLAs, and runbooks	SLA compliance, flow success rate, MTTR
Selected OBS Domain	Application to Document System	Governance Artifact	Metric
Information & Analytics	Data quality, event modeling, and evidence-based decision making	Data dictionary, dashboard, and review protocol	Data completeness, FTR, and cycle time
IT Governance, GRC & Sustainability	Decision rights, risk management, compliance, access control, and continuity	RACI matrix, controls, and risk register	Audit findings, access reviews, and residual risk

OBS presents digital transformation as the reinvention of value chains, and its Information Systems and Technologies Management program incorporates strategic direction, operations management, analytics, cybersecurity, and GRC. The selection above is justified by its direct correspondence with the document management problem; the authors should confirm that it

matches the specific edition taken and adjust module names if their academic syllabus differs. This integration avoids five critical biases: strategy without execution, automation without redesign, operations without learning, analytics without governance, and compliance without user experience. At the core of the model lie public value and traceability—technology is evaluated by its capacity to deliver reliable evidence within an acceptable risk tolerance Figure 1, Table 1.

Methodology

A case study approach integrated with Design Science Research is adopted. The artifact is built upon institutional requirements, document management principles, Zero Trust, and Microsoft 365 governance practices. Evaluation sources must include interviews with management and site owners, an inventory of sites and flows, Entra configurations, a role matrix, access logs, incidents, change records, benefit reviews, and adoption metrics. The analysis is organized into four key activities: maturity diagnosis, operating model design, control design, and roadmap sequencing. Each control is explicitly linked to a risk, an owner, operational evidence, and an exception decision. Validity is reinforced through cross-functional workshops, technical inspections, access exercises, and business continuity scenarios. Security is evaluated through a proportional approach. Conditional Access does not replace primary authentication, nor does it independently resolve authorization; policies must be tested in report-only mode and account for inter-application dependencies. Advanced features—such as PIM, access reviews, or lifecycle workflows—depend on specific licensing SKUs; the paper must explicitly declare the contracted licensing tier and avoid presenting unenabled capabilities as operational controls. Periods, Corpus, and Evidence Traceability The quantitative provisioning intervention was observed from March 4 to August 5, 2026 (155 calendar days). The migration logs subcorpus covers July 20 to August 5, 2026, inclusive (17 days). For the governance analysis, the documentary review was extended through August 22, 2026 (172 days from the start). These windows are declared separately to avoid attributing metrics captured exclusively in the July–August logs to the entire duration of the project. Source traceability and pseudonymization were applied. The publishable corpus contains no administrative email addresses, application IDs, usernames, secrets, private paths, or tenant object identifiers. Data that do not appear in verifiable exports or logs are marked as Not Reported (NR), rather than being imputed Table 2.

Table 2. Corpus and Verified Evidence Traceability

Evidence ID	Verified Artifact	Period / Version	Scientific Use
E01	Master provisioning script (950 lines; SHA-256 AAE76A1261608DA2...)	Aug 5, 2026	Architecture, objects, and implemented functions
E02	Migration engine (698 lines; SHA-256 BE078FBFA5F9A5CC...)	Jul 30, 2026	Simulation, execution, resumption, and reconciliation
E03	Technical README and local configuration	PowerShell 7.6.4; PnP.PowerShell 3.1.0	Requirements, parameters, and operational controls
E04	19 CSV files containing 70 events	Jul 20 to Aug 5, 2026	State distribution and migration scope
E05	Provisioning measurement log	Mar 4 to Aug 5, 2026	Time reduction (180 to 5 min) and throughput increase (10–15 to >150 sites/day)
E06	Component replication evidence and hub site association	2026	Pages, navigation, libraries, lists, backups, and validation
E07	Interactive authentication log with Entra registered app	2026	Workload identity without embedded secrets
E08	Technical log of simulation, confirmation, and restoration	2026	WhatIf mode, explicit confirmation, backup, and logical rollback

Results: Governance Model

Table 3. Baseline and Observed Results

Metric	Baseline	Result	Change / Interpretation	Source
Provisioning time per site	≈180 min	≈5 min	–175 min; 97.2% reduction	E05
Documented daily capacity	10–15 sites/day	>150 sites/day	>10× increase relative to manual upper bound	E05
Declared structure	Non-standardized	18 hubs + 24 sites	42 governable nodes in the manifest	E01
Document pattern per site	Heterogeneous	6 libraries + 24 standard folders	Repeatable and idempotent structure	E01
Migration logs	No comparable corpus	19 CSVs; 70 events	37 SIMULATED, 19 COPIED, and 14 ERROR	E04
Recorded migration scope	NR	4 sources; 5 destinations	Observed coverage; does not represent the entire tenant	E04

In Table 3, the reduction was calculated as . The capacity increase is conservatively expressed as greater than ten times because is compared against the upper bound of the baseline (). The 14 ERROR records do not constitute a failure rate: the log aggregates simulations, retries, and heterogeneous events, lacking a denominator of independent execution runs. Declaring this limitation explicitly prevents unsubstantiated causal inference. The master script declares six libraries per site—Administrative Management, Processes and Procedures, Regulations, Document Management, Monitoring and Control, and Archive—along with 24 standard folders. The architecture separates provisioning, migration, component replication, inventory, validation, and logging; personal permissions are not copied by default Table 4.

Table 4. Governance Maturity Assessment by Domain

Domain	Evidenced Level	Justification
Information Architecture	Level 3 — Automated	42-node manifest and standardized library/folder pattern
Automation	Transition Level 2 → Level 3	Executable scripts, simulation, and logging; comprehensive ALM not yet evidenced
Identity & Access Management	Level 2 — Standardized	Registered Entra application and interactive authentication; Conditional Access/PIM/Access Reviews marked as NR
GRC & Compliance	Level 2 — Standardized	Documented operational controls; Microsoft Purview and advanced retention policy integration marked as NR
Observability	Level 2 — Standardized	Operational CSV exports and execution logs; unified institutional telemetry and event model incomplete
Overall Governance Maturity	Level 2 — Standardized	Consolidation governed by the capability bottleneck rather than a simple mathematical average

Table 5. Licensing and Tenant Controls

Service / Control	Case Status	Evidentiary Basis	Editorial Treatment
SharePoint Online	Operational	Provisioned sites, hub associations, libraries, and logs (E01–E06)	Can be explicitly stated as fully implemented in production
Microsoft Entra & PnP Application	Operational	Registered application and interactive authentication records (E07)	Publish with pseudonymized tenant IDs, application IDs, and account details
Multi-Factor Authentication (MFA)	Reported in corpus	Institutional authentication mechanism; policy export not included	Claim with limitations; do not attribute full tenant-wide coverage
PowerShell / PnP.PowerShell	Operational	Local environment execution versions verified (E03)	Declare tool versions explicitly (PowerShell 7.6.4, PnP.PowerShell 3.1.0)
Power Automate, Power Apps, & Power BI	Designed	Missing solution exports or telemetry in current corpus	Mark as Not Reported (NR) regarding operational execution
Conditional Access	Not evidenced	Missing policy export configurations and SKU verification	Do not claim implementation; specify required Entra ID P1 license
PIM, Access Reviews, & Lifecycle Workflows	Not evidenced	Missing exported configuration files and SKU verification	Position as future roadmap milestones; verify Entra ID P2 / Governance SKU requirements
Microsoft Purview: Retention & Disposition	Not evidenced	Missing exported compliance labels or retention policies	Position as future roadmap milestones; validate required licensing plan

In Table 5, the absence of evidence does not equate to the absence of the service: it means that the available corpus does not allow for its verification. Prior to submission, a licensing administrator must export from the admin center the SKU, assigned units, and aggregate assignments, and an administrator for each service must export the relevant configurations. The manuscript retains NR until these artifacts are available.

4.1 Operating Model and Decision Rights

Table 6. Decision Rights and Governance Operating Matrix

Decision	Responsible Party	Consultation	Minimum Evidence	Cadence
Prioritize site families and benefits	Transformation Committee	Business units, Archive, IT	Value case, risk assessment, and VSM	Quarterly
Approve taxonomy and retention	Information Governance	Legal, Archive, Owners	Data dictionary, standard, and validation test	Per change / Annual
Decision	Responsible Party	Consultation	Minimum Evidence	Cadence
Approve architecture and connectors	Architecture/IT	Security and Product	Design, permissions, data, and support	Per version
Grant functional access	Resource Owner	Management and Security	Request, role, term, and approval	Per event
Activate privileged role	Security/Entra	Service Administrator	Justification, MFA, duration, and log	Just-in-time
Accept release	Product Owner	Users, IT, and Security	Testing, risks, rollback plan, and training	Per release
Close exception or risk	Risk Owner	Audit and Committee	Action plan, date, evidence, and residual risk	Monthly

The documentation product must have an executive sponsor, product owner, information owner, and technical lead. The committee establishes priorities and risks, but does not administer platform objects. Daily operations are distributed through explicit roles, and exceptions are subject to fixed expiration periods. This design reduces reliance on a global administrator and ensures accountability is fully auditable. Change management classifies modifications as standard, normal, or emergency. Workflows, applications, scripts, and configurations are versioned together; every release documents impact, test results, parameters, migration procedures, and rollback plans. Development, testing, and production environments are isolated through distinct groups, connections, and dedicated service accounts Table 6.

4.2 Identity Architecture with Microsoft Entra

Table 7. Entra Identity and Access Governance Controls

Control	Implementation Pattern	Mitigated Risk	Evidentiary Basis
Role-Based Groups	Assign access to groups with designated owners, clear descriptions, and defined lifecycles	Direct individual permissions and orphaned access	Group inventory, membership lists, and periodic review logs
Least Privilege	Assign the lowest role required; segregate administration, development, and operations	Privilege escalation, abuse, or administrative error	Role-task allocation matrix and negative access tests
MFA & Conditional Access	Enforce risk-, role-, device-, or location-based policies; run in report-only mode before enforcement	Credential compromise and unauthorized login vectors	Policy evaluation results, logs, and exception records
PIM / JIT Activation	Enforce time-bound role elevation requiring approval and justification (subject to SKU availability)	Standing or permanent administrative privileges	Elevation request logs, approval workflows, and review records
Access Reviews	Conduct periodic access certifications based on sensitivity; resource owners confirm or revoke	Entitlement drift and privilege accumulation	Decision logs, re-certification reports, and closure records

Control	Implementation Pattern	Mitigated Risk	Evidentiary Basis
Identity Lifecycle Management	Integrate onboarding, role changes, and offboarding with HR systems and resource owners	Stale accounts, active former employees, or obsolete access	Provisioning and revocation SLA execution logs
Workload Identities	Use certificates or managed identities with scoped permissions and scheduled credential rotation	Hardcoded secrets, static credentials, and over-privileged apps	Application inventory, owner assignment, and last-used logs
Emergency Access ("Break-Glass")	Maintain minimal excluded accounts with secured credentials and continuous monitoring	Complete tenant lockout due to aggressive conditional access policies	Periodic verification test logs and instant usage alerts

Microsoft defines Conditional Access as a Zero Trust policy engine that evaluates signals to enforce access decisions based on three core principles: explicit verification, least privilege, and assuming breach [9]. Applying this engine to the document ecosystem requires accounting for cross-service dependencies—such as Teams, Power Apps, and Power Automate accessing SharePoint resources—to prevent improperly tested policies from disrupting downstream workflows. In Table 7, workload identities require the same level of governance as user identities. Every application registration or service connection must maintain a clear operational purpose, designated owner, scoped permissions, target environment, authentication method, scheduled review date, and retirement plan. Embedding plain-text secrets directly within scripts or automation flows is treated as a security defect; when secrets cannot be avoided, they must be stored in a dedicated key vault service, periodically rotated, and strictly restricted from unauthorized read access.

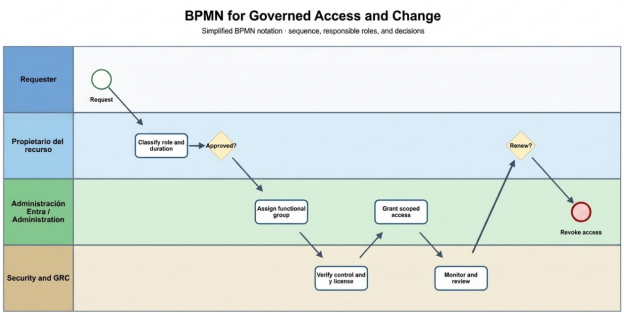


Figure 2. Simplified BPMN map of access grant, review, and revocation

When an advanced capability is not licensed or configured, the workflow does not treat it as operational: it records the limitation and applies the approved manual control. Conditional Access, PIM, and access reviews only transition to the automated branch after testing, configuration export, and license evidence Figure 2.

4.3 Maturity

Model

Table 8. Document Ecosystem Maturity Model

Level	Characteristics	Dominant Risk	Condition to Advance
1. Fragmented	Folders, email, individual permissions, and isolated workflows	Data loss, duplication, and operational dependence	Inventory, designated owners, and pilot project
2. Standardized	Minimum taxonomy, role-based groups, defined processes, and basic support	Uneven or inconsistent application	Testing, service catalog, and user adoption
3. Automated	Portable solutions, structured exceptions, and operational telemetry	Technical and automation debt	ALM, SLOs, and post-failure reviews
4. Governed	GRC, periodic access reviews, benefit tracking, and data-driven decisions	Complacency and ritualistic metrics	Organizational learning and effectiveness audits
5. Adaptive	Continuous optimization, reusable capabilities, and controlled deprecation	Systemic complexity	Evidence-backed innovation within defined boundaries

Maturity is not acquired by purchasing licenses. Each level demands explicit behavior and verified evidence. An institution is not considered governed simply because PIM is configured, but because high-impact roles are activated temporarily, reviewed, tied to specific tasks, and their exceptions systematically closed. Nor is an institution adaptive merely because it displays a dashboard, but because it deprecates obsolete metrics and refines services based on empirical evidence. The baseline evaluation is performed per domain rather than as a single aggregate average. At PUCE Esmeraldas, information architecture achieves Level 3; automation is in transition from Level 2 to 3; while identity and access, GRC, and observability remain at Level 2. The global maturity level is established at Level 2 because the system's operational bottleneck, rather than its mathematical average, dictates consolidated maturity Table 8.

4.4 Four-Wave Implementation

Roadmap

1. Wave 1 — Control and Visibility (0–90 days)

Inventory sites, workflows, applications, connections, groups, and owners; close critical access points; select pilot service families; establish the baseline and decision-making body.

2. Wave 2 — Standardization and Pilot (3–6 months)

Publish taxonomy, templates, functional groups, development standards, environments, and runbooks; deploy the pilot with security, accessibility, and user adoption testing.

3. Wave 3 — Governed Scaling (6–12 months)

Convert automations into formal solutions, automate provisioning, implement access reviews, establish the service catalog, KPI dashboard, and benefits management; systematically retire parallel channels. 4-Wave 4 — Optimization and Learning (12 months onwards). Apply periodic Value Stream Mapping (VSM), exception and reliability analysis, reusable architecture, business continuity drills, license and sustainability reviews, and controlled experiments with emerging technologies under ethical evaluation.

Table 9. Business Benefits, KPIs, and Risk Safeguards Matrix

Benefit	Enabling Capability	KPI	Risk / Safeguard
Timely Access to Evidence	Taxonomy, enterprise search, and role-based permissions	Search time; SLA fulfillment rate	Data overexposure / Access reviews
Reduced Cycle Time & Rework	VSM, source data capture, and automated workflows	P90 duration, PCE, FTR rate	Over-automation / Exception queue
Operational Continuity	ALM, runbooks, and designated system owners	Deployment success rate, MTTR, failed changes	Single point dependency / Testing and role rotation
Demonstrable Compliance	Retention policies, audit logs, and GRC controls	Coverage rate, audit findings	Excessive retention / Data minimization
Institutional Learning	Operational analytics, improvement backlog, and CoEs	Verified process improvements	Ritualistic metrics / Quarterly reviews

Discussion

The model demonstrates that governance is not equivalent to centralization. Leadership defines boundaries, standards, and evidence; operational units retain decisions close to the process within those boundaries. This controlled federation is particularly relevant in universities, where a rigid architecture can induce parallel solutions, while freedom without standards fragments the ecosystem. Aligning with the five OBS domains improves the trajectory of the case because it transforms the implementation into a systems management thesis: it connects objectives, value chain, service operation, analytics, and GRC. The academic contribution consists of five propositions: taxonomy conditions measurability; role-based access reduces permission debt; ALM reduces personal dependency; VSM prevents automating waste; and benefit reviews sustain transformation. Limitations include a single context, technological dependence, and a lack of complete Tenant data in this version. The effectiveness of controls cannot be inferred from their configuration; it requires testing, events, and exception reviews. Future research can compare campuses or document families, study longitudinal adoption, and evaluate total cost of ownership against alternatives.

Conclusions

A sustainable university document ecosystem requires strategic, operational, informational, and identity governance. Microsoft Entra provides controls to verify, limit, and review access; SharePoint and Power Platform provide information and process capabilities; but value emerges only when owners, decisions, metrics, and learning are institutionalized. The roadmap allows progress from global Level 2 toward measurable governance. The paper states which controls are operational and which remain NR; the next review must append SKU and configuration exports for any advanced capability transitioning from roadmap to implemented control.

Declarations Data and Code Availability

A Repositorio_reproducibilidad_PUCESE.zip repository was prepared containing RACI matrices, the maturity rubric, licensing models, CRediT declarations, BPMN diagrams, and aggregated evidence sanitized of tenant identifiers. The persistent identifier will be assigned upon depositing the package into an institutional or open-science repository.

Author Contributions (CRediT)

Luis Adrian Fernandez Tenelanda: Conceptualization, Methodology, Software, Investigation, Data Curation, Validation, Visualization, Writing – Original Draft, and Project Administration. Danna Yolanda Solis Espinoza: Investigation, Resources, Formal Analysis, Validation, and Writing – Review & Editing. This declaration must be ratified by all three authors upon manuscript submission. Funding .No specific external funding was identified in the reviewed corpus; implementation utilized institutional resources and infrastructure. This statement must be ratified by the authors.

Conflicts of Interest

No conflicts of interest were identified in the reviewed corpus; authors must confirm this statement in the editorial submission form.

Ethics and Privacy

Analysis must exclusively utilize necessary operational metadata, adhering to data minimization, pseudonymization, and institutional approval where applicable. Names, sensitive path directories, object identifiers, and Tenant secrets must not be published.

Use of AI Tools

This version received support from a generative AI tool for structuring and editorial refinement. The authors retain full responsibility for the accuracy, originality, references, code, data, and conclusions, and must adapt this declaration to match the specific policy of the target journal.

References

1. L. M. C. Benavides, J. A. Tamayo Arias, M. D. Arango Serna, J. W. Branch Bedoya, and D. Burgos, "Digital transformation in higher education institutions: A systematic literature review," *Sensors*, vol. 20, no. 11, p. 3291, 2020. [Online]. Available: <https://doi.org/10.3390/s20113291>
2. A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004. [Online]. Available: <https://doi.org/10.2307/25148625>
3. M. K. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren, "Action design research," *MIS Quarterly*, vol. 35, no. 1, pp. 37–56, 2011. [Online]. Available: <https://doi.org/10.2307/23043488>
4. G. Vial, "Understanding digital transformation: A review and a research agenda," *The Journal of Strategic Information Systems*, vol. 28, no. 2, pp. 118–144, 2019. [Online]. Available: <https://doi.org/10.1016/j.jsis.2019.01.003>
5. P. C. Verhoef, T. Broekhuizen, Y. Bart, A. Bhattacharya, J. Q. Dong, N. Fabian, and M. Haenlein, "Digital transformation: A multidisciplinary reflection and research agenda," *Journal of Business Research*, vol. 122, pp. 889–901, 2021. [Online]. Available: <https://doi.org/10.1016/j.jbusres.2019.09.022>
6. Information and Documentation—Records Management—Part 1: Concepts and Principles, ISO 15489-1:2016, International Organization for Standardization, 2016.
7. Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements, ISO/IEC 27001:2022, International Organization for Standardization, 2022.
8. Microsoft, "The principle of least privilege with Microsoft Entra ID Governance," Microsoft Learn, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/entra/id-governance/scenarios/least-privilege>
9. Microsoft, "What is Conditional Access?" Microsoft Learn, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview>
10. Microsoft, "Configure identity and access management for Power Platform," Microsoft Learn, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/power-platform/guidance/adoption/conditional-access>
11. Microsoft, "Service dependencies in Microsoft Entra Conditional Access," Microsoft Learn, 2026. [Online]. Available: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/service-dependencies>
12. Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-207>
13. OBS Business School, "Master in Information Systems and Technology Management: Curriculum," 2026. [Online]. Available: <https://www.obsbusiness.school/masters-online/master-en-direccion-de-sistemas-y-tecnologias-de-la-informacion>
14. J. P. Kotter, "Leading change: Why transformation efforts fail," *Harvard Business Review*, vol. 73, no. 2, pp. 59–67, 1995.
15. P. Weill and J. W. Ross, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston, MA, USA: Harvard Business School Press, 2004.
16. SciELO, "Program, publication model, and SciELO Network," n.d. [Online]. Available: <https://www.scielo.org/en/about-scielo/program-publication-model-and-scielo-network/>