ManageEngine

A quick guide to SEPS Resolución 116

Issued by the Superintendencia de Economía Popular y Solidaria (SEPS), Resolution SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116 sets the operational risk requirements for Ecuador's popular and solidarity financial sector. It requires savings and credit cooperatives, mutual associations, central funds, and the National Corporation of Popular and Solidarity Finance (CONAFIPS) to control risk across people, processes, technology, and external events.

Technical controls checklist

Use the checklist below to assess your organization's readiness across SEPS Resolución 116's key requirement areas.

Sl.no	Requirement area	Article	Controls required
1	Operational risk governance and monitoring	5, 7	• Run the six-stage risk cycle • Maintain a central risk-event base • Track key risk indicators • Report residual risk to management
2	Access control and segregation of duties	10, 12	• Enforce role-based access • Separate incompatible duties • Certify access periodically • Restrict data center access
3	Identity life cycle management	13	• Provision access on hire • Adjust access on role change • Revoke access on exit • Report orphaned accounts
4	Change and application control	14(6), 14(9)	• Segregate dev, test, production • Authorize and document changes • Protect version integrity • Promote to production independently
5	Infrastructure and configuration monitoring	14(7)	• Monitor database and network configurations • Maintain technology asset inventory • Set limits and alerts • Audit configuration changes
6	Incident and problem management	16	• Assign an incident handler • Run full incident life cycle • Analyze problem root cause • Sustain 99.99% service availability

Sl.no	Requirement area	Article	Controls required
7	Business continuity and recovery	17	• Set recovery time objective and recovery point objective • Maintain a disaster-recovery plan • Back up critical information • Test continuity plans regularly
8	Third-party and cloud oversight	18	• Assess critical service providers • Require cloud security certifications • Monitor outsourced services • Govern third-party access

SEPS Resolución 116 and ManageEngine

ManageEngine offers solutions that can help your organization govern access, monitor systems, and respond to incidents in line with SEPS Resolución 116. AD360, ManageEngine's IAM solution, and Log360, its SIEM solution, together cover the identity, logging, and monitoring controls the standard calls for. With them in place, you can implement the technical controls required under SEPS Resolución 116.

How can ManageEngine help you implement SEPS Resolución 116?

Role-based access governance

Enforce role-based access and OU-based delegation so no single user holds incompatible entitlements, cutting the chance of fraud or error going unseen.

Helps with Articles 10(3), 12(5).

Access certification

Recertify user entitlements on a schedule so access stays matched to role, and segregation of duties does not drift over time.

Helps with Article 12(5).

Identity life cycle management

Automate provisioning on hire, entitlement changes on role moves, and deprovisioning on exit across the personnel life cycle.

Helps with Article 13(1).

Post-employment access control

Disable accounts and revoke access the moment someone leaves, and report orphaned or inactive accounts before they are misused.

Helps with Article 13(2).

Privileged access monitoring

Track and alert on privileged activity against data center and critical systems, exposing unauthorized access as it happens.

Helps with Article 14(5)(a).

Change control auditing

Record who changed what and when across applications and infrastructure, evidencing that changes were authorized and documented before production.

Helps with Article 14(6)(g), 14(9).

File integrity monitoring

Detect unauthorized modification of files and protect version integrity between development and production libraries.

Helps with Article 14(6)(h), 14(9).

Configuration and infrastructure monitoring

Monitor database, network, and base-software configuration with thresholds and alerts, and inventory the technology assets sending telemetry.

Helps with Article 14(7)(a), 14(7)(f).

Log management and risk-event base

Centralize and retain security events in a searchable, tamper-evident archive that feeds the risk-event base and risk indicators.

Helps with Articles 5(5), 7(4).

Threat detection and anomaly alerting

Detect cyberattacks and external fraud with MITRE ATT&CK®-mapped rules, UEBA anomaly detection, and threat intelligence.

Helps with Article 15.

Incident and problem management

Run the full incident life cycle with an assigned handler, event correlation, SOAR playbooks, and root cause analysis to closure.

Helps with Article 16(1), 16(3), 16(4).

Continuity, recovery, and vendor oversight

Back up and recover identity systems, monitor cloud and outsourced services, and govern third-party access to critical services.

Helps with Articles 17(4)(f), 18(12), 18(14).