ManageEngine

A quick guide to SUSEP Circular 638/2021

Circular SUSEP nº 638/2021, issued by Brazil's Superintendência de Seguros Privados (SUSEP), sets cybersecurity requirements for insurers, open private pension entities (EAPCs), capitalization companies, and local reinsurers. It protects the confidentiality, integrity, and availability of the data and systems these entities depend on.

Technical controls checklist

Use the checklist below to assess your organization's readiness across SUSEP 638's key requirement areas.

Sl.no	Requirement area	Article	Controls required
1	Cyber risk governance	Art. 3	• Treat cyber risk as operational risk • Adopt recognized security good practices • Integrate cyber risk into the EGR • Assess risk posture continuously
2	Cybersecurity policy	Art. 4	• Maintain a documented cybersecurity policy • Record board-level commitment • Classify data by relevance • Classify incidents and services
3	Vulnerability management	Art. 5(I)	• Identify vulnerabilities across systems • Assess attack-surface exposure • Reduce misconfigurations • Monitor file integrity
4	Detection, response and recovery	Art. 5(II), 6	• Detect incidents in real time • Correlate and log events • Apply containment measures • Recover affected systems • Treat exploited vulnerabilities • Preserve incident traceability
5	Access and identity controls	Art. 4, 6	• Enforce multi-factor authentication • Apply role-based access control • Monitor privileged accounts • Restrict access during incidents
6	Business continuity	Art. 7	• Embed incident processes in continuity plan • Plan for relevant scenarios • Preserve investigation evidence • Restore identity and access services
7	Incident reporting and records	Art. 8–9, 15	• Notify SUSEP within five business days • Detail damage and remediation • Produce annual incident report • Retain policy, reports, and contracts
8	Outsourcing and cloud oversight	Art. 10–11	• Monitor outsourced and cloud services • Require provider controls not inferior • Verify data segregation • Notify SUSEP within 30 days

SUSEP 638 and ManageEngine

ManageEngine offers solutions that help insurance-sector organizations govern access, monitor their environment, and respond to incidents in line with Circular SUSEP 638/2021. AD360, ManageEngine's IAM solution, and Log360, its SIEM solution, together provide the identity governance and security monitoring the circular calls for. With these, you can implement the technical controls required under SUSEP 638 and evidence them to the regulator.

How can ManageEngine help you implement SUSEP 638?

Security and risk posture

Scan Active Directory and database configurations for misconfigurations and security gaps, feeding cyber risk into the risk framework and surfacing vulnerabilities to reduce.

Helps with Art. 3, Art. 5(I).

Audit trails and change auditing

Record time-stamped user and system activity and audit changes across Active Directory in real time, providing the accountability and traceability that incident investigations rely on.

Helps with Art. 6, Art. 9.
Helps with Art. 4(III)(a).

Threat detection and correlation

Detect incidents in real time using 2,000+ MITRE-mapped detection rules, event correlation, and behavior analytics across servers, endpoints, and cloud.

Helps with Art. 5(II), Art. 6.

Incident response and recovery

Contain, remediate, and recover from incidents through SOAR playbooks and a central console, with workflows the continuity plan can reference.

Helps with Art. 6(III), Art. 7.

Multi-factor authentication

Enforce risk-based MFA and conditional access on Active Directory, VPN, and applications to control access to relevant systems.

Helps with Art. 4(III)(b), Art. 6(III).

Access governance

Apply role-based access control, access certification, and privileged-account monitoring to limit and periodically review who can reach relevant systems.

Helps with Art. 4(III)(b), Art. 11(III).

File integrity and data protection

Detect unauthorized changes to critical files and flag abnormal data movement across boundaries, supporting vulnerability treatment and data segregation.

Helps with Art. 5(I), Art. 11(IV).

Incident reporting and timelines

Reconstruct incident scope with AI-automated timelines and audit-ready reports to meet the five-business-day SUSEP notification and the annual report.

Helps with Art. 8, Art. 9.

Cloud and log oversight

Monitor outsourced and cloud services and retain time-stamped logs and incident reports for long-term oversight and record-keeping.

Helps with Art. 10, Art. 15.

For more information, contact sales@manageengine.com