INOVE
SOLUTIONS THAT TRANSFORM

E-BOOK · EXECUTIVE GUIDE

Cybersecurity and LGPD

Protecting the operation, not just the perimeter — layers, response time and privacy that works in practice.

Inove Solutions · inovesolutions.com · 2026 edition

CHAPTER 1

The armored door and the service entrance

Almost every company has invested in the digital equivalent of a vault: next-generation firewall, corporate antivirus, VPN. And incidents keep getting in anyway — because they almost never come through the vault. They come through the email someone opened, the reused password, the supplier with far too much access, the test server nobody patched.

Figure 1 — The investment goes into the monumental door; the incident walks in through the side entrance left ajar.

Security in 2026 is not about wall height: it is about **consistently shrinking the attack surface**. Every unnecessary access, every system without an owner and every 'temporary' exception that became permanent is another service entrance left open.

> **The right question** — it is not 'do we have a firewall?', it is 'if someone gets in today, how far can they reach before anyone notices?'. The following pages deal with those two halves: reach and awareness.

CHAPTER 2

Layers: what still works when one of them fails

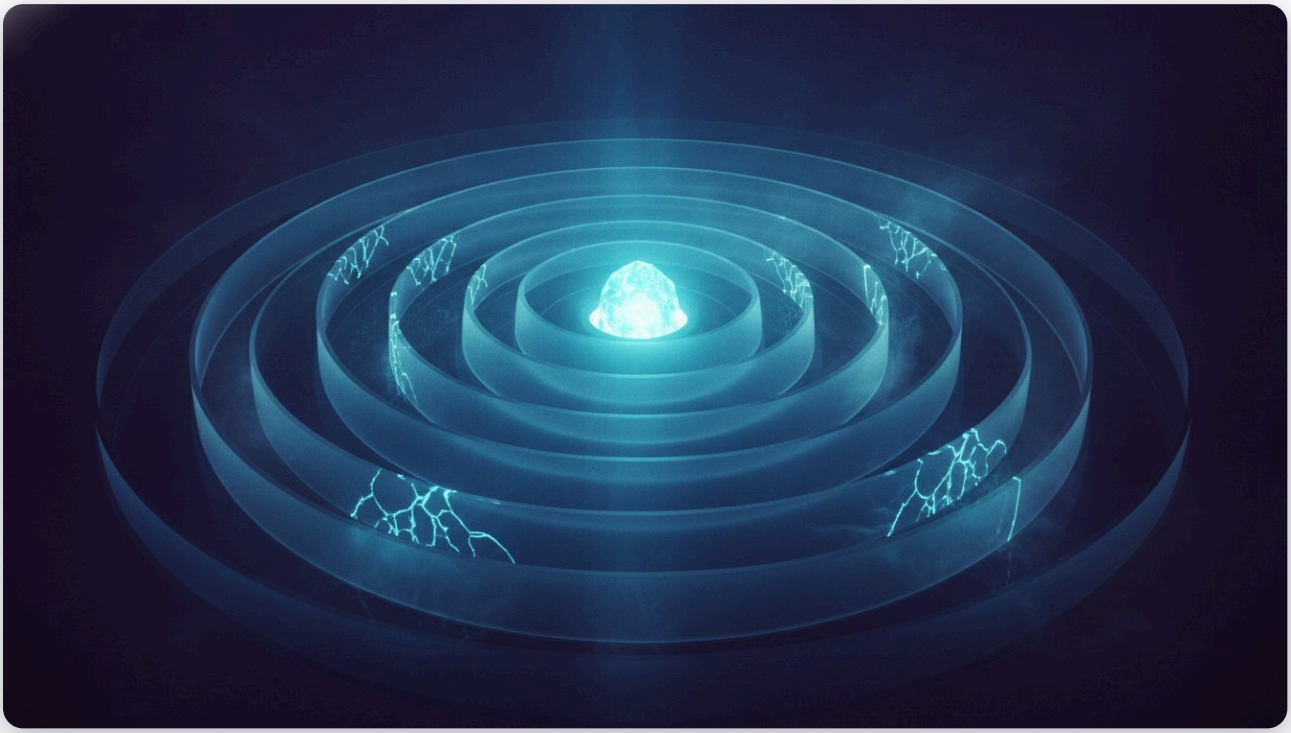

Figure 2 — No layer is perfect; what protects the core is having another one behind it.

Mature defense does not bet on a single infallible control — it assumes every layer can fail and organizes the others to contain the damage:

- **Identity** — MFA on everything exposed, no more shared accounts, least privilege by default. This is the layer with the best return per dollar invested.
- **Device** — managed, patched and monitored endpoints; encrypted disks. An unmanaged workstation is a blind spot.
- **Network** — real segmentation: the guest network, the production network and the critical systems network cannot see each other.
- **Application and data** — role-based access, audit trail and encryption of anything sensitive at rest and in transit.
- **Backup** — isolated, immutable copies, tested with an actual restore. A backup that has never been restored is a hypothesis, not a plan.

> **An honest test** — ask how long it would take to restore your most critical system if it were encrypted today. If the answer is an estimate rather than a number measured in a drill, that layer does not exist yet.

CHAPTER 3

The incident clock

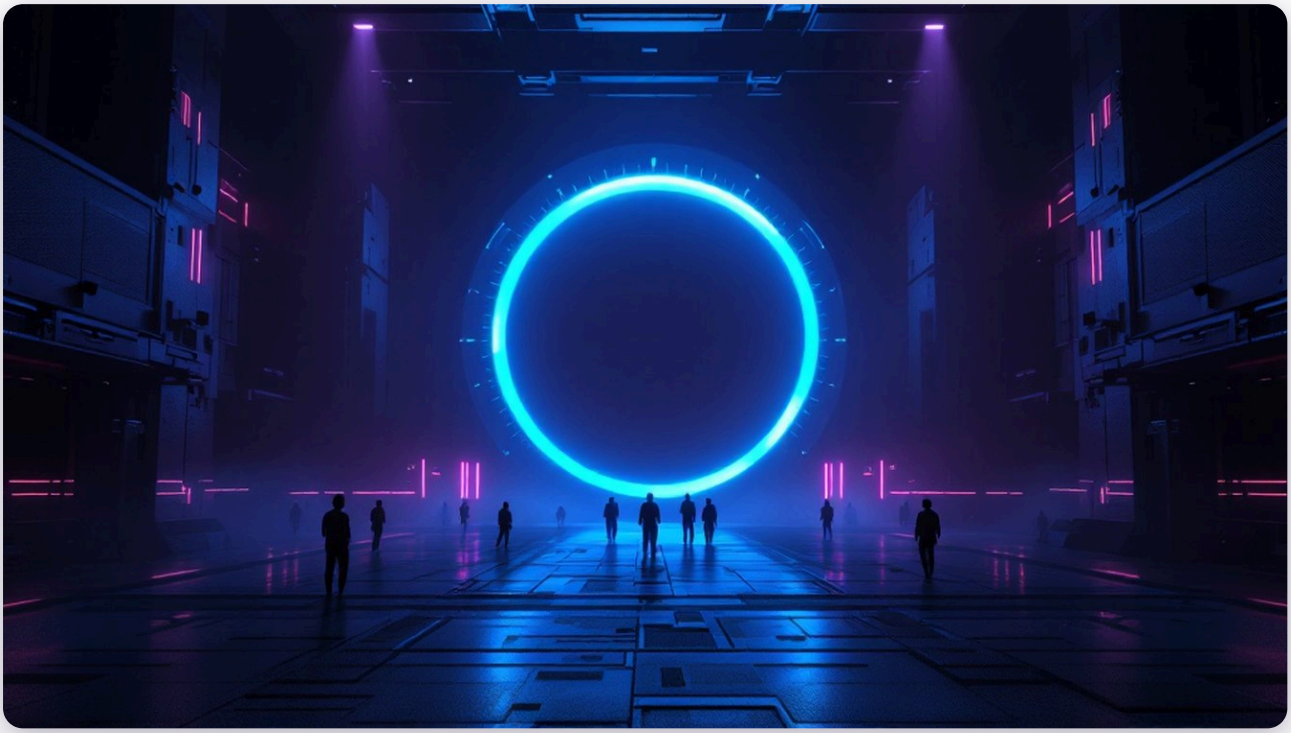

Figure 3 — When the alarm goes off, the difference between a scare and a crisis is the time until someone acts with a method.

Every incident has three clocks that decide the size of the damage — and all three are manageable:

- **Time to detect.** Without monitoring and log correlation, average discovery time is measured in weeks — long enough for the attacker to map the entire network.
- **Time to contain.** This depends on a plan and on authority: who is allowed to shut down what, without waiting for a meeting.
- **Time to restore.** This depends on a tested backup and on a runbook written beforehand, not during.

The plan that fits on one page

A useful response plan answers: who leads, who communicates (internally, to customers, to the ANPD — the Brazilian data-protection authority — where applicable), what gets shut down first, how evidence is preserved and when the incident is declared closed. If it does not fit on one page, nobody will read it at 3 a.m.

> **Rehearsing beats documenting** — one tabletop exercise every six months, with the real team and a plausible scenario (ransomware over a weekend, a customer database leak), exposes more gaps than any paper audit.

CHAPTER 4

LGPD: from compliance to practice

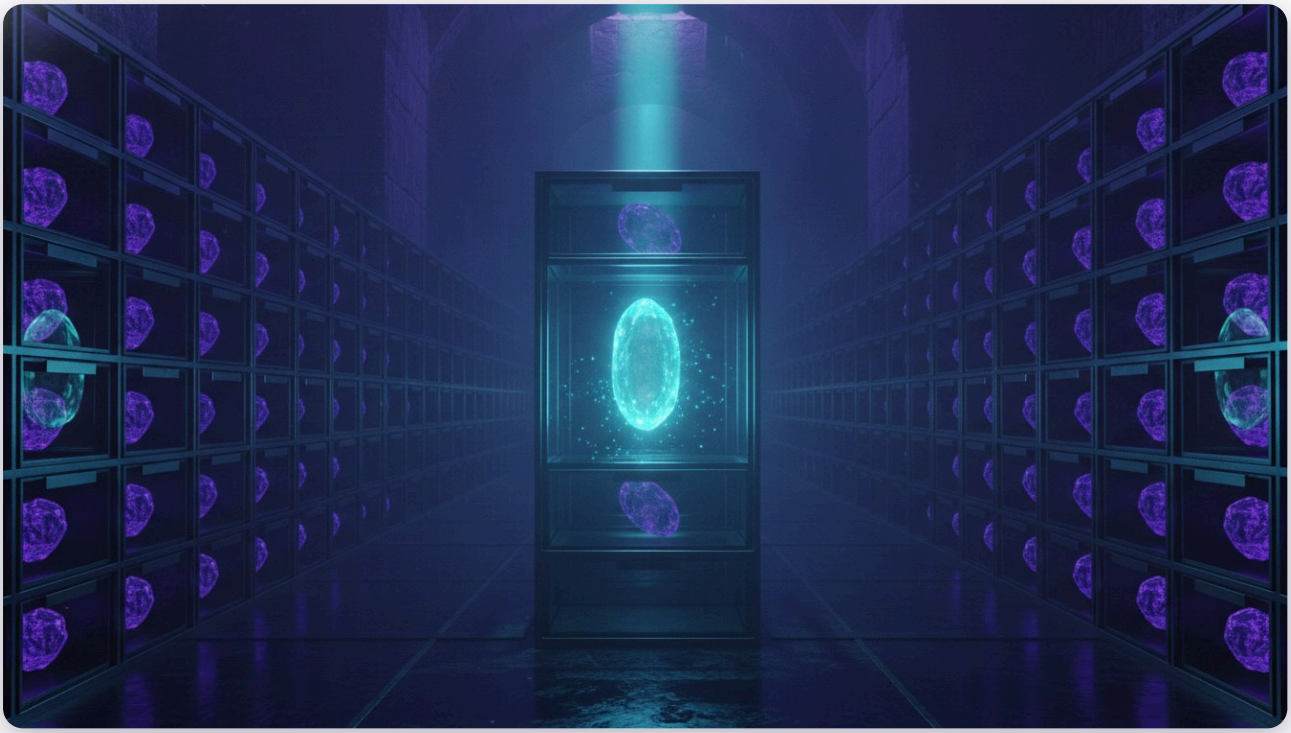

Figure 4 — Personal data has an owner, a deadline and a purpose: each drawer holds a commitment, not just a record.

LGPD, the Brazilian data-protection law, has moved off the page: enforcement and fines are real. But compliance is not achieved with a policy published on the website — it is achieved with four real capabilities:

- **Knowing where the data is.** An inventory of personal data by system, including spreadsheets and test environments — where the production copy usually sleeps unprotected.
- **Knowing why it is there.** Purpose and legal basis declared; anything without a purpose should not exist.
- **Knowing for how long.** Retention defined and expiration executable — the same discipline as archiving, applied to personal data.
- **Knowing how to respond.** Data subject requests, incidents involving personal data and notification deadlines: a defined process, with an owner.

> **Where IT stumbles most** — production copies in non-production environments. It is the most common finding and one of the easiest to fix: masking sensitive data on copy should be the standard, not the exception.

CHAPTER 5

When there is SAP in the environment

The IT environment is bigger than any single system — but the ERP concentrates sensitive data and execution power, and that calls for controls of its own:

Segregation of duties (SoD)

The classic: whoever creates a vendor should not approve payments. SoD is not an audit topic once a year — it is role design, verified at every change.

Privileged access

Users with broad power (administration, firefighter, integration) need an owner, an expiry date and a trail. A generic account shared by several analysts is the antithesis of auditability.

Non-production environments

Copies of production in quality and development carry real data — including personal data. Masking and access control in those environments matter as much as in production.

Patches and security notes

The vendor security note cycle needs a maintenance window and a responsible owner. A critical system with no patching routine is debt that comes due as an incident.

> **Worth noting** — in managed cloud models such as RISE with SAP, part of security belongs to the provider and part remains yours: identity, access, custom code and integrations stay with the client. Reading the responsibility matrix avoids the worst possible surprise.

CHAPTER 6

Where to start — and a checklist

A security program does not start with a tool; it starts by shrinking the attack surface and gaining visibility:

1. **Inventory.** What exists, who owns it, what is exposed to the internet. You cannot protect what you do not know about.
2. **Identity.** MFA on everything exposed, review of privileged accounts and deactivation of whatever is left over from people who have gone.
3. **Tested backup.** An isolated, immutable copy and one real, timed restore.
4. **Visibility.** Centralized logs and alerts that reach someone on call — not an inbox without an owner.
5. **Response plan.** One page, rehearsed twice a year.

Executive checklist

- ✓ Do we know what part of our operation is exposed to the internet today?
- ✓ Is MFA active on email, VPN, cloud and administrative access?
- ✓ When was the last backup restore that was genuinely tested?
- ✓ Is there someone on call for alerts outside business hours?
- ✓ Do our test environments hold real personal data without masking?
- ✓ If we run SAP: are SoD and privileged access reviewed on a regular cycle?
- ✓ Has our response plan been rehearsed — or does it only exist as a PDF?

ABOUT INOVE

Security that keeps the operation running

Security that gets in the way of the operation is abandoned at the first emergency. That is why Inove Solutions treats protection and continuity as the same subject, across the entire IT environment:

- **Cybersecurity** — prevention, monitoring, incident response and compliance with LGPD, the Brazilian data-protection law.
- **Identity and access** — MFA, least privilege, account governance and SoD wherever there is an ERP.
- **Infrastructure and cloud** — segmentation, hardening and tested immutable backup.
- **SAP practices** — roles, privileged access, non-production environments and security notes.
- **Application management** — our 'life insurance' model: the environment cared for end to end, with people who answer when the alarm goes off.

We serve companies such as **Petrobras, Nespresso and Qualicorp** — and we treat security as a measured routine, not an annual campaign.

> **Our vision** — we want our clients to have no IT headaches and to be happy. Including on the day the alarm goes off.

If someone got in today, how far would they get?

Ask for a security and privacy assessment — exposed surface, identity, backup and response, with your environment on the table.

To go deeper, at the Inove Academy: e-book **SAP Archiving** (data retention and expiration) · quick guide **AMS: what to demand in an SLA** · infographics on SAP practices — inovesolutions.com/en/inove-academy-en

inovesolutions.com/en/contact · +55 11 3554-9450