INOVE
SOLUTIONS THAT TRANSFORM

E-BOOK · GUÍA EJECUTIVA

Ciberseguridad y LGPD

Proteger la operación, no solo el perímetro — capas, tiempo de respuesta y privacidad que funciona en la práctica.

Inove Solutions · inovesolutions.com · Edición 2026

CAPÍTULO 1

La puerta blindada y la puerta de servicio

Casi toda empresa invirtió en el equivalente digital de una caja fuerte: firewall de última generación, antivirus corporativo, VPN. Y, aun así, los incidentes siguen entrando — porque casi nunca entran por la caja fuerte. Entran por el correo que alguien abrió, por la contraseña reutilizada, por el proveedor con acceso demasiado amplio, por el servidor de pruebas que nadie actualizó.

Figura 1 — La inversión va a la puerta monumental; el incidente entra por la puerta lateral entreabierta.

La seguridad, en 2026, no es altura de muro: es **reducción consistente de superficie**. Cada acceso innecesario, cada sistema sin dueño y cada excepción 'temporal' que se volvió permanente es una puerta de servicio abierta.

> **La pregunta correcta** — no es '¿tenemos firewall?', sino 'si alguien entra hoy, ¿hasta dónde llega antes de que alguien lo note?'. Las páginas siguientes tratan esas dos mitades: alcance y percepción.

CAPÍTULO 2

Capas: lo que funciona cuando una falla

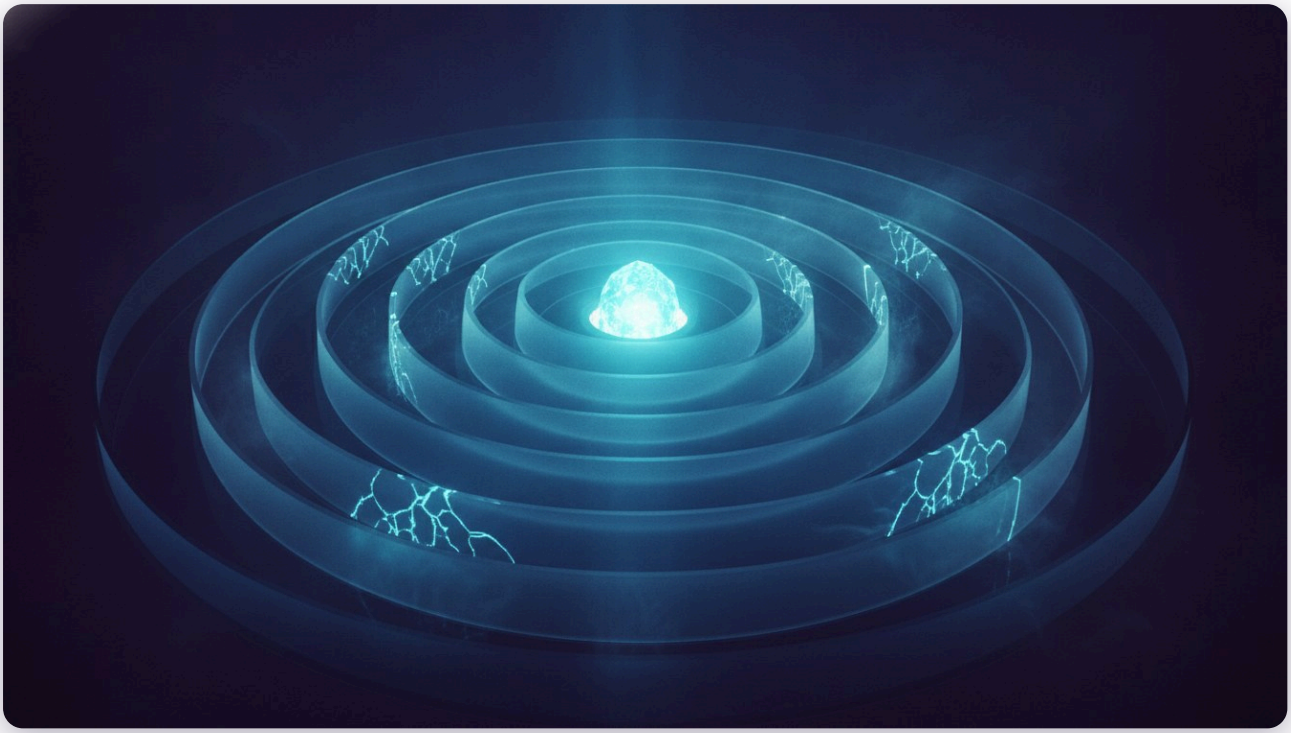

Figura 2 — Ninguna capa es perfecta; lo que protege el núcleo es que haya otra detrás.

Una defensa madura no apuesta a un control infalible — asume que cada capa puede fallar y organiza las demás para contener el daño:

- **Identidad** — MFA en todo lo que está expuesto, fin de las cuentas compartidas, privilegio mínimo por defecto. Es la capa con mejor retorno sobre lo invertido.
- **Dispositivo** — endpoint gestionado, actualizado y monitoreado; disco cifrado. Una estación sin gestión es un punto ciego.
- **Red** — segmentación de verdad: la red de visitantes, la de producción y la de los sistemas críticos no se ven entre sí.
- **Aplicación y datos** — acceso por rol, pista de auditoría y cifrado de lo sensible en reposo y en tránsito.
- **Backup** — copias aisladas e inmutables, probadas con una restauración real. Un backup que nunca se restauró es una hipótesis, no un plan.

> **Prueba honesta** — pregunte cuánto tiempo tomaría restaurar el sistema más crítico si hoy quedara cifrado. Si la respuesta es una estimación, y no un número medido en un ejercicio, esa capa todavía no existe.

CAPÍTULO 3

El reloj del incidente

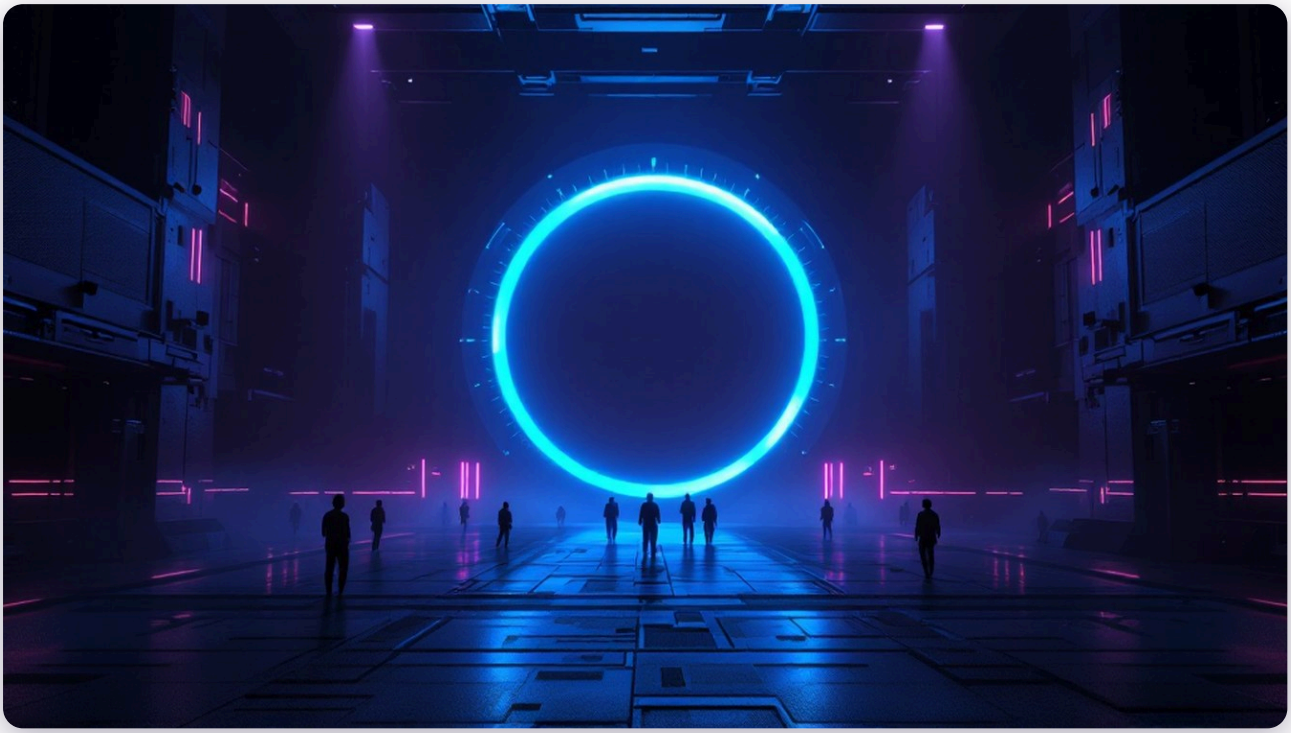

Figura 3 — Cuando suena la alarma, la diferencia entre susto y crisis es el tiempo hasta que alguien actúa con método.

Todo incidente tiene tres tiempos que deciden el tamaño del daño — y los tres son gestionables:

- **Tiempo hasta detectar.** Sin monitoreo y correlación de logs, el promedio de descubrimiento se mide en semanas — tiempo suficiente para que el atacante mapee toda la red.
- **Tiempo hasta contener.** Depende del plan y de la autoridad: quién puede apagar qué, sin esperar una reunión.
- **Tiempo hasta restaurar.** Depende del backup probado y del runbook escrito antes, no durante.

El plan que cabe en una página

Un plan de respuesta útil responde: quién lidera, quién comunica (interno, clientes y la ANPD — la autoridad brasileña de protección de datos — cuando corresponde), qué se apaga primero, cómo se preserva la evidencia y cuándo se declara cerrado. Si no cabe en una página, nadie va a leerlo a las 3 de la mañana.

> **Ensayar vale más que documentar** — un ejercicio de mesa por semestre, con el equipo real y un escenario plausible (ransomware el fin de semana, filtración de la base de clientes), revela más brechas que cualquier auditoría de papel.

CAPÍTULO 4

LGPD: del cumplimiento a la práctica

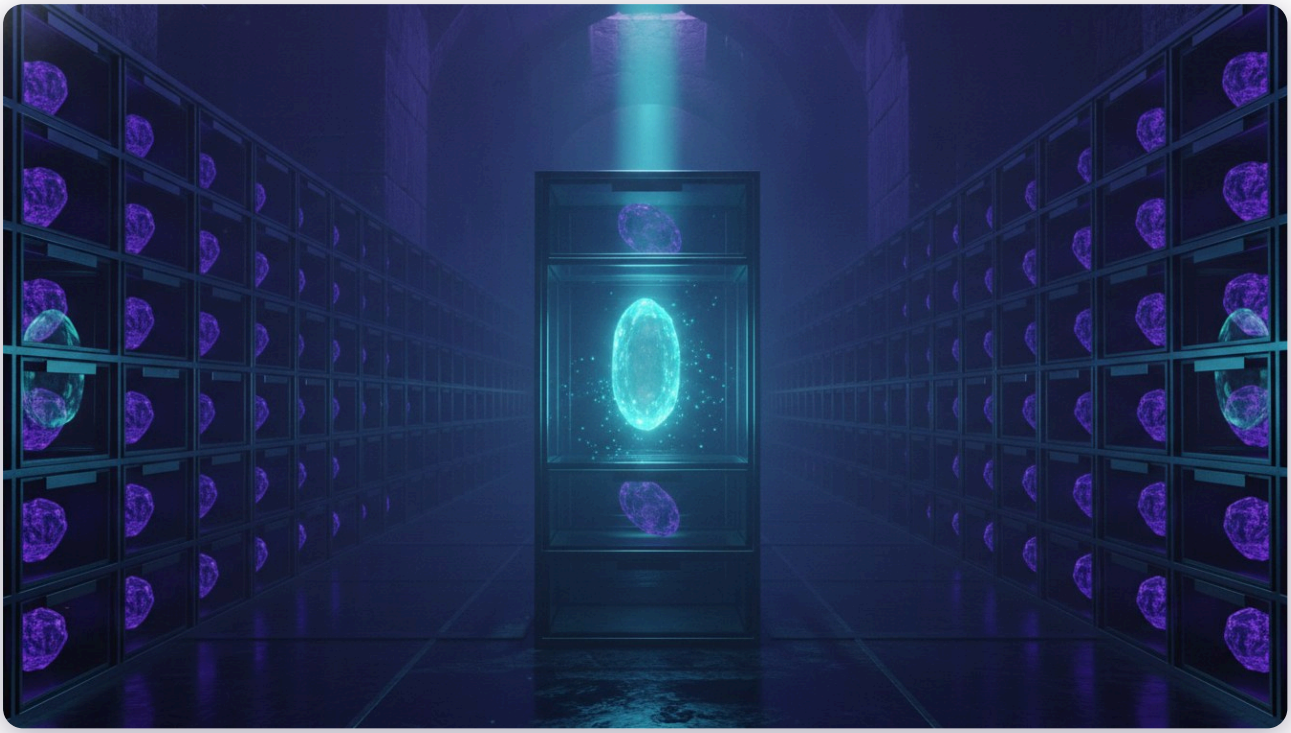

Figura 4 — El dato personal tiene dueño, plazo y finalidad: cada cajón guarda un compromiso, no solo un registro.

La LGPD — la ley brasileña de protección de datos — salió del papel: la fiscalización y las sanciones son realidad. Pero el cumplimiento no se resuelve con una política publicada en el sitio: se resuelve con cuatro capacidades reales:

- **Saber dónde está el dato.** Inventario de datos personales por sistema, incluidas las planillas y los entornos de prueba — donde la copia de producción suele dormir sin protección.
- **Saber por qué está ahí.** Finalidad y base legal declaradas; lo que no tiene finalidad no debería existir.
- **Saber por cuánto tiempo.** Retención definida y expiración ejecutable — la misma disciplina del archiving, aplicada al dato personal.
- **Saber responder.** Solicitud del titular, incidente con dato personal y plazo de notificación: proceso definido, con dueño.

> **Dónde más tropieza TI** — copias de producción en entornos no productivos. Es el hallazgo más común y uno de los más fáciles de corregir: enmascarar el dato sensible al copiar debería ser el estándar, no la excepción.

CAPÍTULO 5

Cuando hay SAP en el entorno

El entorno de TI es más grande que cualquier sistema — pero el ERP concentra dato sensible y poder de ejecución, y por eso pide controles propios:

Segregación de funciones (SoD)

El clásico: quien registra al proveedor no debería aprobar el pago. La SoD no es un tema de auditoría una vez al año — es diseño de perfil, verificado en cada cambio.

Accesos privilegiados

Los usuarios con poder amplio (administración, emergencia, integración) necesitan dueño, plazo y pista de auditoría. Una cuenta genérica compartida por varios analistas es la antítesis de la auditoría.

Entornos no productivos

Las copias del productivo en calidad y desarrollo llevan dato real — incluido el personal. El enmascaramiento y el control de acceso en esos entornos valen tanto como en producción.

Correcciones y notas de seguridad

El ciclo de notas de seguridad del proveedor necesita ventana y responsable. Un sistema crítico sin rutina de patch es una deuda que vence en forma de incidente.

> **Punto de atención** — en modelos de nube gestionada como RISE with SAP, parte de la seguridad es del proveedor y parte sigue siendo suya: identidad, accesos, personalizaciones e integraciones permanecen del lado del cliente. Leer la matriz de responsabilidad evita la peor sorpresa posible.

CAPÍTULO 6

Por dónde empezar — y checklist

Un programa de seguridad no empieza por la herramienta; empieza por reducir superficie y ganar visibilidad:

1. **Inventario.** Qué existe, quién es el dueño, qué está expuesto a internet. No se protege lo que no se conoce.
2. **Identidad.** MFA en todo lo expuesto, revisión de cuentas privilegiadas y desactivación de lo que quedó de quienes ya salieron.
3. **Backup probado.** Copia aislada, inmutable y una restauración real cronometrada.
4. **Visibilidad.** Logs centralizados y alertas que llegan a alguien de guardia — no a un buzón de correo sin dueño.
5. **Plan de respuesta.** Una página, ensayada una vez por semestre.

Checklist ejecutivo

- ✓ ¿Sabemos qué parte de nuestra operación está expuesta a internet hoy?
- ✓ ¿El MFA está activo en correo, VPN, nube y accesos administrativos?
- ✓ ¿Cuándo fue la última restauración de backup probada de verdad?
- ✓ ¿Hay alguien de guardia para las alertas fuera del horario comercial?
- ✓ ¿Nuestros entornos de prueba tienen dato personal real sin enmascarar?
- ✓ Si usamos SAP: ¿la SoD y los accesos privilegiados se revisan periódicamente?
- ✓ ¿Nuestro plan de respuesta ya fue ensayado — o solo existe en PDF?

SOBRE INOVE

Seguridad que sostiene la operación

La seguridad que estorba a la operación se abandona en la primera urgencia. Por eso Inove Solutions trata la protección y la continuidad como un mismo asunto, dentro del entorno de TI completo:

- **Ciberseguridad** — prevención, monitoreo, respuesta a incidentes y cumplimiento de la LGPD.
- **Identidad y accesos** — MFA, privilegio mínimo, gobernanza de cuentas y SoD cuando hay ERP.
- **Infraestructura y nube** — segmentación, hardening y backup inmutable probado.
- **Prácticas SAP** — perfiles, accesos privilegiados, entornos no productivos y notas de seguridad.
- **Soporte continuo** — nuestro modelo 'seguro de vida': el entorno cuidado de punta a punta, con quien atiende cuando suena la alarma.

Atendemos a empresas como **Petrobras, Nespresso y Qualicorp** — y tratamos la seguridad como rutina medida, no como campaña anual.

> **Nuestra visión** — queremos que el cliente no tenga dolores de cabeza con TI y sea feliz. También el día en que suene la alarma.

Si alguien entrara hoy, ¿hasta dónde llegaría?

Pida un diagnóstico de seguridad y privacidad — superficie expuesta, identidad, backup y respuesta, con su entorno sobre la mesa.

Para profundizar, en la Inove Academy: e-book **Archiving SAP** (retención y expiración de datos) · guía rápida **AMS: qué exigir en un SLA** · infografías de prácticas SAP — inovesolutions.com/es/inove-academy-es

inovesolutions.com/es/contacto · +55 11 3554-9450