Infraestrutura auditável

ISO 27001 na prática para redes, cloud e operações de TI

Leandro Silva

CISO · Autor de “Construindo Sistemas Seguros e Escaláveis” (Novatec)

Semana de Capacitação 13 · NIC.br
15 de setembro de 2026

AGENDA

O caminho do tutorial

01

O problema

Por que passar na auditoria e estar seguro viraram coisas diferentes.

02

SGSI sem burocracia

O mínimo de norma que você precisa saber.

03

Do controle à configuração

Tradução de cada controle em artefato técnico e evidência.

04

Laboratório

Wazuh: baseline, integridade, detecção e mapeamento ISO próprio.

05

Operação contínua

Cadência, donos, nuvem, incidentes e o erro que anula tudo.

06

Checklist de partida

Os dez primeiros passos para quem está no zero.

Q&A ao vivo ao final — traga o caso específico da sua rede.

CAPÍTULO 1

O ciclo da véspera

T-21 — **Chega o e-mail**

“A auditoria é daqui a três semanas.”

T-14 — **Começa a corrida**

Exportar config, tirar print, procurar planilha.

T-7 — **A descoberta**

A última revisão de acessos foi há 14 meses.

T-2 — **A fabricação**

Escreve-se a política que descreve o que deveria acontecer.

T+0 — **Aprovado**

Selo no site. E tudo volta ao normal por mais onze meses.

O mais irônico: normalmente a empresa passa.

Passar na auditoria e estar seguro viraram duas coisas diferentes.

Isso não é culpa da norma. É consequência de tratar conformidade como um projeto com data, em vez de uma propriedade do sistema.

CAPÍTULO 1

Por que isso dói mais em provedor

01

Você já é obrigado a guardar evidência

Marco Civil (Lei 12.965/2014): registro de conexão por 1 ano; aplicação por 6 meses.

Isso é logging obrigatório por lei — e conversa direto com o controle A.8.15.

02

Você já tem obrigação regulatória de segurança

Resolução Anatel nº 740/2020: gestão de risco, notificação de incidente, boas práticas em equipamento.

Muito disso é Anexo A com outro nome.

03

Você opera a infraestrutura de terceiros

Cliente em processo de certificação precisa avaliar você como fornecedor (A.5.19).

O questionário que chega no comercial é extrato de norma. Responder bem é receita.

O que falta não é controle.
É rastro.

A distância entre a operação de um provedor bem administrado e um SGSI certificável é muito menor do que parece. Falta conseguir provar, com registro, que o controle existia ontem, anteontem e no mês passado.

A TESE DESTE TUTORIAL

Duas formas de estar em conformidade

MODELO 1

Auditável por esforço

- A evidência é produzida por pessoas
- Existe porque alguém lembrou
- Reflete um estado de três semanas
- Custa duas semanas de trabalho por ciclo
- Falha na primeira vez que a operação apertar

MODELO 2

Auditável por design

- O controle e a evidência são a mesma coisa
- O log não prova o monitoramento — ele é o monitoramento
- O estado é sempre o atual, não uma foto
- Custa uma implementação e roda sozinho
- Sobrevive à rotina

Se a evidência de um controle precisa de trabalho humano para ser produzida, esse controle tem muita chance de falha

MÉTODO

O mapa mental do resto do tutorial

PERGUNTA 1

Controle

O que a norma quer, em uma frase, sem jargão.

PERGUNTA 2

Artefato técnico

Qual configuração, ferramenta ou automação entrega isso.

PERGUNTA 3

Evidência automática

O que isso produz sozinho, sem ninguém pedir.

Todo controle relevante vai passar por essas três perguntas. Guarde esta imagem.

CAPÍTULO 2

Anatomia da ISO/IEC 27001:2022

PARTE 1 — OBRIGATÓRIA

Cláusulas 4 a 10

4 · Contexto da organização
5 · Liderança
6 · Planejamento
7 · Apoio
8 · Operação
9 · Avaliação de desempenho
10 · Melhoria

É o esqueleto de gestão. Não tem negociação nem exclusão possível.

PARTE 2 — CATÁLOGO

Anexo A · 93 controles

Não são todos obrigatórios.

É um catálogo de referência: você escolhe os aplicáveis ao seu contexto e justifica as exclusões.

Esse documento de escolha e justificativa é a Declaração de Aplicabilidade (SoA).

Emenda 1 (2024): incluiu consideração de mudanças climáticas nas cláusulas 4.1 e 4.2.

CAPÍTULO 2

Os quatro temas do Anexo A

37	8	14	34
Organizacionais	Pessoas	Físicos	Tecnológicos

Só um terço dos controles é tecnológico. Isso costuma frustrar o pessoal técnico — e é também a razão pela qual segurança não se resolve comprando appliance.

CAPÍTULO 2

Escopo: a decisão mais importante

ERRO A

Escopo grande demais

Certificar a empresa inteira no primeiro projeto. Descobre-se que é preciso política de mesa limpa em três filiais — e o projeto morre no meio.

ERRO B

Escopo pequeno demais

Certificar uma ilha que depende de serviços não certificados. O auditor vai perguntar como você garante a fronteira — e você não tem resposta.

REGRA PRÁTICA

Um parágrafo

Se você não consegue descrever o escopo em um parágrafo — qual parte da organização, quais serviços, quais localidades — ele está grande demais.

Escopo mal definido é onde a evidência automática mais ajuda: “esse ativo está dentro ou fora?” para de ser opinião e vira consulta.

EXEMPLO COMENTADO

Um escopo inicial razoável para provedor

“Operação de rede, data center e serviços gerenciados de conectividade, incluindo NOC, sistemas de provisionamento e infraestrutura de borda.”

DENTRO

O que isso já cobre

Equipamentos de borda e core · NOC e acesso administrativo · Sistemas de provisionamento e OSS · Data center e ambiente de virtualização · Logs e monitoramento

FORA — POR ORA

O que fica de fora

Processos de RH · Filiais comerciais · Atendimento de varejo · Áreas administrativas sem acesso ao ambiente técnico

CAPÍTULO 2

A.5.9 — Inventário de ativos

O QUE A NORMA QUER

Saber o que existe

Quais equipamentos, sistemas, bases e enlaces existem.

Quem é o dono de cada um.

Qual a criticidade de cada um.

COMO NÃO FAZER

Planilha

Planilha desatualiza em três semanas e vira ficção.

Se você já tem ferramenta de gerenciamento, sistema de monitoramento ou agente instalado nos hosts, o inventário deve sair de lá.

Vamos ver isso funcionando no laboratório.

CAPÍTULO 2

Análise de risco: o ciclo mínimo

1

Identificar o risco

O que pode dar errado, descrito de forma específica o suficiente para ser tratável.

2

Identificar o dono

Uma pessoa com autoridade para decidir sobre esse risco — não um departamento.

3

Analisar probabilidade e impacto

Escala simples resolve. Precisão falsa não ajuda ninguém.

4

Avaliar contra o critério de aceitação

Você precisa ter definido antes o que é risco aceitável. Sem isso, tudo parece urgente.

5

Tratar

Mitigar, transferir, evitar ou aceitar. Aceitar é decisão legítima — desde que registrada e assinada por quem pode.

A ISO/IEC 27005 dá orientação de metodologia, mas a 27001 não obriga nenhuma em particular.

EXEMPLO

Um risco do seu universo, preenchido

Campo	Conteúdo
Risco	Sequestro de rota por anúncio BGP indevido, próprio ou de cliente
Dono	Coordenação de engenharia de rede
Impacto	Alto — indisponibilidade e possível interceptação de tráfego
Tratamento	Mitigar: RPKI com validação de origem, filtros de prefixo por cliente, monitoramento de anúncios
Controles	A.8.20 segurança de redes · A.8.21 segurança de serviços de rede · A.8.16 monitoramento

Vocês já fazem RPKI. A diferença entre “fazer RPKI” e “ter um controle de segurança da informação” é que, no segundo caso, existe um documento ligando aquela configuração a um risco identificado, com dono — e um registro periódico de que aquilo continua funcionando.

CAPÍTULO 2

Declaração de Aplicabilidade: a tabela mestra

Controle	Aplicável?	Justificativa	Implementado?	Referência da evidência
A.8.9	Sim	Configuração de rede e servidores	Sim	Dashboard de baseline — SCA
A.8.15	Sim	Obrigação legal e operacional	Sim	Coletor central de logs
A.8.16	Sim	Detecção de incidentes	Parcial	Regras de correlação + fila
A.7.4	Não	Sem data center próprio	—	Contrato com o provedor

A última coluna é onde este tutorial mora.

Se ela apontar para “planilha na pasta do Fulano”, você tem um SGSI de papel. Se apontar para um dashboard vivo, uma consulta ou um relatório gerado automaticamente, você tem um SGSI que sobrevive à rotina.

RECORTE PRÁTICO

Os controles que realmente tocam a operação

ORGANIZACIONAIS E DE ACESSO

A.5.9 · Inventário de ativos
A.5.15 · Controle de acesso
A.5.16 · Gestão de identidade
A.5.17 · Informação de autenticação
A.5.18 · Direitos de acesso
A.5.23 · Uso de serviços em nuvem
A.5.24–5.28 · Gestão de incidentes
A.5.37 · Procedimentos operacionais

TECNOLÓGICOS

A.8.2 · Acesso privilegiado
A.8.5 · Autenticação segura
A.8.8 · Gestão de vulnerabilidades
A.8.9 · Gestão de configuração
A.8.13 · Backup
A.8.15 · Logging
A.8.16 · Monitoramento
A.8.17 · Sincronização de relógios
A.8.20–8.22 · Redes e segregação
A.8.32 · Gestão de mudanças

Dos 93 controles do Anexo A, este núcleo concentra o trabalho técnico de quem opera infraestrutura.

E NÃO É COINCIDÊNCIA

Três controles que não existiam antes de 2022

A.8.9

Gestão de configuração

Estado correto definido, desvio detectado.

É o coração do laboratório.

A.8.16

Atividades de monitoramento

Não basta guardar log. Alguém precisa olhar — com regra, alerta e tratativa.

A.5.23

Uso de serviços em nuvem

Fronteira de responsabilidade, logs do provedor, identidade da nuvem.

A revisão de 2022 reconheceu que segurança moderna é uma propriedade contínua da infraestrutura, não um conjunto de documentos. A norma andou na direção que estamos discutindo aqui.

RESUMO

O que ficou do capítulo 2

→ **Cláusulas 4 a 10 são obrigatórias**

Formam o sistema de gestão. Não têm exclusão possível.

→ **O Anexo A é catálogo, não checklist**

Você escolhe o aplicável e justifica na Declaração de Aplicabilidade.

→ **Escopo determina se o projeto termina**

Um parágrafo. Se não couber, está grande demais.

→ **Existe um núcleo de ~15 controles**

É onde mora o trabalho técnico de quem opera infraestrutura.

Agora vamos pegar esses controles e transformar em configuração.

CAPÍTULO 3

A estrutura de todo bloco a seguir

1

O que a norma quer

Em uma frase, sem jargão.

2

Qual artefato entrega

Configuração, ferramenta, automação.

3

Que evidência produz

Sozinha, sem ninguém pedir.

A terceira coluna é a que separa o joio do trigo.

O teste da véspera

Para cada controle da sua Declaração de Aplicabilidade, pergunte: se a auditoria fosse amanhã de manhã, quanto trabalho eu teria?

Se a resposta for mais que “abrir um painel e exportar”, esse controle está em dívida técnica.

A.5.15 · A.5.16 · A.5.17 · A.5.18 · A.8.2 · A.8.5

Acesso e identidade

O que a norma quer: que só quem precisa tenha acesso, que cada acesso seja de uma pessoa identificável, que a autenticação seja forte, e que isso seja revisado.

ARTEFATO

Autenticação centralizada

TACACS+ ou RADIUS nos equipamentos, apontando para diretório único. Resolve identidade individual, níveis de privilégio e — o que importa aqui — log de comando por usuário.

ARTEFATO

MFA sem exceção

Em 2026, senha sozinha não passa em A.8.5. Conta privilegiada sem segundo fator é achado direto, e dos fáceis de encontrar.

ARTEFATO

Privilégio separado

A.8.2 pede privilégio por necessidade e por tempo. Sem ferramenta de PAM, a versão pobre e honesta é conta administrativa separada da conta de uso diário, com log de elevação.

Enquanto existir credencial compartilhada, **você não tem A.5.16, não tem A.8.2 e não tem rastreabilidade de incidente.**

REVISÃO DE DIREITOS DE ACESSO

A.5.18 — O controle que mais reprova gente boa

VERSÃO MANUAL

Por que ninguém faz

Alguém exporta a lista de usuários.

Manda planilha para cada gestor.

Cobra resposta por e-mail.

Consolida tudo à mão.

Leva semanas — e ninguém quer o segundo ciclo.

AUDITÁVEL POR DESIGN

Fila de exceções

Relatório automático cruza contas ativas com a base de pessoal e dispara só a exceção:

- Conta ativa sem vínculo
- Sem login há 90 dias
- Privilégio concedido e nunca usado

A revisão deixa de ser projeto trimestral e vira fila que chega sozinha.

Evidência produzida: log de autenticação por indivíduo · relatório de contas com anomalia · histórico de concessão e revogação · decisão registrada.

A.8.9 · A.8.32 · A.5.37

Configuração e mudança

O que a norma quer: que exista um estado correto definido para cada sistema, que desvios sejam detectados, e que mudanças sejam controladas.

CAMADA 1

Baseline definido

Um arquivo versionado dizendo como um roteador de borda, um servidor Linux ou um host de virtualização devem estar configurados.

Benchmarks CIS são ponto de partida excelente e gratuito.

CAMADA 2

Configuração versionada

Config de equipamento em Git, com coleta automática.

Resolve A.8.9 e A.8.32 de uma vez: o histórico de commits é o histórico de mudanças, com autor e data.

Oxidized, RANCID — muita gente já usa sem saber que gera evidência.

CAMADA 3

Detecção de desvio

Alguém alterou o sshd_config fora do processo? Abriu uma ACL na madrugada e esqueceu de fechar?

Monitoramento de integridade e verificação periódica de baseline resolvem — e é o que faremos no lab.

A.8.32 NA PRÁTICA DE PROVEDOR

Gestão de mudanças que sobrevive à madrugada

A tentação é criar um comitê e um formulário. Em provedor, isso quebra na primeira madrugada — porque a rede não espera reunião.

NÍVEL 1

Rotina

Segue procedimento pré-aprovado.

Só registrada, sem aprovação prévia.

NÍVEL 2

Relevante

Passa por aprovação antes de executar.

Janela e plano de reversão definidos.

NÍVEL 3

Emergencial

Pode ser feita na hora.

Mas com registro obrigatório em até 24 horas.

O auditor não quer ver burocracia. Quer ver que toda mudança tem rastro e que emergência é exceção medida, não regra.

A.8.15 · A.8.16 · A.8.17

Logging e monitoramento

O que a norma quer: que eventos relevantes sejam registrados, protegidos contra adulteração, monitorados ativamente — e que os relógios estejam sincronizados.

A.8.17 — O MAIS FÁCIL E O MAIS IGNORADO

Sincronização de relógios

Parece detalhe bobo. Não é.

Se seus equipamentos têm relógios divergentes, sua correlação de incidente é ficção e seu log perde valor probatório. Uma investigação que não consegue ordenar eventos não é investigação.

Configure NTP em tudo, aponte para fonte confiável — o NIC.br opera o ntp.br, referência do horário legal brasileiro. E monitore o drift: NTP configurado e NTP funcionando são coisas diferentes.

TRÊS REQUISITOS

A.8.15 — Quando o log serve como evidência

REQUISITO 1

Centralizado

Log que mora só no equipamento que o gerou some quando o equipamento é comprometido — ou quando alguém dá reload. Precisa sair do host.

REQUISITO 2

Íntegro

Se o administrador pode editar o log, o log não prova nada contra o administrador.

Armazenamento append-only, permissão restrita, verificação de integridade. Não precisa ser blockchain — precisa ser explicável ao auditor.

REQUISITO 3

Retido pelo prazo certo

Vantagem: o Marco Civil já definiu prazos de guarda de registro de conexão.

Armadilha: prazo legal de guarda não é prazo de retenção de log de segurança. São finalidades diferentes.

A LGPD pede que você guarde dado pessoal pelo tempo necessário à finalidade — nem mais, nem menos. Defina prazos por tipo de log e documente a justificativa.

A DISTINÇÃO QUE REPROVA EMPRESAS

A.8.15 é guardar. A.8.16 é olhar.

A.8.15 — LOGGING

Guardar

Eventos registrados, centralizados, íntegros e retidos.

Necessário. Não suficiente.

A.8.16 — MONITORAMENTO

Olhar

Regra de detecção definida, alerta chegando em alguém, resposta registrada.

É isso que fecha o controle.

Muita empresa tem terabyte de log que ninguém lê.

Isso não é monitoramento — é armazenamento caro. Já vi empresa com petabyte de log reprovar em A.8.16, porque guardar não é monitorar.

A.8.20–8.22 · A.8.8 · A.5.23 · A.8.13

Rede, vulnerabilidades, nuvem e backup

A.8.20–8.22

Redes e segregação

Anti-spoofing (BCP 38), RPKI, segregação da rede de gerência, ACL de acesso administrativo.

Vocês são especialistas. Só documentem a intenção de cada um ligada a um risco — e prática operacional vira conformidade.

A.8.8

Vulnerabilidades

Ciclo: identificar, priorizar, corrigir, verificar.

Scanner é a parte fácil. O que reprova é não ter prazo por severidade e não mostrar histórico de correção.

A.5.23

Nuvem

Saber quem é responsável pelo quê — modelo de responsabilidade compartilhada.

Logs do provedor integrados à coleta central, não só no console da nuvem.

A.8.13

Backup

Backup existe em toda empresa. Backup testado existe em poucas.

O auditor vai pedir evidência de restauração, não de execução. Agende teste de restore com registro automático.

CONTROLE → ARTEFATO → EVIDÊNCIA

A tabela de tradução

Controle	Artefato técnico	Evidência automática
A.5.9	Agente / coletor de inventário	Lista de ativos sempre atual
A.5.18	Cruzamento contas × base de pessoal	Fila de exceções + decisão registrada
A.8.2	Conta administrativa separada	Log de elevação de privilégio
A.8.5	MFA + autenticação centralizada	Log de autenticação por indivíduo
A.8.9	Baseline CIS + integridade de arquivo	Relatório de conformidade + alerta de desvio
A.8.13	Teste de restauração agendado	Registro datado da restauração
A.8.15	Coletor central append-only	O próprio acervo, com relógio confiável
A.8.16	Regras de correlação + fila de tratativa	Alerta com responsável e desfecho
A.8.32	Configuração em Git	Histórico de commits com autor e data

Sugestão: use esta tabela como coluna de referência da sua própria Declaração de Aplicabilidade.

CAPÍTULO 4

O que vamos fazer no laboratório

1. **Verificar um host contra baseline CIS**
   E ler o resultado como não conformidade de A.8.9.

2. **Alterar um arquivo crítico**
   E ver o alerta de integridade nascer em segundos.

3. **Simular uma tentativa de acesso indevido**
   E acompanhar a detecção correlacionada de A.8.16.

4. **Criar do zero o mapeamento ISO 27001 que a ferramenta não traz**
   Taggeando regras por controle do Anexo A. Este é o exercício central.

5. **Gerar um relatório**
   E discutir a pergunta que interessa: isso é evidência aceitável para um auditor?

CAPÍTULO 4

A arquitetura do laboratório

VM 1

Servidor Wazuh

Manager + indexador + dashboard
4 vCPU · 8 GB RAM
Dashboard em https://IP

VM 2

Host monitorado

Ubuntu Server limpo
1 vCPU · 2 GB RAM
Agente Wazuh instalado

Nada aqui é exclusivo do Wazuh. Se você usa outro SIEM, ou Zabbix com coletores, ou uma pilha própria de logs — os conceitos se transferem inteiros. Não é aula de produto.

A.8.9 NA VIDA REAL

O cenário: a mudança da madrugada

1

03:00 — Chamado crítico

O plantonista precisa acessar um servidor. O jeito rápido é liberar login de root por SSH.

2

03:20 — Resolvido

Problema contornado. Ele vai dormir.

3

Segunda-feira — Ninguém lembra

A configuração pode ficar aberta por meses.

4

E o pior

Ninguém sabe que ela está aberta, porque não existe rastro.

A.8.9 — GESTÃO DE CONFIGURAÇÃO

Teste da véspera: passou

CONTROLE

A.8.9

Gestão de configuração: estado correto definido, desvio detectado.

ARTEFATO

FIM em tempo real

Monitoramento de integridade sobre os diretórios críticos.

EVIDÊNCIA

Alerta com hash

Arquivo, hash antes e depois, horário e autor — gerado sozinho.

A reversão também gera alerta. O rastro é completo nos dois sentidos — o que responde a uma pergunta clássica de auditoria: “essa correção que vocês dizem ter feito, quando foi feita?”

A.8.15 VS A.8.16

O que você acabou de ver na tela

EVENTOS INDIVIDUAIS

Cada tentativa virou registro

sshd: Attempt to login using a non-existent user

sshd: Attempt to login using a non-existent user

sshd: Attempt to login using a non-existent user

ALERTA CORRELACIONADO

Nasceu da soma dos anteriores

sshd: brute force trying to get access to the system

Severidade maior.
Não corresponde a nenhuma tentativa específica.

Isso é monitoramento.

A.8.15 é guardar. **A.8.16 é olhar.**

O BLOCO CENTRAL DESTE TUTORIAL

O que a ferramenta não faz por você

O QUE VEM PRONTO

Cinco frameworks

PCI DSS
GDPR
HIPAA
NIST 800-53
TSC (SOC 2)

ISO 27001

Não vem.

E isso não é falha da ferramenta — é a realidade de praticamente todo SIEM de mercado.

Então vamos construir. O identificador de conformidade é apenas texto dentro da tag <group> de uma regra — o que significa que eu posso escrever o meu.

Nenhuma ferramenta vai entregar sua conformidade pronta.

O que a ferramenta entrega é a capacidade de coletar, correlacionar e recuperar evidência. A tradução entre o texto da norma e a evidência técnica é trabalho de engenharia — e é seu, porque só você conhece o seu ambiente.

A boa notícia: esse trabalho se faz uma vez. Depois roda sozinho, todo dia, sem você.

TRÊS PERGUNTAS HONESTAS

Olhe seu relatório com olhos de auditor

PERGUNTA 1

Mostra o período coberto?

O auditor precisa saber se sua evidência é contínua ou se é um recorte conveniente.

PERGUNTA 2

Mostra eventos tratados ou só detectados?

Alerta sem tratativa registrada é meio controle. Detectar e não fazer nada é pior que não detectar — agora está documentado que você sabia.

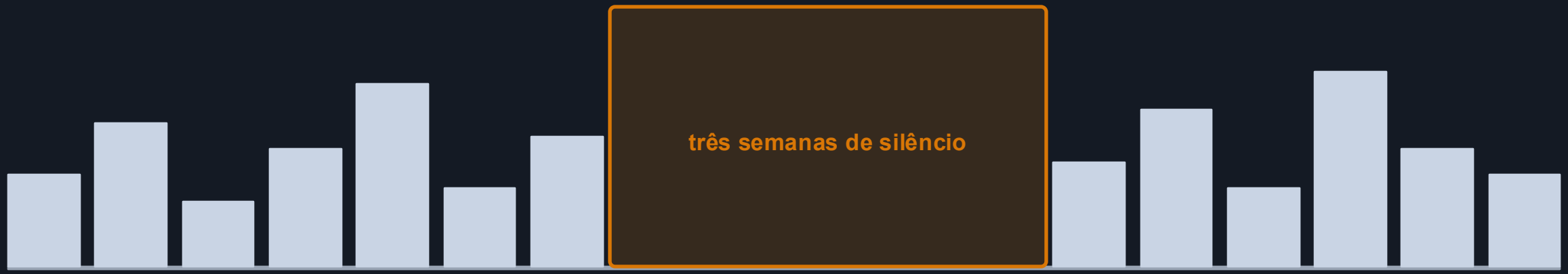
PERGUNTA 3

Prova que a coleta não teve interrupção?

Esta é a armadilha séria. E quase toda implementação que eu vi comete.

A ARMADILHA

O gráfico silencioso



Parece conformidade

Zero alertas. Um período tranquilo. Um gráfico que passa em qualquer auditoria.

A CORREÇÃO

Monitore a saúde da coleta

Agente em disconnected é não conformidade de A.8.16 — com a mesma severidade de um ataque.

O QUE FICOU PROVADO

O placar do laboratório

Controle	O que você provou	Onde está a evidência
A.5.9	Inventário de ativos	Módulo de inventário
A.8.2	Uso de privilégio registrado	Regra customizada 100012
A.8.9	Baseline e desvio de configuração	SCA + integridade de arquivo
A.8.15	Log centralizado e íntegro	Acervo de alertas
A.8.16	Detecção ativa com correlação	Regra 100010 + dashboard ISO

Cinco controles com evidência viva — e nenhum deles exige trabalho manual recorrente.

CAPÍTULO 5

O SGSI depois da festa

6 **Mês 6 — Tudo funciona**

Alertas chegam, pessoas respondem, dashboards são olhados.

10 **Mês 10 — Os alertas viraram ruído**

A caixa de entrada normalizou o vermelho. Ninguém abre mais.

11 **Mês 11 — A descoberta**

Alguém lembra que a auditoria de manutenção é daqui a três semanas.

Automação resolve a coleta. Não resolve a atenção.

CADÊNCIA SUGERIDA

Com que frequência cada coisa acontece

Frequência	O que acontece
Diário	Triagem de alertas de severidade alta · verificação de saúde da coleta
Semanal	Revisão de achados de baseline · fila de vulnerabilidades novas
Mensal	Indicadores para a gestão · revisão de mudanças emergenciais
Trimestral	Revisão de direitos de acesso (A.5.18) · teste de restauração (A.8.13)
Semestral	Auditoria interna (cláusula 9.2) · teste de plano de continuidade
Anual	Análise crítica pela direção (9.3) · revisão completa da SoA e da análise de risco

Ponto de partida, não receita. A frequência certa é a que corresponde ao seu risco.

CLÁUSULAS 9.2 E 9.3

Duas obrigações que não são do Anexo A

CLÁUSULA 9.2

Auditoria interna

Você precisa auditar a si mesmo antes do auditor externo chegar.

É onde mais gente escorrega: investe em controle técnico e é reprovada por processo, não por segurança.

CLÁUSULA 9.3

Análise crítica pela direção

A alta direção precisa revisar o SGSI formalmente, com pauta e registro.

Sem patrocínio da direção não existe SGSI — isso está na cláusula 5.

Para o pessoal técnico: você vai ser convocado para a auditoria interna. Se sua evidência for automática, isso te custa uma tarde. Se for manual, te custa duas semanas.

CAPÍTULO 5

Controle sem dono é controle morto

“Segurança da informação” como dono de tudo é o mesmo que ninguém. E “TI” também não é dono — quando o alerta chega na fila coletiva, a responsabilidade se dissolve.

Regra: dono do controle é quem tem autoridade para mudar a configuração que sustenta aquele controle.

A.8.20

Time de rede

Segurança de redes, segregação, filtros.

A.8.13

Quem opera backup

Execução, teste de restauração e registro.

A.5.18

Gestor de cada área

Decisão sobre acessos; identidade opera o processo.

RISCO

Alguém mais sênior

Quem aceita risco residual precisa de autoridade para aceitar.

ROTEADORES, SWITCHES, APPLIANCES

E o equipamento que não aceita agente?

Syslog. Aponte tudo para o coletor central — roteador, switch, firewall, controladora, no-break. A maior parte do seu parque resolve assim.

GARANTA 1

Log com autenticação e comandos

É por isso que a autenticação centralizada do capítulo 3 importa tanto: sem ela, o log diz o que foi feito mas não quem fez.

GARANTA 2

Relógio sincronizado

A.8.17 de novo. Equipamento com relógio errado contamina toda a correlação do coletor.

GARANTA 3

Regra de detecção do lado do coletor

Log de equipamento chegando e ninguém correlacionando é o problema do A.8.15 versus A.8.16 outra vez.

CONTROLE NOVO EM 2022

Nuvem: o mínimo que A.5.23 exige

1

Saber a fronteira

Modelo de responsabilidade compartilhada: o que o provedor garante, o que é seu. Isso vai documentado — o auditor vai perguntar.

2

Trazer os logs para casa

Log de auditoria que só existe no console do provedor não está no seu monitoramento. Integre à coleta central.

3

Gestão de identidade da nuvem

Chave de acesso sem rotação e conta privilegiada sem MFA são as duas falhas mais comuns — e ambas são achado direto de A.8.2 e A.8.5.

A.5.24 A A.5.28

Incidentes: onde tudo é testado de verdade

O QUE A NORMA PEDE

O ciclo completo

Planejamento · Avaliação · Resposta · Aprendizado

Incluindo a parte que ninguém faz, que é o aprendizado.

A CAMADA JURÍDICA

Prazos que correm

Dado pessoal envolvido → comunicação à ANPD e aos titulares (LGPD)

Serviço de telecom → o que a Resolução Anatel nº 740/2020 determina

Esses prazos correm a partir do momento em que você toma conhecimento.
Aquele agente que ficou três semanas desconectado? Se o incidente aconteceu naquela janela, você não perdeu só evidência. Você perdeu o relógio regulatório.

Cláusula 10 — Melhoria

PASSO 1

Corrigir

Resolver o sintoma. É onde a maioria para.

PASSO 2

Analisar a causa

Por que aconteceu? O que permitiu que acontecesse?

PASSO 3

Impedir a repetição

O que muda no processo ou na configuração para não voltar.

Não conformidade sem análise de causa é conserto, não melhoria. E o auditor sabe distinguir.

Automatizar a coleta sem automatizar a revisão só acelera o acúmulo de evidência que ninguém olha.

A automação precisa chegar até a fila de trabalho de alguém: alerta que vira tarefa atribuída, com prazo e registro de tratativa. Aí o ciclo fecha.

CHECKLIST DE PARTIDA · 1 A 5

Os dez primeiros passos

1 **Defina o escopo, por escrito, em um parágrafo**

Qual parte da organização, quais serviços, quais localidades. Se não couber em um parágrafo, está grande demais.

2 **Levante o inventário — automaticamente**

Não abra planilha. O inventário que você mantém à mão é o que vai estar errado.

3 **Liste seus dez maiores riscos**

Dez, não cem. Com dono e impacto. Uma tabela simples resolve o começo.

4 **Mate as contas compartilhadas**

O item mais doloroso da lista e o de maior retorno. Autenticação centralizada e MFA nas contas administrativas.

5 **Centralize os logs**

Um destino, relógio sincronizado, retenção definida por tipo de log.

CHECKLIST DE PARTIDA · 6 A 10

Os dez primeiros passos

6 **Coloque configuração de rede em versionamento**

Resolve dois controles de uma vez — e você provavelmente já tem a ferramenta.

7 **Aplique um baseline e meça o desvio**

Comece por um benchmark CIS no sistema operacional que você mais tem. Não tente fazer tudo.

8 **Defina uma regra de detecção e um destinatário**

Uma só, para começar. Alerta que chega em quem sabe o que fazer vale mais que cinquenta regras num painel órfão.

9 **Teste uma restauração de backup e registre**

Este mês. É o controle com maior distância entre o que as empresas acham que têm e o que realmente têm.

10 **Monte a SoA com a coluna de evidência apontando para lugares vivos**

Se apontar para uma pasta de prints, você recomeçou o problema.

CHECKLIST

A ordem importa

PASSOS 1 A 3

Gestão

Escopo · Inventário · Riscos

Definem o que importa e o que fica de fora.

PASSOS 4 A 9

Técnica

Acessos · Logs · Versionamento · Baseline · Detecção · Backup

Instrumentam o que foi definido acima.

Não faça os técnicos primeiro. Sem escopo e sem risco você vai instrumentar o que não importa e deixar de fora o que importa. Já vi acontecer.

RECAPITULAÇÃO

Resumo em uma tela

→

A ISO 27001 não é sobre documento

É sobre conseguir demonstrar que um controle existia ontem, existe hoje e vai existir amanhã.

→

O que falta não é controle — é rastro

A distância entre um provedor bem operado e um SGSI certificável é menor do que parece.

→

Nenhuma ferramenta entrega conformidade pronta

Ela entrega a capacidade de recuperar evidência. A tradução é trabalho de engenharia, e é seu.

→

Se a evidência precisa de trabalho humano, ela vai falhar

Automatize a produção da evidência — e a chegada dela na mesa de alguém.

Obrigado.

Agora vamos ao vivo. Traga o caso específico da sua rede, a dúvida que parece boba, e a discordância também — é a melhor parte.

MATERIAL DISPONÍVEL PARA DOWNLOAD

Guia do laboratório · Tabela de tradução de controles · Arquivo de regras ISO 27001 · Estes slides

Leandro Silva

CISO

Autor de “Construindo Sistemas Seguros e Escaláveis” (Novatec)