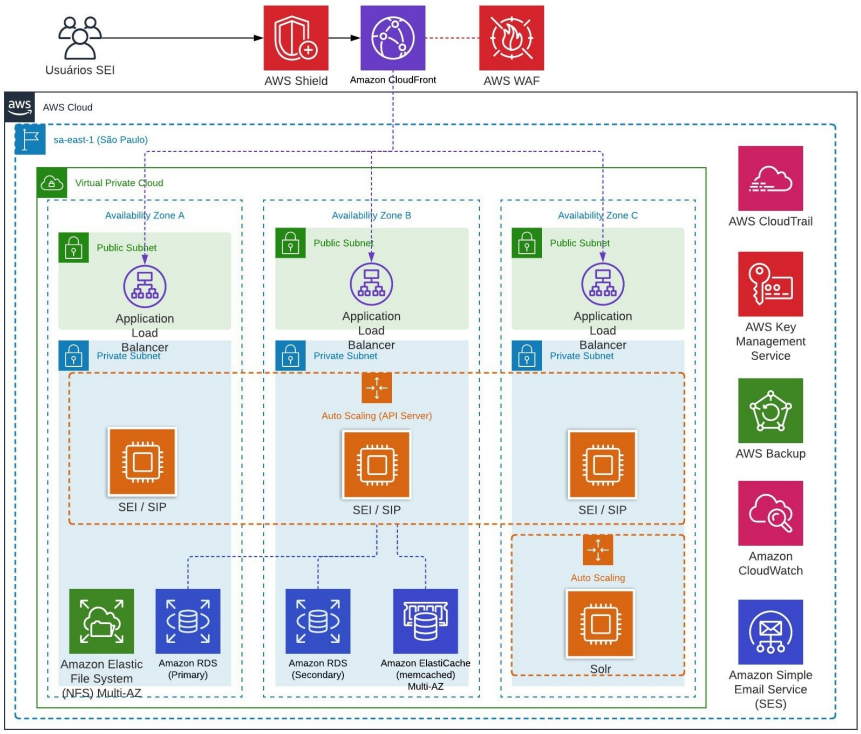
Relatório de análise da solução: Arquitetura2



Análise completa da solução atual

Modelo de cloud:
AWS (região sa-east-1, São Paulo)

Lista com os componentes:
- Amazon CloudFront (CDN) com origem no Application Load Balancer
- AWS Shield (proteção DDoS, presumivelmente Shield Standard; opcionalmente Shield Advanced)
- AWS WAF (Web Application Firewall) em frente ao CloudFront/ALB
- VPC com sub-redes públicas (A, B, C) e privadas (A, B, C)
- Application Load Balancer (ALB) distribuído nas AZs A, B e C
- Auto Scaling Group de EC2 para API/app SEI/SIP nas AZs A e B
- Auto Scaling Group de EC2 para Solr (busca) na AZ C
- Amazon RDS Multi-AZ (primário na AZ A, secundário/standby na AZ B)
- Amazon ElastiCache for Memcached Multi-AZ
- Amazon Elastic File System (EFS) Multi-AZ (NFS) para armazenamento compartilhado
- Amazon SES (Simple Email Service) para envio de e-mails
- AWS Key Management Service (KMS) para chaves e criptografia
- AWS CloudTrail (auditoria de API)
- Amazon CloudWatch (métricas, logs e alarmes)
- AWS Backup (políticas de backup para RDS/EFS/etc.)
- Controles implícitos: Security Groups, NACLs, IAM Roles/Policies, rotas, endpoints VPC (não desenhados, mas recomendados)

Interação entre os componentes:
1) Usuários SEI acessam via Internet -> CloudFront.
2) Requisições passam por AWS Shield e AWS WAF no CloudFront.
3) CloudFront encaminha para o ALB (origem); idealmente o ALB só aceita tráfego vindo do CloudFront.
4) O ALB distribui para instâncias EC2 do Auto Scaling (SEI/SIP) nas sub-redes privadas das AZs A e B.
5) A aplicação consome:
   - Banco transacional no Amazon RDS (conexões TLS).
   - Cache no ElastiCache (Memcached) para sessões/otimizações.
   - Sistema de arquivos compartilhado no EFS (NFS) para anexos/artefatos.
   - Motor de busca no cluster Solr (EC2 ASG na AZ C).
   - Envio de e-mails transacionais pelo Amazon SES.
6) Telemetria e auditoria: aplicações, ALB, WAF e serviços enviam logs/métricas ao CloudWatch;

chamadas de API de conta são registradas pelo CloudTrail.
7) Proteções de dados: chaves no KMS; volumes, RDS e EFS criptografados; backups orquestrados pelo AWS Backup.
8) Alta disponibilidade: ALB multi-AZ; RDS Multi-AZ; EFS multi-AZ; ASGs em múltiplas zonas (app em A/B, Solr em C).

O que esse sistema faz:
- Hospeda o SEI/SIP (aplicação web/API de gestão de processos e documentos) com:
  - Frontend/Backend escaláveis em EC2.
  - Busca full-text via Solr.
  - Banco relacional altamente disponível em RDS.
  - Armazenamento de documentos/anexos via EFS.
  - Cache de alto desempenho via ElastiCache.
  - Entrega de conteúdo e proteção na borda com CloudFront, Shield e WAF.
  - Envio de notificações e e-mails transacionais com SES.
  - Observabilidade, auditoria e backups gerenciados.

Vulnerabilidades e Solução para cada vulnerabilidade:
- Bypass do WAF/CloudFront acessando o ALB diretamente:
  Solução: restringir o ALB para aceitar somente tráfego do CloudFront (Security Group de origem, AWS Managed Prefix List do CloudFront ou validação de cabeçalho secreto no ALB). Considere tornar o ALB interno e usar CloudFront + origem privada via ALB interno com IPs privados e AWS Global Accelerator quando necessário.
- Memcached sem autenticação/TLS (ElastiCache Memcached não oferece auth nativa):
  Solução: restringir estritamente via Security Groups e sub-redes privadas; considerar migração para ElastiCache Redis com TLS e AUTH; segmentar por SG e NACL; monitorar portas 11211.
- Criptografia em trânsito inconsistente entre ALB–EC2/EFS/RDS/Solr:
  Solução: TLS obrigatório ponta a ponta (ALB-to-EC2 com ACM Private CA, RDS require SSL/TLS, EFS mount via TLS, Solr com TLS/Jetty); desabilitar protocolos inseguros; HSTS no CloudFront.
- Segredos em AMIs/user-data ou variáveis de ambiente:
  Solução: usar AWS Secrets Manager/SSM Parameter Store com rotação automática; IMDSv2; proibir segredos no código/repos.
- Falta de bloqueio de acesso público a Solr/ElastiCache/EFS:
  Solução: garantir que todos estes serviços só sejam acessíveis a partir das sub-redes privadas da aplicação; sem IPs públicos; Security Groups com princípio do menor privilégio; NACLs restritivas.
- Logs insuficientes ou não imutáveis:
  Solução: ativar logs de acesso do ALB, WAF e CloudFront em S3 com KMS; CloudTrail multi-região e organização; S3 Object Lock (Governance/Compliance) e MFA Delete; centralização e retenção adequada no CloudWatch Logs.
- Backup/DR apenas na mesma região:
  Solução: cópias de backup cross-region e cross-account (AWS Backup Vault Lock); RDS read replica/multi-region ou estratégia de restauração; EFS Replication; testes periódicos de restauração.
- Desbalanceamento de AZ (app só em A/B, Solr somente em C):
  Solução: distribuir instâncias de app por pelo menos 3 AZs; considerar Solr multi-nó em pelo menos 2 AZs; habilitar cross-zone load balancing no ALB.
- DDoS e picos de carga causando exaustão de conexões no RDS/ALB:
  Solução: Shield Advanced + DRT, regras WAF de rate limiting/bot control; tuning de pool de conexões (RDS Proxy), caching agressivo, escalonamento step/target-based; circuit breakers e filas quando apropriado.
- Vazamento de dados em respostas/cabeçalhos:
  Solução: CSP, X-Content-Type-Options, X-Frame-Options, Referrer-Policy; remoção de Server/Powered-By; validação/mascaração de dados; WAF com regras de Data Loss Prevention.
- Falhas de controle de acesso/IAM excessivo:
  Solução: políticas de menor privilégio, IAM Access Analyzer, revisões periódicas, SCPs no AWS Organizations, MFA obrigatório, chaves de acesso evitadas (use roles), RBAC por aplicação.
- Gestão de chaves KMS insegura:
  Solução: key policies mínimas, rotação, separação de funções (key admins vs key users), CloudTrail para eventos de KMS; considerar CloudHSM/XKS se requisito.
- Exfiltração via egress aberto a Internet:
  Solução: egress controlado por SG/NACL, NAT com listas de destinos permitidos, VPC endpoints para serviços AWS, VPC Flow Logs e inspeção de egress.
- Vulnerabilidades no SO/stack das EC2:
  Solução: hardening (CIS), patching automatizado com SSM Patch Manager, AMIs golden assinadas, verificação de integridade, desabilitar SSH público, SSM Session Manager, antivírus/EDR.
- Risco de envio de e-mails não autenticados/reputação (SES):
  Solução: SPF/DKIM/DMARC corretos, verificação de domínios/identidades, políticas de envio, SNS para bounces/complaints, templates seguros, criptografia end-to-end se necessário.
- Conexões Solr e queries pesadas causando indisponibilidade:
  Solução: autenticação/TLS no Solr, limitar endpoints, timeouts/limites de payload, autoscaling e heap

tuning, snapshots/replicação de índices, WAF para bloquear padrões maliciosos.

Relatório de Modelagem de Ameaças (STRIDE)
- Escopo e ativos:
  - Ativos principais: dados de processos/documentos do SEI, contas de usuários, anexos no EFS, banco RDS, índices Solr, segredos e chaves KMS, logs/auditoria.
  - Superfícies de ataque: CloudFront/ALB endpoints, APIs do SEI, integrações com SES, portas internas (RDS, Memcached, Solr, EFS), plano de controle AWS (IAM, APIs), pipeline de deploy/AMIs.
  - Limites de confiança: Internet -> CloudFront/WAF; Borda -> ALB; ALB -> sub-redes privadas; App -> serviços gerenciados (RDS, EFS, ElastiCache, SES); Conta AWS -> serviços de segurança (KMS, CloudTrail, Backup).

- Data flows resumidos:
  1. Usuário -> CloudFront/WAF -> ALB -> App EC2.
  2. App -> RDS/ElastiCache/EFS/Solr/SES.
  3. Serviços -> CloudWatch/CloudTrail/Backup/KMS.

- Assunções:
  - Somente CloudFront chega ao ALB.
  - Tráfego interno é TLS.
  - SG/NACL seguem menor privilégio.
  - RDS/EFS/ElastiCache não são públicos.

STRIDE por categoria:
1) Spoofing (falsificação de identidade)
   - Ameaças: roubo de credenciais/sessão; chamadas diretas ao ALB; spoof de origem CloudFront; abuso de SES para phishing.
   - Mitigações: MFA e senhas fortes; OAuth/OpenID Connect se aplicável; tokens com rotatividade/expiração; validação de header secreto do CloudFront; ALB restrito por SG; TLS mútuo interno quando possível; SES com SPF/DKIM/DMARC; WAF Bot Control e reCAPTCHA/humans no app.
   - Risco atual: Médio (eleva a Alto se ALB aceitar tráfego público direto).

2) Tampering (violação/alteração)
   - Ameaças: alteração de dados em trânsito; manipulação de logs; alteração de objetos no EFS; queries Solr maliciosas.
   - Mitigações: TLS 1.2+ em todos os hops; criptografia em repouso com KMS; least privilege no IAM; S3 Object Lock e assinatura de logs; controles de integridade no app; WAF para bloquear payloads; backups frequentes do EFS/índices.
   - Risco atual: Médio.

3) Repudiation (negação)
   - Ameaças: usuários negam ações; operadores negam mudanças de configuração.
   - Mitigações: CloudTrail org/multi-região com validação; logs do ALB/WAF/CloudFront em S3 com KMS; correlação de IDs de requisição; NTP sincronizado; retenção adequada; trilhas imutáveis (Object Lock).
   - Risco atual: Baixo-Médio.

4) Information Disclosure (divulgação)
   - Ameaças: vazamento de PII/documentos via respostas, logs, EFS, snapshots, e-mails; má configuração de cache no CloudFront.
   - Mitigações: mascaramento nos logs; headers de segurança (CSP, etc.); Field-Level Encryption no CloudFront se necessário; no-store para conteúdo sensível; segregação de dados; criptografia end-to-end; revisão de conteúdo de e-mail; WAF DLP; IAM restritivo a backups/snapshots; segredos no Secrets Manager.
   - Risco atual: Médio-Alto (dependendo da sensibilidade dos dados do SEI).

5) Denial of Service (DoS)
   - Ameaças: DDoS L3/L7; exaustão de conexões no RDS; consultas pesadas no Solr; thundering herd em autoscaling.
   - Mitigações: Shield Advanced + WAF rate limit; CloudFront cache; RDS Proxy e limites de pool; timeouts/circuit breakers; escalonamento controlado; backpressure/filas; proteção a picos; alocação de capacidade e testes de carga.
   - Risco atual: Médio.

6) Elevation of Privilege (elevação de privilégio)
   - Ameaças: exploração de vulnerabilidades na app/EC2 para assumir IAM Role; SSRF contra IMDS; privilégios excessivos em banco/OS; chaves KMS mal geridas.

- Mitigações: IMDSv2 e bloqueio de metadados via hop-by-hop; roles minimalistas; segmentation por SG; patching/EDR; validação de entrada; RDS contas separadas (aplicação sem superusuário); boundary policies; análise estática/dinâmica; assinatura de imagens; KMS key policies mínimas.
- Risco atual: Médio.

Avaliação resumida de risco:
- Riscos mais críticos a endereçar primeiro: bypass do WAF/CloudFront para ALB; autenticação e TLS no tráfego interno; gestão de segredos; DR multi-região; segurança de Memcached; endurecimento de Solr.
- Plano de tratamento: aplicar controles de origem no ALB, migrar para Redis com TLS ou isolar Memcached estritamente, mTLS/TLS interno, centralizar/imutabilizar logs, habilitar backups cross-region e testar restauração, reforçar IAM/SSM/patching.

Additional resourcing needs:
- Project Manager do STRIDE: coordena escopo, sessões e plano de ação.
- Network Administrator: valida segmentação VPC, SG/NACL, NAT, endpoints VPC, e controles de egress.
- Security Officer/CISO: assegura conformidade com políticas internas e LGPD; define nível de risco aceitável; aprova WAF/KMS/DR.
- Cloud/DevOps Engineers: automatizam infraestrutura (IaC), CI/CD, AMIs hardened, observabilidade, escalabilidade e runbooks.
- Software Developers (SEI/SIP): detalham fluxos das APIs, autenticação/autorização, cabeçalhos de segurança, sanitização de entradas e política de cache no CloudFront.
- Database Administrator: tuning e segurança do RDS, RDS Proxy, criptografia, backups e PITR; gestão de usuários/roles no banco.
- Search/Platform Engineer: segurança e alta disponibilidade do Solr; replicação e backup de índices; TLS e autenticação do cluster.
- Systems Engineer (Linux/EC2): hardening CIS, SSM, IMDSv2, EDR, patching e controle de acesso.
- Email/Deliverability Specialist: configuração de SES, SPF/DKIM/DMARC, monitoramento de reputação, bounces/complaints.
- Compliance/Privacy Officer: classificação de dados, retenção de logs e adequação à LGPD.
- Optional Hardware/Security Module Specialist: se necessário CloudHSM/XKS para chaves KMS e requisitos criptográficos avançados.

Observações finais:
- Documente o modelo de dados e os fluxos em DFD/UML incluindo limites de confiança.
- Versione e mantenha os diagramas; revise o STRIDE a cada mudança material.
- Priorize correções com maior impacto/likelihood e valide com testes de segurança (SAST/DAST/pentest) e testes de recuperação de desastre.

Sugestões de melhorias

Abaixo está um diagrama Mermaid que representa a arquitetura proposta, os relacionamentos entre os componentes e um overlay de mitigações para as vulnerabilidades levantadas.

```mermaid
flowchart LR
  %% ========================
  %% BORDA / INTERNET
  %% ========================
  U[Usuários SEI (Internet)]
  CF[CloudFront\n+ AWS Shield\n+ AWS WAF (regras L7, rate limit, bot control)]
  U -->|HTTPS/TLS| CF

  %% ========================
  %% REGIÃO / VPC / AZs
  %% ========================
  subgraph AWS[Conta AWS - Região sa-east-1 (São Paulo)]
    subgraph VPC[VPC 10.0.0.0/16]
      %% --- Sub-redes Públicas (ALB, NAT) ---
      subgraph PUB[Sub-redes Públicas (A/B/C)]
        ALB[(Application Load Balancer\nCross-Zone ON\nRestrito a CloudFront)]
        NAT[NAT Gateway\n(egress control/allowlist)]
      end

      %% --- Sub-redes Privadas (App, RDS, Solr) ---
      subgraph PVT_A[Sub-redes Privadas - AZ A]
        APPA[EC2 ASG - SEI/SIP (AZ A)]
```

```
    RDSpri[(Amazon RDS (Multi-AZ)\nInstância Primária - AZ A)]
  end

  subgraph PVT_B[Sub-redes Privadas - AZ B]
    APPB[EC2 ASG - SEI/SIP (AZ B)]
    RDSstb[(Amazon RDS (Multi-AZ)\nStandby - AZ B)]
  end

  subgraph PVT_C[Sub-redes Privadas - AZ C]
    SOLR[EC2 ASG - Solr (Busca) (AZ C)]
  end

  %% --- Serviços compartilhados na VPC ---
  RDSProxy[(RDS Proxy)]
  CACHE[(ElastiCache\nMemcached (atual) / Redis (recomendado))]
  EFS[(Amazon EFS - NFS\nMulti-AZ)]
  VPCE[(VPC Endpoints\nS3 GW, SSM, KMS, STS, CloudWatch, SES)]
  SES[(Amazon SES)]
  KMS[(AWS KMS - chaves gerenciadas)]
  CW[(Amazon CloudWatch\nLogs/Métricas/Alarmes)]
  CT[(AWS CloudTrail\nOrg/Multi-região)]
  BAK[(AWS Backup\nVault c/ Vault Lock)]
 end
end

%% ========================
%% FLUXOS PRINCIPAIS
%% ========================
CF -->|HTTPS/TLS\nSomente origem CloudFront| ALB
ALB -->|TLS 1.2+| APPA
ALB -->|TLS 1.2+| APPB

%% App -> serviços
APPA -->|TLS| RDSProxy
APPB -->|TLS| RDSProxy
RDSProxy -->|TLS| RDSpri
RDSpri -.replicação/Failover-. RDSstb

APPA -->|porta 11211/6379\nTLS/AUTH quando Redis| CACHE
APPB -->|porta 11211/6379\nTLS/AUTH quando Redis| CACHE

APPA -->|NFS sobre TLS| EFS
APPB -->|NFS sobre TLS| EFS

APPA -->|TLS| SOLR
APPB -->|TLS| SOLR

APPA -->|API/SMTP via VPCE/NAT\nTLS| SES
APPB -->|API/SMTP via VPCE/NAT\nTLS| SES

%% Observabilidade / Auditoria
CF -->|logs| CW
ALB -->|access logs| CW
APPA -->|app logs/métricas| CW
APPB -->|app logs/métricas| CW
SOLR -->|logs/métricas| CW
CT -->|auditoria API| CW

%% Criptografia / Backups
KMS --- RDSpri
KMS --- EFS
KMS --- BAK
KMS --- CW
BAK -->|políticas/rotinas| RDSpri
BAK -->|políticas/rotinas| EFS

%% Egress control
PVT_A -.egress permitido-> NAT
PVT_B -.egress permitido-> NAT
```

```
  PVT_C -.egress permitido-> NAT
  PVT_A -.serviços AWS privados-> VPCE
  PVT_B -.serviços AWS privados-> VPCE
  PVT_C -.serviços AWS privados-> VPCE

  %% ========================
  %% OVERLAY DE MITIGAÇÕES (VULNS -> CORREÇÕES)
  %% ========================
  subgraph M[Mitigações de Segurança (principais)]
    M1[Bypass WAF/CF -> ALB:\n- SG do ALB permite APENAS CloudFront (Managed Prefix List)\n- Validação de cabeçalho secreto no ALB\n- (Opcional) ALB interno + Global Accelerator]
    M2[Memcached sem auth/TLS:\n- Isolamento estrito por SG/Sub-rede privada\n- Migrar para Redis com TLS + AUTH\n- Monitorar porta 11211]
    M3[TLS ponta a ponta:\n- ACM/Private CA p/ ALB->EC2\n- RDS require SSL\n- EFS mount TLS\n- Solr com TLS/Jetty\n- HSTS no CloudFront]
    M4[Segredos seguros:\n- AWS Secrets Manager/SSM PS com rotação\n- IMDSv2 obrigatório\n- Sem segredos em AMI/user-data]
    M5[Sem acesso público a Solr/EFS/Cache:\n- Sem IPs públicos\n- SG/NACL mínimo necessário]
    M6[Logs completos/imutáveis:\n- Logs ALB/WAF/CF em S3 KMS\n- CloudTrail org/multi-região\n- S3 Object Lock + MFA Delete\n- Retenção no CloudWatch]
    M7[Backup/DR multi-região:\n- AWS Backup cross-region e cross-account\n- Vault Lock\n- EFS Replication\n- Testes de restauração]
    M8[Balanceamento entre AZs:\n- App em 2-3 AZs\n- Solr multi-nó em 2 AZs\n- ALB cross-zone ON]
    M9[DoS/L7 spikes/RDS conexões:\n- Shield Advanced + DRT\n- WAF rate limiting/bot control\n- RDS Proxy + tuning de pools\n- Cache agressivo + circuit breakers]
    M10[Exposição de dados/headers:\n- CSP, X-CTO, X-Frame-Options, Referrer-Policy\n- Remover Server/Powered-By\n- WAF DLP]
    M11[IAM mínimo necessário:\n- Roles sem chaves estáticas\n- IAM Access Analyzer\n- SCPs, RBAC, MFA obrigatório]
    M12[Gestão de chaves KMS:\n- Key policies mínimas\n- Rotação/SoD\n- Monitorar via CloudTrail\n- (Se exigido) CloudHSM/XKS]
    M13[Exfiltração por egress:\n- Allowlist no NAT\n- VPC Endpoints para AWS\n- VPC Flow Logs + inspeção de egress]
    M14[Hardening EC2:\n- CIS hardening\n- SSM Patch/Session Manager\n- Desabilitar SSH público\n- EDR/antimalware]
    M15[Reputação/Autenticação SES:\n- SPF/DKIM/DMARC\n- SNS pra bounces/complaints\n- Políticas/quotas\n- Criptografia E2E se necessário]
    M16[Solr estável/seguro:\n- TLS + autenticação\n- Timeouts/limites\n- Heap tuning/autoscaling\n- Snapshots/replicação\n- Bloquear padrões maliciosos (WAF)]
  end

  %% Ligações das mitigações aos alvos (traceabilidade)
  M1 -.-> ALB
  M2 -.-> CACHE
  M3 -.-> ALB
  M3 -.-> APPA
  M3 -.-> APPB
  M3 -.-> RDSpri
  M3 -.-> EFS
  M3 -.-> SOLR
  M4 -.-> APPA
  M4 -.-> APPB
  M5 -.-> SOLR
  M5 -.-> EFS
  M5 -.-> CACHE
  M6 -.-> CF
  M6 -.-> ALB
  M6 -.-> CW
  M6 -.-> CT
  M7 -.-> BAK
  M7 -.-> RDSpri
  M7 -.-> EFS
  M8 -.-> APPA
  M8 -.-> APPB
  M8 -.-> SOLR
  M9 -.-> CF
  M9 -.-> ALB
  M9 -.-> RDSProxy
```

```
  M10 -.-> CF
  M11 -.-> KMS
  M11 -.-> APPA
  M11 -.-> APPB
  M12 -.-> KMS
  M13 -.-> NAT
  M13 -.-> VPCE
  M14 -.-> APPA
  M14 -.-> APPB
  M14 -.-> SOLR
  M15 -.-> SES
  M16 -.-> SOLR
```

Resumo descritivo e decisões-chave
- Borda e proteção: CloudFront com AWS WAF e Shield absorve DDoS e aplica regras L7. O ALB nas sub-redes públicas aceita tráfego somente do CloudFront (prefix list gerenciada e validação de cabeçalho secreto). Opcionalmente avaliar ALB interno + Global Accelerator.
- Camada de aplicação: EC2 em Auto Scaling distribuído entre AZs (idealmente 2-3 AZs) com TLS entre ALB e instâncias (certificados ACM PCA). Acesso a instâncias via SSM Session Manager; sem SSH público; IMDSv2 obrigatório.
- Dados e serviços:
  - RDS Multi-AZ com RDS Proxy para gerenciar conexões e TLS obrigatório; criptografia KMS e backups via AWS Backup (com Vault Lock e cópias cross-region).
  - EFS Multi-AZ montado com TLS e criptografia com KMS.
  - ElastiCache: isolar Memcached por SG e considerar migração para Redis com TLS e AUTH.
  - Solr: cluster com TLS/autenticação, replicação multi-AZ, limites/timeout e regras WAF para padrões maliciosos.
- E-mail: SES com SPF/DKIM/DMARC, monitoramento de bounces/complaints (SNS) e políticas de envio; usar endpoint VPC da API SES quando aplicável.
- Observabilidade e auditoria: Logs do CloudFront/ALB/WAF no S3 com KMS e Object Lock; CloudWatch para métricas/logs; CloudTrail org/multi-região. Correlacionar IDs de requisição e definir retenção adequada.
- Saída para Internet (egress): NAT com allowlist de destinos, VPC Endpoints para serviços AWS, VPC Flow Logs e inspeção de egress para evitar exfiltração.
- IAM e chaves: Princípio do menor privilégio com roles, MFA obrigatório, IAM Access Analyzer e SCPs. KMS com rotação, key policies mínimas e segregação de funções; avaliar CloudHSM/XKS se exigido.

Checklist de correções prioritárias
- Restringir o ALB a CloudFront (SG + prefix list) e validar cabeçalho secreto.
- Implementar TLS ponta a ponta (ALB->EC2, RDS require SSL, EFS TLS, Solr TLS).
- Migrar Memcached para Redis com TLS/AUTH ou isolar estritamente por SG.
- Adotar Secrets Manager/SSM PS e IMDSv2; remover segredos de AMIs/user-data.
- Ativar logs completos e imutáveis (S3 Object Lock) e CloudTrail multi-região.
- Configurar backups e cópias cross-region com AWS Backup Vault Lock; testar restauração.
- Fortalecer Solr (TLS/auth, limites, replicação) e distribuir app/Solr entre AZs.
- Implementar RDS Proxy e regras WAF de rate limit/bot control; considerar Shield Advanced.
- Endurecer EC2 (CIS, patching SSM, sem SSH público, EDR).
- Configurar SPF/DKIM/DMARC no SES e monitorar reputação.

Desenho da solução