Sumário

Implantação de um ambiente de contingência para segurança dos dados da Cinemateca Brasileira

Escopo

A disponibilidade contínua dos serviços digitais é uma exigência fundamental para a reputação, operação e segurança de uma instituição.

A Cinemateca Brasileira é a principal instituição dedicada à preservação da memória cinematográfica e audiovisual nacional. O patrimônio por ela custodiado engloba, além dos filmes em diferentes suportes e formatos, conjuntos documentais de inestimável valor histórico e cultural. Trata-se de um acervo de projeção e relevância nacional e internacional. O maior da América do Sul.

Além do seu acervo físico, a Cinemateca Brasileira constituiu ao longo de mais de sete décadas, um patrimônio informacional sobre a memória audiovisual brasileira sem precedentes no país. Suas bases de dados fomentam as mais variadas pesquisas no campo da cultura e podem ser acessadas pelo grande público de forma gratuita.

Além dos dados produzidos nas suas atividades cotidianas, a instituição possui um patrimônio digital que depende de uma complexa infraestrutura técnica para sua preservação. Esses ativos digitais são de fundamental importância, pois permitem a ampliação expressiva do acesso da população a obras audiovisuais e documentos históricos sobre nosso cinema e audiovisual, fomentando ações do campo da cultura e da educação.

A proposta ora apresentada, objetiva:

- Continuidade dos serviços online e acesso aos dados internamente e pela comunidade beneficiária da Cinemateca.
- Proteção contra falhas operacionais e ataques cibernéticos.
- Atendimento a requisitos de compliance e auditoria.
- Mitigação de riscos operacionais, legais e reputacionais.

- Segurança do processamento e tráfego de arquivos digitais relativos ao patrimônio arquivístico da instituição.
- Preservação de dados, informações e acervos digitais.

Recomendação Técnica de criação de Site de Contingência e Substituição de equipamentos com status End Of Life (EoL)

1. Introdução e justificativa do projeto

Apresentamos recomendações técnicas que justificam a implementação de um **site de contingência** (também conhecido como **site backup ou site secundário**) para ser ativado automaticamente ou manualmente em situações em que o site principal se torne indisponível.

Adicionalmente também apresentamos as justificativas técnicas, operacionais e estratégicas pelas quais a empresa não deve manter em operação equipamentos classificados como *End of Life* (EoL). O status EoL é atribuído pelo fabricante quando um equipamento ou software chega ao fim do seu ciclo de vida, deixando de receber suporte oficial, atualizações e manutenção.

2. Objetivo

Justifica a necessidade da implementação de um ambiente de contingência para assegurar e substituição dos dispositivos com status EoL.

- Continuidade dos serviços online e acesso aos dados críticos da organização
- Proteção contra falhas operacionais e ataques cibernéticos
- Atendimento a requisitos de compliance e auditoria
- Mitigação de riscos operacionais, legais e reputacionais
- Aumento da taxa de falhas: Componentes antigos apresentam maior propensão a defeitos e falhas críticas.
- Dificuldade de reposição de peças: A indisponibilidade de peças de reposição pode levar a longos períodos de inatividade.
- Melhorar o Desempenho Operacional: Garantindo suporte contínuo e acesso a novas tecnologias.
- Fortalecer a Governança de TI: Alinhando a gestão de ativos às melhores práticas de mercado (ITIL, COBIT, NIST).
- Otimizar Custos a Longo Prazo: Evitando gastos elevados com manutenções corretivas emergenciais.

3. Justificativas Técnicas

3.1. Segurança da Informação

3.1.1. Disponibilidade: A tríade da segurança da informação (CID - Confidencialidade, Integridade e Disponibilidade) destaca a **disponibilidade** como fundamental. Um site de contingência garante que o serviço continue operacional, mesmo diante de falhas.

3.1.2. Resiliência a ataques cibernéticos: Em caso de DDoS, ransomware ou comprometimento da infraestrutura, o ambiente alternativo pode ser acionado para evitar paradas prolongadas.

3.1.3. Segmentação de ambientes: Manter o ambiente de contingência isolado ajuda a reduzir o risco de contaminação cruzada em ataques.

3.1.4. Ausência de patches de segurança: Fabricantes deixam de corrigir vulnerabilidades, aumentando o risco de ataques cibernéticos, ransomwares e invasões.

3.1.5. Incompatibilidade com novas políticas de segurança: Ferramentas de criptografia, autenticação e controle de acesso podem não ser suportadas em sistemas antigos.

3.1.6. Exposição a riscos de conformidade: Equipamentos EoL podem violar requisitos de auditoria e certificações de segurança.

3.2. Compliance e Auditoria

3.2.1. Auditorias externas: A ausência de um plano de contingência pode ser classificada como **não conformidade** crítica em auditorias.

3.2.2. Contratos com clientes: SLAs com garantia de disponibilidade requerem mecanismos de redundância e recuperação.

3.2.3. Risco de não conformidade: Pode gerar falhas no cumprimento de normas como ISO 27001, LGPD, PCI DSS e demais regulamentações aplicáveis.

3.3. Gestão de Riscos

3.4. Redução de impacto financeiro: A indisponibilidade de serviços pode causar perdas de receita, multas e danos à reputação.

3.5. Resposta rápida a desastres: Incidentes como falhas elétricas, incêndios, enchentes ou sabotagens físicas podem deixar o datacenter indisponível. O site de contingência permite continuidade sem grandes interrupções.

3.6. Mitigação de falhas humanas: Mesmo falhas operacionais, como atualizações malsucedidas ou erro de configuração, podem ser recuperadas rapidamente por meio do ambiente secundário.

3.7. Financeiros: (1) Custos não planejados com manutenções emergenciais e substituição urgente. (2) Potenciais prejuízos decorrentes de indisponibilidade de serviços críticos.

4. Exemplos Reais de Falhas e Incidentes

4.1. OVH (França) – Incêndio em Datacenter (2021)

Um incêndio destruiu completamente um datacenter da **OVHcloud** em Strasbourg, impactando milhares de sites, bancos de dados e aplicações de empresas da Europa. Muitas não possuíam ambiente de contingência e **perderam dados permanentemente**.

4.2. Sony Pictures – Ataque Cibernético (2014)

Hackers da Coreia do Norte invadiram a infraestrutura da Sony, causando perda de dados e interrupção dos serviços corporativos. A falta de redundância e contingência atrasou a retomada das operações por semanas.

4.3. Amazon Web Services (EUA) – Falha em Região da AWS (2020)

Uma falha em uma zona de disponibilidade da AWS causou a **queda de múltiplos serviços**. Empresas que não mantinham ambientes de contingência em outra região ficaram completamente offline por horas.

4.4. Furacão Sandy (EUA) – Danos a Datacenters (2012)

Datacenters em Nova York foram inundados, deixando empresas offline por dias. Empresas com redundância em outras localidades recuperaram-se em minutos.

4.5. Incêndio Cinemateca Unidade Vila Leopoldina (2021)

Um incêndio atingiu um galpão da Cinemateca Brasileira, em São Paulo, destruindo toda a infraestrutura instalada.

5. Conclusão

A implementação de um site de contingência é uma **medida estratégica e técnica essencial** para garantir a continuidade dos negócios, a segurança da informação e a conformidade com legislações e normas internacionais.

Empresas que não adotam esse tipo de estratégia estão sujeitas a perdas severas — tanto financeiras quanto de reputação — além de sanções legais e operacionais.

A implementação de um **site de contingência** não deve ser vista como um custo adicional, mas sim como um **investimento essencial na continuidade** das ações, na proteção da informação e conformidade regulatória. Em um cenário cada vez mais dependente da tecnologia e sujeito a ameaças cibernéticas, a falhas operacionais e eventos naturais extremos, a **resiliência digital** tornou-se um diferencial competitivo e um requisito básico para a sustentabilidade das operações.

Os riscos associados à indisponibilidade de um site principal são múltiplos: perda de dados, interrupção de serviços, violação de contratos com clientes (SLA), sanções legais por descumprimento de normas como a LGPD e a ISO 27001, sem contar os impactos financeiros e reputacionais. Casos emblemáticos como o incêndio nos datacenters da OVH, o ataque à Sony Pictures e os efeitos do Furacão Sandy demonstram que **nenhuma organização está imune** — e que a **ausência de um plano de contingência pode resultar em danos irreversíveis**.

Adotar um site de contingência é, portanto, uma **decisão estratégica que evidencia maturidade na gestão de riscos** e compromisso com a entrega contínua de serviços aos clientes, parceiros e usuários internos. Além disso, atende a requisitos de compliance e auditoria, facilitando a atuação em mercados regulados ou com alta exigência técnica.

A recomendação aqui apresentada se alinha às boas práticas internacionais de segurança da informação, gestão de continuidade de negócios (BCM) e governança de TI, sendo um passo fundamental para garantir:

- A **sobrevivência operacional** diante de incidentes críticos;
- A **confiança do mercado e dos clientes** na robustez da infraestrutura tecnológica;
- A **previsibilidade de recuperação**, evitando decisões reativas e caóticas no momento da crise.

Dessa forma, recomenda-se fortemente a priorização da implementação de um site de contingência, com todas as garantias de segurança, sincronização, testes e monitoramento. A negligência nesse aspecto pode não apenas comprometer dados e operações, mas também a **reputação e a credibilidade de toda a organização**.

A permanência de equipamentos classificados como End of Life (EoL) na infraestrutura tecnológica da empresa representa um risco substancial e multifacetado que transcende aspectos puramente técnicos, alcançando diretamente as esferas financeira, operacional, estratégica e de conformidade regulatória. Ao manter ativos que não recebem mais atualizações de segurança, patches críticos ou suporte técnico oficial, a organização se coloca em uma posição de vulnerabilidade perante ameaças cibernéticas crescentes, falhas operacionais inesperadas e potenciais sanções decorrentes do descumprimento de normas e legislações vigentes, como a ISO 27001, LGPD, PCI DSS e outras que regulam o ambiente corporativo.

Além dos riscos de segurança, a utilização contínua de equipamentos obsoletos acarreta a inevitável deterioração da performance operacional, com impactos diretos na disponibilidade de serviços, confiabilidade de processos de negócios e satisfação dos clientes internos e externos. A dificuldade de reposição de peças, a falta de compatibilidade com tecnologias emergentes e o aumento exponencial dos custos de manutenção corretiva tornam a permanência desses ativos uma estratégia não apenas arriscada, mas economicamente inviável no médio e longo prazo.

Do ponto de vista da governança e da sustentabilidade tecnológica, substituir equipamentos EoL não é apenas uma recomendação técnica, mas uma ação estratégica alinhada com os princípios de gestão de risco, planejamento de capacidade e inovação contínua. Essa substituição permite que a organização mantenha sua infraestrutura alinhada às melhores práticas do mercado, aumente a resiliência de seus serviços, garanta conformidade regulatória e reduza significativamente a probabilidade de incidentes de alto impacto que poderiam comprometer a imagem da empresa, gerar prejuízos financeiros e afetar diretamente a continuidade de suas operações críticas.

Portanto, a decisão de substituir proativamente equipamentos com status End of Life deve ser encarada como um investimento na solidez e no crescimento sustentável da empresa, e não apenas como um custo de atualização. Trata-se de uma medida que assegura não apenas a manutenção do desempenho atual, mas também a capacidade de expansão futura, permitindo que a empresa permaneça competitiva, segura e preparada para responder de forma ágil às demandas do mercado e às transformações tecnológicas que inevitavelmente continuarão a ocorrer.

Cronograma de Execução-Projeto Firewall Replace

Projeto 2 - Firewall Replace	Out 1º Quinzena	Out 2º Quinzena	Nov 1º Quinzena	Nov 2º Quinzena	Dez 1º Quinzena	Dez 2º Quinzena	Jan 1º Quinzena	Jan 2º Quinzena
Comprar / Receber equipamentos								
Configurar dispositivos								
Instalar dispositivo para testes								
Instalar dispositivo em Produção								
Validar configurações								
Concluir Projeto								

1. Comprar / Receber Equipamentos

Descrição: Processo de aquisição, pedido formal aos fornecedores, acompanhamento de entrega e recebimento físico.

Atividade: Preparar os firewalls em laboratório.

Responsáveis: Área de Compras + TI.

Marco: Equipamentos recebidos e conferidos.

2. Configurar Dispositivos

Descrição: Configuração em laboratório ou ambiente controlado, aplicando padrões definidos.

Fazer: Preparar os firewalls em laboratório.

Responsáveis: Equipe de Infraestrutura de Rede e Projetos

Principais pontos de atenção: atualização de firmware para última versão estável, configuração de VLANs, trunking, roteamento, SNMP, syslog e segurança (ACLs), configuração dos servidores, configuração das vlans e regras de acesso via Firewall e documentar parâmetros aplicados.

Marco: Dispositivos prontos para instalação.

3. Instalar Dispositivo para Testes

Descrição: Simular tráfego real, validar regras de segurança, redundância, throughput e estabilidade.

Fazer: Instalar o firewall em ambiente de homologação ou rede controlada.

Responsáveis: Engenharia de Redes + Segurança da Informação.

Pontos de Atenção: criar cenários de falha para validar failover, testar integrações (Active Directory, autenticação multifator, monitoramento) e analisar logs e relatórios de eventos.

4. Instalar Dispositivo em Produção

Descrição: Instalar fisicamente no rack/datacenter e aplicar a configuração validada em testes, durante janela de manutenção.

Fazer: Realizar a substituição do firewall antigo pelo novo no ambiente produtivo.

Responsáveis: Equipe de Infraestrutura de Rede / Suporte de Campo.

Pontos de Atenção: planejar janela de mudança com mínimo impacto, ter plano de rollback documentado (caso ocorra falha) e validar conectividade de serviços críticos logo após a instalação.

5. Validar Configurações
Descrição: Testar conectividade de usuários, servidores e aplicações críticas, avaliar performance e monitoramento inicial.
Fazer: Realizar testes em produção após a instalação.
Responsáveis: Equipe de Redes + Operações de TI.
Pontos de Atenção:

- Garantir redundância e alta disponibilidade funcionando.
- Monitorar tráfego e alertas em tempo real (SNMP/syslog).
- Validar acessos externos (VPN, clientes remotos).

6. Concluir Projeto
Descrição: Documentar topologia final, configurações aplicadas, repassar conhecimento para equipe de operação e registrar aceite formal.

Fazer: Encerrar o projeto formalmente.

Responsáveis: PMO / Gestor de TI / Engenharia de Redes.

Pontos de Atenção: garantir que toda a documentação esteja completa e armazenada, realizar treinamento da equipe de suporte e obter assinatura de aceite da gestão/cliente interno.

Cronograma de Execução-Projeto Site CoB

Projeto 3 - Site CoB	Out 1º Quinzena	Out 2º Quinzena	Nov 1º Quinzena	Nov 2º Quinzena	Dez 1º Quinzena	Dez 2º Quinzena	Jan 1º Quinzena	Jan 2º Quinzena
Comprar / Receber equipamentos								
Contratar link de internet								
Instalar link de internet								
Instalar equipamentos físicamente								
Configurar novo ambiente e mantê-lo de forma isolada								
Configurar ambiente de sincronização dos dados								
Implementar solução de conexão entre os Sites								
Sincronizar dados entre os Sites								
Validar configurações técnicas								
Concluir Projeto								

1. Comprar / Receber Equipamentos
Descrição: Realizar processo de aquisição dos equipamentos necessários (servidores, storages, switches, roteadores, firewalls, racks, climatização).

Responsabilidades: Área de Compras / TI Infraestrutura.

Pontos de Atenção: garantir compatibilidade de hardware e licenciamento, antecipar prazos de importação/entrega e conferir garantias e contratos de suporte.

2. Contratar Link de Internet

Descrição: Selecionar provedor, negociar SLA, redundância e contratar circuitos de internet para o site de contingência.

Responsabilidades: equipe de Compras / TI.

Pontos de Atenção: contratar mais de um provedor para redundância, garantir tempo de ativação compatível com cronograma e formalizar SLA e suporte 24x7 com o provedor.

Dados Importantes: circuitos devem suportar replicação de dados e acesso remoto seguro.

3. Instalar Link de Internet

Descrição: Acompanhar a instalação física dos links pelos provedores, testes de ativação e homologação de banda.

Responsabilidades: provedor de Serviços / Equipe de TI.

Pontos de Atenção: Validar contrato de endereçamento IP público, garantir redundância física (entradas distintas no site) e testar conectividade e latência antes de avançar.

4. Instalar Equipamentos Fisicamente

Descrição: instalação de racks, servidores, storages, switches e firewalls no site CoB.

Responsabilidades: Equipe de Infraestrutura e TI.

Pontos de Atenção: Verificar climatização e energia elétrica estabilizada, garantir organização do cabeamento estruturado e testar redundância de energia (Nobreak/gerador).

5. Configurar Novo Ambiente (Isolado)

Descrição: configuração inicial dos equipamentos e serviços do site CoB de forma isolada da produção, simulando ambiente independente.

Responsabilidades: Engenharia de Redes + Equipe de Servidores.

Pontos de Atenção: configurar VLANs e roteamento internos sem interferir na produção. Garantir segurança (firewall e segregação de rede) e validar licenciamento de sistemas.

6. Configurar Ambiente de Sincronização de Dados

Descrição: Implantar mecanismos de replicação (storage replication, backup, base de dados, AD, etc.) entre produção e CoB.

Responsabilidades: equipe de TI.

Pontos de Atenção: testar replicação incremental e full, monitorar latência e janelas de replicação e validar integridade dos dados replicados.

7. Implementar Solução de Conexão entre os Sites

Descrição: Estabelecer conectividade segura entre produção e CoB (MPLS, VPNs, SD-WAN).

Responsabilidades: Equipe de Redes / Segurança da Informação.

Pontos de Atenção: garantir criptografia de ponta a ponta e validar redundância (túneis múltiplos).

- **Dados Importantes:** requisito crítico para suportar sincronização de dados e failover.

8. Sincronizar Dados entre os Sites

Descrição: Efetivar a sincronização dos dados de produção com o site CoB, seguindo política de replicação definida.

Responsabilidades: equipe de Infraestrutura

Pontos de Atenção: verificar performance durante replicação inicial (bulk sync), garantir consistência entre bancos de dados e validar replicação contínua sem perda de pacotes.

9. Validar Configurações Técnicas

Descrição: testar conectividade, integridade de dados, failover e acessos ao site CoB.

Responsabilidades: engenharia de redes + segurança + Aplicações.

Pontos de Atenção: executar plano de testes de contingência (DRP), garantir que SLAs de RTO/RPO sejam atendidos e documentar resultados e eventuais ajustes.

10. Concluir Projeto

Descrição: Encerramento formal do projeto com aceite da gestão. Inclui documentação final, transferência de conhecimento e treinamento da equipe.

Responsabilidades: PMO / Gestor de TI / Equipes Técnicas.

Pontos de Atenção:

- Treinamento das equipes de operação e suporte, garantir que a documentação esteja completa (diagramas, configs, procedimentos) e formalizar aceite final do cliente interno.

Dados Importantes: Registrar o site CoB no plano de continuidade de negócios (BCP/DRP).

Cronograma de Execução-Projeto Switch Replace

Projeto 1 - Switch Replace	Out 1º Quinzena	Out 2º Quinzena	Nov 1º Quinzena	Nov 2º Quinzena	Dez 1º Quinzena	Dez 2º Quinzena	Jan 1º Quinzena	Jan 2º Quinzena
Comprar / Receber equipamentos								
Configurar dispositivos								
Efetuar instalações dos dispositivo								
Validar configurações								
Concluir Projeto								

3. Comprar / Receber Equipamentos

Descrição: Processo de aquisição, pedido formal aos fornecedores, acompanhamento de entrega e recebimento físico.

Responsáveis: Área de Compras + TI.

Marco: Equipamentos recebidos e conferidos.

4. Configurar Dispositivos

Descrição: Configuração em laboratório ou ambiente controlado, aplicando padrões definidos.

Responsáveis: Equipe de Infraestrutura de Rede e Projetos

Principais pontos de atenção: atualização de firmware para última versão estável, configuração de VLANs, trunking, roteamento, SNMP, syslog e segurança (ACLs), configuração dos servidores, configuração das vlans e regras de acesso via Firewall e documentar parâmetros aplicados.

Marco: Dispositivos prontos para instalação.

5. Efetuar Instalações dos Dispositivos

Descrição: Substituição física dos switches antigos pelos novos, em racks e datacenters.

Responsáveis: Equipe de TI + Projetos

Principais pontos de atenção:

Planejamento de janela de manutenção.

Verificação de energia, cabeamento e redundância.

Backup das configurações antigas antes da troca.

Marco: Todos os switches novos instalados em produção.

6. Validar Configurações

Descrição: Testes pós-instalação para validar conectividade, desempenho e segurança.

Responsáveis: Engenheiros de Rede / Equipe de Suporte.

Principais pontos de atenção: Testar redundância, enlaces e roteamento, validar conectividade e servidores críticos, monitoramento inicial (logs, SNMP, desempenho).

Marco: Rede homologada e estável.

7. Concluir Projeto

Descrição: Etapa final de documentação, passagem de conhecimento e aceite formal.

Responsáveis: PMO / Gestor de TI.

Principais pontos de atenção: documentar topologia final e configurações aplicadas, treinar a equipe de operação e suporte, obter aceite formal do projeto

Marco: Projeto encerrado oficialmente.

Orçamento Previsto

ORÇAMENTO PREVISTO DO PROJETO

Descrição	Referência	Quantidade	Valor Unitário	Previsto	Tipo
PROJETO DE INFRAESTRUTRUA DE REDE E OU CABEAMENTO ESTRUTURADO - Serviço de mão de obra - Projeto Switch Replace	9256	1	23.904	23.904	Serviço
PROJETO DE INFRAESTRUTRUA DE REDE E OU CABEAMENTO ESTRUTURADO-Serviço de mão de obra - Projeto Firewall	9255	1	27.750	27.750	Serviço
Switch HPE Networking Instant On 1930 48G 4SFP/SFP+ JL685A	9088	7	3.239	22.671	Aquisição
Transceiver - Conversor de Mídia HPE - LC SR 300m - 10G SFP+ - MPN: J9150D	9088	3	4.081	12.242	Aquisição
Rack Servidor Perfurado 44U x 1070mm	9091	1	7.708	7.708	Aquisição
Patch panel 24p cat6 modular multilan (35030015) - 7170	9091	2	1.320	2.641	Aquisição
Patch Cord CAT.6 Azul SohoPlus 1,50 Metros - 5899	9091	30	42	1.256	Aquisição
Switch PoE HPE Networking Instant On 1930 48G 370W 4SFP+ JL686B	9091	1	5.897	5.897	Aquisição
Storage NAS Enterprise - 144TB | 8GB Memória | 1 PROC | 4 Network Interface	9091	1	181.763	181.763	Aquisição
Regua de tomada 4 / 4 colares sem cabo - 7601	9091	3	260	781	Aquisição
Acessórios gerais rack	9091	1	1.998	1.998	Aquisição
Kit FortiGate 80F + UTP + FortiCloud – Gestão na Nuvem (12 meses)	9091	1	22.637	22.637	Aquisição
Projeto / licença de criação de SW de sincrinização de dados	9091	1	24.000	24.000	Licenciamento
Fortigate FG-100F - Fortinet - FG-100F	9092	1	26.932	26.932	Aquisição
Licença Fortinet ATP - 1 ano	9092	1	10.746	10.746	Licenciamento
PROJETO DE INFRAESTRUTRUA DE REDE E OU CABEAMENTO ESTRUTURADO-Serviço de mão de obra - Site CoB	9257	1	59.940	59.940	Serviço
PROJETO DE INFRAESTRUTRUA DE REDE E OU CABEAMENTO ESTRUTURADO-Serviço de garantir e gestão do ambiente por 12 meses.	9257	1	67.155	67.155	Serviço
			TOTAL	**500.021**	

Cronograma de Desembolso

Descrição/Meses	out/25	nov/25	dez/25	jan/26	Total
Serviço	44.687	44.687	44.687	44.687	**178.749**
Aquisição	143.263	143.263			**286.526**
Licenciamento	34.746				**34.746**
				TOTAL	**500.021**