IT Disaster Recovery Plan & Data Backup

Introduction

Modern businesses, regardless of size, rely on large volumes of digital information to sustain operations. Loss or corruption of data caused by hardware failure, human error, cyberattacks, or natural disasters can jeopardize business continuity.

An IT Disaster Recovery Plan (DRP), combined with a Data Backup Plan, is essential to ensure resilience, continuity, and protection of IT infrastructure.

Plan Objectives

1. Ensure business continuity during incidents.
2. Define recovery priorities based on Business Impact Analysis (BIA).
3. Restore critical systems, data, and connectivity as quickly as possible.
4. Minimize financial and reputational losses.
5. Ensure regulatory compliance (GDPR, HIPAA, LGPD, ISO 27001).

Core Components of an IT Disaster Recovery Plan

1) Business Impact Analysis (BIA)

Identify critical business functions and their dependencies.

Define Recovery Time Objective (RTO) — maximum acceptable downtime.

Define Recovery Point Objective (RPO) — maximum acceptable data loss.

Quantify the financial and operational impact of downtime.

2) Inventory & Prioritization of Resources

1. Hardware: servers, networks, desktops, laptops, mobile devices.
2. Software: ERP, CRM, email, collaboration, internal apps.
3. Data: databases, critical files, and digital records.
4. Infrastructure: secure rooms, redundant power and cooling.
5. Connectivity: dedicated internet, redundant ISPs, VPNs.

3) Recovery Strategies

1. Hardware: standardization, maintenance SLAs, golden images for rapid rebuild.
2. Software: licensed copies, configuration documentation, hot/warm/cold sites.
3. Data: local, remote, and cloud backup strategies (3-2-1 rule).
4. Connectivity: multiple ISPs, redundant routing and failover.

5. Physical Environment: UPS systems, generators, redundant cooling.

4) Testing & Validation

Run semi-annual or annual exercises; simulate power loss, ransomware, or database corruption.

Validate that restoration times meet RTOs and that data currency meets RPOs.

Perform post-exercise reviews and continuously improve procedures and documentation.

Data Backup Plan

Data is a critical asset. Without reliable backups, data loss can result in severe disruption or business failure.

Backup Strategies

1. Full Backup: complete copy of all data.
2. Incremental Backup: only changes since the last backup.
3. Differential Backup: changes since the last full backup.
4. 3-2-1 Rule: 3 copies of data, 2 different media, 1 off-site copy (cloud or separate location).

Frequency & Scheduling

1. Daily backups for critical systems; weekly for less sensitive datasets.
2. Schedule backups outside peak hours; monitor job success and duration.
3. Perform regular restore tests to validate integrity and recovery time.

Protection & Security

1. Encrypt data in transit and at rest.
2. Apply least-privilege access controls and multi-factor authentication for backup consoles.
3. Keep auditable logs for backup and restore operations.
4. Align storage security with ISO 27040; review vendor SLAs and support contracts.

DRP + Backup Integration

A DRP is ineffective without a reliable Backup strategy. RTO must align with restoration time; RPO with business tolerance. Plans should be documented, tested, and integrated.

Best Practices

1. Keep documentation up to date; train stakeholders regularly.
2. Automate backup and monitoring; prefer immutable or versioned storage where possible.
3. Use hybrid on-prem + cloud approaches and ensure geographic redundancy.
4. Protect backup infrastructure from the primary domain (separate credentials, network segmentation).
5. Implement tabletop exercises and executive-level reporting on readiness.

Conclusion

A robust IT DRP combined with a Data Backup program prepares organizations to respond effectively to failures, attacks, or disasters — preserving continuity, reputation, and customer trust.

References

NIST SP 800-34: Contingency Planning Guide for Federal Information Systems.

ISO/IEC 27031: Guidelines for ICT Readiness for Business Continuity.

ITIL v4: Service Continuity Management.

CIS Controls v8 – Control 11: Data Recovery.

Plano de Recuperação de Desastres em TI & Backup de Dados

Introdução

Empresas modernas, independentemente do porte, dependem de grandes volumes de informações digitais para manter suas operações. A perda ou corrupção de dados causada por falhas de hardware, erro humano, ataques cibernéticos ou desastres naturais pode comprometer a continuidade do negócio.

Um Plano de Recuperação de Desastres em TI (DRP), aliado a um Plano de Backup de Dados, é essencial para garantir resiliência, continuidade e proteção da infraestrutura tecnológica.

Objetivos do Plano

1. Garantir a continuidade do negócio durante incidentes.
2. Definir prioridades de recuperação com base na Análise de Impacto nos Negócios (BIA).
3. Restaurar rapidamente sistemas críticos, dados e conectividade.
4. Minimizar perdas financeiras e de reputação.
5. Assegurar conformidade regulatória (LGPD, GDPR, HIPAA, ISO 27001).

Componentes Essenciais de um Plano de Recuperação de Desastres em TI

1) Análise de Impacto nos Negócios (BIA)

Identificar funções críticas do negócio e suas dependências.

Definir RTO — tempo máximo aceitável de indisponibilidade.

Definir RPO — ponto máximo de perda de dados aceitável.

Quantificar o impacto financeiro e operacional da indisponibilidade.

2) Inventário e Priorização de Recursos

1. Hardware: servidores, redes, desktops, laptops, dispositivos móveis.
2. Software: ERP, CRM, e-mail, colaboração, aplicativos internos.
3. Dados: bancos de dados, arquivos críticos e registros digitais.
4. Infraestrutura: salas seguras, energia e climatização redundantes.
5. Conectividade: internet dedicada, ISPs redundantes, VPNs.

3) Estratégias de Recuperação

1. Hardware: padronização, SLAs de manutenção, imagens 'golden' para reconstrução rápida.
2. Software: cópias licenciadas, documentação de configuração, ambientes hot/warm/cold site.

3. Dados: estratégias de backup locais, remotas e em nuvem (regra 3-2-1).
4. Conectividade: múltiplos provedores, roteamento redundante e failover.
5. Ambiente Físico: UPS, geradores, climatização redundante.

4) Testes e Validação

Realizar exercícios semestrais ou anuais; simular falta de energia, ransomware ou corrupção de banco de dados.

Validar que os tempos de restauração atendem aos RTOs e que a atualidade dos dados atende aos RPOs.

Executar revisões pós-exercício e promover melhoria contínua de procedimentos e documentação.

Plano de Backup de Dados

Dados são ativos críticos. Sem backups confiáveis, a perda pode causar interrupções severas ou até a falência do negócio.

Estratégias de Backup

1. Full Backup: cópia completa de todos os dados.
2. Incremental Backup: apenas mudanças desde o último backup.
3. Differential Backup: mudanças desde o último backup completo.
4. Regra 3-2-1: 3 cópias, 2 mídias diferentes, 1 cópia off-site (nuvem ou local distinto).

Frequência e Agendamento

1. Backups diários para sistemas críticos; semanais para conjuntos menos sensíveis.
2. Agendar fora do horário de pico; monitorar sucesso e duração dos jobs.
3. Realizar testes regulares de restauração para validar integridade e tempo de recuperação.

Proteção e Segurança

1. Criptografar dados em trânsito e em repouso.
2. Aplicar controle de acesso de menor privilégio e MFA no console de backup.
3. Manter logs auditáveis das operações de backup e restauração.
4. Alinhar a segurança de armazenamento à ISO 27040; revisar SLAs e contratos de suporte de fornecedores.

Integração DRP + Backup

Um DRP é ineficaz sem uma estratégia de Backup confiável. O RTO deve estar alinhado ao tempo de restauração; o RPO à tolerância do negócio. Os planos precisam ser documentados, testados e integrados.

Boas Práticas

1. Manter a documentação atualizada; treinar stakeholders regularmente.

2. Automatizar backup e monitoramento; preferir armazenamento imutável ou versionado quando possível.
3. Usar abordagem híbrida on-prem + cloud e garantir redundância geográfica.
4. Isolar a infraestrutura de backup do domínio primário (credenciais separadas, segmentação de rede).
5. Executar exercícios de mesa e relatórios executivos de prontidão.

Conclusão

Um DRP sólido, combinado a um programa de Backup de Dados robusto, prepara a organização para responder a falhas, ataques ou desastres — preservando continuidade, reputação e a confiança dos clientes.

Referências

NIST SP 800-34: Contingency Planning Guide for Federal Information Systems.

ISO/IEC 27031: Guidelines for ICT Readiness for Business Continuity.

ITIL v4: Service Continuity Management.

CIS Controls v8 – Control 11: Data Recovery.