UNIVERSIDADE SÃO JUDAS TADEU – USTJ

SISTEMAS COMPUTACIONAIS E SERGURANÇA

Arthur Frederico Piasse Pereira - 824219186

Guilherme Pereira da Silva – 825129559

Jhonatan de Lima Alves dos Santos – 824215769

Sophia Grave Silva - 824213875

Zahra Neqcha - 824221748

ELABORAÇÃO DE UM PLANO DE CONTINUIDADE DE NEGÓCIOS

São Paulo

2025

Arthur Frederico Piasse Pereira - 824219186

Guilherme Pereira da Silva – 825129559

Jhonatan de Lima Alves dos Santos – 824215769

Sophia Grave Silva - 824213875

Zahra Neqcha - 824221748

ELABORAÇÃO DE UM PLANO DE CONTINUIDADE DE NEGÓCIOS

Este documento apresenta a Elaboração de um Plano de Continuidade de Negócios desenvolvidas para uma pequena empresa fictícia do comércio eletrônico, denominada "Controtec". O objetivo é desenvolver um esboço de Plano de Continuidade de Negócios para uma empresa fictícia, levando em consideração os principais componentes de um BCP.

Orientador: Prof. Robson Calvetti

São Paulo
2025

SUMÁRIO

1 INTRODUÇÃO 3
2 RECURSOS CRÍTICOS IDENTIFICADOS 5
3 ANÁLISE DE IMPACTO NOS NEGÓCIOS (BIA) 6
4 RECURSOS CRÍTICOS IDENTIFICADOS 7
5 PLANO DE AÇÃO DETALHADO 8
6 RECURSOS CRÍTICOS IDENTIFICADOS 9
7 REFERÊNCIAS 10

1 INTRODUÇÃO

A Controtec é uma empresa de comércio eletrônico que atua nos segmentos varejista e atacadista de produtos eletrônicos, com sede no centro de São Paulo. Com foco em inovação e qualidade no atendimento ao cliente, a empresa reconhece que sua operação está fortemente apoiada em tecnologias da informação e conectividade digital.

Diante de possíveis ameaças que possam comprometer sua atividade — como falhas técnicas, desastres naturais ou ataques cibernéticos — torna-se essencial contar com um **Plano de Continuidade de Negócios (BCP)**. Este plano tem como objetivo garantir que, mesmo em situações críticas, a Controtec consiga manter suas operações, proteger seus ativos e restabelecer a normalidade no menor tempo possível.

2 RECURSOS CRÍTICOS IDENTIFICADOS

Para a Controtec, alguns recursos são absolutamente essenciais para o funcionamento contínuo da empresa. São eles:

- **Sistema de Gestão ERP:** responsável por controlar estoque, pedidos, faturamento e integração com setores como financeiro e logística.
- **Plataforma de E-commerce:** principal canal de vendas online da empresa. Sua indisponibilidade significa prejuízo direto.
- **Servidores de Dados (locais e em nuvem):** armazenam informações estratégicas e operacionais da empresa.
- **Sistema de Pagamentos Online:** permite a finalização de compras via cartão, PIX ou boleto.
- **Conectividade com a Internet:** fundamental para operação interna, atendimento online e vendas.
- **Equipe de TI e Suporte Técnico:** responsáveis por manter os sistemas operacionais e solucionar falhas.
- **Infraestrutura de Rede (firewall, roteadores, switches):** possibilita a comunicação segura e estável entre os sistemas e dispositivos.
- **Base de Dados de Clientes:** contém dados pessoais e históricos de compra, sendo protegida pela LGPD.
- **Sistema de Backup Automático:** garante a segurança e integridade dos dados críticos.
- **VPN com Autenticação Multifator (MFA):** permite acesso remoto seguro aos sistemas internos da empresa.

3 ANÁLISE DE IMPACTO NOS NEGÓCIOS (BIA)

Evento Disruptivo	Impacto no Negócio	Consequências Possíveis
Falha nos Servidores	Interrupção total da operação do e-commerce	Perda de vendas, insatisfação de clientes
Ataque Cibernético (ransomware)	Vazamento de dados, sequestro de informações	Danos à reputação, multas por violação da LGPD
Queda de Energia Prolongada	Parada física dos sistem s internos	Impossibilidade de operação em loja física
Inundação/Incêndio	Danos físicos à infraestrutura de TI	Perda de equipamentos, indisponibilidade dos serviços
Falha de Conectividade	Impossibilidade de operar remotamente ou atender clientes	Interrupção do atendimento e vendas online

4 RECURSOS CRÍTICOS IDENTIFICADOS

A Controtec adota uma combinação de medidas preventivas, corretivas e operacionais para manter a continuidade do negócio em situações adversas. As principais estratégias são:

- **Redundância de Servidores:** além dos servidores locais, a empresa mantém cópias em nuvem para garantir continuidade imediata em caso de falhas físicas.
- **Backups Diários com Criptografia:** todos os dados críticos são armazenados com segurança tanto localmente quanto na nuvem.
- **Plano de Comunicação de Crise:** define os canais de comunicação internos e externos em emergências (WhatsApp, e-mail, comunicados no site).
- **Acesso remoto seguro via VPN com MFA:** permite que colaboradores continuem operando remotamente com segurança.
- **Estoque de Equipamentos e Contratos de Substituição Rápida:** previne longas paralisações por falhas em dispositivos.
- **Contrato com fornecedor de energia de emergência:** uso de nobreaks e gerador para manter sistemas essenciais funcionando.
- **Equipe de Resposta a Incidentes (ERI):** treinada para conter, investigar e recuperar rapidamente em caso de falhas, ataques ou acidentes.

5 PLANO DE AÇÃO DETALHADO

Etapa	Responsável	Prazo	Ações
Acionamento do BCP	Diretor de TI	Imediato após o incidente	Comunicação à equipe e início dos procedimentos
Avaliação do Impacto	ERI	1 hora	Levantamento de sistemas afetados
Ativação de servidores em nuvem	Administrador de Redes	2 horas	Restauração de backups
Comunicação com clientes	Gerente de Comunicação	2 a 4 horas	E-mails e notas públicas explicando a situação
Reestabelecimento das operações	Equipe Técnica de TI	Até 24 horas	Testes e retorno gradual dos serviços
Análise pós-incidente	Segurança da Informação	Após normalização	Relatório com lições aprendidas e prevenção futura

6 RECURSOS CRÍTICOS IDENTIFICADOS

Um plano só é útil se funcionar **na prática**. Por isso, a Controtec estabelece um cronograma de testes para validar a eficácia do BCP:

- **Simulação de Crises:** realização periódica de cenários fictícios como pane em servidores, ataque hacker ou queda de energia, com atuação da equipe como se fosse real.
- **Teste de Restauração de Backup:** executado trimestralmente, garante que os dados podem ser recuperados com segurança e rapidez.
- **Exercícios de Mesa (Tabletop):** reuniões estratégicas com líderes das áreas para discutir ações em diferentes tipos de incidentes.
- **Avaliação de Tempo de Resposta (RTO/RPO):** após cada teste, avalia-se se o tempo de recuperação e a perda de dados estão dentro do aceitável.
- **Atualização do BCP:** com base nos testes, o plano é ajustado e melhorado continuamente.

7 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2022 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.** Rio de Janeiro: ABNT, 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/L13709.htm. Acesso em: 30 abr. 2025.

SANS INSTITUTE. **Security Policy Templates.** Disponível em: https://www.sans.org/information-security-policy/. Acesso em: 30 abr. 2025.

OFFICE OF CIVIL AND DEFENSE MOBILIZATION (U.S.). **Business Continuity Planning.** U.S. Government Printing Office, 2020. Disponível em: https://www.ready.gov/business. Acesso em: 30 abr. 2025.

COLES, Steve. **Business Continuity Management: Building an Effective Incident Management Plan.** 2. ed. London: IT Governance Publishing, 2021.