Política de Gestão de Continuidade de Negócios

São Paulo: Av. Paulista 1.439, 1º | Bela Vista | CEP 01.311-926 | SP | Brasil | 55 (11) 4280-9247
Rio de Janeiro: Av. Rio Branco 81, 6º | Centro | CEP 20.040-914 |RJ | Brasil | 55 (21) 3544-3946
Brasília: Setor Comercial Sul, Q.9, bl C | Asa Sul | CEP: 70308-200 | DF | Brasil | 55 (61) 3995-0429
www.swotglobal.com

Documento	Política
Classificação	Publica/Externa
Elaboração	TI – Israel da Silva Leite Junior
Aprovação	INTERV – Interventor
Vigência	Indeterminada, a partir da data de aprovação.
Revisado em	
Versão	1.0

São Paulo: Av. Paulista 1.439, 1° | Bela Vista | CEP 01.311-926 | SP | Brasil | 55 (11) 4280-9247
Rio de Janeiro: Av. Rio Branco 81, 6° | Centro | CEP 20.040-914 |RJ | Brasil | 55 (21) 3544-3946
Brasília: Setor Comercial Sul, Q.9, bl C | Asa Sul | CEP: 70308-200 | DF | Brasil | 55 (61) 3995-0429
www.swotglobal.com

1. Introdução

Esta política define as diretrizes e os procedimentos que garantem a continuidade das operações críticas da SWOTGLOBAL em eventos de interrupções graves, utilizando principalmente os serviços Microsoft Office 365. A política cobre a identificação de riscos, a criação de planos de continuidade, a recuperação de desastres e o monitoramento contínuo das operações.

2. Objetivo

O objetivo desta política é minimizar os impactos de interrupções não planejadas nos processos de negócios, assegurar a proteção dos dados e garantir que os serviços essenciais, especialmente aqueles que dependem do Microsoft Office 365, sejam restaurados rapidamente e de forma eficiente.

3. Escopo

Esta política é aplicável a todos os departamentos, colaboradores, prestadores de serviços e parceiros de negócios que utilizam ou administram os serviços da empresa, particularmente os serviços relacionados ao Microsoft Office 365, incluindo Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams e outras ferramentas da suíte.

4. Princípios de Continuidade de Negócios

4.1 Análise de Impacto no Negócio (BIA)

Objetivo: Identificar funções e processos críticos, determinar os impactos financeiros e operacionais de sua interrupção, e estabelecer prioridades de recuperação.

Processo:

- **Identificação dos Processos Críticos:** Listar todos os processos de negócios que dependem do Office 365, como comunicação via Exchange Online, colaboração via Teams e gerenciamento de documentos no SharePoint.
- **Avaliação do Impacto:** Determinar o impacto financeiro, operacional, legal e de reputação caso esses processos sejam interrompidos. Por exemplo, a perda de acesso ao Exchange Online pode resultar em falhas na comunicação, afetando as operações diárias.
- **Definição de RTO e RPO:** Estabelecer o Tempo Máximo de Recuperação (RTO) e o Ponto de Recuperação de Dados (RPO) para cada processo. Por exemplo, o RTO para
-

São Paulo: Av. Paulista 1.439, 1º | Bela Vista | CEP 01.311-926 | SP | Brasil | 55 (11) 4280-9247
Rio de Janeiro: Av. Rio Branco 81, 6º | Centro | CEP 20.040-914 | RJ | Brasil | 55 (21) 3544-3946
Brasília: Setor Comercial Sul, Q.9, bl C | Asa Sul | CEP: 70308-200 | DF | Brasil | 55 (61) 3995-0429
www.swotglobal.com

restaurar o Exchange Online pode ser de 4 horas, enquanto o RPO pode ser de 1 hora, garantindo que não haja perda significativa de dados.

4.2 Plano de Continuidade Operacional

Objetivo: Garantir que os processos críticos possam continuar ou ser rapidamente restaurados após uma interrupção.

Estratégias:

- **Replicação de Dados e Failover:** Configurar a replicação contínua de dados para data centers secundários ou em nuvem. O Office 365 já fornece replicação geográfica automática, mas deve-se garantir que os dados críticos estejam sempre disponíveis e que o failover seja automático e transparente para os usuários.
- **Políticas de Backup e Restauração:** Definir e implementar políticas de backup para dados armazenados no OneDrive e SharePoint, garantindo que os backups sejam realizados de forma regular e que as restaurações possam ser feitas sem perda significativa de dados.
- **Acesso Offline e Redundância:** Utilizar recursos como o sincronismo offline do OneDrive para garantir que documentos essenciais estejam acessíveis mesmo durante uma falha de rede. Em paralelo, configurar redundância para ferramentas de comunicação, como permitir o uso de aplicativos móveis para continuar o acesso ao Teams durante interrupções de desktop.

4.3 Plano de Recuperação de Desastres (DRP)

Objetivo: Fornecer uma resposta estruturada a eventos catastróficos para restaurar rapidamente os serviços críticos.

Componentes:

- **Ativação de Suporte Emergencial:** Estabelecer procedimentos para ativar o suporte emergencial da Microsoft em caso de interrupções graves nos serviços do Office 365. Isso inclui ter em mãos contatos diretos com os representantes de suporte da Microsoft e os procedimentos de escalonamento de incidentes.
- **Monitoramento e Comunicação:** Utilizar o Microsoft 365 Service Health para monitorar o status dos serviços em tempo real e reportar rapidamente quaisquer interrupções aos stakeholders. Além disso, configurar canais de comunicação alternativos, como grupos de WhatsApp ou sistemas de SMS, para manter todos informados.
-

São Paulo: Av. Paulista 1.439, 1° | Bela Vista | CEP 01.311-926 | SP | Brasil | 55 (11) 4280-9247
Rio de Janeiro: Av. Rio Branco 81, 6° | Centro | CEP 20.040-914 |RJ | Brasil | 55 (21) 3544-3946
Brasília: Setor Comercial Sul, Q.9, bl C | Asa Sul | CEP: 70308-200 | DF | Brasil | 55 (61) 3995-0429
www.swotglobal.com

- **Testes Regulares de DRP:** Realizar simulações de desastres para testar a eficácia do plano. Estes testes devem incluir falhas nos principais serviços do Office 365 e verificar se o plano de recuperação pode ser executado conforme o esperado.

4.4 Avaliação de Riscos

Objetivo: Identificar e avaliar continuamente os riscos que possam afetar a continuidade dos serviços.

Abordagem:

- **Identificação de Ameaças:** Mapear possíveis ameaças, como ataques cibernéticos que comprometam a segurança do Office 365, falhas de infraestrutura local que possam impactar o acesso à nuvem, e mudanças regulatórias que exijam novas medidas de conformidade.
- **Análise de Vulnerabilidades:** Realizar auditorias regulares no ambiente do Office 365 para identificar e corrigir vulnerabilidades. Utilizar o Secure Score da Microsoft para obter uma visão detalhada das configurações de segurança e conformidade.
- **Gerenciamento de Terceiros:** Avaliar o risco de fornecedores que têm acesso aos dados processados pelo Office 365, garantindo que eles adotem as mesmas práticas de segurança e continuidade.

4.5 Testes e Validações

Objetivo: Garantir que os planos de continuidade e recuperação sejam funcionais e eficazes.

Práticas:

- **Simulações de Falhas:** Realizar testes periódicos de falhas nos principais serviços do Office 365, como simular uma queda no Exchange Online ou uma indisponibilidade no SharePoint, para testar a resposta da equipe e a funcionalidade dos planos.
- **Testes de Backup:** Verificar regularmente a integridade dos backups e realizar restaurações simuladas para garantir que os dados possam ser recuperados dentro dos tempos estabelecidos.
- **Revisão Pós-Testes:** Analisar os resultados dos testes e revisões para identificar áreas de melhoria e atualizar os planos conforme necessário.

4.6 Monitoramento e Revisão

Objetivo: Manter a política atualizada e garantir a eficácia contínua dos planos de continuidade.

São Paulo: Av. Paulista 1.439, 1° | Bela Vista | CEP 01.311-926 | SP | Brasil | 55 (11) 4280-9247
Rio de Janeiro: Av. Rio Branco 81, 6° | Centro | CEP 20.040-914 |RJ | Brasil | 55 (21) 3544-3946
Brasília: Setor Comercial Sul, Q.9, bl C | Asa Sul | CEP: 70308-200 | DF | Brasil | 55 (61) 3995-0429
www.swotglobal.com

Processo:

- **Revisão Contínua dos SLAs:** Analisar regularmente os acordos de nível de serviço (SLAs) com a Microsoft para garantir que estejam alinhados com as necessidades de continuidade da empresa.
- **Monitoramento de Uso e Ameaças:** Utilizar ferramentas como o Microsoft Cloud App Security para monitorar o uso dos serviços do Office 365 e identificar possíveis ameaças ou anomalias que possam indicar um risco à continuidade.

- **Atualizações Regulares:** Revisar e atualizar os planos de continuidade e recuperação com base em mudanças no ambiente de TI, resultados de auditorias, ou após a ocorrência de incidentes significativos.

5. Papéis e Responsabilidades

Gestor de TI:

- Implementar e manter os planos de continuidade relacionados ao Office 365.
- Garantir a conformidade com os processos de backup, recuperação e monitoramento.

Equipes de Suporte:

- Executar procedimentos de recuperação e continuidade.
- Participar de testes e simulações de falhas.

Colaboradores:

- Seguir as diretrizes estabelecidas e participar de treinamentos e testes conforme necessário.

Fornecedores:

- Garantir que os serviços prestados estejam em conformidade com os requisitos de continuidade da empresa.

6. Comunicação e Treinamento

Comunicação:

São Paulo: Av. Paulista 1.439, 1° | Bela Vista | CEP 01.311-926 | SP | Brasil | 55 (11) 4280-9247
Rio de Janeiro: Av. Rio Branco 81, 6° | Centro | CEP 20.040-914 | RJ | Brasil | 55 (21) 3544-3946
Brasília: Setor Comercial Sul, Q.9, bl C | Asa Sul | CEP: 70308-200 | DF | Brasil | 55 (61) 3995-0429
www.swotglobal.com

- Estabelecer canais claros para comunicação durante interrupções, incluindo uso de sistemas alternativos de notificação.

Treinamento:

- Realizar treinamentos regulares para garantir que todos estejam preparados para responder a incidentes que afetem a continuidade dos negócios.

7. Conformidade e Revisão

Revisão Anual:

- Esta política será revisada anualmente ou após qualquer evento significativo que possa impactar a continuidade dos negócios.

Auditorias Regulares:

- Conformidade com esta política será auditada regularmente para garantir que todos os aspectos estejam sendo seguidos conforme estabelecido.

São Paulo: Av. Paulista 1.439, 1º | Bela Vista | CEP 01.311-926 | SP | Brasil | 55 (11) 4280-9247
Rio de Janeiro: Av. Rio Branco 81, 6º | Centro | CEP 20.040-914 | RJ | Brasil | 55 (21) 3544-3946
Brasília: Setor Comercial Sul, Q.9, bl C | Asa Sul | CEP: 70308-200 | DF | Brasil | 55 (61) 3995-0429
www.swotglobal.com