Plano de Continuidade de Negócios

Plano de Continuidade de Negócios

Tipo: Plano	PLNO-0001	**Nº Revisão**: 3.9
Aprovação: CGSI	**Elaboração**: Segurança da Informação	**Classificação**: Pública

Sumário

- 1. Introdução
- 2. Plano de Continuidade de Negócio
  - 2.1 Continuidade da Equipe de Operação e de Segurança da Informação
  - 2.2 Continuidade Técnica - Alta disponibilidade da Infraestrutura
  - 2.3 Disaster Recovery
  - 2.4 Continuidade da Gestão da Segurança da Informação

1. Introdução

A Plusoft utiliza serviços de computação em nuvem com arquitetura projetada para alta disponibilidade, incluindo mecanismos de redundância, continuidade operacional e recuperação de serviços, de forma a reduzir riscos de indisponibilidade e apoiar a continuidade dos negócios.

As aplicações e serviços abrangidos pelo escopo do SGSI são estruturados para operar com níveis adequados de disponibilidade e resiliência, observando os requisitos de Segurança da Informação, proteção de dados e continuidade dos serviços.

Apesar das medidas preventivas adotadas, eventos que afetem a continuidade das operações podem ocorrer. Por essa razão, a Plusoft mantém estratégias, processos e planos destinados à continuidade dos negócios, à recuperação dos serviços e à redução dos impactos decorrentes de situações de indisponibilidade ou desastre.

Este Plano foi elaborado com base em práticas reconhecidas de continuidade de negócios e recuperação de serviços, apoiando a resiliência operacional da organização e a manutenção dos serviços prestados aos seus clientes.

2. Plano de Continuidade de Negócio

O Plano de Continuidade de Negócio da Plusoft estabelece as medidas necessárias para reduzir os impactos de interrupções operacionais, técnicas ou ambientais que possam afetar a continuidade dos serviços e das atividades da organização.

O plano contempla as ações a serem executadas antes, durante e após situações que possam comprometer a continuidade dos negócios, definindo estratégias de resposta, recuperação e restabelecimento dos serviços.

A efetividade do plano é verificada por meio de exercícios, testes periódicos, análise de resultados, ações corretivas e lições aprendidas, contribuindo para a melhoria contínua da capacidade de continuidade de negócio da organização.

2.1 Continuidade da Equipe de Operação e de Segurança da Informação

As equipes de Operação e de Segurança da Informação possuem condições de executar suas atividades de forma remota quando necessário, utilizando os recursos, ferramentas e controles previstos pela organização para garantir a continuidade das operações.

A Plusoft adota modelo de trabalho que permite a continuidade das atividades operacionais e de Segurança da Informação em situações que impeçam a utilização dos ambientes físicos habituais de trabalho.

Em caso de indisponibilidade da Governança no papel de Security Officer, suas atividades deverão ser assumidas pelo Diretor de Segurança da Informação (Diretor de SI), com apoio da Infraestrutura no papel de Segurança, até o restabelecimento das condições normais de operação.

2.2 Continuidade Técnica - Alta disponibilidade da Infraestrutura

A Plusoft utiliza ambientes com múltiplas zonas de disponibilidade, de forma a reduzir os riscos de indisponibilidade dos serviços e permitir a continuidade da operação em caso de falha de um dos ambientes utilizados.

Os mecanismos de redundância e continuidade são projetados para possibilitar a recuperação dos serviços em tempo compatível com as necessidades do negócio e com os requisitos definidos pela organização.

Testes dos processos de alta disponibilidade são realizados e evidenciados trimestralmente, com o objetivo de verificar a eficácia dos mecanismos de continuidade e recuperação implementados.

2.3 Disaster Recovery

Em situações de desastre que afetem simultaneamente as zonas principal e secundária utilizadas pela organização, deverá ser acionado o ambiente de Disaster Recovery (DR), observando as etapas descritas a seguir.

Declaração de Desastre

1. A declaração de desastre é realizada pelo **Diretor de Segurança da Informação (Diretor de SI)**, com apoio da Área de Segurança da Informação e da Infraestrutura, considerando os impactos ao negócio, aos serviços e aos ativos abrangidos pelo escopo do SGSI.
2. É realizada comunicação interna para preparação das equipes envolvidas
3. É realizada comunicação externa aos clientes afetados, conforme os planos de comunicação aplicáveis.
4. É iniciado o processo de execução do plano de Disaster Recovery (DR).
5. Durante a execução do plano, as comunicações internas e externas devem ser atualizadas de acordo com a evolução das atividades.
6. Ao final da recuperação, os ambientes são validados e disponibilizados para operação.
7. É realizada comunicação informando o restabelecimento dos ambientes e serviços.

Plano de retorno

1. É realizada comunicação interna e externa com as diretrizes do plano de retorno ao ambiente principal.
2. É iniciado o processo de retorno do ambiente contingenciado para o ambiente principal.
3. Durante a execução do retorno, as comunicações internas e externas devem ser atualizadas de acordo com a evolução das atividades.
4. Ao final do processo, os ambientes são validados.
5. Os ambientes são disponibilizados para operação normal.
6. É realizada comunicação informando o restabelecimento das condições operacionais originais.

Encerramento

Após a conclusão do processo de recuperação e retorno operacional, deverão ser realizadas as seguintes atividades:

- Registro das ações corretivas relacionadas ao Plano de Continuidade de Negócio (PCN);
- Registro das lições aprendidas identificadas durante a execução do processo;
- Elaboração da análise de causa raiz (RCA), quando aplicável;
- Avaliação da necessidade de atualização dos planos, procedimentos e controles relacionados à continuidade de negócio.

Os testes do processo de Disaster Recovery devem ser realizados e evidenciados, no mínimo, uma vez por ano, com o objetivo de validar sua eficácia e garantir sua aderência aos requisitos da organização.

2.4 Continuidade da Gestão da Segurança da Informação

Em caso de indisponibilidade dos documentos, processos ou repositórios utilizados pela Área de Segurança da Informação, os colaboradores deverão utilizar o canal oficial da área (**si@plusoft.com**) para solicitar orientações relacionadas aos processos, documentos ou atividades de Segurança da Informação.

A Área de Segurança da Informação deverá fornecer as orientações necessárias ou disponibilizar os documentos aplicáveis para apoiar a continuidade das atividades até o restabelecimento dos sistemas e processos afetados.

Após o restabelecimento dos sistemas e processos, a Área de Segurança da Informação deverá registrar as solicitações e orientações fornecidas nos registros corporativos apropriados, mantendo a rastreabilidade das atividades executadas durante o período de contingência.

Última atualização: 02/10/2026