

Plano de Continuidade de Negócios



Plano de Continuidade de Negócios



Tipo: Plano

PLNO-0001

Nº Revisão: 3.4

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 trabalha em ambientes de nuvem públicas com padrões globais que possui sistema autossustentado, com equipamentos de refrigeração e alimentação de energia redundantes, ou seja, um equipamento backup em cada segmento permanece ligado, permitindo assim que manutenções planejadas possam ser feitas sem desligamento do Data Center, possuindo assim Alta Disponibilidade.

As nossas aplicações são construídas de forma a garantir alta disponibilidade, utilizando múltiplas zonas de disponibilidade das nuvens, respeitando as normas de Segurança e Privacidade de Dados.

Apesar de todos esses cuidados, desastres podem acontecer, e a Plusoft mantém uma estratégia robusta de continuidade de negócios para os serviços e plataformas de produção. Este plano foi desenvolvido a partir de metodologias aceitas pelo setor e engloba princípios de engenharia de alta disponibilidade.

2. Plano de Continuidade de Negócio

O plano de continuidade da Plusoft descreve medidas para evitar e reduzir interrupções ambientais e técnicas. Ele inclui detalhes operacionais sobre as etapas a serem seguidas antes, durante e depois de um evento. O plano de continuidade é constantemente medido contra rigorosos requisitos regulatórios e de governança, com testes evidenciados, ações corretivas e lições aprendidas, garantindo assim o aprimoramento contínuo.

2.1 Continuidade da Equipe de Operação e de Segurança da Informação

Tanto nossa Equipe de Operação quanto a de Segurança da informação, têm total condição de atender o cliente de forma remota, caso necessário.

A Plusoft já possibilita o home-office com todas as garantias de segurança e as ferramentas adequadas para a realização das atividades de cada departamento.

Caso ocorra alguma indisponibilidade do Security officer, o Diretor da área de Segurança juntamente com o Gestor da área de Infraestrutura serão os responsáveis pelas tarefas por ele exercidas até que a indisponibilidade seja resolvida.

2.2 Continuidade Técnica - Alta disponibilidade da Infraestrutura

Trabalhamos com mais de uma Zona de disponibilidade para garantir que caso alguma delas sofra alguma interrupção, a outra passe a operar o mais rapidamente possível.

Testes desse processo são realizados e evidenciados a cada 3 meses para garantir que tudo está funcionando conforme o esperado.

2.3 Disaster Recovery

Em situações de Desastre, onde nossas Zonas Principais e Secundárias são afetadas, toda nossa Infraestrutura é direcionada para nosso ambiente de DR, seguindo os passos:

1. A Declaração do desastre é feita através do comitê de continuidade de negócio
 - a. É feita uma comunicação interna do Desastre para preparação das equipes.
 - b. É feita a comunicação externa para os clientes afetados.
 - c. Inicia-se o processo de execução do DR onde a cada finalização de etapa é feita uma atualização da comunicação interna e externa.
 - d. Ao final do processo é feita a validação dos ambientes.

- e. Os ambientes são disponibilizados
 - f. As comunicações são feitas para informar que os ambientes estão recuperados.
2. Plano de retorno
- a. É feita uma comunicação interna e externa com o Plano de retorno.
 - b. Inicia-se o processo de retorno onde a cada finalização de etapa é feita uma atualização da comunicação interna e externa.
 - c. Ao final do processo é feita a validação dos ambientes.
 - d. Os ambientes são disponibilizados
 - e. As comunicações são feitas para informar que os ambientes estão funcionando adequadamente nas condições originais.
3. Ações corretivas do PCN.
4. Lições aprendidas durante a realização do processo de PCN,
5. Elaboração e disponibilização do RCA (Análise de causa raiz).

Testes desse processo são realizados e evidenciados uma vez ao ano para garantir que tudo está funcionando conforme o esperado.

2.4 Continuidade da Gestão da Segurança da Informação

Em caso de indisponibilidade dos documentos e processos sob a Gestão da Segurança da Informação disponibilizados na intranet da Plusoft:

1. Os colaboradores devem enviar email para a área de SI (si@plusoft.com) com as dúvidas sobre o processo ou documento para nortear suas ações nos pontos relacionados a Segurança.
2. A área de SI irá retornar o email com a orientação ou com o documento que deve ser seguido.
3. Após restabelecimento do sistemas e processos, a área de SI irá documentar a demanda recebida via email no gerenciador de tarefas para registro.

Última atualização: 29/09/2023