POLÍTICA DE PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Versão Atualizada: 3.0.0 – Julho/2026

PLANO DE PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Objetivo

Definir as bases, princípios e regras para contingências e continuidade de negócios da IAAS CONSULTORIA E SERVICOS LTDA ("IAAS");

A quem se aplica?

Sócios, diretores, funcionários, prestadores de serviço, terceirizados, consultores e demais pessoas físicas ou jurídicas contratadas ou outras entidades, que participem, de forma direta, das atividades diárias e negócios, representando a IAAS (doravante, "Colaboradores").

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos neste Plano de Contingência e Continuidade de Negócios ("PCN"), informando imediatamente qualquer irregularidade ao Diretor de *Compliance* e PLD.

Revisão e Atualização e Testes

Este PCN deverá ser revisado e atualizado a cada 2 (dois) anos, ou em prazo inferior, caso necessário em virtude de mudanças legais/regulatórias/autorregulatórias.

Responsabilidades

Caberá ao Diretor de *Compliance* e PLD a avaliação das ocorrências, registro de ocorrências e tomadas de decisão.

Contexto Operacional e de Negócios

Esta política foi elaborada considerando as seguintes premissas e particularidades do modelo operacional e de negócio da IAAS:

- ✓ A IAAS utiliza sistemas proprietários e de terceiros para executar os serviços contratados pelos seus clientes;
- ✓ Os fornecedores dos sistemas terceirizados utilizados pela IAAS se comprometem com disponibilidade, segurança e planos de contingência compatíveis com as necessidades da IAAS;
- ✓ Os Colaboradores da IAAS estabelecem tratativas e formalizam seus entendimentos com clientes por meio de ferramentas e aplicativos de mensagens e/ou e-mail corporativo;
- ✓ Os arquivos contendo informações pessoais e financeiras dos clientes da IAAS são armazenados em nuvem, com *backups* periódicos diários;
- ✓ Os dispositivos eletrônicos (*laptops, smartphones, tablets*) utilizados no exercício das atividades da IAAS possuem senha de acesso e criptografia;
- ✓ A infraestrutura, atividades e sistemas da IAAS são configurados para permitir execução remota.

Princípios e Obrigações

O PCN é um conjunto de procedimentos que objetiva, no caso de ocorrência de incidentes, manter as atividades e sistemas considerados críticos em nível de funcionamento previamente estabelecido e/ou recuperá-los no prazo previamente estabelecido.

Para identificação dos ativos críticos[1], são considerados os riscos a seguir, no caso de interrupção do processo:

a) impacto financeiro – situações em que a descontinuidade de negócios possa atingir diretamente os clientes da IAAS, ou sua situação financeira e patrimonial;

b) impacto legal – descontinuidade de negócios passível de gerar consequências legais aos clientes ou mesmo à própria IAAS;

c) impacto de imagem – risco de a descontinuidade de negócios impactar a reputação e confiabilidade da IAAS perante seus clientes e respectivas contrapartes;

d) acidentes, casos fortuitos e força maior – risco de ocorrência de circunstâncias imprevisíveis que escapam completamente ao controle da IAAS, tais como incêndios, terremotos, desastres naturais ou comoções sociais de grandes proporções, que determinem a descontinuidade de suas atividades e/ou a sua continuidade em local diverso da sua sede atual.

As posições, áreas e sistemas considerados críticos constam do Anexo I a este PCN.

Classificação de Riscos e Providências

A IAAS adota a seguinte classificação de riscos, com as respectivas providências a serem tomadas:

Nível 1: baixa probabilidade de ocorrência e/ou de impacto nas atividades da IAAS, com monitoramento cotidiano para a sua prevenção;

Nível 2: riscos demandantes de atenção constante, com impacto potencial médio nas atividades da IAAS e necessidade de maior nível de controles preventivos;

Nível 3: riscos que devem ser incondicionalmente evitados, com impacto relevante nas atividades da IAAS, com adoção de rigorosos controles preventivos.

São exemplos de riscos de nível 3 as situações de indisponibilidade e inacessibilidade total[2] de pessoas a seus meios. Nestes casos, medidas preventivas incluem a definição de substitutos para as posições chave devidamente treinados, habilitados e capacitados para atuar no desempenho das funções requeridas.

Também são classificados desta forma (nível 3), a título de exemplo, falhas de segurança/manutenção/atualização dos *softwares* e serviços críticos utilizados pela IAAS na execução dos serviços contratados e nas ferramentas disponibilizadas diretamente a seus clientes;

Controles Preventivos da IAAS

- ✓ Identificação, treinamento e capacitação profissional de substitutos para exercer as atividades chave da operação da IAAS;

[1] Todo e qualquer sistema, equipamento, arquivo etc., em suma, todo ativo essencial para o mínimo funcionamento da IAAS, atendendo a suas obrigações legais críticas.

[2] Entendendo-se como inacessibilidade e indisponibilidade de um profissional, a situação em que este está totalmente impedido de acessar as ferramentas e informações necessárias para os exercícios de suas atividades. O acesso eletrônico/virtual é o ativo relevante para a adequada disponibilidade do profissional, independente se nas dependências físicas da IAAS.

- ✓ Manutenção de manuais de procedimentos para utilização dos Colaboradores em caso de necessidade;
- ✓ Manutenção de provedores para acesso a arquivos eletrônicos, planilhas e demais documentos de forma segura e transparente ao usuário, bem como dos respectivos back-ups desses materiais;
- ✓ Manutenção de sistema antivírus nas máquinas dos usuários para salvaguardar os arquivos eletrônicos utilizados pela IAAS;
- ✓ Servidores/provedores de serviços tecnológicos, de dados, ferramentas contratadas etc. – controles e redundâncias dos serviços de servidores e prestadores de serviço em ambiente em nuvem, com as devidas proteções antivírus, *firewall*, *backup* etc.

O *backup* é armazenado diariamente em ambiente em nuvem. O serviço de *e-mail* e servidores também são armazenados em nuvem e as interfaces operacionais são acessadas de qualquer lugar via internet.

Os procedimentos definidos a seguir compõem este PCN:

Procedimentos	Periodicidade
Identificar as pessoas críticas para a operação da IAAS e suas respectivas atividades e garantir que estejam capacitadas para exercer tais atividades	Sempre que necessário, no caso de novas atividades e pessoas, no mínimo anualmente.
Identificar e reavaliar os sistemas críticos, e atualizar o Anexo I, bem como os telefones do plano de comunicação.	Sempre que necessário, no caso de novas atividades, pessoas e sistemas, no mínimo anualmente.
Decidir pelo início da contingência. A comunicação deve ser efetuada conforme o Anexo II.	Na efetiva ocorrência de incidentes.
Acionar o plano de contingência.	Na aprovação do início da contingência.
Informação à equipe.	Após decisão pelo início da contingência na estrutura alternativa.
Após a contingência, verificar o que motivou o incidente/crise, e se o motivo é passível de ações de aprimoramentos, bem como aprimoramento do PCN.	Após contingência.
Realizar testes do Plano.	Anualmente.

Testes de Continuidade dos Negócios

O Plano de Continuidade de Negócios será objeto de validação e testes a cada 12 (doze) meses.

Os sistemas de informações da IAAS, em especial aqueles mantidos em meio eletrônico, serão submetidos a testes periódicos de segurança, de forma a assegurar a existência e efetividade dos controles de segurança aplicáveis.

ANEXO I - Atividades e Sistemas Críticos

Quadro mínimo de profissionais com acesso aos sistemas, redes etc. em situação de contingência
1 de Tecnologia
1 de Operações

Sistemas críticos com acesso em situação de contingência
Plataforma IAAS!
Sistema de Cadastro, PLD e Suitability (Goliza)
Pacote Office e demais ferramentas de apoio
E-mail
Dados e arquivos da IAAS! (Microsoft 365)

Em ocorrendo situações de problemas de acesso às suas dependências, a equipe da IAAS deve continuar a desempenhar suas atividades através de Home Office, uma vez que todos os arquivos e e-mails podem ser acessados pela nuvem pelos colaboradores da IAAS. Assim, é possível permanecer trabalhando ainda que fora do escritório da IAAS.

Os sistemas utilizados pela IAAS são acessados do website da plataforma IAAS e site dos provedores, o que viabiliza acessá-los de qualquer local desde que se disponha de um computador com um link de internet.

A comunicação com clientes, parceiros e administradores poderá continuar sendo realizada através da utilização de telefones celulares da equipe da IAAS. Para tanto, há procedimento de comunicar a esses terceiros o estado de contingência da IAAS, de forma a que estes também tenham conhecimento da situação tão logo ela ocorra, buscando impactar o mínimo possível a operação dos clientes.

ANEXO II - Pessoas Autorizadas a Iniciar Plano de Contingência e Continuidade de Negócios na Estrutura Alternativa

- Sócios da IAAS Consultoria e Serviços;
- Gerente de Operações;
- Gerente de Tecnologia.

Quaisquer das pessoas acima está autorizada a ativar o PCN de forma a sempre possibilitar a preservação ininterrupta das atividades da IAAS.

ANEXO III - Plano de Comunicação
Modelo – "Call Tree"

A IAAS utiliza primordialmente o acesso remoto (via celular ou computadores pessoais) e listas em aplicativos de mensagens via telefone celular (*Whatsapp*) como forma de comunicação de contingência, visando principalmente à efetividade e agilidade proporcionada por tais ferramentas em contextos dessa natureza.

A comunicação é iniciada pelos indivíduos mencionados no Anexo II, e enviada a todos os membros das respectivas equipes, os quais participam dos grupos pertinentes, de maneira a assegurar a pronta e eficiente comunicação da contingência em questão, em tempo hábil e oportuno.