POLÍTICA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS CREDI NESTLÉ

SUMÁRIO

1. OBJETIVO

Este documento tem por objetivo estabelecer rotinas e procedimentos para assegurar a não interrupção das atividades do negócio, proteger os processos críticos contra efeitos de falhas ou desastres significativos, considerando sua retomada em tempo hábil e em conformidade com diretrizes de segurança da informação da Credi Nestlé

2. ABRANGÊNCIA

Este é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir de sua publicação, aos colaboradores, parceiros e fornecedores da Credi Nestlé.

3. DEFINIÇÕES

Colaborador: Empregado, estagiário, prestador de serviço, terceirizado, fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venham a ter relacionamento profissional, direta ou indiretamente com a organização.

Continuidade de Negócios: compreende a capacidade da organização para manter a entrega de produtos e serviços a níveis aceitáveis e predefinidos, em seguida a um evento de interrupção.

Gestão de Continuidade de Negócios: processo de gestão holística com o objetivo de identificar ameaças potenciais para uma organização e antecipar ações corretivas e reativas para minimizar os impactos, caso estes se concretizem.

Incidente de Segurança da Informação: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à Política de Segurança da Informação ou Normas Complementares, falha de controles ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

Objetivo de Ponto de Recuperação: tolerância para a perda de dados de sistemas.

Tempo de Recuperação Emergencial: tempo máximo que um processo crítico pode ficar indisponível, medido a partir da detecção da falha e/ou interrupção até o restabelecimento do processo.

Tentativa de Burla: A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

Testes de Mesa: avaliação das ações descritas em Plano de Continuidade de Negócios (PCN), com objetivo de atualizar e ou validar conteúdo do PCN, tendo como base um exercício de simulação, a partir da apresentação de um cenário de falhas.

Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos.

4. PREVENÇÕES A VIOLAÇÕES DE DADOS

O processo de continuidade de negócios na Credi Nestlé deve ser definido formalmente pela Gerência Administrativa, apoiada por Unidades chave da empresa apoiadora como TI, SHE, Recursos Humanos, Jurídico entre outras que, conforme característica da ocorrências se façam necessária a participação.

O Plano de Continuidade de Negócios (PCN), bem como esta política, devem ser aprovados pela Diretoria executiva da Credi Nestlé.

O escopo dos processos de continuidade de negócio deve garantir um nível aceitável de risco e proteger os interesses das principais partes interessadas, além de ser baseado nos processos críticos do negócio que suportam:

a) o cumprimento das obrigações contratuais e legais;

b) operações e atividades críticas do negócio;

c) operações financeiras relevantes.

5. EQUIPES DE CONTINUIDADE DE NEGÓCIO

Para a gestão da continuidade do negócio da Credi Nestlé, deve ser:

a) estabelecida uma estrutura de planejamento e equipes de continuidade de negócios responsáveis pela manutenção da documentação dos processos, ativação dos planos, tomada de decisão em cenário de crise (gestão de crise);

b) definido um grupo de colaboradores para compor o time de gestão de crise (grupo de tomada de decisão) e aprovar o acionamento do plano.

6. ANÁLISE DE RISCOS

O desenvolvimento dos Planos de Continuidade de Negócios – “PCN” deve ser iniciado pela execução de Análise de Riscos para identificação das ameaças que podem interromper os processos de negócio.

Os PCNs devem ser elaborados para assegurar que as operações essenciais sejam recuperadas dentro de uma escala de tempo aceitável, limitando as consequências aos danos verificados, e garantindo que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

As áreas responsáveis pela realização de auditorias internas e externas e identificação de riscos devem detectar os processos críticos de negócio das áreas da Credi Nestlé, por meio de entrevistas com as áreas/departamentos da Credi Nestlé, e avaliá-los quanto a ocorrência e consequências de desastres, falhas de segurança, perda de serviços e disponibilidade de serviços e quais os impactos nos negócios decorrentes. Nas entrevistas também devem ser identificados:

a) RTO – Tempo de Recuperação Emergencial;

b) RPO – Objetivo de Ponto de Recuperação;

c) Pessoas chave responsáveis pela execução do processo;

d) Recursos necessários para execução do processo (registros vitais, formulários, manuais, equipamentos, dispositivos móveis dentre outros).

Sempre que for identificado um risco relacionado à Segurança da Informação e de Segurança Cibernética, devem ser seguidos os procedimentos de Gestão de Riscos de Segurança da Informação e Riscos Cibernéticos.

7. INTERRUPÇÕES DE PROCESOS POR INCIDENTES

Alguns processos críticos podem ser interrompidos devido à indisponibilidade e/ou falhas de seus processos diante de ataques externos, dentre outros. Nestes casos, a contingência

necessária para interromper o fato gerador da falha ou interrupção deve acontecer conforme descrito no PCN correspondente, incluindo a comunicação com partes externas se necessário.

8. DESENVOLVIMENTO DE PLANOS

Após a identificação dos processos considerados críticos deve-se planejar as ações necessárias de recuperação para caso de falha ou interrupções e as documentar nos PCNs.

O **Plano de Continuidade de Negócios** deve conter, no mínimo:

a) Escopo e Objetivos: Escopo do plano e objetivos;

b) Premissas: Cenários cobertos pelo plano;

c) Responsabilidades: descreve quem é responsável por cada uma das atividades, incluindo possíveis substitutos quando necessário;

d) Como e quando deve ser utilizado o plano;

e) Ciclo de Gestão de Continuidade de Negócios: Começo, meio e fim do processo de gestão de continuidade de negócio;

f) Estrutura de Continuidade de Negócios (Equipes): Indicação das Equipes responsáveis pelas atividades descritas no plano;

g) Processo de Resposta Inicial de Incidente: descreve quais as ações que devem ser executadas após a ocorrência de um incidente. Exemplos: isolamento de um servidor, parada de um serviço, dentre outros. Deve-se descrever também o responsável pelo PCN e seus substitutos. Seria uma solução imediata ou de contorno da situação indesejada;

h) Processo de Gestão de Crises: Processos e respectivas regras para tomada de decisão em cenário de crise;

i) Plano de Avaliação de Danos: descreve ações para avaliar danos decorrentes do incidente;

j) Condições de ativação do PCN: descreve os processos obrigatórios antes da ativação do plano;

k) Procedimentos de retorno a operação normal: ações necessárias durante a restauração e recuperação do processo. Exemplo: voltar base de dados, reconfigurar os acessos dos usuários, dentre outros;

l) Procedimentos de finalização: descreve as ações a serem tomadas após o restabelecimento das operações. Exemplo: comunicações, atualizações de softwares, dentre outros;

m) Procedimentos Alternativos: Procedimentos alternativos são ações manuais que podem ser empregadas para executar as atividades críticas do processo se os sistemas que apoiam estes processos de negócio não estiverem disponíveis;

n) Identificação dos prazos aceitáveis: Descreve o Tempo de Recuperação Emergencial, isto é, qual o tempo máximo que um processo crítico pode ficar indisponível, que mede desde o momento aproximado que o processo ficou indisponível até o momento em que este é restabelecido;

o) Serviços e recursos em geral: descreve os recursos em geral, além dos de Tecnologia da informação;

p) Testes e Manutenção: Plano de testes do plano. Neste caso, para cada tipo de ocorrência, os testes e manutenção serão ajustados de modo que reflitam com a máxima fidedignidade a situação;

q) Programa de Conscientização: Processo de conscientização das partes interessadas sobre o plano;

r) Aprovações e Revisão: Histórico de revisões e aprovações.

O PCN deve ser desenvolvido e mantido de modo a atender também as normas de segurança da informação e de Riscos Cibernéticos da Credi Nestlé.

O **Plano de Recuperação de Desastres** deve:

a) conter as instruções para acionamento e recuperação do ambiente operacional produtivo, assim como as equipes responsáveis por essas atividades;

b) Prever a redundância dos recursos de processamento da informação e recursos de tecnologia que suportam os processos críticos.

9. DETECÇÃO E COMUNICAÇÃO PARA ACIONAMENTO DO PLANO

A Gerência Administrativa da Credi Nestlé, com o auxílio das demais unidades da Credi Nestlé, deve implementar controles para detecção de interrupção ou falha de um processo crítico, tais como:

a) monitoramento dos sistemas (através da verificação dos logs);

b) informação de usuários;

c) sistemas automáticos de detecção (sensor de calor, sensor de fumaça, discadora automática, dentre outros);

d) monitoramento de terceiros (por exemplo, links de transmissão de dados).

Após a detecção de falhas ou interrupção de um processo crítico, o processo de acionamento do PCN pode ser iniciado, conforme descrito a seguir.

10. ACIONAMENTO DO PCN

O PCN só deve ser ativado mediante declaração de situação de crise pela Gerência Administrativa. Antes da ativação, caberá a Gerência Administrativa, justificar e propor a Diretoria executiva o acionamento do PCN.

O gerenciamento de crise, que envolve o atendimento de emergências como incêndio e outros desastres naturais, devem ser tratados observando também a normativos próprios elaborados por áreas relacionadas.

Devem ser observadas também instruções da Credi Nestlé e da empresa apoiadora (Nestlé) para a fuga e abandono quando ocorrer emergências desta natureza. Estes planos devem conter os responsáveis por verificações necessárias antes da evacuação da área.

10.1. REGISTRO DO INCIDENTE NO MONITORAMENTO DE RISCO OPERACIONAL

Após acionamento do PCN, deve ser registrada a ocorrência, conforme cada natureza, no controle de monitoramento de Risco Operacional.

O registro da ocorrência exige o estabelecimento de Plano de Ação com objetivo de mitigação de novas ocorrências e melhoria contínuo nos processos internos da cooperativa.

Semestralmente, o monitoramento do Risco Operacional é apresentado à Diretoria Executiva para acompanhamento e direcionamentos, quando for o caso.

11. RETORNO À NORMALIDADE

Após o retorno à normalidade, deve-se então avaliar quais foram os impactos causados no negócio pela interrupção/crise, avaliando impactos em cada processo crítico, ativos e equipes.

Caso seja necessário, a Diretoria Executiva deve ser convocada novamente para aprovações quanto à disponibilização de recursos financeiros ou estratégias alternativas para mitigar os danos e consequências causados a Credi Nestlé durante a crise.

Todas as atividades executadas, desde o acionamento do PCN, até o retorno à normalidade, devem ser registradas em um formulário interno de registro de informações elaborado pela Equipe de Continuidade de Negócios.

12. SIMULAÇÕES, TESTES, MANUTENÇÃO E TREINAMENTO DO PCN

O PCN deve ser testado regularmente pelas áreas responsáveis pela realização de auditorias e identificação de riscos, no mínimo, anualmente, de forma a assegurar, de forma permanente, sua atualização e efetividade, além de garantir que todos os envolvidos no PCN estejam aptos a atuar em caso de necessidades, conhecendo e sabendo executar as ações a eles atribuídas.

Os ativos e recursos críticos devem também ser testados de modo a verificar se estão aptos a desempenhar os procedimentos de emergências de recuperação e reativação.

Após a sua realização, a simulação deve ser avaliada e registrada na “Avaliação da Simulação/ Ativação de PCN”. O responsável pela execução do teste, conforme descrito no programa, é também o responsável pelo preenchimento do formulário e envio a Segurança da Informação.

Todos os colaboradores envolvidos no Sistema de Gestão de Continuidade de Negócios devem participar do processo de conscientização de continuidade de negócios.

A realização das simulações deve contemplar:

a) Testes de mesa simulando diferentes cenários;

b) Simulações de recuperação técnicas, assegurando que os sistemas possam ser efetivamente recuperados;

c) Testes de recuperação em local alternativo, executando os processos de negócio em paralelo com a recuperação das operações distantes do local principal;

d) Testes de recursos, serviços e instalações de fornecedores, assegurando que os serviços e produtos fornecidos por terceiros atendem aos requisitos contratados;

e) Simulação do PCN, onde aplicável, testando se a organização, o pessoal, os equipamentos, os recursos e os processos estão aptos para enfrentar interrupções.

13. AVALIAÇÃO E ATUALIZAÇÃO DO PCN

O PCN deve ser atualizado pela gerência Administrativa, com apoio de unidades técnicas da empresa apoiadora, quando for o caso, nas situações ocorridas abaixo:

a) Ocorrência de um incidente, com ativação do PCN;

b) Realização de testes do PCN;

c) Mudanças significativas nas atividades do negócio;

d) Mudança de pessoal ou funções, ou informações sobre estes;

e) Mudança de localização, instalação e recursos;

f) Mudança de legislação;

g) Mudança de prestadores de serviços e fornecedores;

h) Mudanças nos processos.

Adicionalmente, os riscos devem ser tratados e revisados anualmente.

14. RESPONSABILIDADES

Diretoria Executiva:

a) Aprovar o processo de continuidade de negócios;

b) Declarar situação de crise.

Gerência Administrativa:

a) Cumprir e fazer cumprir esta Norma e demais documentos complementares por todos os colaboradores da Credi Nestlé;

b) Definir o escopo de continuidade de negócios da organização alinhado com objetivos estratégicos;

c) Avaliar a relação custo x benefício das estratégias de continuidade propostas e dos planos que compõem a Gestão de Continuidade de Negócios da Credi Nestlé e decidir sobre a sua implementação;

d) Propor as diretrizes estratégicas da Gestão de Continuidade de Negócios;

e) Gerir a implementação e gestão do ciclo de continuidade de negócios;

f) Coordenar a elaboração, implantação, testes e atualização dos planos da Credi Nestlé;

g) Manter esta política atualizada e submetê-la para aprovação da Diretoria Executiva;

h) Definir e controlar a operação do processo de gestão de continuidade de negócios;

i) Atuar na divulgação, conscientização e treinamento dos envolvidos no processo de gestão de continuidade de negócios;

j) Participar do processo de desenvolvimento do Plano de Recuperação de Desastres;

k) Revisar o Plano de Recuperação de Desastres da Credi Nestlé.

Unidade de Tecnologia da Informação da Nestlé:

a) Fornecer os recursos de tecnologia necessários para estabelecer, implementar, operar e manter a gestão de continuidade de negócio e suas estratégias;

b) Executar as atividades, com apoio das áreas da Credi Nestlé, previstas nessa norma;

c) Propor melhorias nos controles de continuidade de negócios;

d) Implementar as estratégias de recuperação de desastres em conformidade com as diretrizes de continuidade de negócios da Credi Nestlé;

e) Fornecer os insumos necessários para revisão das estratégias de continuidade que envolvem ações de tecnologia.

Gestores (Gerentes e Coordenadores):

a) Garantir e gerenciar o cumprimento desta Política e demais documentos complementares pelos seus colaboradores;

b) Participar do processo de desenvolvimento dos Planos de Continuidade de Negócio de suas áreas;

c) Revisar os planos de suas áreas;

d) Realizar testes e exercícios dos planos;

e) Avaliar e aprimorar os planos a partir dos resultados dos testes e exercícios;

f) Administrar a contingência quando da interrupção de atividades, com base nos planos desenvolvidos;

g) Revisão os resultados da Análise de Impacto nos Negócios anualmente;

Colaboradores:

a) Cumprir, estar ciente e manter-se atualizado com essa Política e documentos complementares;

15. PENALIDADES

Violações: Qualquer atividade que desrespeite as disposições estabelecidas nesta política ou em quaisquer dos documentos complementares da Credi Nestlé, deve ser considerada como uma violação e tratada pela Credi Nestlé a fim de apurar as responsabilidades dos envolvidos de acordo com as “Medidas Disciplinares” da Credi Nestlé visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

Tentativa de Burla: A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

16. DISPOSIÇÕES FINAIS

Esta política deve ser revisada, no mínimo, anualmente, ou sempre que existir a necessidade de alterações nos critérios definidos nas demais normas e políticas específicas da Credi Nestlé.

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as normas e procedimentos aplicáveis pela Credi Nestlé.

Este documento bem como os demais documentos que a complementam encontram-se disponíveis no Diretório Y > Políticas Credi Nestlé, em caso de indisponibilidade, podem ser solicitadas ao Encarregado pelo Tratamento de Dados Pessoais da Credi Nestlé.

Qualquer dúvida relativa a esta Política deve ser encaminhada ao Encarregado pelo Tratamento de Dados Pessoais da Credi Nestlé por meio do e-mail protecaodedados11@br.nestle.com

PROTOCOLO DE AÇÕES

Este é um documento assinado eletronicamente pelas partes, utilizando métodos de autenticações eletrônicas que comprovam a autoria e garantem a integridade do documento em forma eletrônica. Esta forma de assinatura foi admitida pelas partes como válida e deve ser aceito pela pessoa a quem o documento for apresentado. Todo documento assinado eletronicamente possui admissibilidade e validade legal garantida pela Medida Provisória nº 2.200-2 de 24/08/2001.

Data de emissão do Protocolo: 22/06/2023

Dados do Documento

Tipo de Documento	POLÍTICAS_Normativos Internos
Referência Contrato	Política de Gestão de Cont de Negócios_07.06.2023
Situação	Vigente / Ativo
Data da Criação	12/06/2023
Validade	12/06/2023 até Indeterminado
Hash Code do Documento	745A94022D2CD142E82B071A2E98BD552D41AF24DB9D1BF242F05E6F585ADA1B

Assinaturas / Aprovações

Papel (parte) Diretoria (Outorgantes Procuração NÃO Eletrônica)
Relacionamento 62.562.012/0001-67 - Credi Nestlé

Representante	CPF
Francisco Gonçalves Neto	144.039.528-44

Ação:	Assinado em 13/06/2023 08:36:22 - Forma de assinatura: Usuário + Senha	**IP:**	172.69.3.140
Info.Navegador	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.42		
Localização	Não Informada		
Tipo de Acesso	Normal		

Representante	CPF
Marcos Valentim Baccarin	027.765.218-98

Ação:	Assinado em 14/06/2023 03:10:31 - Forma de assinatura: Usuário + Senha	**IP:**	172.70.82.147
Info.Navegador	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.42		
Localização	Latitude: -23.640251/ Longitude: -46.722493		
Tipo de Acesso	Normal		

Representante	CPF
Douglas Deivid Santos de Oliveira Sartori	082.687.506-85

Ação:	Assinado em 15/06/2023 01:43:25 - Forma de assinatura: Usuário + Senha	**IP:**	108.162.212.33
Info.Navegador	Mozilla/5.0 (iPhone; CPU iPhone OS 16_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.5 Mobile/15E148 Safari/604.1		
Localização	Latitude: -23.640494127852286/ Longitude: -46.722319581916544		
Tipo de Acesso	Normal		

Representante	CPF
RAFAEL MARTINES DA COSTA	301.060.728-89

Ação:	Assinado em 22/06/2023 11:21:34 - Forma de assinatura: Usuário + Senha	**IP:**	172.70.254.101
Info.Navegador	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.54		
Localização	Latitude: -20.338328328899095/ Longitude: -40.308927666356695		
Tipo de Acesso	Normal		

Enquanto estiver armazenado no Portal, a autenticidade, validade e detalhes de cada assinatura deste documento poderá ser verificada através do endereço https://www.qualisign.com.br/portal/dc-validar, utilizando o código de acesso (passcode) abaixo:

Código de Acesso (Passcode): **MAPZX-UPKM4-V9MJB-FH0C5**

No caso de assinatura com certificado digital também pode ser verificado no site https://validar.iti.gov.br/, utilizando-se o documento original e o documento com extensão .p7s.

Os serviços de assinatura digital deste portal contam com a garantia e confiabilidade da **AR-QualiSign**, Autoridade de Registro vinculada à ICP-Brasil.

Validação de documento não armazenado no Portal QualiSign

Caso o documento já tenha sido excluído do Portal QualiSign, a verificação poderá ser feita conforme a seguir;

a.) Documentos assinados exclusivamente com Certificado Digital (CADES)

A verificação poderá ser realizada em https://www.qualisign.com.br/portal/dc-validar, desde que você esteja de posse do documento original e do arquivo que contém as assinaturas (.P7S). Você também poderá fazer a validação no site do ITI – Instituto Nacional de Tecnologia da Informação através do endereço https://validar.iti.gov.br/

b.) Documentos assinados exclusivamente com Certificado Digital (PADES)

Para documentos no formato PDF, cuja opção de assinatura tenha sido assinaturas autocontidas (PADES), a verificação poderá ser feita a partir do documento original (assinado), utilizando o Adobe Reader. Você também poderá fazer a validação no site do ITI – Instituto Nacional de Tecnologia da Informação através do endereço https://validar.iti.gov.br/

c.) Documentos assinados exclusivamente SEM Certificado Digital ou de forma híbrida (Assinaturas COM Certificado Digital e SEM Certificado Digital, no mesmo documento)

Para documento híbrido, as assinaturas realizadas COM Certificado Digital poderão ser verificadas conforme descrito em (a) ou (b), conforme o tipo de assinatura do documento (CADES ou PADES).

A validade das assinaturas SEM Certificado Digital é garantida por este documento, assinado digitalmente pelo {*PortalNome3*}.

Validade das Assinaturas Digitais e Eletrônicas

No âmbito legal brasileiro e em também em alguns países do Mercosul que já assinaram os acordos bilaterais, as assinaturas contidas neste documento cumprem, plenamente, os requisitos exigidos na Medida Provisória 2.200-2 de 24/08/2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e transformou o ITI – Instituto Nacional de Tecnologia da Informação em autarquia garantidora da autenticidade, integridade, não-repúdio e irretroatividade, em relação aos signatários, nas declarações constantes nos documentos eletrônicos assinados, como segue:

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º. As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.

§ 2º. O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Pelo exposto, o presente documento encontra-se devidamente assinado pelas Partes, mantendo plena validade legal e eficácia jurídica perante terceiros, em juízo ou fora dele.