POLÍTICA DE CONTINUIDADE DE NEGÓCIOS (PCN)

I - OBJETIVO

- Esta política foi desenvolvida com o objetivo assegurar a continuidade dos serviços executados pela **Noxtec Serviços LTDA (Empresa)**, pessoa jurídica de direito privado, inscrita no CNPJ sob n. 21.388.231/0001-94, com sede na Rua Domingos José Martins, nº 75, sala 501, Recife - PE, CEP 50030-200, nos casos de situações adversas internas ou externas que afetem as atividades da empresa, seguindo os princípios da **Gestão a Continuidade de Negócios (GCN),** bem como definir os papéis de responsabilidade de execução e estratégia, alinhados aos princípios, valores e missão da Noxtec.

II - ABRANGÊNCIA

- Todos os colaboradores que atuam com a Noxtec.

III - DOCUMENTAÇÃO COMPLEMENTAR

- Política de Riscos
- ISO 22300
- ISSO 22301
- Lei nº 13709 - LGPD

IV - CONCEITOS E SIGLAS

- Não se aplica

V - DIRETRIZES

1. Continuidade de negócio e sua gestão.

- A continuidade de negócios é a capacidade da organização para continuar a prestar serviços ou produtos a níveis predefinidos e aceitáveis, após um incidente de interrupção (ISO 22.300). Segundo a ISO 22.301, a Gestão da Continuidade de Negócio é um processo holístico de gestão que sistematiza as práticas de planejamento, coordenação e implementação de ações e estratégias para garantir a precursão das atividades críticas para o negócio, no caso de um incidente crítico.

2. Definições

- **Crise:** Situação de um cenário de incidente ou emergência que não foi possível evitar, de acordo com os planos de resposta estruturados para a organização.

- **Desastre:** Situação de materialização de uma crise, com alta complexibilidade de mensuração dos impactos gerados aos negócios ou pessoas.
- **Evento:** Acontecimento interno ou externo, que pode gerar ou não impacto na organização.
- **Emergência:** Evento que pode ocorrer a partir de uma vulnerabilidade física, que gera impacto direto sobre os ativos e patrimônio da organização.
- **Incidente:** Situação que poderá levar à interrupção de negócios, perdas, emergências ou crises.
- **BIA** (*Business Impact Analysis*): Descreve os impactos que a organização poderá vir a sofrer devido à interrupção de um ou mais processos do negócio.
- **PGI** (Plano de Gestão de Incidentes): Plano responsável em dar suporte e orientação para o Comitê de Gestão de Crises, com a documentação necessária para determinar a resposta aos incidentes que levam à indisponibilidade, parcial ou total, da organização.
- **PCO** (Plano de continuidade Operacional): Plano que tem por objetivo garantir a continuidade dos serviços essenciais de TIC críticos, na ocorrência de um desastre, enquanto recupera-se o ambiente principal.
- **PRD** (Pano de Recuperação de Desastres): Plano que envolve um conjunto de políticas e procedimentos para permitir a recuperação ou continuação da operação da infraestrutura de tecnologia e sistemas vitais, na sequência de um desastre natural ou provocado pelo homem.
- **Recuperação:** Momento estratégico de implantação dos planos de continuidade de negócios da Organização, que tem como objetivo habilitar a organização para operar de forma alternativa, enquanto não se restabelece a operação normal.
- **Restauração:** Momento estratégico de implantação dos planos de continuidade de negócios da Organização que tem como objetivo retornar à operação normal da organização.

3. Gestão de continuidade de negócios

A gestão de continuidade de negócios da Noxtec, se estabelece a partir de 5 pilares, que devem ser respeitados, conforme as categorias descritas abaixo:

- Conhecer a organização
- Opções de continuidade de negócios
- Implementar a resposta de continuidade de negócios
- Executar e testar
- Incorporar competência conscientização

3.1. Conhecer a organização

3.1.1. Planejamento do ciclo operacional

- Realizar o planejamento e identificar os novos cenários de continuidade dos negócios. Esse processo deve ocorrer anualmente e conter as atividades referentes à **Gestão a Continuidade de Negócios (GCN)**, que serão praticadas no ano vigente. A revisão deverá contemplar todas as etapas subsequentes:
    - Para cada novo cenário, deverá ser definido um novo plano de ação, considerando ainda as mudanças relevantes de processos e sistemas.
    - Com os planos de ação definidos, deverão ser estabelecidos todos os esforços e orçamentos para execução do ciclo operacional, bem como o cronograma de **GCN**, devendo ser aprovado pelo grupo executivo e obter o "de acordo" da diretoria.

3.1.2. Gestão da análise de impacto nos Negócios (BIA)

- Sempre considerar dependências externas e internas dos processos de negócio, na visão de serviços de negócio.
- Analisar o impacto financeiro, de imagem e legal em relação aos tempos de parada, conforme os critérios estabelecidos na Política de Riscos da Organização.
- Os processos mais críticos devem ser claramente identificados e priorizados por TMI (tempo máximo de indisponibilidade).
- Identificar de forma clara os recursos necessários em contingência por área/processo de negócio.
- O período de indisponibilidade, devem ser obtidos junto às áreas de negócio e validado com os gestores.

3.1.3. Avaliação dos riscos

- A avaliação dos riscos deverá possuir escopo definido, abordando aspectos relacionados à continuidade dos negócios, como estrutura e segurança física, dependência de terceiros, colaboradores e sistemas.
- A avaliação dos riscos deverá ter um mapeamento detalhado dos riscos, considerando ameaças potenciais e respectivos graus de vulnerabilidade.
- A avaliação dos riscos deverá avaliar os cenários dos riscos que possam deixar a organização exposta, e assim orientar as estratégias de recuperação.

3.2. Opções de continuidade de negócios

3.2.1. Determinar estratégias de continuidade dos negócios

- A estratégia deverá ser definida levando em consideração a priorização dos processos críticos de negócio e as principais exposições a risco da organização.
- Deverão ser documentadas todas as modificações de infraestrutura nas áreas de negócios, que darão origem ao Relatório de Estratégia de Continuidade.
- Os relatórios deverão possuir estimativa de custos e planos de implementação, definidos junto às áreas responsáveis e aprovadas pelo grupo Executivo.
- Sempre que ocorrer a definição de uma nova estratégia de continuidade, esta deverá ser submetida à aprovação pelo grupo Executivo.

3.3. Implementar a resposta de continuidade de negócios

3.3.1. Implementar procedimentos de continuidade de negócios

- A confecção dos documentos, que darão suporte à resposta a incidentes (Plano de Recuperação de Desastres – PRD, Plano de continuidade Operacional – PCO e Plano de Gestão de Incidentes – PGI), deverá o ocorrer junto as áreas responsáveis, de acordo com a implementação das estratégias de continuidade e de TI e com as diretrizes estabelecidas na fase de Planejamento do Ciclo Operacional de GCN.
- Os documentos deverão ficas disponíveis em locais de fácil acesso a todos os colaboradores envolvidos na GCN, sendo possível acessá-los sempre que necessário. O seu armazenamento deverá considerar inclusive cenários de interrupção nos serviços de tecnologia, como indisponibilidade de servidores, recomendando-se manter vias impressas.
- O PRD deve conter o escopo, responsáveis e propósitos definidos e as atividades a serem executadas dependendo do cenário de indisponibilidade.
- O PDR deve conter o detalhamento de todas as atividades necessárias para a recuperação dos sistemas, contemplando os passos das atividades de operação das estratégias de recuperação dos sistemas de informação e infraestrutura tecnológica.
- O PCO deve conter o escopo, responsáveis e auxiliar a organização a minimizar o impacto imediato legal, financeiro, de imagem e operacional que um incidente possa causar.
- O PCO deve conter todas as atividades necessárias para a recuperação dos processos de negócio, bem como as diretrizes de como os funcionários devem atuar em uma situação de contingência.

3.4. Executar e testar

3.4.1. Executar e testar a resposta a incidentes

- Em caso de incidentes críticos de qualquer natureza, os procedimentos de resposta deverão ser aqueles estabelecidos nos documentos de suporte à resposta a incidentes (PRD, PCO e PGI).
- Os testes dos procedimentos descritos nos documentos de suporte à resposta a incidentes deverão ser realizados de acordo com o período definido durante o processo de Planejamento do Ciclo Operacional de GCN.
- Durante a realização de teste, para cada procedimento avaliado, deverá ser preenchido um Formulário de Acompanhamento de Testes contendo os resultados identificados.

3.5. Incorporar competência conscientização

3.5.1. Desenvolver programas de conscientização e educação de GCN

- Com o cronograma definido no processo de Planejamento do Ciclo Operacional de GCN, a área responsável pela Gestão de Continuidade de negócios deverá realizar treinamentos, para conscientizar todos os funcionários sobre o seu papel e sua responsabilidade diante a GCN, bem como sobre o funcionamento básico dos procedimentos de resposta a incidentes.

4. Responsabilidades

DIRETORIA EXECUTIVA

- Designar e atribuir responsabilidades pela Coordenação da Gestão da Continuidade do Negócio.
- Certificar que a Gestão da Continuidade de Negócio está adequada as necessidades da Noxtec;
- Garantir os recursos necessários para a manutenção da Gestão da Continuidade de Negócio.
- Deliberar sobre assuntos estratégicos no Gerenciamento de Incidentes.
- Garantir a execução das respostas a um incidente.

COMISSÃO DE RESPOSTAS A INCIDENTES

- Determinar o momento em que serão acionadas as áreas relacionadas ao PCO.
- Centralizar as ações e esforços para a recuperação e restauração dos ambientes impactados, com o objetivo de acelerar o processo de tomadas de decisão e alinhamento das atividades.
- Monitorar e realizar escalonamento sempre que necessário para atendimento das necessidades das áreas de negócio e tecnologia.

GESTÃO DE RISCOS

- Avaliar periodicamente os critérios para a criação de novos Planos de Continuidade do Negócio e manutenção das atuais.
- Determinar as ações necessárias para a realização das avaliações de impacto e riscos ao negócio.
- Criar Planos de Continuidade do Negócio sempre que for identificar a necessidade.
- Apoiar a comunicação entre as equipes de continuidade e gestores.
- Garantir que os requisitos regulamentares estejam sendo atendidos pelos Planos de Continuidade do Negócio.
- Apoiar a comunicação de retomada entre as equipes e a gestão corporativa.
- Gerenciar o sistema de Gestão da Continuidade do Negócio, definindo os prazos de manutenção dos planos e assessoramento técnico aos usuários.
- Criar e mandar a documentação de continuidade do negócio.
- Apoiar e acompanhar o desenvolvimento dos treinamentos e campanhas de continuidade do negócio.
- Desenvolver das atividades deliberadas pelo Comitê de Gestão de Crises.
- Gerenciar toda a resposta, retomada, recuperação e atividades de restauração das áreas de negócio. LGPD e a Continuidade de negócios A Lei (LGPD) prevê que as empresas a observem para garantir que no contexto da regulação, haja entre elas, o Compliance, a gestão de riscos e a governança de forma geral. Estar em conformidade é obedecer a lei, entretanto esta conformidade precisa considerar os aspectos de impacto nos negócios e a tecnologia que deve suportar de forma robusta estes processos. Alinhar ações de continuidade de negócios com os DPO das companhias é uma questão vital para o sucesso dos projetos de segurança.

  Além disso, é preciso que se observe a disponibilidade de medidas de proteção:

- Validar a resiliência dos processos de negócios;
- Incluir o tratamento de dados na Análise de impacto (BIA);
- Validar a transferência internacional de dados para ambientes de contingência e usar a LGPD como cenário para simulação de crises e desastres, a fim coibir eventos.

GESTORES

- Atuar em conjunto com a Gestão de Continuidade do Negócio para atender às responsabilidades compartilhadas.
- Apoiar os treinamentos e testes dos Planos de Continuidade do Negócio.
- Atualizar os procedimentos e macro atividades críticas, definidas nos Planos.

- Informar a área de Gestão de Risco a mudança do quadro funcional.
- Desenvolver o relatório de teste, para apresentar os resultados dos planos testados, em conjunto com a área de Gestão de Riscos.

TECNOLOGIA DA INFOMAÇÃO – TI

- Gerenciar e atualizar os Planos de Recuperação de Desastres de TI (PRD-TI), sempre que ocorrer alterações de versão, hardware, equipamento ou alguma outra alteração de nível operacional, troca de funcionários da área ou criação de novos procedimentos de trabalho, ou quando identificar alguma inconformidade por meio de testes.
- Atualizar e gerenciar procedimentos e tarefas das equipes que apoiam os serviços de TI em ambiente de contingência.
- Executar testes dos Planos de Recuperação de Desastres de TI de acordo com as demandas do negócio.
- Desenvolver o relatório de testes, sempre que o Planos de Recuperação de Desastres de TI for testado, em conjunto com a Área de Gestão de Riscos.
- Atuar com foco na garantia da alta disponibilidade dos ambientes críticos da Noxtec.
- Atuar como agente de riscos, apoiando e alimentando os processos de Gestão de Riscos da Noxtec, com o objetivo de minimizar a exposição da companhia a eventos que comprometam a disponibilidade, confidencialidade e integridade das informações.
- Assegurar que o desenvolvimento e implantação de novos sistemas e ambientes de TI sempre sejam avalizados em aspectos de continuidade dos negócios.
- Atuar na otimização de custos e recursos da Noxtec, no que se refere as estratégias de Continuidade Operacional e Negócios.
- Garantir o cumprimento de requisitos(infraestrutura) contratuais da Noxtec com terceiros, no que se refere às estratégias de Continuidade Operacional e Negócios.

COLABORADORES

- Entender e cumprir as diretrizes da Política de Continuidade do Negócio e os procedimentos, nos respectivos Planos de Continuidade do Negócio.
- Participar efetivamente dos testes dos Planos de Continuidade do Negócio, sempre que envolvidos.

Gestão de Consequências

Colaboradores, clientes, terceiros, diretores ou outros que observarem quaisquer desvios às diretrizes desta política, poderão relatar o fato ao Canal dpo@noxtec.com.br podendo ou não se identificar. Internamente, o descumprimento das diretrizes desta Política enseja a aplicação de

medidas cabíveis para a responsabilização dos agentes que a descumprirem, conforme a respectiva gravidade do descumprimento.

Disposição Gerais

É competência da área de Compliance alterar esta Política sempre que se fizer necessário. Esta Política entra em vigor na data de sua aprovação pelo Conselho de Diretoria e revoga quaisquer normas e procedimentos em contrário.

RAMON MEDINA CATAO:58452419449

Assinado de forma digital por RAMON MEDINA CATAO:58452419449