



1º SEMESTRE

2024

MANUAL GCN E GCSTI

VANERVEN SOLUTION



Aprovação:

1º Semestre 2024

Este documento é institucional, executivo e restrito, podendo ser divulgado unicamente para suas finalidades comerciais e técnicas.



(61) 3218-8750



www.vns.inf.br



contato@vns.inf.br

SUMÁRIO

1. APRESENTAÇÃO	3
2. METODOLOGIAS DE GESTÃO DE CONTINUIDADE	7
2.1. CONSIDERAÇÕES GERAIS	7
2.2. PROCESSO DE GESTÃO	10
2.3. RESPONSABILIDADES	11
2.4. GRUPOS FUNCIONAIS	16
2.5. ESCOPO DO PROGRAMA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS	18
2.6. ANÁLISE DE IMPACTO NOS NEGÓCIOS (BIA)	18
2.7. DEFINIÇÃO DA ESTRATÉGIA	22
2.8. PLANOS DE CONTINUIDADE.....	26
2.9. TREINAMENTOS E CAPACITAÇÃO SOBRE PROCESSOS.....	32
2.10. ACIONAMENTO DO PLANO	32
2.11. GESTÃO DE CRISE	33
2.12. AUDITORIA	34
3. MELHORIA CONTÍNUA	37

1. Apresentação

1.1. Política de GCN:

- a) A Metodologia de Gestão de Continuidade dos Negócios e de Tecnologia da Vanerven Solution tem por finalidade institucionalizar um processo e política de Gestão de Continuidade e estabelecer metodologias de análise, avaliação de riscos e gestão da atividade no ambiente corporativo e para atendimento a legislações e recomendações pertinentes aos principais clientes e área de atuação no mercado para seu ambiente principal e secundário geridos internamente. Conforme exemplificado:



- b) Este manual é elaborado e será atualizado como proposta da área de Tecnologia da Informação em conjunto com as áreas de negócio que tiverem seus processos indicados como críticos a operação corporativa, juntamente com os fornecedores e terceiros que tenham impacto a execução das atividades internas.
- c) No corpo desta metodologia, apresentamos o propósito para a organização, a Política, as Gerências e áreas que terão responsabilidade nas atividades. Caso outras sedes e equipes de contratos de atendimento não disponham dessa estrutura, os Gerentes locais corresponderão aos Gerentes do ambiente principal eventualmente existente.
- d) A adesão a esta metodologia ocorrerá por meio da aprovação e institucionalização do documento conforme as diretrizes institucionais.
- e) A reprodução parcial ou total deste documento só será permitido pela Vanerven Solution, que irá considerar este documento e as análises preliminares documentação interna, sendo apenas públicos os Planos de Continuidade, porém com divulgação ampla também aberta apenas a clientes, parceiros e funcionários específicos (não sendo público finalístico qualquer público em geral, visto conter informações pessoais de fornecedores e grupo de colaboradores).
- f) Ainda em relação a política de GCN é relevante ter consciência da importância de vida dos colaboradores como principal prioridade do programa na elaboração de todos os planos.
 - a) distribuição, acesso, recuperação e uso dos documentos (que poderá ocorrer periodicamente por Whatsups, e-mails, materiais impressos e via rede (ECM));
 - a) armazenamento e preservação, incluindo preservação de legibilidade;
 - c) controle de mudanças (ex.: controle de versão);
 - d) retenção e disposição;
 - e) recuperação e uso;
 - f) preservação de legibilidade (por exemplo: escrita legível);
 - g) prevenção de uso não intencional de informações obsoletas.
- g) Informações de origem externa documentadas determinadas necessárias pela Vanerven Solution para o planejamento e operação do SGCN devem ser identificadas através das

análises de impacto nos negócios e estarão sempre que possível relacionadas no próprio plano de continuidade se apropriado, e controladas através do versionamento dos documentos.

- h) Ao estabelecer controle de informações documentadas já existente, a Vanerven Solution garante que haja proteção adequada a elas (por exemplo: proteção contra comprometimento, modificação não autorizada ou deleção).

NOTA: O Acesso para algumas informações e planos, que pode permitir o acesso a informações sensíveis implica uma decisão sobre a permissão para visualizar informações documentadas, ou permissão e autoridade para visualizar informações documentadas, que deve em suas revisões e testes sempre serem avaliadas também.

1.2. Escopo

- a) Português: Aderência de práticas em conformidade a gestão de continuidade e atendimento para a unidade de datacenter primária na sede da empresa, além de recursos disponíveis em ambiente de datacenter redundante.
- b) Inglês: Adherence to consistent practices for continuity and service management for the primary datacenter unit at the company headquarters, in addition to features available in a redundant datacenter environment.

1.3. Indicadores

- a) Os principais indicadores que serão considerados para análise e monitoramento serão periodicamente definidos em relação à:
- a. Não conformidades identificadas;
 - b. Ocorrência de crises;
 - c. Novos planos de continuidade e análises de negócio por semestre;

- d. Histórico de execução de testes de continuidade;
 - e. Ocorrências de acionamento de planos;
 - f. Ocorrência de atualizações realizadas dentro e fora dos prazos estabelecidos, buscando como procedimento inicial implícito sempre confirmar se a versão mais atualizada está em uso.
- b) Tais indicadores e atualizações deverão ser apurados impreterivelmente no mínimo após 6 meses da implantação da norma, ou da execução de testes e análises.

1.4. Palavra da Diretoria

- a) Assim como a Vanerven Solution, qualquer organização, independentemente do porte ou segmento de atuação, corre o risco de sofrer situações adversas que podem atrapalhar as operações. Estas instabilidades podem surgir a qualquer momento e serem motivadas por problemas técnicos ou desastres naturais.
- b) Conforme estudo da ICTS Protiviti, realizado em 2016, sobre os maiores riscos enfrentados pelos executivos, os ataques cibernéticos são a terceira maior preocupação. Para reverter estas atribuições você pode implementar um Plano de Continuidade de Negócios (PCN) – também conhecido como Business Continuity Planning que é o que buscamos com o apoio de todos na Vanerven Solution. Ele funciona como um conjunto de planos de ação e estratégias preventivos para garantir o funcionamento dos serviços essenciais, enquanto não são plenamente normalizados.
- c) Sistemas invadidos podem resultar em perdas e gerar fraudes e prejuízos financeiros. A sobrevivência do negócio da Vanerven Solution e a credibilidade da empresa precisam de uma estratégia que as mantenha íntegras. Ao optar por um PCN, a Vanerven Solution consegue vencer momentos difíceis, demonstrar uma visão abrangente de seus negócios e oferecer segurança aos seus clientes.
- d) Sabemos que manter Planos de Continuidade de Negócios determinará a sobrevivência da empresa e garantirá a sustentabilidade de todos. Esta postura

norteará a manutenção dos serviços e estabelecerá uma boa imagem entre os clientes que a empresa já conquistou e atrairá novos. Com uma abordagem concentrada unicamente sob responsabilidade do departamento de TI, os custos para resolver problemas e “apagar incêndios” serão ainda mais imprevisíveis se não atuarmos proativamente.

- e) Não existe um PCN sem apoio da gestão e isto é reflexo do momento atual que buscamos e vivemos na Vanerven Solution, que visa a integração e o desenvolvimento contínuo. Hoje, dependemos muito de serviços de tecnologia, por isso é necessário manter os serviços em caso de interrupções graves para não perder todo o trabalho realizado.
- f) Não faltam medidas e opções para manter a integridade dos dados. Fazer backups dos arquivos é de extrema importância para manter os arquivos.
- g) Um PCN é influenciado pelo tipo de empreendimento da organização e deve se adequar a ele e às suas particularidades para ser efetivo e empregado com a agilidade exigida pela situação. Assim, é importante cumprir três condições essenciais: Análise de risco, Análise de Impacto e Planejamento Estratégico.

1.5. Exclusões

- a) Não há exclusões previstas até o momento, apenas metodologia correlata ao escopo especificado. A norma e práticas atuarão em conjunto com as outras normas e metodologias as quais a empresa seja certificada.

2. Metodologias de Gestão de Continuidade

2.1. Considerações Gerais

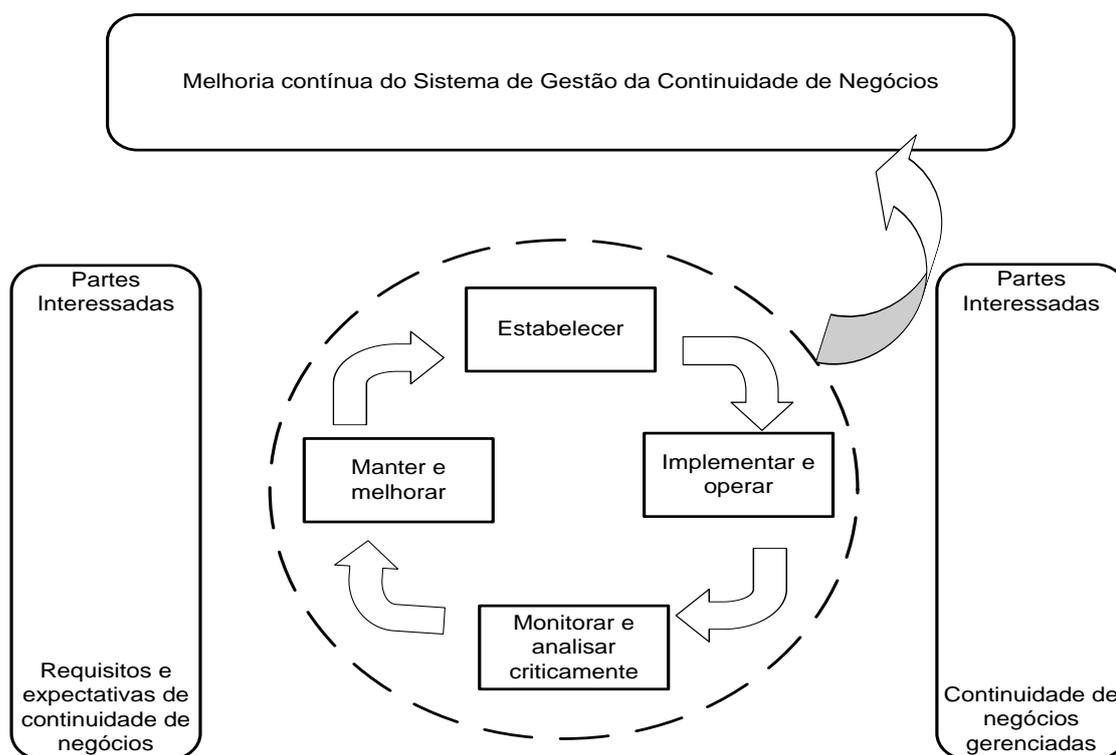
1. Com o acirramento da competitividade e obrigação de manter operacional uma estrutura corporativa em qualquer ocasião, a gestão de continuidade passou a ser o diferencial da capacidade de permanecer no mercado de forma sustentável e prover serviços de qualidade, sem a perda de informações ou ocorrência de prejuízos financeiros.

2. A gestão correta e eficaz de riscos é considerada um diferencial capaz de reduzir custos e impactos negativos as operações de negócios corporativos.
3. Dentre os vários tipos de risco catalogados no mercado, há o de descontinuidade das atividades da empresa, o qual pode gerar perdas pela não realização de negócios e, caso ocorra de forma impactante, perdas financeiras, de arrecadação ou de segmento de mercado, podendo proporcionar necessidade de indenizações e, até mesmo, afetar significativamente a imagem da Vanerven Solution.
4. O gerenciamento de continuidade é um processo de melhoria contínua que objetiva dar maturidade a Vanerven Solution na identificação e avaliação dos riscos de descontinuidade.
5. As perdas potenciais (o que pode ser perdido, como perdas financeiras, de imagem etc.) e o custo, para manter as atividades parcial ou totalmente, devem ser levantados pela empresa e o resultado, inclusive as opções de alternativas, encaminhado aos gerentes e superintendentes, que após analisar e aprovar a definição para o assunto, devem remeter o resultado a Diretoria que realiza acompanhamento das ações.
6. O gerenciamento de continuidade pode ser resumido nas seguintes etapas:
 - a) Planejamento: os Diretores e Gestores decidirão o que fazer, após a identificação dos pontos que podem gerar descontinuidade, avaliação das perdas potenciais, e levantamento dos investimentos relacionados às alternativas levantadas, além dos requisitos legais e regulamentares;
 - b) Execução: o plano de trabalho, seja para implementar mecanismos alternativos de retomada das operações ou apenas para justificar a interrupção, deve especificar os procedimentos descritos formando os planos de contingência, as pessoas treinadas e os testes realizados. É importante ainda levar em consideração as partes interessadas, como clientes, investidores, acionistas, fornecedores, público e comunidade (quando apropriado);
 - c) Avaliação do processo: ao longo da realização dos testes e da execução do Plano de Contingência faz-se necessário avaliar o que foi bem sucedido e o que falhou.

Novos processos podem ser entendidos como necessários a qualquer momento e inclusos para análise sempre que julgados pertinentes;

- d) Novo planejamento: para aprimorar os pontos fracos identificados na alínea anterior, novas ações devem ser especificadas analisando-se: o que fazer, quem vai fazer e quando fazer. Diante disto, relatórios semestrais devem ser emitidos para monitoramento, acompanhamento e continua gestão dos processos;
- e) Execução do novo planejamento: com novos treinamentos, testes e reavaliações, forma-se um processo que não terá fim, mas que será muito importante para uma percepção positiva da sociedade e gestores (internos e externos) em relação a empresa.

7. Esse ciclo possibilita a manutenção e melhoria do processo, conforme demonstrado no diagrama a seguir:



Fonte: ABNT NBR 15999-1

8. Aos departamentos que executam operações críticas e sensíveis as operações corporativas cabe identificar os riscos de descontinuidade de suas atividades, avaliar os riscos e decidir sobre a implementação de arranjos alternativos para garantir, mesmo

que parcialmente, as operações. Tais operações poderão ser realizadas mediante acionamento de consultor ou especialista (interno ou externo).

9. A interrupção de operações críticas atendimento as operações e atividades corporativas são fatores de risco à imagem da Vanerven Solution como um todo. Recomenda-se que os assuntos relacionados a esse evento, tal como interrupção do fornecimento de energia elétrica, do serviço de vigilante, de canais de comunicação com os ambientes de Data Center, etc., sejam analisados pelos Gestores da Vanerven Solution, mediante o devido suporte técnico, com consequente deliberação acerca do assunto, exceto quando houver fato realmente significativo que justifique decisão contrária.

2.2. Processo de gestão

1. A Gestão de Continuidade dos Negócios (GCN) é um processo abrangente de gestão que identifica ameaças potenciais de descontinuidade das operações de negócios para uma organização e os possíveis impactos. Caso essas ameaças se concretizem, com base na relação custo e benefício, os gestores devem aprovar a forma de tratamento da situação.
2. Esse processo fornece estrutura para que se desenvolva resiliência organizacional, ou seja, a capacidade de resposta efetiva ao incidente gerador da paralisação das atividades, salvaguardando, os interesses das partes interessadas, a reputação da Vanerven Solution.
3. O processo de Gestão de Continuidade se desenvolve com base nas seguintes atividades:
 - a) Identificação da possibilidade de paralisação das atividades;
 - b) Avaliação dos resultados e consequências (impactos potenciais) que possam atingir a entidade provenientes da paralisação das atividades;
 - c) Definição de uma estratégia de recuperação para a possibilidade da ocorrência do incidente;
 - d) Definição das implementações (definição de plano para as ações a serem providenciadas, com especificação clara de o que fazer, o responsável e prazo para

execução) para gerenciamento de incidentes adversos que possam gerar interrupção de um processo ou atividade considerada crítica;

- e) Continuidade planejada das operações (ativos, inclusive pessoas, sistemas e processos), considerados procedimentos para antes, durante e após a interrupção;
- f) A transição entre a contingência e o retorno à normalidade (saída do incidente);
- g) Análise das ações e procedimentos que garantam a continuidade de negócios, em situação de contingência, observando o que funcionou e o que precisa ser aprimorado para evitar falhas futuras, providenciando as correções necessárias.

2.3. Responsabilidades

1. As responsabilidades apresentadas neste capítulo objetivam gerar as condições adequadas para a efetiva implementação das diretrizes da Metodologia de Gestão de Continuidade de Negócios e de TI na Vanerven Solution.
2. Compete ao Comitê de Qualidade e Diretoria:
 - a) Aprovar a estratégia de continuidade e os respectivos orçamentos;
 - b) Acompanhar o processo de implementação da estratégia de continuidade, em função dos riscos operacionais envolvidos;
 - c) Aprovar a estratégia de continuidade para os equipamentos e sistemas que possibilitam o processamento de operações, bem como os orçamentos necessários para a efetiva implementação;
 - d) Aprovar cronogramas de teste propostos.
3. Compete aos responsáveis pelos Planos de Continuidade dos Negócios (PCN):
 - a) Aprovar a metodologia de continuidade;
 - b) Propor ao Comitê as estratégias de continuidade de Tecnologia da Informação, e das demais áreas que prestam serviços a empresa, assim como aprovar os

respectivos orçamentos referentes às estratégias de continuidade, encaminhando as matérias para deliberação do Comitê, negociando, quando necessário, o rateio dos investimentos com parceiros, órgãos externos e fornecedores;

- c) Zelar para que a estratégia de continuidade de negócios e para que os respectivos orçamentos sejam efetivamente cumpridos, bem como manter o Comitê periodicamente informado do cumprimento das estratégias e dos orçamentos;
- d) Implementar os procedimentos adequados para minimizar os riscos de descontinuidade de acordo com a estratégia aprovada;
- e) Sempre que possível, providenciar a implementação de gestão centralizada de serviços que podem propiciar descontinuidade de atividades em outras sedes e pontos de atendimento, como serviços de vigilância armada, fornecimento de canais de comunicação, aquisição de equipamentos padronizados e compatíveis com a necessidade tecnológica, sem prejuízo de quaisquer outros identificados;
- f) Aprovar calendário anual de testes.

4. Compete a Diretoria, por meio das suas respectivas Gerências:

- a) Identificar, avaliar e tratar, riscos de descontinuidade relacionados às suas atividades;
- b) Atender às solicitações da equipe ou consultoria referente à Gestão de Continuidade de Negócios (GCN) e de Serviços de TI (GCSTI);
- c) No caso de incidente que gere paralisação, mesmo que momentânea, dos processos que dão suporte aos produtos e serviços fundamentais, informar à área ou responsável interno de gestão de continuidade de negócios referente ao processo:
 - c.1) A sua ocorrência;
 - c.2) A causa geradora do incidente;
 - c.3) As soluções empreendidas e os consequentes resultados;

- c.4) A necessidade de adequação de sistemas, processos e(ou) pessoas e os respectivos planos de ação para a efetiva implementação.
- d) Se ofertados produtos e(ou) serviços, fazer a identificação dos riscos que podem paralisar as atividades, avaliando a possibilidade de perda potencial e, em uma análise de custo e benefício, empreender as ações necessárias à implementação de procedimentos (planos) específicos para continuidade dos negócios, tomando-se o cuidado de alinhar as ações de Continuidade de Negócios aos riscos operacionais identificados e avaliados;
- e) Manter os Planos de Continuidade atualizados, de forma que sejam efetivos quando acionados ou consultados;
- f) Garantir, quando aplicável, que estejam definidos, em contrato, acordos de nível de serviços que garantam o alinhamento das prestações de serviços de terceiros com as estratégias de continuidade de negócios das suas áreas;
- g) Manter os empregados e prestadores de serviços, que participam dos Planos de Continuidade Operacional e Recuperação de Desastres, devidamente treinados, garantindo, assim, a efetividade das atividades, de acordo com os níveis previamente estabelecidos;
- h) Estabelecer anualmente, cronograma de testes dos planos, realizando-os e formalizando o resultado, com apontamento do que deu certo e das necessidades de aprimoramento, com o consequente plano de ação, especificando responsáveis pela execução e prazo;
- i) Providenciar que as atividades relacionadas aos produtos e serviços, mantidas sejam analisadas, com base no custo e benefício, e se conveniente, seja(m) implementado(s) plano(s) específicos que mantenham as atividades nos níveis desejados;
- j) Comunicar, imediatamente, à área ou responsável interno de gestão de continuidade de negócios qualquer alteração no cenário de negócio da área que requeira manutenção nos planos definidos para continuidade dos processos de negócio;

- k) Treinar os colaboradores objetivando à capacitação dos profissionais envolvidos na gestão de continuidade de negócios, bem como orientar sobre os conceitos e as metodologias aplicáveis;
 - l) Criar cronograma e relatórios de testes periódicos.
5. Compete A Vanerven Solution, por meio da sua Gerencia de Infraestrutura:
- a) Considerar, nas definições de estratégia de contingência de serviços de TI, as necessidades dos clientes (internos e externos) que utilizam os recursos;
 - b) Propor a estratégia de continuidade de negócios para os equipamentos e sistemas que possibilitam o processamento de operações, bem como os orçamentos necessários para a efetiva implementação, especificando, de forma clara e concisa para que haja o entendimento pelas pessoas que não são especialistas em tecnologia da informação:
 - b.1) Os ativos (*hardware* e *software*) que suportam processos de negócios identificados como críticos e aplicados questionários BIA;
 - b.2) Arranjos de contingência existentes;
 - b.3) Propor soluções futuras de TI;
 - b.4) Custo e prazo de implementação;
 - c) Implementar planos de recuperação de desastre, visando a recuperar os ativos de TI dentro dos prazos definidos (tempos objetivados de recuperação) nos processos de negócios considerados;
 - d) Fornecer, tempestivamente, todas as informações solicitadas à área ou responsável interno de gestão de continuidade de negócios.
6. Compete ao departamento de Qualidade:
- a) Revisar este manual, pelo menos, uma vez ao ano;

- b) Prover A Vanerven Solution metodologia que garanta a implementação do Gerenciamento de Continuidade de Negócios e de Tecnologia da Informação devidamente aprovado;
- c) Coordenar e orientar a implementação da estrutura de gerenciamento de continuidade de negócios;
- d) Comunicar, periodicamente, aos gestores sobre o andamento da Gestão de Continuidade de Negócios e de Tecnologia da Informação e das necessidades de aprimoramentos identificadas;
- e) Coordenar processo em que os gestores identifiquem e avaliem riscos de descontinuidade, baseados na relação entre o benefício da manutenção das atividades e os custos financeiros e não-financeiros provenientes da interrupção das atividades, adotar procedimentos adequados para minimização e mitigação;
- f) Estabelecer orientações na adoção de procedimentos de minimização e mitigação, quando da identificação de riscos de descontinuidade;
- g) Solicitar das áreas contempladas por planos de contingência o cronograma de testes dos planos de continuidade de negócios;
- h) Acompanhar a realização de testes dos Planos de Continuidade de Negócios, podendo, para isso, convocar para o dia e horário necessário os empregados indispensáveis à execução;
- i) Solicitar, caso necessário, testes adicionais fora das datas agendadas, podendo, para isso, requisitar aos respectivos superiores a presença de empregados em dias e horas previamente estabelecidos;
- j) Verificar se os responsáveis pelos Planos de Continuidade de Negócios estão mantendo os executores dos respectivos planos devidamente treinados, de forma a garantir a sua efetividade;

- k) Interagir com a área de desenvolvimento de serviços e fornecer as informações e metodologias necessárias para que as diretrizes de Gestão de Continuidade de Negócios e de Tecnologia da Informação sejam incorporadas aos novos serviços;
- l) Garantir a execução dos testes;
- m) Sempre que houver evento que gere a indisponibilidade, mesmo que parcial, de produto ou serviço, inclusive de Tecnologia da Informação deverão ser consolidadas as informações recebidas e registrar em relatório específico, contendo:
 - m.1) Descrição do incidente;
 - m.2) Causa da paralisação;
 - m.3) Os aprimoramentos implementados ou a serem implementados, com os respectivos prazos, que objetivam minimizar novas ocorrências do gênero.
- n) Manter os planos de continuidade de negócios atualizados, bem como os funcionários treinados;
- o) Garantir, quando aplicável, que estejam definidos, em contrato, os acordos de nível de serviços que garantam o alinhamento das prestações de serviços de terceiros com as estratégias de continuidade de negócios das suas áreas.

2.4. Grupos Funcionais

1. Grupos funcionais são constituídos pelos empregados designados para realizar os procedimentos de contingência descritos nos planos.
2. Componentes: líder e empregados designados no respectivo plano.
3. Coordenador: líder do processo citado no plano.
4. Compete ao Grupo Operacional:
 - a) *Antes da contingência*:

- a.1) Propor os procedimentos que mantenham as atividades de negócio em nível previamente definido;
- a.2) Realizar testes periódicos dos planos de continuidades, para garantir a sua efetividade, bem como treinar os empregados envolvidos.

b) Durante a contingência:

- b.1) Acionar o Plano de Continuidade de Negócio e, concomitantemente, o gestor responsável pelo respectivo plano;
- b.2) Avisar o representante do Grupo da respectiva área o acionamento de contingência;
- b.3) Empreender as ações necessárias à execução do plano;
- b.2) Caso não haja procedimentos de contingência descritos para o incidente identificado, ou não seja possível, por qualquer razão, acionar o plano, comunicar imediatamente informar, se possível, sugestões de recuperação da atividade e (ou) de gestão de crise;
- b.3) Manter-se, em caso de não funcionamento do plano, em sobreaviso para executar as orientações do gestor de crise.

c) Depois da contingência:

- c.1) Registrar, em relatório específico, a descrição do incidente e as soluções de contorno aplicadas;
- c.2) Verificar o que motivou o incidente/crise, emitindo e encaminhando ao gestor responsável as causas e as ações de aprimoramentos implementadas ou a implementar, para elaboração de relatório;
- c.3) Caso seja necessário, implementar procedimentos de aprimoramento dos respectivos planos.

2.5. Escopo do Programa de Gestão de Continuidade de Negócios

1. Os Gestores de cada Gerência da Vanerven Solution devem:
 - a) Identificar os produtos e serviços fundamentais que suportam os objetivos, obrigações e deveres da empresa;
 - b) Elencar os processos ou conjunto de processos que dão suporte a esses produtos e serviços identificados;
 - c) Designar um gestor responsável por cada processo ou conjunto de processos elencados;
 - d) Designar um responsável principal pela Gestão de Continuidade de Negócios na entidade, que inicialmente já foi definido como a área de qualidade (que pode ser alterada a qualquer momento através de reuniões de análise crítica);
 - e) Designar empregado (interno ou externo) para coordenar a implementação de Gestão de Continuidade de Negócios e de TI periodicamente;
 - f) Providenciar canais de comunicação, inclusive contingenciais, para acesso.
2. Essas informações devem estar devidamente documentadas e aprovadas pelos gestores da Vanerven Solution.
3. Caso seja necessário, A Vanerven Solution poderá nomear comitês ou grupo(s) funcional(is) para trabalhar na implementação do programa de Gestão de Continuidade de Negócios e de Tecnologia da Informação, observando o disposto na Metodologia Institucional de Gestão de Continuidade.
4. A coordenação dos trabalhos pode ser atribuída a profissional com conhecimento da matéria, sem perda da responsabilidade dos gestores responsáveis pelo produto ou serviço, a quem compete mobilizar a equipe e empreender as ações necessárias para que o assunto seja adequadamente tratado.

2.6. Análise de Impacto nos Negócios (BIA)

1. Os gestores, devem realizar as seguintes atividades para os processos elencados no escopo desta metodologia:
 - a) Identificar os riscos de paralisação dos processos, devido à incidentes, tais como falha no fornecimento de energia elétrica, falha nos canais de comunicação, ausência de empregado, escassez dos principais insumos, etc.;
 - b) Avaliar a perda potencial decorrente da paralisação dos processos, utilizando do formulário de análise de impacto nos negócios (BIA);
 - c) Identificar alternativas ou arranjos de contingência;
 - d) Levantar o investimento e custeio para implementação das alternativas descritas para evitar a interrupção e (ou) recuperar as operações;
 - e) Decidir sobre as alternativas, recursos e seus custos, com base em análise de custo X benefício;
 - f) Encaminhar as informações levantadas e análises efetuadas para os gestores, com todas as informações necessárias para o entendimento;
 - g) Providenciar que o quadro técnico implemente as soluções aprovadas pelos Coordenadores.
2. O impacto da interrupção deve ser verificado por meio da Análise de Impacto nos Negócios (BIA) para riscos identificados, como “médios”, “altos” e “muitos altos”, bem como para os casos em que o gestor entender necessária a aplicação;
3. A revisão da Análise de Impacto nos Negócios (BIA) deve ser feita a cada 2 anos ou sempre que houver mudanças significativas das atividades que suportam os produtos e (ou) serviços, devendo, nesse caso, a área de negócio responsável solicitar a revisão.
4. A avaliação do risco de descontinuidade e análise da viabilidade de se implementar arranjo de contingência é feita a partir da experiência do gestor responsável pelas atividades que podem sofrer paralisações.

5. Para a realização da Análise de Impacto nos Negócios (BIA), devem ser considerados, no caso de interrupção do processo:
 - a) Impacto financeiro;
 - b) Impacto legal; e
 - c) Impacto de imagem.

6. Os riscos de descontinuidade, cuja perda financeira, legal e de imagem, de acordo com os resultados da Análise de Impacto nos Negócios, apresentam alto impacto e necessitam ser recuperados mais rapidamente são classificados como críticos.

7. Para verificação do nível de criticidade do risco, serão utilizadas as informações dos formulários de Análise de Impacto nos Negócios (BIA), contendo três critérios, cada um com peso diferenciado, tendo em vista o contexto de negócio da entidade:
 - a) impacto legal: descumprimento de lei e (ou) norma (peso 20);
 - b) impacto financeiro: perdas financeiras geradas pelo não atendimento, registro ou arrecadação (peso 30);
 - c) impacto de imagem: afeta a imagem da Vanerven Solution pela interrupção de atendimento ou operação interna (peso 40).

8. Para cada critério estabelecido acima, o impacto será determinado pelo gestor responsável pela avaliação, ao definir uma nota, na seguinte escala:

Opção escolhida	Nota	Impacto
E	50	Critica
D	40	Alta
C	30	Média
B	20	Pouca importância

Opção escolhida	Nota	Impacto
A	10	Irrelevante

9. A cada critério (legal, financeiro e imagem) é atribuída uma nota, de acordo com a tabela do item 8 deste capítulo, somam-se as notas e divide-se o resultado por 90 (soma dos pesos do item 7 deste capítulo):

$$\frac{(\text{Nota de impacto legal} + \text{nota de impacto financeiro} + \text{nota de impacto de imagem})}{90}$$

10. O resultado da Análise de Impacto nos Negócios (BIA) sinaliza o grau de impacto da não implementação de contingência, conforme apresentado a seguir:

Resultado	Severidade	Impacto da não implementação de contingência
4,00 a 5,00	Crítico	Alto
3,00 a 3,99	Moderado	Médio
1,00 a 2,99	Leve	Baixo

11. As informações descritas no formulário de Análise de Impacto nos Negócios (BIA), servirão de base para definição da estratégia para o processo em análise.
12. Na avaliação da implementação de arranjo de contingência, deve ser observada, sempre que possível, a relação custo X benefício, de forma que o valor investido na implementação dos arranjos de contingência seja compatível com as perdas potenciais identificadas (financeiras, legais e de imagem).
13. A avaliação do risco, as conclusões da Análise de Impacto nos Negócios (BIA) informada no item anterior, o resultado, as alternativas de contingência, bem como os

investimentos e (ou) custos levantados devem ser aprovadas pelos gestores responsáveis pelos processos.

2.7. Definição da Estratégia

1. A estratégia é uma solução para manter a continuidade das atividades que suportam o produto ou serviço crítico, dentro de níveis previamente estabelecidos, e deve ser apropriada, possível e de custo adequado à relação benefício/custo.
2. Os recursos essenciais exigidos para a realização dos processos críticos no nível mínimo estabelecido devem ser identificados e podem contemplar, a critério do gestor do processo crítico:
 - a) Pessoas;
 - b) Instalações;
 - c) Tecnologia;
 - d) Informação;
 - e) Suprimentos; e
 - f) Partes interessadas.
3. A partir dos resultados da avaliação de atividades críticas, o gestor responsável pelos processos de negócios, conhecedor dos riscos de interrupção de atividades e das perdas potenciais, deve considerar opções estratégicas para recuperação de suas atividades críticas e para os recursos que cada atividade consumirá durante sua restauração, devendo, para isso, definir:
 - a) As consequências de não se implementar mecanismos de contingência, ou seja, as perdas potenciais já estimadas (financeiras, legais e de imagem, analisadas na Análise de Impacto nos Negócios);
 - b) Nível mínimo a ser mantido nas atividades contingenciadas;
 - c) Período máximo suportável para recuperação das atividades críticas;

- d) Os custos de investimento da(s) estratégia(s) escolhida(s).
4. As implementações a serem providenciadas devem considerar o tempo máximo suportável para a recuperação das atividades críticas, geralmente quanto menor o tempo, maior o investimento.
 5. Selecionados os recursos essenciais, devem ser identificadas alternativas que irão suportar a restauração das atividades exigidas, dentro do tempo de recuperação desejado, podendo ser minutos, horas ou dias, dependendo da atividade crítica, com base no impacto potencial, sempre do ponto de vista da área gestora do negócio e com aprovação.
 6. Os Coordenadores de negócio devem tomar cuidados especiais na escolha da alternativa de continuidade, para que essa não seja afetada pelo mesmo incidente que gerou a interrupção da atividade, por exemplo, duas concessionárias de *link* de internet que utilizam o mesmo cabo (fibra ótica), nessa situação, problemas afetarão a operação normal e a contingência.
 7. Para as ameaças relativas a cada recurso, por meio da decisão dos gestores, podem escolher uma ou mais estratégias de mitigação, entre as descritas a seguir:
 - a) Recuperação das atividades dentro de prazo objetivado: as operações precisam estar novamente em funcionamento total ou parcial (definição prévia que impactará o investimento necessário) no prazo estabelecido;
 - b) Manutenção das operações mesmo com o acontecimento de incidente: as operações não são paralisadas, por exemplo, *no-breaks* e gerador de energia elétrica são adquiridos para manter as operações em funcionamento;
 - c) Aceitação do risco: no caso de paralisação das atividades, não se adota qualquer arranjo de contingência, bem como não dispõe de qualquer arranjo que possibilite a recuperação, mesmo que parcial. O que norteia essa decisão é o fato de o custo de implementar arranjos de contingência ser desproporcional ao benefício potencial;

- d) Transferência: para alguns riscos, a melhor resposta pode ser transferi-los. Isso pode ser realizado por meio de um seguro convencional.
8. A empresa poderá optar por definir estratégias de continuidade, quando viável, para:
- a) Pessoas: estratégias para manter as habilidades e conhecimentos fundamentais, tais como: documentação dos procedimentos de execução das atividades críticas, rodízio de empregados, segregação das atividades fundamentais, uso de recursos humanos terceirizados, planejamento de sucessão, gestão do conhecimento (adequada capacitação) entre outras opções.
- b) Instalações: estratégia para tratar indisponibilidade das instalações de trabalho, tais como: alternativas próprias ou de terceiros (por meio ou não de acordos recíprocos), realização de trabalho em casa ou em locais remotos, uso de força de trabalho alternativa, etc.
- c) Tecnologia: estratégias de tecnologia devem considerar o tempo máximo que a entidade esteja disposta a esperar a restauração das atividades críticas (tempo objetivado de recuperação), onde as estratégias podem incluir: distribuição geográfica da tecnologia, adotar o equipamento mais antigo como substituto em caso de emergências, utilização de redundância de equipamentos, acesso remoto, etc.
- d) Informação: estratégias para garantir que a informação vital para a continuidade das atividades da entidade esteja protegida e seja recuperável de acordo com os limites de tempo estabelecidos na Análise de Impacto nos Negócios. As estratégias podem incluir:
- d.1) Formatos físicos: cópias de documentos impressos disponíveis, atualizados e protegidos contra acessos indevidos;
- d.2) Formatos virtuais: *backup* das informações e soluções de alta disponibilidade disponível para restauração em qualquer tempo.

- e) Suprimentos: estratégias para garantir que os suprimentos estejam prontamente disponíveis nos locais da execução dos processos críticos. As estratégias podem incluir:
- e.1) Armazenamento de suprimentos adicionais em outro local;
 - e.2) Acordos com terceiros para entregas emergenciais;
 - e.3) Remanejamento de entregas programadas para outros locais;
 - e.4) Armazenamento de materiais em armazéns ou bases de envio;
 - e.5) Transferência de atividades de montagem de unidades para um local alternativo que possua esses suprimentos;
 - e.6) Identificação de suprimentos alternativos/substitutos;
 - e.7) Aumento do número de fornecedores;
 - e.8) Recomendação ou exigência de que os fornecedores tenham uma capacidade de continuidade de negócios validada;
 - e.9) Obrigações contratuais e (ou) acordos de nível de serviços com os principais fornecedores;
 - e.10) Identificação de fornecedores alternativos que sejam capazes de atender à demanda.
- f) Partes interessadas: estratégias apropriadas para gerenciar as relações com as principais partes interessadas, fornecedores e parceiros de negócios ou serviços. As estratégias podem incluir:
- f.1) Identificação de pessoas para garantir o bem estar de todos durante e após o incidente;
 - f.2) Identificação de responsável pela centralização da comunicação com funcionários, contribuintes e fornecedores;

- f.3) Identificação de responsável pela comunicação com a mídia.
- g) Emergências civis: estratégias de antecipação, avaliação, prevenção, preparação, resposta e recuperação em casos de emergências civis. As estratégias podem incluir:
 - g.1) Identificação de responsável pela comunicação com as autoridades competentes para responder em caso emergências, com intuito de obter ajuda pré ou pós-incidente;
 - g.2) Definição de procedimentos de aviso e informação;
 - g.3) Acordos de recuperação comunitária após uma emergência civil;
 - g.4) Evacuação das instalações;
 - g.5) Mobilização das equipes de segurança, de primeiros socorros ou assistência à evacuação;
 - g.6) Manutenção de comunicação que seja relevante para o gerenciamento de incidentes ou para restabelecimento das atividades.
- 2. As estratégias podem ser definidas para toda a empresa ou individualmente para cada processo.
- 3. A estratégia é uma maneira definida para manter a continuidade das atividades que suportam o produto ou serviço crítico e deve ser apropriada, possível e de custo adequado à relação benefício/custo.
- 4. As estratégias devem ser submetidas à aprovação dos gestores, que decidirão o prazo para a implantação, quando aprovada.

2.8. Planos de continuidade

- 1. Planos de Continuidade são um conjunto de procedimentos que objetivam, no caso de ocorrência de determinado(s) incidente(s), manter as atividades em nível de funcionamento previamente estabelecido ou recuperá-las no prazo previamente

- estabelecido (tempo objetivado de recuperação - comumente chamado no mercado de RTO).
2. Os planos de continuidade devem ser elaborados sempre que os gestores decidirem pela implementação de contingência. Quando a decisão for de não implementação, as entidades documentarão a decisão.
 3. Os planos devem ser ativados com base na estratégia selecionada para gerenciar o incidente e devem ser seguidos total ou parcialmente em qualquer estágio de resposta ao incidente.
 4. Os planos de continuidade de negócios devem ser objetivos, concisos, acessíveis àqueles que possuam responsabilidades neles definidas e devem prever:
 - a) Situação em que cada plano pode ser utilizado (relação de ativos, eventos ou cenários);
 - b) Os responsáveis pelos procedimentos de recuperação;
 - c) Os procedimentos que devem ser executados para o incidente ou recuperação dos recursos que sofreram interrupção, quando existentes.
 5. O objetivo de cada plano deve estar bem definido e ser compreendido pelas pessoas que irão executá-lo e compreender dados e ações como:
 - a) detectar um incidente,
 - b) monitorar regularmente a possibilidade de um incidente,
 - c) fazer a comunicação interna dentro da Vanerven Solution, bem como receber, documentar e responder a comunicações das partes interessadas,
 - d) receber, documentar e responder a qualquer sistema de aviso de riscos regional, nacional ou equivalente,
 - e) garantir a disponibilidade dos meios de comunicação durante um incidente,
 - f) facilitar a comunicação estruturada com equipes de emergência,

- g) armazenar informações vitais sobre o incidente, ações e decisões tomadas, assim como os itens a seguir devem ser considerados e implementados quando aplicável:
 - h) alertar as partes interessadas potencialmente impactadas por um incidente de interrupção real ou iminente,
 - i) assegurar a interoperabilidade de múltiplas organizações e pessoal;
 - j) operar uma instalação de comunicações.
6. Os procedimentos de comunicação e alerta deve ser regularmente exercitados.
7. Os planos de continuidade de negócios podem ser classificados como:
- a) Plano de Continuidade Operacional (PCO): voltado à continuidade das atividades operacionais críticas;
 - b) Plano de Recuperação de Desastres (PRD): voltado à recuperação dos ativos de Tecnologia da Informação (processamento, links de comunicação e armazenamento de dados) que dão suporte aos procedimentos operacionais do processo;
 - c) Plano de Gestão de Incidentes (PGI): voltado a recuperação do ambiente em casos de incidentes ou ações da natureza, tais como incêndio, inundação, não acesso, pandemia, falta de energia elétrica.
8. Os Planos de Continuidade podem ser elaborados visando a vários tipos de eventos ou riscos operacionais, entre os mais comuns:
- a) Incêndio;
 - b) Inundação;
 - c) Interrupção no fornecimento de energia elétrica;
 - d) Atos de vandalismos;
 - e) Outros, a critério da administração da empresa.

9. Os Planos de Continuidade devem:
 - a) Definir os papéis e responsabilidades, nos aspectos relacionados à tomada de decisão durante e após um incidente;
 - b) Fornecer referência dos contatos essenciais das partes que viabilizam a sua execução;
 - c) Ser revisados anualmente ou sempre que os responsáveis realizarem alteração nos procedimentos executados;
 - d) Ser aprovados pela respectiva gerência ou área equivalente, no caso de ativos de Tecnologia da Informação;
 - e) Ser aprovados pelos gestores das áreas contingenciadas, que devem assegurar que estão em conformidade com a Metodologia Corporativa de Gestão de Continuidade;
 - f) Os planos de continuidade de negócios, bem como suas alterações, devem ser submetidos à aprovação pelo gestor da área, com a presença do representante responsável pelo desenvolvimento do plano;
 - g) As aprovações pelos Gestores responsáveis pelos processos, devem ser evidenciadas por meio de assinatura no próprio documento ou, quando for o caso, atas de reunião;
10. Planos de continuidade de negócios para atividades realizadas que tiverem desmembramentos do processo realizado, deverão especificar os procedimentos sob a responsabilidade de todas as empresas (ex: fornecedores, terceiros, parceiros) que participarem do processo, inclusive com nomes dos responsáveis, e meios de contato;
11. A atualização dos planos em decorrência de realização de testes também é considerada revisão. A Vanerven Solution determina, implementa, mantém e atualiza continuamente o SGCN, incluindo os processos necessários e suas interações de acordo com os requisitos da norma ISO 22301;

12. Os testes devem ser formalmente registrados observando as necessidades de aprimoramento que, quando identificadas, devem ser alvo de plano de ação por parte do responsável pelo plano para que sejam providenciadas as devidas correções e (ou) adequações que visem a acrescentar melhorias na sua utilização;
13. Auditorias (internas ou externas) também podem, sempre que julgar necessário, acompanhar a realização de testes, assim como ter total acesso aos seus resultados;
14. Planejar os testes conforme o tipo selecionado: o planejamento do teste consiste em determinar um cenário a ser utilizado, quais áreas e planos serão envolvidos, tempo de duração dos testes, pessoas envolvidas, preparação do ambiente (seja uma sala de reunião ou um ambiente alternativo);
15. Selecionar o tipo de teste a ser executado: é importante que o tipo de teste selecionado seja adequado à maturidade do processo, devendo ser realizado no mínimo o teste de mesa. Para que possa garantir o sucesso na condução e finalização, adequando a realidade aos planos. Os testes podem ser:
 - b.1) Testes de mesa: geralmente realizado em uma mesa de reunião, é um teste de complexidade simples, no qual é realizada uma análise (crítica ensaios de execução), dos procedimentos e informações descritas, com o objetivo de atualizar e(ou) validar os procedimentos e as informações contidas no plano;
 - b.2) Simulação: é um teste de complexidade média no qual uma situação “artificial” é criada, por exemplo, é realizada a parada de um processo em horários diferentes das operações diárias (finais de semana, após expediente, etc.) sendo o resultado utilizado para validar se os planos possuem as informações necessárias e suficientes, de forma a permitir recuperação de determinado arranjo de contingência ou processo com sucesso;
 - b.3) Teste real: *testar em tempo real os planos de continuidade, o que envolve alta complexidade;*

16. Utilizar controle de versão para os planos e testes: visa garantir que o plano a ser utilizado esteja atualizado e que dúvidas em eventuais mudanças sejam facilmente verificadas através das versões anteriores;
17. Gerar plano de teste e validação (PTV) para todos os planos testados: esses planos darão suporte para a condução dos testes, pois indicarão quais são os procedimentos de cada plano e o resultado do teste;
18. Disponibilização dos planos aos seus respectivos responsáveis;
19. Equipe preparada para a realização dos testes;
20. O ambiente para testes deve ser controlado de forma a não interromper as atividades de produção.
21. O programa de testes deve ser consistente com o escopo dos planos e com as devidas considerações legais e (ou) normativas.
22. Ao estabelecer cronograma de testes do ano, as seguintes informações, não limitadas à, deverão ser consideradas:
 - a) quem serão os responsáveis;
 - b) o que deverá ser executado;
 - c) quais serão os recursos necessários;
 - d) quando a execução será concluída; e
 - e) como os resultados serão avaliados.
22. Além dos aspectos já relacionados, é importante considerar sempre na elaboração dos planos e atualizar na execução dos testes:
 - a) comunicação interna entre os grupos interessados e empregados da Vanerven Solution, através dos grupos funcionais formalizados das alterações e versão válida do documento;

- b) comunicação externa com clientes, entidades parceiras, comunidade local, e outros grupos interessados, inclusive a mídia, onde deverão estar disponíveis os canais no grupo de comunicação de fornecedores no documento;
- c) recebimento, documentação e resposta à comunicação dos grupos interessados;
- d) adaptação e integração a um sistema de assessoria à ameaças nacionais ou regionais, ou equivalente, onde atualmente é disponível pela mídia e o grupo de defesa civil do estado.
- e) no planejamento ou operação, se apropriado;
- f) garantia de disponibilidade dos meios de comunicação durante o incidente gerador de interrupção, mantendo sempre que possível as informações disponíveis por mais de um canal em sua versão mais atualizada;
- g) facilitação da estrutura de comunicação com as autoridades apropriadas para garantir interoperabilidade de múltiplas organizações e pessoal, quando apropriado; e
- h) operação e teste das capacidades de comunicação destinados a serem utilizados durante a interrupção dos meios normais de comunicação.

2.9. Treinamentos e capacitação sobre processos

1. Os treinamentos relacionados à operacionalidade das atividades de cada área são de responsabilidade da respectiva gerência, seguindo os processos corporativos já estabelecidos;
2. Os treinamentos visam a assegurar que coordenadores, empregados e terceiros sejam conscientizados das ameaças que podem gerar interrupção dos processos, das consequências e da importância do estabelecimento de estratégias e dos Planos de Continuidade.

2.10. Acionamento do Plano

1. Sempre que ocorrer um incidente que gere a descontinuidade das atividades, o gestor do processo (líder do plano) deve contatar o Gestor ou responsável pela Gestão de

- Continuidade para analisar o incidente, definindo se o Plano de continuidade será acionado ou não;
2. O responsável por acionar o plano deve acompanhar todo o processo de restabelecimento das atividades normais;
 3. O Grupo funcional, coordenado pelo líder do grupo, deve seguir os procedimentos estabelecidos no Plano de Continuidade.
 4. Após todo e qualquer processo de ativação de Plano de Continuidade ou de gestão de crise, cabe registrar a descrição do incidente, o que foi bem sucedido, o que falhou e os aprimoramentos implementados para correção das fragilidades identificadas, bem como as ações com os responsáveis e prazo para implementação, se necessário;
 5. Relatórios emitidos devem ser submetidos aos gestores para conhecimento e adoção de medidas julgadas necessárias.

2.11. Gestão de Crise

1. Os planos devem permitir estabelecer uma diretriz de comunicação a ser seguida pelas equipes em situações de crise, de modo a unificar e garantir procedimentos rápidos, precisos e eficientes a quaisquer eventos que venham a pôr em risco a imagem e reputação da Vanerven Solution. O que deve sempre que possível ser formalizado em ata de reunião formalizando a crise, após isto uma análise crítica é necessária e a posterior atualização e ajuste dos planos,
2. Caso a crise afete toda a Vanerven Solution, compete as equipes (internas ou externas) aguardar ações da equipe de Comunicação, sem tomar a frente de uma situação junto a mídia.
3. Caso o acionamento do Plano de Continuidade ou a gestão de crise gere a necessidade de atendimento à imprensa, essa atribuição deve ser desempenhada de forma organizada, centralizada e por responsável ou departamento previamente definido corporativamente.

4. Em relação a Crises, será necessário agir para endereçar tendências adversas ou resultados antes que uma não conformidade ocorra, e manter informações relevantes como evidência dos resultados.
5. Os procedimentos para monitoração do desempenho devem prever a configuração de métricas de desempenho apropriadas às necessidades da Vanerven Solution, que normalmente constam em legislações, contratos com clientes e fornecedores ou acordos internos. A monitoração da medida em que a política de continuidade dos negócios da Vanerven Solution em relação aos seus objetivos e metas sejam atingidas.
6. Desempenho dos processos, procedimentos e funções que protegem as atividades prioritizadas, monitoração da conformidade com a norma ISO 22301 e os objetivos de continuidade dos negócios em relação a crises deve ser mantido registrado através das atas de reunião, constando dados da monitoração das evidências históricas de desempenho deficitário no SGCN. Além de armazenamento de dados e resultados da monitoração e medição para facilitar ações corretivas subsequentes.
7. Quando um incidente que cause interrupção e resulte na ativação dos seus procedimentos de continuidade dos negócios ocorre, A Vanerven Solution deve realizar uma análise crítica pós-incidente e registrar os resultados

2.12. Auditoria

1. O processo de auditoria a ser executado, deve seguir as práticas corporativas já existentes e estabelecidas.

2.13. Análise crítica

1. Na execução de análises críticas é recomendável sempre o envolvimento da Direção, que deve comunicar a importância de uma gestão de continuidade de negócios eficaz e alinhada com os requisitos do SGCN.
2. A nomeação ou atualização dos responsáveis pelo GCN - responsabilidades e competências para o gerenciamento da continuidade de negócios, e nomeação de um ou

mais colaboradores aptos a serem responsáveis pelo SGCN, com autoridades e competências apropriadas para a implantação e manutenção do ciclo que podem ser discutidas e avaliadas a qualquer momento, porém impreterivelmente nas análises críticas.

3. A Direção deve assegurar que as responsabilidades e papéis relevantes sejam atribuídos e comunicados dentro da Vanerven Solution por definição de critérios e níveis de aceitação de riscos, envolvimento ativo em exercícios e testes, garantia de que auditorias internas para o SGCN sejam realizadas, realização de análises críticas da gestão do SGCN e demonstração do comprometimento com a melhoria contínua, além de outras informações como:

- a) Informar e aprovar a política de SGCN, Escopo.
- b) Indicar as principais áreas consideradas para os BIAS e Planos.
- c) Indicar comitê de crises.
- d) Dados e ações de monitoramento e medição;
- e) O status das ações de análises críticas pelas Direções anteriores;
- f) As mudanças em questões internas e externas que sejam relevantes ao sistema de gestão de continuidade dos negócios;
- g) informação do desempenho da continuidade dos negócios, inclusive tendências em:
 - 1) não conformidades e ações corretivas;
 - 2) resultados da avaliação de monitoração e medição e,
 - 3) resultados de auditoria;
- d) oportunidades de melhoria contínua.
- e) As análises críticas pela Direção devem considerar o desempenho da Vanerven Solution, inclusive:
 - 1. ações de acompanhamento de análises críticas pelas Direções anteriores;
 - 2. a necessidade de mudanças do SGCN, inclusive a política e objetivos;

3. oportunidades de melhoria;
4. resultados das auditorias e análises críticas do SGCN, incluindo aquelas de fornecedores-chave e parceiros, quando apropriado;
5. técnicas, produtos ou procedimento, que podem ser usados na Vanerven Solution para melhorar o desempenho e a eficácia do SGCN;
6. status de ações corretivas;
7. resultados de exercícios e testes;
8. riscos ou questões não endereçadas adequadamente em nenhum processo de avaliação de riscos anterior;
9. quaisquer mudanças que possam afetar o SGCN, tanto internas quanto externas ao escopo do SGCN;
10. adequação da política;
11. recomendações de melhoria;
12. lições aprendidas e ações decorrentes de incidentes que causem interrupção, e
13. boas práticas e orientações emergentes.

f) As saídas da análise crítica pela Direção devem incluir decisões relacionadas a oportunidades de melhoria contínua e à possível necessidade de mudanças do SGCN, e incluem o seguinte:

1. variações do escopo do SGCN;
2. melhoria da eficácia do SGCN;
3. atualização do processo de avaliação de riscos, análise de impacto nos negócios, plano de continuidade dos negócios e processos relacionados;
4. modificação de procedimento e controles para responder eventos externos ou internos que possam impactar no SGCN, inclusive mudanças em:

5. requisitos operacionais e de negócio;
6. requisitos de redução de risco e segurança;
7. condições operacionais e processos;
8. requisitos legais e regulatórios;
9. obrigações contratuais;
10. níveis de risco e/ou critério de aceitação de riscos;
11. necessidades de recurso;
12. requisitos de orçamento e financiamento; e
13. como a eficácia dos controles é medida.

g) A Vanerven Solution deve manter informações documentadas como evidência dos resultados das análises críticas pela Direção.

h) A Vanerven Solution deve:

- a) Comunicar os resultados da análise crítica pela Direção para as partes interessadas, e
- b) realizar ações apropriadas para os resultados.

3. MELHORIA CONTÍNUA

- 3.12. Melhoria contínua é a prática adotada por diversas empresas que visa atingir ininterruptamente resultados cada vez melhores, sejam eles nos produtos e serviços da empresa, ou então em seus processos internos. A melhoria contínua pode ser atingida através de diversas metodologias e boas práticas organizacionais.
- 3.13. Durante as últimas décadas, especialmente a partir dos anos 1980 e 1990, o termo “melhoria contínua” vem sendo um mantra na maioria das organizações. Isso decorre principalmente do aumento da competição global entre as empresas, que força a gerarem cada vez mais valor aos clientes, de forma cada vez mais onerosa.

- 3.14. Todos estamos cientes da necessidade por melhoria. Mas, como fazer ela acontecer de fato? Por onde começar? Bom, alguns princípios básicos devem ser contemplados para que possamos atingir resultados cada vez melhores.
- 3.15. Geralmente, podemos melhorar duas coisas: nossos processos principais ou nossos processos secundários. Processos principais, ou produtivos, são aqueles que estão ligados diretamente com o que fazemos (nosso core business). Processos secundários são aqueles que nem sempre estão ligados ao cerne do negócio, mas também são importantes em um cenário geral.
- 3.16. Eu só melhora o que eu consigo medir. Essa é uma verdade universal em melhoria contínua. Para tal, será necessário o acompanhamento de indicadores e auditorias internas e externas periodicamente para gerar esta garantia corporativa
- 3.17. É preciso ter uma métrica para definir qualidade. Para se obter sucesso em melhoria contínua, devemos saber onde estamos e para onde vamos. Para isso, devemos desdobrar o que é qualidade e definir indicadores para medi-la. Por exemplo: podemos estimar nossa qualidade como o número de refugos produzidos. Assim, podemos medir como estamos e estimar aonde queremos chegar.