PLANO DE CONTINUIDADE DE NEGÓCIOS

Plano de Continuidade de Negócios

CONTROLE DE VERSÕES E ALTERAÇÕES					
Versão	Data	Tipo de Alteração	Responsável	Revisor	Aprovador
01.0	22/11/2023	Criação	Marco Maurício Tinoco	Comitê de Privacidade	
01.1	11/02/2025	Revisão	Luiz Eduardo de Freitas Simões	Comitê de Privacidade	
01.2	18/03/2025	Revisão	Marco Maurício Tinoco	Comitê de Privacidade	
02.0	07/04/2025	Revisão	Marco Maurício Tinoco	Comitê de Privacidade	

Plano de Continuidade de Negócios

Sumário

Plano de Continuidade de Negócios

1. OBJETIVOS

Expor a todos os clientes, parceiros e colaboradores da MOSTEN NEGÓCIOS & TECNOLOGIA LTDA., pessoa jurídica de direito privado, inscrita no CNPJ/ME sob o nº 67.201.640/0001-30, com sede na Rua Visconde do Rio Branco, 02, 6º andar, CEP 11013-030, Centro, na cidade de Santos, SP, doravante denominada simplesmente "MOSTEN" os conceitos da correta operação de um Plano de Continuidade de Negócios (PCN) e a importância da adoção das melhores práticas.

Apresentar as diretrizes gerais que devem ser observadas pela MOSTEN no processo de gestão de riscos estabelecendo responsabilidades e limites de atuação reforçando o desenvolvimento da cultura interna e priorizando as ações necessárias conforme o negócio, seguindo as normas de Segurança da Informação para garantir a tríade de confidencialidade, integridade e disponibilidade dos dados.

O Plano de Continuidade de Negócios (PCN) da MOSTEN tem como objetivos principais:

- Implementar e seguir os seis estágios do processo de continuidade: O PCN estrutura a resposta a incidentes e a recuperação das operações críticas em seis estágios distintos, que visam garantir uma abordagem sistemática e eficaz. Estes estágios são:
    1. Identificação e Avaliação: Este estágio inicial envolve a identificação da ocorrência de um evento disruptivo, a avaliação de sua natureza, escopo e potencial impacto nos processos de negócios críticos da MOSTEN. Inclui a coleta de informações preliminares e a comunicação inicial aos responsáveis.
    2. Acionamento do PCN: Com base na avaliação inicial, este estágio define os critérios e os procedimentos para a formal ativação do PCN, incluindo a convocação do Comitê de Segurança e Continuidade e a comunicação da situação para as partes interessadas relevantes.
    3. Resposta e Contenção: Uma vez acionado o PCN, este estágio foca na implementação das ações imediatas para responder ao incidente, conter seus efeitos e minimizar os danos. Isso pode envolver a ativação de planos de emergência específicos, a isolamento de áreas afetadas e a implementação de

medidas de segurança.

4. Recuperação: Este estágio compreende a execução das estratégias de recuperação predefinidas para restaurar os processos de negócios críticos dentro dos Objetivos de Tempo de Recuperação (RTOs) estabelecidos. Inclui a ativação de backups, a utilização de sites de contingência (se aplicável) e a mobilização de recursos necessários.
5. Restauração: Após a recuperação dos processos críticos a um nível mínimo operacional, este estágio visa o retorno às operações normais, incluindo a restauração completa dos sistemas, a reconciliação de dados e a resolução de quaisquer pendências decorrentes da interrupção.
6. Análise Pós-Incidente e Melhoria Contínua: O estágio final envolve a análise detalhada do incidente, da resposta implementada e da eficácia do PCN. O objetivo é identificar lições aprendidas, lacunas no plano e oportunidades de melhoria para fortalecer a resiliência da MOSTEN a futuras interrupções.

- Garantir a especificidade dos "Seis Estágios" (Objetivos do PCN): Cada um dos seis estágios do PCN possui objetivos específicos que detalham as metas a serem alcançadas em cada fase do processo de continuidade, contribuindo para a restauração eficiente e eficaz das operações críticas da MOSTEN.
- Definir o desencadeamento de ações do PCN: O PCN estabelece claramente os gatilhos (critérios de acionamento) e os procedimentos para o início das ações de resposta e recuperação em cada um dos seis estágios, garantindo uma atuação oportuna e coordenada em situações de crise.

O presente Plano de Continuidade de Negócios (PCN) será desenvolvido e mantido em aderência a este ciclo de seis estágios, garantindo uma abordagem sistemática e abrangente para a resiliência operacional da MOSTEN.

Desencadeamento de ações:

O objetivo de "Desencadear ações coordenadas de resposta e recuperação" estabelece a necessidade de procedimentos bem definidos para lidar com incidentes disruptivos. Em

consonância com este objetivo, o presente Plano de Continuidade de Negócios (PCN) detalhará, em seções subsequentes, os procedimentos específicos para as seguintes categorias de ações, adaptados aos diversos cenários de interrupção identificados:

- Ações de Resposta: Correspondem às medidas imediatas a serem implementadas na ocorrência de um incidente. Estas ações visam, de forma geral:
    - Realizar a avaliação inicial do incidente e seus impactos.
    - Acionar as equipes de resposta e os planos de contingência pertinentes, conforme a "Tabela de Acionamento Emergencial/Contingência – Escalation".
    - Implementar medidas para contenção e isolamento do incidente.
    - Priorizar a segurança de pessoas e a proteção de ativos.
    - Estabelecer a comunicação inicial com as partes interessadas relevantes.
- Ações de Recuperação: Referem-se aos procedimentos planejados para o restabelecimento das operações de negócios críticas aos níveis de serviço definidos, dentro de prazos aceitáveis. Estas ações incluem, tipicamente:
    - Ativar os planos de recuperação específicos para as funções de negócios afetadas.
    - Utilizar recursos de contingência, como o "SITE DE CONTINGENCIAMENTO", quando aplicável.
    - Executar os procedimentos de restauração de sistemas, dados e infraestrutura.
    - Verificar a integridade e a funcionalidade dos recursos recuperados.
    - Coordenar o retorno gradual às operações normais.

Os detalhes específicos dos procedimentos de resposta e recuperação, incluindo os responsáveis, os recursos necessários e os tempos de recuperação esperados, serão apresentados nas seções subsequentes deste documento, em alinhamento com os diferentes cenários de interrupção considerados.

2. DEFINIÇÕES E DIRETRIZES

Para fins deste Plano de Continuidade de Negócios (PCN), as seguintes definições e diretrizes serão aplicadas:

2.1. ACIONAMENTO DO COMITÊ DE SEGURANÇA:

O acionamento do Comitê de Segurança do PCN é um processo formal que visa reunir os membros chave para avaliar um evento disruptivo e decidir sobre a ativação e implementação dos procedimentos de continuidade. O acionamento ocorrerá com base nos seguintes critérios:

Critérios de Acionamento:

O Comitê de Segurança do PCN será acionado quando ocorrer um ou mais dos seguintes eventos ou situações:

- Indisponibilidade de Serviços Críticos: Falha ou interrupção de um ou mais serviços de negócios considerados críticos por um período superior ao limite predefinido (a ser especificado na Análise de Impacto nos Negócios - BIA).
- Incidentes de Segurança da Informação Significativos: Confirmação de incidentes de segurança cibernética com potencial de impacto significativo nas operações, dados ou reputação da MOSTEN (ex: ataques de ransomware, vazamento de dados, intrusão em sistemas críticos).
- Falhas na Infraestrutura Crítica: Falhas graves ou iminentes na infraestrutura de TI (servidores, rede, telecomunicações, CPD), energia elétrica ou outras instalações essenciais que possam levar à interrupção de serviços críticos.
- Desastres Naturais ou Causados por Humanos: Ocorrência de eventos como incêndios, inundações, tempestades severas, acidentes graves ou outras emergências que afetem as instalações da MOSTEN ou a capacidade de operação dos colaboradores.
- Alerta de Autoridades Competentes: Recebimento de alertas ou ordens de evacuação ou restrição de acesso por parte de autoridades governamentais (Defesa Civil, Corpo de Bombeiros etc.).
- Escalonamento de Incidentes: Incidentes que não puderam ser resolvidos pelas equipes de suporte de primeiro e segundo nível dentro dos prazos estabelecidos e que representam uma ameaça à continuidade dos negócios.
- Outros Eventos: Qualquer outro evento que, a critério da alta gestão ou do Ponto Focal do PCN, represente uma ameaça significativa à capacidade da MOSTEN de manter suas operações.

Responsabilidades no Processo de Acionamento:

Os seguintes indivíduos ou grupos têm responsabilidades específicas no processo de

acionamento do Comitê de Segurança do PCN:

- Qualquer Colaborador: Ao identificar um evento que possa atender aos critérios de acionamento, o colaborador tem a responsabilidade de comunicar imediatamente o fato ao seu superior imediato ou ao Ponto Focal do PCN.
- Superior Imediato/Ponto Focal do PCN: Ao receber a notificação de um possível evento de acionamento, o superior imediato ou o Ponto Focal do PCN deverá realizar uma avaliação preliminar da situação para verificar se os critérios de acionamento são atendidos.
- Ponto Focal do PCN (Responsabilidade Primária): O Ponto Focal do PCN é o principal responsável por:
    - Receber e registrar as notificações de possíveis eventos de acionamento.
    - Realizar a avaliação inicial ou coordenar essa avaliação com as áreas competentes (ex: TI, Segurança da Informação, Gerenciamento de Facilidades).
    - Confirmar se os critérios de acionamento foram atendidos.
    - Acionar formalmente os membros do Comitê de Segurança do PCN através dos canais de comunicação predefinidos (telefone, e-mail etc.).
    - Manter um registro do processo de acionamento, incluindo a data, hora, motivo e membros notificados.
- Membros do Comitê de Segurança do PCN: Ao serem acionados, os membros do comitê têm a responsabilidade de:
    - Confirmar o recebimento da notificação de acionamento.
    - Participar da reunião de avaliação inicial (presencial ou remota, conforme definido nos procedimentos).
    - Contribuir com informações relevantes de suas respectivas áreas para a avaliação da situação.
    - Participar da tomada de decisão sobre a necessidade de ativação total ou parcial do PCN e sobre as primeiras ações a serem implementadas.

A lista dos membros do Comitê de Segurança do PCN e seus respectivos contatos de emergência serão mantidos atualizados e facilmente acessíveis. Os procedimentos detalhados para a comunicação de acionamento e a realização da reunião inicial do comitê serão definidos em um documento de suporte ao PCN.

2.2. TABELA DE IMPLANTAÇÃO:

A Tabela de Implantação do PCN detalha as responsabilidades e os prazos para a execução das principais atividades relacionadas ao desenvolvimento, implementação, teste e manutenção do Plano de Continuidade de Negócios da MOSTEN. Esta tabela visa garantir que todas as ações necessárias sejam atribuídas a responsáveis específicos e concluídas dentro de prazos definidos, assegurando a efetividade e a atualização contínua do PCN.

A estrutura da Tabela de Implantação incluirá as seguintes colunas:

- Atividade: Descrição clara e concisa da atividade a ser realizada no âmbito do PCN.
- Responsável Primário: Área, cargo ou indivíduo principal responsável pela execução da atividade.
- Responsáveis de Apoio (se aplicável): Áreas, cargos ou indivíduos que fornecerão suporte para a execução da atividade.
- Prazo Estimado para Conclusão: Data ou período esperado para a conclusão da atividade (a ser definido durante o planejamento detalhado).
- Status: Campo para indicar o status atual da atividade (ex: Não Iniciado, Em Andamento, Concluído, Pendente).
- Observações: Espaço para comentários adicionais ou informações relevantes sobre a atividade.

Conteúdo da Tabela de Implantação (Exemplos Iniciais - a serem detalhados e completados):

Atividade	Responsável Primário	Responsáveis de Apoio	Prazo Estimado para Conclusão	Status	Observações
Conduzir a Análise de Impacto nos Negócios (BIA)	Gerenciamento de Riscos	Todas as áreas de negócio	[A Definir]	Não Iniciado	
Identificar os processos críticos da MOSTEN	Gerenciamento de Riscos	Todas as áreas de negócio	[A Definir]	Não Iniciado	Resultado da BIA.
Definir os Objetivos de Tempo de Recuperação (RTOs)	Gerenciamento de Riscos	Todas as áreas de negócio	[A Definir]	Não Iniciado	Para cada processo crítico.
Definir os Objetivos de Ponto de Recuperação (RPOs)	TI, Gerenciamento de Riscos	Todas as áreas de negócio	[A Definir]	Não Iniciado	Para cada processo crítico e seus dados.

Desenvolver as estratégias de continuidade para processos críticos	[A Definir - Responsável pela Área]	TI, Gerenciamento de Riscos, Gerenciamento de Facilidades	[A Definir]	Não Iniciado	
Elaborar os planos de ação detalhados para cada estratégia	[A Definir - Responsável pela Área]	TI, Gerenciamento de Riscos, Gerenciamento de Facilidades	[A Definir]	Não Iniciado	Incluindo procedimentos passo a passo, recursos e responsabilidades.
Definir os procedimentos de acionamento do PCN	Comitê de Governança de Continuidade	Ponto Focal do PCN, TI, Segurança da Informação	[A Definir]	Não Iniciado	
Estabelecer os canais de comunicação de emergência	TI, Comunicação	Todas as áreas	[A Definir]	Não Iniciado	Listas de contato atualizadas.
Configurar o site de contingência (se aplicável)	TI, Gerenciamento de Facilidades		[A Definir]	Não Iniciado	
Implementar as soluções de backup e restauração	TI		[A Definir]	Não Iniciado	
Desenvolver o plano de testes do PCN	Comitê de Governança de Continuidade	TI, Todas as áreas	[A Definir]	Não Iniciado	Definir cenários, frequência e critérios de sucesso.
Executar os testes do PCN (simulações)	[A Definir - Responsáveis pelos Testes]	Todas as áreas envolvidas	[A Definir]	Não Iniciado	Registrar resultados e lições aprendidas.
Revisar e atualizar o PCN	Comitê de Governança de Continuidade	Ponto Focal do PCN, Todas as áreas	[A Definir - Periodicidade]	Não Iniciado	Com base nos resultados dos testes, incidentes e mudanças no negócio.
Treinar os colaboradores sobre o PCN	Recursos Humanos, Ponto Focal do PCN	Todas as áreas	[A Definir - Periodicidade]	Não Iniciado	Conscientização e responsabilidades individuais.

Observação: Esta tabela será completada com todas as atividades identificadas como necessárias para o PCN, com a designação clara dos responsáveis e a definição de prazos realistas para sua conclusão. A Tabela de Implantação será um documento vivo, monitorado e atualizado regularmente para garantir a contínua melhoria e efetividade do Plano de Continuidade de Negócios da MOSTEN.

2.3. PLANO DE CONTINUIDADE DE NEGÓCIO (PCN):

O Plano de Continuidade de Negócios (PCN) da MOSTEN é um conjunto abrangente de procedimentos documentados e estratégias predefinidas, elaborado com o objetivo

de garantir a resiliência das operações críticas da empresa frente a interrupções significativas. Este plano estabelece as diretrizes, as responsabilidades e os passos a serem seguidos para prevenir, mitigar, responder e recuperar de eventos disruptivos, assegurando a continuidade das funções essenciais do negócio com o mínimo de impacto possível. O PCN abrange desde a identificação de riscos e a análise de impacto até a implementação de planos de recuperação e a realização de testes periódicos para validar sua eficácia.

Para um melhor entendimento, apresentamos a relação do PCN com outros termos frequentemente utilizados:

- Plano de Contingência: O Plano de Contingência é geralmente considerado um componente específico dentro do PCN. Ele se concentra em respostas táticas e operacionais para lidar com incidentes ou falhas particulares (e.g., falha de um sistema específico, perda de um local). O PCN, por sua vez, é um documento de nível superior que engloba diversos planos de contingência, estratégias de recuperação e procedimentos para garantir a continuidade global dos negócios.
- Contingenciamento Operacional: O termo "Contingenciamento Operacional", conforme mencionado em outras partes deste documento (e.g., "IMPORTANTE IMPORTANTE"), refere-se às ações e procedimentos práticos implementados para mitigar os efeitos de uma interrupção nas operações diárias. O contingenciamento operacional pode envolver a utilização de recursos alternativos, a ativação de planos de contingência específicos ou a execução de processos manuais temporários. Ele representa a execução prática de partes do PCN em resposta a um evento disruptivo.

Em resumo, o PCN é o documento estratégico guarda-chuva que estabelece a estrutura para a resiliência da MOSTEN. Os Planos de Contingência são planos específicos dentro do PCN que abordam ameaças ou cenários particulares, e o Contingenciamento Operacional são as ações práticas de resposta implementadas em linha com o PCN e seus planos de contingência.

2.4. PLANEJAMENTO DO PCN

O planejamento do Plano de Continuidade de Negócios (PCN) da MOSTEN é um processo iterativo e contínuo, essencial para garantir a sua relevância e eficácia. As principais etapas deste processo incluem:

- Análise de Impacto nos Negócios (BIA): Esta etapa fundamental envolve a identificação e a avaliação dos processos de negócios críticos da MOSTEN. A BIA tem como objetivo determinar os impactos financeiros, operacionais, legais e de reputação que poderiam resultar da interrupção desses processos. Ela também estabelece os Objetivos de Tempo de Recuperação (RTO) e os Objetivos de Ponto de Recuperação (RPO) para cada processo crítico, definindo as janelas aceitáveis de indisponibilidade e a quantidade máxima de perda de dados tolerável.
- Identificação de Recursos Críticos: Com base nos resultados da BIA, são identificados os recursos essenciais para a operação dos processos críticos. Estes recursos podem incluir infraestrutura de TI (hardware, software, redes), dados, pessoal chave, instalações, equipamentos, fornecedores terceirizados e outros elementos indispensáveis para a continuidade dos negócios.
- Definição de Estratégias de Recuperação: Para cada processo crítico e seus respectivos recursos, são definidas estratégias de recuperação apropriadas. Estas estratégias descrevem as ações e os procedimentos a serem implementados para restaurar as operações normais dentro dos RTO estabelecidos. As estratégias podem envolver soluções como backups e restauração, sites alternativos de operação (contingência), planos de comunicação de crise, realocação de pessoal e outras medidas de mitigação e recuperação. As "ESTRATÉGIAS DE CONTINUIDADE" são detalhadas na Seção 4 deste documento.
- Elaboração dos Planos de Ação: Os planos de ação detalham os passos específicos a serem seguidos para implementar as estratégias de recuperação definidas. Cada plano de ação deve incluir:
    - Objetivos claros e mensuráveis.

- Ações detalhadas e sequenciais.
- Responsabilidades designadas para cada ação (referenciando a Tabela de Implantação).
- Recursos necessários para a execução do plano.
- Prazos estimados para a conclusão de cada etapa.
- Procedimentos de comunicação e escalonamento.

- Testes e Simulações: Para validar a eficácia dos planos de ação e das estratégias de recuperação, o PCN prevê a realização periódica de testes e simulações em diferentes cenários de interrupção. Os resultados desses testes são utilizados para identificar lacunas, ajustar os planos e garantir que a equipe esteja preparada para responder a incidentes reais.
- Manutenção e Atualização: O PCN é um documento vivo que requer manutenção e atualização regulares. Isso inclui a revisão periódica do plano para refletir mudanças nos processos de negócios, na infraestrutura de TI, nos requisitos regulatórios e nos resultados dos testes. As versões e alterações do documento são controladas conforme a seção "CONTROLE DE VERSÕES E ALTERAÇÕES".

2.5. DESASTRES

No contexto do Plano de Continuidade de Negócios (PCN) da MOSTEN, um desastre é definido como qualquer evento repentino, inesperado e significativo que causa uma interrupção grave nas operações normais da empresa, podendo resultar em perdas financeiras, danos à reputação, impactos legais ou regulatórios, e/ou riscos à segurança de pessoas e ativos. Para facilitar o planejamento da resposta e a implementação das estratégias de continuidade, os desastres são categorizados da seguinte forma:

2.5.1. Desastres Naturais:

São eventos causados por forças da natureza que podem impactar as instalações da MOSTEN, a infraestrutura de suporte ou a capacidade de operação dos colaboradores. Exemplos incluem:

- Eventos climáticos extremos: Tempestades severas, inundações (considerando a localização em Santos), raios, ventos fortes, granizo, ondas de calor ou frio extremos.
    - Procedimentos Específicos: Monitoramento de alertas meteorológicos, planos de evacuação de áreas de risco de inundação ou deslizamento, proteção de equipamentos sensíveis contra intempéries, avaliação de danos estruturais após o evento.
- Terremotos: Embora menos frequentes na região, representam um risco potencial.
    - Procedimentos Específicos: Planos de evacuação de edifícios, inspeção de segurança estrutural após o tremor, procedimentos de comunicação em caso de falha de infraestrutura.

2.5.2. Desastres Tecnológicos:

São eventos relacionados a falhas ou incidentes na infraestrutura de tecnologia da informação e comunicação da MOSTEN. Exemplos incluem:

- Falhas de infraestrutura de TI: Pane em servidores críticos, falhas de rede (internet, comunicação interna), interrupção prolongada no fornecimento de energia elétrica para o CPD ou outras instalações essenciais.
    - Procedimentos Específicos: Ativação de sistemas redundantes, failover para ambientes de contingência (conforme Seção 4), restauração de backups de dados e sistemas, diagnóstico e reparo de hardware e software.
- Ataques cibernéticos: Ransomware, ataques DDoS (negação de serviço), invasões de sistemas que comprometam a disponibilidade, a integridade ou a confidencialidade dos dados e sistemas da MOSTEN.

- Procedimentos Específicos: Implementação do Plano de Resposta a Incidentes de Segurança da Informação, isolamento de sistemas comprometidos, restauração de backups seguros, comunicação com autoridades e stakeholders relevantes.

2.5.3. Desastres Causados por Humanos:

São eventos resultantes de ações humanas, que podem ser não intencionais ou maliciosas. Exemplos incluem:

- Não Maliciosos: Erros humanos (falhas em procedimentos operacionais), acidentes (incêndios, vazamentos, explosões), interrupção prolongada de serviços essenciais (energia elétrica, água, telecomunicações por parte de fornecedores).
    - Procedimentos Específicos: Implementação de planos de emergência específicos (plano de combate a incêndio, plano de contenção de vazamentos), ativação de fornecedores alternativos (se aplicável), comunicação com fornecedores de serviços essenciais para obter informações sobre a restauração.
- Maliciosos: Ataques terroristas ou vandalismo, ações de insiders maliciosos (sabotagem, roubo de informações).
    - Procedimentos Específicos: Acionamento de protocolos de segurança, comunicação com autoridades policiais, avaliação de danos e impacto nas operações, implementação de medidas de segurança adicionais.

2.5.4. Outros Eventos Disruptivos:

Incluem eventos que não se enquadram nas categorias anteriores, mas que podem impactar significativamente as operações da MOSTEN. Exemplos incluem:

- Pandemias ou surtos de doenças: Que causem a ausência em massa de colaboradores.
    - Procedimentos Específicos: Implementação de políticas de trabalho remoto, medidas de higiene e segurança, planos de comunicação com colaboradores e clientes.

- Greves ou conflitos trabalhistas: Que impeçam o funcionamento normal das atividades.
    - Procedimentos Específicos: Desenvolvimento de planos de contingência para manter operações críticas com pessoal disponível, comunicação com sindicatos e colaboradores.

Para cada categoria de desastre, estratégias de continuidade mais detalhadas e planos de ação específicos serão desenvolvidos na Seção 4 deste PCN, levando em consideração os potenciais impactos e os recursos necessários para a recuperação.

2.6. DISPONIBILIDADE

Disponibilidade, no âmbito do PCN da MOSTEN, refere-se à capacidade dos serviços, sistemas, dados, infraestrutura e demais recursos críticos de estarem acessíveis e operacionais para atender às necessidades do negócio, conforme os níveis de serviço definidos. O foco da disponibilidade é garantir o acesso oportuno aos recursos necessários para a continuidade das operações durante e após uma interrupção. A disponibilidade será medida e monitorada através de métricas como tempo de uptime, tempo de downtime e o cumprimento dos Objetivos de Tempo de Recuperação (RTOs) estabelecidos para cada processo crítico. As estratégias de continuidade (Seção 4) visam maximizar a disponibilidade dos recursos essenciais em situações de crise.

2.7. CONFIABILIDADE

Confiabilidade, no contexto do PCN da MOSTEN, diz respeito à garantia de que os dados e sistemas recuperados e utilizados para a continuidade das operações serão precisos e consistentes ao longo do tempo. Enquanto a disponibilidade foca no acesso, a confiabilidade se concentra na qualidade e na validade das informações. Um sistema pode estar disponível, mas se os dados estiverem inconsistentes ou imprecisos, sua

confiabilidade estará comprometida. O PCN implementará processos robustos de backup e restauração, bem como verificações de integridade pós-recuperação, para assegurar a confiabilidade dos dados e sistemas essenciais.

2.8. INTEGRIDADE

Integridade, no âmbito do PCN da MOSTEN, refere-se à garantia de que os dados e sistemas permanecerão completos, precisos, consistentes e inalterados, protegidos contra modificações não autorizadas ou corrupção, tanto em condições normais quanto durante e após um evento de interrupção. A integridade complementa a confiabilidade, focando na proteção contra alterações indevidas. Medidas como controles de acesso rigorosos, trilhas de auditoria (logs), backups seguros e verificações de integridade serão implementadas para preservar a integridade dos ativos de informação críticos para a continuidade dos negócios.

Em resumo:

- Disponibilidade: Capacidade de acessar os recursos quando necessário.
- Confiabilidade: Garantia de que os dados e sistemas são precisos e consistentes.
- Integridade: Garantia de que os dados e sistemas não foram alterados indevidamente.

Esses três conceitos são interligados e essenciais para a efetividade do Plano de Continuidade de Negócios da MOSTEN, assegurando que, em caso de interrupção, a organização possa acessar recursos íntegros e confiáveis para manter suas operações críticas.

2.9. SOBREVIVÊNCIA

No contexto do Plano de Continuidade de Negócios (PCN) da MOSTEN, sobrevivência refere-se à capacidade da organização de manter um nível mínimo de

operações críticas aceitável após a ocorrência de um desastre ou interrupção significativa. Este conceito engloba a habilidade de continuar entregando produtos ou serviços essenciais, manter funções vitais e preservar a capacidade de retornar às operações normais dentro de um prazo razoável. A sobrevivência não implica necessariamente a manutenção de todas as operações em sua capacidade total, mas sim a priorização e sustentação das atividades mais cruciais para a continuidade do negócio e a mitigação de danos maiores.

A garantia da sobrevivência da MOSTEN após uma interrupção será buscada através de:

- Identificação e Priorização de Processos Críticos (BIA): A Análise de Impacto nos Negócios (BIA), mencionada na seção "PLANEJAMENTO DO PCN" (2.4), é fundamental para identificar os processos essenciais cuja continuidade é prioritária para a sobrevivência da organização.
- Desenvolvimento de Estratégias de Recuperação Mínimas: Para os processos críticos identificados, serão definidas estratégias de recuperação que permitam a operação em um nível mínimo aceitável, mesmo que com recursos limitados ou em um ambiente alternativo (como mencionado em "Contingência CPD Interna" na página 49).
- Alocação de Recursos Essenciais: O PCN deverá prever a alocação prioritária dos recursos disponíveis (financeiros, humanos, tecnológicos) para suportar a continuidade dos processos críticos durante a fase de sobrevivência.
- Planos de Comunicação de Crise: A capacidade de comunicar-se efetivamente com stakeholders (clientes, colaboradores, fornecedores, reguladores) durante e após uma interrupção é vital para manter a confiança e gerenciar a situação, contribuindo para a sobrevivência da organização.
- Foco na Recuperação Gradual: A fase de sobrevivência é transitória e visa estabilizar as operações críticas para, posteriormente, dar lugar a um processo de recuperação mais completo e ao retorno às operações normais.

O objetivo principal da dimensão de sobrevivência no PCN da MOSTEN é assegurar que,

mesmo diante de um evento adverso grave, a empresa possa continuar funcionando em um nível essencial, preservando sua capacidade de recuperação e seu futuro a longo prazo.

2.10. ABANDONO DE ÁREA

No contexto do Plano de Continuidade de Negócios (PCN) da MOSTEN, abandono de área refere-se à necessidade de evacuação total ou parcial de uma ou mais instalações da empresa devido a uma ameaça iminente ou à ocorrência de um evento perigoso que coloque em risco a segurança dos ocupantes ou a integridade dos ativos. Esta situação pode ser desencadeada por diversos fatores, como incêndios, explosões, vazamentos de substâncias perigosas, ameaças de bomba, desastres naturais (inundações severas, deslizamentos), ou ordens de autoridades competentes.

Os procedimentos específicos a serem seguidos em caso de abandono de área visam garantir a evacuação segura e ordenada de todas as pessoas presentes e, na medida do possível, a proteção dos ativos críticos. Estes procedimentos incluem:

- Reconhecimento da Necessidade de Abandono: A decisão de abandonar uma área pode ser tomada por diversos indivíduos, incluindo:
    - Membros da alta gestão da MOSTEN.
    - Responsáveis pela segurança patrimonial.
    - Líderes de brigada de emergência.
    - Autoridades competentes (Corpo de Bombeiros, Defesa Civil etc.).
    - Alertas automáticos de sistemas de detecção (incêndio, vazamento de gás etc.).
- Emissão do Alerta de Evacuação: Uma vez determinada a necessidade de abandono, um alarme sonoro e/ou visual será acionado (se disponível). Adicionalmente, a comunicação da ordem de evacuação será realizada através dos

canais de comunicação de emergência definidos (megafones, rádios comunicadores, mensagens de texto/aplicativos, conforme aplicável).

- Procedimentos de Evacuação: Ao ouvir o alarme ou receber a ordem de evacuação, todos os ocupantes da área afetada deverão:
    - Interromper imediatamente suas atividades.
    - Desligar equipamentos que possam representar riscos se deixados ligados (ex: máquinas com aquecimento, equipamentos elétricos não essenciais).
    - Seguir as rotas de fuga sinalizadas.
    - Auxiliar pessoas com mobilidade reduzida ou que necessitem de ajuda.
    - Não utilizar elevadores.
    - Dirigir-se aos pontos de encontro designados, localizados em áreas seguras e afastadas da instalação evacuada.
    - Manter a calma e evitar correria.
- Ponto de Encontro e Checagem: Ao chegar ao ponto de encontro, os evacuados deverão se apresentar aos responsáveis pela coordenação da emergência (brigadistas, membros do Comitê de Governança de Continuidade designados) para que seja realizada a contagem e a verificação de todos os presentes. Qualquer pessoa ausente deverá ser imediatamente reportada para que as equipes de resgate possam ser acionadas, se necessário.
- Controle de Acesso à Área Evacuada: Após a evacuação, o acesso à área abandonada será restrito apenas a pessoal autorizado (equipes de emergência, segurança) para avaliação da situação e realização das ações necessárias.
- Avaliação da Situação e Liberação da Área: Apenas após a avaliação da segurança da área pelas autoridades competentes e a emissão de um parecer favorável, a área poderá ser liberada para o retorno dos ocupantes. A comunicação da liberação será realizada através dos mesmos canais utilizados para o alerta de evacuação.
- Proteção de Ativos (Quando Seguro e Possível): Em situações em que houver

tempo e segurança para tal, funcionários designados poderão ser instruídos a realizar ações para proteger ativos críticos, como desligar equipamentos sensíveis ou cobrir materiais importantes, desde que isso não coloque em risco sua segurança pessoal.

A prioridade máxima em qualquer situação de abandono de área é a segurança e a integridade física de todas as pessoas. Os procedimentos aqui descritos visam garantir uma evacuação eficiente e segura, minimizando os riscos e facilitando a atuação das equipes de emergência.

2.11. SINISTRO

No contexto do Plano de Continuidade de Negócios (PCN) da MOSTEN, sinistro refere-se a um evento súbito e imprevisto que causa danos, perdas ou interrupções nas operações da empresa, podendo ter origem em diversas fontes, como falhas técnicas, acidentes, eventos naturais ou ações de terceiros. Embora possa haver sobreposição com o conceito de "desastre" (definido no item 2.5), o termo "sinistro" geralmente abrange uma gama mais ampla de eventos disruptivos, incluindo ocorrências de menor escala que ainda exigem uma resposta organizada para minimizar seus impactos.

A diferenciação entre sinistro e desastre pode residir na magnitude e na extensão dos impactos. Enquanto um desastre geralmente implica uma interrupção severa e generalizada das operações, um sinistro pode ser um evento mais localizado ou com impactos mais limitados, mas que ainda requer a ativação de procedimentos de resposta do PCN.

Os procedimentos gerais de resposta a um sinistro no âmbito do PCN da MOSTEN incluem:

- Identificação e Avaliação do Sinistro: O primeiro passo é identificar a ocorrência do sinistro, avaliar sua natureza, extensão e os potenciais impactos nas operações, nos ativos e nas pessoas. Esta avaliação inicial ajudará a determinar a necessidade de acionar o PCN e o nível de resposta requerido.

- Comunicação Inicial: Uma vez identificado e avaliado preliminarmente o sinistro, a informação deverá ser comunicada aos responsáveis designados, conforme a "Tabela de Acionamento Emergencial/ Contingência – Escalation" (mencionada na página 50). Esta comunicação inicial deve incluir detalhes sobre o evento, sua localização e os impactos observados.
- Acionamento do Plano de Resposta (se necessário): Com base na avaliação do sinistro, o Comitê de Segurança (ou os responsáveis designados) determinará se é necessário acionar procedimentos específicos do PCN. O critério para acionamento dependerá da gravidade do sinistro e de seu potencial para interromper processos críticos. O processo de acionamento do Comitê de Segurança está detalhado no item 2.1.
- Implementação das Estratégias de Continuidade Relevantes: Uma vez acionado o plano de resposta, as estratégias de continuidade predefinidas para o tipo de sinistro ocorrido serão implementadas. Estas estratégias podem envolver a ativação de backups, a transferência de operações para locais alternativos (conforme mencionado em "Contingência CPD Interna" na página 49), a comunicação com stakeholders, a mobilização de equipes de recuperação, entre outras ações. As "ESTRATÉGIAS DE CONTINUIDADE" serão detalhadas em uma seção posterior deste documento (Seção 6, conforme análise inicial).
- Gerenciamento da Crise: Durante a resposta ao sinistro, será estabelecida uma estrutura de gerenciamento de crise para coordenar as ações, comunicar informações atualizadas, tomar decisões e alocar recursos de forma eficaz.
- Recuperação e Restauração: Após a contenção do sinistro, o foco se voltará para a recuperação das operações afetadas e a restauração das condições normais de funcionamento, seguindo os planos de recuperação definidos.
- Análise Pós-Sinistro: Após a resolução do sinistro e a retomada das operações normais, será realizada uma análise para identificar as causas do evento, avaliar a eficácia da resposta implementada e identificar oportunidades de melhoria no PCN e nos procedimentos de prevenção.

Em resumo, o tratamento de um sinistro no âmbito do PCN da MOSTEN envolve um processo de identificação, avaliação, comunicação, acionamento (se necessário), implementação de estratégias, gerenciamento da crise, recuperação e análise pós-evento, visando minimizar os impactos e fortalecer a resiliência da organização.

2.12. COMITÊ EXECUTIVO

O Comitê Executivo é responsável pela aprovação de alto nível e pelo suporte estratégico ao PCN. Suas responsabilidades incluem:

- Aprovar a política de continuidade de negócios e garantir que ela esteja alinhada com os objetivos estratégicos da MOSTEN.
- Designar os recursos financeiros, humanos e tecnológicos necessários para o desenvolvimento, implementação e manutenção do PCN.
- Receber relatórios periódicos do Comitê de Governança de Continuidade sobre o status do PCN, os resultados de testes e simulações, e os riscos identificados.
- Fornecer diretrizes e apoio para a superação de obstáculos e a implementação de melhorias no PCN.

2.13. COMITÊ DE AUDITORIA

O Comitê de Auditoria exerce uma função de supervisão independente sobre o PCN. Suas responsabilidades incluem:

- Avaliar a adequação e a eficácia do PCN em relação aos riscos de continuidade dos negócios identificados.
- Verificar a conformidade do PCN com as políticas internas, regulamentações e melhores práticas de mercado.
- Analisar os resultados dos testes e simulações do PCN e as ações corretivas implementadas.

- Reportar suas conclusões e recomendações ao Comitê Executivo e ao Comitê de Governança de Continuidade.

2.14. COMITÊ DE CONTINGENCIAMENTO E SEGURANÇA DA INFORMAÇÃO (CCSI)

O CCSI tem um papel operacional e técnico fundamental no desenvolvimento e na implementação do PCN, com foco específico na tecnologia da informação e segurança da informação. Suas responsabilidades incluem:

- Participar da Análise de Impacto nos Negócios (BIA) para identificar os processos críticos e seus requisitos de tecnologia e segurança.
- Desenvolver e implementar as estratégias de continuidade relacionadas à infraestrutura de TI, sistemas, dados e segurança da informação.
- Definir e manter os planos de recuperação de desastres de TI.
- Implementar e gerenciar as soluções de backup e restauração.
- Garantir a segurança lógica e física do site de contingência (se aplicável).
- Participar do planejamento e execução dos testes e simulações do PCN, com foco nos aspectos de TI e segurança.
- Responder a incidentes de segurança da informação que possam impactar a continuidade dos negócios.
- Fornecer suporte técnico durante a ativação e execução do PCN.

2.15. COMITÊ DE RISCO

O Comitê de Risco tem a responsabilidade de identificar, avaliar e monitorar os riscos que podem afetar a continuidade dos negócios da MOSTEN. Suas responsabilidades incluem:

- Participar da Análise de Impacto nos Negócios (BIA) para identificar e avaliar os riscos de interrupção dos processos críticos.
- Contribuir para o desenvolvimento das estratégias de continuidade, garantindo que os riscos identificados sejam adequadamente mitigados.
- Monitorar o ambiente de riscos e alertar o Comitê de Governança de Continuidade sobre novas ameaças ou mudanças nos riscos existentes.
- Avaliar a adequação das medidas de continuidade em relação ao perfil de risco da MOSTEN.
- Colaborar com o CCSI e outras áreas para garantir a integração da gestão de riscos com o planejamento da continuidade.

A coordenação e a comunicação eficaz entre esses comitês, juntamente com o Comitê de Governança de Continuidade (conforme proposto anteriormente), são essenciais para garantir uma abordagem abrangente e bem-sucedida para a continuidade dos negócios na MOSTEN.

2.16. GERENCIAMENTO DE FACILIDADES

Formada pela equipe de Gerentes e tem como responsabilidade as simulações e treinamentoda equipe para processos de contingenciamento, bem como o acionamento dos Analistas e Operadores, contribuindo para que as informações sejam repassadas a quem de direito de forma filtrada. Deverá também, ter relação completa e atualizada do Mapa de Relacionamentos.

2.17. HELPDESK/SERVICE DESK

Constituído pela equipe de Suporte (acionamento de 1º nível) localizados no site e terão como responsabilidade manter contato com as áreas técnicas necessárias da Empresa,

Cliente, Fornecedores e Parceiros; bem como acionamentos de níveis acima da equipe interna de TI e de demais áreas, informando imediatamente qualquer sinistro seja ele total, parcial ou de qualquer anormalidade que interfira no processo de atendimento, permitindo o início do PCN após autorização da equipe de CCSI.

2.18. PONTO FOCAL NA MOSTEN

O ponto de Contato será indicado pela MOSTEN e terá como responsabilidade manter a documentação necessária permitindo a inter-relação de informações para correto contingenciamento dos recursos necessários à disponibilidade.

2.19. SITE DE CONTINGENCIAMENTO

O site a ser utilizado será definido quando o PCN for ativado pelo Comitê Executivo, após análise da situação em que se encontra o ambiente.

2.20. TESTES

A realização de testes periódicos é fundamental para validar a eficácia do Plano de Continuidade de Negócios (PCN) da MOSTEN e garantir que a organização esteja preparada para responder e se recuperar de interrupções. Os testes permitirão identificar lacunas no plano, avaliar a capacidade da equipe de resposta e garantir que os Objetivos de Tempo de Recuperação (RTOs) e Objetivos de Ponto de Recuperação (RPOs) possam ser atendidos.

Tipos de Testes:

A MOSTEN poderá realizar diferentes tipos de testes do PCN, incluindo:

- Testes de Mesa (Tabletop Exercises): Simulações de cenários de interrupção em um ambiente de discussão, envolvendo os membros do Comitê de Governança de

Continuidade e outras partes interessadas para revisar os planos e procedimentos.

- Testes de Caminhada (Walkthrough Tests): Revisão passo a passo dos planos de ação, verificando a clareza dos procedimentos, a disponibilidade dos recursos e a compreensão das responsabilidades.
- Testes Funcionais (Functional Tests): Simulação da falha de um sistema ou processo específico para verificar a ativação e a eficácia dos procedimentos de recuperação correspondentes (ex: teste de restauração de backup, teste de failover de um servidor).
- Testes de Simulação Completa (Full-Scale Simulations): Simulação abrangente de um cenário de desastre, envolvendo a ativação do plano de continuidade em um ambiente o mais próximo possível da realidade, testando a coordenação entre diferentes equipes e a eficácia das estratégias de recuperação.

Cronograma de Testes:

Para garantir a validação contínua do PCN, será estabelecido o seguinte cronograma de testes:

- Testes de Mesa: Serão realizados anualmente, com o objetivo de revisar os planos, discutir cenários e garantir a compreensão dos procedimentos por parte das equipes envolvidas. O Comitê de Governança de Continuidade será o principal responsável pela organização e condução desses testes.
- Testes de Caminhada: Serão realizados semestralmente, focando em planos de ação específicos e envolvendo as equipes diretamente responsáveis pela sua execução. Os responsáveis pela elaboração e manutenção de cada plano de ação serão responsáveis pela organização e condução dos testes de caminhada para suas respectivas áreas.
- Testes Funcionais: Serão realizados anualmente para os sistemas e processos críticos identificados na Análise de Impacto nos Negócios (BIA). A área de Tecnologia da Informação (TI), em colaboração com os responsáveis pelas áreas de negócio, será responsável pelo planejamento e execução desses testes. Diferentes sistemas e processos críticos poderão ser testados em diferentes momentos ao longo do ano.

- Testes de Simulação Completa: Serão realizados a cada dois anos, com o objetivo de testar a resposta coordenada da organização a um cenário de interrupção significativo. O Comitê de Governança de Continuidade, com o apoio de todas as áreas relevantes, será responsável pelo planejamento, execução e avaliação desses testes.

O cronograma específico de cada teste será definido e comunicado com antecedência. Os resultados de todos os testes serão documentados, incluindo as lições aprendidas e as ações de melhoria identificadas, que serão incorporadas à revisão e atualização do PCN.

Tipo de Teste	Responsável Principal	Responsáveis de Apoio
Testes de Mesa	Comitê de Governança de Continuidade	Todas as áreas relevantes
Testes de Caminhada	Responsáveis pela elaboração e manutenção dos planos	Equipes diretamente envolvidas na execução dos planos
Testes Funcionais	Tecnologia da Informação (TI)	Responsáveis pelas áreas de negócio dos sistemas/processos testados
Testes de Simulação Completa	Comitê de Governança de Continuidade	Todas as áreas da MOSTEN, Ponto Focal do PCN, Equipes de Resposta

Este cronograma e a atribuição de responsabilidades visam garantir que o PCN seja testado de forma abrangente e regular, mantendo sua relevância e eficácia para a continuidade dos negócios da MOSTEN.

3. CENÁRIO DE INFRAESTRUTURA

3.1. ENERGIA ELÉTRICA

A MOSTEN não possui no atual modelo de gestão a existência de um *Data Center*, porem possui equipamentos de contingência elétrica abastecida por baterias "*no-break*" para atender a Infraestrutura contratada.

- Cenário de Interrupção: Falha total ou parcial no fornecimento de energia elétrica da concessionária.
- Procedimentos de Resposta e Estratégias de Continuidade (Referência à Seção

4):

- Ativação de sistemas de alimentação ininterrupta (UPS) para manter a energia de equipamentos críticos por um período limitado (Estratégia de Continuidade para Falha de Energia).
- Acionamento de geradores de energia para fornecer energia de backup para sistemas essenciais durante interrupções prolongadas (Estratégia de Continuidade para Falha de Energia).
- Implementação de procedimentos de desligamento seguro de equipamentos não essenciais para preservar a autonomia das fontes de energia alternativas.

3.1.1. PONTO DE ACESSO ELÉTRICO

As Instalações possuem pontos elétricos de 110v ou 220v na sua maioria, obedecendo ao novopadrão brasileiro de tomadas de acordo com a norma NBR 14.136.

3.2. ESCADA E EXTINTORES DE INCÊNDIO

O acesso ao site da MOSTEN disponibiliza escada de incêndio com portas anti chamas e iluminação de emergência em todos os andares com extintores adequados, distribuídos em locais estratégicos.

- Cenário de Interrupção: Bloqueio de rotas de fuga primárias, número insuficiente de extintores em caso de incêndio.
- Procedimentos de Resposta e Estratégias de Continuidade (Referência à Seção 4):
  - Utilização de rotas de fuga alternativas sinalizadas (Estratégia de Continuidade para Abandono de Área).

- Acionamento da Brigada de Incêndio para combate inicial e orientação (Procedimentos de Resposta a Sinistros e Abandono de Área).
- Evacuação da área afetada para os pontos de encontro designados (Estratégia de Continuidade para Abandono de Área).

3.2.1. EQUIPE DE BRIGADA DE INCÊNDIO TREINADA/SOCORRISTAS TREINADA

Possuímos estrutura de pessoas alinhadas com as definições da CIPA e realizamos treinamentos periódicos.

- Cenário de Interrupção: Indisponibilidade da equipe de brigada em caso de emergência.
- Procedimentos de Resposta e Estratégias de Continuidade (Referência à Seção 4):
  - Acionamento de socorro externo (Corpo de Bombeiros) conforme os procedimentos de emergência (Procedimentos de Resposta a Sinistros).
  - Designação de colaboradores alternativos treinados (se aplicável e conforme planos de treinamento).

3.3. AR-CONDICIONADO

O site da MOSTEN utiliza equipamentos de ar-condicionado compatíveis com as necessidades técnicas operacionais bem como visando atender as normas de conforto estabelecidas na NR-17.

- Cenário de Interrupção: Falha no sistema de ar-condicionado, especialmente em áreas críticas como o CPD.
- Procedimentos de Resposta e Estratégias de Continuidade (Referência à Seção

4):

- Monitoramento da temperatura em áreas críticas e implementação de medidas para evitar superaquecimento (ex: ventilação alternativa, desligamento temporário de equipamentos não essenciais).
- Ativação de sites de contingência com infraestrutura adequada (se a falha for prolongada e impactar a operação de sistemas críticos - Estratégia de Continuidade para Indisponibilidade do CPD).

3.4. SISTEMA DE SEGURANÇA

O sistema de segurança da MOSTEN abrange um conjunto de procedimentos e controles destinados a proteger suas instalações, ativos físicos e sistemas de informação contra acessos não autorizados. Em um cenário de infraestrutura, especialmente durante uma contingência, a manutenção da segurança é primordial para garantir a integridade das operações e a proteção de informações sensíveis.

3.4.1. Procedimentos de Segurança – Controle de Acesso Físico

Os procedimentos de controle de acesso físico visam restringir a entrada às instalações da MOSTEN a pessoal autorizado, especialmente em situações de normalidade e, de forma reforçada, durante um cenário de contingência. Estes procedimentos incluem:

- Identificação e Credenciamento: Todos os colaboradores, visitantes e prestadores de serviço devem ser devidamente identificados e, quando aplicável, possuir credenciais de acesso válidas (e.g., crachás de identificação com foto, cartões de acesso magnéticos).
- Registro de Acesso: O acesso às instalações será registrado por meio de sistemas automatizados (e.g., catracas eletrônicas, leitores de cartão) ou por registros

manuais, incluindo a identificação da pessoa, a data e a hora de entrada e saída.

- Níveis de Acesso: Serão definidos diferentes níveis de acesso às áreas das instalações, com base nas responsabilidades e na necessidade de cada indivíduo. As credenciais de acesso serão configuradas de acordo com esses níveis.
- Monitoramento de Segurança: As instalações serão monitoradas por câmeras de segurança e, quando aplicável, por vigilância física, 24 horas por dia, 7 dias por semana.
- Procedimentos em Caso de Alarme: Em caso de disparo de alarmes de segurança, procedimentos específicos serão seguidos para verificação da ocorrência e resposta adequada.
- Controle de Acesso em Cenário de Contingência: Em caso de ativação do PCN e possível necessidade de operar em locais alternativos ou com equipes reduzidas, os procedimentos de controle de acesso físico serão revisados e reforçados para garantir a segurança das áreas críticas e evitar acessos não autorizados. Isso pode incluir a restrição ainda maior do acesso e a intensificação do monitoramento.
- Cenário de Interrupção: Falha no sistema de controle de acesso, necessidade de acesso emergencial durante uma interrupção.
- Procedimentos de Resposta e Estratégias de Continuidade (Referência à Seção 4):
    - Implementação de procedimentos manuais de controle de acesso (listas de acesso autorizadas, identificação visual).
    - Acionamento da segurança patrimonial para controle e monitoramento (Procedimentos de Resposta a Sinistros e Emergências).

3.4.2. Procedimentos de Segurança – Controle de Acesso Lógico

Os procedimentos de controle de acesso lógico visam proteger os sistemas de

informação, as redes e os dados da MOSTEN contra acessos não autorizados. Estes procedimentos incluem:

- Autenticação de Usuários: O acesso aos sistemas e às aplicações será protegido por mecanismos de autenticação robustos, como senhas complexas, autenticação de múltiplos fatores (MFA) e/ou biometria.
- Gerenciamento de Identidades e Acessos (IAM): Será implementado um sistema de IAM para gerenciar as identidades digitais dos usuários, os direitos de acesso e os privilégios em todos os sistemas e aplicações.
- Políticas de Senhas: Serão estabelecidas políticas de senhas claras e rigorosas, incluindo requisitos de complexidade, periodicidade de troca e proibição de reutilização.
- Controle de Acesso Baseado em Funções (RBAC): O acesso aos recursos de TI será concedido com base nas funções e responsabilidades de cada usuário, seguindo o princípio do menor privilégio necessário.
- Monitoramento de Acessos e Auditoria: Os acessos aos sistemas e as atividades dos usuários serão monitorados e registrados em logs de auditoria para detecção de atividades suspeitas ou não autorizadas.
- Segurança de Redes: Serão implementadas medidas de segurança de rede, como firewalls, sistemas de detecção e prevenção de intrusão (IDS/IPS) e segmentação de rede, para proteger o ambiente de TI contra ameaças externas e internas.
- Controle de Acesso em Cenário de Contingência: Em caso de ativação do PCN e possível necessidade de acesso remoto aos sistemas ou operação em infraestruturas alternativas, os procedimentos de controle de acesso lógico serão revisados e reforçados para garantir a segurança dos dados e sistemas. Isso pode incluir a exigência de VPNs (Redes Virtuais Privadas) seguras e a intensificação do monitoramento de acessos remotos.
- Cenário de Interrupção: Falha nos sistemas de autenticação, necessidade de acesso a sistemas críticos durante uma interrupção.

- Procedimentos de Resposta e Estratégias de Continuidade (Referência à Seção 4):
    - Utilização de contas de acesso de emergência predefinidas e seguras (Procedimentos de Recuperação de Desastres de TI).
    - Implementação de procedimentos alternativos de autenticação, se disponíveis e seguros.

Ao vincular cada cenário de infraestrutura e tecnologia aos procedimentos de resposta e às estratégias de continuidade correspondentes, esta seção se torna mais prática e orientada para a ação, facilitando a implementação do PCN em caso de interrupção. A Seção 4 (Estratégias de Continuidade do PCN) deverá conter o detalhamento das ações mencionadas aqui.

A aderência a estes procedimentos de segurança – controle de acesso físico e lógico – é responsabilidade de todos os colaboradores e partes interessadas da MOSTEN, contribuindo para a proteção dos ativos e a garantia da continuidade dos negócios.

4. CENÁRIO DE TECNOLOGIA

4.1. ESTRUTURA NETWORK E COMUNICAÇÃO DE DADOS

A infraestrutura de rede é formada por cabeamento estruturado para ambiente deservidores;

- Os racks de servidores e equipamentos de redes (exemplo: roteadores, switches, DIO) possuem redundância elétrica, de acordo com as normas dos órgãos responsáveis.
- Todos os racks possuem patch painel espelhado que viabiliza uma melhor organização e um melhor desempenho da infraestrutura.
- Toda a Infraestrutura de comunicação LAN e WAN é padronizada, onde os acessos

pela WAN são estabelecidos através do uso de diferentes operadoras, havendo ponto de presença das principais empresas de telecomunicação. Utilizamos um sistema de gerenciamento de rede para monitoramento dos principais componentes (Roteador, Servidor, Link etc.);

- A rede é segregada logicamente por VLANs, gerenciadas pelo firewall e pelo switch Core;
- Todas as portas de acesso são configuradas na velocidade 100FULL-Duplex;
- Todas as portas de distribuição e fibras são configuradas na velocidade 1000FULL-Duplex;
- Todas as portas de servidores são configuradas na velocidade 1000FULL-Duplex;

4.2. SUPORTE TÉCNICO E OPERAÇÕES EM CENÁRIO DE CONTINGÊNCIA

Em um cenário de contingência tecnológica, a continuidade do suporte técnico e das operações de TI é fundamental para a recuperação dos sistemas e a manutenção das funções de negócios críticas da MOSTEN. Esta seção detalha os procedimentos e as responsabilidades para garantir o suporte técnico e a operação dos sistemas de informação durante uma interrupção.

4.2.1. SEGURANÇA, BACKUP E RECUPERAÇÃO DE DADOS EM CENÁRIO DE CONTINGÊNCIA

A segurança dos dados é uma prioridade fundamental para a MOSTEN, especialmente em cenários de interrupção tecnológica. Esta seção detalha os procedimentos de backup, recuperação e proteção de dados, em estrito alinhamento com a "POLÍTICA DE DESCARTE DE MÍDIAS" da MOSTEN, para garantir a integridade, a confidencialidade e a disponibilidade das informações críticas durante uma contingência.

4.2.1.1. Procedimentos de Backup:

A MOSTEN mantém uma estratégia de backup robusta para garantir a possibilidade de

recuperação dos dados em caso de falha de sistemas, desastres ou outros eventos disruptivos. Os procedimentos de backup incluem:

- Identificação dos Dados Críticos: Os dados essenciais para a continuidade dos processos de negócios da MOSTEN são identificados e priorizados para backup regular.
- Frequência dos Backups: A frequência dos backups é definida com base nos Objetivos de Ponto de Recuperação (RPOs) estabelecidos para cada tipo de dado, garantindo a mínima perda de informações possível.
- Tipos de Backup: Serão utilizados diferentes tipos de backup (e.g., completo, diferencial, incremental) conforme a necessidade e a infraestrutura disponível, buscando otimizar o tempo de backup e o espaço de armazenamento.
- Armazenamento dos Backups: Os backups são armazenados eletronicamente e uma cópia é enviada sob controle de protocolo para um Site alternativo seguro, conforme especificado na "POLÍTICA DE DESCARTE DE MÍDIAS". O acesso aos backups é restrito e controlado pela área de Tecnologia e Suporte.
- Monitoramento dos Backups: O processo de backup é monitorado regularmente para garantir sua conclusão bem-sucedida e a integridade dos arquivos de backup. Falhas no processo de backup são tratadas imediatamente.

4.2.1.2. Procedimentos de Recuperação de Dados:

Em caso de perda de dados devido a uma interrupção, serão seguidos os seguintes procedimentos de recuperação:

- Avaliação da Perda de Dados: A extensão da perda de dados e o impacto nos processos de negócios serão avaliados para determinar a estratégia de recuperação mais adequada.
- Seleção do Ponto de Recuperação: Com base nos RPOs definidos e na disponibilidade dos backups, será selecionado o ponto de recuperação mais apropriado para restaurar os dados.
- Execução da Restauração: A restauração dos dados será realizada pela equipe de

Tecnologia e Suporte, seguindo os procedimentos documentados e garantindo a integridade dos dados restaurados.

- Verificação da Integridade dos Dados Restaurados: Após a restauração, a integridade dos dados será verificada por meio de comparações com registros anteriores e testes de funcionalidade dos sistemas.
- Teste de Recuperação (Simulado): Periodicamente, serão realizados testes de recuperação simulados para validar a eficácia dos procedimentos de backup e restauração e para garantir que os tempos de recuperação (RTOs) possam ser atendidos.

4.2.1.3. Proteção de Dados em Cenários de Interrupção:

Durante uma interrupção tecnológica, a proteção dos dados continua sendo uma prioridade. As medidas de proteção de dados em cenários de contingência incluem:

- Controles de Acesso Reforçados: Os controles de acesso aos sistemas e dados no ambiente de contingência serão revisados e, se necessário, reforçados para evitar acessos não autorizados.
- Comunicação Segura: A comunicação envolvendo informações sensíveis durante a contingência será realizada por meio de canais seguros e criptografados, quando aplicável.
- Conscientização sobre Segurança: Serão reforçadas as orientações aos colaboradores sobre a importância da segurança da informação e os cuidados a serem tomados durante a operação em um ambiente de contingência.
- Política de Descarte de Mídias: A "POLÍTICA DE DESCARTE DE MÍDIAS" será rigorosamente seguida para garantir a eliminação segura de qualquer mídia de armazenamento que não seja mais necessária, protegendo contra a exposição de informações confidenciais. A retenção dos backups obedecerá às regras de descarte estabelecidas na política, com um período de retenção de 05 anos.

A implementação e a aderência a estes procedimentos de segurança, backup e recuperação de dados são essenciais para garantir a resiliência tecnológica e a continuidade dos negócios da MOSTEN em caso de interrupção.

4.2.2. Suporte Técnico:

Durante uma contingência, o suporte técnico será essencial para auxiliar na resolução de problemas, na restauração de serviços e no apoio aos usuários que possam estar operando em ambientes alternativos ou com sistemas degradados. Os procedimentos de suporte técnico em cenário de contingência incluem:

- Ponto de Contato Central: Será definido um ponto de contato central para o recebimento de solicitações de suporte técnico relacionadas à contingência. Este ponto de contato será comunicado a todos os colaboradores no momento da ativação do PCN.
- Canais de Comunicação Alternativos: Caso os canais de comunicação usuais (e.g., e-mail, sistema de helpdesk) estejam indisponíveis, serão utilizados canais alternativos predefinidos (e.g., telefone, mensagens instantâneas em plataformas específicas) para o contato com o suporte técnico.
- Priorização de Incidentes: Os incidentes reportados durante a contingência serão priorizados com base no seu impacto nos processos de negócios críticos. Incidentes que afetem diretamente a continuidade das operações terão prioridade máxima.
- Equipes de Suporte Designadas: Serão designadas equipes de suporte técnico específicas para atuar durante a contingência. Estas equipes estarão familiarizadas com os planos de contingência e os procedimentos de recuperação.
- Documentação de Soluções: As soluções para os problemas identificados durante a contingência serão documentadas para referência futura e para auxiliar na restauração completa dos serviços.

- Escalada de Problemas: Serão definidos procedimentos claros para a escalada de problemas que não puderem ser resolvidos pelas equipes de suporte de primeiro nível.

4.2.3. Operações de TI:

A continuidade das operações de TI em um cenário de contingência envolverá a execução de procedimentos predefinidos para manter ou restaurar os sistemas e serviços críticos. Estes procedimentos incluem:

- Ativação do Site de Contingenciamento (se aplicável): Em caso de indisponibilidade do site principal, serão seguidos os procedimentos para a ativação e operação do site de contingenciamento, conforme detalhado na seção 2.19.
- Restauração de Backups: Serão executados os procedimentos de restauração de backups para recuperar dados e sistemas críticos, conforme a Política de Descarte de Mídias e os planos de recuperação específicos.
- Monitoramento dos Sistemas de Contingência: Os sistemas e serviços em operação no ambiente de contingência serão monitorados continuamente para garantir sua disponibilidade e desempenho.
- Gerenciamento da Infraestrutura de Contingência: Será realizado o gerenciamento da infraestrutura de TI no ambiente de contingência, incluindo servidores, redes e armazenamento.
- Comunicação sobre o Status dos Sistemas: Serão fornecidas atualizações regulares sobre o status dos sistemas e serviços em operação no ambiente de contingência para as partes interessadas.
- Retorno ao Ambiente de Produção: Após a resolução da interrupção no site principal, serão executados os procedimentos para o retorno seguro e controlado das operações ao ambiente de produção, incluindo a migração dos dados e a desativação do ambiente de contingência.

A eficácia do suporte técnico e das operações em cenário de contingência dependerá da adequada preparação, do treinamento das equipes e da clareza dos procedimentos definidos neste Plano de Continuidade de Negócios (PCN).

4.2.4. SEGURANÇA DE DADOS:

Segurança de Dados		Gerencia
FIREWALL	Possuímos o Firewall com Security Plus para garantir a segurança de dados docliente e da própria segurança tecnológica	MOSTEN
ANTIVÍRUS	Além do Firewall possuímos Antivírus em todos os equipamentos (Servidores e Estações de Trabalho). Possuímos recursos tecnológicos que permitem restrição a acesso a páginas *web* e acesso a conteúdo restrito, conforme acordado com cada um dos clientes.	

4.3. INFRAESTRUTURA DE ENERGIA EM CENÁRIO DE CONTINGÊNCIA

A disponibilidade contínua de energia elétrica é essencial para a operação da infraestrutura de tecnologia da MOSTEN, especialmente em cenários de contingência. Esta seção detalha os recursos e os procedimentos para mitigar os impactos de falhas de energia e garantir a continuidade das operações de TI.

4.3.1. Fontes de Energia Primária e Secundária:

- Energia Primária: A MOSTEN depende da rede pública de energia elétrica como sua principal fonte de alimentação.
- Fontes de Energia Secundária (Nobreaks - UPS): Para proteger os equipamentos críticos de TI contra interrupções breves de energia, flutuações e picos de tensão, a

MOSTEN utiliza Sistemas de Alimentação Ininterrupta (UPS) em áreas estratégicas, como o Centro de Processamento de Dados (CPD) e outras salas de equipamentos. Os UPS fornecem energia temporária, permitindo a continuidade das operações por um período limitado e possibilitando o desligamento seguro dos equipamentos em caso de falha prolongada da energia primária.

- Geradores de Energia (se aplicável): [Caso a MOSTEN possua geradores de energia, esta seção deve detalhar sua capacidade, localização, procedimentos de ativação, planos de manutenção e capacidade de fornecimento de energia para as áreas críticas em caso de falha prolongada da rede pública.]

4.3.2. Procedimentos de Resposta a Falhas de Energia:

Em caso de falha no fornecimento de energia elétrica, os seguintes procedimentos serão acionados:

- Detecção da Falha: A falha de energia será detectada por meio de alarmes dos sistemas UPS, monitoramento da infraestrutura ou relatos dos colaboradores.
- Verificação da Extensão da Falha: A equipe de Gerenciamento de Facilidades e/ou a equipe de Tecnologia e Suporte avaliará a extensão da falha (localizada ou generalizada) e a sua causa, se possível.
- Ativação dos UPS: Os sistemas UPS entrarão em operação automaticamente para fornecer energia aos equipamentos conectados. A duração da autonomia dos UPS será monitorada.
- Acionamento dos Geradores (se aplicável): [Se aplicável, os procedimentos para o acionamento manual ou automático dos geradores de energia serão iniciados, seguindo os protocolos estabelecidos. Isso incluirá a verificação do nível de combustível e a garantia de que as áreas críticas recebam energia.]
- Comunicação da Falha: A ocorrência da falha de energia e o status das fontes de energia secundária serão comunicados às equipes relevantes (e.g., CCSI, Comitê

Executivo, responsáveis pelas áreas de negócio impactadas) conforme o Plano de Comunicação de Crise.

- Priorização do Consumo de Energia: Durante uma falha prolongada, o consumo de energia será priorizado para os equipamentos e sistemas críticos para a continuidade dos negócios. Equipamentos não essenciais poderão ser desligados para preservar a autonomia dos UPS ou a capacidade dos geradores.
- Monitoramento da Situação: A situação do fornecimento de energia será monitorada continuamente, e serão mantidos contatos com a concessionária de energia (se a falha for externa) para obter informações sobre a previsão de restabelecimento.
- Desligamento Controlado (se necessário): Se a falha de energia persistir e a autonomia das fontes secundárias estiver se esgotando, serão seguidos os procedimentos para o desligamento controlado e seguro dos equipamentos de TI para evitar danos.
- Restauração da Energia Primária: Após o restabelecimento da energia primária, a equipe de Tecnologia e Suporte verificará a estabilidade do fornecimento e iniciará o processo de religamento dos equipamentos, seguindo uma ordem de prioridade predefinida.
- Verificação dos Sistemas: Após o religamento, os sistemas serão verificados para garantir seu funcionamento correto e a integridade dos dados.

4.3.3. Manutenção Preventiva:

A MOSTEN implementa um programa de manutenção preventiva para garantir a confiabilidade das fontes de energia secundária (UPS e geradores, se aplicável). Este programa inclui inspeções regulares, testes de funcionamento das baterias dos UPS e dos geradores, e a substituição de componentes conforme a necessidade.

- A adequada implementação destes procedimentos de resposta a falhas de energia

é crucial para minimizar o impacto de interrupções no fornecimento elétrico sobre a infraestrutura de tecnologia e a continuidade dos negócios da MOSTEN.

4.3.4. ENERGIA ELÉTRICA:

- Falha na alimentação pública;
- Falha no gerador;
- Falha no no-break;
- Pane elétrica por causas da natureza;

4.3.5. CONTROLE DE ACESSO:

- Falha na segurança;
- Falha no sistema CFTV;

4.3.6. PONTO DE ACESSO ELÉTRICO:

- Falha na fiação;
- PLUG com defeito ou com umidade;
- Rompimento do cabo;
- Ponto não alimentado;

4.3.7. NO-BREAK:

- Falha no hardware do equipamento;

- Falha no software do equipamento;

4.3.8. ESCADA E EXTINTORES DE INCÊNDIO:

- Falha por falta de vistoria e manutenção;

4.3.9. AR-CONDICIONADO:

- Falha por falta de vistoria e manutenção;

4.4. CENÁRIO DE RISCOS E AMEAÇAS: RH

4.4.1. GREVE:

- Paralisação em massa da categoria;
- Paralisação parcial da categoria;
- Vandalismo ao patrimônio por parte dos grevistas;
- Distúrbios civis e tumultos;

4.4.2. TRANSPORTE:

- Paralisação de ônibus;
- Paralisação de Trem;
- Paralisação de Metro.

Nota: É importante que os principais executivos das Diretorias e Recursos Humanos deemapoio e orientação aos gestores locais durante todo o movimento grevista.

4.5. CENÁRIO DE RISCOS E AMEAÇAS: TECNOLOGIA

4.5.1. Circuito:

- Causas da natureza (desastres naturais, terremotos, tempestades, tornados e furacões);
- Rompimento de fibra ótica;
- Roubo de cabos;
- Falha no conector do cabo do link;

- Falha na configuração do link;
- Lentidão no link com alto índice de perda de pacote;

4.5.2. Hardware:

- Causas da natureza;
- Imprudência de funcionário durante manutenção;
- Defeito de fabricação.

4.5.3. Software:

- Conflito de drives;
- Imprudência de funcionário durante manutenção;
- Corrompimento de arquivo de base de dados;
- Invasão por Crackers;
- Softwares maliciosos (Vírus, Spywares, Trojan Horse ("Cavalos de Tróia"), Worms e pode ser considerada *malware* uma aplicação legal que por uma falha de programação (intencional ou não) execute funções que se enquadrem na definição acima.

5. AUTORIDADES E RESPONSABILIDADES

PREMISSAS

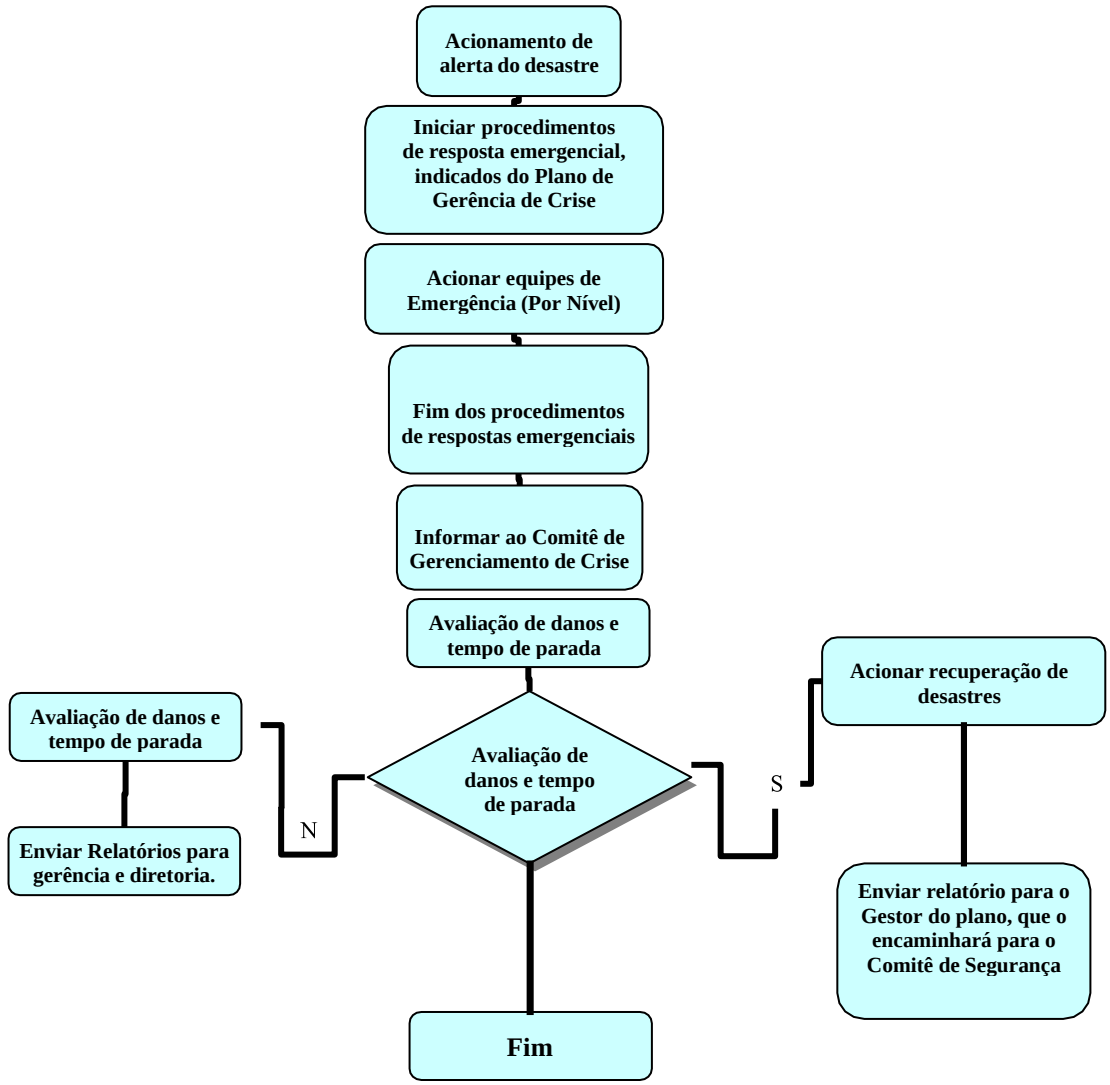
- Acionar o presente Plano de Contingência sempre que constatada qualquer informação sobre possibilidade de greve no transporte coletivo, que interfira no

trajeto / itinerário dos empregados, impedindo ou prejudicando sua chegada ao local de trabalho; problemas de infraestrutura e, ou de Tecnologia detectados pelo Suporte

Observações: O plano sempre será acionado pelo Comitê de Contingenciamento e Segurança da Informação (CCSI) e pelo Comitê de Risco (CR).

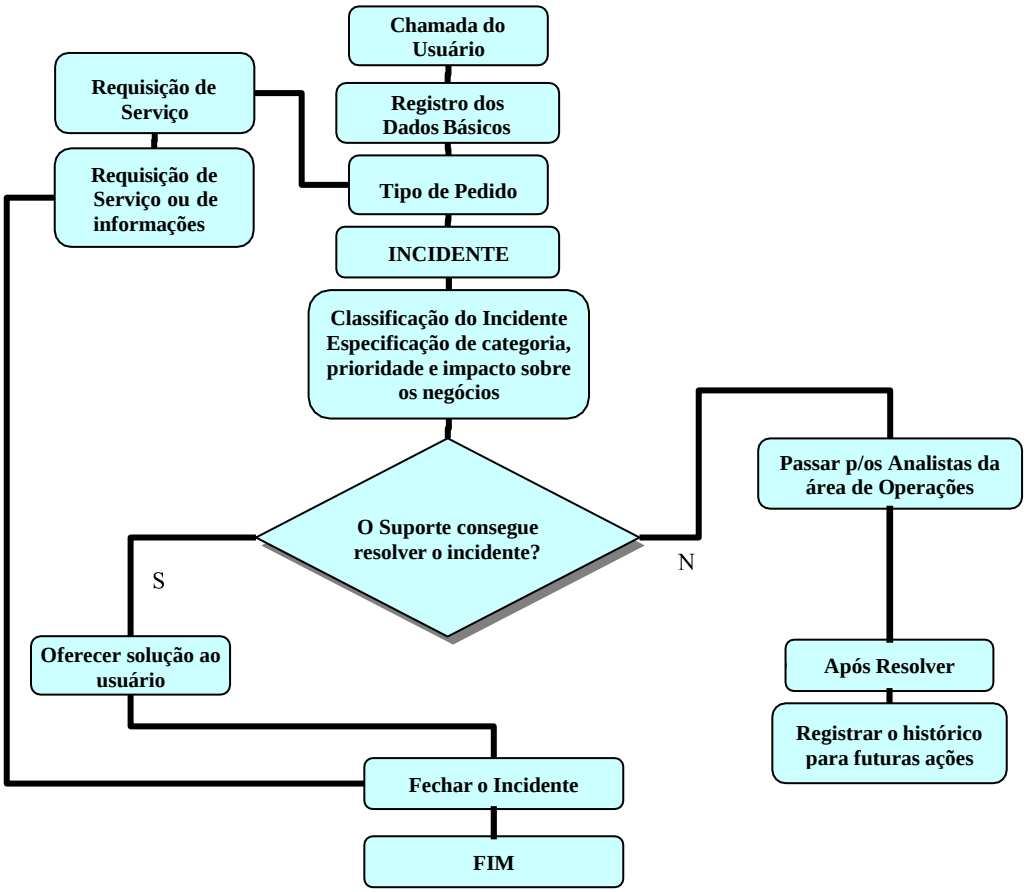
5.1 EXEMPLO DE CENÁRIO DE PCN MOSTEN: FLUXOGRAMAS

5.1.1 FLUXOGRAMA DE ACIONAMENTO DO PCN:

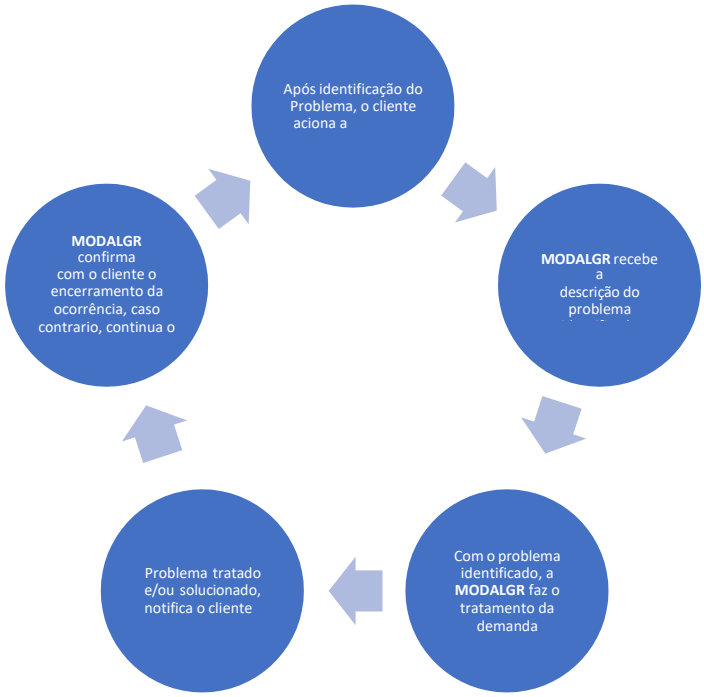


Plano de Continuidade de Negócios

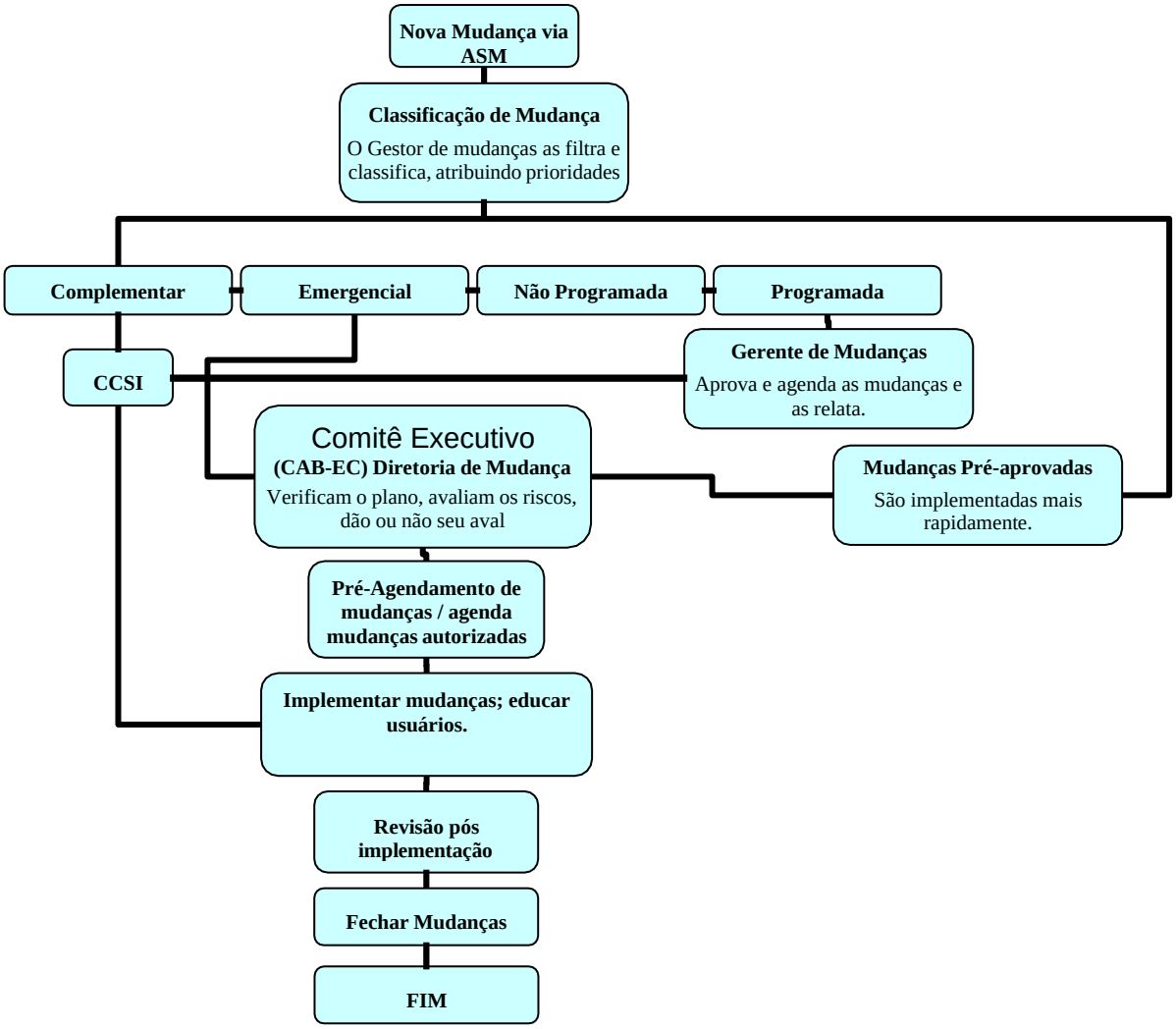
5.1.2. EXEMPLO DE FLUXOGRAMA EM CASOS DE INCIDENTES NO CLIENTE:



5.1.3. EXEMPLO DE FLUXOGRAMA EM CASOS DE PROBLEMA NO CLIENTE:



5.1.4. EXEMPLO DE FLUXOGRAMA DE GERENCIAMENTO DE MUDANÇAS NO CLIENTE:



5.2 EXEMPLO DE CENÁRIO DE PCN MOSTEN: INFRAESTRUTURA

5.2.1 PARA ENERGIA ELÉTRICA:

- No caso de pane elétrica que afete algum cliente, é ativado o PCN para o Cliente. O comitê executivo comunicará ao CLIENTE a situação atual e as medidas providenciadas para continuar a operabilidade do negócio. O CLIENTE tomará as devidas providências de "sinistro total" quando for aplicável ao mesmo.

5.2.2. INSTRUÇÕES DIRIGIDAS À INFRAESTRUTURA:

- Isolar a área de risco e evacuar imediatamente todos os andares;
- Controlar a entrada e saída constantemente;
- Análise dos pontos de melhoria e revisão de planejamento.

5.2.3. CENÁRIO DE PCN PARA PONTO DE ACESSO ELÉTRICO:

- Se ocorrer problemas em qualquer um dos pontos elétricos, através de abertura de chamado,imediatamente um técnico da Infraestrutura predial providenciará outro ponto elétrico de 110v na PA.

NOTA: Nosso ambiente obedece ao novo padrão brasileiro de tomadas de acordo com a normaNBR 14136

5.2.4. CENÁRIO DE PCN PARA NO-BREAK:

- Caso ocorrer falha no *no-break* do site imediatamente é acionada a equipe de Infraestruturapara realizar a manutenção ou troca imediata do no-break;

- No caso de não ter tempo hábil para troca ou manutenção no no-break, todo o negócio é direcionado para o site de contingência.

5.2.5. CENÁRIO DE PCN PARA ESCADA E EXTINTORES DE INCÊNDIO:

- A equipe de Infraestrutura realiza vistoria periódica nas escadas de incêndio, nas portasanti chamas e na iluminação de emergência;
- A equipe de Infraestrutura realiza vistoria periódica nos extintores de cada andar doedifício, distribuídos em locais estratégicos.

5.2.6. CENÁRIO DE PCN PARA EQUIPE DE BRIGADA:

- Primeiros Socorros: Os primeiros socorros serão prestados às eventuais vítimas conforme treinamento específico dado aos Brigadistas.
- Investigação: Após o controle total da emergência e a volta à normalidade, o Chefe da Brigada deve iniciar o processo de investigação e elaborar um relatório, por escrito,sobre o sinistro e as ações de controle, para as devidas providências.

(*) Possuímos equipe formada de brigada de incêndio;

5.2.7. CENÁRIO DE PCN PARA AR-CONDICIONADO:

- Quaisquer indisponibilidades de ar-condicionado no site que houver acionarão a Infraestrutura para realizar a devida manutenção.
- Caso a manutenção seja insuficiente para manter a operabilidade do negócio, direcionamos o negócio para o site de contingência que está munido de ar-condicionado nas condições ambientais conforme certificação e determinações oficiais.

NOTA: Possuímos equipamentos de ar-condicionado dedicados para atender 24x7 nosso CPD nas temperaturas ideais para manter a integridade dos equipamentos eletrônicos.

5.2.8. CENÁRIO DE PCN PARA CONTROLE DE ACESSO E MONITORAÇÃO CFTV:

- Conforme Procedimentos de Segurança – Controle de acesso aos sites

5.3 EXEMPLO DE CENÁRIO DE PCN MOSTEN: RH

5.3.1. CENÁRIO DE PCN PARA GREVE:

a) Comunicação pública: Interna e Externa:

- Comitê definido para redigir e distribuir rapidamente os comunicados:
  - Departamento de Recursos Humanos;
  - Gerência de Relações Trabalhistas e Sindicais;

b) Conteúdo do comunicado:

- Esclarecer de forma clara e objetiva o porquê a empresa considera o movimento abusivo;
- Explicar a posição da empresa;
- Definir o tratamento para os dias de greve.

Importante: Manter coerência do discurso oral ou escrito, o que se fala para os empregadosse fala para clientes, sindicatos, governo, mídia etc.

c) Ações junto à chefia / Gerência e Empregados-Chave (Operação e RH):

- Reunir a todos para orientar e avaliar o cenário;
- Definir local para reunião com o grupo;
- Orientar para chegar ao trabalho 2 (duas) horas antes do início do expediente;
- Orientar todos a manter a calma;
- Manter atualizada a lista com nº de telefones, e-mail e local onde os principaisgestores e executivos poderão ser encontrados;
- Distribuir a lista acima aos gestores envolvidos para ocasião de ameaça de paralisação;
- Orientar a todos os empregados para evitar confronto e tentar entrar para o trabalhoem outro horário etc.

d) Durante Eventuais Paralisações:

- Ações em caso de impedimento de entrada e distúrbios:
  - Solicitar intervenção policial registrando o BO (Boletim de Ocorrência);
  - Comunicar imediatamente as pessoas abaixo:
    - Infraestrutura;
    - Tecnologia e Processos;
    - Operações;
    - RH;

e) Comunicado Público Interno:

- Situação do movimento;
- Posição da Empresa;

- Pedir a volta ao trabalho;
- Definir tratamento durante os dias de greve;

f) Abordagem por Veículos de Mídia e Imprensa em Geral:

- Em qualquer abordagem por veículos de mídia / imprensa em geral, não prestar nenhuma informação / entrevista, e pedir ao demandante que entre em contato comnossa Diretoria.

g) Acompanhamento do Movimento:

- Reunir diariamente o grupo para avaliação e orientação;
- Reforçar medidas anteriores;
- Reforçar a comunicação;
- Controlar as ausências;

h) Após Eventuais Paralisações:

- Balanço do movimento;
- Resultados;
- Tratamento dos dias parados.

i) Coordenação, Gerência e Pessoas Chave:

- Avaliação sobre o movimento;
- Orientar para não retaliar, perseguir e não provocar empregados que tenham participado do movimento;
- Não enaltecer ou premiar os que não participaram.

j) Diretoria de RH e Operações:

- Análise da avaliação sobre o movimento;
- Mapear riscos de nova paralisação;
- Estratégias para evitar outro movimento;
- Cumprimento dos itens de pauta de negociações.

5.3.2. CENÁRIO DE PCN PARA TRANSPORTE:

a) Paralisação de Trem, Metrô ou Ônibus:

- Em caso de paralisação do sistema de transporte público (ônibus, metrô ou trem), o plano de contingência poderá, mediante acordo entre as partes, disponibilizar conforme a necessidade transporte em pontos estratégicos para buscar e levar os colaboradores.
- Com base no banco de dados, será identificada a localidade (Bairro e/ou Zona), que se concentra o maior número de colaboradores, para disponibilização do transporte alternativo até nosso site.
- Desta forma as principais consequências na operação como a redução da equipe na linha de frente e a degradação do nível de serviços serão reduzidas.
- Disponibilização de Vans ou ônibus fretado para locais estratégicos de embarque até a empresa, as informações dos pontos de encontro são informadas aos colaboradores através envio de SMS ou discagens para números de telefones dos mesmos.
- Veiculação de informações das opções de serviços de apoio aos funcionários.

IMPORTANTE: É importante que os principais gestores da Operação, Suporte e RecursosHumanos deem apoio e orientação aos demais colaboradores durante todo o movimentode paralisação.

5.4 EXEMPLO DE CENÁRIO DE PCN MOSTEN: TECNOLÓGICO

5.4.1. CENÁRIO DE PCN PARA CIRCUITOS TECNOLÓGICOS:

- Substituição, ou realocação do circuito quando houver implicações de causas da natureza;
- Acionamento das concessionárias e, elas por sua vez, das autoridades competentes parainibir o roubo de cabos;
- Acionar a concessionária para testes e reconfiguração no link quando necessário;
- Implantação de novos links de contingência se houver necessidade;
- Acionar concessionária para análise da qualidade do link com equipamentos adequadossensíveis aos ruídos no link com alto índice de perda de pacote;

5.4.2. CENÁRIO DE PCN PARA HARDWARE:

- Reconfiguração no software do hardware;
- Realização de manutenção necessária;
- Realização de troca de hardware quando necessário conforme contrato;

5.4.3. CENÁRIO DE PCN PARA SOFTWARE:

- Reconfiguração ou reinstalação de software;
- Realização de manutenção nas licenças;
- Atualizar ou retornar a versão do software sempre que necessário;
- Desenvolver aplicação conforme demandas;

5.4.4. POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO:

- Conforme Procedimento de Segurança de informação.

5.5 EXEMPLO DE CENÁRIO DE PCN MOSTEN: ACIONAMENTOS

5.5.1. CENÁRIO DE PCN PARA ACIONAMENTOS:

Ver tabela de acionamento (*Escalation*)

- Procedimento para acionamento:
  - Registrar ocorrência e acionar equipe de 1º nível;
  - A equipe de 1º Nível registra chamado no ASM e acionará a equipe de 2º Nível;
  - A equipe de 2º Nível analisará a ocorrência e conforme necessidade acionará aequipe de 3º Nível;
  - A equipe de 3º Nível notificará o CCSI e acionará a diretoria;
  - A diretoria manterá informada em tempo real todas as equipes

ATENÇÃO:

- É importante que se acione conforme as instruções acima respeitando o nível do 1º nível até a diretoria, pois cada nível é quem irá filtrar as informações entre

incidentes e problemas e repassará ao nível superior conforme criticidade de SLA[1]das ocorrências.

- A tabela de escalation contempla todos os contatos necessários para acionamentos emergenciais, sendo assim é muito importante que cada gerente tenha consigo impressa uma cópia segura e de fácil acesso.

5.6 EXEMPLO DE CENÁRIO DE PCN MOSTEN: FERRAMENTAS

5.6.1. TELE-TRABALHO:

Nota: Por definição, Home Office ou teletrabalho, é a forma de trabalho realizada em lugar distante do escritório central e/ou centro de produção, que permite a separação física e que implique no uso de uma tecnologia facilitadora de comunicação. (Definição segundo a OIT – Organização Internacional do Trabalho). É obrigatório que o tele trabalhista assine concordandocom a ficha de contrato de teletrabalho.

Identifique em quais tarefas pode ser usado o Teletrabalho;

- Monte um "KIT DE TELE-TRABALHO":
  - Espaço físico seguro, homologado e aprovado pela empresa;
  - Mesa com iluminação adequada;
  - Cadeira ergonomicamente confortável;

[1] SLA é a sigla de *Service Level Agreement*, que significa "Acordo de Nível de Serviço - ANS", na tradução para o português. O SLA consiste num contrato entre duas partes: entre a entidade que pretende fornecer o serviço e ocliente que deseja se beneficiar deste.

- Net book/Notebook ou Desktop completo;
- Celular corporativo;
- Linha telefônica;
- Internet Banda Larga;

5.6.2. ESCRITÓRIO VIRTUAL:

- Consiste das seguintes informações:
  - Local alternativo de trabalho identificando aspectos de segurança, linhas telefônicas, equipamentos;
  - Comunicação e acionamentos emergenciais (vide tabela de Escalation);
  - Quais os meios de mobilidade disponíveis ao seu redor conforme orientação da Gerência/ Diretoria;
  - Identificar local virtual para disposição e dispersão de recursos (dados, arquivos e pessoal).

5.7 EXEMPLO DE CENÁRIO DE PCN MOSTEN: ACESSOS ON-LINE

5.7.1. ACESSO VIA WEB (EXTRANET):

- Utilização de chats e redes sociais (Somente será permitido em situações determinantes de impactos, com aprovação e controle da segurança de informação epor tempo definido por eles);

5.7.2. POLÍTICA DE USO DE INTERNET:

- Conforme procedimento de Segurança

5.7.3. INTRANET:

- Utilize os procedimentos publicados na intranet nos locais e sites disponíveis.

5.8 EXEMPLO DE CENÁRIO DE PCN MOSTEN: TREINAMENTO

5.8.1. DO TREINAMENTO TEÓRICO (por simulação virtual):

- INDIVIDUAIS:

Identificar e pôr em prática as responsabilidades de cada um, definidas para as emergências.

- PLANO ESCRITO TEÓRICO:
  - Contagem;
  - Evacuação;
  - Procedimento de resgate de feridos se necessário;
  - Descrever claramente tarefas de cada equipe;
  - Direcionar quem deve ser acionado;
  - Cada departamento deve nomear um líder para apoiar os integrantes do CCSI e aequipe de Infraestrutura na:
    a) Contagem dos funcionários;
    b) Evacuação organizada direcionando para a rota de fuga planejada;
    c) Montar um centro de comunicação eficaz contra boataria;

d) Manter a integridade no fluxo de informações;

5.8.2. DO TREINAMENTO PRÁTICO (por simulação real):

- Vide Programa de treinamento em situações de contingência;(*) Exercícios de campo;

5.9 EXEMPLO DE CENÁRIO DE PCN MOSTEN: ATIVAÇÃO DE CONTINGÊNCIA

5.9.1. ORIGEM:

Site da MOSTEN

5.9.2. MIGRAÇÃO:

Conforme Procedimento de Segurança

5.9.3. DESTINO:

(Outros sites definidos pelo Comitê Executivo)

5.9.4. QUEM TEM AUTORIDADE PARA ATIVAR O PLANO DE CONTINGÊNCIA?

Comitê de Contingenciamento e Segurança da Informação (CCSI)

5.9.5. QUAL É O MEDIDOR ANALISADO PARA ATIVAÇÃO?

- Conforme grau de risco definido na tabela de aspectos e impactos (Diretoria)

NOTA: O Plano de contingência só será ativado após análise do CCSI (Comitê de Contingenciamento e Segurança da Informação). Obedecendo ao critério do risco conforme Graude risco definido na Tabela de aspectos e impactos de SI.

5.9.6. COMO ACIONAR O CCSI E OS RESPONSÁVEIS DOS DEPARTAMENTOS?

- Ver tabela de Escalation publicada na Intranet;

NOTA: É de fundamental importância que esta tabela também se encontre impressa na guarda dos Gerentes e Coordenadores de cada área ou departamento.

5.9.7. TESTES DO PLANO DE CONTINGÊNCIA:

- Simular evacuação junto com equipe de bombeiros;
- Simular acionamentos externos de emergência;
- Simular ajuda médica de primeiros socorros;
- Simular serviços de fechamento das operações e realocações.

5.10. REVISÃO DO PLANO:

O Plano de contingência será revisto anualmente ou conforme necessidade apontada pela operação.

6 ANEXOS

6.1. Tabela de Acionamento Emergencial/ Contingência – Escalation

6.2. Plano central de atendimento Tabela de Aspectos e Impactos de SI – ASM

6.3. Ficha de Contrato de Teletrabalho – Recursos Humanos

Nota: Os documentos aqui destacado, não obrigatoriamente serão públicos em função de contatos pessoais.

7 REGISTROS DA QUALIDADE

7.1 ARMAZENAMENTO DO PLANO:

- O Plano de Continuidade de Negócios (PCN) tem sua sustentação básica composta pelos procedimentosde cópias de base de dados e a respectiva guarda destas cópias em local seguro.
- Em uma primeira abordagem, podemos distinguir entre dois tipos de arquivos: os arquivos de uso Corporativo e os arquivos de uso Pessoal. Independentemente do tipo de arquivo, sua cópia e a respectiva armazenagem desta cópia é uma exigência do Plano de Continuidade de Negócios (PCN), claro de acordo com a política de segurança estabelecida.

7.1.1 As cópias (backups) de todas as bases de dados corporativas devem ser feitas com a frequência que suas atualizações demandarem pela área gestora dos Recursos de Tecnologia de Informação.

7.1.2 A guarda deve ser feita em local seguro, com uma distância geográfica mínima que eviteque problemas nas instalações tenham repercussão no local de guarda das cópias (ou vice-versa).

7.1.3 Baseado na importância dos backups, pois guardam uma cópia fiel dos dados minutos, ouaté segundos, antes de um desastre, foram criadas diversas estratégias para o seu armazenamento, que são:

Estratégias	Atribuições
ContingênciaHot-Site	Recebe este nome por ser uma estratégia pronta para entrar em operação assim que uma situação de risco ocorrer. O tempo de operacionalização desta estratégia está diretamente ligado ao tempo de tolerância a falhas do objeto. Se a aplicássemos em um equipamento tecnológico, um servidor de banco de dados, por exemplo, estaríamos falando de milissegundos de tolerância para garantir a disponibilidade do serviço mantido pelo equipamento
ContingênciaWarm-Site	Esta se aplica a objetos com maior tolerância à paralisação, podendo se sujeitar à indisponibilidade por mais tempo, até o retorno operacional da atividade, como exemplo, o serviço de e-mail interno dependente de uma conexão. Vemos que o processo de envio e recebimento de mensagens é mais tolerante que o exemplo usado na estratégia anterior, pois poderia ficar indisponível por minutos, sem, no entanto, comprometer o serviço ou gerar impactos significativos
ContingênciaCold-Site	Dentro da classificação nas estratégias anteriores, esta propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infraestrutura e telecomunicações, desprovidos de recursos de processamento de dados. Portanto, aplicável à situação com tolerância de indisponibilidade ainda maior, claro que esta estratégia foi analisada e aprovada pelos gestores.
ContingênciaCPD Externa	Considera a probabilidade de transferir a operacionalização da atividade atingida para um ambiente terceirizado; portanto, fora dos domínios da empresa. Por sua própria natureza, em que requer um tempo de indisponibilidade menor em função do tempo de reativação operacional da atividade, torna-se restrita a poucas organizações, devido ao seu alto custo. O fato de ter suas informações manuseadas por terceiros e em um ambiente fora de seu controle, requer atenção na adoção de procedimentos,critérios e mecanismos de controle que garantam condições de segurança adequadas à relevância e criticidade da atividade contingenciada.
ContingênciaCPD Interna	Considera a probabilidade de transferir a operacionalização da atividade atingida para um ambiente da mesma empresa; porém, em outra filial da empresa. Por sua própria natureza, isso reduz para um tempo de indisponibilidade menor em função do tempo de reativação operacional da atividade, torna-se viável a maioria das organizações, devido ao seu baixo custo. O fato de ter suas informações manuseadas pela própria equipe facilita o controle, e a adoção de procedimentos, critérios e mecanismos de controle que garantam condições de segurança adequadas à relevância e criticidade da atividade contingenciada.

7.2. POLÍTICA DE DESCARTE DE MÍDIAS:

Identificação: Backups do negócio MOSTEN

Recuperação: Por data de referência do

BackupProteção: Restrito/Tecnologia e

Suporte

Armazenamento: Eletrônico com cópia enviada sob controle de protocolo para outro Site.

Retenção: 05 anos obedecendo s regras de descartes.

IMPORTANTE

É de suma importância, que todos os envolvidos neste processo de contingenciamento operacional (Escalation), possuam uma cópia deste documento para que os procedimentossejam tomados alinhadamente.

7.3. PLANO CENTRAL DE ATENDIMENTO TABELA DE ASPECTOS E IMPACTOS DE SI – ASM

Tabela de Acionamento Emergencial/ Contingência – Escalation

Plano de Continuidade de Negócios

Glossário de Termos e Papéis Padronizados

Termo Padronizado	Definição / Uso no Documento
Abandono de Área	Necessidade de evacuar um local devido a uma ameaça iminente ou ocorrência de um incidente grave.
Acionamento do Comitê de Segurança	O acionamento do Comitê de Segurança ocorrerá mediante a identificação de uma situação de potencial risco ou incidente que possa impactar a segurança física das instalações, a segurança lógica dos sistemas ou a segurança das informações da MOSTEN.
Alta Gestão	Refere ao grupo de indivíduos no nível mais sênior de uma organização, responsáveis por planejar, dirigir e controlar as atividades da empresa. Este grupo é tipicamente composto por: Diretores (Board of Directors), Presidente (CEO - Chief Executive Officer), Vice-Presidentes (VPs - Vice Presidents) e outros executivos de nível sênior (como CFO, COO, CTO).
Análise de Impacto no Negócio (Business Impact Analysis - BIA)	Processo para identificar e avaliar os impactos potenciais de interrupções nos processos de negócio críticos, determinando prioridades de recuperação e recursos necessários.
Áreas de Negócio	referem-se a segmentos distintos dentro de uma organização, cada um focado em um conjunto específico de produtos, serviços, clientes ou mercados.
Comitê de Auditoria	Órgão responsável por avaliar a adequação e a eficácia dos controles internos, incluindo os relacionados à continuidade de negócios.
Comitê de Continuidade de Negócios (CCN)	Também conhecido como Comitê de Gerenciamento de Continuidade de Negócios ou Comitê de BCM (Business Continuity Management), é um grupo multifuncional de indivíduos designados para supervisionar e gerenciar as atividades de continuidade de negócios de uma organização.
Comitê de Contingenciamento e Segurança da Informação (CCSI)	Grupo responsável por desenvolver, implementar e gerenciar os planos de contingência e segurança da informação para garantir a resiliência dos sistemas e dados.
Comitê de Gestão de Crise	Responsável por liderar o Grupo de Gestão de Crise, garantindo a execução do plano e comunicação entre as áreas. Substitui: "Gestor de Crise".
Comitê de Risco	Grupo responsável por identificar, avaliar e mitigar os riscos que podem afetar os objetivos da organização, incluindo riscos de interrupção de negócios.
Comitê Executivo	Grupo de alta liderança responsável por decisões estratégicas e alocação de recursos em situações de crise.
Comunicação de Crise	Plano para informar stakeholders internos e externos sobre a ocorrência de uma crise, as ações tomadas e as expectativas futuras.

Confiabilidade	Capacidade de um sistema, serviço ou processo operar sem falhas durante um período específico, mantendo a precisão e consistência dos resultados.
Coordenador de Crise	Pessoa responsável por liderar o Grupo de Gestão de Crise, garantindo a execução do plano e comunicação entre as áreas. Substitui: "Gestor de Crise".
Desastres	Eventos severos e repentinos que causam danos significativos, interrupções nas operações e podem resultar em perdas financeiras, humanas ou de reputação.
Diretriz de Aplicação	Todos os termos acima devem ser utilizados de forma única e exclusiva ao longo do documento. Menções a nomenclaturas alternativas devem ser revisadas e substituídas conforme este glossário.
Disponibilidade	Capacidade de um sistema, serviço ou informação estar acessível e operacional quando necessário.
Equipe de Tecnologia da Informação (TI MOSTEN)	Equipe técnica encarregada de identificar, conter, recuperar e prevenir incidentes relacionados à infraestrutura tecnológica da organização. Substitui: "Equipe de Tecnologia", "TI".
Estratégia de Continuidade	Abordagem geral definida para garantir a continuidade dos negócios, podendo envolver redundância de sistemas, sites alternativos, equipes de contingência etc.
Gerenciamento de Facilidades	Função responsável pela manutenção e operação das instalações físicas da organização, incluindo edifícios, infraestrutura e serviços de apoio.
Grupo de Gestão de Crise (GGC)	Equipe multidisciplinar responsável pela tomada de decisões estratégicas em situações de crise. Substitui: "Grupo de Resposta a Incidentes".
Helpdesk/Service Desk	Ponto de contato central para usuários que necessitam de suporte técnico ou assistência relacionada a serviços de TI.
Impacto no Negócio (Business Impact)	Consequências financeiras, operacionais, legais e de reputação resultantes de uma interrupção nos processos de negócio.
Integridade	Garantia de que a informação e os processos não foram alterados de forma não autorizada ou acidental, mantendo sua precisão e completude.
Níveis de Gravidade do Incidente	Classificação da severidade de um incidente com base em seu impacto nos processos críticos da organização (baixa, moderada, alta e crítica).
Ponto de Recuperação (Recovery Point Objective - RPO)	Momento mais antigo para o qual os dados devem ser restaurados após uma interrupção, representando a quantidade máxima de perda de dados aceitável.
Ponto Focal na MOSTEN	Pessoa designada como principal contato para questões específicas dentro da MOSTEN.
Planejamento do PCN	Refere-se ao processo sistemático e contínuo de identificar, avaliar e mitigar os riscos que podem interromper as operações de uma organização, com o objetivo de garantir a capacidade de continuar as funções essenciais durante e após uma interrupção.

Plano de Continuidade de Negócios

Plano de Continuidade de Negócios (PCN)	Documento que estabelece os procedimentos para garantir a continuidade das operações essenciais em situações de crise.
Plano de Resposta a Incidentes (PRI)	Subconjunto do PCN com foco específico em resposta a falhas técnicas, ataques cibernéticos ou indisponibilidade de sistemas.
Resiliência	Capacidade da organização de absorver e se adaptar a mudanças e perturbações, mantendo suas funções essenciais.
Sinistro	Ocorrência de um evento danoso ou prejudicial que causa perdas ou danos materiais, financeiros ou operacionais.
Site de Contingenciamento	Local alternativo onde as operações críticas podem ser retomadas em caso de indisponibilidade do site principal.
Stakeholders Críticos	Partes interessadas cujas operações são diretamente impactadas por interrupções, incluindo clientes-chave, fornecedores estratégicos e órgãos reguladores.
Tabela de Implantação	Detalha as ações específicas a serem tomadas em resposta a diferentes tipos de incidentes ou cenários de interrupção definidos no Plano de Continuidade de Negócios (PCN).
Tempo de Recuperação Desejado (Recovery Time Objective - RTO)	Período máximo aceitável para restaurar um processo de negócio ou sistema após uma interrupção.
Sobrevivência	Capacidade da organização de continuar operando seus processos críticos durante e após uma interrupção.
Teste de Continuidade de Negócios	Simulação de cenários de interrupção para validar a eficácia do PCN e identificar áreas de melhoria.

Diretriz de Aplicação

Todos os termos acima devem ser utilizados de forma única e exclusiva ao longo do documento. Eventuais menções a nomenclaturas alternativas devem ser revisadas e substituídas conforme este glossário.

Além disso, os fluxos de processos correlatos deverão ser revisados para refletir a terminologia padronizada, assegurando que cada papel, grupo e etapa mantenha coesão textual e funcional.