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 Mauricio Tinoco	Comitê de Privacidade	

Sumário

1. OBJETIVOS

Expor a todos os clientes, parceiros e colaboradores da **MODAL GESTAO & RESULTADOS 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 "**MODALGR**" 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 **MODALGR** 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.

Estabelecendo a sistemática para implementação e operação do plano de contingência para tratar crises relativas à administração de pessoas, e em caso de sinistros (parcial ou total), tecnologia, infraestrutura ou possíveis interrupções, ou eventos externos. Este plano é revisto periodicamente, visando garantir a integridade, confidencialidade, disponibilidade dos ativos da organização e a continuidade dos serviços alcançando os níveis mínimos de desempenho definidos como meta de SLA[1];

Garantir a continuidade dos negócios identificando possíveis riscos e ameaças na tecnologia do ambiente;

Obedecer aos seis estágios:

1. Compreender o negócio;
2. Definir estratégia de continuidade;
3. Seguir o plano de continuidade do negócio;

[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 o cliente que deseja se beneficiar deste.

4. Construir e disseminar a cultura do plano;
5. Exercitar, manter e auditar;
6. Testar, avaliar e melhorar.

Desencadeamento de ações:

1. Assegurar serviços contínuos e com os processos com os quais ele se relaciona;
2. Manter integridade nos recursos críticos de TI;
3. Recuperação e retomada de serviços de TI;
4. Armazenamento de backup e revisão pós-retomada;
5. Relação com outros processos;
6. Ativação do Plano de Emergência:
   - Divulgação interna e externa;
   - Integração com outros planos;
   - Suprimento dos recursos;
   - Acionamento dos executivos para efetuar avaliações;
   - Para qualquer acionamento usar a Tabela de *Escalation Gerencial*;
7. Procedimento de combate:
   - Notificar diretoria da empresa;
   - Definir o ponto de encontro das pessoas;
   - Ações compatíveis com os impactos;
   - Rotinas pré-estabelecidas para isolamento e evacuação;
   - Transporte emergencial;
   - Reparos de emergência;
   - Ações de rescaldo diante de um incêndio.
8. Manutenção pós-combate:
   - Sistema de atualização do plano de contingência;
   - Avaliação de treinamentos e atendimentos realizados;
   - Reposição de recursos;
   - Documentação \ Lições aprendidas.

2. DEFINIÇÕES E DIRETRIZES

2.1. ACIONAMENTO DO COMITÊ DE SEGURANÇA:

Sempre que for identificada a real necessidade da ativação do **Plano de Continuidade de Negócios (PCN)** da **ModalGR** a gerência deverá acionar o **COMITÊ DE CONTINGENCIAMENTO E SEGURANÇA DA INFORMAÇÃO (CCSI)**.

2.2. TABELA DE IMPLANTAÇÃO:

Posição	Atribuições
Gestor do Plano / Substituto (*)	✓ Nomear os participantes do plano. ✓ Garantir a documentação atualizada dos sistemas. ✓ Garantir cópias redundantes das informações e dados da **ModalGR**. ✓ Disponibilizar recursos para ação de resposta. ✓ Promover treinamento dos colaboradores. ✓ Promover exercícios simulados. ✓ Garantir a revisão periódica do plano. ✓ Enviar relatório final de situação para o CCSI.
Grupo de Atuação direta	✓ Planejamento das ações de resposta relacionadas à sua área. ✓ Determinar as orientações para as equipes de atuação. ✓ Seguir os procedimentos descritos para o cenário. ✓ Auxiliar, no que for necessário, nas ações de combate. ✓ Avaliar a participação do grupo após um incidente. ✓ Elaborar relatório final de situação.
Grupo de Apoio	✓ Planejamento das ações de resposta relacionadas à sua área. ✓ Seguir as orientações do coordenador do plano. ✓ Executar as atividades de infraestrutura de engenharia e manutenção. ✓ Executar as atividades de provimento de recursos. ✓ Elaborar relatório final de situação.

2.3. PCN – PLANO DE CONTINUIDADE DO NEGÓCIO:

Um plano para a resposta de emergência, operações backup e recuperação de ativos atingidos por uma falha ou desastre. Tem como objetivo assegurar a disponibilidade de recursos de sistema críticos, recuperar um ambiente avariado e promover o retorno à sua normalidade; o **PCN** abrange um conjunto de três planos que são focados cada um em uma determinada variável de risco, numa situação de ameaça ao negócio da empresa (ou ambiente):

Planos	Descrição dos Planos
PGC – Plano de Gerenciamento de Crises:	Este documento tem o propósito de definir as responsabilidades de cada membro das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente. Além disso, tem que definir os procedimentos a serem executados pela mesma equipe no período de retorno à normalidade. O comportamento da empresa na comunicação do fato à imprensa é um exemplo típico de tratamento dado pelo plano. Focado nas atividades que envolvem as respostas aos eventos;
PCO – Plano de Continuidade Operacional:	Tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, consequentemente, os impactos potenciais ao negócio. Orientar as ações diante de queda de uma conexão à Internet exemplifica os desafios organizados pelo plano. Focado nas atividades que garantam a realização dos processos
PRD – Plano de Recuperação de Desastres:	Tem o propósito de definir um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação, no menor tempo possível. Focado para as substituições ou reposição de componentes que venham a ser danificados.

NOTA: Para obtenção de sucesso nas ações dos planos, é necessário estabelecer adequadamente os gatilhos de acionamento para cada plano de continuidade. Estes gatilhos são parâmetros de tolerância usados para sinalizar o início da operacionalização da contingência, evitando acionamentos prematuros ou tardios.

Após o retorno à normalidade, relatórios deverão ser entregues pelas equipes que operacionalizaram o plano ao Gestor do plano, com informações sobre o evento, apontando, por exemplo, características do objeto da contingência, percentual de recurso afetado, quantidade de recursos afetados, tempo de indisponibilidade, impactos financeiros etc.

2.4. PLANEJAMENTO DO PCN

Diz respeito ao planejamento da recuperação de processos organizacionais críticos em seguida a um desastre.

2.5. DESASTRES

Não se resumem somente a fogo, inundação e outras causas de dano à propriedade; eles também podem resultar de problemas corriqueiros como mau funcionamento de *hardware* ou *software*, invasões por *hackers* e *crackers*. E ainda que a restauração do processamento computacional seja um passo importante do processo de recuperação, outros problemas igualmente importantes frequentemente precisam ser resolvidos. Por isso é fundamental uma análise e avaliação baseada nos riscos que identifique, quantifique e priorize os critérios

e os objetivos pertinentes à organização, incluindo recursos críticos, impactos de interrupção, possibilidade de ausência de tempo e prioridades de recuperação.

2.6. DISPONIBILIDADE

A propriedade que um sistema ou um dos seus recursos de estarem acessíveis e utilizáveis sob demanda por uma entidade autorizada, de acordo com especificações de desempenho projetadas; isto é, um sistema que está disponível para fornecer serviços de acordo com o seu projeto, sempre que uma solicitação for realizada.

2.7. CONFIABILIDADE

A habilidade de um sistema de executar uma função requerida sob condições indicadas por um período especificado.

2.8. INTEGRIDADE

A propriedade de manutenção dos dados da forma como foram gerados, não sofrendo alteração durante a sua vida útil especificada.

2.9. SOBREVIVÊNCIA

A habilidade de um sistema de continuar em operação ou existindo apesar das condições adversas, inclui as ocorrências naturais, ações acidentais, e ataques ao sistema.

2.10. ABANDONO DE ÁREA

Ato de retirar de forma ordenada todos os colaboradores da área sinistrada para uma área segura;

2.11. SINISTRO

Entende-se por sinistro, quaisquer ocorrências motivadas que impossibilite o desenvolvimento normal da operação, seja ela motivada por queda de energia, links, enchentes e incêndio.

- **SINISTRO PARCIAL:** Situação identificada através da paralisação de atividades operacionais mesmo dispondo dos recursos de energia elétrica, acesso à rede, telefonia etc.
- **SINISTRO TOTAL:** Situação identificada através da paralisação total do Site ocasionada por queda de energia, não funcionamento de *Nobreak* e geradores, incêndios etc.

2.12. COMITÊ EXECUTIVO

Formado pela área de Tecnologia, (Operações e Suporte) e pelo representante da gestão do PCN, serão os responsáveis por todas as atividades do Plano de Contingência, inclusive pela divulgação de informações durante sua execução.

2.13. COMITÊ DE AUDITORIA

Formado pela equipe Executiva responsável pelo **Comitê de Compliance** por elaborar, validar, publicar e auditar documentos referentes aos procedimentos desenvolvidos e atualizados periodicamente.

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

Seus integrantes deverão ser previamente definidos e pertencerem ao quadro de colaboradores operacionais da empresa, sendo o comitê, gestor das atividades descritas neste **PCN**, devendo todos os envolvidos com o processo, respeitar as premissas do Comitê de Risco.

2.15. COMITÊ DE RISCO

Formada pela equipe de Planejamento Operacional e terá a responsabilidade pelo planejamento do estado de contingência, bem como as definições sobre a implantação, dimensionamento, tempo de implementação e sobre as responsabilidades inerentes de acordo com as premissas de contrato ou pela revisão do mesmo e será constituído por representante(s) da empresa.

2.16. GERENCIAMENTO DE FACILIDADES

Formada pela equipe de Gerentes e tem como responsabilidade as simulações e treinamento da 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

Será 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 MODALGR

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

2.19. REPRESENTANTE DE TELECOM

Terá como responsabilidade, manter as Centrais de comunicação (VOZ) em funcionamento, bem como ações para restauração e/ou contingenciamento para as estruturas de comunicação de dados.

2.20. 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.

2.21. TESTES

O Plano de Contingenciamento poderá ser testado em datas previamente acordadas.

3. CENÁRIO DE INFRAESTRUTURA

3.1. ENERGIA ELÉTRICA

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

(Necessidade de local isolado e controlado para servidor e infra).

3.1.1. PONTO DE ACESSO ELÉTRICO

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

3.2. ESCADA E EXTINTORES DE INCÊNDIO

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

3.2.1. EQUIPE DE BRIGADA DE INCÊNDIO TREINADA/SOCORRISTAS TREINADA

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

3.3. AR-CONDICIONADO

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

3.4. SISTEMA DE SEGURANÇA

3.4.1. Controle de Acessos:

- ✓ **Procedimentos de Segurança – Controle de acesso**

Existem câmeras de vigilância na recepção da sede, bem como as regras de acessos estabelecidas para entrada.

4. CENÁRIO DE TECNOLOGIA

4.1. ESTRUTURA NETWORK E COMUNICAÇÃO DE DADOS

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

- Os racks de servidores e equipamentos de redes (exemplo: roteadores, switches, DIO) possuem redundância elétrica, além de ter cabeamento estruturado 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 TECNICO E OPERAÇÕES

- A **ModalGR** possui Gerencias de Suporte e Operações para suportar a monitoração do ambiente de forma proativa, sem interromper a prestação dos serviços aos clientes,

mantendo a qualidade e possibilitando o atendimento a chamados de Incidentes, Problemas ou Requisições.

- Asseguramos através das melhores práticas a excelência da gestão do nível de serviço contratado e a maximização da produtividade dos recursos alocados.
- Dentre as principais atividades de responsabilidade do Suporte Técnico, ressalta-se:
  - Identificar, acionar os responsáveis em caso de falhas, acionamento da equipe de suporte técnico, e controlar o processo das Melhores Práticas de Gestão de Serviços junto às áreas envolvidas, assegurando o seu cumprimento e os padrões estabelecidos;
  - Apoiar a tomada de decisão e as atividades das equipes de Operações;
  - Gerar relatórios analíticos indicando os problemas e soluções;
- Além de reuniões internas, são realizados contatos diários com fornecedores, visando o melhor entendimento e identificação de pontos críticos.
- Ao identificar qualquer anormalidade que esteja comprometendo o resultado, os responsáveis são imediatamente contatados e em conjunto definem e implementam as devidas ações para corrigir ou minimizar os possíveis impactos.

4.2.1. SEGURANÇA DE DADOS:

Segurança de Dados		Gerencia
FIREWALL	Possuímos o Firewall com Security Plus para garantir a segurança de dados do cliente e da própria segurança tecnológica	**ModalGR**
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. CENÁRIO DE RISCOS E AMEAÇAS: INFRAESTRUTURA

4.3.1. ENERGIA ELÉTRICA:

- Falha na alimentação pública;
- Falha no gerador;
- Falha no Nobreak;
- Falha no banco de baterias;
- Pane elétrica por causas da natureza;

4.3.2. CONTROLE DE ACESSO:

- Falha na segurança;
- Extravio de Crachá;
- Falha no sistema CFTV;

4.3.3. PONTO DE ACESSO ELÉTRICO:

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

4.3.4. NO-BREAK:

- Falha no hardware do equipamento;
- Falha no software do equipamento;
- Falha no banco de baterias;

4.3.5. ESCADA E EXTINTORES DE INCÊNDIO:

- Falha por falta de vistoria e manutenção;

4.3.6. 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 deem apoio 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 óptica;
- 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

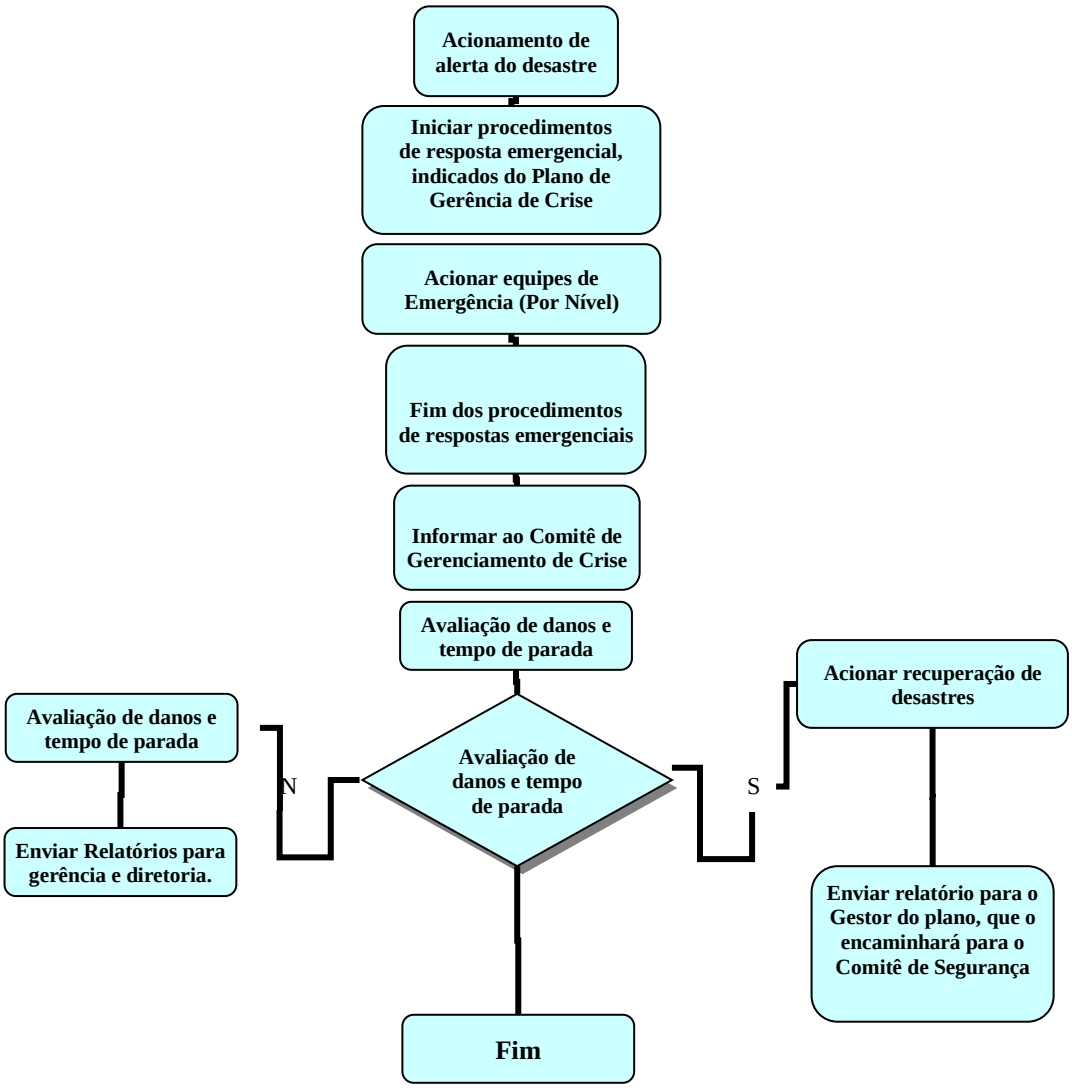
PREMISSAS

- 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

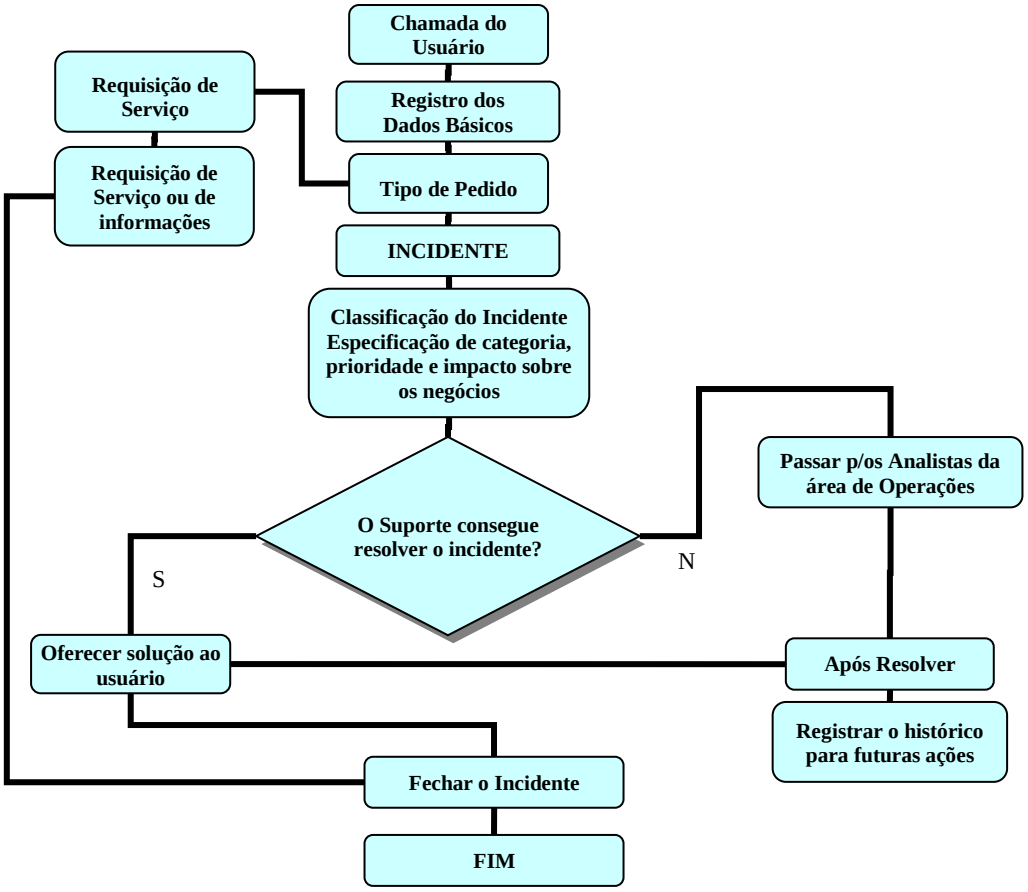
  Observações: O plano sempre será acionado pelo Comitê de Contingenciamento e Segurança da Informação (**CCSI**) e pelo Comitê de Risco (**CR**).

5.1 EXEMPLO DE CENÁRIO DE PCN ModalGR: FLUXOGRAMAS

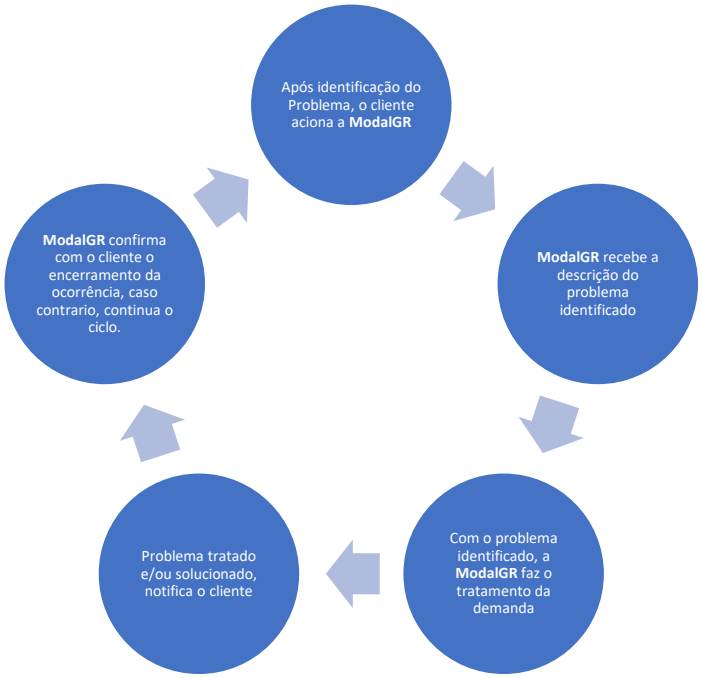
5.1.1 FLUXOGRAMA DE ACIONAMENTO DO PCN:



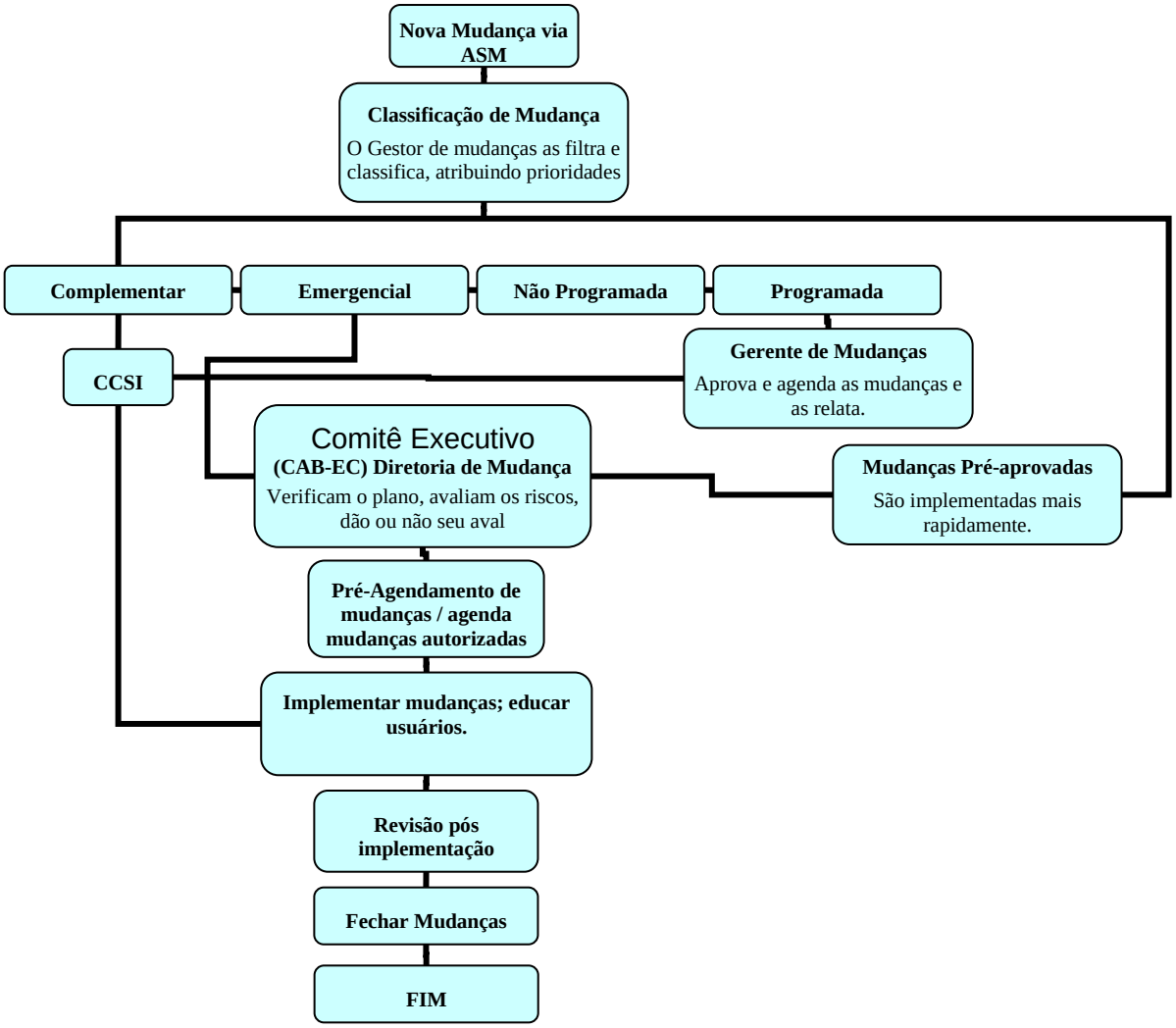
5.1.2. EXEMPLO DE FLUXOGRAMA EM CASOS DE INCIDENTES NO CLIENTE:



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 ModalGR: INFRAESTRUTURA

5.2.1 PARA ENERGIA ELÉTRICA:

- Ocorrendo falta de energia no site, automaticamente é ativado o Gerador, abastecido por diesel. (em processo de identificação e tratamento de possível instalação junto a edificação existente na **ModalGR**)
- No caso de problema com o gerador, 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 norma NBR 14136

5.2.4. CENÁRIO DE PCN PARA NO-BREAK:

- Caso ocorrer falha no *no-break* do site imediatamente é acionada a equipe de Infraestrutura para 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 portas antichamas e na iluminação de emergência;
- A equipe de Infraestrutura realiza vistoria periódica nos extintores de cada andar do edifício, 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 ModalGR: 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 empregados se 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 principais gestores 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 trabalho em 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 com nossa 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 estratégico 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 Recursos Humanos deem apoio e orientação aos demais colaboradores durante todo o movimento de paralisação.

5.4 EXEMPLO DE CENÁRIO DE PCN ModalGR: 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 para inibir 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 adequados sensíveis 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 ModalGR: 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 a equipe 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´s 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 ModalGR: 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 concordando com 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;
  - 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 ModalGR: 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 e por 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 ModalGR: 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 a equipe 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 ModalGR: ATIVAÇÃO DE CONTINGÊNCIA

5.9.1. ORIGEM:

***Site da* ModalGR**

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 Grau de 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 Contingenciamento 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 tem sua sustentação básica composta pelos procedimentos de 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, 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 evite que 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, ou até segundos, antes de um desastre, foram criadas diversas estratégias para o seu armazenamento, que são:

Estratégias	Atribuições
Contingência Hot-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
Contingência Warm-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

Contingência Cold-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.
Contingência CPD 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.
Contingência CPD 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 **ModalGR**

Recuperação: Por data de referência do Backup

Proteção: 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 procedimentos sejam tomados alinhadamente.

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

Tabela de Acionamento Emergencial/ Contingência – Escalation