POLÍTICA DE CONTINUIDADE DE NEGÓCIOS E SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

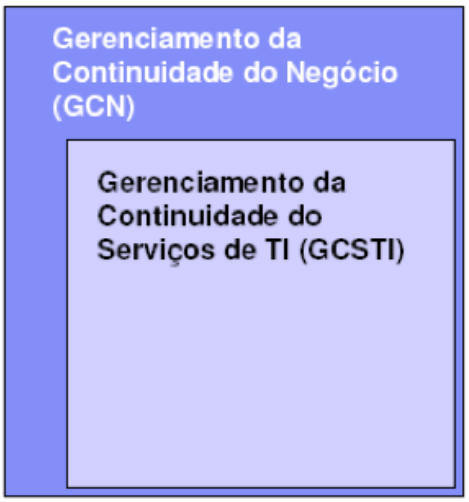
São Paulo
01/05/2026

Sumário

1. INTRODUÇÃO

A HABITASEC, por meio da Consultoria de Tecnologia da Informação (CTI), apresenta o Plano de Continuidade Macro dos Serviços de TI, que dispõe sobre a política de segurança da informação dos ambientes de tecnologia da informação e comunicação (TIC).

Este documento tem o objetivo de apresentar a preocupação da HABITASEC com as informações e a visão de como irá garantir a continuidade dos negócios da HABITASEC, assegurando a disponibilidade de recursos críticos e recuperação do ambiente de TI, promovendo seu retorno à normalidade minimizando os impactos e custos que tal incidente poderia trazer para a HABITASEC.



Principais objetivos:

- Sobrevivência do Negócio
- Minimização de falhas
- Redução de vulnerabilidades e riscos
- Transferência de risco para terceiros
- Elaboração do plano de recuperação para TI
- Suporte ao Plano de Continuidade do Negócio
- Prevenir a perda de Segurança

Este documento apresenta de uma forma geral as normas gerais para uso adequado das informações e recursos de tecnologia na HABITASEC e orientará nossas atitudes sobre o tema, oferecendo padrões de comportamento a serem seguidos.

A partir deste ponto devemos construir os planos propriamente ditos, conforme as definições do item 2 deste documento.

- Plano de Gerenciamento de Crises PGC;
- Plano de Continuidade Operacional PCO;
- Plano de Recuperação de Desastres.

2. PLANO DE CONTINUIDADE DE NEGÓCIOS DOS SERVIÇOS DE TI

Desenvolvimento do Plano

Para elaboração do Plano de Contingência da HABITASEC, propõe-se a seguinte abordagem:

2.1. IDENTIFICAR OS PROCESSOS DE NEGÓCIO

- Definir Política
- Alocação de Recursos
- Definição do Projeto e estruturas de controle
- Acordo dos planos de projeto

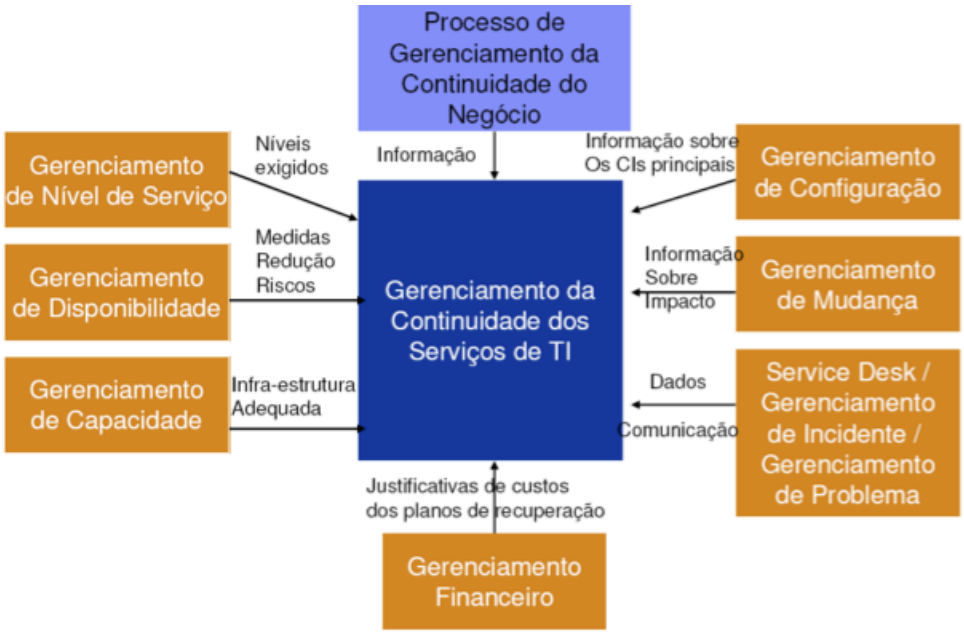
2.2. AVALIAR OS RISCOS E IMPACTOS DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO PARA A HABITASEC

- Identificar serviços críticos
- Determinar consequências da indisponibilidade
- Avaliar cenários de impacto Obrigações legais
- Avaliar a sobrevida do negócio sem serviços de TI
- Estimar tempo mínimo e máximo de recuperação

2.3. IDENTIFICAÇÃO DE MEDIDAS PARA CADA INCIDENTE COM BASE NA ANÁLISE DE RISCOS E IMPACTO

- Gerenciamento do Plano
- Infraestrutura de TI
- Procedimentos de Operação
- Equipe técnica
- Segurança do Plano
- Site de Contingência
- Retorno a operação normal

3. DIAGRAMA DE AÇÃO DO GCSTI



4. ANÁLISE E IMPACTO DE RISCOS PARA O HABITASEC

Obstáculos:

- Disponibilidade de orçamento para implementar o GCSTI
- GCSTI não baseado no GCN
- Falta de comprometimento da TI e gerentes de Negócio
- Recuperação não funciona por falta de testes
- Falta de conscientização

Benefícios Esperados:

- Redução de impacto
- Confiança do cliente Redução do valor do seguro
- Redução da interrupção dos negócios durante um incidente com habilidade de recuperação de forma eficiente
- Relacionamento mais amistoso entre Negócios e TI

5. Análise e Impacto de Riscos da Tecnologia da Informação para HABITASEC

5.1. O que proteger (quais processos?);

- Informação e dados que estão no servidor
- Continuidade dos trabalhos operacionais e recursos humanos

5.2. O que proteger (Quais desastres?);

Ameaça	Severidade	Probabilidade	Risco	Medida de Controle
Enchente	Média	Média	Estrago da água, falta de acesso	Colocar o datacenter em andar seguro
Blackout	Baixa	Média	Perda de dados, Perda de controles de segurança	Gerador de energia. Estação elétrica auxiliar
Falha no servidor de aplicação do ERP	Alta	Alta	Parada dos processos de Venda, Faturamento, etc	Site backup com base de dados duplicada

5.3. GRAU DE EXPOSIÇÃO (QUANTO O(S) PROCESSO(S) ESTÁ(ÃO) EXPOSTO(S) A UM DESASTRE?);

Site	Custo	Equipamentos Hardware	Estrutura de Telecomunicações	Tempo para migração	Local
Cold-site	Baixo	Nenhum	Nenhuma	Longo	Fixo
Warm-site	Médio	Parcial	Parcial/Completo	Médio	Fixo
Hot-site	Baixo/Médio	Completo	Completo	Curto	Fixo
Mobile-site	Alto	Depende	Depende	Depende	Móvel
Mirrored-site	Alto	Completo	Completo	Nenhum	Fixo

Visando minimizar os impactos, a HABITASEC construiu sua infraestrutura interna da seguinte forma:

Cuidados com a Segurança da Informação:
A HABITASEC possui um equipamento Fortigate 80F - Fortinet, que permite o balanceamento de links de internet e um gerenciamento seletivo de navegação na internet, dando ao corpo diretivo da empresa controle total do ambiente.

Cuidados com a Internet:
- Dois links de internet de operadoras independentes
- 01 Link de 700MB VIVO Empresas
- 01 Link de 300MB Dinâmico American Net

Cuidados com a Telefonia:
- Dois links de VOZ e operadoras independentes
- 01 Link E1 30 ramais da operadora GVT
- 04 Linhas analógicas da operadora VIVO Empresas

Cuidados com o PABX:
- A HABITASEC possui um contrato de comodato e manutenção da central telefônica, que contempla a substituição completa em caso de qualquer avaria.

Cuidados com os Servidores e Informação:

A HABITASEC possui um servidor de domínio, habilitado com os recursos de Backup em nuvem que estão programados para efetuar cópias diariamente em um ambiente seguro em nuvem dos serviços de System State e Backup de Dados, possibilitando a reconstrução do ambiente em caso de falha do sistema operacional ou desastre natural;

Solução coorporativa VBox, onde é realizada regularmente cópia de todos os dados, sincronizados imediatamente com o servidor online protegido por um contrato coorporativo que garante durabilidade, versionamento de arquivos e recuperação dos trabalhos

5.4. ESTIMATIVA DE IMPACTO DE UM DESASTRE (QUAL A CONSEQUÊNCIA DE UM DESASTRE?);

De acordo com a severidade do impacto, a diretoria da HABITASEC definiu que suas operações podem permanecer fora do AR por até 72 horas, sem prejuízo da operação.

Este plano de contingência atenderá um tempo de aproximadamente 2 dias para reestabelecer as operações

5.5. ESTRATÉGIA DE CONTINUIDADE (COMO MANTER A CAPACIDADE PRODUTIVA NO CASO DE UM DESASTRE?).

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.

Cada tipo de arquivo irá exigir um tipo de cópia. Entretanto, numa 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.

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.

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).

Baseado na importância dos backups, pois guardam uma cópia fiel dos dados minutos, ou até segundos, antes de um desastre, a estratégias definida pela HABITASEC para o seu reestabelecimento foi:

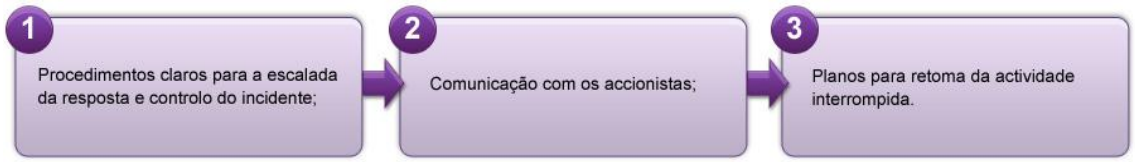
6. ESTRATÉGIA DE CONTINGÊNCIA COLD-SITE

Esta propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infraestrutura e telecomunicações, desprovido 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 da HABITASEC.

A HABITASEC possui uma parceria com o (local a ser contratado), que mantêm disponível uma sala preparada com quatro posições de trabalho completa, equipado com energia elétrica, infraestrutura de cabos de rede e telefonia em um ambiente controlado.

7. IDENTIFICAÇÃO DE MEDIDAS PARA CADA INCIDENTE

Os fatores chaves para qualquer resposta baseiam-se em:



As ações descritas nos planos não têm a validade de cobrir todas as situações, pois estas, pela sua natureza, podem ser muito diversas. Assim sendo, qualquer procedimento pré-definido pode ter de ser adaptado com total flexibilidade e com uma significativa dose de iniciativa por quem está responsável pela sua implementação.

8. GLOSSÁRIO

Alinhamento Estratégico

É um processo gerencial contínuo e sistemático, que diz respeito à formulação de objetivos para a seleção de programas de ação e para sua execução, levando em conta as condições internas e externas à empresa e sua evolução esperada.

Análise de Riscos

A Análise de Riscos é o processo pelo qual são relacionados os eventos, os impactos e avaliadas as probabilidades destes se concretizarem.

Na área administrativa geralmente se executa uma análise de riscos dentro de organizações que estão planejando ou desenvolvendo projetos específicos ou para negócios, sendo a abordagem de negócios a mais utilizada.

Atitude

Querer fazer. Comportamentos que temos diante de situações do nosso cotidiano e das tarefas que desenvolvemos no nosso dia-a-dia.

Conhecimento

Saber. Conhecimentos adquiridos no decorrer da vida, nas escolas, universidades, cursos etc.

Diagrama

Um diagrama é uma representação visual estruturada e simplificada de um determinado conceito, ideia, etc.

Função

As funções devem ser identificáveis e definíveis em termos de atividades, responsabilidades e atribuições, devem ser o mais independente possível das estruturas organizacionais existentes.

Governança

Governança é a capacidade dos governos ou empresas de planejar, formular e implementar políticas e cumprir funções.

Governança de TI

Conjunto de praticas, padrões e relacionamentos estruturados, assumidos por executivos, gestores, técnicos e usuários de TI de uma organização, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos, ampliar o desempenho, otimizar a aplicação de recursos, reduzir os custos, suportar as melhores decisões e consequentemente alinhar TI aos negócios.

Meta

São objetivos organizacionais futuros, isto é os resultados a serem alcançados. Após serem quantificados e definidos no tempo, estes objetivos organizacionais passam a designar-se por Metas.

PCN

Plano de Continuidade de Negócios. O Plano de Continuidade de Negócios (PCN), o qual é a tradução de Business Continuity Plan (BCP), é o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, e até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio do qual ela faz parte.

PDCA

É um método de gestão que se carateriza por um ciclo de ações que se repete continuamente de forma a incorporar alterações no ambiente. Plan: Planejamento, Do: Executar, Check: Verificar e Act: Agir.

Plano de Contingência

Um plano de contingência, também chamado de planejamento de riscos, plano de continuidade de negócios ou plano de recuperação de desastres, tem o objetivo de descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos a corporação.

Processo

Processo é definido como a sequência completa de um comportamento de negócio, provocado por algum evento e que produz um resultado significativo para o negócio e que, de preferência, tenha foco no cliente.

Risco

O termo Risco é utilizado em administração, atuária, economia, direito e outras ciências, para designar o resultado objetivo da combinação entre a probabilidade de ocorrência de um determinado evento, aleatório, futuro e que independa da vontade humana, e o impacto resultante caso ele ocorra. Para a ciência atuarial esse conceito pode ser ainda mais específico ao se classificar o risco como uma a probabilidade de ocorrência de um determinado evento que gere prejuízo econômico.

Serviço

Podem conter um ou mais processos que em comum devem servir para compor o mesmo resultado de negócio.

SLA

Um Acordo de Nível de Serviço (ANS ou SLA, do inglês Service Level Agreement) é um acordo firmado entre a área de TI e seu cliente interno, que descreve o serviço de TI, suas metas de nível de serviço, além dos papéis e responsabilidades das partes envolvidas no acordo.

TIC

Tecnologia da Informação e Comunicação. Sigla para designar a informática e sua potencialização com os recursos de comunicação.