POLÍTICA DE RECUPERAÇÃO CONTRA DESASTRES

adx movidos por transformação

VERSÃO 1.0 – 29 DE JULHO DE 2022

DENOMINAÇÃO DO DOCUMENTO: Política de Recuperação Contra Desastres da Informação	**DATA DA PUBLICAÇÃO:** 29/07/2022
ÁREA REPONSÁVEL: Diretoria Geral	**CLASSIFICAÇÃO:** Uso interno
RESPONSÁVEL PELA ELABORAÇÃO: Comitê Gestor de Privacidade	**RESPONSÁVEL PELA APROVAÇÃO:** **XXXXXX**

Comitê Gestor de Privacidade do SENAC AL

Nome	Setor	E-mail
Vagner de Gusmão Cavalcanti	Planejamento/Controladoria	vagner.cavalcanti@al.senac.br
Samuel Vasconcelos da Silva	TI	samuel.vasconcelos@al.senac.br
Felipe Dietschi Falcão	Contratos, Estoque e Licitação	felipe.falcao@al.senac.br
Diego de Souza Pinto	TI	diego.souza@al.senac.br
João Carlos Azarias de Oliveira	TI - Unidade Arapiraca	joao.oliveira@al.senac.br
Cristiane Calaça Correia Botelho	Marketing/Comunicação/Centrais de atendimento/Callcenter	cristiane.calaca@al.senac.br
Aline Baracho Wanderley de Oliveira	Ouvidoria	aline.baracho@al.senac.br
Aristóteles da Silva Oliveira	Gerência de Educação Profissional	aristoteles.oliveira@al.senac.br
Sheila Vieira de Melo	RH	sheila.vieira@al.senac.br
Rosimeire Guedes da Silva	Financeiro	rosimeire.guedes@al.senac.br

Equipe Técnica do Grupo ADX

Adriano Lima Head de Projetos	**Adgenison Nascimento** Head de Negócios
Géssica Alcântara Gestora de Projetos	**Laís Gomes** Analista de Processos

Lavínia França Analista de Processos	**Saulo Vieira** Advogado

Sigilo e direitos de propriedade
As informações contidas nesse documento são propriedade do SENAC AL e não poderão ser disseminadas, distribuídas ou de qualquer outra forma passadas a terceiros, sem o expresso consentimento escrito.

Histórico de revisões			
Versão	**Data**	**Autor**	**Descrição**
1.0	29/07/2022	ADX	Documento elaborado

SUMÁRIO

1 – Introdução

Este documento declara o comprometimento da diretoria em estabelecer a PRD - Política de Recuperação Contra Desastres do SENAC AL, que é um conjunto das diretrizes, normas e procedimentos que fornece estratégias para garantir que serviços essenciais sejam identificados, para garantir sua preservação após a ocorrência de um desastre e até o retorno da situação normal de funcionamento da instituição. Também provê quais planos de ação devem ser realizados em cada momento.

Esta política define o Plano de Continuidade de Negócio (PCN) e será de nível mais macro, dividida em 4 (quatro) planos menores (Plano de Contingência, Plano de Continuidade Operacional, Plano de Recuperação de Desastres e Plano de Administração de Crises), os quais proverão basicamente: objetivo, escopo, papéis, responsabilidades, condições de ativação do plano, procedimentos que devem ser adotados, comunicação em caso de ocorrência de desastres e encerramento do plano.

2 – Objetivo

A PRD deverá estabelecer cenários de situações inesperadas ou incidentes (quer sejam operacionais, desastres ou crises), além de formas de gerenciar os impactos imediatos de um incidente de interrupção, dando a devida atenção para:

- ✓ alternativas estratégicas, táticas e operacionais para responder à interrupção;
- ✓ prevenção de novas perdas ou indisponibilidade de atividades prioritárias;
- ✓ detalhes sobre como e em que circunstâncias a empresa irá se comunicar com as partes interessadas e seus familiares ou contatos de emergência.
- ✓ Atendimento aos requisitos da LGPD dentro dos prazos determinados por lei.

A PRD fornece normas e padrões para que a empresa consiga recuperar, retomar e dar continuidade aos seus processos de negócios mais cruciais, evitando que eles sofram danos maiores. Ao passo que pequenas organizações podem incluir seus planos em apenas um documento, a PRD é dividida em quatro (4) planos menores:

- ✓ **Plano de Administração de Crises**: Define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência;
- ✓ **Plano de Contingência**: Define as necessidades e ações mais imediatas. Deve ser utilizado somente quando todas as prevenções tiverem falhado;
- ✓ **Plano de Recuperação de Desastres**: Determina o planejamento para que, uma vez controlada a contingência e passada a crise, sejam retomados os níveis originais de operação;
- ✓ **Plano de Continuidade Operacional**: Seu objetivo é restabelecer o funcionamento dos principais ativos que suportam as operações da instituição, reduzindo o tempo de queda e os impactos provocados por um eventual incidente.

A imagem a seguir mostra a interação entre os quatro planos citados.

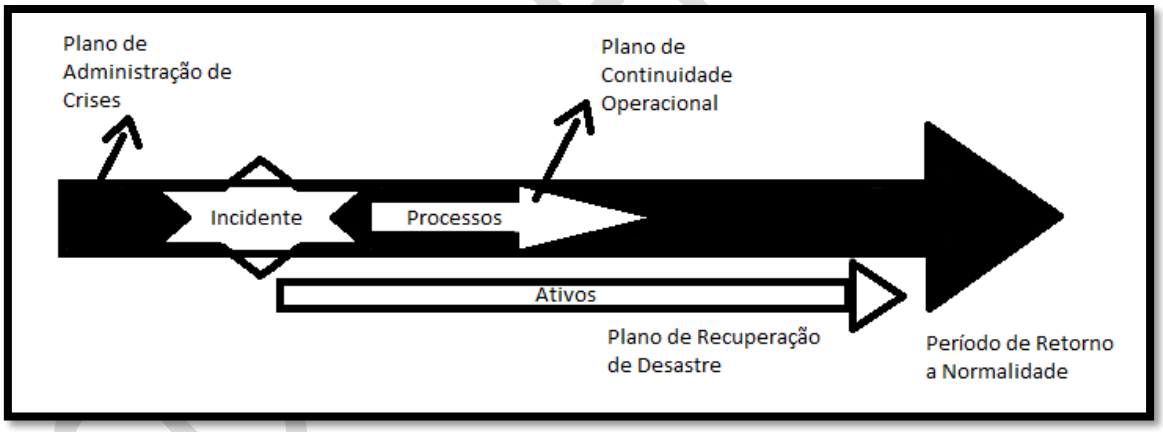


Figura 1 - Ordem cronológica dos planos.

Os planos aqui definidos seguirão o Modelo "Plan-Do-Check-Act" (PDCA) para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente a eficácia do Sistema Gestor de Continuidade de Negócios (SGCN) de TIC da empresa. O modelo PDCA ajudará na melhoria contínua do Sistema de Gestão de Continuidade de Negócios.

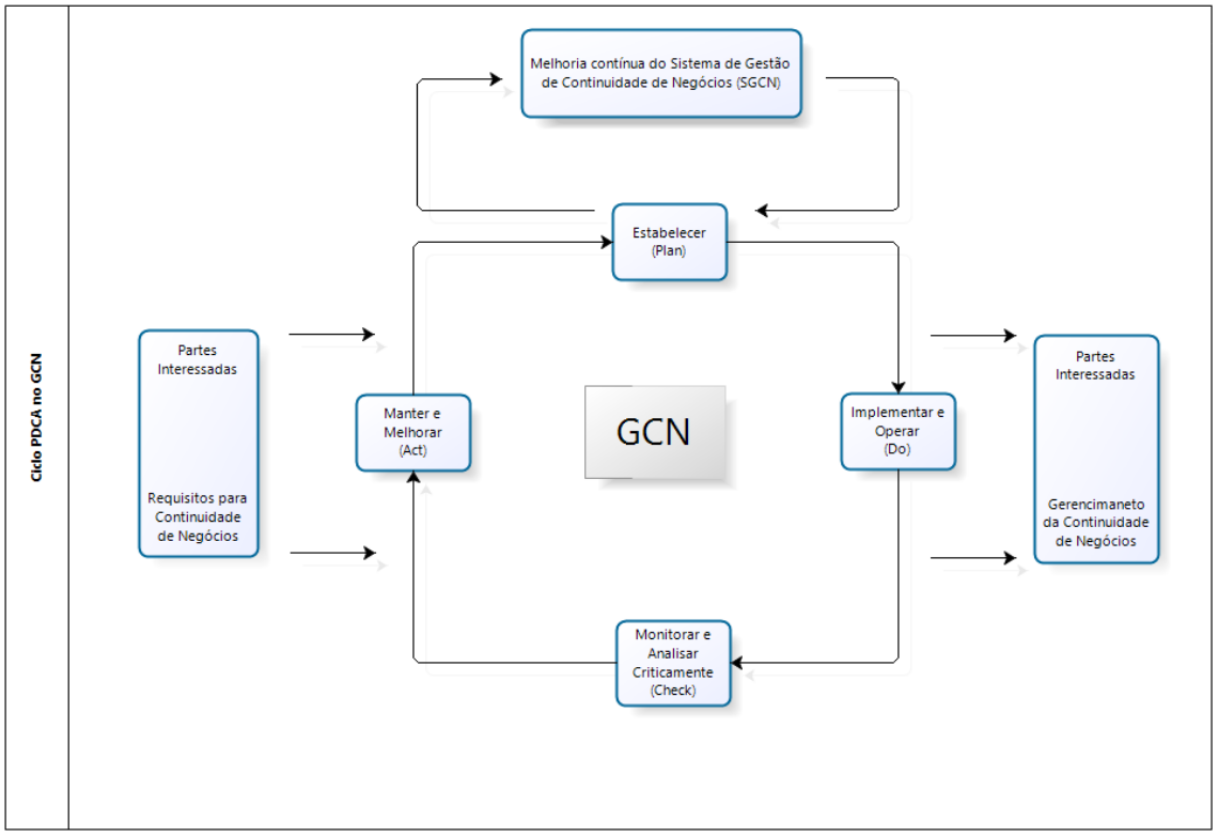


Figura 2 - Ciclo PDCA no Gestão de Continuidade de Negócios.

Plan (estabelecer) - Seguir uma política de continuidade de negócios, objetivos, metas, controles, processos e procedimento pertinentes para a melhoria da continuidade de negócios, de forma a ter resultados alinhados com os objetivos.

Do (Implementar e operar) - Implementar e operar a política de continuidade de negócios, controles, processos e procedimentos.

Check (Monitorar e analisar criticamente) - Monitorar e analisar criticamente o desempenho em relação aos objetivos e política de continuidade de negócios, reportar os resultados para a direção para análise crítica, e definir e autorizar ações de melhorias e correções.

Act (Manter e Melhorar) - Manter e melhorar o SGCN tomando ações corretivas e preventivas, baseadas nos resultados da análise crítica da direção e reavaliando o escopo do SGCN e as políticas e objetivos de continuidade de negócios.

3 – Escopo e abrangência

O escopo e abrangência dessa Política de Recuperação Contra Desastres engloba não apenas os requisitos de segurança lógica, mas também os de segurança física, segurança dos processos e de pessoal, direta ou indiretamente relacionados com todos os departamentos da empresa.

4 – Integração com os procedimentos existentes

Os seguintes documentos são parte integrante dessa política e devem ter todo o seu conteúdo respeitado como todas as regras e diretrizes aqui descritas:

- Política de Privacidade Interna;
- Política de Privacidade Externa;
- Política de Proteção de Dados Pessoais;
- Termo de Confidencialidade dos Colaboradores;
- Contratos com Fornecedores;

5 – Análise dos processos de negócio

Para o perfeito entendimento do funcionamento da empresa, em busca das customizações e ajustes necessários pelas boas práticas de segurança, foi feito o mapeamento dos principais processos de negócio existentes. Esses processos foram detalhadamente analisados, pela ótica da segurança da informação, e as sugestões de melhoria foram registradas no plano de ações para adequação à LGPD. Cada ação desse plano possui uma data limite para implementação e responsável, detalhados em outro documento que foi apresentado à diretoria da empresa. A figura a seguir demonstra, de forma macro, quais processos de negócio foram analisados:

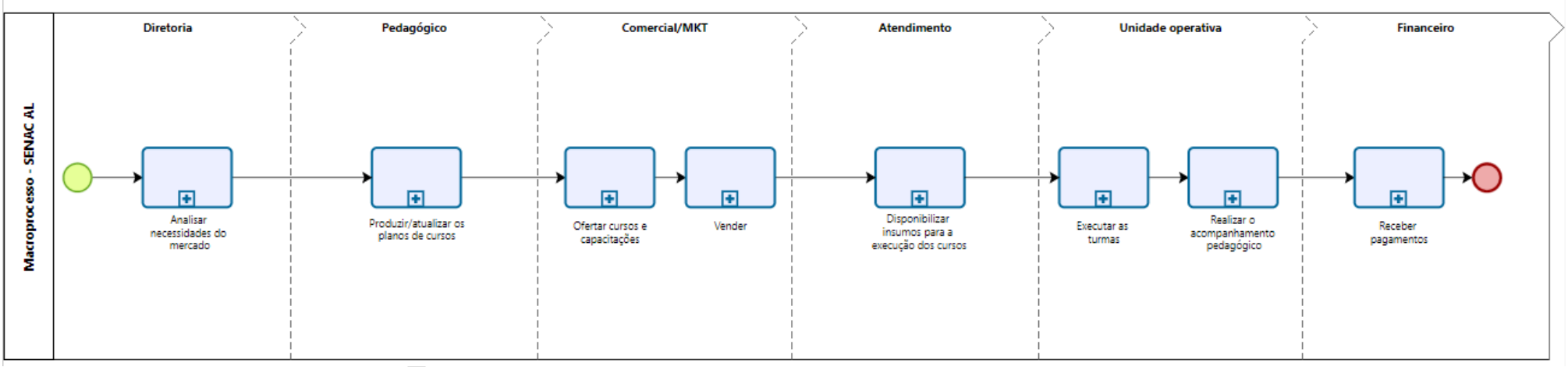


Figura 02 – Macroprocesso de negócio.

6 – Serviços Essenciais

São os seguintes serviços considerados essenciais, por ordem de priorização, para o acionamento e execução destes planos.

Serviço	Criticidade[1]	RPO[4]	RTO[3]	Impacto[2]			
				Financeiro	Legal	Imagem	Operacional
SIG	Alta	Backup mais recente	1 dia	Alto	Alto	Alto	Alto
SGA	Alta	Backup mais recente	1 dia	Alto	Alto	Médio	Alto
MXM	Alta	Backup mais recente	1 dia	Alto	Alto	Médio	Alto
RM TOTVS	Alta	Backup mais recente	1 dia	Alto	Alto	Médio	Alto
BNWEB	Média	Backup mais recente	1 dia	Médio	Médio	Médio	Médio
AVA	Alta	Backup mais recente	1 dia	Médio	Médio	Médio	Alto
SEND	Alta	Backup mais recente	1 dia	Médio	Médio	Médio	Médio
MIRA	Baixa	Backup mais recente	1 dia	Baixo	Médio	Médio	Baixo
Site	Média	Backup mais recente	1 dia	Médio	Médio	Alto	Médio

Serviço	Criticidade[1]	RPO[4]	RTO[3]	Impacto[2]			
				Financeiro	Legal	Imagem	Operacional
Intranet	Média	Backup mais recente	1 dia	Baixo	Baixo	Baixo	Médio
GLPI	Média	Backup mais recente	1 dia	Baixo	Baixo	Baixo	Médio
MySQL	Alta	Backup mais recente	1 dia	Alto	Alto	Médio	Alto
SQL server	Alta	Backup mais recente	1 dia	Alto	Alto	Médio	Alto
Links Internet	Alta	Backup mais recente	1 dia	Alto	Alto	Alto	Alto
E-mail Institucional	Alta	Backup mais recente	1 dia	Médio	Baixa	Médio	Médio
WK Radar	Alta	Backup mais recente	1 dia	Baixo	Alto	Baixo	Médio
Active Directory	Média	Backup mais recente	1 dia	Baixo	Baixo	Baixo	Alto
Rede WI-FI	Média	Backup mais recente	1 dia	Baixo	Baixo	Baixo	Médio
VPN	Baixa	Backup mais recente	1 dia	Baixo	Baixo	Baixo	Baixo

1 (A)lta, (M)édia, (B)aixa, (I)ndefinida.

2 (A)lto, (M)édio, (B)aixo, (I)ndefinido.

3 Período de tempo dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção.

4 Ponto em uma linha de tempo em que os dados devem ser recuperados após a ocorrência de uma ruptura.

A relação entre os principais processos de negócio, os sistemas mais importantes e os itens de infraestrutura de TI podem ser vistos na figura a seguir.

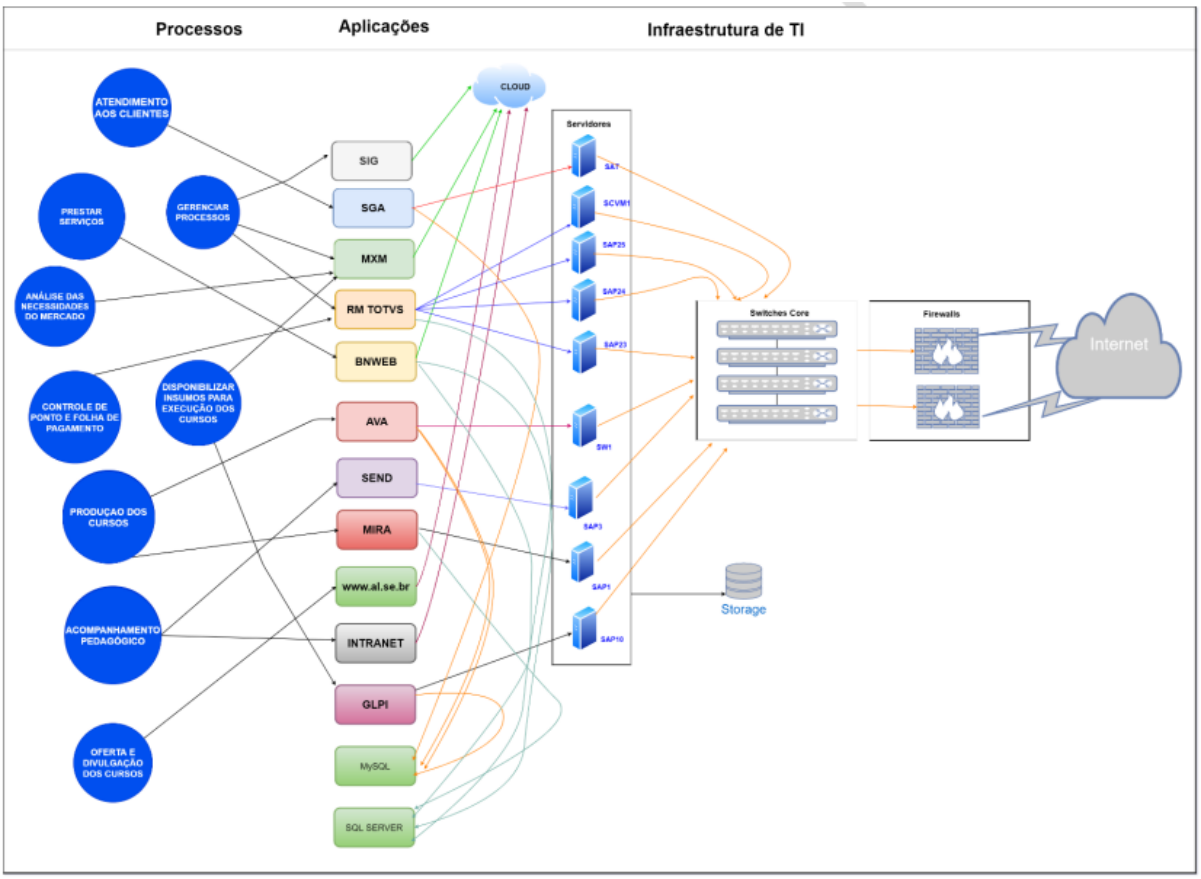


Figura 3 - Processos X Sistemas X Infraestrutura.

PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

7 – Objetivo do PAC

O PAC busca definir ações e responsabilidades das equipes envolvidas com o acionamento da contingência, antes, durante e após a ocorrência do desastre. Ele consiste em administrar todos os outros planos de Continuidade.

Representa a garantia mais eficaz em termos de administração em situações adversas. O PAC relaciona o funcionamento das equipes antes, durante e depois da ocorrência do evento. Através deste programa são definidos os planos de ação para o retorno à normalidade num determinado período.

Figura 4 - Tempo do PAC.

8 – Escopo do PAC

A abrangência deste plano é focada nas equipes e leva em conta os fatores históricos. Também considera os fatos que estão ocorrendo e por fim as ações futuras, que são delimitadas somente após a ocorrência de um evento.

9– Papéis e Responsabilidades

Comitê de privacidade e segurança da informação

- Propor ajustes, aprimoramentos e modificações desta Política;
- Analisar os casos de violação desta Política e das Normas de Segurança da Informação, encaminhando-os à diretoria, quando for o caso;
- Propor projetos e iniciativas relacionados à melhoria da segurança da informação e continuidade dos negócios;
- Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;
- Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;
- Avaliar essa política periodicamente e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.
- Responsável por todas as comunicações durante um desastre. Especificamente, eles se comunicarão com os funcionários, clientes, autoridades, fornecedores e até mesmo com a mídia, se necessário.

Atribuições e responsabilidades da Diretoria:

- Aprovar a Política de Recuperação Contra Desastres e suas revisões;
- Aprovar a nomeação dos membros do comitê de privacidade e segurança da informação;
- Definir, junto com os responsáveis, as estratégias para recuperação de incidentes ocorridos;
- Aprovar os investimentos necessários para manter a continuidade dos negócios;

Atribuições e responsabilidades do departamento de TI

- Avaliar os danos específicos de qualquer incidente para fornecer dados e conectividade de rede, incluindo WAN, LAN ou de infraestrutura externa junto aos prestadores de serviço.
- Garantir que o backup das informações críticas se encontra atualizado, testado e com uma cópia armazenada fora das instalações da empresa.
- Fornecer a infraestrutura de servidores físicos e virtuais necessária para que a empresa execute suas operações e processos essenciais durante um desastre.
- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes conforme necessário.
- Fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível. Eles precisarão provisionar todos os funcionários na solução de contingência e aqueles que trabalham remotamente com as ferramentas específicas à sua atuação.
- Analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas.
- Prover mecanismos de segurança no ambiente principal e alternativo, resguardando aplicações e dados e evitando que desdobramentos de segurança afetem o acionamento da continuidade;
- Executar os planos de ações, em caso de incidentes, para garantir o mais rápido retorno do funcionamento dos ativos críticos de TI;
- Prover todas as informações de gestão de segurança da informação solicitadas pelo Comitê;

- Oferecer orientação e treinamento sobre segurança e sobre a Política de Recuperação Contra Desastres e suas Normas a todos os colaboradores;
- Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação, mantendo-se atualizada em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;
- Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;
- Analisar os riscos relacionados à segurança da informação e apresentar relatórios periódicos sobre tais riscos ao Comitê, acompanhados de proposta de aperfeiçoamento do ambiente de controle, quando for o caso;
- Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações;
- Requisitar informações às demais áreas (diretorias, gerências, supervisões etc.), realizar testes e averiguações em sistemas e equipamentos com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação e estabelecer mecanismo de registro e controle de não conformidade a esta Política e às Normas de Segurança da Informação, comunicando sempre ao Comitê.
- Configurar o acesso remoto dos colaboradores a qualquer serviço da rede do SENAC AL, e-mails, sistemas, ferramentas de comunicação etc., apenas durante o horário comercial;
- Auditar os computadores dos visitantes em relação a ferramenta de antivírus atualizada e conexão em segmento de rede separado, quando for preciso se conectar na rede do SENAC AL;
- Criar um perfil de acesso, detalhando todas as permissões necessárias em todos os sistemas, para cada colaborador ou prestador de serviço do SENAC AL;

Atribuições e responsabilidades do DPO

- Analisar cada evento de desastre ocorrido para avaliar se houve comprometimento de dados pessoais e definir as ações necessárias previstas na LGPD;
- Contribuir na Definição das Políticas e Diretrizes do Programa de Governança em Privacidade;
- Gerir a Revisão da posição da organização como agente de tratamento de Dados Pessoais;
- Revisar práticas de Segurança da Informação voltadas a tratamento de Dados Pessoais e Dados Pessoais Sensíveis;
- Revisar e Propor melhorias no Processo de Gestão de Incidentes voltado a Dados Pessoais e Dados Pessoais Sensíveis;
- Revisar e Propor métodos de armazenamento e compartilhamento de dados seguros;
- Aprovar avaliação do impacto da proteção de dados (RIPD), de acordo com a metodologia definida;
- Acompanhamento e apoio nos projetos de software que envolvem Gestão de Privacidade de Dados Pessoais e Dados Pessoais Sensíveis;
- Aconselhar sobre proteção de dados na arquitetura de TI na organização;
- Aconselhar programadores e administradores de sistemas sobre a proteção prática de sistemas de acordo com as boas práticas;
- Aconselhar sobre tecnologias de aprimoramento da privacidade, incluindo criptografia, anonimização e pseudonimização;
- Coletar informações de violações de segurança;

- Apoiar a empresa no registro e documentação dos incidentes relacionados a privacidade e proteção de dados;
- Apoiar nas decisões do comitê de privacidade e acompanhar as ações relacionados aos incidentes;
- Apoiar a empresa na investigação de incidentes de segurança e privacidade;
- Entender o impacto do incidente e ajudar o cliente a gerir as crises objetivando evitar sanções;
- Ajudar a empresa a Notificar a Agência de Proteção e Dados sobre uma violação de segurança dentro do prazo estabelecido em Lei;
- Ajudar a empresa a Notificar os titulares dos dados da violação de segurança;
- Garantir a conformidade com os requisitos da LGPD;
- Realizar controle anual de conformidade de segurança de TI para Dados Pessoais e Dados Pessoais Sensíveis;
- Ajudar a empresa a garantir mais foco na segurança de TI para Dados Pessoais e Dados Pessoais Sensíveis;
- Criar recomendações técnicas e operacionais para proteger sistemas, redes e dispositivos;
- Apresentar relatórios de acompanhamento de nível de conformidade com a LGPD e segurança da TI para a Administração.

10 Atividades e papéis principais

Caberá ao mais alto Gestor de TI em exercício, atuar como elo de ligação entre o corpo técnico e as áreas interessadas ou afetadas pela não Continuidade de Negócios. Além disso, poderá ter representação pontual no Comitê Permanente de Gestão de Crises, sempre que a crise for relacionada a Tecnologia da Informação e Comunicação.

11 Condições para ativação do plano

Este plano será acionado quando da ocorrência de algum dos cenários de desastres, a ocorrência de um risco desconhecido ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada. O plano também poderá ser invocado em casos de testes ou por determinação do gestor de TI em conjunto com a alta administração da empresa. Os integrantes do comitê de privacidade e segurança da informação serão responsáveis por acionar os contatos e partes interessadas, prioritariamente por telefone, ou pessoalmente caso seja possível.

Os principais contatos estão descritos na tabela a seguir:

Tipo de incidente	Empresa	Telefone
Problemas com energia elétrica	EQUATORIAL	0800 082 0196
Problemas com incêndios	BOMBEIROS	193
Problemas de roubo ou assalto	Polícia Militar Polícia Civil	190 3213-1119
Problemas de infraestrutura civil	Defesa Civil	3246-3453

Tipo de incidente	Empresa	Telefone
Problemas de saúde com colaboradores, alunos ou visitantes	SAMU	192

12 Lista de tarefas e ações

A gestão da(s) crise(s) na área de TIC deverá ser executada conforme o tipo da crise, seguindo uma linha geral de procedimentos listados:

1. O Gestor de TI deve avaliar a extensão do que foi avariado;
2. Diretor responsável pela área de TI deve ser informado para buscar soluções para a gestão da crise;
3. Deve-se instituir o Comitê Permanente de Gestão de Crises com os membros diretamente ligados à área onde aconteceu o problema;
4. Montar um centro de Gerenciamento de Incidentes em local disponível e seguro.

O desenho a seguir mostra o fluxo de atividades para gerenciamento de crise para um desastre ocorrido.

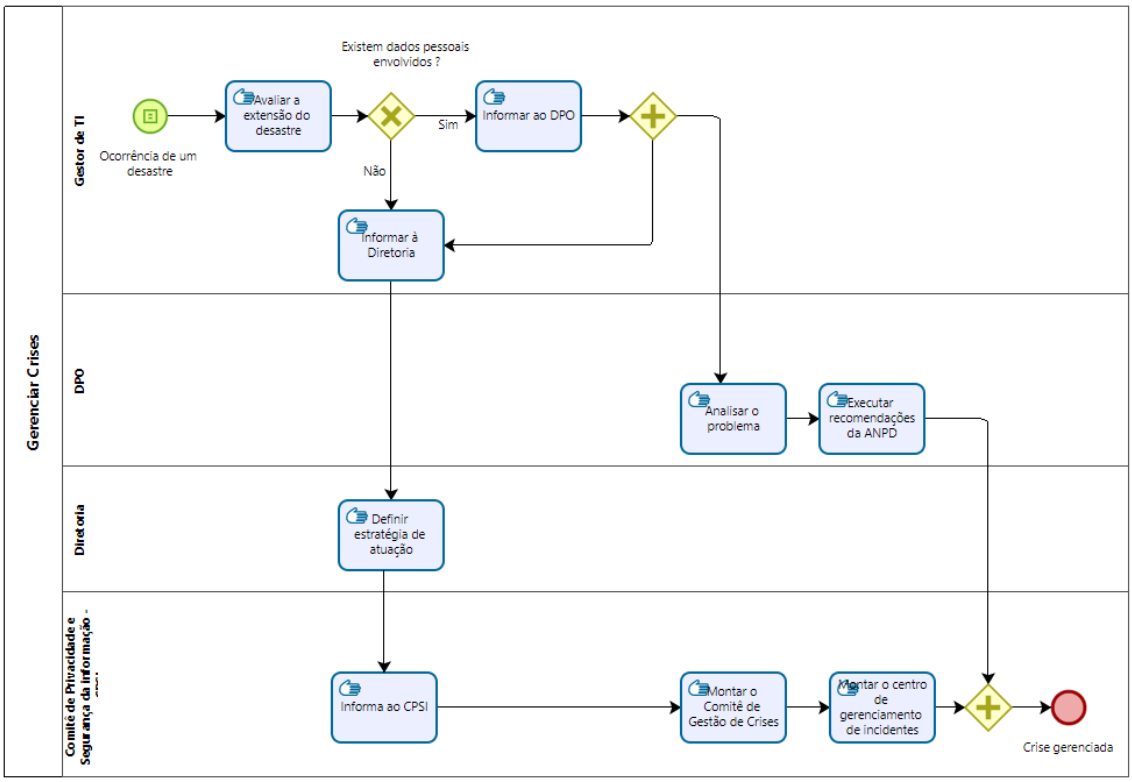


Figura 5 - Fluxo do gerenciamento de crises.

13 Encerramento do plano de gerenciamento de crises

O plano será encerrado assim que o funcionamento dos sistemas essenciais estiver validado. A equipe responsável pelo retorno deve emitir um parecer relatando as atividades realizadas para o gestor de TI, que por sua vez deve informar do retorno das atividades à instituição.

PLANO DE CONTINGÊNCIA (PC)

14 – Objetivo do PC

Este documento busca estabelecer um plano para recuperação após desastres, com objetivo de assegurar o restabelecimento das atividades da empresa. Seu propósito é listar um conjunto de procedimentos definidos formalmente para permitir que serviços de processamento e armazenamento de dados continuem a operar, mesmo que com um certo grau de degradação, caso ocorra algum evento que não possibilita seu funcionamento normal.

15 – Principais ameaças

Este plano deve ser acionado quando da ocorrência de cenários de desastres que apresentam risco à continuidade dos serviços essenciais. Os principais eventos e suas causas estão descritos na tabela a seguir.

Evento	Possível causa
Interrupção de energia elétrica	Problemas na rede elétrica externa; Problemas na rede elétrica interna; Problemas em nobreaks;
Falha da climatização do Data Center	Superaquecimento dos ativos devido a falha no dimensionamento do equipamento; Problemas técnicos no equipamento;
Falha humana	Acidente ao manusear ativos críticos de TI
Ataques internos	Ataques internos aos ativos críticos de TI
Incêndio	Incêndio iniciado nas instalações externas da empresa Incêndio iniciado nas instalações internas da empresa

Evento	Possível causa
Desastres naturais	Terremotos, tempestades, alagamento, desabamento etc.
Falha de Hardware	Falha que necessite de reposição de peça ou reparo de algum equipamento
Ataque cibernético	Ataque virtual que comprometa a disponibilidade, integridade ou disponibilidade dos serviços críticos da instituição
Indisponibilidade de colaborador	Doenças, Licenças etc.

16 Lista de tarefas e ações

São recomendadas algumas etapas a serem seguidas para um Plano de Contingência de TI.

- ✓ **Diagnóstico** – consiste na identificação dos pontos fracos que poderiam ser foco de problemas para o setor de TI da empresa.
- ✓ **Análise de riscos** – A partir das vulnerabilidades, deve-se considerar as possíveis ameaças e os fatores que possam levar à concretização desses riscos, como o ataque de vírus e a ausência de um antivírus corporativo.
- ✓ **Definição de prioridades** – Identificar os processos vitais da empresa e apontar quais os sistemas que precisam ser recuperados primeiro ou preferencialmente em casos de problemas.
- ✓ **Determinação de estratégias** – Esse é o caminho para se definir como cada sistema deve ser recuperado (usando softwares ou aplicações), quando e quem são os responsáveis por isso.
- ✓ **Redação e divulgação do documento** – o plano de contingência precisa ser detalhadamente redigido e divulgado para que os envolvidos conheçam seus papéis no processo de gerenciamento de crises, bem como as estratégias a serem seguidas em cada caso.

17 Soluções para contingências previstas

Em caso de desastres e catástrofes naturais ou não, estão disponíveis os seguintes artefatos:

- **Incêndio**: Os equipamentos de combate a incêndio estão presentes em todas as unidades.
- **Energia elétrica**: Existem dois nobreaks para proteção do sistema de fornecimento de energia.
- **Condicionadores de ar**: Existem dois aparelhos de ar condicionado na sala dos servidores para garantir uma redundância em caso de falhas de um dos equipamentos.
- **Serviço de internet**: A rede sem fio da Sede é segmentada em ambiente público e privado e é sustentada por 10 Access Point da marca Ruckus. A rede WAN é composta por dois WatchGuards M370 na sede com HA, dois WatchGuards T70 na Carlo Melito e Arapiraca e o modelo T35 nos postos avançados de União dos Palmares e Palmeiras dos Índios. O Centro Gastronómico é interligado via fibra com a rede da Carlo Melito. Os firewalls da sede utilizam dois links de Internet, sendo um link da Alfa de 150Mbps e outro da 1Telecom de 300 Mbps, ambos para a rede corporativa.
- **Perda acidental de documentos**: Deve solicitar a restauração do backup dos arquivos ao setor de TI, segundo disposições da Política de Backup Corporativa.

18 Encerramento do plano de contingência

O plano será encerrado assim que o funcionamento dos sistemas essenciais estiver validado. A equipe responsável pelo retorno deve emitir um parecer relatando as atividades realizadas para o gestor de TI, que por sua vez deve informar do retorno das atividades à instituição.

PLANO DE CONTINGÊNCIA (PC)

19 – Objetivo do PCO

Este documento tem como objetivo restabelecer o funcionamento dos principais ativos que suportam a operação de TI da empresa, reduzindo o tempo de queda e os impactos provocados por eventual incidente.

Este plano é composto por um conjunto de procedimentos previamente definidos, destinados a manter a continuidade dos processos de negócios e serviços vitais de uma organização. Através do PCO, os gestores dos processos de negócios saberão como agir na falta ou falha de algum componente que o suporte, garantindo a continuidade do processo de negócio reduzindo o impacto no negócio da Organização.

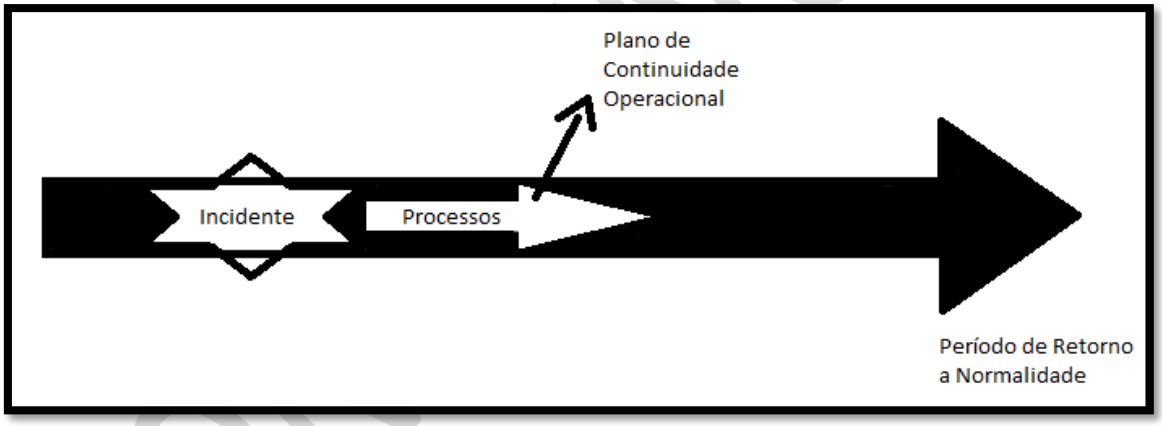


Figura 6 - Tempo do PCO.

19 – Escopo do PCO

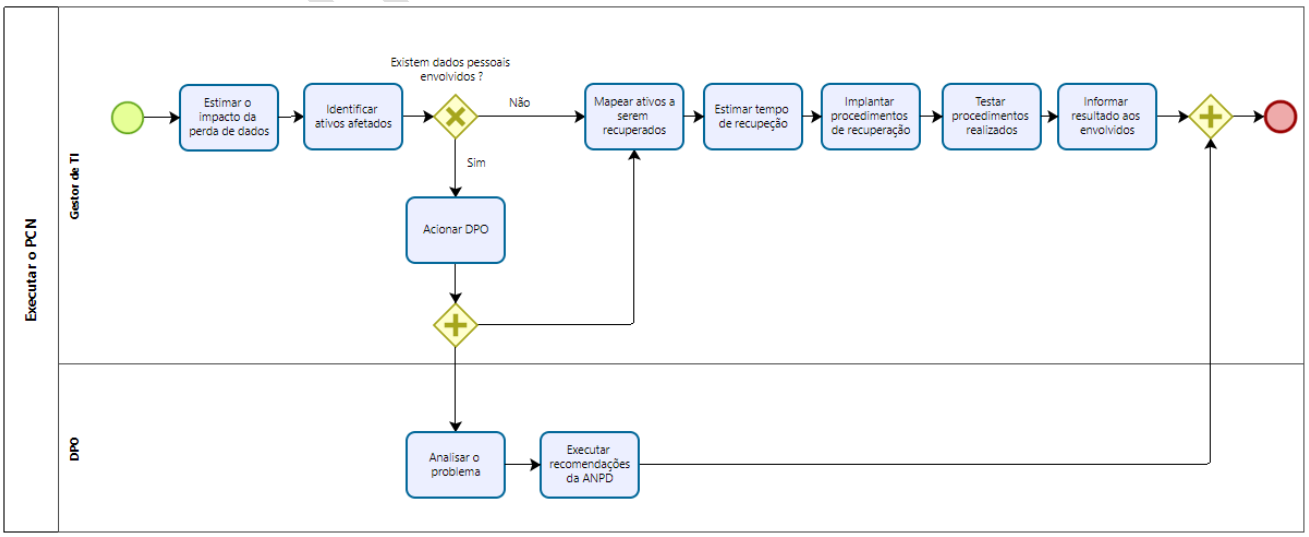
Este plano se aplica ao prédio onde está localizada a matriz do SENAC AL, contendo o Data Center e os seus principais ativos de TI.

20 Lista de tarefas e ações

As etapas aqui realizadas são denominadas “Procedimentos de Retomada”. O gestor de TI deve:

1. Estimar impacto de perda de dados;
2. Identificar ativos afetados;
3. Notificar o DPO, caso existam dados pessoais envolvidos, para execução das obrigações previstas na LGPD;
4. Mapear ativos a serem recuperados;
5. Estimar volume de dados a serem recuperados, tempo de recuperação e possíveis perdas operacionais;
6. Implantar procedimentos de recuperação;
7. Testar procedimentos realizados;

O desenho a seguir mostra o fluxo de atividades para gerenciamento de crise para um desastre ocorrido.



21 Encerramento do plano de continuidade dos negócios

O plano será encerrado assim que o funcionamento dos sistemas essenciais estiver validado. A equipe responsável pelo retorno deve emitir um parecer relatando as atividades realizadas para o gestor de TI, que por sua vez deve informar do retorno das atividades à instituição.

PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

22 – Objetivo do PRD

Este documento determina o plano para que, uma vez controlada a contingência e passada a crise, a organização retorne aos seus níveis normais de operação. Além de avaliar possíveis vulnerabilidades dos componentes que suportam os processos de negócios críticos ao se deparar com eventos. Cabe executar um mapeamento e planejamento de sua recuperação ou restauração, sempre considerando as necessidades da empresa.

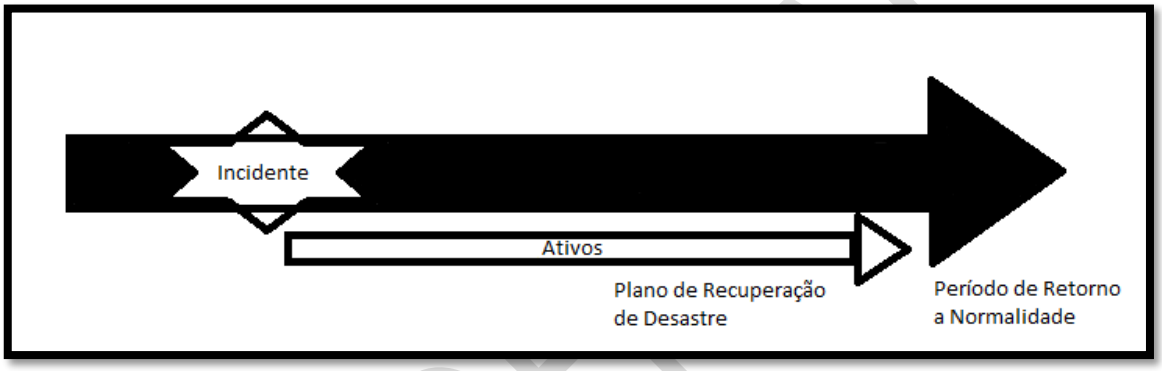


Figura 7 - Tempo do PRD.

23 – Escopo do PRD

Este documento se restringe a última etapa da recuperação de desastres. Visa garantir o retorno à normalidade das operações e não mais sua recorrência no caso de riscos controláveis.

24 Lista de tarefas e ações

Os processos aqui realizados são denominados “Procedimentos de Recuperação ou Restauração”. As seguintes macros etapas devem ser necessárias para normalizar os serviços de forma ampla:

1. **Identificar ativos danificados**: O Gestor de TI deve listar ativos danificados com a ocorrência de um desastre.

2. **Listar serviços interrompidos**: O Gestor de TI deve identificar interrupções de conexões e acessos gerados, informando abrangência.

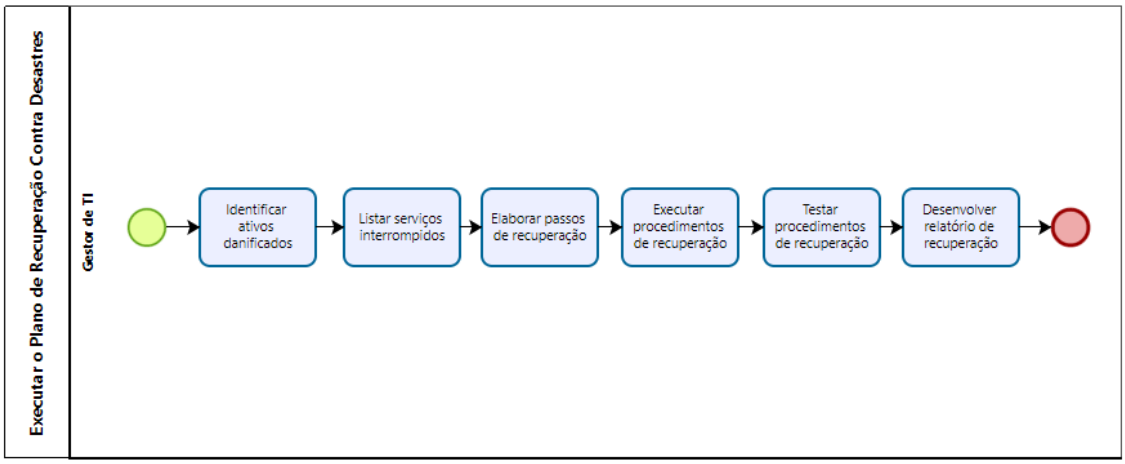
3. **Elaborar passos de recuperação**: O Gestor de TI deve manter seu Catálogo de Serviços atualizado e informar componentes necessários para a plena operação de todos os ativos físicos (servidores, banco de dados, storages, switches), assim como suas configurações através de diagramas e documentação. Com isso O Gestor de TI deve elaborar um cronograma de recuperação de aplicações, levando em conta os prazos de entrega dos fornecedores.

4. **Executar ciclos de recuperação**: Substituir ativos perdidos, reconfigurar ativos que podem ser reparados ou reconfigurados.

5. **Testar procedimentos de recuperação**: O Gestor de TI deve testar os ativos de forma a garantir que o processo de recuperação esteja conforme o planejado. Este teste deve garantir os mesmos níveis anteriores ao desastre.

6. **Desenvolver relatório do que foi realizado**: desenvolver relatório com todos os problemas encontrados e como foi resolvido.

O desenho a seguir mostra o fluxo de atividades para gerenciamento de crise para um desastre ocorrido.



No caso de possível perda de dados ao restaurar os serviços, deverão ser avaliadas opções de ponto de restauração do último backup disponível. Neste caso a restauração dependerá da disponibilidade de backup, sendo que cabe ao Gestor de TI avaliar a forma disponível que seja mais confiável e rápida de acordo com a Política de Backup da empresa.

Caso possível, deverá ser provido estimativas de prazos para restabelecimento dos serviços, tendo em vista o cálculo que depende do volume de dados gerados. Demais etapas que envolvam operacionalização de restauração e testes, estão explicitados na Política de Plano de Backup da empresa.

25 – Referências bibliográficas

- ✓ ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT ISO/IEC Guia 73:2009: Gestão de riscos – Vocabulário. Rio de Janeiro: ABNT, 2009a.
- ✓ ABNT NBR 15999-1:2007 – Gestão de Continuidade de Negócios – Código de Prática. Rio de Janeiro: ABNT, 2007.
- ✓ ABNT NBR 15999-2: Gestão de continuidade de negócios – Parte 2: Requisitos. Rio de Janeiro: ABNT, 2008a.
- ✓ ABNT NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.
- ✓ NBR ISO 31000:2009 – Gestão de Riscos – Princípios e Diretrizes. Rio de Janeiro: ABNT, 2009b.
- ✓ ABNT NBR ISO/IEC 27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2008b
- ✓ ABNT NBR ISO/IEC 22301: 2013 Segurança da Sociedade — Sistema de Gestão de Continuidade de Negócios — Requisitos. Rio de Janeiro: ABNT, 2013.
- ✓ ABNT NBR ISO/IEC 22313: 2015 Segurança da Sociedade — Sistema de Gestão de Continuidade de Negócios — Orientações. Rio de Janeiro: ABNT, 2015.
- ✓ ABNT NBR ISO/IEC 31010:2012. Gestão de riscos — Técnicas para o processo de avaliação de riscos. ABNT - Associação Brasileira de Normas Técnicas, 2012.
- ✓ ABNT NBR ISO/IEC 38500:2015. Governança de tecnologia da informação para a organização. ABNT - Associação Brasileira de Normas Técnicas, 2015.
- ✓ ABNT NBR ISO/IEC 15999-1:2007. Gestão de Continuidade de Negócios. Parte 1: Código de Prática. ABNT - Associação Brasileira de Normas Técnicas, 2007.
- ✓ ABNT NBR ISO/IEC 17799:2005. Tecnologia da Informação - Técnicas de Segurança - Código de Práticas para a Gestão de Segurança da Informação. ABNT - Associação Brasileira de Normas Técnicas, 2005.

ANEXO I – Conceitos e definições

- **Ameaça**: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;
- **Ativos de informação**: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
- **Capacitação em SIC**: saber o que é segurança da informação e comunicações, aplicando em sua rotina pessoal e profissional, servindo como multiplicador do tema e aplicando os conceitos e procedimentos na organização como gestor de SIC;
- **Classificação da informação**: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;
- **Comitê Gestor de Privacidade**: Comitê de caráter deliberativo, responsável pela normatização e supervisão da segurança da informação;
- **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
- **Conscientização em SIC**: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema;
- **Controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

- **Custodiante do ativo de informação**: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;
- **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido;
- **Gestão de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;
- **Gestão de continuidade dos negócios**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;
- **Gerenciamento de operações e comunicações**: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporte, satisfazendo os acordos de níveis de serviço;
- **Gestão de riscos de segurança da informação e comunicações - GRSIC**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação;
- **Gestão de segurança da informação e comunicações - GSIC**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;
- **Incidente de Segurança**: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma

atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

- **Informação**: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;
- **Infraestrutura de TI**: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;
- **Integridade**: propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental;
- **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
- **Recursos criptográficos**: sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;
- **Risco**: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
- **Segurança física e do ambiente**: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;
- **Sensibilização em SIC**: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional;
- **Terceiros**: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao SENAC AL;
- **Tratamento de incidentes**: é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

- **Tratamento da informação**: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação; e
- **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaça.