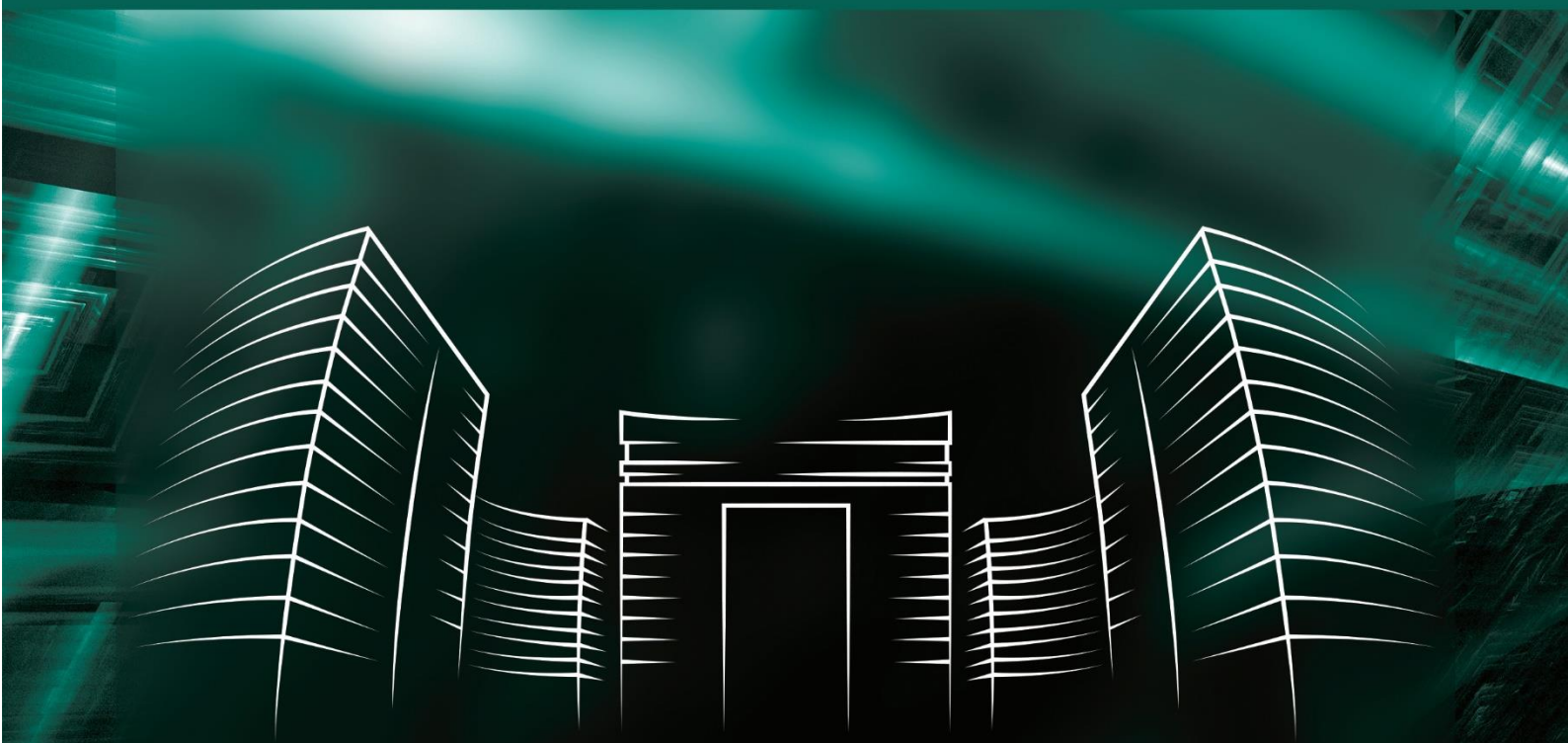
PLANO DE CONTINUIDADE DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PCTIC



2022

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Delner Freire
Superintendente

Abdenildo Deividy Sobreira dos Santos
Diretor Técnico

COORDENADOR DE SEGURANÇA DA INFORMAÇÃO

Leonardo Courinos Lima da Silva
Coordenador

ELABORAÇÃO

Rosemeire Vidal
Daltro Barbosa

REVISÃO

Anderson Gomes de Souza
Diego da Silva Oliveira
Ed Carlos Egert Galvão
Eduardo Falkemback Zimmer
Idan Luiz Souza Santos
Jean Franco Ronconi de Lima
Leonardo Courinos
Luma Damon de Oliveira Melo
Ricardo Fernandes Neto da Silva
Sâmara Ascoli de Queiroz
Tiago Lopes de Aguiar
Valéria Rodrigues da Silva

VERSÃO

VERSÃO	DATA	AUTOR	AÇÃO
1.0	22.09.2022	Rosemeire Vidal e Daltro Barbosa	Elaboração do Plano de Continuidade.

LISTA DE ABREVIATURAS E GLOSSÁRIO

SETIC	Superintendência Estadual de Tecnologia da Informação e Comunicação
COSEGI	Coordenadoria de Segurança da Informação
PSI	Política de Segurança da Informação
CAF	Coordenadoria de Administração e Finanças
CAGD	Coordenadoria de Análise e Gestão de Dados
COGE	Coordenadoria de Gestão Estratégica
CODE	Coordenadoria de Desenvolvimento
COINFRA	Coordenadoria de Infraestrutura e Serviços
CPSI	Comissão Permanente de Segurança da Informação
DOD	Documento de oficialização de demanda
ETP	Estudo Técnico Preliminar
LGPD	Lei Geral de Proteção de Dados Pessoais
TIC	Tecnologia da Informação e Comunicação
PDCA	Ciclo Plan (Planejar), Do (Fazer), Check (Checar), Act (Agir). É um mecanismo interativo e contínuo de administração baseada nessas quatro etapas.
PCTIC	Plano de Continuidade de Tecnologia da Informação e Comunicação
PGISI	Plano de Gestão de Incidente de Segurança da Informação
TR	Termo de Referência
EqT	Equipes de Tratamento

Para os efeitos deste plano, serão utilizados os conceitos e definições do Glossário de Segurança da Informação do Departamento de Segurança da Informação - DSI do Gabinete de Segurança Institucional da Presidência da República - GSI/PR, instituído pela Portaria Nº 93, de 26 de setembro de 2019 (Glossário de Segurança da Informação).

SUMÁRIO

1 INTRODUÇÃO

A Coordenadoria de Segurança da Informação - COSEGI, tem como uma de suas atribuições, manter a segurança cibernética do ecossistema digital da Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC.

Este documento observa a importância de se estabelecer objetivos, princípios e diretrizes da NBR ISO/IEC 27001:2013, que trata da segurança da informação; da norma NBR ISO/IEC 27005:2019, que trata da gestão de riscos segurança da informação; a lei nº 13.709/2018, com a redação dada pela Lei no 13.853/2019, sobre a proteção de dados pessoais e o que dispõe a Portaria nº 87 de 03 de setembro de 2021 que Regulamenta a Comissão Permanente de Segurança da Informação - CPSI.

A segurança da informação abrange segurança cibernética, defesa cibernética, segurança física, proteção de dados organizacionais e as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

O Plano de Continuidade e Recuperação de TIC fornece estratégias para garantir que serviços essenciais sejam identificados e mantidos, também provê quais planos devem ser realizados em cada momento para manter sua preservação após a ocorrência de um desastre até o retorno da situação normal de funcionamento da instituição.

É um instrumento que visa a redução de interrupção das atividades do negócio e proteção dos processos críticos contra defeitos, falhas ou desastres, promovendo a retomada em tempo hábil.

Este plano de continuidade é de nível macro e dividido em estratégias de continuidade através de 4 (quatro) planos menores a conhecer: Plano de Administração de Crises - PAC, Plano de Continuidade Operacional - PCO, Plano de Recuperação de Desastres - PRD, e Plano de Teste e Validação (PTV), os quais fornecem basicamente: objetivo, papéis e responsabilidade, condições para ativação dos planos, procedimentos que devem ser adotados, comunicação e encerramento do plano. Para cada plano, deverão ser ativados os procedimentos preconizados, assim como dar-se os ocorridos, com base na

temporalidade e impactos. Os registros dos ocorridos devem formar um banco de registros, para que em cada acontecimento seja possível verificar o que foi feito anteriormente.

2 ESCOPO

O Plano de Continuidade de TIC deverá abranger os 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:

1. Atendimento aos usuários internos, externos e parceiros, conforme a Política de Segurança da Informação - PSI da SETIC;
2. Alternativas estratégicas, táticas e operacionais para responder a interrupções;
3. Prevenir novas perdas ou indisponibilidade de atividades prioritárias;
4. Determinação de como e em que circunstâncias a CPSI irá comunicar com as partes interessadas ou contatos de emergência.

Este plano é focado na segurança dos ativos de informação e leva em consideração 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.

A gestão de riscos de TIC tem uma missão permanente de identificar vulnerabilidades e adotar estratégias para proteger a infraestrutura e sistemas da SETIC. Além disso, deve-se obter dados para avaliar o sucesso dessas ações e aperfeiçoá-las continuamente.

3 VIGÊNCIA, ABRANGÊNCIA E REVISÃO

Este plano de Continuidade de TIC tem vigência de 2 (dois) anos com abrangência na Superintendência de Tecnologia da Informação e Comunicação - SETIC.

A revisão do Plano de continuidade de TIC pode ser realizada nas seguintes situações:

1. Em no máximo 2 (dois) anos;
2. Nos momentos em que a Comissão Permanente de Segurança da Informação - CPSI julgar necessário;
3. Em decorrência dos resultados dos testes realizados; ou
4. Após a ocorrência de algum evento ou mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

4 METODOLOGIA

O processo de elaboração foi realizado em conjunto com servidores da COSEGI e COINFRA. As reuniões ocorreram através de metodologia geradora de ideias chamada *Brainstorming*, validando os ativos identificados anteriormente, análise dos serviços fornecidos e o cenário de cada ativo, impacto, probabilidade, respostas aos riscos e monitoramento.

Este plano baseou-se em normas e pesquisas de outras instituições, políticas internas e reuniões de levantamento e análise de cenário com todas as áreas envolvidas.

Este documento foi aprovado pela Comissão Permanente de Segurança da Informação - CPSI, através de reunião ordinária e a aprovação da Superintendência da SETIC.

Como metodologia para o funcionamento deste Plano de Continuidade de TIC é o alinhamento ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme definido na Norma Complementar nº 02/DSIC/GSIPR, publicada no Diário Oficial da União nº 199, Seção 1, de 14 de outubro de 2008, de modo a fomentar a sua melhoria contínua.

5 PRINCIPAIS RISCOS

A análise dos principais riscos elencados abaixo, visa garantir a continuidade dos serviços. Os riscos e ameaças podem afetar os serviços essenciais e devem ser identificados, avaliados, tratados, monitorados, controlados e documentados, de forma a mitigar os impactos na continuidade dos serviços de TI.

Possíveis Desastres	Possíveis Causas	Controle
1. Interrupção de Energia Elétrica	- Paralisação do fornecimento de energia elétrica pela concessionaria local. - Rede elétrica interna com curto-circuito, incêndio e infiltração. - Falha do Grupo Gerador.	- Se possível, contratar segundo canal de fornecimento de energia elétrica. - Solicitar manutenção elétrica da SUGESP. - Solicitar manutenção e testes periódicos no Grupo Gerador.
2. Incêndio	- Ações humanas. - Curto circuitos. - Queimadas.	- Extintores. - Profissionais de combate a incêndio para Data Center.
3. Falha na Climatização	- Mal funcionamento das condicionadoras de ar-condicionado; - Falha no fornecimento de energia elétrica.	- Monitoramento da temperatura, com alarme no ambiente ao ultrapassar o limite de temperatura permitido.
4. Falha de conexão na solução de Backup	- Erros de comunicação da rede. - Queda ou oscilação de energia elétrica. - cópia não disponível	- Monitoramento contínuo na estratégia de criação e restauração de backups. - Sistema mais robusto de Storage.
5. Ataques Cibernéticos	- Desatualização de Sistemas operacionais e softwares. - Falha humana relacionada a configuração das regras de segurança dos Sistemas de detecção de intrusos. -Vulnerabilidades ou erros de configuração em equipamentos, serviços e sistemas operacionais.	- Atualização dos Sistemas Operacionais. - Realizar treinamentos periódicos. - Planos de Gestão de Incidentes e de Continuidade dos serviços atualizados.
6. Desastres Naturais	- Vendavais. - Tempestades. - Alagamento. - Raios	- Infraestrutura de serviços redundante em nuvem computacional.
7. Falha de Hardware	- Queima de componentes eletrônicos.	- Aquisição de hardware redundante.
8. Indisponibilidade de rede/circuitos	- Rompimento de fibra óptica decorrente de execução obras públicas, desastres ou acidentes. - Mal funcionamento de switch gerenciador de segmento de rede. - Interrupção dos serviços de conectividade com as operadoras de telecomunicação por mais de 12 horas.	- Manutenção constante. - Treinamento. - Redundância.

Tabela 1 - Riscos. Fonte: Próprio Autor

6 SOLUÇÕES PARA CONTINGÊNCIAS PREVISTAS

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

- **Incêndio**: Extintor de incêndio portátil com carga de pó químico para combate em princípio de incêndio classe B/C (Combustíveis líquidos e equipamentos energizados) específico para Equipamentos Elétricos, localizado nas duas salas de Data Center, somando um total de 6 (seis) unidades distribuídas nas duas salas.

- **Energia Elétrica**: Há 2 (dois) sistemas de Fonte de Energia Ininterrupta (UPS ou *nobreak*) com banco de baterias independentes para o momento da queda de energia, até que o gerador entre em funcionamento. Os equipamentos de *nobreak* são gerenciados pela COINFRA e mantém contrato de manutenção trimestral, os geradores e manutenção elétrica são gerenciados pela equipe da SUGESP.

- **Condicionadores de ar**: Existem um total de 7 (sete) unidades de centrais de ar-condicionado adequados para a refrigeração dos equipamentos instalados nas duas salas de Data Center.

- **Serviço de Internet**: Os acessos são providos pela SETIC, que possui links redundantes de internet, por meio de fibra óptica.

7 PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades são definidos a fim de garantir a eficiência na execução deste plano. Estes papéis são fundamentais para a eficiência da continuidade de serviços de TI.

> *Conforme a **IN GSI/PR Nº 3**, de 28 de maio de 2021, Art. 16. Cabe ao gestor de segurança da informação de cada órgão ou entidade:*
> *I - coordenar a gestão de riscos de segurança da informação;*
> *II - designar o agente responsável pela gestão de riscos de segurança da informação, dentre os servidores efetivos do órgão;*

III - aprovar o plano de gestão de riscos de segurança da informação;
IV - aprovar o relatório de identificação, análise e avaliação dos riscos de segurança da informação e encaminhá-lo à alta administração;
V - aprovar o relatório de tratamento de riscos de segurança da informação; e
VI - propor medidas preventivas à alta administração.
Art. 17. Cabe ao agente responsável pela gestão de riscos de segurança da informação elaborar:
I - o plano de gestão de riscos de segurança da informação;
II - o relatório de identificação, análise e avaliação dos riscos de segurança da informação; e
III - o relatório de tratamento de riscos de segurança da informação.

Comissão Permanente de Segurança da Informação - CPSI.

- Implantar e garantir a conformidade com as políticas internas de segurança da informação e comunicação, atuar como responsável por este plano e determinar a gestão das informações de guarda da SETIC;
- Tratar incidentes de segurança da informação;
- Propor iniciativas para aumentar o nível de segurança da informação;
- Avaliar o Plano de Continuidade periodicamente e decidir pelo seu acionamento quando da ocorrência de desastres; e
- Responsável por munir a ASCOM de informações durante um desastre, para realizar a comunicação com os funcionários, clientes, autoridades, fornecedores e até mesmo com a mídia, se necessário.

Coordenação Segurança da Informação.

- Coordenar e assessorar a implantação e o funcionamento do Sistema de Gestão de Segurança da Informação;
- Implantar e garantir a conformidade com as políticas de segurança e informações internas;
- Assegurar a disponibilidade de recursos de conectividade para a operação e integração das plataformas, interoperabilidade das aplicações com serviços dos órgãos do Poder Executivo Estadual com demais conveniados na Rede Governamental;

- Adotar controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware; e
- Estabelecer diretrizes, padrões e normas de Segurança da Tecnologia da Informação e submetê-los à CPSI.

Equipe de Tratamento.

- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios, durante ocorrência de desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes de TIC, conforme necessidade;
- Responsável por analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação de dados;
- Avaliar os danos específicos de qualquer infraestrutura de rede no fornecimento de dados e supervisionar a execução do Plano de Continuidade;
- Manter a infraestrutura de serviços físicos e virtuais necessárias para a execução das operações e processos essenciais durante um desastre;
- Responsável pelas instalações físicas que abrigam sistemas de TI e pela garantia que as instalações de alternativa são mantidas adequadamente;
- Fornecer aos usuários as ferramentas de que necessitam para desempenhar suas funções de forma mais rápida e eficiente possível. É necessário provisionar todos os serviços no ambiente de contingência;
- A CPSI administrará e manterá o PCTIC, bem como definir cronograma de testes de viabilidade do plano constantemente;
- Formular estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas;
- Promover mecanismos de segurança no ambiente principal e no ambiente do container, localizado no CIRETRAN;
- Monitorar e Analisar os ambientes de datacenter principal e de contingência; e

- Realizar cópias dos dados armazenados nos servidores para que possam ser restaurados em caso de perda dos dados originais.

8 INVOCAÇÃO DO PLANO

O PCTIC será invocado pelas Equipes de Tratamento e pela CPSI quando da ocorrência de algum dos cenários desastres, insurgência, mediante a ocorrência de um incidente crítico ou caso de vulnerabilidade com alta probabilidade de ser explorada.

O Plano também poderá ser invocado em casos de testes ou por determinação da CPSI em consonância com a Superintendência da SETIC.

O rito de tratamento dos eventos definidos neste PCTIC está disposto abaixo e definidos nos sub planos inerentes para cada área de atuação, quando da ocorrência de um desastre.

As atividades a serem realizadas, a saber:

- Acionamento através do contato do Presidente da CPSI ou equipes de tratamento (anexo I), e em casos possíveis através dos canais de entrada como GLPI e SEI;
- Identificação e declaração de desastres;
- Avaliação e prevenção da agravação de danos;
- Ativação da solução de Contingência necessária;
- Reparação e reconstrução da instalação principal; e
- Retorno das operações para o Ambiente principal.

A organização dos subplanos, juntamente com os seus objetivos estão da seguinte forma:

- **Plano de Administração de Crises (PAC)**: Definição das atividades das equipes envolvidas e gerenciar as ações de contingência e comunicação durante e após a ocorrência de um desastre, com intuito de minimizar impactos, até a superação da crise.

- **Plano de Continuidade Operacional (PCO)**: Seu objetivo é garantir a continuidade dos serviços essenciais de TIC na ocorrência de um incidente ou descontinuidade, enquanto recupera-se o ambiente principal. O PCO é principalmente orientado aos processos (sistemas) e serviços.
- **Plano de Recuperação de Desastre (PRD)**: Seu objetivo é planejar e agir de forma que, uma vez controlada a contingência e passada a crise, a SETIC retorne seus níveis originais de operações no ambiente principal.
- **Plano de Testes e Validação (PTV)**: Este plano define a periodicidade e tipos de teste que serão realizados, a fim de manter o Plano de continuidade da SETIC apto a funcionar após ser testado e exercitado.

O acionamento poderá ocorrer através das equipes e contatos abaixo, prioritariamente por telefone, aplicativo de troca de mensagens, ou pessoalmente havendo a possibilidade ou de acordo com a gravidade do ocorrido.

Árvore de Acionamento de Contatos

Presidente da CPSI: Leonardo Courinos

E-mail: leonardocourinos@setic.ro.gov.br

Vice-Presidente: Rogério Eduardo

E-mail: rogerioalves@setic.ro.gov.br

Central de atendimento da SETIC:

69 3212-9513

WhatsApp: 9.8446-0144

www.atendimento.setic.ro.gov.br

Equipes de Tratamento:

INFOVIA	
Equipe de Tratamento:	Francismar Alves Waldemar Passarinho Caê Aires José José Kerlon de Oliveira Teo Cabral Marcos Aurélio

E-mail:	infovia@setic.ro.gov.br
Canal de atendimento:	atendimento.setic.ro.gov.br

CODE/DEV

Equipe de Tratamento:	João Batista Matheus Maia
E-mail:	setic.comissaotecnica@gmail.com
Canal de atendimento:	atendimento.setic.ro.gov.br

DATA CENTER

Equipe de Tratamento:	Jean Franco Ederson Vanazzi Caio Henrique Ramissés Evangelista Rodrigo meireles
E-mail:	datacenter@setic.ro.gov.br
Canal de atendimento:	atendimento.setic.ro.gov e sistema SEI

GPREV

Equipe de Tratamento:	Daltro Barbosa Eduardo Zimmer Jairo Barbosa Levi Viana Andearlisson Oliveira Hendrei Maia
E-mail:	gprevi@setic.ro.gov.br
Canal de atendimento:	atendimento.setic.ro.gov e sistema SEI

OPERAÇÕES

Equipe de Tratamento:	Rogério Alves Rafael Domingues Alecsander Damasceno Matheus Maia
E-mail:	operacoes@setic.ro.gov.br
Canal de atendimento:	atendimento.setic.ro.gov e sistema SEI

CAGD

Equipe de Tratamento:	Abdenildo santos Wagner Uchoa Pedro Henrique Gomes Caio Cesar Freitas Caio Henrique Camargo Denizard Camargo Juan David Anderson Souza Daniel Manvailler José Lucas Silva João Thomas Telles Ana Flavia
E-mail:	abdenildosantos@setic.ro.gov.br
Canal de atendimento:	atendimento.setic.ro.gov e sistema SEI

ENCARREGADO DE DADOS

Equipe de Tratamento:	Tiago Aguiar Pedro Barbosa
E-mail:	ci@setic.ro.gov.br encarregadolgpd@setic.ro.gov.br
Canal de atendimento:	atendimento.setic.ro.gov e sistema SEI

Tabela 2 - Equipe de Tratamento. Fonte: própria.

Os detalhes com nomes e números de contato dos envolvidos estão listados em documentos à parte, tornando-se anexo desmembrado da publicação deste documento, disponibilizado a Central de Atendimento, mantido atualizado e sob a guarda da COSEGI.

O documento “Lista de Responsáveis pelo PC” é um anexo deste Plano.

As equipes de Tratamento de Riscos têm autonomia compartilhada, ou seja, participarão do resultado da decisão, recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterão as ações a serem tomadas, seus impactos e a repercussão, caso as recomendações não sejam seguidas.

Cada Equipe de Tratamento pode desempenhar diversos serviços como:
Serviços reativos: Acionados por um evento ou requisição, como um alerta do computador comprometido com vírus; relatórios de análise de vulnerabilidade; identificação por ferramenta IDS/IPS, sistema de análise de log ou alerta de intrusão. O centro de uma equipe de resposta são os serviços reativos da equipe de resposta a incidentes de segurança.
Serviços proativos: proveem assistência e informações necessárias para ajudar a preparar, proteger e manter seguro os sistemas e computadores, se antecipando a ataques, problemas ou eventos.

O tratamento de incidente envolve as ações para recebimento, triagem, análise e resposta às requisições e reportes de eventos e incidentes.

Execução de ações são realizadas para proteger sistemas e segmentos de rede, afetados ou ameaçados por atividade de intrusão, promoção de soluções e estratégias de mitigação provenientes de recomendações de segurança, atualização ou reparos de sistemas e constante busca pelo desenvolvimento de outras respostas ou estratégias de contorno.

9 SERVIÇOS ESSENCIAIS

A tabela abaixo demonstra os serviços considerados essenciais e que precisam ser mantidos diante de circunstâncias de incidentes e desastres. Estes serviços garantem o funcionamento da SETIC como superintendência de tecnologia da informação do Governo de Rondônia.

SERVIÇOS ESSENCIAIS					
INFOVIA	**CODE / Desenvolvimento**	**DATACENTER**	**GPREV**	**OPERAÇÕES**	**CAGD**
Fornecimento de link através da rede INFOVIA.	Hospedagem de Sistemas.	Hospedagem de servidores virtuais.	Mitigação e correção das vulnerabilidades.	Gestão dos equipamentos de segurança de perímetro e comunicação com a internet.	Construção e ajuste de ferramenta personalizada para acesso a dados de transparência dos sistemas ofertados pela SETIC.
Ligação entre unidades governamentais.	Armazenamento (backup) de versões de código fonte e suas dependências de sistemas utilizados na SETIC.	Backup dos serviços web hospedados.	Gestão e Análise de Logs.	Intercomunicações e conexão entre as unidades internas e externas, por meio dos switches core e de borda.	Administração dos acessos e manutenção ao banco de dados.
Gestão dos acordos de cooperação.	Inspeção de código fonte de sistemas da SETIC.	Compartilhamento de arquivos (Microsoft Windows Server)	Tratamento de Incidentes de segurança da informação.	Gerência de acessos por meio de firewall para navegação via proxy	Disponibilização de dados para auditoria.
	Armazenamento de dados em nuvem.	Autenticação centralizada.	Conscientização sobre Segurança da Informação.	Gestão e configuração de redes sem fio por meio dos Access Points internos e externos.	Consolidação de estrutura das bases de dados.
		Gerenciamento de DNS externo zona ro.gov.br		Consultoria de projetos de conectividade para outras unidades	Instalar e realizar manutenção nos Sistemas Gerenciadores de Banco de Dados e Servidores de relatórios.
					Migração de Base de dados e Dados entre as mesmas.
					Construção e administração de Armazém de Dados (DW e DM).

Tabela 3 - Serviços Essenciais. Fonte: própria.

10 PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

Este plano, específica as ações e responsabilidades para a comunicação entre as equipes de tratamento envolvidas com os serviços interrompidos ou que sofreram algum desastre.

As ações dizem respeito a gerir, administrar, eliminar ou neutralizar os impactos, inerentes ao relacionamento entre as equipes de tratamento envolvidas nas ações antes, durante e após a ocorrência de um incidente.

O PAC compreende em seu escopo os eventos classificados como incidentes no âmbito da SETIC e desastres classificados no PRD. Não faz parte do escopo deste documento estabelecer procedimentos operacionais das equipes de tratamento e restabelecimentos dos serviços nos casos de crises, sendo estabelecido e mantido dentro das áreas responsáveis o tratamento do incidente.

Objetivos:

- Assegurar a existência de procedimentos de comunicação, respostas e soluções frente a incidentes que possam trazer impactos negativos à organização junto às principais partes interessadas;
- Minimizar transtornos sobre os desdobramentos de incidentes e estimular o esforço em conjunto para superação da crise;
- Definir responsabilidades acerca do processo de gestão de crises;
- Orientar os servidores e demais colaboradores com informações e procedimentos de conduta; e
- Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido, através do canal oficial de comunicação da SETIC (ASCOM).

10.1 EXECUÇÃO DO PLANO DE ADMINISTRAÇÃO DE CRISE DE TI

Os incidentes que comprometem a continuidade dos serviços ofertados pela SETIC, afetando a operação normal das atividades são as crises tratadas neste plano. Caracteriza-se através dos acontecimentos ou série deles que resulta no rompimento das operações normais, vindo a culminar em consequências graves. Dessa forma a administração das crises serão tratadas nos níveis estratégicos, táticos e operacionais.

Nível Estratégico: são deliberadas as definições estratégicas encaminhadas pela Comissão Permanente de Segurança da Informação - CPSI, aprovar as decisões sugeridas pelas equipes de tratamento para tratar incidentes que demandem impactos críticos, as comunicações às instâncias superiores do Governo e todas as partes interessadas durante a crise.

Nível Tático: formado pelo CPSI e pelos líderes das equipes de tratamento, que atuam na avaliação de incidentes graves e apontam estratégias de resolução, podendo convocar outras pessoas para identificação e tratamento do incidente e submeter as resoluções para diretoria e superintendência aprovar. Neste nível decide-se pela ativação ou não do Plano de Continuidade em conformidade com a classificação de incidente, do PGISI e instruções da CPSI. Mantém a informação atualizada a todos os envolvidos, realiza a análise do impacto das áreas afetadas, monitoramento do incidente até a resolução.

Nível Operacional: formado pelas equipes de tratamento, que atuam através do Plano de Gestão de incidentes e Plano de Recuperação de Desastres, entram em ação quando há necessidade de ativação dos planos e reportam o andamento do tratamento dos incidentes ao nível tático. Responsáveis pela atualização dos PCO e PRD de cada ativo classificado.

As comunicações de ocorrência de um desastre ou incidente deverão ser efetuadas a diversas áreas, informando os efeitos da continuidade dos serviços e tempo previsto de recuperação. A ASCOM é responsável pelas comunicações oficiais aprovadas pela Superintendência e Diretoria da SETIC O presidente da CPSI será responsável por contatar estas unidades e passar as informações pertinentes a cada equipe e as demais partes interessadas.

Na ocorrência de desastres que envolvam risco à vida, qualquer pessoa deverá assegurar a comunicação com as autoridades competentes, fornecendo as informações de localização, natureza, magnitude e impacto do desastre. Recomenda-se que o comunicante deverá anotar a data, hora e número da ocorrência para registro pela COSEGI.

Polícia	190
SAMU	192
Bombeiros	193

A Coordenadoria de Segurança da Informação (COSEGI), junto às equipes de tratamento deverá realizar a comunicação dos principais envolvidos e das partes que podem contribuir para recuperação e continuidade dos serviços, sempre observando as autorizações necessárias com os níveis de hierarquia para publicar ou fornecer informações, criando uma estratégia da melhor forma de acionar as partes envolvidas e afetadas de modo a mantê-los informados, inclusive das ações necessária para o restabelecimento dos serviços inativos.

A central de atendimento será o canal para estabelecer a entrada principal dos registros de desastres e incidentes conforme seu endereço de abertura de chamados, e-mail e telefone.

O contato específico para os setores de forma individual caso seja necessário, deverá ser realizado pela Central de Atendimento, pelo Coordenador da SETIC ou membro da equipe de tratamento, a fim de mantê-los informados da ocorrência de um incidente e da inatividade dos serviços essenciais de TI.

Caso não haja conectividade ou linha telefônica disponível, fornecer as informações do ambiente seguro, os serviços indisponíveis, previsão de retorno e as expectativas durante o desastre ou incidente deverá ser através de publicações, ou alguma estratégia definida no momento.

10.2 COMUNICAÇÃO COM OS FORNECEDORES E PRESTADORES DE SERVIÇOS

Os fornecedores e prestadores de serviços deverão ser acionados conforme o protocolo de atendimento e estratégia de continuidade dos serviços transferidos através de contratação com essas empresas em casos de incidentes ou descontinuidades. Nos casos de desastres será construído um planejamento de continuidade baseado no contrato existente com os fornecedores/prestadores.

FORNECEDORES / PARCEIROS		
Descrição	Contato	Comunicação
DATACOM	Atendente	https://supportcenter.datacom.com.br/Qualitor/loginUsuario.php
Venge Construções e Tecnologia ltda	Ednilson Govea de Lima	(69) 98403-0718
Telebrás	Natasha	(61) 98111-3321
RNP	Robert	(69) 99972-5066
Clear IT	Ronny, Andre ou Paulo Vitor	(92) 99360-0842 https://clearit.odoo.com/helpdesk/ (92) 98118-1171 (92) 98458-0149
Servix	Leonardo e Jean Paes	(11) 98960-0556 (69) 99380-3365
MDC "Container"	Aldo Cipriano	(92) 99237-6825
F5 big ip	Daniel	(61) 98136-6601 https://layer.movidesk.com/Account/Login?ReturnUrl=%2f
Teltec (Seduc)	Wanderlei	(69) 99237-5639
Oi	SOC	0800-061-3031 Opção 3
Telebrás	Suporte	0800 880 7000

Tabela 4 - Fornecedores/Parceiros. Fonte: Autor próprio.

A Coordenadoria de Segurança da Informação (COSEGI) e a equipe de tratamento deverá monitorar os incidentes e as crises, bem como acompanhar sua repercussão nos meios de comunicação, agindo de forma proativa e ágil, atendendo as demandas, principalmente prestando esclarecimentos, quando necessário, e permitindo a veiculação da posição oficial da CPSI e da alta gestão

da SETIC, provendo as informações de retorno das operações e as informações de status dos serviços de TI.

Comunicação do retorno das operações - A COSEGI em conjunto as equipes de tratamento comunicarão a todas as partes envolvidas direta e indiretamente quando ocorrer o retorno das operações à normalidade, através dos meios formais de comunicação da SETIC.

Encerramento do PAC - A partir da validação do restabelecimento dos serviços afetados e estabilidade na SETIC, a COSEGI em consonância com as equipes que trataram o incidente entrará em contato com as partes envolvidas e descritas neste plano provendo as informações de retorno das operações com as informações de situação dos serviços afetados.

As atividades deverão ser registradas e emitido relatório especificando equipamentos que foram realocados, procedimento de recuperação, fornecedores que foram acionados, entre outras informações relevantes, além da abertura e acompanhamento de chamados correlatos ao ocorrido.

Após todos os procedimentos descritos acima e retorno à normalidade, o PAC deverá ser encerrado.

11 PLANO DE CONTINUIDADE OPERACIONAL (PCO)

Este plano descreve os cenários de descontinuidade dos serviços e seus respectivos procedimentos alternativos provisionados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais.

Descreve os procedimentos para uma situação de falha ou interrupção nos ativos que sustentam os serviços operantes na SETIC.

O escopo deste plano garante ações de continuidade durante e depois da ocorrência de uma crise ou cenário de desastre, tratando-se apenas ações de

contingência estabelecidas na estratégia. Não faz parte do seu escopo definir procedimentos técnicos necessários para garantir a continuidade dos serviços da SETIC.

As ações estratégias a serem adotadas pelas equipes de tratamento neste plano operacional, abrange a continuidade dos serviços da SETIC.

Objetivos:

- Provisionar formas de atendimento a fim de manter o funcionamento dos serviços essenciais e a continuidade das operações de TI;
- Determinar procedimentos, controles e regras alternativas que possibilitem a continuidade das operações de TI durante um incidente ou cenário de desastres;
- Ter uma equipe de tratamento em cada área de distribuição dos serviços; e
- Registrar as contingências realizadas.

11.1 ACIONAMENTO DO PLANO

O principal meio de entrada das demandas de incidentes é através do Sistema de Documentação Eletrônico e da central de atendimento com a abertura de chamado na ferramenta de chamados oficial da SETIC, exceto os casos de emergência que coloque em risco a vida conforme previsto no PRD, deve ser acionado imediatamente às autoridades competentes e em seguida acionar o Presidente da CPSI, o Vice-presidente da CPSI ou a Central de Atendimento.

Nos incidentes classificados como baixo no PGISI, deverá ser acionada a equipe de tratamento e seguir protocolo estabelecido no PGISI, devendo o tratamento e resposta do incidente ser realizado através da equipe de tratamento.

Nos incidentes classificados como médio e que tenha envolvimento de dados pessoais e os incidentes Alto (Impacto Grave), será convocada reunião de emergência com os líderes da Equipe de Tratamento, através da CPSI, onde será estabelecido o processo de continuidade operacional.

Dentre as atividades a serem realizadas através da CPSI, estão:

Avaliar o impacto de perda de dados e dos ativos - recepcionar a demanda e realizar avaliação do incidente ou crise e verificar o impacto, extensão de possíveis desdobramentos, bem como se houve vazamento de dados pessoais.

Identificar ativos de informação afetados - A equipe de tratamento envolvida deverá listar todos os ativos danificados e dados envolvidos da ocorrência.

Mapear os dados a serem recuperados - mapear os serviços descontinuados e as informações de perda de ativo e de conexão. Emitir um relatório abrangendo envolvimento com dados pessoais em casos de ocorrência, e os componentes necessários à plena operação das aplicações dos servidores, máquinas virtuais, banco de dados, firewall, storage, routers e switches, bem como respectivas configurações de proxy, DNS, rotas, VLANs e etc.

Estimar o volume de dados, perdas e tempo de recuperação - A equipe de tratamento estimulará o volume de dados a serem recuperados, ou se houve vazamento de dados pessoais e o prazo de recuperação ou danos causados pelo vazamento. Após o mapeamento das perdas e impactos deverá elaborar um cronograma de recuperação das aplicações levando em consideração o tempo de recuperação de cada sistema crítico.

Executar procedimento de recuperação - A equipe de tratamento realizará os procedimentos de recuperação para retomar a continuidade operacional dos serviços da SETIC. A equipe deverá realizar o planejamento estabelecido pela CPSI, este planejamento deverá ser divulgado para toda a equipe.

Testar procedimentos de restauração de dados - A equipe de tratamento deverá simular os eventos. Os eventos poderão ser simples, como queda de energia ou complexo como um incêndio, para conferir se as ações de contingência previstas são suficientes, os testes deverão ser realizados para identificar falhas e corrigi-las antes da ocorrência real. As simulações serão o meio da equipe ter condições de conhecer se a estratégia de continuidade funcionou e o que fazer em cada situação.

Documentar procedimentos apresentando melhorias - A equipe de tratamento deverá documentar o ocorrido, a solução e diagnósticos de melhorias, caso seja necessário.

A CPSI após a aprovação deverá encaminhar para o coordenador da COSEGI realizar a apresentação e disponibilização do plano, bem como os responsáveis pelas ações.

11.2 PLANO DE CONTINUIDADE OPERACIONAL PRIORIZADO

Os serviços essenciais descritos na tabela 3, foram priorizados através da ferramenta GUT (Gravidade, urgência e tendência). A “Gravidade” analisa o impacto negativo que a descontinuidade do serviço pode causar para o negócio, caso não seja resolvido. A “Urgência” considera o prazo necessário para a resolução do problema, levando em consideração o tempo despendido na resolução do incidente. A “Tendência” mede o quanto o problema está predisposto a piorar com o tempo.

Cada um dos aspectos analisados na GUT leva em consideração uma escala de 1 a 5, sendo:

- **Gravidade**: 1 sem gravidade, 2 pouco grave, 3 grave, 4 muito grave e 5 extremamente grave.
- **Urgência**: 1 não tem pressa, 2 pode esperar um pouco, 3 o mais rápido possível, 4 com alguma urgência e 5 requer uma ação imediata.
- **Tendência**: 1 não vai piorar, 2 vai piorar em longo prazo, 3 vai piorar em médio prazo, 4 vai piorar em pouco tempo e 5 vai piorar rapidamente.

Após os dados analisados será realizado a multiplicação das notas elencadas e dessa forma possibilita ter uma sequência listadas dos serviços mais graves ao menos grave não perdendo a sua essencialidade analisada para a continuidade dos serviços disponibilizados para a SETIC.

Na sequência é possível visualizar o protocolo de atendimento dos serviços e a estratégia de continuidade dos mesmos, conforme a tabela 5 a seguir.

SERVIÇOS PRIORIZADOS			
SERVIÇOS	**PRIORIDADE**	**PROTOCOLO DE ATENDIMENTO**	**ESTRATÉGIA DE CONTINUIDADE**
1. Gestão dos equipamentos de segurança de perímetro e comunicação com a internet.	125	. Conferi a demanda existente e se a continuidade depende do Setor de Operações de ou terceiros. . Confirma a demanda e realiza o atendimento. . Finaliza o chamado ou despacha através do sistema eletrônico.	. Nova contratação ou adoção de ferramenta open source, para dar continuidade ao serviço de firewall.
2. Hospedagem de máquinas virtuais.	125	. Identificação do motivo do interrompimento. . Correção através da equipe de tratamento. . Comunicação para equipe de Datacenter/Redes e demais partes interessadas se houver necessidade. . Fechamento do chamado no GLPI.	1. Em casos de indisponibilidade de segunda opção é acionado o sistema redundante. 2. Em casos de indisponibilidade de energia elétrica ou quaisquer impedimentos de funcionamento de hardware é disparado pelo Sistema de monitoramento de sistemas e pane física um alerta no aplicativo de mensagem instantânea da equipe de tratamento responsável, além do coordenador. Onde o responsável entrará em contato com a SUGESP, detentora da administração elétrica e predial. . Comunicar às partes interessadas, e em casos graves a comunicação pública deve ser realizada através dos canais oficiais da SETIC. . Reestabelecimento através da equipe de tratamento.
3. Backup das máquinas virtuais hospedadas	125	. Identificação do motivo do interrompimento. . Correção através da equipe de tratamento. . Comunicação para equipe de Datacenter/Redes e demais partes interessadas se houver necessidade. . Fechamento do chamado no GLPI.	. Em caso de descontinuidade da rotina de backup ou algum sinistro é realizado alerta para equipe de tratamento através de sistema de monitoramento através do aplicativo de mensagem instantânea. Em seguida é realizada uma inspeção remota ou física de detecção do problema. . Comunicar a chefia imediata. . O restabelecimento é realizado através da equipe de tratamento.
4. Autenticação centralizada	125	. Identificação do motivo do interrompimento. . Correção através da equipe de tratamento. . Comunicação para equipe de Datacenter/Redes e demais partes interessadas se houver necessidade. . Fechamento do chamado no GLPI.	1. Em casos de indisponibilidade de redundância, a mesma é acionada automaticamente. 2. Em caso de indisponibilidade do serviço é realizado alerta para equipe de tratamento através de sistema de monitoramento via aplicativo de mensagem instantânea. Em seguida é realizado uma inspeção remota ou física de detecção do problema. . Comunicar as partes interessadas, e em casos graves a comunicação pública deve ser realizada através dos canais oficiais da SETIC. . Reestabelecimento é realizada pela equipe de tratamento da SETIC.
5. Gerenciamento de DNS externo zona ro.gov.br	125	. Identificação do motivo do interrompimento. . Correção através da equipe de tratamento. . Comunicação para equipe de Datacenter/Redes e demais partes interessadas se houver necessidade. . Fechamento de chamado no GLPI.	. Em casos de disponibilidade a redundância é acionado automaticamente. . Comunicar às partes interessadas, e em casos graves a comunicação pública deve ser realizada através dos canais oficiais da SETIC. . O restabelecimento é realizado pela equipe de tratamento da SETIC
6. Tratamento de Incidentes de segurança da informação.	125	. Registrar Incidente de Segurança. . Validar notificação. . Definir nível de criticidade. . Aplicar ações de contenção. . Propor ações para tratar incidente. . Aplicar medidas de contenção imediata. . Documentar incidente. . Verificar a necessidade de melhorias. . Analisar e implantar propostas de melhorias. . Verificar ocorrência de dano ao titular. . Comunicar aos interessados.	. Aciona a ferramenta redundante.
7. Gestão e Análise de Logs.	125	. Coleta dos logs através das ferramentas oficiais. . Realiza análise dos logs coletados suspeitos ou com anomalias. . Registra e encaminha o incidente através dos canais de atendimento aos órgãos ou setores pertinentes. . Acompanha o atendimento do chamado.	. Aciona a ferramenta redundante.

8. Fornecimento de link através da rede INFOVIA.	125	. Recepciona demandas de incidentes através do sistema GLPI ou Sistema de Monitoramento. . Realiza inspeção do ocorrido. . Prioriza a demanda. . Comunica as partes interessadas. . Verificar disponibilidade orçamentária para a correção caso envolva algum custo. . Restabelece o link ou serviço e . Finaliza o chamado no GLPI.	1. Em caso de descontinuidade física é acionado o contratado prestador do serviço. 2. Em descontinuidade através de problemas lógicos é restabelecido pela equipe de tratamento da Infovia.
9. Ligação entre unidades governamentais.	125	. Recepciona demandas de incidentes através do sistema GLPI ou Sistema de Monitoramento. . Realiza inspeção do ocorrido. . Prioriza a demanda. . Comunica as partes interessadas. . Verificar disponibilidade orçamentária para a correção caso envolva algum custo. . Restabelece o link ou serviço e . Finaliza o chamado no GLPI.	1. Em caso de descontinuidade física é acionado o contratado de prestação de serviço. 2. Em descontinuidade através de problemas lógicos é restabelecido pela equipe de tratamento da Infovia.
10. Hospedagem de Sistemas.	125	. Recepciona demandas e incidentes através do sistema GLPI. . Realizar inspeção da plataforma de hospedagem. . Correção através da equipe de tratamento. . Comunicação para equipe de Datacenter/Redes e demais partes interessadas se houver necessidade. . Fechamento de chamado no GLPI.	1. Na ocorrência de descontinuidade de uma das plataformas de hospedagem é acionada a segunda opção. 2. Em casos de indisponibilidade de energia elétrica ou quaisquer impedimentos de funcionamento de hardware é acionado a equipe de tratamento de Data Center. . Comunicar às partes interessadas, e em casos graves a comunicação pública deve ser realizada através dos canais oficiais da SETIC.
11. Armazenamento (backup) de versões de código fonte e suas dependências de sistemas utilizados na SETIC.	125	. Recepciona demandas e incidentes através do sistema GLPI. . Realizar inspeção da plataforma de hospedagem. . Correção através da equipe de tratamento. . Comunicação para equipe de Datacenter/Redes e demais partes interessadas se houver necessidade. . Fechamento do chamado no GLPI.	1. Em casos de indisponibilidade de energia elétrica ou quaisquer impedimentos de funcionamento de hardware é acionado a equipe de tratamento de Data Center. . Comunicar às partes interessadas.
12. Administração dos acessos e manutenção ao banco de dados	25	. Recepcionar a demanda. . Identifica se a demanda é competência da CAGD. . Inseri no backlog ou devolve para o Gabinete. . Processo de priorização. . Atendimento da demanda. . Validação e entrega ao cliente. . Realiza o encerramento do chamado. . Coleta o feedback do cliente.	1. Equipe de Tratamento.
13. Disponibilização de dados para auditoria	125	. Recepcionar a demanda. . Identifica se a demanda é competência da CAGD. . Inseri no backlog ou devolve para o Gabinete. . Processo de priorização. . Atendimento da demanda. . Validação e entrega ao cliente. . Realiza o encerramento do chamado. . Coleta o feedback do cliente.	1. Em caso de indisponibilidade da ferramenta ou de recursos para ajuste, poderá ser extraído os dados diretamente com acesso manual ao banco de dados.
14. Intercomunicações e conexão entre as unidades internas e externas, por meio dos switches core e de borda.	100	. Conferi a demanda existente e se a continuidade depende do Setor de Operações de ou terceiros. . Realiza o atendimento da demanda. . Encerra ou despacha o chamado através do sistema eletrônico.	1. Parceria com o órgão proprietário para viabilizar a continuidade dos serviços.
15. Compartilhamento de arquivos (Microsoft Windows Server)	64	. Identificação do motivo do interrompimento. . Correção através da equipe de tratamento. . Comunicação para equipe de Datacenter/Redes e demais partes interessadas se houver necessidade. . Fechamento de chamado no GLPI.	1. Em caso de indisponibilidade do serviço é realizado alerta para equipe de tratamento através de sistema de monitoramento via aplicativo de mensagem instantânea. Em seguida é realizada uma inspeção remota de detecção do problema. . Comunicar às partes interessadas, e em casos graves a comunicação pública deverá ser realizada através dos canais oficiais da SETIC. . O restabelecimento é realizado pela equipe de tratamento da SETIC e quando necessário deverá acionar a equipe de tratamento de órgão afetado.

16. Inspeção de código fonte de sistemas da SETIC.	60	. Recepcionar demandas e incidentes através do sistema GLPI. . Realizar inspeção da plataforma de hospedagem. . Correção através da equipe de tratamento. . Comunicação para equipe de Datacenter/Redes e demais partes interessadas se houver necessidade. . Fechamento de chamado no GLPI.	1. Equipe de Tratamento.
17. Armazenamento de dados em nuvem.	27	. Recepcionar demandas e incidentes através do sistema GLPI. . Realizar inspeção da plataforma de hospedagem. . Correção através da equipe de tratamento. . Comunicação para equipe de Datacenter/Redes e demais partes interessadas se houver necessidade. . Fechamento do chamado no GLPI.	1. Equipe de Tratamento.
18. Mitigação e correção das vulnerabilidades.	24	. Análise através das ferramentas oficiais. . Gera um relatório. . Encaminha através dos canais de atendimento aos órgãos ou setores pertinentes. . Acompanha o atendimento do chamado.	1. Em caso de indisponibilidade acionar ferramenta redundante.
19. Gestão dos acordos de cooperação.	18	. Gerencia o contrato. . No período inicia as tratativas de renovação do contrato no final do período ou via manifestação de interesse por qualquer uma das partes integrantes do contrato. . Comunica todas as partes interessadas. . Inicia as tratativas com o jurídico e alta gerência. . Efetiva a renovação do contrato ou o encerramento no final da data descrita no acordo de cooperação.	1. Equipe de gestão do acordo de cooperação.
20. Gerência de acessos por meio de firewall para navegação via proxy	12	. Conferi a demanda existente e deliberei através da análise de conformidade com as regras e PSI. . Executa o atendimento ou informa no chamado o deferimento/indeferimento. . Finaliza o chamado.	1. Nova contratação ou adoção de ferramenta open source, para dar continuidade ao serviço de firewall.
21. Consolidação de estrutura das bases de dados	12	. Recepcionar a demanda. . Identifica se a demanda é competência da CAGD. . Inseri no backlog ou devolve para o Gabinete. . Processo de priorização. . Atendimento da demanda. . Validação e entrega ao cliente. . Realiza o encerramento do chamado. . Coleta o feedback do cliente.	1. Equipe de tratamento.
22. Instalar e realizar manutenção aos Sistemas Gerenciadores de Banco de Dados e Servidores de relatórios	8	. Recepcionar a demanda. . Identifica se a demanda é competência da CAGD. . Inseri no backlog ou devolve para o Gabinete. . Processo de priorização. . Atendimento da demanda. . Validação e entrega ao cliente. . Realiza o encerramento do chamado. . Coleta o feedback do cliente.	1. Em caso de indisponibilidade de acesso aos servidores, poderá ser acionado a equipe de tratamento do Datacenter.
23. Gestão e configuração de redes sem fio por meio dos Acess Points internos e externos	4	. Análise da demanda antes de deliberar. . Estando em conformidade, é executado o pedido. . Emitir despacho	1. Acionamento do suporte e garantia dos equipamentos.
24. Construção e administração de Armazém de Dados (DW e DM)	4	. Recepcionar a demanda. . Identifica se a demanda é competência da CAGD. . Inseri no backlog ou devolve para o Gabinete. . Processo de priorização. . Atendimento da demanda. . Validação e entrega ao cliente. . Realiza o encerramento do chamado. . Coleta o feedback do cliente.	1. Equipe de Tratamento.

25 - Conscientização sobre Segurança da Informação.	2	. Atendimento de demandas solicitadas interna e externamente. . Manter agenda de comunicação e campanhas. . Realizar atendimento do cronograma agendado.	1. Equipe de Tratamento.
26. Consultoria de projetos de conectividade para outras unidades	2	. Analisa o pedido e requisitos para execução do projeto. . Confirma a viabilidade da execução ou repassa os requisitos para a confecção do mesmo. . Executa ou emite despacho com o resultado da consultoria. . Acompanhamento da implantação.	1. Alternância no atendimento pela equipe de tratamento.
27. Construção e ajuste de ferramenta personalizada para acesso a dados de transparência dos sistemas ofertados pela SETIC.	2	. Recepcionar a demanda. . Identifica se a demanda é competência da CAGD. . Inseri no backlog ou devolve para o Gabinete. . Processo de priorização. . Atendimento da demanda. . Validação e entrega ao cliente. . Realiza o encerramento do chamado. . Coleta o feedback do cliente.	1. Em caso de indisponibilidade da ferramenta ou de recursos para ajuste, poderá ser extraído os dados diretamente com acesso manual ao banco de dados.
28. Migração de Base de dados e Dados entre as mesmas	2	. Recepcionar a demanda. . Identifica se a demanda é competência da CAGD. . Inseri no backlog ou devolve para o Gabinete. . Processo de priorização. . Atendimento da demanda. . Validação e entrega ao cliente. . Realiza o encerramento do chamado. . Coleta o feedback do cliente.	1. Equipe de Tratamento.

Tabela 5 – Serviços Priorizados. Fonte: própria

11.3 ENCERRAMENTO DO PCO

Após o retorno das operações à normalidade no ambiente principal, deverá ser emitido parecer descrevendo as atividades realizadas de contingência. Em seguida, deverá ser dada publicidade dos dados às equipes de tratamento, a CPSI e realizar a guarda do relatório para as lições aprendidas.

Providenciar avisos que se fizerem pertinentes aos usuários e comunicação pública através dos meios de comunicação oficiais da SETIC, com aprovação da alta gestão.

12 PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

Este plano descreve os cenários de descontinuidade dos serviços e seus respectivos procedimentos, definindo a sequência de restabelecimento de um novo ambiente de forma sequencial e priorizada, restabelecendo dessa forma as atividades necessárias para recuperação do ambiente de forma correta e de acordo com um prazo tolerável.

O escopo principal deste plano é realizar o retorno das operações dos serviços hospedados no ambiente principal da SETIC, após a ocorrência de um desastre ou crise, tratando-se somente dos ativos, conexões e disponibilidade dos serviços, bem como as configurações deste ambiente, tornando-o ele acessível aos usuários finais.

OBJETIVOS

O PRD da SETIC visa restabelecer o ambiente e as condições originais de operação. Este plano possui os seguintes objetivos:

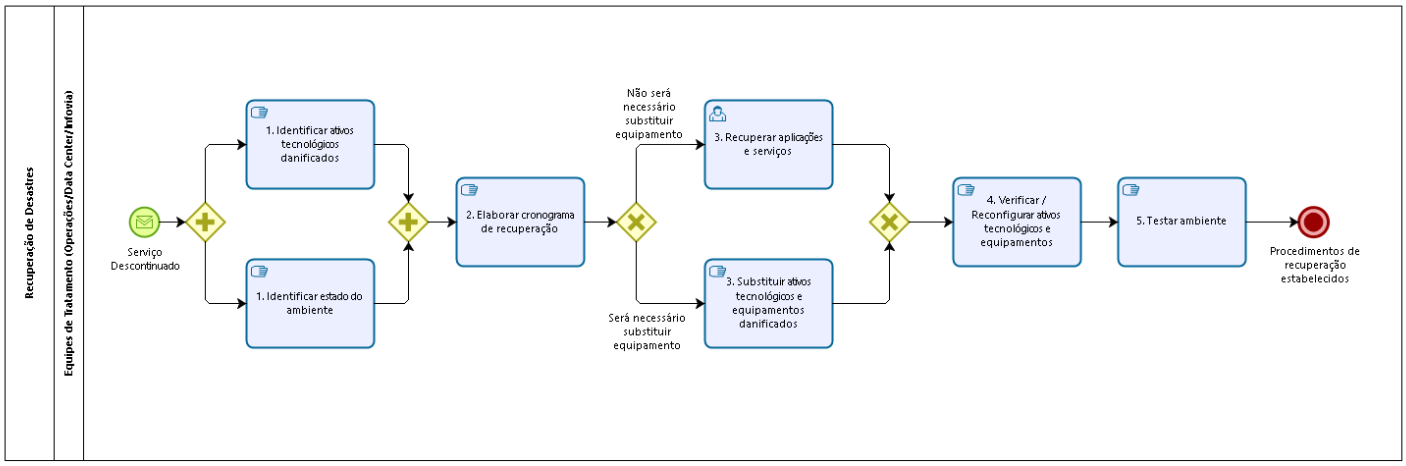
- Estabelecer uma estratégia de recuperação conhecida por toda a equipe de tratamento;
- Ações que previnam a facilidade de acesso a esse ambiente;
- Recuperar o ambiente de datacenter dentro de um prazo aceitável;
- Prover meios de recuperação dos ativos e conexões do datacenter; e

Documentar todos os incidentes, a fim de garantir arcabouço para estudo de caso e estratégias de prevenção.

12.1 FLUXO DE EXECUÇÃO DO PRD

Recuperação de Desastres

Autor: 00708411282
Versão: 1.0
Descrição: Este processo tem como escopo a Recuperação de Desastres, onde é descrito os cenários de descontinuidade dos serviços e seus respectivos procedimentos, definindo a sequência de restabelecimento de um novo ambiente de forma sequencial e priorizado, até o término dos procedimentos de recuperação estabeleddos.



Powered by bizagi Modeler

Elementos do Processo

- Serviços Descontinuado.
- Gateway (Li
- Procedimentos de recuperação estabelecidos.

12.1.1 Descrição do Processo de Recuperação de Desastres

Identificar ativos tecnológicos danificados.

Equipes de tratamento: Operações/Data Center/Infovia

A identificação dos ativos tecnológicos danificados, será realizado através das equipes de tratamentos. As equipes de tratamento deverão identificar e gerar

uma lista dos ativos tecnológicos danificados e/ou inoperantes na ocorrência de desastres.

Identificar estado do ambiente.

Equipes de tratamento: Operações/Data Center/Infovia.

Inspecionar o ambiente, a fim de diagnosticar climatização, parte elétrica, controle de acesso demais aspectos quanto à segurança física que viabilizem a reestruturação do ambiente ou a necessidade de migração.

Elaborar Cronograma de Recuperação.

Equipes de tratamento: Operações/ Data Center/ Infovia/CODE.

Após a emissão do relatório de levantamento do cenário, onde foram mapeadas as perdas e impactos, será elaborado um breve roteiro de recuperação das aplicações e serviços, levando em consideração a sequência necessária de levantamento dos serviços e sua priorização.

O Coordenador da área envolvida (CODE, COINFRA ou COSEGI), deverá dar ciência no cronograma de recuperação.

Recuperar Aplicações e Serviços.

Equipes de tratamento: Operações/ Data Center/ Infovia.

Nessa etapa será feita a recuperação das aplicações e serviços que tiveram suas operações comprometidas temporariamente. A recuperação será feita seguindo o roteiro de recuperação elaborado na fase anterior.

Substituir ativos tecnológicos e equipamentos danificados.

Equipes de tratamento: Operações/ Data Center/ Infovia/CODE.

Será realizada a troca do ativo ou equipamento danificado, caso não seja possível essa substituição por falta em estoque, poderá ser realizada a abertura de um processo licitatório para aquisição equipamento.

A equipe de tratamento irá mensurar o impacto do período do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção de cada serviço, e se há uma solução alternativa a ser tomada enquanto é realizada a aquisição. Também será verificado através da equipe de tratamento, se os ativos danificados estão cobertos por garantia, podendo ser acionada, neste caso, através da lista de fornecedores.

 **Verificar / Reconfigurar ativos tecnológicos e equipamentos.**

Equipes de tratamento: Operações/ Data Center/ Infovia/CODE.

Será verificado se as configurações dos ativos reparados ou substituídos estão em pleno funcionamento. Caso não estejam, prover cronograma estimado para configurar estes ativos, informando as partes envolvidas.

 **Testar ambiente.**

Equipes de tratamento: Operações/ Data Center/ Infovia/CODE.

O teste tem o objetivo de garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre.

Observação:

1. Ao término dos procedimentos de recuperação estabelecidos, as informações de recuperação de serviços serão consolidadas em parecer específico informando horário de restabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

13 PLANO DE TESTE E ALIDAÇÃO (PTV)

Com objetivo de reavaliar os procedimentos previstos nos planos estabelecidos neste documento, a fim de viabilizar uma melhoria contínua, o PCTIC será testado e validado anualmente, com datas previstas no cronograma de testes realizado em reunião de planejamento das equipes de tratamento que irão participar ativamente dos testes, levando sempre em consideração a insurgência de novos fatores de riscos, mudança da análise de impacto, ou com a inclusão de um novo serviço no plano de continuidade.

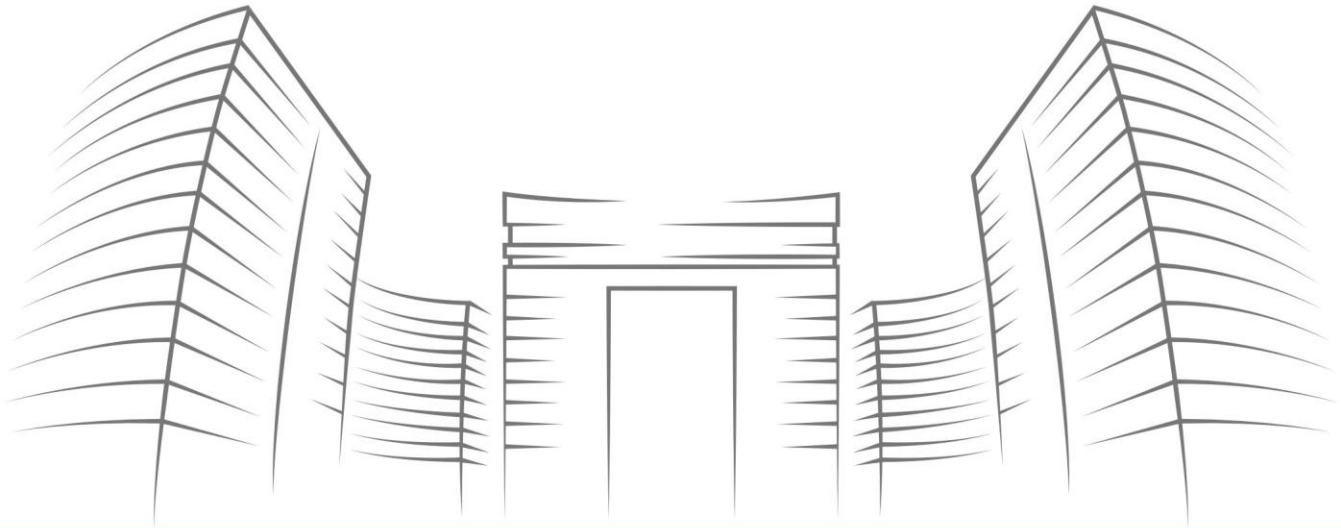
Os testes devem ser realizados o mais próximo possível da realidade para garantir a continuidade e/ou recuperação dos serviços de TI.

A execução do cronograma de testes e validação dos serviços deve ser registrado no GLPI e deverá configurar um ambiente de teste respeitando os critérios mínimos:

- Teste de complexidade simples, no qual é realizada uma análise (crítica ensaios de execução), dos procedimentos e informações descritas, com o objetivo de atualizar ou validar os procedimentos e as informações contidas no plano;
- Deverá simular condições específicas, eventos e cenários de risco;
- O teste deve utilizar um ambiente isolado do ambiente de produção, tendo em vista que o teste não irá interromper os serviços em produção.

Governo do Estado de

RONDÔNIA



setic.ro.gov.br

@setic.rondonia

Telefone: 69 3212 9541
Endereço: Av. Farquar, 2986 - Bairro Pedrinhas
Palácio Rio Madeira, Edifício Rio Cautário - 6º Andar
Porto Velho, RO - CEP 76801470