PLANO DE CONTINUIDADE DE SERVICOS ESSENCIAIS

STIC - 2019

Sumário

HISTÓRICO DE VERSÕES

Versão	Descrição	Responsável
1.0	Criação da primeira versão do PCTIC	Nelson Guimarães
1.0	Aprovação em 15/02/2019	Comitê Gestão de TIC
1.0	Publicação em 22/02/2019	STIC
1.1	Revisão	

HISTÓRICO DE ALTERAÇÃO E INCLUSÃO

Data	Inclusão/Alteração	Modificado por

1. Justificativa e Objetivo

Uma vez que falhas nos serviços de TIC impactam diretamente na continuidade da prestação jurisdicional no âmbito da Justiça eleitoral do DF, almeja-se com este plano prover medidas de proteção rápidas e eficazes para os processos críticos de TIC, relacionados aos sistemas essenciais em casos de incidentes graves ou desastres. O plano de continuidade atuará como resposta aos resultados da Análise de Impacto nos Negócios, formalizada no processo SEI 0003655-96.2018.6.07.8100.

2. Escopo

O Plano de Continuidade de TIC (PCTIC) abrange as estratégias necessárias à continuidade dos serviços de TIC essenciais: contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos na abrangência da STIC deste Tribunal e serviços essenciais judiciais, de acordo com a ENTIC-JUD, no seu Art 10º-§ 2º.

Os serviços/sistemas abordados neste plano estão alinhados com aqueles indicados no relatório de Análise de Impacto (BIA), respeitando o critério considerado no processo SEI 0003655-96.2018.6.07.8100, qual seja desenvolver detalhamento das estratégias para ativos de informação que possuem Índice de Criticidade superior a Criticidade Média aferida.

3. Área

O PCTIC será administrado, avaliado e acionado no âmbito da Secretaria de Tecnologia da Informação e Comunicação do TRE-DF, tendo sua manutenção, organização e melhoria revistas e atualizadas periodicamente pela Coordenadoria de Soluções Corporativas (COSC) e pela Coordenadoria de Infra Estrutura (COIE).

4. Principais Riscos

O PCTIC foi desenvolvido para ser acionado quando da ocorrência de cenários de desastres que apresentam risco à continuidade dos serviços essenciais. O quadro abaixo procura dar uma dimensão do universo de riscos dentro da realidade de TIC, cada um possuindo graus diversos de severidade no contexto de TIC deste tribunal, e que serão tratados com mais detalhes dentro do Plano de Recuperação de Desastres (PRD) que compõe o PCTIC.

De fato, a relação de eventos de desastre que se segue não pretende esgotar todas as possibilidades de acontecimentos danosos, porém objetiva apresentar de forma macro um mapeamento inicial que deve ser aperfeiçoado ao longo do tempo, com as revisões previstas na utilização deste plano.

EVENTO DE DESASTRE	POSSÍVEIS CAUSAS
01- Interrupção de energia elétrica	- Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 12 horas. - Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuitos, incêndio e infiltrações. - Impossibilidade de acionar o Grupo gerador no momento de uma queda de energia
02 - Falha Climatização da sala cofre	- Superaquecimento dos ativos devido a falha no dimensionamento de carga na sala cofre - Falha na Unidade de Climatização e não emissão de Alertas de monitoração.
03 Indisponibilidade de Backup	- Cópia de segurança dos dados não disponível ou sem integridade
04 Indisponibilidade de rede/circuitos	- Rompimento de fibra ótica 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
05 Falha humana	- Acidente ao manusear equipamentos, ou abastecimento do tanque de combustível.
06 Ataques internos	- Ataque aos ativos do DataCenter.
07 Incêndio	- Fogo causado por curto circuito nas instalações
08 Desastres Naturais	- Descargas elétricas (raios) - Ocorrencias Sísmicas
09 Falha de hardware	- Falha que necessite reposição de hardware critico ou reparo, e cujo reparo ou aquisição dependa de processo licitatório.
10 Ataque cibernético	- Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais.
11 Falha de Conectividade	- Perda da capacidade de conexão entre TRE, TSE e Cartórios eleitorais

5. Papéis e Responsabilidades

Considerando que os tratamentos dos eventos de desastre requerem a necessidade de atuação multidisciplinar de vários perfis profissionais, temos que a construção deste PCTIC torna necessário atribuir responsabilidades, componentes e papéis definidos para grupos de trabalho, que juntos executarão tarefas definidas.

Os grupos a serem definidos podem possuir participantes lotados em várias unidades do organograma da STIC. Estes componentes podem participar cumulativamente de vários grupos, maximizando a equipe técnica disponível.

Seguem abaixo os grupos e suas atribuições para consecução do PCTIC:

COMITÊ DE DISASTER/RECOVERY (DR):

- Avaliar o plano de Continuidade de Serviços Essenciais de forma periódica e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.
- Inclui autoridades em nível institucional e tomadores de decisão da Secretaria de Tecnologia da Informação e Comunicação.

EQUIPE DE REDES:

- Avaliar os danos específicos de qualquer infraestrutura de rede no fornecimento de dados e conectividade de rede de voz, incluindo WAN, LAN e quaisquer conexões de telefonia interna dentro do TRE-DF ou de infraestrutura externa junto aos servidores.

EQUIPE DE SERVIDORES/SEGURANÇA DE INFORMAÇÕES:

- Fornecer a infraestrutura de servidores físicos e virtuais necessária para que a STIC execute suas operações e processos essenciais durante um desastre.
- Prover mecanismos de segurança no ambiente principal e alternativo. Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança.
- Monitoramento e Análise da estrutura de hiperconvergência

EQUIPE DE GESTÃO INFRA ESTRUTURA:

- Responsável pela infraestrutura que abriga os sistemas de TIC e pela garantia que as as estruturas alternativas (lógicas ou físicas) são mantidas adequadamente.
- Avaliar os danos e supervisiona a execução do Plano de Recuperação de Desastres.
- O líder desta equipe administrará e manterá o Plano de Recuperação de Desastres.

EQUIPE DE APLICAÇÕES:

- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios, durante ocorrência do desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes de TIC, conforme necessário.
- O líder desta equipe administrará e manterá o Plano de Continuidade Operacional.

EQUIPE DE OPERAÇÕES :

- Fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível. Eles precisarão provisionar os servidores do TRE-DF na solução de contingência.
- Monitorar e recuperar as estruturas de armazenamento do BD

EQUIPE DE COMUNICAÇÃO:

- Responsável por informar sobre a evolução das providências em andamento visando restaurar o serviço inoperante junto a servidores, autoridades, fornecedores e Assessoria de comunicação, que se encarregará de prestar informações à Mídia, se for o caso.
- O líder desta equipe administrará e manterá o Plano de Administração de Crises.

EQUIPE DE BACKUP:

- Responsável por 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.

6. Invocação do Plano

O PCTIC será acionado quando da ocorrência de algum dos cenários de desastres, a insurgência ou 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 **COMITÊ DE DR** em conjunto com a alta administração do TRE-DF. O acionamento das demais equipes será realizado pelos integrantes do **Comitê de DR**, de acordo com as características de cada ocorrência, havendo o registro do evento através do Formulário de invocação do Plano onde serão consignados informações como data do incidente, descrição sucinta do ocorrido e quais as equipes acionadas.

REGISTRO DE ACIONAMENTO DO PCTIC

	Data/Hora Início _____/____/_____ ____:_____	Data/Hora Fim ____/____/____ ____:_____	
Descrição			
Resultado			

Os integrantes das equipes, após acionados, iniciarão a avaliação e investigação do ocorrido, podendo acionar outras equipes caso necessário. Os protocolos e procedimentos de recuperação deverão ser imediatamente iniciados visando cumprir os parâmetros de TMP (Tolerância a Paralisação) e RTO (Tempo Máximo de Recuperação), ambos contidos no documento de Análise de Impacto (BIA).

Segue abaixo o planejamento da árvore de acionamento de Contatos, que estabelece o registro das informações dos principais atores, na eventualidade de acionamento do plano.

7. Árvore de Acionamento de Contatos

Comitê de DR (Disaster Recovery)

Servidor	Ramal	Contato Alternativo
Ricardo Negrão (Líder)	4132	ricardonegrao@tre-df.jus.br
Rafael Dittberner	4139	rafa@tre-df.jus.br
Andrey	4040	andrey.correa@tre-df.jus.br

Equipe de Redes

Servidor	Ramal	Contato Alternativo
Fernando Batelli (Líder)	4480	fbatelli@tre-df.jus.br
Marcelo Missias	4149	mmissias@tre-df.jus.br
Leonardo	4146	lamorim@tre-df.jus.br

Equipe de Equipamentos Servidores/Segurança de informações

Servidor	Ramal	Contato Alternativo
Marcelo Missias (Líder)	4149	mmissias@tre-df.jus.br
Leonardo	4146	lamorim@tre-df.jus.br

Equipe de Gestão Infra Estrutura

Servidor	Ramal	Contato Alternativo
Andrey (Líder)	4040	andrey.correa@tre-df.jus.br
Fernando Batelli	4480	fbatelli@tre-df.jus.br

Equipe de Aplicações

Servidor	Ramal	Contato Alternativo
Giuliano (Líder)	4137	giuliano@tre-df.jus.br
Camila Kinoshita	4039	camilak@tre-df.jus.br

Equipe de Operações

Servidor	Ramal	Contato Alternativo
Fernando Batelli (Líder)	4480	fbatelli@tre-df.jus.br
Nishiyama	4141	nishyiama@tre-df.jus.br
Anderson	4011	ameneses@tre-df.jus.br
Leandro	4278	lcarisio@tre-df.jus.br

Equipe de Comunicação

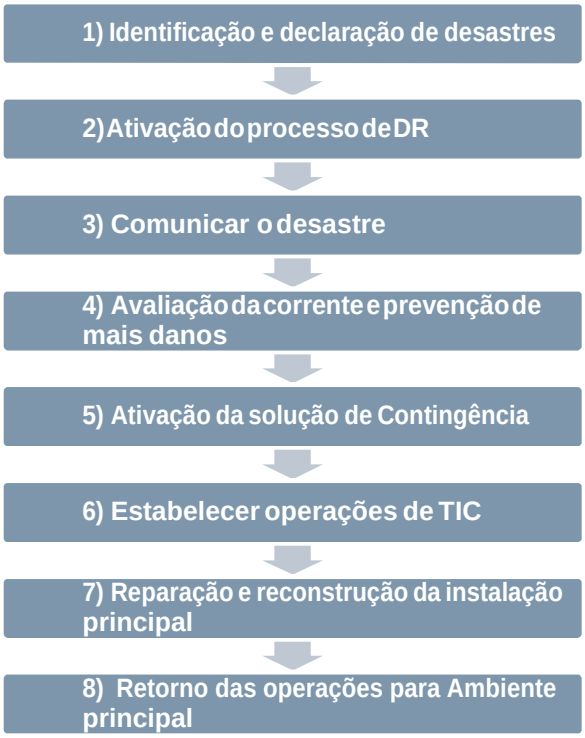
Servidor	Ramal	Contato Alternativo
Ricardo Negrão (Líder)	4132	ricardonegrao@tre-df.jus.br
Nelson Guimarães	4136	nelson.neto@tre-df.jus.br
Aline/Marcia	6007	helpdesk@tre-df.jus.br

Equipe de Backup

Servidor	Ramal	Contato Alternativo
Marcelo Missias (Líder)	4149	mmissias@tre-df.jus.br
Leandro Carisio	4278	lcarisio@tre-df.jus.br

8. Protocolo de Tratamento do PCTIC

O protocolo de tratamento dos eventos definidos neste Plano de continuidade de Serviços Essenciais (PCTIC) é composto de fases ou macroprocessos que se encontram definidos e desmembrados em sub-planos específicos para cada área de atuação, quando da ocorrência de um desastre. A sequencia das atividades estão representadas abaixo, de forma genérica, a saber:



Os sub-planos do PCTIC juntamente com seus objetivos estão assim organizados:

- Plano de Continuidade Operacional (PCO):
  - Seu objetivo é garantir a continuidade dos serviços críticos de TIC na ocorrência de um desastre, enquanto recupera-se o ambiente principal. O PCO é fortemente orientado aos processos(sistemas) e serviços.

- Plano de Administração de Crise (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 Recuperação de Desastre (PRD):
  - O Planejar e agir para que, uma vez controlada a contingência e passada a crise, a STIC do TRE-DF retome seus níveis originais de operação no ambiente principal.O PRD é fortemente orientado aos processos de recuperação de ativos físicos.

9. Estratégias de Continuidade

A estratégia de continuidade para o cenário atual de TIC e serviços essenciais judiciais está formulada em 2 níveis distintos, ativados pela severidade do tipo de desastre ocorrido, se utilizando em seu primeiro nível de estruturas de hiperconvergência, e em seu segundo nível em site alternativo do tipo “cold site”.

Os sistemas essenciais abrangidos pelas estratégias de continuidade descritas abaixo estão indicados no relatório de Análise de Impacto (BIA), respeitando o critério considerado no processo SEI 0003655-96.2018.6.07.8100.

Os níveis que compoem a estratégia de continuidade são:

9.1 Estrutura de hiperconvergência

Estrutura composta de equipamentos que contem os sistemas essenciais, trabalhando em paralelo com regime de redundância e sincronização de dados, possuindo 9 nós na configuração corrente.

Atualmente esta estrutura possibilita a perda de até 2 servidores e 3 storages de armazenamento de forma simultânea, viabilizando um tempo de parade reduzido quanto aos sistemas essenciais.

Esta estrutura se destina a tratar de severidades onde há o comprometimento pontual do servidor que hospeda os dados dos sistemas.

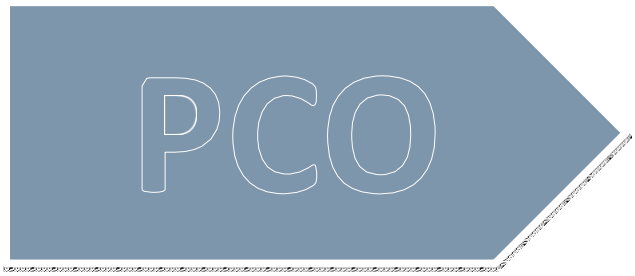
9.2 Cold site em ambiente diverso da Sala Cofre

Backup dos sistemas essenciais armazenados em local alternativo localizado na estrutura de TIC do Tribunal Superior Eleitoral, realizado semanalmente, porem sem possuir equipamentos servidores configurados no local.

A conectividade entre a estrutura de TIC do TRE e do TSE possui redundância, contudo depende da restauração operacional do ambiente principal no TRE para restauração das informações hospedadas nos Backups hospedados no TSE.

Esta estrutura se destina a tratar ocorrências de severidade onde há o comprometimento total da Sala Cofre, possuindo tempo de parada medio-alto.

As ações de contingência e recuperação são detalhadas nos subplanos a seguir.



PLANO DE CONTINUIDADE OPERACIONAL

10. PLANO DE CONTINUIDADE OPERACIONAL (PCO)

Conforme definido nos Artigos 14 e 15 da Portaria PRES 125/2018, o PCO descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais.

O PCO deve ser revisado, atualizado e gerenciado conjuntamente pelos líderes das equipes de **GESTÃO DE INFRAESTRUTURA** e **APLICAÇÕES**.

10.1 Objetivo e Escopo

É escopo deste plano garantir ações de continuidade durante e depois da ocorrência de uma crise ou cenário de desastre, tratando-se apenas das ações de contingência definidas na estratégia, prioritariamente aquelas referentes aos ativos de informação indicados no relatório de Análise de Impacto (BIA), respeitando o critério considerado no processo SEI 0003655-96.2018.6.07.8100, qual seja desenvolver detalhamento das estratégias para ativos de informação que possuem Indice de Criticidade superior a Criticidade Média aferida.

São objetivos PCO:

- Prover meios para manter o funcionamento dos principais serviços de TIC e a continuidade das operações de TIC, dos sistemas essenciais.
- Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações de TIC durante uma crise ou cenário de desastre.
- Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência.

10.2 Gestão do plano

A STIC é a unidade responsável por implementar, manter e melhorar o PCO e toda a documentação inerente. Genericamente podemos definir que o processo de gestão do PCO é composto das seguintes fases:

I. Planejar: definição de estratégias, políticas internas, controles e procedimentos de rotina para garantir segurança das informações;

II. Executar: os processos definidos são implementados. Coleta de informações são de extrema relevância;

III. Checar: são feitas avaliações de processos implementados para verificar se o planejado foi realmente executado de forma

adequada para alcançar as metas. São identificados desvios de execução e apresentados resultados para análise crítica da direção da empresa. Há um monitoramento contínuo dos processos no intuito de evitar qualquer tipo de falha ou erros;

IV. Agir: são realizadas ações corretivas e preventivas baseadas na identificação de desvios de execução e nas considerações apresentadas nas etapas (I), (II) e (III).

Conforme determina o Art. 15 da Portaria PRES 125/2018 TRE-DF, as informações referentes a criticidade de cada ativo, seus indicadores de RTO, RPO e TMP foram levantados e estão explicitados no documento BIA, Pags. 9 e 10, processo SEI 0003655-96.2018.6.07.8100.

10.3 Ativação do Plano

A utilização da estratégia de hiperconvergência para mitigação da continuidade operacional se realiza de forma transparente, sem intervenção manual, sendo necessário apenas o registro de sua ativação, indicando data e hora da ocorrência, bem como descrição suscinta dos servidores afetados.

No caso de utilização da estratégia “cold site” temos as seguintes etapas a serem observadas:

10.3.1 Avaliação de Impacto de Desastre

Nos casos não cobertos pela estratégia de hiperconvergência e tão logo identificada a ocorrência de um incidente ou crise, os líderes das equipes **OPERAÇÕES, EQUIPAMENTOS SERVIDORES** e **BACKUP** devem verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido.

As informações devem ser consolidadas e submetidas ao **COMITÊ DE DR** para avaliação e decisão sobre o acionamento do plano e início das ações de contingência.

Dado o aval pelo **COMITÊ DE DR** ao acionamento do plano, este convocará reunião de emergência com os líderes do PRD e PAC com o intuito de:

- Coordenar prazos e orquestrar as ações de contingência.
- Informar as equipes das ações de contingência com a priorização dos serviços essenciais definidos na Análise de Impacto no Negócio (BIA).

10.3.2 Execução

Na utilização do estratégia de “cold site” devem ser adotadas as seguintes ações de contingência e continuidade por processo ou serviço essencial, provendo o registro de sua duração, quaisquer observações pertinentes e o resultado atingido

Registros de Continuidade Cold Site				
Id	**Instrução**	**Duração**	**Observação**	**Resultado**
1	Verificar status da aplicação de backup e estimar impacto de perda dados (janela)			☐
2	Estimar volume de dados a serem recuperados, tempo de recuperação dos dados e possíveis perdas operacionais			☐
3	Prover recovery de Aplicação e Dados no ambiente temporário			☐
4	Teste de aplicação após desastre			☐
5	Validar reconfigurações de acesso/policies implementadas			☐
6	Atestar retorno do funcionamento do ambiente com Líder do PRD			☐

10.4 Encerramento do PCO

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter deverá ser emitido um parecer ao comitê relatando as atividades realizadas neste PCO.

Informar à equipe de **COMUNICAÇÃO** o retorno das atividades.

PAC

PLANO DE ADMINISTRAÇÃO DE CRISES

11. PLANO DE ADMINISTRAÇÃO DE CRISE (PAC)

Este plano especifica as ações ante os cenários de desastres. As ações incluem gerir, administrar, eliminar ou neutralizar os impactos, inerente ao relacionamento entre os agentes envolvidos e/ou afetados, até a superação da crise, através da orquestração das ações e de uma comunicação eficaz.

O PAC deve ser revisado, atualizado e gerenciado conjuntamente pelo líder do **COMITE DE DR**.

11.1 Objetivo

O objetivo deste plano é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de uma catástrofe.

São objetivos específicos do PAC:

- Garantir a segurança à vida das pessoas;
- Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise.
- Orientar os servidores e demais colaboradores com informações e procedimentos de conduta.
- Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido, através do repasse de informações a Assessoria de Comunicação do TRE-DF.

11.2 Ativação do Plano

A ativação do plano sera feito pela STIC e tem por objetivo gerenciar e coordenar as providências a serem tomadas no âmbito da continuidade operacional e recuperação do desastre, como tambem criar um canal de comunicação centralizado com a administração sobre o trabalho realizado até a normalização da situação.

As recomendações para consecução do plano estão assim elencadas:

11.2.1 Comunicação da ocorrência de um Desastre

Na ocorrência de um desastre faz-se necessário entrar em contato com diversas áreas, principalmente as afetadas para informá-las de seu efeito na continuidade dos serviços e tempo de recuperação. A Equipe de **COMUNICAÇÃO** será responsável por

contatar estas unidades e repassar as informações pertinentes a cada grupo, setor ou seguimento.

Após reunião com líderes do PRD e PCO, a equipe de comunicação elaborará um breve programa de comunicação para acionar as partes envolvidas e afetadas, objetivando informar a todos sobre a perspectiva de esforços necessários para o reestabelecimento dos serviços nativos.

Os itens abaixo definem os níveis necessários de comunicação.

11.2.2 Comunicação com os Servidores e Colaboradores

A Equipe de **COMUNICAÇÃO** deverá prover um meio de contato específico para este fim, com intuito de que os servidores e colaboradores do TRE-DF mantenham-se informados da ocorrência de um desastre e da inatividade dos serviços essenciais de TIC.

Contatos de E-mail: helpdesk@tre-df.jus.br (caso serviço de e-mail esteja operacional)

Central de Serviços (helpdesk): 3048-6007 (caso telefonia esteja operacional)

As informações a serem fornecidas, de forma a padronizar o nivel de informação sobre o evento ocorrido, compreenderão a estimativa de defasagem de atualização das informações que estarão disponíveis, possíveis restrições de acesso quanto a horários ou de performance, quais serviços ainda estão disponíveis e expectativas de conclusão da recuperação durante o desastre.

11.2.3 Comunicação com Unidades do TRE-DF

A Equipe de **COMUNICAÇÃO** deverá acionar diretamente às unidade afetadas pelo desastre e fornecer contato, mantendo informado o titular da unidade atingida quanto a natureza, impacto, abrangência da ocorrência, ações de contingência em andamento e dos processos/sistemas e serviços cobertos pelo plano de continuidade (serviços essenciais).

11.2.4 Comunicação com fornecedores e prestadores de serviço

No caso de ocorrência de desastre que envolva comprometimento parcial ou total do Data Center, a Equipe de **COMUNICAÇÃO** deverá acionar diretamente os fornecedoras e empresas envolvidas, registrando Data/Hora do contado realizado, bem como pessoa contatada.

Para registro do referido contato será utilizado a seguinte Lista de Principais Fornecedores:

LISTA DOS PRINCIPAIS FORNECEDORES	
Empresa: **HP** Nº Contato: **0800-7097751 ou 0800-710-2029**	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ___:___:___
Empresa: **ORACLE** Nº Contato: **0800-7097751 ou 0800-556405**	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ___:___:___
Empresa: **DELL** Nº Contato: 0800 722 3300 / **0800 7703811**	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ___:___:___
Empresa: **GREEN4T (ACECO)** Contato: 0800-883-6018	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ___:___:___
Empresa: **AMERICA (HUAWEI)** Nº Contato: **(061) 3349-9785**	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ___:___:___
Empresa: **VERT(AVAYA)** Contato: **(61) 2103-1038**	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ___:___:___
Empresa: **SISTECH (NUTANIX/VMWARE)** Nº Contato: **(061) 3342-3781**	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ___:___:___
Empresa: **VEEAM** Contato: 0800-761-2311	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ___:___:___

Empresa: **CLARO/EMBRATEL** Contato: (61) 2106-7389	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ___:___:___
Empresa: **TELEFONICA** Contato: (61) 3962 7616	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ___:___:___

11.2.5 Comunicação com Colaboradores Externos, Cidadãos e Mídia

A Equipe de **COMUNICAÇÃO** em consonância com a Assessoria de Comunicação do TRE-DF, deverá fornecer informações pertinentes aos colabores externos: Advogados, cidadãos e outros órgãos.

As atividades a serem desenvolvidas serão de validação da situação ocorrida de acordo com o cenário,e conforme o caso, requerendo publicação da interrupção dos serviços em meios oficiais e de ampla divulgação, com aval da administração da Corte.

Tão logo haja o retorno à normalidade, comunicar a todas as partes citadas.

11.3 Encerramento do PAC

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter, a Equipe de **COMUNICAÇÃO** entrará em contato com as partes descritas neste plano provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

Compor relatório com relação das atividades necessárias após a ocorrência do desastre como: remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

PRD

PLANO DE RECUPERAÇÃO DE DESASTRES

12. PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para reestabelecer o nível de operação dos serviços no ambiente afetado dentro de um prazo tolerável.

O PRD deve ser revisado e atualizado conjuntamente pelos líderes das equipes de **GESTÃO DE INFRAESTRUTURA** e **APLICAÇÕES**.

12.1 Objetivo e Escopo

É escopo deste plano garantir o retorno das operações do ambiente principal depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas dos ativos, conexões e configurações deste ambiente.

São objetivos PRD:

I. Avaliar danos aos ativos, serviços essenciais e conexões do datacenter, provendo meios para sua recuperação.

II. Evitar desdobramentos de outros incidentes na instalação principal.

III. Reestabelecer o datacenter ou serviço/sistema essencial, dentro do prazo tolerável

12.2 Possíveis Cenários de Inoperância

A partir da determinação e levantamento de potenciais riscos frente as possíveis situações que se apresentam dentro do universo da STIC, procuramos elencar no quadro abaixo os principais incidentes, suas possíveis causas e medidas macro mais adequadas para recuperação destes cenários de inoperância. São eles:

Identificação de Incidentes		**Tratamento do Incidente**
Incidente	**Causas**	**Procedimentos Macro de Recuperação**
Falha de alimentação de energia elétrica	Externa	- Acionamento junto á prestadora de energia elétrica de solicitação de reestabelecimento dos services elétricos. - Solicitação de previsão de conclusão das providências
	Interna	- Acionar o setor de administração predial para verificação dos geradores emergenciais. - Acionar setor de administração predial solicitando verificação de cabeamento elétrico, disjuntores, fusíveis, etc, considerando os 2 circuitos independents (Sala/Ar condicionado)
	Danos ao nobreak	- Solicitar ao setor de administração predial a manutenção do mesmo e execução de reparos (limpeza, trocas de baterias, ou conserto de placa, etc)

Indisponibilidade dos serviços /aplicações pela rede Interna	Danos a Switch	- Verificação de cabeamento UTP e Fibra - Verificação existencia de equipamento reserva - Acionar a garantia, se for o caso - Reconfiguração do novo equipamento através da biblioteca de configurações - Instalar e testar equipamento
	Danos ao cabeamento	- Substituir ou reparar o cabo danificado - Verificação de segmento/porta logica para via de conexão alternative
	Danos a servidor de arquivos/aplicação	- Verificação de montagem de máquina virtual ou disponibilidade de equipamento reserva - Acionar a garantia, se for o caso - Identificação do backup de dados mais recente e restauração das informações - Ativação do equipamento em produção, baseado na biblioteca de configurações - Testes
	Danos a servidor de autenticação	- Verificação de montagem de máquina virtual ou disponibilidade de equipamento reserva - Acionar a garantia, se for o caso - Identificação do backup de dados mais recente e restauração das informações - Ativação do equipamento em produção, baseado na biblioteca de configurações - Testes
	Danos na estação de Trabalho	- Identificação das causas que ocasionaram o dano - Verificação da existencia de equipamento de contingência - Acionar a garantia, se for o caso. - Restaurar imagem do equipamento de acordo com a biblioteca de configurações - Testes
	Remoção de dados pelo usuário	- Identificar meios pelos quais foram possíveis se fazer a remoção e tratá-los em conformidade com a Política de Segurança da Informação adotada. - Identificação do backup de dados mais recente e restauração das informações removidas. - Restauração do backup e Testes.
	Indisponibilidade da linha telefônica	- Verificar Central Telefônica. - Verificar configurações de ramal - Acionar representante/consultor da prestadora de serviços de telecomunicação, o qual realizará o devido reparo ou troca do equipamento danificado
Indisponibilidade dos serviços de Internet	Servidor Internet indisponível	- Abrir chamado Service Desk TRE - Verificar configurações e conteúdos WEB - Recomposição de rotinas dos serviços, se for o caso - Testes
	Link Internet indisponível	- Abrir chamado Service Desk TRE - Verificar configurações e conteúdos WEB - Recomposição de rotinas dos serviços, se for o caso - Testes
	Estação de Trabalho desconfigurada	- Reconfiguração segundo política de acesso. - Verificação de perfil de usuário, se for o caso - Testes

Vírus	Infecção do equipamento por acesso a sítio malicioso ou arquivo suspeito	- Fazer atualização e varredura de antivirus e identificar os meios que possibilitaram a contaminação. - Descontaminar equipamento com ferramentas apropriadas. - Verificação e reconfiguração da estação de trabalho, se for o caso. - Medidas de conscientização quanto a política de segurança para os usuários envolvidos. - Testes
Indisponibilidade de restauração de backups	Mídia indisponível	- Verificação da disponibilidade de mídia alternativa. - Identificação do backup de dados mais recente e restauração das informações, se for o caso. - Notificar comitê DR sobre a data/hora do backup que sera recuperado. - Verificar causas de indisponibilidade e revisar processo de execução. - Testes
	Backup mais recente de usuário não existe	- Verificar existencia de backup anterior - Recomendar ao usuário a inclusão de seus arquivos no drive Corporativo.
Indisponibilidade de Links de Comunicação com o TSE		- Verificação de infraestrutura interna - Abrir chamado no Service Desk do TSE, se for o caso.
Indisponibilidade de Links de Comunicação com Cartórios Eleitorais		- Verificação de infraestrutura interna e nos Cartórios eleitorais - Abrir chamado no Service Desk da concessionária dos Links de comunicação - Monitoramento do SLA acordado
Falta de refrigeração No Data Center	Falha de alimentação de energia para o circuito Ar condicionado	- Abrir chamado na Administração Predial para avaliação e reparos - Solicitar previsão para término dos reparos
	Falha no circuito elétrico	- Abrir chamado na Administração Predial para avaliação e reparos - Solicitar previsão para término dos reparos
	Falha no equipamento de Ar condicionado.	- Abrir chamado no Service Desk da empresa de manutenção do Data Center - Monitoramento do SLA acordado

Os procedimentos macro de recuperação elencados na tabela acima, serão conduzidos pela execução formal das seguintes etapas definidas abaixo sob a supervisão da Equipe de **GESTAO DE INFRAESTRUTURA**:

12.2 Ativação do Plano

A ativação do presente plano se dará na ocorrência de um dos cenários elencados acima, ou ainda por conta de ocorrência de evento ainda não mapeado que tenha gerado interrupção nos serviços essenciais, seguindo o fluxo de fases definidos abaixo.

12.2.1 Identificação de Ativos Inoperantes

As equipes de **BACKUP, EQUIPAMENTOS SERVIDORES, REDE e OPERAÇÕES** deverão identificar e listar todos os Ativos/Serviços inoperantes em decorrência do desastre.

As informações de cada ativo inoperante devem ser condensadas em levantamento contendo no mínimo identificação, IP, breve descrição de sua função, indicação se está em periodo de garantia, se há redundância física disponível, responsável, fornecedor.

12.2.2 Identificação de acessos interrompidos

A Equipe de **REDE** deverá identificar a existência de interrupções de conexões e acessos gerados após o desastre, informando sua abrangência(rede local, rede WAN ou provedor de serviços), quando aplicável.

12.2.3 Identificação de serviços descontinuados

A equipe de **GESTAO DE INFRAESTRUTURA** deverá mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento do **COMITÊ DE DR**. O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, *firewall*, *storage*, *routers* e *switches*, bem como respectivas configurações de *proxy*, DNS, rotas, *vlans*, etc.

12.2.4 Elaboração de cronograma de recuperação

A equipe de **GESTAO DE INFRAESTRUTURA** após o mapeamento das perdas e impactos elaborará um breve cronograma de recuperação dos serviços/aplicações atingidos pelo desastre levando em consideração:

- A priorização dos serviços essenciais, ou se for o caso, outra determinação de prioridades de nível institucional desde que formalmente solicitada à STIC.
- A utilização da rotina existente de tratamento de recuperação existente, para cada um dos ativos de informação.
- O RTO (Tempo Máximo de Recuperação) definido para cada serviço essencial.
- A força de trabalho disponível.

12.2.5 Substituição de ativos e equipamentos

Em caso de perda de ativos, deverá ser imediatamente informado ao **COMITÊ DE DR**, a necessidade de aquisição de ativos perdidos que não puderem ser recuperados.

A equipe irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço, comunicando ao **COMITÊ DE DR** se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição.

A equipe de **OPERAÇÕES** deve verificar dentre os ativos danificados quais estão cobertos por garantia e se a mesma poderá ser acionada neste caso através da lista de fornecedores.

As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes do PCO e PAC.

12.2.6 Reconfiguração de ativos e equipamento

A equipe de **OPERAÇÕES** deverá verificar se as configurações dos ativos reparados ou substituídos, estão em funcionamento pleno. Caso não estejam, prover cronograma estimado para configurar estes ativos informando ao **COMITÊ DE DR**.

12.2.7 Teste de ambiente/homologação

O ambiente principal do datacenter deverá ser testado antes do recovery dos dados do backup, afim de garantir que o processo de recuperação ocorra conforme o planejado.

Os testes incluem:

- Avaliar performance para garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais, antes do desastre.
- Validar as configurações

12.2.8 Recuperar dados do backup

Nos casos de recuperação de dados para as aplicações, este será realizado pela Equipe **BACKUP** com a cópia de segurança mais recente disponível, notificando o líder do PRD da data e hora do mesmo.

12.3 Encerramento do PRD

Ao término do procedimento de recovery, as informações da recuperação de serviços serão consolidadas em parecer específico informando horário de reestabelecimento de cada serviço, equipamentos adquiridos (se for o caso), procedimentos de recuperação realizados e fornecedores acionados.

13. Validação e Teste do PCTIC

Cumprindo o proposito de reavaliar os procedimentos planejados visando a melhoria continua, o PCTIC será testado e validado em reunião entre os líderes de cada subplano a cada semestre ou com a insurgência de novos fatores de risco, mudança na análise de impacto, ou com a inclusão de um novo serviço no plano de continuidade.

A execução dos passos planejados deve ser registrada indicando Data de execução, Tipo do teste, descrição de motivo e Status, respeitando os seguintes critérios a serem informados no registro:

Tipos de testes a serem realizados:

- Teste de mesa

  Teste de complexidade simples, no qual é realizada uma análise (crítica ensaios de execução), dos procedimentos e informações descritas, com o objetivo de atualizar e(ou) validar os procedimentos e as informações contidas no plano;

- Simulação no ambiente: Simular uma situação real de interrupção.

  Teste de complexidade média no qual uma situação “artificial” é criada, por exemplo, é realizada a parada de um processo em horários diferentes das operações diárias (finais de semana, após expediente, etc.) sendo o resultado utilizado para validar se os planos possuem as informações necessárias e suficientes, de forma a permitir recuperação de determinado arranjo de contingência ou processo com sucesso;

Status:

- Programado
- Executado
- Planejado
- Agendado

	Registros de Validação e Testes - PCTIC				
Tipo de Teste	**Descrição**	**Status**	**Data**	**Observação**	**Resultado**
					☐
					☐
					☐