Poder Judiciário do Estado do Amapá
Tribunal de Justiça

POLÍTICA DE CONTINUIDADE DE NEGÓCIOS

Código:	
Versão:	
Data da versão:	
Criado por:	
Aprovado por:	
Nível de confidencialidade:	

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
14/07/2017	0.1	Jonas Gil	Esboço básico do documento
22/07/2017	0.2	Jonas Gil	Finalizando

Sumário

1. Introdução

Todos os processos de negócio do Tribunal de Justiça do Amapá (TJAP) são, de alguma forma, suportados pelos recursos providos pela Secretaria de Gestão Processual Eletrônica (SGPE), pelo Departamento de Informática e Telecomunicações (DEINTEL) e pelo Departamento de Sistemas (DESIS). Alguns deles têm uma dependência tão grande da TI que seria impossível de se imaginar sua operacionalização, pelo menos em um tempo hábil, sem o apoio dos recursos da TI.

Nesse contexto, é necessário que a SGPE, DEINTEL e DESIS entendam como deverão ser tratados as possíveis falhas que afetam a operação dos processos de negócio do TJAP. De que forma ela deve se prevenir, ou reagir, a eventos que podem comprometer a operação dos serviços de TI? Qual o impacto que a falha desses recursos pode ocasionar?

A intenção inicial deste documento é fazer com que a SGPE, DEINTEL e DESIS passem a responder com mais clareza os questionamentos acima e, além disso, permitir que o TJAP continue operando os seus principais processos de negócio em caso de falhas nos serviços de TI.

Posteriormente, espera-se que ele sirva como marco inicial para que o processo de Gestão de Continuidade de Negocio - GCN - seja um processo institucionalizado no TJAP, com a participação ativa da alta administração e a elaboração de um plano de continuidade dos negócios - PCN.

2. Finalidade, escopo e usuários

A finalidade desta Política é definir o escopo e as regras básicas de gestão de continuidade dos negócios.

Os usuários deste documento são funcionários do TRIBUNAL DE JUSTIÇA DO AMAPÁ, além de fornecedores e parceiros terceirizados que possuem papel na gestão de continuidade.

3. Documentos de referência

- Norma ISO 22301, cláusulas 4.1, 4.3, 5.3, 6.2 e 9.1.1
- Norma BS 25999-2, cláusulas 3.2.1, 3.2.2 e 3.2.3
- Norma ISO/IEC 27001, cláusula A.14
- Norma NBR 22301, <clausulas>
- Resolução CNJ 176/2013 - <Link>
- Resolução CNJ 239/2016 - <Link>
- Resolução CNJ 211/2013 - <Link>

4. Gestão da continuidade de negócios

4.1. Conceitos Gerais

Conforme exposto na Introdução, este documento pretende ser o marco inicial para a confecção e institucionalização de um PCN no TJAP. Ele contém boa parte das informações necessárias para a confecção deste plano. Por isso, para melhorar o entendimento das ações aqui detalhadas, é necessário a apresentação de alguns conceitos importantes sobre o tema de continuidade de serviços.

4.1.1. Plano de Continuidade de Negócios – PCN

O PCN é um documento que visa realizar o planejamento das ações que devem ser executadas em uma situação de crise que afete as operações de negócio. Ele possibilita a à organização continuar suas atividades em um nível aceitável pré-definido.

Esse plano é, na verdade, constituído de 3 documentos:

A. Plano de administração de crise: é um documento disponibilizado para a alta gestão que objetiva dá mais controle para organização em caso de uma situação de crise. Contém informações como: listas de contatos e relação de atividades das equipes envolvidas.
B. Plano de continuidade operacional: documento onde são definidos os procedimentos de resposta para estabilizar a situação na ocorrência de um incidente ou evento indesejado. Seu principal objetivo é identificar principais tipos de incidentes, checar a existência de procedimentos de respostas apropriados e criar procedimentos novos de contingência que ainda não existem. As etapas desse plano são: realizar uma análise do ambiente, elaborando as hipóteses e os possíveis cenários de crise; definir objetivos e metas, analisando a viabilidade e a prioridade com que os danos serão tratados; organizar a equipe, elaborando a estrutura organizacional que vai dar suporte ao plano, definindo procedimentos para ativação do plano, níveis de autoridade, papéis e as responsabilidades.
C. Plano de recuperação de desastre - define os procedimentos para restaurar, no menor tempo possível, as operações de tecnologia da informação em caso de interrupção não-programada. Também devem prever os impactos da paralisação e o tempo máximo necessário para a recuperação as atividades essenciais da organização.

4.1.2. Crise X Contingência

Crise é o momento em que ocorre qualquer evento que compromete o funcionamento correto da organização;

Contingência é o instante que são alocados recursos para responder aos eventos de falha e garantir a continuidade das operações.

4.1.3. Níveis de maturidade

Os níveis de maturidade de processos de TI propostos pelo COBIT descrevem perfis de processos da organização. Ele utiliza uma escala de seis níveis.

Aplicado ao contexto deste documento - processos de continuidade -, pode-se definir esses níveis da seguinte maneira:

Nível 0 (Inexistente) - Não existe nenhum tipo de processo. Os riscos e ameaças não são conhecidos.

Nível 1 (Inicial) - A organização reconhece que a continuidade de negócios é necessária. Nesse nível, as responsabilidades são informais e a resposta aos incidentes são reativas, desorganizadas e inapropriadas.

Nível 2 (Repetitivo) - Nesse nível os processos são estruturados e rotinas similares são seguidas por diferentes pessoas para a mesma tarefa. Existe um alto nível de dependência em relação ao conhecimento individual.

Nível 3 (Definido) - Os processos e rotinas são documentados, padronizados e divulgados. Há rotinas para identificar, minimizar ou eliminar situações de indisponibilidade. Porém, os processos não são monitorados, logo, é possível que algumas inconformidades sejam encontradas.

Nível 4 (Administrado) - Os processos são monitorados e mensurados objetivamente. Há a realização de testes que possibilitam verificar a aderência dos processos. Os incidentes são classificados e conhecimentos por todos os envolvidos.

Nível 5 (Otimizado) - Os processos e procedimentos são definidos ao nível de melhores práticas, baseado na comparação com os resultados encontrados por outras empresas. O PCN é elaborado e mantido pela direção e o gerenciamento de risco faz parte da cultura da organização. Os procedimentos de continuidade são atualizados, melhorados e validados periodicamente.

4.1.4. Situação atual

O TJAP encontra-se no nível 1 e espera-se que após esse plano ele passe para o nível 2 de maturidade em até 1 ano.

4.2. Objetivo da gestão da continuidade de negócios

O objetivo da gestão da continuidade de negócios é identificar ameaças em potencial a uma organização, os impactos nas operações de negócios que estas ameaças podem vir a causar, e oferecer uma estrutura para desenvolver resiliência organizacional com a capacidade de responder de forma eficaz

5. Plano de continuidade de serviços no TJAP

O Comitê gestor de segurança da informação (CGSI) e o DEINTEL mapearam 14 atividades para o processo de plano de continuidade dos serviços de TI.

1. Identificação e classificação dos sistemas/ativos importantes;
2. Identificação e classificação dos sistemas ativos críticos, com base em análise de impacto no negócio;
3. Realizar análise de riscos dos sistemas críticos;
4. Identificar quais riscos serão aceitáveis e quais serão tratáveis;
5. Definição dos responsáveis e formas de contato pelos procedimentos de contingência e recuperação dos ativos listados no item 5.1;
6. Criar o check list de contingência dos sistemas do item 5.1;
7. Criar o check list de recuperação dos sistemas do item 5.1;
8. Definir os prazos de revisão dos planos;
9. Definir prazos para realização dos testes;
10. Divulgar para as equipes o plano;
11. Realizar testes;
12. Atualizar plano de acordo com as não conformidades encontradas nos testes;
13. Aprovar o plano.

As atividades acima serão detalhadas através dos tópicos subsequentes.

5.1. Identificação dos principais sistemas/ativos de TI

Além de sistemas que apoiam diretamente os processos de negócio do TJAP, alguns ativos de TI foram incluídos nessa lista, devido a relevância desses ativos para o funcionamento de todos os sistemas do TJAP.

- TUCUJURIS
- TUCUJURIS Web
- DJE
- Portal Web (Inter)
- Backbone (Link)
- Servidor de arquivos corporativos (SA).
- SIG
- E-mail
- Malote Digital (MD)
- Sistema de telefonia (ST)
- Sistema de autenticação de usuários (AD)
- E-Cidade (EC)
- Folha de Pagamento (FP)

5.2. Análise de impacto no negócio

Em decorrência da baixa maturidade da organização nos processos da GCN, da falta de comitês ou equipes multidisciplinares com a responsabilidade definidas para essa atividade e do grande volume de processos de negócios no TJAP, não foi possível realizar as atividades desse plano para todos os sistemas e ativos de TI do TJAP.

Em vez disso, foi realizada uma análise de impacto no negócio da lista de sistemas e ativos de TI descritos no item anterior, considerados importantes para o TJAP. Para cada item dessa lista, a Comitê Gestor de Segurança da Informação - CGSI- e o

Departamento de Informática e Telecomunicações - DEINTEL fizeram a análise de impacto do negócio desse item, através do preenchimento do **formulário** abaixo.

Do resultado desta análise, será escolhido nesta versão os sistemas mais críticos com nota de corte superior a 70.

Sugestão: Existir uma meta de redução da nota de corte em 10 pontos a cada revisão deste documento.

INFORMAÇÕES GERAIS DO SISTEMA/ATIVO DE TI			
ID			
Nome do Sistema/Ativo			
Avaliador			
Processos de negócio relacionados			
Setores impactados			
ANÁLISE DO IMPACTO			
Pergunta	**Item**	**Valor do Item**	**Resposta**
1 - Qual o nível de criticidade?	As atividades **param** caso o serviço esteja indisponível	30	
	As atividades podem ser **continuadas, mas por pouco tempo**.	15	
	As atividades podem ser realizadas normalmente, comprometendo apenas a performance.	5	
2 - Apoia que tipo de área no TJAP?	Ambas	15	
	Área fim	10	
	Área meio	5	
3 - Existem prejuízos financeiros caso este serviço pare?	Significantes	30	
	Moderados	7	
	Pouco	4	
	Nenhum prejuízo	0	
4 - Garante o cumprimento de alguma legislação?	Sim	25	
	Não	0	
RESULTADO			

As instruções para preenchimento do formulário

No campo de **INFORMAÇÕES GERAIS DO SISTEMA/ATIVO DE TI** deve-se preencher informações gerais sobre o sistema. O campo ID é um número aleatório único para cada sistema/ativo.

No campo **ANÁLISE DO IMPACTO** deve-se escolher, para cada pergunta, uma única resposta.

O campo **RESULTADO** deriva da aplicação da seguinte fórmula.

RESULTADO = Somatória dos pontos obtidos em cada questão

Todos os formulários acima foram respondidos pela CGSI e pela DEINTEL e consolidados na tabela a seguir. Em versões posteriores deste documento, pretende- se envolver outras áreas de negócio do TJAP, de forma que as informações aqui apresentadas sejam mais condizentes com a realidade do Tribunal.

INFORMAÇÕES GERAIS DO SISTEMA/ATIVO DE TI													
ID	1	2	3	4	5	6	7	8	9	10	11	12	13
Nome do Sistema/Ativo	TUC	TUC-W	DJE	WWW	LINK	SA	SIG	MAIL	MAL	TELE	AD	ECID	FOL
Avaliador	CGSI e DEINTEL												
Processos de negócio relacionados	Tramitação de processos judiciais- Interno / Cliente-Servidor	Tramitação de processos judiciais- Externo - WEB	Publicação de atos	Comunicação institucional	Comunicação de dados	Armazenamento de arquivos de apoio a vários processos de negócios	Sistema de Gestão administrativo	Sistema de correio eletrônico	Sistema de comunicação do judiciário	Sistema de telefonia	Sistema de autenticação	Sistema administrativo	Sistema de cáculo da folha de pgto.
Setores Impactados	1º E 2º GRAUS	1º E 2º GRAUS	Todos	Todos	Todos	Todos	1º E 2º GRAUS	Todos	Todos	Todos	Todos	Adm	Todos

ANÁLISE DE IMPACTO														
PERGUNTA	ITEM	VALOR	TUC	TUC-W	DJE	WWW	LINK	SA	SIG	MAIL	MAL	TELE	AD	ECID	FOL
1 - Qual o nível de criticidade?	As atividades **param** caso o serviço esteja indisponível	30	X										X	X	
	As atividades podem ser **continuadas, mas por pouco tempo.**	15		X	X	X	X		X		X				X
	As atividades podem ser realizadas normalmente. Degrada apenas a performance.	5						X		X		X			
2 - Apoia principalmente que tipo de área no TJAP?	Ambas	15			X	X	X	X	X	X	X	X	X		
	Área fim	10	X	X											
	Área meio	5												X	X
3 - Existem prejuízos financeiros caso este serviço pare?	Significantes	30	X										X		X
	Moderados	7					X		X	X	X	X		X	
	Pouco	4		X	X	X		X							
	Nenhum prejuízo	0													
4 - Garante o cumprimento de alguma legislação?	Sim	25	X	X	X	X	X		X	X	X	X	X	X	X
	Não	0						X							
			95	54	59	59	62	24	62	52	62	52	100	67	75

Dos resultados obtidos, 3 sistemas/ativos foram escolhidos, por obterem as maiores notas na análise de impacto: TUC, AD e FOL.

5.3. Análise de riscos, responsáveis e procedimentos de recuperação e contingência

Após a identificação dos sistemas/ativos críticos, foram mapeados os riscos para cada sistema/ativo, a respostas a esses riscos, os responsáveis pelas ações e os procedimentos para prevenção, contingência e recuperação, conforme planos de ação definidos a seguir.

Sistema de gestão processual eletrônica - TUCUJURIS

Sumário do Plano I	
Sistema / Ativo	TUC
Arquitetura	O sistema é composto por três aplicações: 1. TUCUJURIS → Aplicação usada pelos usuários para tramitação de processos judiciais; 2. ODBC → Aplicação para gerenciamento de conexão entre aplicação e banco de dados. 3. BD_PGSQL → Banco de dados
Localização	Os componentes da arquitetura servidor estão localizados no Data Center do TJAP, em maquinas físicas, com recursos de HA (Alta Disponibilidade), informações armazenadas no Storage EMC - Aplicação cliente e ODBC instalados nas máquinas cliente.

Plano de Ação							
Risco e Probabilidade	**Resposta**	**Responsável**	**Tipo de falha**	**Ação Preventiva**	**Ação Contingência**	**Ação Recuperação**	**Tempo estimado até a recuperação**
Falha de Hardware (média)	Mitigar	Diogo, Leandro e Francisco	Qualquer tipo de problema de hardware (memória, disco, cpu, fonte de energia, etc.)	Monitorar, periodicamente, logs dos servidores em busca de mensagens de erro relacionadas a hardware.	**Para processos judiciais novos:** tramitar fisicamente. Ao final da recuperação, importá-los no sistema. **Processos em andamento**: Necessário realizar recuperação.	1 – Restaurar o serviço nas máquina secundária ou terciária 2 - Realizar restauração do banco de dados, conforme instruções do **anexo III** desse documento, caso seja necessária restauração completa.	1 dia
Vírus (baixa)	Mitigar	Dimicro	Vírus que impactem no funcionamento do sistema	Manter maquinas atualizadas			
Ataque de Crackers	Mitigar	Francisco, Diogo e Leandro	Ataques que impactem no funcionamento do sistema				
Ataques Internos (funcionários insatisfeitos s)	Mitigar	Marco Craveiro, Jonas, Francisco e Leandro	Ataques que impactem no funcionamento do sistema	Melhorar controle de acesso a maquinas.			

Falta de Energia	Mitigar	DAA	Falta de energia para os servidores do Datacenter	Adquirir novos nobreaks com banco de baterias. Estabilização de energia.	Ativar gerador de energia	Desativar gerador e ativar energia através da rede comum.	N/A
Umidade / Vazamento (baixa)	Mitigar	DAA	Umidade ou Vazamento	Verificar, periodicamente, condições físicas do Data Center	N/A	Realizar obras e adaptações necessárias para solucionar o problema	n/A
Incêndio	Mitigar	DAA	Incêndio no Data Center	Monitorar temperatura do Data Center	Não há	Usar as mesmas instruções relatadas para o risco "falha de hardware" dessa tabela.	3 dias
Intempéries (baixa)	Aceitar	DAA, Marco Craveiro	Qualquer problema da natureza que impacte no funcionamento **completo** do Data Center TJAP.	Criar sala segura	Não há		
Indisponibilidade do BD (baixa)	Mitigar	Diogo e Leandro	Problema físico nos discos do servidor	Monitorar os logs do sistema operacional e do banco de dados	Não há	Criar nova partição em outro local de armazenamento e restaurar backup (se necessário)	1 dia
Indisponibilidade da Rede Lógica (baixa)	Mitigar	Tiago	Problema físico nos ativos de rede	Monitorar os logs dos equipamentos	Substituir o ativo de rede		0 dias

Sistema de autenticação e autorização de usuários – Active Directory (AD)

Sumário do Plano II							
Sistema / Ativo	AD						
Arquitetura	O sistema é composto por três aplicações: 1. AD → Serviço de autenticação e autorização de usuários do TJAP 2. DNS → Sistema de resolução de nomes.						
Localização	Os componentes da arquitetura servidor estão localizados no Data Center do TJAP, em maquinas virtuais, com recursos de HA (Alta Disponibilidade), informações armazenadas no Storage EMC						
Plano de Ação							
Risco e Probabilidade	**Resposta**	**Responsável**	**Tipo de falha**	**Ação Preventiva**	**Ação Contingência**	**Ação Recuperação**	**Tempo estimado até a recuperação**

Falha de Hardware (média)	Mitigar	Leandro e Francisco	Qualquer tipo de problema de hardware (memória, disco, cpu, fonte de energia, etc.)	Monitorar, periodicamente, logs dos servidores em busca de mensagens de erro relacionadas a hardware.	**Para processos judiciais novos:** tramitar fisicamente. Ao final da recuperação, importá-los no sistema. **Processos em andamento**: Necessário realizar recuperação.	1 – Restaurar backup da VM nas máquina secundária ou terciária 2 - Realizar restauração do backup do sistema	1 dia
Vírus (baixa)	Mitigar	Leandro e Francisco	Vírus que impactem no funcionamento do sistema	Manter maquinas atualizadas			
Ataque de Crackers	Mitigar	Francisco e Leandro	Ataques que impactem no funcionamento do sistema				
Ataques Internos (funcionários insatisfeitos s)	Mitigar	Leandro e Francisco	Ataques que impactem no funcionamento do sistema	Melhorar controle de acesso a maquinas.			
Falta de Energia	Mitigar	DAA	Falta de energia para os servidores do Datacenter	Adquirir novos nobreaks com banco de baterias. Estabilização de energia.	Ativar gerador de energia	Desativar gerador e ativar energia através da rede comum.	N/A
Umidade / Vazamento (baixa)	Mitigar	DAA	Umidade ou Vazamento	Verificar, periodicamente, condições físicas do Data Center	N/A	Realizar obras e adaptações necessárias para solucionar o problema	n/A
Incêndio	Mitigar	DAA	Incêndio no Data Center	Monitorar temperatura do Data Center	Não há	Usar as mesmas instruções relatadas para o risco "falha de hardware" dessa tabela.	3 dias
Intempéries (baixa)	Aceitar	DAA, Marco Craveiro	Qualquer problema da natureza que impacte no funcionamento **completo** do Data Center TJAP.	Criar sala segura	Não há		

Indisponibilidade do AD (baixa)	Mitigar	Francisco e Leandro	Problema físico nos discos do servidor	Monitorar os logs do sistema operacional e do banco de dados	Não há	Entregar VM para novo host físico.	1 dia
Indisponibilidade da Rede Lógica (baixa)	Mitigar	Tiago	Problema físico nos ativos de rede	Monitorar os logs dos equipamentos	Substituir o ativo de rede		0 dias

Sistema de Gestão de Recursos Humanos (folha de pagamento) – SGRH

Sumário do Plano III	
Sistema / Ativo	SGRH / Folha de pagamento
Arquitetura	O sistema é composto por três aplicações: 1. SGRH → Aplicação usada pelos usuários cadastro de pessoas e gestões sobre a folha; 2. BD_PGSQL → Banco de dados
Localização	Os componentes da arquitetura servidor estão localizados no Data Center do TJAP, em maquinas físicas, com recursos de HA (Alta Disponibilidade), informações armazenadas no Storage EMC - Aplicação cliente instalados nas máquinas cliente.

Plano de Ação							
Risco e Probabilidade	**Resposta**	**Responsável**	**Tipo de falha**	**Ação Preventiva**	**Ação Contingência**	**Ação Recuperação**	**Tempo estimado até a recuperação**
Falha de Hardware dos servidores (média)	Mitigar	Diogo, Leandro e Francisco	Qualquer tipo de problema de hardware (memória, disco, cpu, fonte de energia, etc.)	Monitorar, periodicamente, logs dos servidores em busca de mensagens de erro relacionadas a hardware.	**Para alterações:** Aguardar o final da recuperação, importá-los no sistema.	1 – Restaurar o serviço nas máquina secundária ou terciária 2 - Realizar restauração do banco de dados, conforme instruções do anexo III desse documento, caso seja necessária restauração completa.	1 dia
Vírus em estações ou servidores (baixa)	Mitigar	Dimicro	Vírus que impactem no funcionamento do sistema	Manter maquinas atualizadas			
Ataque de Crackers	Mitigar	Francisco, Diogo e Leandro	Ataques que impactem no funcionamento do sistema				
Ataques	Mitigar	Marco Craveiro,	Ataques que impactem no	Melhorar controle de			

Internos (funcionários insatisfeitos s)		Jonas, Francisco e Leandro e Diogo	funcionamento do sistema	acesso a aplicação, base de dados. Política de BKP			
Falta de Energia	Mitigar	DAA DITEL	Falta de energia para os servidores do Datacenter	Adquirir novos nobreaks com banco de baterias. Estabilização de energia.	Ativar gerador de energia	Desativar gerador e ativar energia através da rede comum.	N/A
Umidade / Vazamento (baixa)	Mitigar	DAA DITEL	Umidade ou Vazamento	Verificar, periodicamente, condições físicas do Data Center	N/A	Realizar obras e adaptações necessárias para solucionar o problema	n/A
Incêndio	Mitigar	DAA DITEL	Incêndio no Data Center	Monitorar temperatura do Data Center	Não há	Usar as mesmas instruções relatadas para o risco "falha de hardware" dessa tabela.	3 dias
Intempéries (baixa)	Aceitar	DAA DITEL	Qualquer problema da natureza que impacte no funcionamento **completo** do Data Center TJAP.	Criar sala segura	Não há		
Indisponibilidade do BD e STORAGE (baixa)	Mitigar	Diogo e Leandro	Problema físico nos discos do servidor	Monitorar os logs do sistema operacional e do banco de dados	Não há	Criar nova partição em outro local de armazenamento e restaurar backup (se necessário)	1 dia
Indisponibilidade da Rede Lógica (baixa)	Mitigar	Tiago Jonas	Problema físico nos ativos de rede	Monitorar os logs dos equipamentos	Substituir o ativo de rede		0 dias

Além dos riscos acima, foram identificados **riscos genéricos** que podem acontecer e impactar negativamente no processo de continuidade dos serviços de TI. São eles:

Baixa de capacitação e conscientização da equipe

Problema: Para que um plano de recuperação seja realizado adequadamente é preciso que os envolvidos estejam capacitados e conscientizados para esta atividade. Regras, responsabilidade, níveis de serviço mínimos, procedimentos, tudo deve ser do conhecimento de todos. Ignorar esta necessidade provavelmente causará uma desordem no momento do desastre, agravando a situação.

Solução: Apresentar esse plano para os responsáveis e capacitação dos servidores neste tema.

Falta de testes rotineiros para a recuperação

Problema: A DEINTEL não possui documentado procedimentos responsáveis pela recuperação dos sistemas em caso de pane. E não há processo definido para realização de testes desses roteiros.

Solução: Realizar, trimestralmente, escrita e testes de plano.

Baixo controle de mudanças

Problema: Ainda não há processo formal de gestão de mudanças no DEINTEL. Isso pode, algumas vezes, invalidar o plano de continuidade dos serviços de TI, caso esses não sejam atualizados quando necessário.

Solução: Definir processo de gestão de mudanças Falta de alinhamento entre TI e alta direção

Problema: Por falta de alinhamento entre a STI e alta direção, é possível que a STI tome decisões de criar estruturas de recuperação desalinhadas com necessidades da organização.

Solução: Solicitar ao Comitê de Gestão Estratégica realizar a análise de impacto desse plano.

5.4. Prazos, divulgação e atualização do plano

Premissa	Recomendação
Período de atualização do plano	Anualmente
Período para realização dos testes	Semestralmente
Publicação	Site de Intranet
Período de Divulgação	Anualmente
Responsáveis pelo plano	Comitê gestor de TI obs.: o ideal é que esse documento seja elaborado e monitorado pelo Comitê de Gestor de TI do TJAP.
Revisão	Semestralmente

6. ANEXO I - TUCUJURIS

PLANO DE RECUPERAÇÃO DE DESASTRES PARA A BASE DE DADOS DO TRIBUNAL DE JUSTIÇA DO AMAPÁ: TUCUJURIS - DBSGJ.

1 OBJETIVO

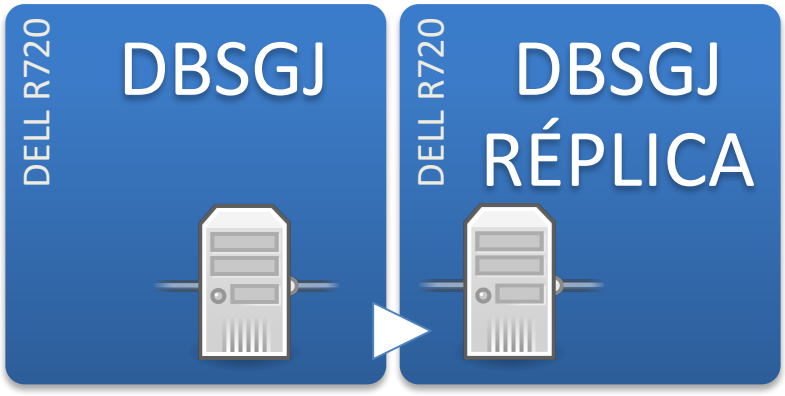
O objetivo deste plano é assegurar a continuidade das operações do TJAP na eventualidade de uma indisponibilidade prolongada dos equipamentos (*hardware*) e informações (base de dados) que dão suporte aos sistemas eletrônicos de gestão judiciária e administrativa. Servidores e *storage.*

2 NETWORK

A insfraestrutura de rede, ou seja, o sistema cabeado e os equipamentos que são responsáveis por prover comunicação entre os usuários e a base de dados, é componente essencial para o funcionamento satisfatório do sistema de processo judicial eletrônico. Por isso, faz-se necessário um trabalho conjunto entre o Departamento de Sistemas - DESIS e o Departamento de Informática e Telecomunicações – DEINTEL, na execução dos planos que necessitam manobras na infraestrutura de comunicação.

3 INFORMAÇÕES SOBRE HARDWARE

Os equipamentos que compõem a infraestrutura de *hardware* são padronizados, ou seja, possuem a mesma configuração variando apenas a quantidade discos rígidos. Esse fato tem como ponto positivo alcançarmos a mesma performance em caso de substituição do equipamento principal em produção pela sua respectiva réplica. Por outro lado, se o *hardware* disponível for inferior, o desempenho diminui podendo gerar lentidão no sistema.



Sobre a performance, em caso de perda dos equipamentos DELL R720 que compõem a infraestrutura de *hardware*, considerando a relevância dos sistemas judiciários para o negócio fim do TJAP e a queda de performance no caso de utilizar um *hardware* inferior para recuperação de desastre, é possível utilizar – caso esteja operacional – o equipamento DELL R720 que opera como réplica da base administrativa DBGERAL.

3.1 CONFIGURAÇÃO

Os Sistemas Judiciários, possuem dois servidores DELL R720 com as seguintes características:

- **Descrição**: Máquina (física) de produção dos sistemas judiciários do TJAP.

- **Banco de dados**: PostgreSQL 9.5.2 on x86_64-pc-linux-gnu, compiled by gcc (GCC) 4.8.2 20140120 (Red Hat 4.8.2-16), 64-bit
- **Instância**: dbgeral
- **Sistema Operacional**: Red Hat Enterprise Linux Server release 7.0 (Maipo)
- **Memória RAM**: 130 GB
- **Processador**: Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz (32 processadores
- Informações de 19/08/2017.

4 CENÁRIOS

4.1 CENÁRIO A – INDISPONIBILIDADE DO HARDWARE

Indisponibilidade do equipamento (*hardware*) que hospeda o SGBD PostgreSQL. Neste caso apenas o hardware primário foi comprometido. A base de dados permanece protegida no *storage* EMC.

- PLANO A: Promover a réplica localizada no *data center* para servidor primário.
  - **Tempo estimado**: 01 hora;
  - **Responsável**: DESIS;
  - **Procedimento**: desligar completamente o hardware danificado, alterar o endereço IP da réplica localizada no data center, para o de produção e por fim configurar o PostgreSQL para modo produção.
- PLANO B: Promover a réplica localizada no no *site-backup* Fórum da Comarca de Macapá.
  - **Tempo estimado**: 6-12 horas;
  - **Responsável**: DESIS e DEINTEL;
  - **Procedimento DESIS**: desligar completamente o hardware danificado, alterar o endereço IP da réplica localizada no *site-backup*, para o de produção e por fim configurar o PostgreSQL para modo produção.
  - **Procedimento DEINTEL**: fornecer conectividade sem que seja necessário trocar o endereço IP de produção.

4.2 CENÁRIO B - INDISPONIBILIDADE DO HARDWARE E DA BASE DE DADOS

Indisponibilidade do equipamento (*hardware*) que hospeda o SGBD PostgreSQL. Neste caso tanto o hardware primário foi comprometido, quanto base de dados localizada no *storage* EMC.

- PLANO A: Restaurar um backup usando a técnica *PITR – Point In The Recovery a.k.a.* "alpha+deltas".
  - **Tempo estimado**: 32-48 horas;
  - **Responsável**: DESIS e DEINTEL;
  - **Procedimento DESIS**: consultar o manual de procedimentos para *backup/restore do PostgreSQL*. Instalar o sistema operacional conforme manual.
  - **Procedimento DEINTEL**: providenciar o hardware onde a cópia de segurança será restaurada.
- PLANO B: Promover a réplica localizada no *site-backup* Fórum da Comarca de Macapá.
  - **Tempo estimado**: 6-12 horas;
  - **Responsável**: DESIS e DEINTEL;
  - **Procedimento DESIS**: desligar completamente o hardware danificado, alterar o endereço IP da réplica localizada no *site-backup*. para o de produção e por fim configurar o PostgreSQL para modo produção.

- **Procedimento DEINTEL**: fornecer conectividade sem que seja necessário trocar o endereço IP de produção.

- PLANO C: Fazer um procedimento de *backup/restore* no servidor réplica localizado no *site-backup* Fórum da Comarca de Macapá.
  - **Tempo estimado**: 5 dias;
  - **Responsável**: DESIS e DEINTEL;
  - **Procedimento DESIS**: Consultar manual de *backup/restore do PostgreSQL*. Realizar uma análise na base de dados para determinar o último *backup* válido e informar a data da cópia de segurança e/ou possível perda de dados. Instalar o sistema operacional conforme manual. conforme manual.
  - **Procedimento DEINTEL**: providenciar o hardware onde a cópia de segurança será restaurada.
- PLANO D: Fazer um procedimento de *backup/restore* no servidor de testes.
  - **Tempo estimado**: 5 dias;
  - **Responsável**: DESIS e DEINTEL;
  - **Procedimento DESIS**: Consultar manual de *backup/restore do PostgreSQL*. Realizar uma análise na base de dados para determinar o último *backup* válido e informar a data da cópia de segurança e/ou possível perda de dados. Instalar o sistema operacional conforme manual.
  - **Procedimento DEINTEL**: providenciar o hardware onde a cópia de segurança será restaurada.

5 CONSIDERAÇÕES FINAIS

O tempo estimado para a recuperação pode variar nos casos onde é necessário alterar local onde a base de dados está armazenada. O desvio o tráfego de rede para o Fórum da Comarca de Macapá é uma operação fundamental para a execução dos planos que envolvem usar o *site-backup*.

Os planos apresentados neste documento, contemplam apenas e recuperação da base de dados. Outros componentes imprescindíveis da solução como, por exemplo, servidores de aplicação e serviços não fazem parte do escopo.

6 GLOSSÁRIO

Hardware: equipamento de informática.

Network: Insfraestrutura de comunicação.

Storage: armazenamento.

Data center: centro de dados, onde dados e equipamentos estão localizados.

RAM: *Random Access Memory,* memória de acesso aleatório.

Storage EMC: equipamento de armazenamento de dados.

Site-backup: local com de armazenamento de dados geograficamente distinto do principal.

Backup: cópia de segurança

Restore: procedimento de recuperação de informações.

IP: Internet Protocol, protocolo de internet.

PITR – Point In Time Recovery: recuperação de informações baseado em linha do tempo.

PostgreSQL: sistema gerenciador de banco de dados objeto relacional de código aberto.

Pg_restore: procedimento de recuperação de uma cópia de segurança.

Pg_dump: procedimento de produção de uma cópia de segurança.

SGBD: sistema gerenciador de banco de dados

A.k.a: also know as, vulgo.

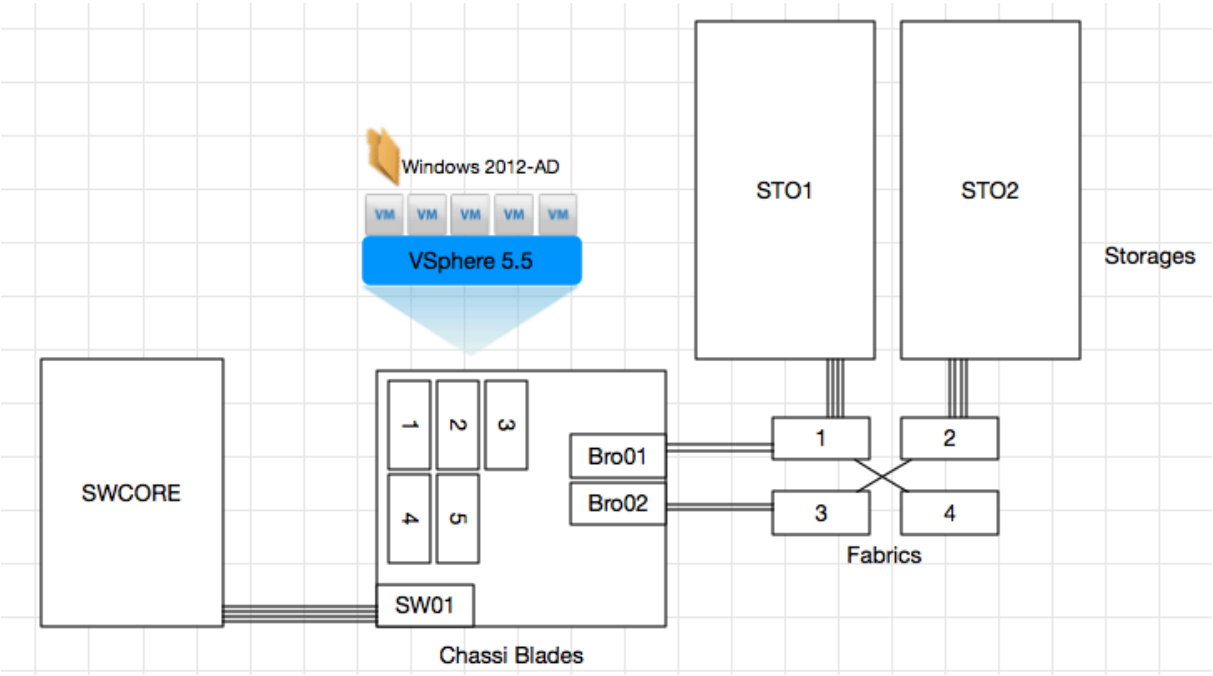
Dbgeral: base de dados administrativa.

Dbsgj: base de dados do Tucujuris.

7. ANEXO II – ACTIVE DIRECTORY

7.1. Arquitetura

O Sistema está instalado em ambiente virtualizado, baseado no software VMWARE que instalado nos servidores BLADE HP e armazenado nos Storage EMC 1 e 2, porém com estrutura de backup dos arquivos da VM armazenados no STORAGES HITACHI e geridos pelo software Netbackup.



7.2. Processos de recuperação

7.2.1. Recuperação do serviço nos casos de indisponibilidade parcial

Entende-se por indisponibilidade parcial, a paralização ou mal funcionamento de serviços do sistema, onde o Sistema Operacional continua em funcionamento, porém algum aspecto do sistema está indisponível.

Os processos de recuperação neste caso, deve priorizar a identificação do problema, com a devida documentação do mesmo, assim como os processos utilizados para recuperação. De forma que seja possível a construção de uma base de conhecimento para problemas comuns.

O prazo máximo para os processos recuperação do ambiente, sem que seja restaurado o backup da VM deverá ser de 4 horas.

Ultrapassando o período estipulado, deverão ser adotadas as medidas de recuperação do ambiente através da restauração do backup da VM.

7.2.2. Recuperação do serviço nos casos de indisponibilidade total da VM

Nos casos de indisponibilidade total do servidor Windows, deverão ser adotados procedimentos de recuperação do backup da VMWARE para a versão mais antiga em funcionamento.

7.2.3. Recuperação do serviço nos casos de indisponibilidade total de HARDWARE

Nos casos onde os problemas de indisponibilidade forem causados por problemas de hardware em algum dos elementos da estrutura, os procedimentos atuais de recuperação, por falta de redundância de equipamentos na estrutura do TJAP, dependem do conserto ou substituição do elemento defeituoso.

7.2.4. Processos de recuperação de backup da VMWARE no Netbackup

Nos casos onde o mal funcionamento esteja no arquivo da VM ou o período de aceitabilidade para recuperação de erros estiver expirado, será necessário realizar os procedimentos de restauração completa da VM no ambiente de backup. Procedimentos, disponíveis no caderno: ANEXOII-PROCEDIMENTOS-RESTORE_BACKUP-VM.

8. ANEXO III – SGRH-FOLHA

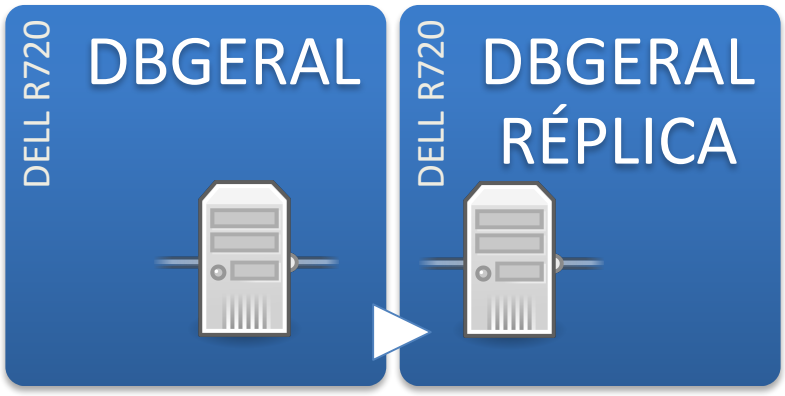
PLANO DE RECUPERAÇÃO DE DESASTRES PARA A BASE DE DADOS DO TRIBUNAL DE JUSTIÇA DO AMAPÁ: ADMINISTRATIVA - DBGERAL.

7 OBJETIVO

O objetivo deste plano é assegurar a continuidade das operações do TJAP na eventualidade de uma indisponibilidade prolongada dos equipamentos (*hardware*) e informações (base de dados) que dão suporte aos sistemas eletrônicos de gestão judiciária e administrativa. Servidores e *storage.*

8 INFORMAÇÕES SOBRE HARDWARE

Os equipamentos que compõem a infraestrutura de hardware são padronizados, ou seja, possuem a mesma configuração variando apenas a quantidade discos rígidos. Esse fato tem como ponto positivo alcançarmos a mesma performance em caso de substituição do equipamento principal em produção, por outro lado, se o *hardware* disponível for inferior, o desempenho diminui podendo gerar lentidão no sistema.



8.1 CONFIGURAÇÃO

Os Sistemas Administrativos, possuem dois servidores DELL R720 com as seguintes características:

- **Descrição**: Máquina (física) de produção dos sistemas judiciários do TJAP.
- **Banco de dados**: PostgreSQL 9.5.2 on x86_64-pc-linux-gnu, compiled by gcc (GCC) 4.8.2 20140120 (Red Hat 4.8.2-16), 64-bit
- **Instância**: dbgeral
- **Sistema Operacional**: Red Hat Enterprise Linux Server release 7.0 (Maipo)
- **Memória RAM**: 130 GB
- **Processador**: Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz (32 processadores
- Informações de 19/08/2017.

Até a data de 21/08/17, a base de dados dbgeral não possui réplica no *site-backup* localizado no Fórum da Comarca de Macapá.

9 CENÁRIOS

9.1 CENÁRIO A – INDISPONIBLIDADE DO HARDWARE

Indisponibilidade do equipamento (*hardware*) que hospeda o SGBD PostgreSQL. Neste caso apenas o hardware primário foi comprometido. A base de dados permanece protegida no *storage* EMC.

- PLANO A: Promover a réplica localizada no data center para servidor primário.
  - **Tempo estimado**: 01 hora;
  - **Responsável**: DESIS;
  - **Procedimento**: desligar completamente o hardware danificado, alterar o endereço IP da réplica localizada no data center para o de produção e por fim configurar o PostgreSQL para modo produção.
- PLANO B: Hospedar o SGBD PostgreSQL em outro equipamento.
  - **Responsável**: DESIS e DEINTEL;
  - **Procedimento DESIS**: Consultar manual de instalação *do PostgreSQL*. Instalar o sistema operacional conforme manual e SGBD no equipamento provisório.
  - **Procedimento DEINTEL**: providenciar o hardware ou máquina virtual.

9.2 CENÁRIO B – INDISPONIBLIDADE DO HARDWARE E DA BASE DE DADOS

Indisponibilidade do equipamento (*hardware*) que hospeda O SGBD PostgreSQL. Neste caso tanto o hardware primário foi comprometido, quanto base de dados localizada no *storage* EMC.

- PLANO A: Restaurar um backup usando a técnica *PITR – Point In The Recovery a.k.a.* "alpha+deltas".
  - **Tempo estimado**: 12-24 horas;
  - **Responsável**: DESIS e DEINTEL;
  - **Procedimento DESIS**: consultar o manual de procedimentos para *backup/restore do PostgreSQL*. Instalar o sistema operacional conforme manual.
  - **Procedimento DEINTEL**: providenciar o hardware onde a cópia de segurança será restaurada.
- PLANO B: Restaurar um cópia de segurança usando a técnica *pg_restore*.
  - **Tempo estimado**: 3 horas;
  - **Responsável**: DESIS e DEINTEL;
  - **Procedimento DESIS**: consultar o manual de procedimentos para *backup/restore do PostgreSQL.* Instalar o sistema operacional conforme manual.
  - **Procedimento DEINTEL**: providenciar o hardware onde a cópia de segurança será restaurada.
  - O procedimento de *backup pg_dump* é realizado diariamente na base de produção dos sistemas administrativos. Possível cópia de segurança mais recente: dia anterior as 19:30:00.

10 CONSIDERAÇÕES FINAIS

É recomendável a instalação de um sistema de réplica no *site-backup,* com isso, teremos mais opções/planos para a recuperação do serviço.

A base de dados do sistema E-cidade, não faz parte do escopo deste documento.

11 GLOSSÁRIO

Hardware: equipamento de informática.

Storage: armazenamento.

Data center: centro de dados, onde dados e equipamentos estão localizados.

RAM: *Random Access Memory,* memória de acesso aleatório.

Storage EMC: equipamento de armazenamento de dados.

Site-backup: local com de armazenamento de dados geograficamente distinto do principal.

Backup: cópia de segurança

Restore: procedimento de recuperação de informações.

IP: Internet Protocol, protocolo de internet.

PITR – Point In Time Recovery: recuperação de informações baseado em linha do tempo.

PostgreSQL: sistema gerenciador de banco de dados objeto relacional de código aberto.

Pg_restore: procedimento de recuperação de uma cópia de segurança.

Pg_dump: procedimento de produção de uma cópia de segurança.

SGBD: sistema gerenciador de banco de dados

A.k.a: also know as, vulgo.