TRIBUNAL DE CONTAS DO
ESTADO DE GOIÁS

Diretoria de Tecnologia da Informação (DI-TI)

Serviço de Infraestrutura e Segurança em TI (Serv-Infra TI)

Plano de Continuidade de TI

Versão nº: 001

07/10/2024

SUMÁRIO

1. OBJETIVO

O objetivo deste documento é apresentar a estratégia adotada no desenvolvimento da infraestrutura necessária para a continuidade do negócio, de forma a preservar a alta disponibilidade e as condições para uma rápida restauração do ambiente de trabalho em caso de interrupção dos serviços desenvolvidos pelo TCE-GO.

Uma vez que falhas nos serviços de TI impactam diretamente a continuidade da gestão e fiscalização de contas do Estado de Goiás, almeja-se ainda, com este plano, prover medidas de proteção rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais em casos de incidentes ou desastres de segurança da informação.

2. SERVIÇOS ESSENCIAIS

São os seguintes serviços considerados essenciais, por ordem de priorização, para o acionamento e execução deste plano:

SERVIÇO	CRITICIDADE	RPO	RTO	IMPACTO			
				FINANCEIRO	LEGAL	IMAGEM	OPERACIONAL
eTCE-GO	Alta	Backup mais recente	4 dias	Indefinido	Alto	Alto	Alto
TCE-DOCS	Alta	Backup mais recente	4 dias	Indefinido	Alto	Alto	Alto
Active Directory	Alta	Backup mais recente	1 dia	Indefinido	Baixo	Alto	Alto
Banco de Dados Oracle	Alta	Backup mais recente	1 dia	Indefinido	Alto	Alto	Alto

Legenda:
RPO: ponto em uma linha de tempo em que os dados devem ser recuperados após a ocorrência de uma ruptura.
RTO: período de tempo dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção.

3. PRINCIPAIS AMEAÇAS

Este plano deve ser acionado quando da ocorrência de cenários de incidentes/desastres que apresentem risco à continuidade dos serviços essenciais. As principais ameaças aqui mencionadas estão descritas na Planilha de Gestão de Ativos, cujo detalhamento de informações estão dispostos no PO Gerir Ativos de Tecnologia da Informação.

TIPOS DE AMEAÇAS	AMEAÇAS	POSSÍVEL CAUSA
Dano Físico	Fogo	1. Incêndios que comprometam os serviços de TIC;
	Água	

	Poluição	2. Alteração de Temperaturas; 3. Curto-circuito; 4. Ausência de manutenção.
	Acidente grave	
	Destruição de equipamento	
	Poeira, corrosão e/ou congelamento	
Eventos Naturais	Fenômeno Climático	1. Terremotos; 2. Tempestades; 3. Altas temperaturas; 4. Alagamentos e etc.
	Inundação	
Paralisação de Serviços Essenciais	Falha do ar condicionado ou do sistema de suprimento de água	1. Filtros entupidos; 2. Fiação e equipamento de telecomunicações sem manutenção; 3. Rompimento de cabos de interconexão decorrente da execução de obras públicas; 4. Desastres ou acidentes; 5. Dutos do ar condicionado congelados.
	Interrupção do suprimento de energia	
	Falha do equipamento de telecomunicação	
Comprometimento da Informação	Interceptação de sinais de interferência comprometedores	1. Falha que necessite reposição de peça ou reparo, cujo reparo ou aquisição dependa de processo licitatório; 2. Falha no controle de acessos físicos e virtuais; 3. Ausência de sanitização de dispositivos móveis; 4. Falha na aplicação de políticas de segurança da informação; 5. Ataque aos ativos do DataCenter.
	Espionagem à distância	
	Escuta não autorizada	
	Furto de mídia ou documentos	
	Furto de equipamentos	
	Recuperação de mídia reciclada ou descartada	
	Divulgação indevida	
	Dados de fontes não confiáveis	
	Alteração do hardware	
	Alteração do software	
	Determinação da localização	
Falhas Técnicas	Falha de equipamento	1. Ausência de manutenção de equipamentos; 2. Má gestão de documentação; 3. Falha no cumprimento das políticas de segurança da informação.
	Defeito de equipamento	
	Saturação do sistema de informação	
	Defeito de software	
	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	
Ações não autorizadas	Uso não autorizado de equipamento	1. Downloads indevidos; 2. Falta de cumprimento da LGPD; 3. Ausência de antivírus; 4. Falha no cumprimento das políticas de segurança da informação.
	Cópia ilegal de software	
	Uso de cópias de software falsificadas ou ilegais	
	Comprometimento dos dados	
	Processamento ilegal de dados	
Comprometimento	Erro durante o uso	

de Funções	Abuso de direitos	1. Falta de treinamento de integração de sistemas; 2. Falha no cumprimento das políticas de segurança da informação; 3. Falha no controle de acesso físico e virtual.
	Forjamento de direitos	
	Repúdio de ações	
	Indisponibilidade de recursos humanos	
Seres Humanos	Invasão de sistemas por meio de Hacker	1. Falha no cumprimento das políticas de segurança da informação; 2. Falha no controle de acesso físico e virtual. 3. Invasão de Sistemas, infiltrações e entradas não autorizadas
	Criminoso Digital	
	Terroristas	
	Servidores	

4. PAPÉIS E RESPONSABILIDADES

4.1. Comitê de Segurança da Informação (CSI)

Avaliar o plano periodicamente e decidir pelo seu acionamento quando da ocorrência de incidentes/desastres de segurança da informação, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.

4.2. DPO

Responsável por todas as comunicações durante um incidente/desastre de segurança da informação.

4.3. Serviço de Infraestrutura e Segurança em TI

Responsável pelas instalações físicas que abrigam sistemas de TI e pela garantia que as instalações de alternativa são mantidas adequadamente. Responsável também por avaliar os danos e supervisionar os reparos, compreendendo ainda qualquer infraestrutura de rede, incluindo WAN, LAN ou de infraestrutura externa junto aos prestadores de serviço.

Fornecer a infraestrutura de servidores físicos e virtuais necessária para que a TI execute suas operações e processos essenciais durante um desastre.

Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre. Responsável por assegurar e validar o desempenho das aplicações essenciais e pode auxiliar outras equipes de TI e o Comitê de Segurança da Informação conforme necessário.

Fornecer aos colaboradores as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível. Sendo responsável por provisionar todos os colaboradores do TCE-GO na solução de contingência com as ferramentas específicas à sua atuação.

4.4. Serviço de Sistemas de Informação

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.

Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança da informação.

4.5. Telefones e e-mails úteis em caso de emergência

Local	Contato
Presidência	Ramal 2826
Serviço de Manutenção Predial e Paisagismo	Ramal 2508
Diretoria de TI	Ramal 2865
Serviço de Segurança e Qualidade de Vida	Ramal 2884
Assessoria Militar	Ramal 2866
SAMU	192
Corpo de Bombeiros	193
Equatorial	0800 062 0198
Saneago	0800 645 0116
SEMMA	3524-1408
CIPA	cipa@tce.go.gov.br
Brigada	brigada@tce.go.gov.br
CSIRT (*Computer Security Incident Response Team*)	csirt@tce.go.gov.br

5. INVOCAÇÃO DO PLANO

Este plano 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 Segurança da Informação em conjunto com a alta administração do TCE-GO.

5.1. Elaborar cronograma de recuperação

O presidente do Comitê de Segurança da Informação (CSI), após o mapeamento das perdas e impactos, elabora um breve cronograma de recuperação das aplicações levando em consideração:

- A priorização dos serviços essenciais, ou determinação de nível institucional.
- O RTO definido para cada serviço essencial.
- A força de trabalho disponível.

5.2. Substituição de ativos e equipamentos

Em caso de perda de ativos, esta situação deve ser imediatamente informada ao CSI, para avaliação da necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe de Infraestrutura e Segurança irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço, comunicando ao CSI se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição.

A equipe de Infraestrutura e Segurança deve verificar, dentre os ativos que foram danificados, quais estão cobertos por garantia e se poderá ser acionada através dos fornecedores.

5.3. Reconfiguração de ativos e equipamento

A equipe de Infraestrutura e Segurança deve verificar se as configurações dos ativos reparados ou substituídos estão em pleno funcionamento. Caso não estejam, devem prover um cronograma estimado para configurar esses ativos, comunicando o CSI e o DPO.

5.4. Teste de ambiente

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

Os testes incluem:

- Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre;
- Recuperar dados do backup;
    - Proceder a recuperação dos dados para as aplicações, seja do storage ou fitas de backup (vide Anexo I – Manual para Restauração de Backup).
- Validar as configurações e funcionalidades dos sistemas;
    - A validação pode ser realizada pelos testes automatizados de monitoramento dos serviços.
    - Por pessoal designado pela equipe de configuração dos sistemas (SERV-SISTEMAS).

Os testes de recuperação, em ambiente controlado, dos sistemas listados neste plano, serão executados anualmente para validação e possível atualização do próprio plano ou do roteiro de recuperação.

6. ESTRATÉGIAS DE CONTINUIDADE

O TCE-GO busca assegurar a continuidade dos negócios adotando a abordagem descrita nos tópicos seguintes.

6.1. Políticas Internas

Estrutura que contempla políticas, normas, procedimentos, papéis e responsabilidades visando a implementação de uma gestão de continuidade de negócios efetiva na organização.

O TCE-GO possui toda documentação vinculada a diretrizes e normas de segurança da informação registradas em seu Manual de Segurança da Informação e implantadas por meio de comunicações e treinamentos específicos.

6.2. Identificação dos Processos Críticos e Análise de Impacto nos Negócios

A Gestão de Incidentes de Segurança é o processo da continuidade de negócios que identifica e mensura uma eventual interrupção operacional e possibilita a determinação das prioridades de recuperação, dos tempos de retomada e das necessidades mínimas de recursos e equipes. A documentação de procedimentos e informações desenvolvida, consolidada e mantida de forma que esteja disponível para utilização em eventuais interrupções, possibilitando a retomada de atividades críticas do TCE-GO em prazos e condições aceitáveis.

6.3. Ambiente Tecnológico Alternativo

A infraestrutura de TI que suporta as operações do TCE-GO está instalada atualmente em área estratégica dentro do prédio administrativo, contendo todo aparato para gestão de incidentes/desastres.

A seguir, listamos algumas características da arquitetura implantada.

6.3.1. Energia

O TCE-GO possui usina fotovoltaica para geração de energia elétrica e tendo como fonte de energia secundária um gerador instalado. Cada datacenter (externo e interno) possui um conjunto UPS independente, o edifício-sede tem três nobreaks de grande porte para a rede elétrica dos computadores, responsáveis por estabilizar a tensão e suportar a operação do TCE-GO em uma eventual falta de energia até que a fonte de energia secundária esteja ativada.

6.3.2. Redundância na Infraestrutura

A fim de garantir alta disponibilidade no funcionamento de seus equipamentos, a arquitetura concebida prevê redundância em diversos níveis:

- Redundância de fonte: serviços são suportados com equipamentos que em sua maioria possuem mais de uma fonte (não estando entre esses os switches);
- Disco rígido: serviços são suportados com equipamentos que possuem redundância de discos (RAID) ou replicação em nós nos casos de clusters.
- Redundância de equipamentos: serviços são suportados por equipamentos idênticos instalados em paralelo de forma a garantir que não haja paralisação dos negócios. Exceção é o servidor de arquivos, que possui seus arquivos em storage.
- Contingência no servidor de arquivos: pode-se subir outra máquina e apontar os discos para essa outra máquina, uma vez que todas as unidades compartilhadas na rede ficam no storage.

- Contingência no firewall: atualmente existem dois equipamentos configurados para alta disponibilidade (HA ativo-passivo), porém em situação de desastre pode-se fazer reconfiguração da rede para funcionar sem o equipamento de firewall físico, substituindo por appliance virtual ou por solução open source baseada em software até que o equipamento seja ajustado.
- Rede Corporativa: A comunicação entre os escritórios e o Datacenter é suportada por conexões redundantes em cada uma das pontas. Cada conexão é capaz de suportar toda a comunicação do escritório ou Datacenter.
- Internet: O TCE-GO possui redundância de links de internet, configurados para operação simultânea e balanceada (SD-WAN). Possui também acordo de nível de serviço com disponibilidade mínima mensal de 94,7%, com previsão de penalidades em caso de descumprimentos.

7. ENCERRAMENTO DO PCN

Ao término do procedimento de recuperação, as informações são consolidadas em parecer específico, informando o horário de restabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

Deve-se ainda compor relatório com relação das atividades necessárias após a ocorrência de desastres como remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido, respectivas configurações de proxy, dns, rotas, vlans etc, conforme determinado em PO Gerir Incidentes de Segurança da Informação.

Considerando que uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter, o Comitê de Segurança da Informação em conjunto com o DPO realizarão o contato com as partes descritas neste plano provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

8. ANEXOS

Anexo I – Manual para Restauração de Backup

9. ELABORAÇÃO, REVISÃO E APROVAÇÃO

Plano de Continuidade de TI		
Diretoria de Tecnologia da Informação - DI-TI		
Responsável por	***Nome***	***Função***
Elaboração	Leandro dos Santos	Chefe do Serviço de Infraestrutura e Segurança em TI
Revisão/Aprovação	Licardino Siqueira	Diretor de TI
Controle de Qualidade	Fabrício Borges dos Santos	Chefe do Serviço de Gestão da Melhoria Contínua
Datas das Versões do PO		
Versão anterior: n. 000 de 23/11/2023	Versão atual: n. 001 de 07/10/2024	Próxima revisão programada: 07/10/2027