PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO TRT7.GP Nº 225, DE 9 DE OUTUBRO DE 2024

Estabelece o Processo de Gestão da Continuidade dos Serviços Essenciais de Tecnologia da Informação e Comunicação (PGC-TIC) no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT-7).

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça (CNJ), que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça (CNJ), que aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

CONSIDERANDO a Resolução Normativa TRT7 nº 5, de 3 de março de 2023, que estabelece a nova Política de Segurança da Informação e Comunicação no âmbito do TRT-7;

CONSIDERANDO a Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021 do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

CONSIDERANDO o Acórdão 2201-66.2022.5.90.0000 do Conselho Superior da Justiça do Trabalho, que determina ao TRT-7 que "defina formalmente, aprove e implante programa de gestão da continuidade dos serviços essenciais de TI";

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Estabelecer o Processo de Gestão da Continuidade dos Serviços Essenciais de Tecnologia da Informação e Comunicação (PGC-TIC) no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT-7).

CAPÍTULO II
DOS OBJETIVOS

Art. 2º São objetivos do PGC-TIC:

I - aumentar o nível de resiliência dos serviços e dos sistemas de TIC, contribuindo para continuidade do negócio;

II - reduzir o risco e minimizar o impacto de interrupções dos serviços e dos sistemas de TIC que suportam as atividades críticas do TRT-7;

III - elaborar planos de continuidade de TIC, com vistas a documentar os procedimentos necessários à operação em nível de contingência e comunicações necessárias, bem como ao retorno à normalidade, quando da ocorrência de interrupções dos serviços e dos sistemas de TIC;

IV - fornecer subsídios para o correto direcionamento e dimensionamento de recursos humanos, tecnológicos e financeiros, visando prover a gestão da continuidade de TIC;

V - estabelecer os papéis e as responsabilidades para a execução do processo.

CAPÍTULO III
DAS DIRETRIZES

Art. 3º O PGC-TIC deverá considerar:

I - o resultado das análises de riscos de TIC;

II - a Política de Cópia de Segurança do Tribunal;

III - a capacidade de TIC instalada e planejada, de acordo com o Processo de Gerenciamento de Capacidade e Disponibilidade de TIC.

Art. 4º O PGC-TIC deverá garantir:

I - a realização de análises de impacto de negócio, com a definição dos serviços essenciais de TIC, tolerância à perda de dados e metas de prazo para disponibilizar o serviço em caso de incidentes no ambiente de produção, a fim de nortear as estratégias de continuidade;

II - as avaliações anuais pela Secretaria de Tecnologia da Informação e Comunicação (SETIC), e, sempre que necessário, a implementação de medidas visando à melhoria contínua do PGC-TIC;

III - a construção de Planos de Continuidade de TIC para os serviços essenciais de TIC;

IV - a realização de testes e de revisões periódicas dos Planos de Continuidade de TIC, de forma a garantir sua efetividade.

CAPÍTULO IV
DO PROCESSO DE GESTÃO DA CONTINUIDADE DOS SERVIÇOS ESSENCIAIS DE TIC (PGC-TIC)

Art. 5º O PGC-TIC, estabelecido na forma do Anexo Único, descreve as atividades, o fluxo de trabalho, os documentos a serem produzidos, as áreas envolvidas e as respectivas responsabilidades no processo.

Art. 6º A SETIC poderá alterar o PGC-TIC sem a necessidade de expedição de novo ato, garantido o versionamento e a gestão documental, quando cumulativamente:

I - não implicar em aumento de despesas, de qualquer natureza;

II - não incluir, remover ou alterar competências atribuídas às unidades ou aos colegiados externos à SETIC;

III - manter o processo alinhado aos objetivos e às diretrizes estabelecidas neste ato.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 7º Estabelecer o prazo de 120 (cento e vinte) dias para a Secretaria de Tecnologia da Informação e Comunicação implantar o Processo de Gestão da Continuidade dos Serviços Essenciais de TIC.

Art. 8º Revogar o Ato TRT7.GP nº 2, de 3 de janeiro de 2017.

Art. 9º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 9 de outubro de 2024.
DURVAL CÉSAR DE VASCONCELOS MAIA
Presidente do Tribunal

ANEXO ÚNICO

Processo de Gestão da Continuidade dos Serviços Essenciais de Tecnologia da Informação e Comunicação (PGC-TIC)

Responsável pelo processo
Coordenadoria de Segurança da Informação (CSI)

Papéis e responsabilidades

Papéis	**Responsabilidades**
Presidência	Aprovar os planos de continuidade propostos pela SETIC. Principal interessada nas atividades-fim críticas do TRT-7.
Comitê de Segurança da Informação e Proteção de Dados	Analisar a documentação de continuidade de TIC produzida pela SETIC, bem como e manifestar-se sobre essa documentação, apoiando a Presidência na avaliação do processo.
Subcomitê de Gestão de Tecnologia da Informação e Comunicação	Validar a lista de atividades críticas, validar os planos elaborados pelas áreas da SETIC e auxiliar na definição dos testes a serem realizados.
	Avaliar as proposições e os documentos encaminhados pela CSI.
	Encaminhar as proposições às instâncias superiores, para avaliação e aprovação. Quando necessário, retornar à CSI, indicando pontos de melhorias a serem realizados.
	Elaborar e atualizar modelos de documentos utilizados na gestão da continuidade de TIC.

Coordenadoria de Segurança da Informação (CSI)	Assessorar o Comitê de Segurança da Informação e Proteção de Dados e a SETIC na análise e na tomada de decisões a respeito de situações decorrentes de desastres de segurança da informação.
	Gerenciar o Processo de Gestão da Continuidade dos Serviços Essenciais de TIC e manter a documentação relacionada atualizada.
Outras áreas da SETIC	Preencher e revisar os Planos de Continuidade e de Recuperação de Desastres. Executar os testes e documentar os resultados.

Indicador de processo

Descrição	Método de apuração / fórmula de cálculo	Frequência
Percentual de planos testados no último biênio	Percentual de planos de gestão de continuidade Plano de Continuidade Operacional (PCOs) e Plano de Recuperação de Desastres (PRDs) testados ao longo dos últimos dois anos, pelo total de planos previstos para testes.	Anual

Controle de execução

Controle	Método de execução	Frequência
Auditoria	Realizar uma reunião com as equipes executoras do processo para avaliar a aderência, os benefícios gerados e as oportunidades de melhoria do processo. Essa avaliação deve identificar se o processo necessita de revisão.	Anual

Termos e definições

Termo	Descrição

Atividades Críticas	Atividades que devem ser executadas de forma a garantir a consecução dos produtos e dos serviços fundamentais da organização, atingindo os objetivos mais importantes e sensíveis ao tempo.
Análise de Impacto nos Negócios (AIN)	Estimativa dos impactos resultantes da interrupção de atividades e de cenários de desastres que possam afetar a prestação jurisdicional do Tribunal, bem como técnicas para quantificar e qualificar tais impactos. Define também a criticidade dos processos de negócio, prioridades, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.
Desastre	Incidente que tenha causado algum dano grave, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo superior ao aceito pela organização.
Estratégia de Continuidade	Abordagem do órgão que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior.
Continuidade de Negócios	Capacidade estratégica e tática de uma organização de se planejar e responder a incidentes e interrupções dos negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.
Gestão da Continuidade	Processo abrangente de gestão que identifica as ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso tais ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e as atividades de valor agregado.
Plano de Continuidade	Nome dado à documentação que abrange os procedimentos referentes à continuidade dos serviços de TIC. É composta pelo Plano de Continuidade Operacional (PCO) e pelo Plano de Recuperação de Desastres (PRD).
Plano de Continuidade Operacional (PCO)	Documento que descreve os procedimentos operacionais e técnicos a serem realizados frente a determinados cenários de falha, para a manutenção dos serviços, ainda que em um nível mínimo de operação.
Plano de Recuperação de Desastres (PRD)	Documento que descreve os procedimentos técnicos, focado em ativos e serviços tecnológicos, a serem realizados frente a determinados cenários de falhas dos principais serviços de TIC, visando ao retorno à normalidade.
Resiliência	Poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

RPO (*Recovery Point Objective*)	Tempo máximo suportado de perda de dados de um determinado serviço ou processo de negócio após a ocorrência de um desastre.
RTO (*Recovery Time Objective*)	Tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre.

Descrição das tarefas

Analisar o impacto de eventos adversos nos processos de negócio		
Descrição	Identificar os processos de negócios sensíveis ao tempo de indisponibilidade e os requisitos para recuperá-los em um prazo aceitável para o TRT-7, de acordo com o nível de criticidade de cada um. Para tal, são identificados os eventos potenciais e os prováveis impactos sobre o Tribunal, os processos afetados e os critérios que serão usados para quantificar e qualificar tais impactos.	
Considerações importantes	Esta atividade corresponde, basicamente, à realização de uma Análise de Impacto nos Negócios (AIN), também comumente conhecida como BIA (Business Analisys Impact), e utiliza também os dados provenientes de análises de riscos realizadas anteriormente. É importante que representantes do negócio contribuam para identificação dos impactos e prazos aceitáveis, definindo o RPO e o RTO.	
Papéis	Coordenadoria de Segurança da Informação, Subcomitê de Gestão de Tecnologia da Informação e Comunicação, Presidência.	
Entradas	Análise de riscos realizadas.	
Saídas	Relatório de Análise de Impacto.	
	Realizar análise de impacto no negócio	De acordo com o nível do risco envolvido, deve-se avaliar qual o impacto (financeiro, operacional, imagem, etc) causado pelo evento negativo ao serviço.
	Determinar prazos	Estabelecer os prazos de RTO e RPO para cada serviço crítico analisado com base no valor do impacto obtido.

Atividades	**Documentar resultados**	Elaborar relatório com os serviços críticos, seus prazos de recuperação e recursos mínimos necessários para recuperação de funções essenciais do serviço.
	Encaminhar relatório	Encaminhar relatório para avaliação do Subcomitê de Gestão de Tecnologia da Informação e Comunicação.
	Adequar relatório	Caso o Subcomitê de Gestão de Tecnologia da Informação e Comunicação não esteja de acordo com os dados contidos no relatório, refazer a análise.

Definir estratégias de continuidade de TIC		
Descrição	Identificar, com base nas avaliações realizadas na atividade anterior, as estratégias de continuidade e de recuperação disponíveis para os serviços de TIC mais críticos. Tais estratégias norteiam as tarefas e os procedimentos a serem executados na ocorrência de um desastre (ou até mesmo antes) e a identificação dos recursos humanos, tecnológicos, financeiros, etc necessários para sua implementação.	
Considerações Importantes	Nesta fase, avaliam-se quais as possíveis ações a adotar para implementar a gestão da continuidade de TIC, levando em conta a viabilidade de adoção da solução técnica.	
Papéis	Coordenadoria de Segurança da Informação, Subcomitê de Gestão de Tecnologia da Informação e Comunicação e outras áreas da SETIC.	
Entradas	Relatório de análise de impacto (serviços críticos).	
Saídas	Estratégia de continuidade de TIC para os serviços críticos.	
Atividades	**Definir estratégia de continuidade de TIC**	Para cada serviço crítico, avaliar as possíveis ações para manter o serviço a um nível minimamente operável, de acordo com os prazos estabelecidos nas fases anteriores, a quantidade de recursos necessária, etc.

Identificar necessidade de revisão dos planos		
Descrição	Identificar a necessidade de revisão dos planos ou circunstâncias que ensejem a alteração dos documentos que compõem o Plano de Continuidade.	
Considerações Importantes	Elencar quais planos deverão ser revisados, quais descontinuados, etc. Para a revisão do ciclo que se inicia, deverão ser consideradas as oportunidades de melhorias identificadas no ciclo anterior.	
Papéis	Coordenadoria de Segurança da Informação.	
Entradas	Planos já existentes em sua última versão, solicitações de mudanças, oportunidades de melhorias identificadas no ciclo anterior.	
Saídas	Identificação dos fatores que ensejam a revisão.	
Atividades	**Identificar a necessidade de revisão dos planos.**	Os PCO´s e PRD´s devem ser revisados no mínimo uma vez por ano.
	Identificar circunstâncias que ensejem a alteração dos documentos que compõem o Plano de Continuidade.	A necessidade de alteração dos documentos pode decorrerem razão: • de alterações na infraestrutura de TIC, tais como substituição, instalação, modernização ou remoção de equipamentos e softwares; • de mudanças em procedimentos operacionais; • dos resultados dos testes dos planos; • da ocorrências de eventos que evidenciem falhas nos documentos.

Solicitar a elaboração/revisão dos Planos	
Descrição	Disponibilizar os modelos de PCO e PRD ou suas últimas versões às áreas da SETIC responsáveis pela administração do serviço/atividade crítica ou por coletar as informações necessárias ao seu preenchimento.
Papéis	Coordenadoria de Segurança da Informação.
	Relatório de serviços críticos ou identificação da necessidade de criação ou de revisão dos Planos.

Entradas		
Saídas	Comunicação às áreas envolvidas sobre a necessidade de elaboração/revisão de documentos.	
Atividades	**Disponibilizar os documentos**	Procedimento operacional realizado pela CSI para disponibilizar uma nova cópia do modelo do plano em questão.
	Avisar área e combinar um prazo de entrega	Avisar a área responsável pelo preenchimento do documento e negociar uma data para entrega do documento.
Templates	Plano de Continuidade Operacional e Plano de Recuperação de Desastres.	

Elaborar/revisar PCO's		
Descrição	Elaboração de proposta de Plano de Continuidade Operacional com o objetivo de elencar as atividades e os procedimentos necessários para garantir a operacionalidade da atividade/serviço a um nível mínimo aceitável frente aos cenários de falhas descritos.	
Considerações Importantes	A área responsável preenche os planos, elencando as atividades necessárias para a manutenção de um mínimo de operacionalidade do serviço/atividade. São definidos/revisados os procedimentos, atividades e os(as) responsáveis pela execução das atividades.	
Papéis	Outras áreas da SETIC, Coordenadoria de Segurança da Informação.	
Entradas	Modelos dos Planos.	
Saídas	Plano de Continuidade Operacional.	
Atividades	**Coleta de informações**	A área responsável coleta as informações para identificar os principais cenários de falha e a forma de atuação em cada cenário de falha identificado.

	Preenchimento dos planos	A área preenche os planos, descrevendo os procedimentos a serem executados para cada cenário de falha levantado.
Templates	Plano de Continuidade Operacional.	

Elaborar/revisar PRD's		
Descrição	Elaboração de proposta de Plano de Recuperação de Desastres com o intuito de descrever as atividades e os procedimentos necessários para retornar as operações dos serviços críticos à normalidade frente à ocorrência de eventos adversos.	
Considerações Importantes	A área responsável preenche os planos, elencando as atividades necessárias para a manutenção de um mínimo de operacionalidade do serviço/atividade. São definidos/revisados os procedimentos, atividades e os(as) responsáveis pela execução das atividades.	
Papéis	Outras áreas da SETIC, Coordenadoria de Segurança da Informação.	
Entradas	Modelos dos Planos.	
Saídas	Plano de Recuperação de Desastres.	
Atividades	**Coleta de informações**	A área responsável coleta as informações para identificar os principais cenários de falha e a forma de atuação em cada cenário identificado.
	Preenchimento dos planos	A área preenche os planos, descrevendo os procedimentos a serem executados para cada cenário de falha levantado.
Templates	Plano de Recuperação de Desastres.	

Validar planos

Descrição	A CSI recebe os planos elaborados/revisados (PCO's e PRD's) pelas áreas técnicas com o intuito de validá-los em relação ao formato, à estrutura do documento e aos demais itens. Estando de acordo, a CSI compila as informações referentes à elaboração e/ou à revisão dos planos para encaminhamento ao Subcomitê de Gestão de Tecnologia da Informação e Comunicação, para validá-los.	
Considerações Importantes	Se houver necessidade de ajustes, o Subcomitê de Gestão de Tecnologia da Informação e Comunicação deve retornar suas observações à CSI, que providenciará perante as equipes técnicas as modificações indicadas e retornará para nova validação. A necessidade ou não de testes dos planos existentes deverá ser definida na avaliação.	
Papéis	Coordenadoria de Segurança da Informação, Subcomitê de Gestão de Tecnologia da Informação e Comunicação.	
Entradas	PCO's e PRD's.	
Saídas	Planos validados.	
Atividades	**Avaliar planos**	A CSI avalia os planos apresentados pelas áreas técnicas.
	Encaminhar para Subcomitê de Gestão de Tecnologia da Informação e Comunicação	Avaliados os planos, a CSI encaminha um compêndio dos planos ao Subcomitê de Gestão de Tecnologia da Informação e Comunicação, para validação.
	Validar plano	O Subcomitê de Gestão de Tecnologia da Informação e Comunicação valida ou não os planos.

Informar os ajustes a serem realizados	
Descrição	Informar à CSI sobre os ajustes e as adequações a serem realizados nos planos, definidos pelo Subcomitê de Gestão de Tecnologia da Informação e Comunicação, pelo Comitê de Segurança da Informação e Proteção de Dados ou pela Presidência.
Papéis	Subcomitê de Gestão de Tecnologia da Informação e Comunicação.

Entradas	Planos elaborados pelas áreas ou definições da Presidência.	
Saídas	Lista de ajustes necessários.	
Atividades	**Repassar lista de ajustes**	Informar à CSI a lista de ajustes identificados.

Encaminhar para manifestação superior		
Descrição	Encaminhar os planos já validados para o Comitê de Segurança da Informação e Proteção de Dados e, após, à Presidência, para aprovação final dos documentos.	
Considerações Importantes	O encaminhamento para manifestação superior (aprovação formal pela Presidência) é necessário nos casos de novo plano ou de alteração significativa nos procedimentos dos planos já existentes. No caso de alterações meramente técnicas ou pequenos ajustes na redação ou no procedimento, não há necessidade de encaminhamento à Presidência, bastando a validação pelo Subcomitê de Gestão de TIC.	
Papéis	Coordenadoria de Segurança da Informação.	
Entradas	PCO's e PRD's.	
Saídas	Informação/parecer do Subcomitê de Gestão de Tecnologia da Informação e Comunicação, acompanhado dos Planos validados.	
Atividades	**Encaminhar documentação**	Encaminhar formalmente os documentos ao Comitê de Segurança da Informação e Proteção de Dados e, após, à Presidência do TRT-7.

Opinar sobre os documentos	
Descrição	O Comitê de Segurança da Informação e Proteção de Dados avalia criticamente a documentação produzida pela SETIC. Após avaliação, manifesta-se, formalmente, dando seu parecer sobre a documentação.
Considerações	Conforme estabelecido na Política de Segurança da Informação, o Comitê de Segurança da Informação e Proteção de Dados assessora a Presidência do TRT-7 em questões relacionadas à

Importantes	matéria.	
Papéis	Comitê de Segurança da Informação e Proteção de Dados.	
Entradas	Documentação encaminhada para aprovação.	
Saídas	Parecer sobre a documentação.	
Atividades	**Avaliar documentação**	O Comitê analisa a documentação encaminhada.
	Encaminhar expediente à Presidência	A manifestação do Comitê de Segurança da Informação e Proteção de Dados deve ser juntada ao expediente, que deve ser encaminhado à Presidência.

Apreciar os documentos e manifestação		
Descrição	De posse da manifestação do Comitê de Segurança da Informação e Proteção de Dados, a Presidência avalia os documentos e decide pela aprovação ou não. Caso não aprove, a Presidência indicará os ajustes necessários.	
Papéis	Presidência.	
Entradas	Manifestação do Comitê de Segurança da Informação e Proteção de Dados acerca dos Planos de Continuidade de TIC.	
Saídas	Aprovação ou reprovação da documentação.	
Atividades	**Analisar manifestação do Comitê e avaliar a documentação**	A Presidência avalia a manifestação do Comitê e analisa criticamente a documentação encaminhada.
	Decisão final	A Presidência dá seguimento ao fluxo, informando a aprovação ou não da documentação, com ciência à SETIC sobre a deliberação.

Gerir documentação		
Descrição	A CSI armazena e registra a versão e atribui as permissões necessárias da documentação aprovada.	
Considerações Importantes	A manutenção de versionamento é importante para manter um registro histórico das atualizações e de seus(suas) responsáveis. O controle de acesso é necessário, pois nem todos os(as) colaboradores(as) podem ter acesso a alguns documentos que possuem informações restritas.	
Papéis	Coordenadoria de Segurança da Informação.	
Entradas	Documentos aprovados.	
Saídas	Documentos em sua versão final, com as permissões atribuídas, com registro do versionamento.	
Atividades	**Armazenar os documentos**	A CSI organiza e armazena os documentos no ambiente de colaboração da SETIC, assegurando a realização de cópias de segurança, em ambiente digital ou físico, externo ao data center principal.
	Atualizar a tabela de versionamento	Preencher a tabela de versionamento, incluindo quem realizou a mudança, quais mudanças foram feitas e quando elas foram realizadas.
	Conceder acesso aos(às) interessados(as)	Revisar documento por documento para conceder o correto permissionamento.

Divulgar documentos	
Descrição	A CSI divulga os documentos aprovados às áreas necessárias, para consulta, quando necessário.
Considerações Importantes	A divulgação é essencial para que as equipes saibam da existência dos documentos, os utilize quando necessário e para que informem à CSI quando for necessário atualizar a documentação.
Papéis	Coordenadoria de Segurança da Informação.

Entradas	Planos versionados.	
Saídas	Planos divulgados.	
Atividades	**Mandar e-mail aos(às) interessados(as)**	A CSI divulga, via e-mail, para o Subcomitê de TIC o local onde os arquivos estão disponíveis, incluindo as cópias de segurança.

Definir cronograma de testes dos planos		
Descrição	Definir com as áreas técnicas quais planos serão testados, bem como as datas em que os testes serão executados.	
Considerações Importantes	Os testes têm como finalidade validar os planos elaborados, executando os procedimentos descritos, analisando se os passos estão corretos, se o tempo de execução está estimado corretamente e se o fluxo de atividades está corretamente ordenado, além de também servirem como entrada para a próxima revisão do plano. Novos planos deverão ser testados.	
Papéis	Coordenadoria de Segurança da Informação.	
Entradas	Planos de Continuidade Operacional e Planos de Recuperação de Desastres.	
Saídas	Testes que serão realizados.	
Atividades	**Definir testes a serem realizados**	Determinar quais cenários de incidentes serão testados. Na definição dos testes deve ser avaliado o impacto nos serviços, isto é, se é aceitável a indisponibilidade, ainda que parcial, para realização dos testes ou se devem ser realizados em um ambiente simulado ou de homologação, de forma a evitar a indisponibilidade).
Templates	Relatório de Testes.	

Executar e documentar testes

Descrição	As equipes técnicas executam os testes planejados, com acompanhamento da CSI. Os testes e os resultados são documentados para fins de análise crítica.	
Considerações Importantes	O teste deve ser executado exatamente conforme descrito nos Planos, de forma a validar sua eficácia. Caso seja detectada a necessidade de alteração dos procedimentos descritos, isso deve ser documentado nos resultados dos testes, para que seja encaminhada para a revisão do respectivo plano.	
Papéis	Outras equipes.	
Entradas	PCO's e PRD's.	
Saídas	Resultado dos testes.	
Atividades	**Executar os testes agendados**	As equipes realizam os testes agendados, seguindo as instruções presentes nos PCO´s e PRD´s.
	Documentar o resultado	A CSI disponibiliza às equipes o template para a documentação do teste e pode auxiliá-las no preenchimento. Toda execução do teste deve ser documentada, em especial sobre a necessidade de correção ou melhoria nos procedimentos ou nos planos, bem como os resultados práticos dos testes, para posterior avaliação.
Templates	Documento de resultado dos testes.	

Avaliar e armazenar os resultados dos testes	
Descrição	Os resultados obtidos nos testes são analisados criticamente para definição das ações necessárias e armazenados na rede e no Google Drive, para servirem como evidências de análise crítica do processo e da documentação.
Considerações Importantes	As evidências podem ser utilizadas para eventuais auditorias realizadas no TRT-7, para demonstrar que os planos são efetivamente testados e validados, além de servirem como entrada para futura revisão dos planos.

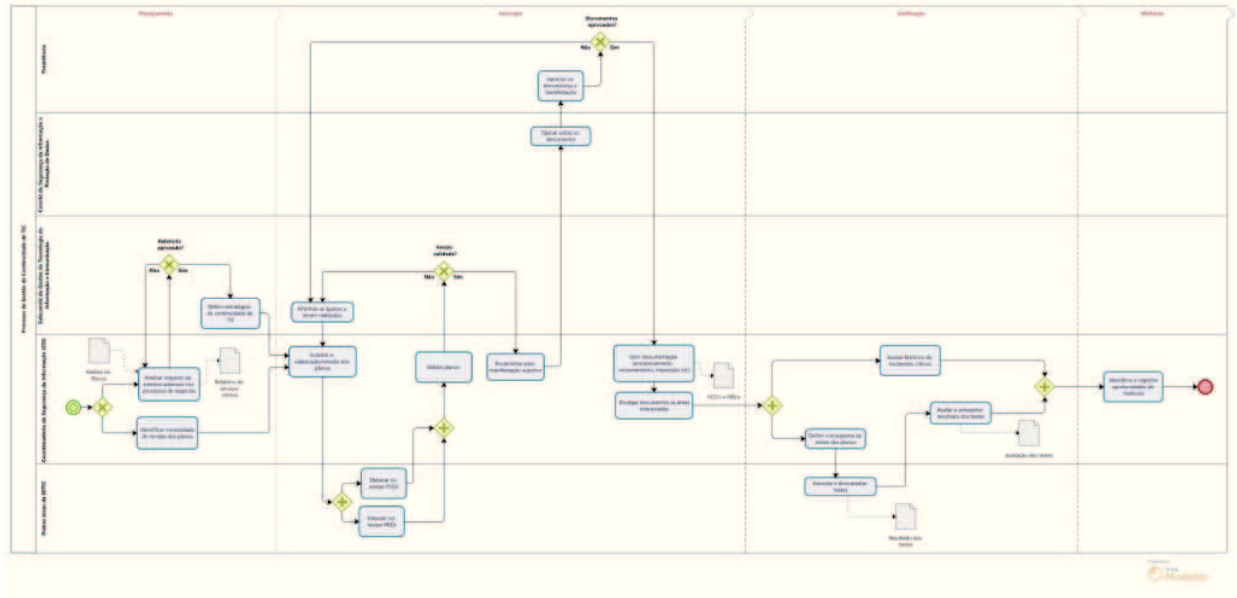
Papéis	Coordenadoria de Segurança da Informação.	
Entradas	Resultado dos testes.	
Saídas	Avaliação dos testes.	
Atividades	**Analisar criticamente os resultados obtidos**	Os resultados dos testes devem ser avaliados para a definição do prosseguimento do fluxo do processo.
	Armazenar documentação dos testes	A CSI armazena na rede e no Google Drive a documentação dos testes realizados.

Avaliar histórico de incidentes críticos		
Descrição	Analisar os incidentes críticos ocorridos (desastres) que ensejaram/ensejariam a utilização do Plano de Gestão da Continuidade dos Serviços Essenciais de TIC.	
Considerações Importantes	O foco da análise é identificar a necessidade de elaboração/revisão dos planos existentes	
Papéis	Coordenadoria de Segurança da Informação.	
Entradas	Relatórios de Incidentes de Segurança da Informação (RISI).	
Saídas	Análise da CSI.	
Atividades	**Avaliar os RISI's do período**	Identificar nos relatórios dos incidentes ocorridos situações que ensejam a revisão dos Planos ou a elaboração de novos, bem como a necessidade de treinamento da equipe envolvida.

Identificar e registrar oportunidades de melhoria	
Descrição	Identificar e registrar oportunidades de melhoria, tanto no que diz respeito ao processo de Gestão da Continuidade, quanto aos documentos em vigor, para serem implementadas no próximo ciclo.

Considerações Importantes	Devem ser analisados os resultados dos testes e da avaliação dos incidentes críticos.	
Papéis	CSI.	
Entradas	Resultados dos testes, análise histórica de incidentes.	
Saídas	Documento com oportunidades de melhoria.	
Atividades	**Identificar oportunidades de melhoria**	A CSI poderá consultar as áreas envolvidas para a elaboração do documento que será submetido à Diretoria da SETIC.

Fluxo do Processo de Gerenciamento de Continuidade de TIC



Fonte: Baseado do fluxo do TRT da 4ª Região.