Secretaria de TIC do TRT24

Processo Gerenciar Continuidade de TIC

HISTÓRICO DO DOCUMENTO

	DATA	DESCRIÇÃO
01	01/08/2013	Mapeamento e desenho do processo
02	10/10/2014	Criação do documento de descrição do processo
03	29/10/2015	Alinhamento com indicadores do Processo Gerenciar Riscos de TIC
04	29/04/2016	Revisão do processo
05	20/09/2016	Alinhamento de atividades e indicadores ao processo COBIT 5.0 - DSS04 (Gerenciar Continuidade)
06	05/06/2017	Revisão da Política, definição do Manual de Execução do PCN e revisão fluxo do processo
07	07/02/2018	Ajuste nos indicadores
08	30/06/2022	Revisão do fluxo das atividades do processo
09	14/02/2024	Revisão do processo

EQUIPE DE DOCUMENTAÇÃO

	Nome	Cargo
01	João Carlos Ferreira Filho	Chefe da Divisão de Governança de TIC
02	Geslaine Perez Maquerte	Chefe da Divisão de Proteção de Dados e Segurança da Informação
03	Fábio Nogueira da Silva	Servidor da Divisão de Proteção de Dados e Segurança da Informação
04	Alex Sandro Pontes da Silva	Chefe do Setor de Apoio a Processos e Iniciativas Nacionais

Sumário

1 Objetivo

Elaborar a Política, a Estratégia e os Planos de gestão de Continuidade de TIC.

2 Abrangência

Tribunal Regional do Trabalho da 24ª Região.

3 Definições

- **Política de Gestão de TIC para a Continuidade de Negócios:** regulamentação do órgão sobre as diretrizes, escopo, responsabilidades e procedimentos relativos à continuidade de negócio.
- **Estratégia de Gestão de Continuidade de TIC**: abordagem de um órgão ou entidade 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;
- **Ferramenta ITSM**: Aplicação utilizada para o gerenciamento de serviços de TIC;
- **Planos de Continuidade de TIC:** conjunto de planos de ações preventivas para garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre até o retorno a situação normal de funcionamento;
- **PROAD:** sistema de processo administrativo eletrônico.

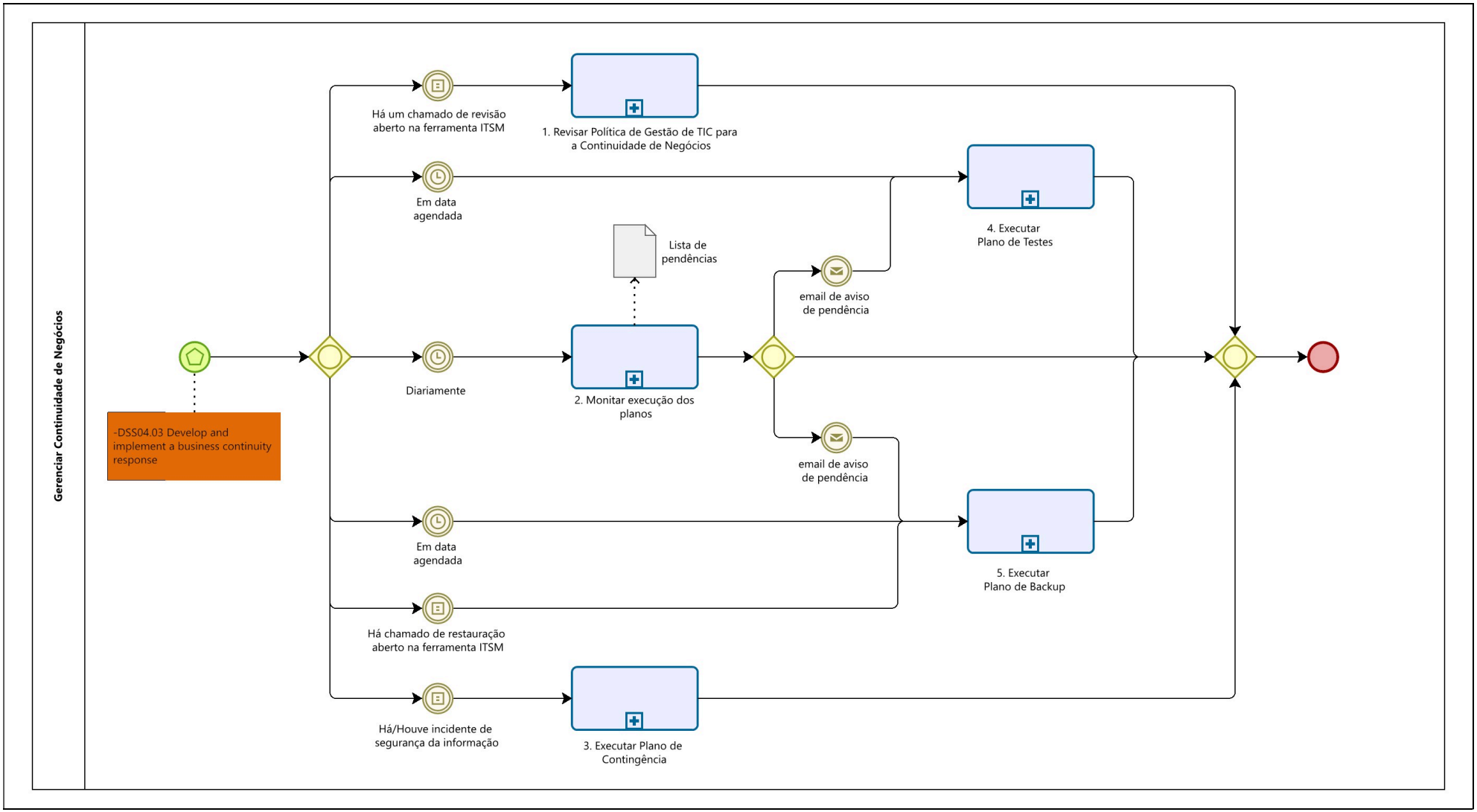
4 Processo Gerenciar Continuidade de TIC

4.1 Papéis e Responsabilidades

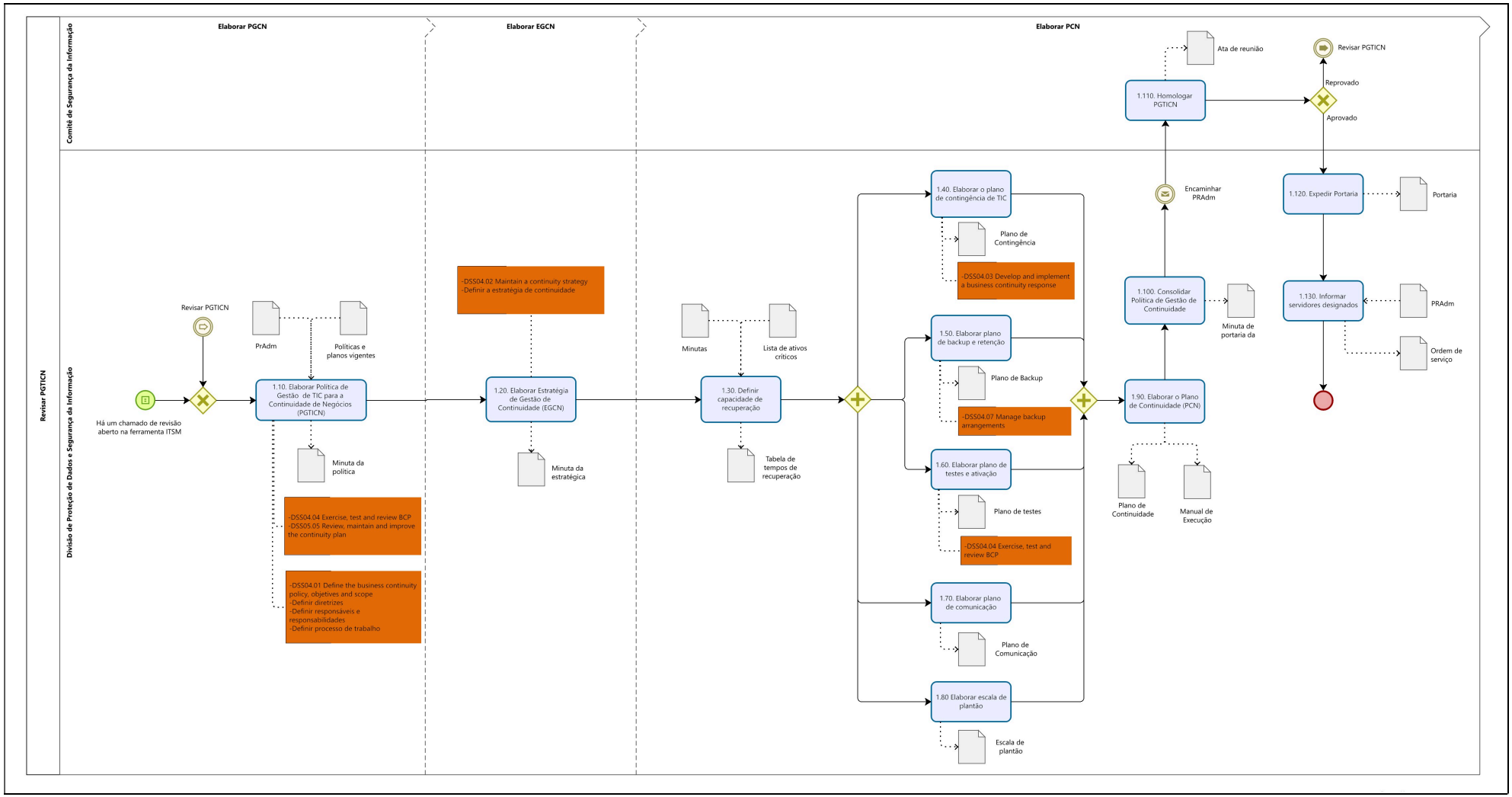
Papel	Responsabilidades	Responsável
Dono do Processo	• Buscar a qualidade e eficiência do processo • Assegurar que todos os envolvidos na execução do processo sejam informados das mudanças e suporte efetuados	Secretário da SETIC
Gerente do Processo	• Buscar a qualidade, eficiência e efetividade do processo • Produzir informações gerenciais (indicadores) • Promover a execução das atividades do processo • Manter o desenho e indicadores do processo atualizados, garantindo que estejam adequados aos propósitos da organização	Chefe da Divisão de Proteção de Dados e Segurança da Informação
Comitê de Segurança da Informação	• Homologar a PGTICN, EGCN e revisões	Magistrado designado
Divisão de Proteção de Dados e Segurança da Informação	• Elaborar a PGTICN, EGCN e PCN • Elaborar o Manual de Execução do PCN • Executar os planos táticos • Promover as revisões necessárias	Chefe da Divisão de Proteção de Dados e Segurança da Informação
Divisão de Infraestrutura de TIC	• Executar e restaurar backups • Executar testes	Servidores integrantes da Divisão de Infraestrutura de TIC
Grupo de Gestão de Crises Cibernéticas	• Avaliar e deliberar a respeito das ações necessárias para o tratamento do incidente a partir das soluções possíveis apresentadas pela ETIR, orientando a ETIR sobre as prioridades estratégicas nas atividades a serem executadas • Gerir ações de comunicação sobre o incidente para a comunidade afetada pelo incidente • Representar oficialmente o Tribunal em contatos externos necessários durante o tratamento de crise • Avaliar e deliberar sobre recursos extraordinários que possam ser necessários para a solução do incidente;	Desembargador Presidente do TRT24
Equipe Técnica Contratada	• Executar atividades do processo externo denominado “Equipe técnica contratada”	Fornecedores de soluções de TIC e empresas contratadas para suporte de soluções e aplicações em nuvem

4.2 Fluxo do Processo

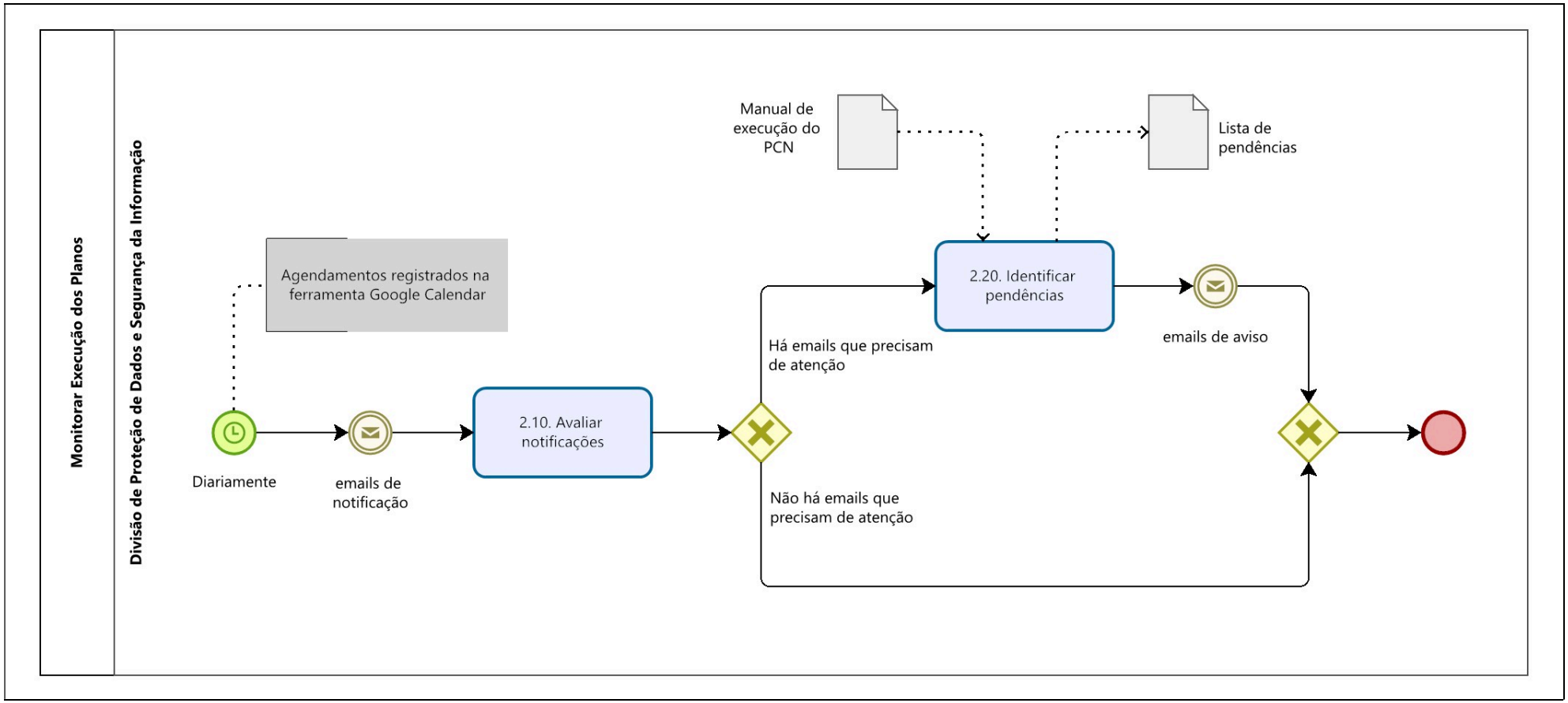
4.2.1 Fluxo Macro



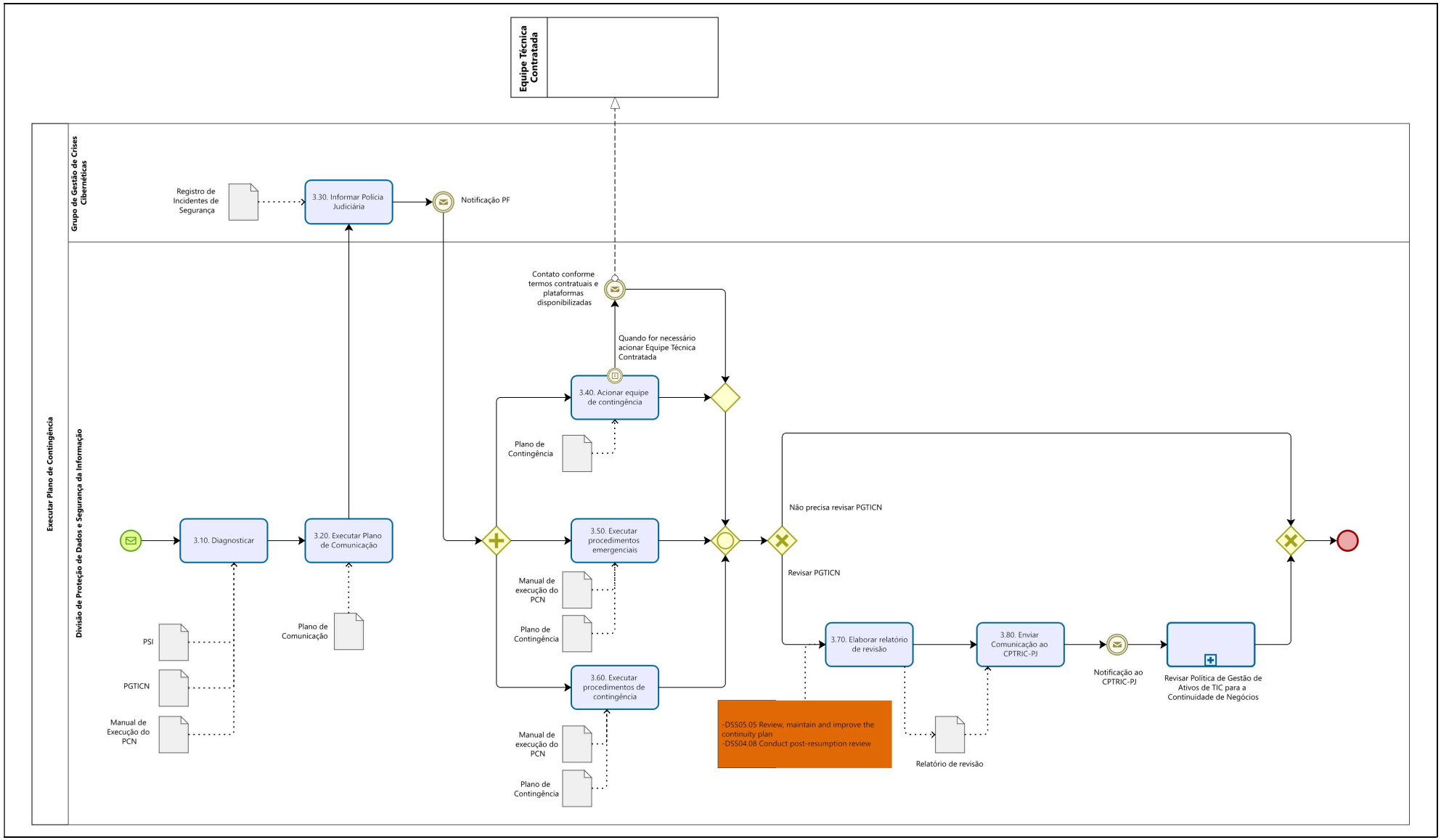
4.2.2 Fluxo Detalhado – Subprocesso Revisar Política de Gestão de TIC para a Continuidade de Negócios



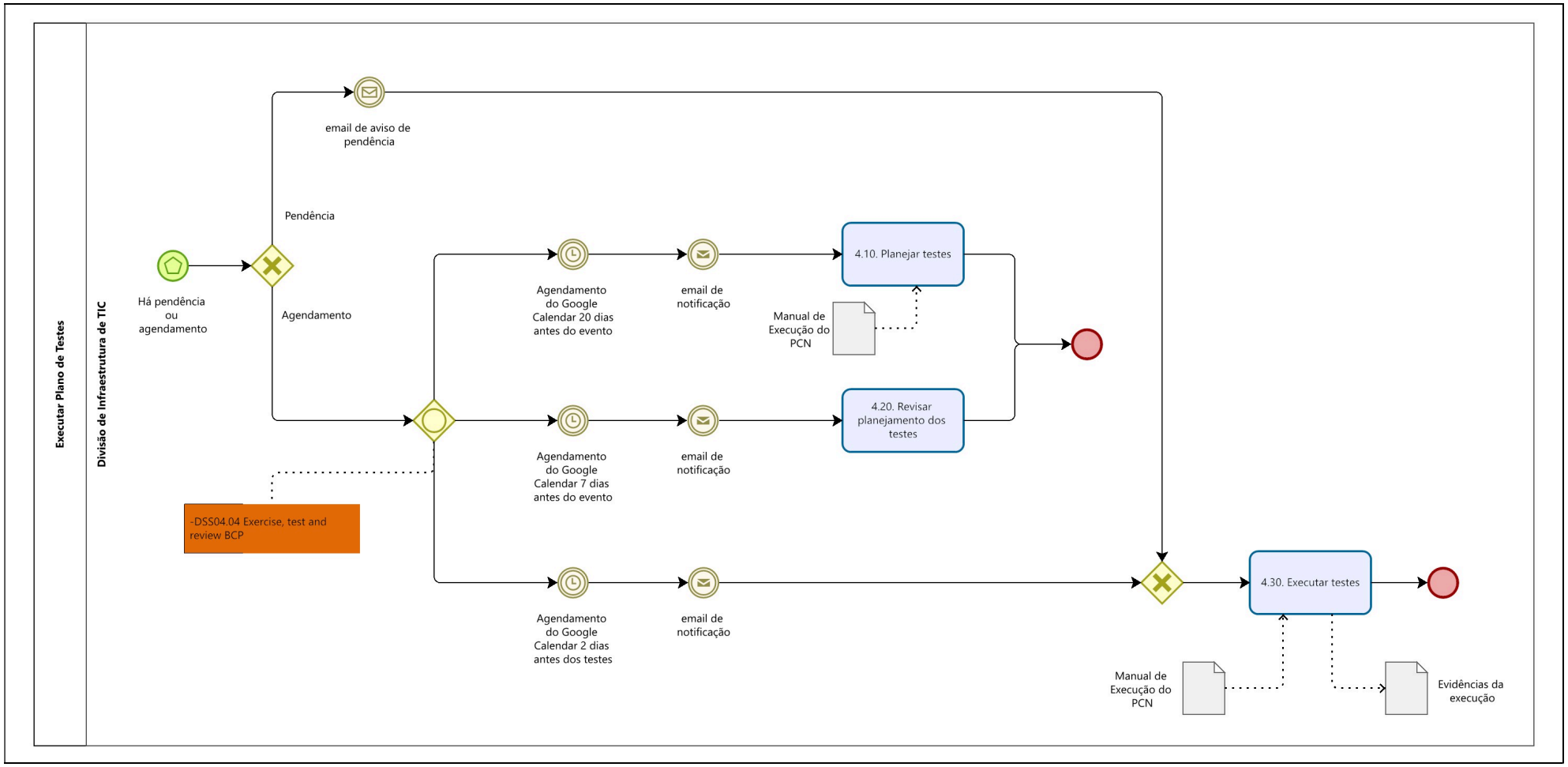
4.2.3 Fluxo Detalhado – Subprocesso Monitorar Planos



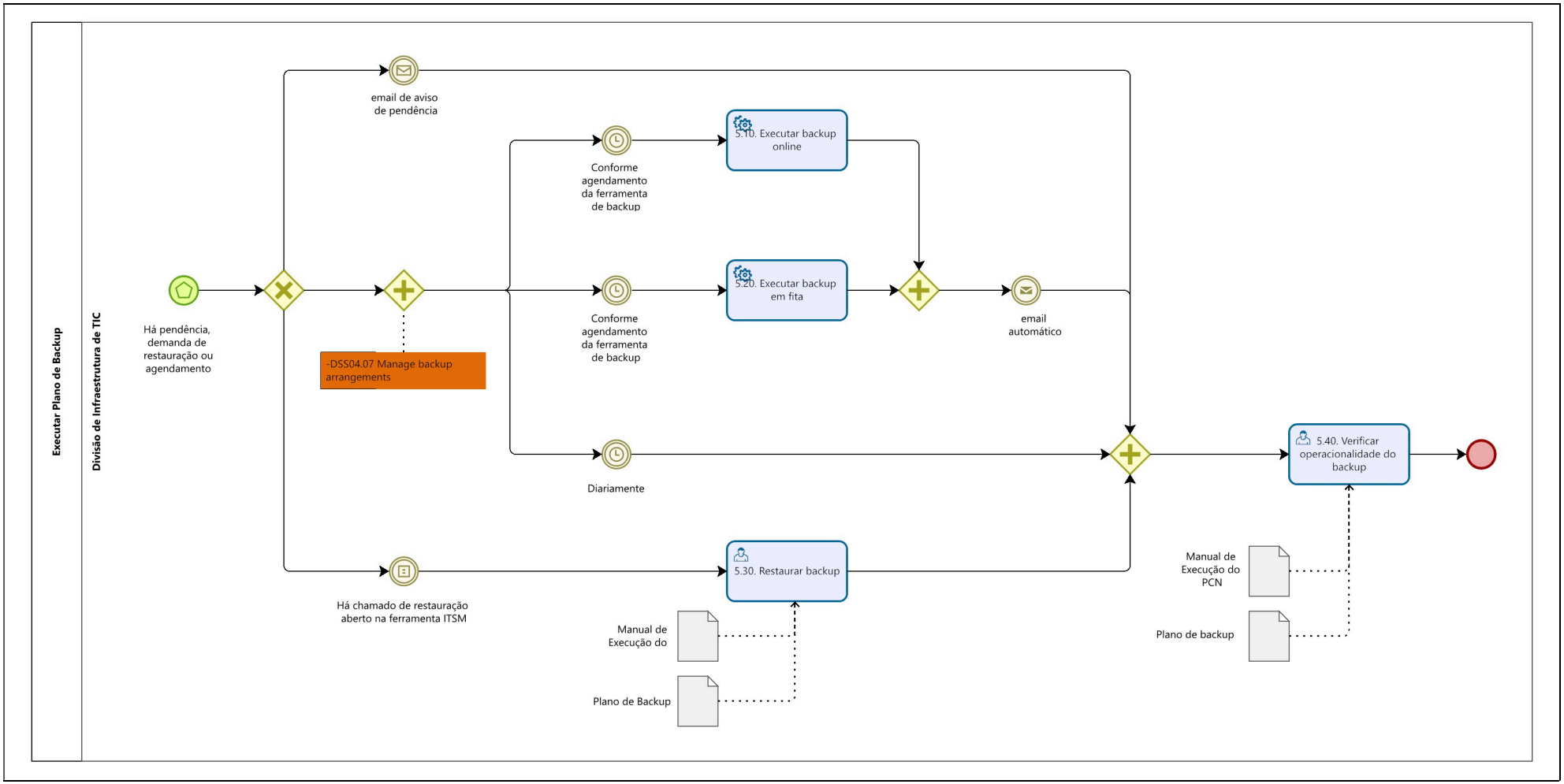
4.2.4 Fluxo Detalhado – Subprocesso Executar Plano de Contingência



4.2.5 Fluxo Detalhado – Subprocesso Executar Plano de Testes



4.2.6 Fluxo Detalhado – Subprocesso Executar Plano de Backup



4.3 Descrição do processo

4.3.1 Descrição do subprocesso Revisar Política de Gestão de TIC para a Continuidade de Negócios

Id	Atividade	Responsável	Descrição
1.10	**Elaborar Política de Gestão de TIC para a Continuidade de Negócios (PGTICN)**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	Entradas: PROAD de acompanhamento do processo de trabalho, políticas e planos em vigência
			Processamento: • Descrever as diretrizes, responsáveis, responsabilidades e processo de trabalho.
			Saídas: minuta da política
1.20	**Elaborar Estratégia de Gestão de Continuidade (EGCN)**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** minuta da política
			Processamento: • Definir em nível macro as diretrizes estratégicas para a Continuidade de TIC; • Definir os fundamentos técnicos (redundância X centralização); • Estabelecer os objetivos para garantia dos dados e da capacidade de processamento; • Estabelecer os requisitos de operação para ativos críticos; • Estabelecer a tolerância para perda de dados, tempo de interrupção ou tempo de indisponibilidade, conforme as características de cada ativo
			Saídas: minuta da estratégia
1.30	**Definir capacidade de recuperação**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** minutas da política e da estratégia e lista de ativos críticos
			Processamento: • Definir os eventuais cenários de recuperação (redundância X fitas de armazenamento); • Definir qual a forma preferencial de recuperação (redundância X fitas de armazenamento); • Definir o tempo de recuperação para cada um dos ativos críticos, em função dos níveis de tolerância.
			Saídas: Tabela de tempos de recuperação dos ativos críticos
1.40	**Elaborar o plano de contingência de TI**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** minutas e tabela de recuperação dos ativos
			Processamento: • Descrever as características técnicas dos ativos críticos (tipo, localização, disponibilidade de backup/reposição, disponibilidade de contratos de apoio, cobertura de garantia e outros); • Definir os procedimentos emergenciais mínimos; • Definir a ordem de prioridade de restauração dos ativos; • Definir requisitos para utilização do site backup.

			Saídas: Plano de Contingência de TI
1.50	**Elaborar o plano de backup e retenção de dados**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** minutas e tabela de recuperação dos ativos
			Processamento: • Definir o escopo dos serviços que terão dados armazenamentos em fitas; • Definir a temporalidade da retenção dos dados; • Definir os componentes de infraestrutura necessários para a execução dos backups; • Definir os procedimentos para execução dos backups; • Definir os procedimentos para armazenamento das fitas de backup; • Definir os critérios para recuperação de dados; • Definir as informações que devem ser produzidas/fornecidas em cada backup. • Definir as responsabilidades pela execução do Plano.
			Saídas: Plano de Backup e Retenção de Dados
1.60	**Elaborar o plano de testes e ativação**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** minutas e tabela de recuperação dos ativos
			Processamento: • Definir o escopo para aplicação dos testes de recuperação • Definir os componentes de infraestrutura necessários para a execução dos testes; • Definir a quantidade ou intervalo de tempo mínimo para execução dos testes; • Definir as informações que devem ser produzidas/fornecidas em cada teste. • Definir os servidores responsáveis pela execução dos testes.
			Saídas: Plano de Testes e Ativação
1.70	**Elaborar plano de comunicação**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** minutas
			Processamento: • Definir o escopo da comunicação (interno X externo); • Definir os meios de comunicação (físico, eletrônico, email, popup, malote digital, outros); • Definir a frequência; • Definir o conteúdo mínimo da comunicação.
			Saídas: Plano de Comunicação da EGCN
1.80	**Elaborar escala de plantão**	Chefe da Divisão de Proteção de Dados e Segurança da	**Entradas**: minutas e planos
			Processamento:

		Informação	• Definir a escala conforme os requisitos e normas administrativas vigentes
			Saídas: escala de plantão
1.90	**Elaborar o Plano de Continuidade de TIC**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** minutas e planos
			Processamento: • Compilar os planos de contingência, de backup, de testes e de comunicação para formar o PCN. • Elaborar o Manual de Execução do PCN contendo o detalhamento técnico para aplicação das atividades previstas no PCN
			Saídas: Plano de Continuidade de TIC e do Manual de Execução
1.100	**Consolidar a Política de Gestão de TIC para a da Continuidade de Negócios**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** minutas e planos
			Processamento: • Consolidar as minutas e planos em documento único no formato de minuta de portaria • Juntar ao PROAD de acompanhamento do processo de trabalho • Despachar para aprovação
			Saídas: PROAD despachado para aprovação
1.110	**Homologar PGTICN**	Comitê de Segurança da Informação	**Entradas**: PROAD
			Processamento: • Deliberar sobre a aprovação • Juntar a ata da reunião ao PROAD
			Saídas: ata de reunião
1.120	**Expedir portaria**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas**: PROAD
			Processamento: • Elaborar a minuta da portaria de regulamentação da PCGN • Juntar minuta ao PROAD • Encaminhar PROAD para expedição da portaria • Publicar a portaria no Portal de Governança
			Saídas: Publicação da portaria
1.130	**Informar servidores designados**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entrada:** PROAD, PGTICN, planos, manuais e processo de trabalho
			Processamento: • Despachar no PROAD Ordem de Serviço informando aos servidores designados e demais

			stakeholders sobre as providências cabíveis e documentos operacionais, tais como: ○ Manual de execução ○ Escala de plantão • Cadastrar todos os stakeholders como coassinantes do despacho de informação
			Saída: despacho de informação com stakeholders cadastrados como coassinantes

4.3.2 Descrição do subprocesso Monitorar Planos

Id	Atividade	Responsável	Descrição
2.10	**Avaliar notificações**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** e-mails recebidos do Google Calendar
			Processamento: • Verificar as informações e selecionar os e-mails que precisam de atenção
			Saídas: e-mails selecionados
2.20	**Identificar pendências**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** e-mails selecionados
			Processamento: • Elaborar os e-mails de aviso de pendência
			Saídas: e-mails de aviso enviados

4.3.3 Descrição do subprocesso Executar Plano de Contingência

Id	Atividade	Responsável	Descrição
3.10	**Diagnosticar**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** informação sobre a ocorrência de um incidente de segurança da informação, PSI, PGTICN e Manual de Execução do PCN
			Processamento: • Avaliar o incidente e definir a ações necessárias para aplicação do Plano de Contingência
			Saídas: ações para aplicação do Plano de Contingência
3.20	**Executar Plano de Comunicação**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** Plano de Comunicação e diagnóstico do incidente
			Processamento: • Executar os procedimentos previstos no Plano de Comunicação
			Saídas: informações para os stakeholders
3.30	**Informar Polícia Judiciária**	Grupo de Gestão de Crises Cibernéticas	**Entradas:** Registro de Incidente de Segurança
			Processamento: • O integrante estratégico do GGCC, representante da Presidência do Tribunal, deve notificar a PF (responsável pelo papel de Polícia Judiciária) sobre o incidente cibernético, para que a instituição dê as adequadas instruções para liberação das atividades. Essa informação é notadamente obrigatória quando há indícios de crime cibernético.
			Saídas: informações para os stakeholders
3.40	**Acionar equipe de contingência**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** Plano de Contingência
			Processamento: • Contatar e Convocar para trabalho os membros da equipe de contingência, definida no Plano de Contingência da PGTICN, para atuar na execução dos procedimentos de contingência • Quando a execução dos procedimentos de contingência envolver fornecedores de soluções de TIC e empresas contratadas para suporte de soluções e aplicações em nuvem, acionar a Equipe Técnica Contratada nos termos contratuais e plataformas disponibilizadas, podendo haver acionamento direto pelos integrantes da ETIR com os contatos disponibilizados pelos contratados
			Saídas: membros da equipe de contingência convocados para trabalho
3.50	**Executar procedimentos emergenciais**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** Plano de Contingência e Manual de Execução do PCN
			Processamento: • Executar os procedimentos previstos no plano de Contingência e descritos no Manual de Execução do PCN

			Saídas: procedimentos de emergência executados
3.60	**Executar procedimentos de contingência**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** Plano de Contingência e Manual de Execução do PCN
			Processamento: • Executar os procedimentos previstos no plano de Contingência e descritos no Manual de Execução do PCN
			Saídas: procedimentos de emergência executados
3.70	**Elaborar relatório de revisão**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** resultados das execuções dos planos
			Processamento: • Avaliar se a execução dos planos táticos está alinhada ou aderente a PGTICN • Determinar a eficácia da PGTICN e dos planos, recursos de continuidade, papéis e responsabilidades, habilidades e competências, a resiliência do incidente, infraestrutura técnica, estruturas organizacionais e relacionamentos entre os envolvidos • Identificar os pontos fracos ou omissões na PGTICN e nos planos e fazer recomendações para melhorias, observando: a) A identificação e análise da causa-raiz do incidente; b) A linha do tempo das ações realizadas; c) A escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise; d) Os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas; e) O escalonamento da crise; f) A investigação e preservação de evidências; g) A efetividade das ações de contenção; h) A coordenação da crise, liderança das equipes e gerenciamento de informações; e i) A tomada de decisão e as estratégias de recuperação.
			Saídas: relatório de revisão
3.80	**Enviar Comunicação ao CPTRIC-PJ**	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** relatório de revisão
			Processamento: • Elaborar comunicação a ser realizada ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça. Todos os incidentes graves deverão ser comunicados ao CPTRIC-PJ.
			Saídas: Comunicação ao CPTRIC-PJ

4.3.4 Descrição do subprocesso Executar Plano de Testes

Id	Atividade	Responsável	Descrição
4.10	**Planejar testes**	Divisão de Infraestrutura de TIC	**Entradas:** email de notificação e Manual de Execução do PCN
			Processamento: • Elaborar lista de procedimentos • Agendar e/ou reservar os recursos necessários • Informar eventuais stakeholders
			Saídas: planejamento dos procedimentos dos testes
4.20	**Revisar planejamento dos testes**	Divisão de Infraestrutura de TIC	**Entradas:** planejamento dos procedimentos dos testes
			Processamento: • Confirmar se a lista de procedimentos está adequada • Confirmar se os recursos agendados/reservados estarão disponíveis • Confirmar se os stakeholders estão cientes dos testes
			Saídas: planejamento revisado
4.30	**Executar testes**	Divisão de Infraestrutura de TIC	**Entradas:** planejamento dos procedimentos e Manual de Execução do PCN
			Processamento: • Executar os procedimentos planejados em alinhamento ao Manual de Execução do PCN • Produzir as evidências necessárias a comprovação dos testes • Ao final dos testes as evidências da execução deverão ser armazenadas em pasta compartilhada, ou anexadas nos chamados da ferramenta ITSM abertos
			Saídas: evidências de comprovação dos testes

4.3.5 Descrição do subprocesso Executar Plano de Backup

Id	Atividade	Responsável	Descrição
5.10	**Executar backup online**	Divisão de Infraestrutura de TIC	**Entradas:** não se aplica
			Processamento: procedimento automático configurado nos dispositivos
			Saídas: backup de dados em equipamentos redundantes
5.20	**Executar backup em**	Divisão de Infraestrutura de TIC	**Entradas:** não se aplica

	fita		**Processamento:** Procedimento automático configurado nos dispositivos
			Saídas: backup de dados em fita
5.30	**Restaurar backup**	Divisão de Infraestrutura de TIC	**Entradas:** requisição de serviço de restauração de dados de backup
			Processamento: • Executar os procedimentos conforme previsto no Plano de Backup e no Manual de Execução do PCN • Produzir as evidências necessárias a comprovação do resultado da restauração • Ao final da restauração as evidências da execução deverão ser armazenadas em pasta compartilhada, ou anexadas nos chamados da ferramenta ITSM abertos
			Saídas: restauração de dados e evidências de comprovação
5.40	**Verificar operacionalidade do backup**	Divisão de Infraestrutura de TIC	**Entradas:** e-mails automáticos enviados pelos dispositivos de backup ou aviso de pendência enviado pela Divisão de Proteção de Dados e Segurança da Informação
			Processamento: • Consultar os e-mails automáticos e avaliar se há registro de problemas na execução dos procedimentos Ou • Tomar as devidas providências para resolver a pendência informada pela Divisão de Proteção de Dados e Segurança da Informação
			Saídas: não se aplica

5 Tabelas RACI

5.1 Subprocesso Revisar Política de Gestão de TIC para a Continuidade de Negócios

	Atividade	Comitê de Segurança da Informação	Divisão de Proteção de Dados e Segurança da Informação
1.10	Elaborar PGTICN		**R**
1.20	Elaborar EGCN		**R**
1.30	Definir capacidade de recuperação		**R**
1.40	Elaborar o plano de contingência de TI		**R**
1.50	Elaborar o plano de backup e retenção de dados		**R**
1.60	Elaborar o plano de testes e ativação		**R**
1.70	Elaborar plano de comunicação		**R**
1.80	Elaborar escala de plantão	**I**	**R**
1.90	Elaborar o Plano de Continuidade de TIC		**R**
1.100	Consolidar a PGTICN		**R**
1.110	Homologar PGTICN	**R**	**C**
1.120	Expedir portaria	**I**	**R**
1.130	Informar servidores designados	**I**	**R**

Legenda: Responsável (R), Consultado (C) e Informado (I).

5.2 Subprocesso Monitorar Planos

	Atividade	Comitê de Segurança de Informação	Divisão de Proteção de Dados e Segurança da Informação
2.10	Avaliar notificações		**R**
2.20	Identificar pendências		**R**

Legenda: Responsável (R), Consultado (C) e Informado (I).

5.3 Subprocesso Executar Plano de Contingência

	Atividade	Grupo de Gestão de Crises Cibernéticas	Comitê de Segurança da Informação	Divisão de Proteção de Dados e Segurança da Informação
3.10	Diagnosticar		I	R
3.20	Executar Plano de Comunicação	I	I	R
3.30	Informar Polícia Judiciária	R	I	I
3.40	Acionar equipe de contingência			R
3.50	Executar procedimentos emergenciais			R
3.60	Executar procedimentos de contingência			R
3.70	Elaborar relatório de revisão	I	I	R
3.80	Enviar Comunicação ao CPTRIC-PJ	I	I	R

Legenda: Responsável (R), Consultado (C) e Informado (I).

5.4 Subprocesso Executar Plano de Testes

	Atividade	Divisão de Proteção de Dados e Segurança da Informação	Divisão de Infraestrutura de TIC
4.10	Planejar testes	I	R
4.20	Revisar planejamento dos teste	I	R
4.30	Executar testes	I	R

Legenda: Responsável (R), Consultado (C) e Informado (I).

5.5 Subprocesso Executar Plano de Backup

	Atividade	Divisão de Proteção de Dados e Segurança da Informação	Divisão de Infraestrutura de TIC
5.10	Executar backup online	**I**	**I**
5.20	Executar backup em fita	**I**	**I**
5.30	Verificar operacionalidade do backup		**R**
5.40	Restaurar backup	**I**	**R**

Legenda: Responsável (R), Consultado (C) e Informado (I).

6 Indicadores

6.1 Descrição dos Indicadores

Nome do indicador	**Índice de restaurações de backup realizadas com sucesso**
Origem	• COBIT 5.0 ○ DSS04 (Gerenciar Continuidade) ○ PAM outcome: DSS04-01 ○ PAM base practices: DSS04.BP1 e DSS04.BP7 ▪ Enabling process Key management practice: DSS04.01 e DSS04.07
Objetivo	Medir a disponibilidade de Informações críticas para o negócio
Meta	90%
Periodicidade	Semestral
Forma de cálculo	Nº de restaurações com sucesso / nº de restaurações previstas
Fonte	• Planilha do ANEXO I ○ Nº de restaurações com sucesso: ver o total da coluna "**Nº de restaurações realizadas com sucesso**" ○ Nº de restaurações realizadas com sucesso: ver o total da coluna "**Nº de restaurações previstas**"

Nome do indicador	**Índice de testes de recuperação com sucesso**
Origem	• COBIT 5.0 ○ DSS04 (Gerenciar Continuidade) ○ PAM outcome: DSS04-03 ○ PAM base practices: DSS04.BP3 e DSS04.BP4 ▪ Enabling process Key management practice: DSS04.03 e DSS04.04
Objetivo	Medir a eficácia dos planos de restauração
Meta	80%
Periodicidade	Semestral
Forma de cálculo	Nº de testes com sucesso / nº de testes previstos

Fonte	• Planilha do ANEXO II ○ Nº de testes com sucesso: ver o total da coluna "**Nº de testes realizados com sucesso**" ○ Nº de testes previstos: ver o total da coluna "**Nº de testes previstos**"

Nome do indicador	**Índice de revisões**
Origem	• DSS04 (Gerenciar Continuidade) • PAM outcome: DSS04-04 • PAM base practices: DSS04.BP1, DSS04.BP2, DSS04.BP4, DSS04.BP5 e DSS04.BP8 ○ Enabling process Key management practice: DSS04.01, DSS04.02, DSS04.04, DSS04.05 e DSS04.08
Objetivo	Medir as revisões do plano de continuidade para verificar se as efetivas necessidades do negócio estão atendidas num plano atualizado
Meta	75%
Periodicidade	Semestral
Forma de cálculo	Nº de revisões realizadas / nº de revisões previstas
Fonte	• Planilha do ANEXO III ○ Nº de revisões realizadas: ver a quantidade total de revisões registradas na planilha de controle ○ Nº de revisões previstas: ver o último valor registrado na coluna "nº de revisões previstas até o momento"
Observação	Acumular valores

7 Divulgação dos Resultados

Os resultados do processo serão demonstrados através dos indicadores de desempenho disponibilizados no site de Governança de TIC da Secretaria de Tecnologia da Informação e Comunicações, menu Indicadores, item Indicadores de Processos, processo Gerenciar Continuidade de TIC.

8 Anexo I – Índice de restaurações de backup realizadas com sucesso

Data do registro	Período da apuração	Nº de restaurações realizadas com sucesso	Nº de restaurações previstas

Onde:

- **Para cada apuração**
  - **Data do registro:** informar a data em que está sendo feito o registro
  - **Período da apuração:** informar o período a que se referem os valores apurados
  - **Nº de restaurações realizadas com sucesso**: informar o nº de restaurações com sucesso realizadas pelos responsáveis, conforme Manual de Execução do Plano de Continuidade e evidências registradas na pasta compartilhada
  - **Nº de restaurações previstas:** informar o nº de restaurações previstas, conforme Manual de Execução do Plano de Continuidade publicado no site de Governança da SETIC

9 Anexo II – Índice de testes de recuperação com sucesso

Data do registro	Período da apuração	Nº de testes realizados com sucesso	Nº de testes previstos

Onde:

- **Para cada apuração:**
  - **Data do registro:** informar a data em que está sendo feito o registro

- **Período da apuração:** informar o período a que se referem os valores apurados
- **Nº de testes realizados com sucesso**: informar o total de testes com sucesso realizados pelos responsáveis, conforme Manual de Execução do Plano de Continuidade e evidências registradas na pasta compartilhada
- **Nº de testes previstos:** informar o total previsto, conforme Manual de Execução do Plano de Continuidade publicado no site de Governança da SETIC.

10 Anexo III – Índice de revisões

Data do registro	Data das Revisões	Nº revisões realizadas até o momento	Nº revisões previstas até o momento

Onde:

- **Para cada revisão realizada:**
  - **Data do registro:** informar a data em que está sendo feito o registro
  - **Data da revisão**: anotar a data de publicação da revisão da política, plano ou processo (se houver)
  - **Nº de revisões realizadas até o momento: informar** o nº de revisões realizadas, conforme demonstrado pelas datas anotadas na coluna anterior
  - **Nº de revisões previstas até o momento:** anotar o nº previsto considerando a realização de 1 (um) revisão por ano